**Ph.D. Dissertation in Engineering**

# Cybersecurity Information Sharing Ecosystems:

## From the Perspective of Value Creation and Security Investments

**August 2019**


**Graduate School of Seoul National University**

**College of Engineering**

**Technology Management, Economics and Policy Program**

**Zahid Rashid**

## Abstract

# Cybersecurity Information Sharing Ecosystems:

## From the Perspective of Value Creation and Security Investments

Zahid Rashid

Technology Management, Economics, and Policy Program

College of Engineering, Seoul National University

Enterprises are employing a portfolio of security strategies to enhance their level of information security. Achieving an effective level of security in enterprises require investments in multiple information security strategies. These security strategies include cybersecurity information sharing, attack detection, prevention, vulnerability reduction, risk assessment, threat deterrence, education and training.

Although researchers have studied several areas of information security over the last few decades, but it is still considered as an uncertain area, which can pose very high level of risks to enterprises. The emerging complexity of information security reflects the fact that there are still a lot of issues to be investigated for sustainable security posture of enterprises. By reviewing the existing literature from the several areas of information security, we have identified two major research problems that are not fully addressed so far and

need further investigations. Therefore, this dissertation deals with these two main research problems and propose their solutions, respectively.

With respect to the first, this thesis investigates the stakeholder's value creation in cybersecurity information sharing ecosystems. The utilization of information for improving the security posture of organizations resulted in the evolution of cybersecurity information sharing ecosystems. There are five major types of stakeholders in cybersecurity information sharing ecosystems including cybersecurity solution providers, information providers, end users, government organizations and standardization bodies. These stakeholders obtain different values, their value creation is interrelated, and creating a complex value distribution system. The market is highly attractive for new entrants (i.e., solution and information providers), but their survival rate is very low and most of them disappear within couple of years. We have identified seven value parameters, which can simultaneously impact the values of stakeholders, forming a complex interdependency among the stakeholders. In order to better align the utilities and profits of stakeholders, understanding of value creation and distribution is a critical step forward to minimize the cost of security. There is a gap in determining the value creation and values obtained by stakeholders in cybersecurity information sharing ecosystem for formulation of business strategies and policies.

In this study, we investigated whether all the involved stakeholders in cybersecurity information sharing ecosystems are generating sufficient value. In addition, interrelationships among the stakeholders are also analyzed. The outcome of the study shows a model of value creation and distribution among

the stakeholders, and an another model to determine the effects of value parameters on the values obtained by stakeholders. Our simulation results show that, end users are the main source of value, and all stakeholders in the ecosystem mainly benefit from a growing installed base of end users. Further, the results show that in the current value creation model, the value of cyber security solution providers is higher than the information providers. In the saturated market, there is a risk of potential unsustainability of the value creation and distribution, due to the high prices of the cybersecurity solutions and information sources. The findings of this study have implications for business managers with respect to policy decisions related to the business models and pricing schemes for the cybersecurity solution providers and information providers.

With respect to the second research problem, this thesis investigate the issue of establishing justifications related to security investments within enterprises specifically for the cybersecurity information management systems. Several kinds of security tools are being employed in enterprises to enhance the cyber-attacks protection and detection abilities. In combination with these security tools, cybersecurity information management systems are utilized for managing the enterprise's internal and external cybersecurity information for improving the security situational awareness of the enterprises. Attaining an effective level of information security in enterprises, requires the availability of sufficient amount of funds. Therefore, for investments in any area of information security, the security managers have to provide appropriate justifications and a cost

benefit analysis for approval from the executive management and for the sanction of funds.

In the case of cybersecurity information management systems, formulation of investment justifications requires a systematic method that can bridge the performance evaluation and cumulative benefits of enterprises obtained from these systems. Using a system dynamics model, we analyzed the impact of investments in cybersecurity information management systems in terms of security cost, detection ability, cumulative benefits, attacker's value, successful attacks, prevented attacks and damage magnitude. The results suggest that these systems bring threefold benefits to the enterprises: (1) increase the level of information security; (2) reduction in operating cost of enterprise; and (3) significantly increase the cumulative benefits. The security managers can use this model to establish the foundation of justifications for investment in the cybersecurity information management systems and other security tools.

**Keywords:** Information Sharing, Cybersecurity, Ecosystems, Stakeholders, Value Parameters, Value Creation, Network Effects, Cybersecurity Information Management Systems, Security Investment Decisions, System Dynamics, Simulation

**Student Number:** 2016-38153

# Contents

# List of Figures

# List of Tables

# Chapter 1: Overall Introduction

## 1.1 Research Background

Today's societies are becoming more dependent on information and communication technology (ICT) due to increased automation and reliance on critical infrastructures such as telecommunication, financial services, transport and utilities (e.g. energy and water). Disruptions in critical services due to cyber-attacks cause potentially devastating impacts on societies. These disruptions can distract the functioning of governments, pose severe impacts on the environment, negatively affects the economy, and can have serious impact on the well-being and health of citizens (Zhao & White, 2017). Securing the emerging digital world is becoming a challenging task (Gordon, Loeb, Lucyshyn, & Zhou, 2015c). High diffusion of the internet has further enhanced threat landscape and increased the complexity to achieving the adequate level of information security. More advanced and collaborative approaches are required to handle the serious security situation in addition to currently available information security solutions such as access control systems, antivirus software, virtual private networks (VPN), firewalls, intrusion detection systems (IDSs) and content filters (Skopik, Settanni, & Fiedler, 2016).

Cybersecurity information sharing is one of the promising approach to get ahead of security threats and proactively prevent threats before they actually happen (Brown, Gommers, & Serrano, 2015; He, Devine, & Zhuang, 2018; Hernandez-Ardieta, Tapiador, & Suarez-Tangil, 2013; Skopik et al., 2016). The availability of updated cybersecurity information about ongoing cyber-attacks

and potential threats is a precondition for effective preparation, which can create an overall situational awareness picture about the information security. The information sharing is considered to be an effective approach to confront different information security scenarios including terrorism, cyber war, financially driven cyber-crimes, and hacktivism (Skopik et al., 2016). By receiving the precise information at the right time, enterprises can retain themselves up to date on recent information security issues and empower decision makers to reduce risks, deter cyber-attacks, and enhance resilience ([C], 2015; Skopik et al., 2016). Such cybersecurity information sharing decreases the threats detection time, increases the accuracy of threats detection and more effectively prevent the malicious behaviors within the systems.

Several other benefits can also be achieved by sharing the cybersecurity information including: reduced cyber risks, allow enterprises to closely work together for improving the level of cybersecurity at individual, national and global level ([C], 2015), reducing damage from cyber-attacks (Fleming & Goldstein, 2012), reducing cybersecurity incidents (Zheng & Lewis, 2015), increasing the response effectiveness (Zheng & Lewis, 2015) and reduced cost on cyber defense (Hausken, 2006, 2007; Praditya & Janssen, 2015).

The importance of collaborative cybersecurity information sharing has also been realized at the governmental levels and some countries have established the legal infrastructure for cybersecurity information sharing (e.g., European Union and United States). The regulatory landscape has already been established by developing several laws, strategies and policies to encourage the collaboration among different stakeholders ([C], 2015; [CD], 2015a, 2015b;

[DHS], 2016; [EC], 2013; [KCC], 2001; [NIS], 2016; [TWH], 2013, 2015). As a result, cybersecurity information sharing ecosystems have been evolved, comprising of several stakeholders including cybersecurity solution vendors, cybersecurity information providers, end users, government organizations and standardization bodies. Several open source and commercial cybersecurity solutions for instance "Threat Intelligence Platforms (TIP)" have been emerged in the market. Similarly, cybersecurity information is also available from open source feeds as well as from commercial venders (i.e., threat intelligence vendors and threat data feed providers). There are instances of cybersecurity information sharing among private organizations as well as between private and government organizations. Different types of information are being shared among stakeholders using different sharing models and mechanisms. In order to make the information sharing more effective, several organizations are involved in activities such as establishing standards and development of information sharing protocols.

The stakeholders in cybersecurity information sharing ecosystems obtain different values and their value creation is interrelated, which creates a complex value distribution system. In order to better align the utilities and profits of stakeholders, understanding of value creation and distribution is a critical step forward for sustainable cybersecurity information sharing ecosystems. Therefore, it is essential to analyze the value creations of stakeholders in cybersecurity information sharing ecosystems.

These ecosystems are anticipated to develop rapidly in the up-coming years due to the emergence of key technologies that are likely to cause major disruptions

in the society: such as (1) machine-learning, (2) artificial intelligence, (3) collaborative robotics, (4) cloud / edge technology, (5) big data, (6) virtual / augmented reality & next generation human machine interaction (HMIs), (6) internet of things, and (7) 3D printing. The European Cyber Security Organization (ECSO) pointed out that the security will be one of the top key challenge among the other challenges to the society and industry ([ECSO], 2018). According to Forbes Inc., it is estimated that the global cybersecurity market will be expanded rapidly and will reach up to $170 billion by 2020 (Ezrati, 2018). Similarly, the results of study conducted by IBM shows that the data breaches costs has increased significantly. In the year 2018, global average cost of a data breach is $3.86 million which is high by 6.4 percent than the previous year ([IBM], 2018). On the other side, Gatner Inc. reported that, with the increase by 12.4 percent, the expenses on information security services and products reached to around $114 billion in year 2018. They also forecasted that in 2019, the market is anticipated to grow at the rate of 8.7 percent and reach to $124 billion ([G], 2018).

Furthermore, the investment strategy for information security needs to be understood in depth for instance, investments in cybersecurity information management systems. Enterprises are employing a portfolio of security strategies to enhance their level of information security. These security strategies include the cybersecurity information sharing, attack detection, prevention, vulnerability reduction, risk assessment, threat deterrence, education and training. Each of these security strategies have different payoffs, effectiveness, and costs in the complex environment of information security.

The enterprises have to deploy their resources on a set of security strategies for effective management of information security. Different security tools, controls and measures are being used to implement the security strategies. For investments in these strategies and security tools, security managers have to provide justifications and a cost-benefit analysis for obtaining sufficient funds for investments in different areas of information security. The security investments bring several benefits to the enterprises (i.e., operational benefits, managerial benefits, tactical benefits, strategic benefits and organizational benefits) in addition to enhanced level of information security.

## 1.2 Problem Description

We have identified two research issues, the first issue is related to stakeholder's value creations in cybersecurity information sharing ecosystems and the second issue deals with the security investments decision making particularly related to cybersecurity information management systems.

The first research problem is related to the value creation of stakeholders in the cybersecurity information sharing ecosystems. In cybersecurity information sharing ecosystems, the process of stakeholder's value creation is highly interrelated and they obtain different values, which creates a complex value creation and distribution structure. Therefore, it is important to have clear understanding on how to better align the utilities and profits of stakeholders to minimize the costs incurred in achieving the effective level of security. The market of cybersecurity information is growing with more number of end users, cybersecurity solutions and information providers (Dey, Lahiri, & Zhang, 2014). Specifically, the market is highly attractive for new entrants (i.e.,

solution and information providers), but their survival rate is very low and most of them disappear within a couple of years (Dey, Lahiri, & Zhang, 2012).

It has been observed that, existing literature mostly covers special aspects such as technological aspects of cybersecurity (i.e., information sharing, quality of information, automation, standards and protocols (Skopik et al., 2016)), cybersecurity investments, incentives, public-private collaboration in cybersecurity information sharing (He et al., 2018; Praditya & Janssen, 2015; Zheng & Lewis, 2015). But, there is a gap in determining the value creation and values obtained by stakeholders in cybersecurity information sharing ecosystem for the formulation of business strategies and policies. Therefore, this research is conducted to determine the values that are generated for the involved stakeholders.

The second research problem is related to the enterprise's benefits realization due to the investments in cybersecurity information management systems. The cybersecurity information management systems are used to manage the multidimensional cybersecurity information received from multiple information sources. These systems provide the necessary functionalities and capabilities to convert the received information into valuable and actionable information.

In enterprises, along with several other tasks, the security managers are responsible for security technology selection and establishing the appropriate justifications for investment related to the selected technology (Nazareth & Choi, 2015; Whitman & Mattord, 2011). These justifications of investment are then communicated to the executive management for their approval and release

of funds. It is a fact that information security investments are difficult to justify and it is not always possible to prove returns on investments in the area of information security. The traditional approaches to calculate the return on information security investments (such as ROI, ROSI, ALE, NPV and ROA) are difficult to apply in the information security area, because these investments are not directly generating revenues or profits. Instead, the information security investments address mitigation of threats and loss prevention to the enterprise's assets (Robert Putrus & CFE, 2016). Further, the traditional methods of calculating return on information security investments are unable to quantify the intangible benefits such as organizational, strategic, operational, managerial and tactical benefits that it brings to enterprises.

## 1.3 Research Objectives

Considering the two research gaps identified, the dissertation has two research objectives, presented in two essays (chapter 3 and chapter 4). The two research objectives of this thesis are:

1) To model the structure of value creation and distribution among stakeholders in the cybersecurity information sharing ecosystems. This study will help in investigating whether all stakeholders obtain enough value when participating in the cyber security information sharing ecosystems.
2) To quantify the benefits that cybersecurity information management systems bring to the enterprises and help security managers to communicate with the executive management and support them in the investment decisions.

## 1.4 Research Questions

### 1.4.1 Value Creation in Cybersecurity Information Sharing Ecosystems

On the basis of the first research objective, four research questions have been defined:

1) How value is created in cybersecurity information sharing ecosystems?
2) How value is distributed among stakeholders?
3) How do the value parameters affect the values obtained by stakeholders?
4) How distribution of value changes in different situations?

The research questions related to the first research objective have been answered by identifying the stakeholders and value parameters in the cybersecurity information sharing ecosystems. Five types of stakeholders are identified (i.e., cybersecurity solution providers, cybersecurity information providers, end users, governmental organizations, and standardization bodies). Seven value parameters are also identified including install base (number of end users), quality of services (QoS), trusted communities, quality of information (QoI), trust on information sources, timeliness of information, and cost. The net value is explained by these value parameters for stakeholders, which is generated, from cybersecurity solutions and information in the cybersecurity information sharing ecosystems. Three additive utility functions are used to represent the values of stakeholders, which integrates all the value parameters. These utility functions allow the calculation of value creation and distribution throughout the ecosystems.

In this study, relative changes of values of stakeholders has been analyzed in the ecosystem having simulation technique using system dynamics methodology. Vensim software (Ventana Systems) is utilized for simulation which supports the system dynamics methodology ([VS], 2015).

### 1.4.2 Benefits of Investment in Cybersecurity Information Management Systems

Based on the second research objective, three research questions have been defined:

1) How investments in cybersecurity information management systems impact the security level of enterprises?
2) How cybersecurity information management systems enhance security and mitigate the risk of advanced cyber threats?
3) How cybersecurity information management systems are contributing to cumulative benefits to the enterprises?

To answer the questions related to the second research objective, we conducted the literature survey to analyze the features and capabilities of the cybersecurity information management systems. After that, we proposed a framework to analyze the benefits that these systems bring to the enterprises. The framework is majorly consisting of five categories of benefits: organizational, strategic, operational, managerial and tactical benefits. Subsequently, we developed a system dynamics based model incorporating the use cases of the cybersecurity information management system and the cumulative benefits they bring to the organization. Vensim software of Ventana Systems is utilized for simulation which supports the system dynamics methodology ([VS], 2015).

## 1.5 Contributions

The contributions related to the first research objective are the provision of a framework to evaluate the values obtained by stakeholders in the cybersecurity ecosystems. To the best of our knowledge, analysis of the values of all the stakeholders in the cybersecurity ecosystems is not well known, in fact there are several studies on the incentives and return on security investments, but these studies do not cover the overall picture of the cybersecurity information sharing ecosystems. This understanding is necessary, as a high level of cybersecurity is the need of the day. If sufficient revenues are generated for the cybersecurity solution and information providers, they will leverage innovation in the area of cybersecurity, which ultimately have positive impacts on the overall cybersecurity situation. The results of this research will help in specifying sustainable cybersecurity information sharing ecosystems, in which all the stakeholders can generate sufficient values. Furthermore, the business managers can improve the value exchange methods among the end users, cybersecurity solution and information providers.

The contributions related to the second research objective help in determining the benefits for enterprises to invest in cybersecurity information management systems. The issue of investing in cybersecurity information management systems is described using the framework of agency theory (Eisenhardt, 1989; Hill & Jones, 1992; S. A. Ross, 1973; Weill & Ross, 2004). The cumulative benefits of cybersecurity information management systems are modeled based on the utility maximization principles. Information security risk reduction &

cumulative benefits for enterprises are considered as justifications of investments in these systems.

## 1.6 Thesis Outline

The following thesis outline provides an overview of contents of the thesis, its flow, and presents an explanation of the contents. This thesis is composed of five chapters as shown in (***Figure 1)***. Besides providing a summary of the research presented in the different chapters of this dissertation, the (***Figure 1)*** also indicates the relationships between the different chapters.

The Chapter 2 is a state-of-the-art overview of cybersecurity information sharing ecosystems with particular focus on stakeholders, information sharing method & mechanisms, types of cybersecurity information, standards & protocols, laws, regulation, strategies and policies. In addition, this chapter also describes the state-of-the-art cybersecurity information sharing and management systems along with details about information sources, capabilities and target audience.

Chapter 3 (first essay) is designed to investigate the value creation, value distribution and the interdependency among the stakeholders of cybersecurity information sharing ecosystems. In particular, we demonstrate a value creation model for different types of stakeholders using the additive utility functions.

Chapter 4 (second essay) intends to investigate the organizational benefits that the cybersecurity information management systems bring to the enterprises by providing a framework for analyzing different types of the benefits. Furthermore, this research provides a tool to security managers for establishing

the justifications for investments in cybersecurity information management systems, which are aligned with the overall goals of their enterprises.

Finally, chapter 5 summarizes the analysis results by answering the research questions raised in introduction, addresses the implications and contributions, and finally ends with the limitations and future directions.

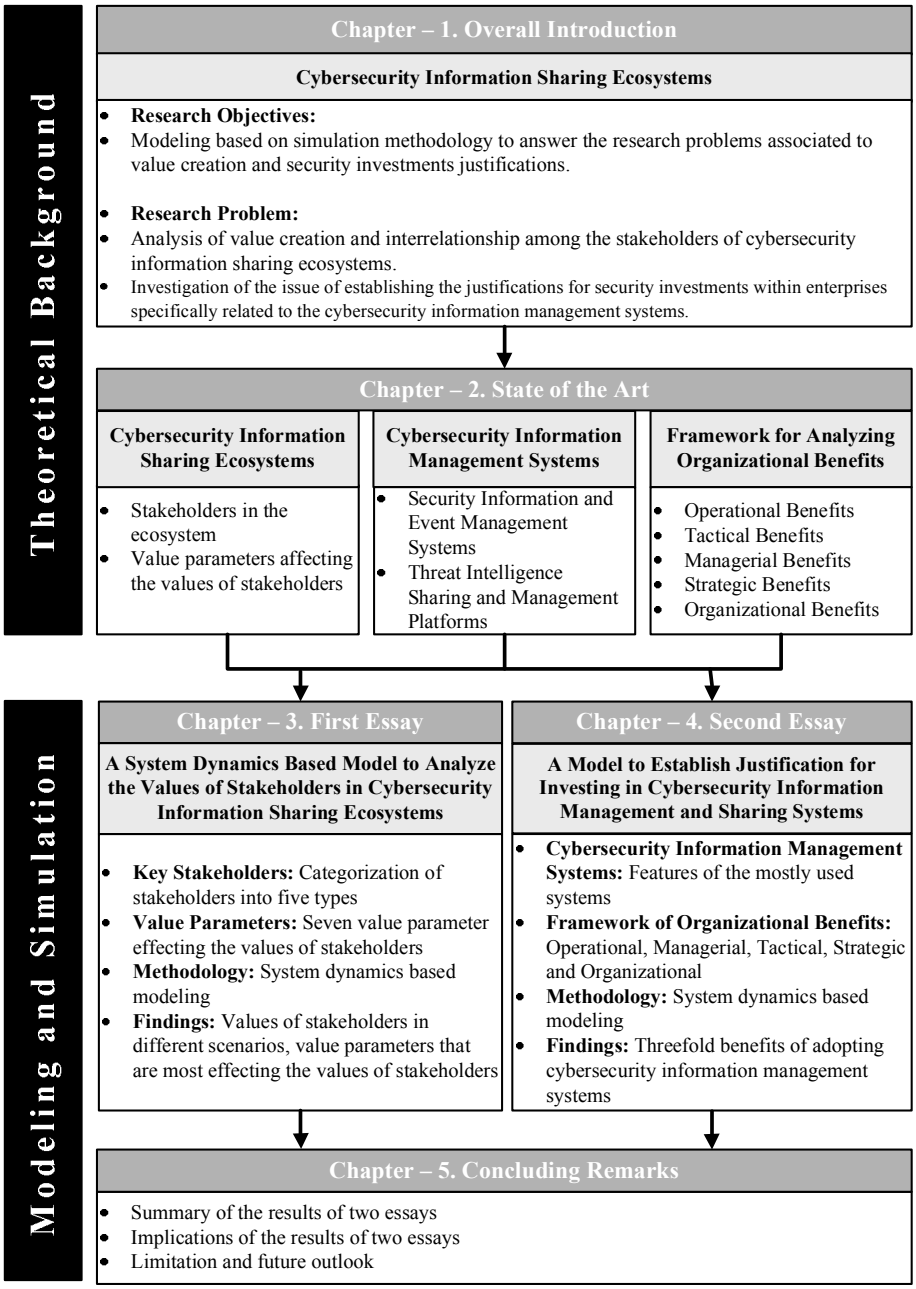



**Figure 1. Thesis Outline**

# Chapter 2: State-of-the-Art Review

This section presents the state-of-the-art review of cybersecurity information sharing ecosystems and cybersecurity information management systems.

## 2.1 Constructs of Cybersecurity Information Sharing Ecosystems

Stakeholders participate in these ecosystems, the value is created and distributed based on utilization of cybersecurity solutions, information sources and other related services. Cybersecurity is inherently dynamic, diverse and consist of a complex array of stakeholders which perform diverse activities and creates specialized ecosystems ([ETSI], 2017). The activities such as response, detection, and prevention are ongoing challenge that needs innovation and requires collaborative efforts to secure valuable digital assets in the enterprises. The increased connectivity through internet results in exposure to global cybersecurity threats which makes it difficult for individual enterprises to address full spectrum of cybersecurity issues and maintain resilience. The need for exchanging the cybersecurity information for supporting the management of threats, incidents, and vulnerabilities, as well as other cybersecurity activities has been felt by the cybersecurity professionals as wells as governments (Luc Dandurand & Serrano, 2013).

The sharing of cybersecurity information is emerged as an effective strategy to improve the cybersecurity posture (Luc Dandurand & Serrano, 2013; Garrido-Pelaz, González-Manzano, & Pastrana, 2016). Enterprises can leverage their capabilities, practical experiences and collective knowledge by getting

cybersecurity information from multiple information sources and gain more comprehensive understanding about ongoing and potential threats. The enterprises can utilize the shared cybersecurity information in threat informed decision making regarding detection techniques, mitigation strategies and defensive capabilities (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016). Enterprises receive cyber threats related information and utilize it for the control of threats spreading, which ultimately promotes a degree of protection to others. Additionally, sharing cybersecurity information allows enterprises to detect the targeted cyber-attack campaigns more effectively (Johnson et al., 2016).

The different stakeholders involved in the cybersecurity information sharing interact and perform several activities at different levels. The summary of overall cybersecurity information sharing ecosystem is mentioned in (***Figure 2)***.

The remainder of this section provides a detailed discussion about the stakeholders of the cybersecurity information sharing ecosystem and their relevant activities.

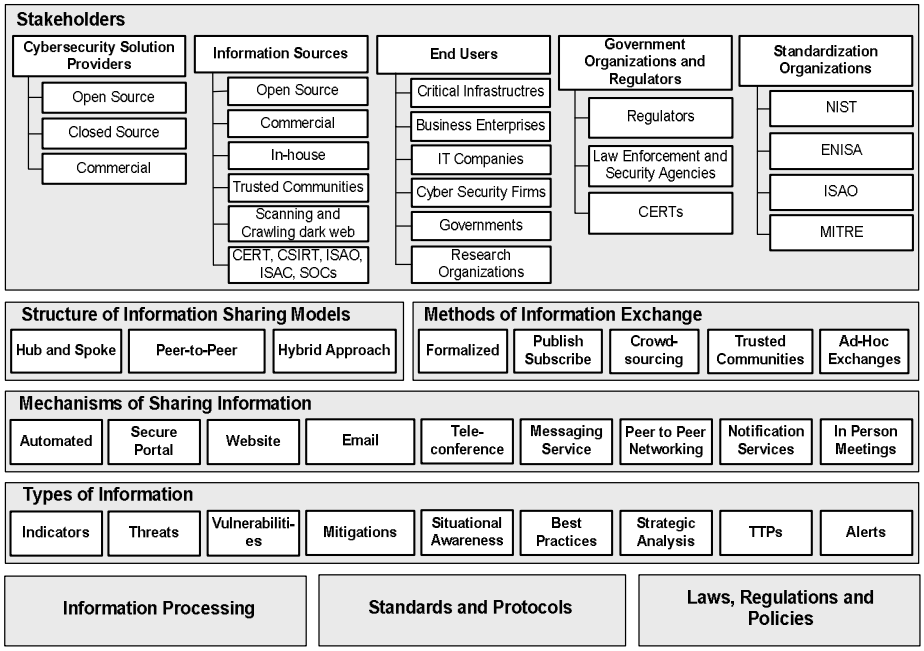



**Figure 2. Cybersecurity Information Sharing Ecosystem**

### 2.1.1 Stakeholders

Majorly five types of stakeholders are involved in cybersecurity information sharing ecosystems including cybersecurity solution providers, information providers, end users, government / regulatory organizations, and standardization organizations. These stakeholders have varying degree of goals, technical capabilities and have different motivations for acting in response of cybersecurity information. Each of these stakeholders have their own perspectives, interests, and needs that drives them to play their roles in the ecosystem (Goodwin et al., 2015). Some of these stakeholders are consumers, and others are producers of cybersecurity information while some of them are acting as both. The stakeholders such as governments organizations and regulators have the responsibility to establish a favorable environment which leverages the innovation and collaborations related to cybersecurity

information sharing ecosystems. The standardization organizations are working for establishing the standards and protocols through which the quality of shared information can be improved and it encourages automation in cybersecurity information exchanges.

#### 2.1.1.1 Cybersecurity Solution Providers

Several types of software solutions with varying capabilities are currently being used for consuming, storing, generating and sharing of cybersecurity information. These solutions include network traffic analysis tools, intrusion monitoring platforms, security information and event management systems (SIEM), open source and commercial cyber threat intelligence management platforms, cyber threat intelligence service provider, third-party visualization and reporting platforms, forensics platforms other security analytics platforms (Dave Shackleford, 2018). The survey reported by (Dave Shackleford, 2018) indicates a significant growth in the use of dedicated systems for managing cyber security information. These solutions are developed and provided by cyber security solution vendors under different types of licenses including open source, closed source or commercial. These solutions are in different forms such as dedicated platforms, APIs, API development kits, custom APIs, services, prebuilt connectors to content-oriented systems and third party integrators (Dave Shackleford, 2018).

#### 2.1.1.2 Information Providers

Cybersecurity threats related information is generated from several sources including open and commercial information sources. Antivirus vendors, computer forensics experts, IT security companies, and penetration testers,

collects cybersecurity related information from multiple sources and by adding value added services are sold to other stakeholders in the ecosystem (Goodwin et al., 2015). A lot of cybersecurity information is freely available from multiple sources such as open source intelligence (OSINT), public websites, repositories and blogs for instance National Vulnerability Database (NVD) ([NIST], 2014b), Open Sourced Vulnerability Database (OSVDB) ([OSF], 2014), Red Hat repositories ([RH], 2014), Japan Vulnerability Notes (JVN) ([JPCERT], 2014) and MITRE repositories ([MITRE], 2014f).

The cyber threat intelligence feeds (i.e., cybersecurity information) are streams of indicators or artifacts, with the goal of learning from other organization's experiences to improve the actionable response. Commercial feeds are generated by the security vendors and are available on payment basis while open source or free threat intelligence feeds are generated and distributed by non-profits entities and industry groups (e.g., FS-ISAC).

Commercial information providers are IT security companies, that actively generate variety of cyber threat intelligence, and they offer it either as a customer-specific report, a bundle of threat intelligence or software product, or as a premium threat feed. Many companies are selling threat intelligence within their commercial solutions. The cyber threat intelligence sharing is becoming a big market; as number of end users are significantly increased as compared to previous years (D Shackleford, 2018). Many big companies are already entered in the cyber intelligence sharing market for instance, IBM, CISCO, Dell Secure Works, McAfee, ThreatConnect, CheckPoint and Anomali (D Shackleford, 2018).

The trusted communities are also an important sources of highly relevant cybersecurity information that complements existing threat information capabilities such as National Detection Network (NDN) from the National Cyber Security Center (NCSC) in The Netherlands (Fransen, Smulders, & Kerkdijk, 2015) and Financial Services Information Sharing and Analysis Center (FS-ISAC) ([FS-ISAC], 2019). These communities or networks of organizations exchange threat intelligence amongst each other with the major role of connecting relevant stakeholders to collectively enhance the cyber resilience by taking appropriate measures to reduce the damage (Fransen et al., 2015). By participating in different cybersecurity information sharing communities and forums (i.e., public, private sharing communities, government repositories), the end users can get relevant information that meets their operational needs (Fransen et al., 2015).

The organizations internal information sources such as telemetry, IDS or SIEM also provide valuable information which is contextualized by comparing and correlation with the information received from the other external sources. The Computer Emergency Response Teams (CERTs), Information and Security Analysis Centers (ISAOs), CSIRTs, security operations center (SOCs) and ISACs are also issuing advisories and threat reports which are important sources of cybersecurity information. The other sources of cybersecurity information include human intelligence, honeypots, malware processing, crawling, darknets and scanning.

#### 2.1.1.3 End Users

The potential end users of the cybersecurity information can be the enterprises that are using digital technologies in their routine activities or in their business processes. Several enterprises are using cybersecurity information for improving their cybersecurity posture such as government organizations, critical infrastructures, IT companies, business enterprises, cybersecurity companies, and research organizations. The critical infrastructures such as telecommunication, banking, financial services, transport and utilities (e.g., energy and water) are heavily using digital technologies, and the updated cybersecurity information give them broader picture about the ongoing cyber threats. The chief information officers (CIOs), administrators (network & system), chief information security officers (CISOs), cybersecurity specialists, computer security incident response teams (CSIRTs), privacy officers, technical support staff, and computer security program managers in business enterprises and IT companies are utilizing the cybersecurity information because they are responsible for securing the sensitive information, such as customer data, trade secrets, contract information, and other intellectual property (Goodwin et al., 2015; Johnson et al., 2016). In order to cure existing vulnerabilities in software products, the software development companies distribute software update patches among their customers. Some IT companies share information about vulnerabilities of their products or services to security experts or security companies so that they can develop solutions for them (Goodwin et al., 2015). The research organizations and academic researchers are utilizing and generating information for recovering vulnerabilities in

software, hardware and other services (Goodwin et al., 2015) as well as to track the targeted attack campaigns and malwares.

#### 2.1.1.4 Government Organizations and Regulators

The governments have extensive role in reducing the cybersecurity risk to its citizens. In addition to duties related to national cybersecurity, governments have the responsibility to provide a collaboration environment, in which all relevant stakeholders of cybersecurity ecosystem work together to achieve a high level of cybersecurity of their assets. The leading role of governments in cybersecurity ecosystem is to define objectives, law enforcement, define ways to achieve them and clarify the roles and responsibilities of all the relevant stakeholders, improvements to its own cybersecurity, sharing its research and experience with all relevant stakeholders, and engaging in a public-private dialogue to obtain the suggestions from the industry. The establishment of robust regulatory framework includes the establishment of legal instruments (such as rules, regulations), development of cybersecurity policy & strategy, regulating the industry, instruments to enhance coordination (such as: public-private cooperation), cybersecurity readiness assessment & incident management and capacity building. The regulators are responsible for implementation of cybersecurity strategy, policy and regulations. Cybersecurity information sharing is one of the core activity in the overall cybersecurity ecosystem. The governments have already recognized its importance & benefits and have issued laws relevant to cybersecurity information sharing. Cybersecurity Incident Response Teams (CSIRTs) and Computer Emergency Teams (CERTs) are usually national-level organizations

including governmental and non-governmental institutions that provide a coordination and response functions ([CSIRT], 2019).

To improve the working relationships among the cross boarder CERTs in Asia, Asia Pacific Computer Emergency Response Team (APCERT) was established in which 15 CERTs from 12 courtiers are working together to improve the regional network security ([APCERT], 2019). Europe's TF-CSIRT ([APCERT], 2019) is an example of regional collaboration in cybersecurity information sharing. Besides regional level, there are efforts at international level to bring together the international stakeholder for improving the cybersecurity level. Forum of Incident Response and Security Teams (FIRST) is a global forum and premier organization, and is considered as a global leader in incident response ([FIRST], 2019). Hundreds of organizations around the globe are members of FIRST including government organizations, commercial, research institutes and other organizations. The basic aim of FIRST is to promote the coordination and cooperation at international level for incident prevention and encourage cybersecurity information sharing among members for stimulating rapid reaction to incidents ([FIRST], 2019).

#### 2.1.1.5 Standardization Organizations

In cybersecurity information sharing ecosystem, several organizations are working for standardizations of procedures, processes, data formats and protocols. The standardization efforts help in efficient and effective information sharing as well as these efforts enables the interoperable exchange of information between different implementations of open source or vendor

products. The details of organization along with their standards, protocols or specifications are mentioned in ***(Table 1)***.

**Table 1. Standards / Specifications / Protocols / Guidelines**

| Organization | Recommendation / Specifications / Protocols / Guideline | Reference |
|---|---|---|
| National Institute of Standards and Technology (NIST) | • Asset Reporting Format (ARF)<br>• Common Configuration Enumeration (CCE)<br>• Common Configuration Scoring System (CCSS)<br>• Common Platform Enumeration (CPE)<br>• Open Checklist Interactive Language (OCIL)<br>• Extensible Configuration Checklist Description Format (XCCDF)<br>• Common Vulnerabilities and Exposures (CVE)<br>• Open Vulnerability and Assessment Language (OVAL)<br>• eXtensible Configuration Checklist Description Format (XCCDF) | • (Halbardier, Waltermire, & Johnson, 2011)<br>• ([NIST], 2014a)<br>• (Scarfone & Mell, 2010)<br>• (Cheikes, Brant A., David Waltermire, 2011)<br>• (Waltermire David, Karen Scarfone, 2011)<br>• (Ziring, N., & Quinn, 2007)<br>• (Mell & Grance, 2002)<br>• (Banghart, Quinn, & Waltermire, 2010)<br>• (Waltermire, D., Schmidt, C., Scarfone, K., & Ziring, 2011) |
| International Telecommunication Union, Telecommunication (ITU-T) | • Common Attack Pattern Enumeration and Classification (CAPEC)<br>• Common Vulnerabilities and Exposures (CVE)<br>• Common Vulnerability Scoring System (CVSS)<br>• Common Weakness Enumeration (CWE)<br>• Malware Attribute Enumeration and Characterization (MAEC)<br>• Open Vulnerability and Assessment Language (OVAL)<br>• Cyber Security Information Exchange Framework (CYBEX) | • ([ITU-T], 2013)<br>• ([ITU-T], 2014a)<br>• ([ITU-T], 2011)<br>• ([ITU-T], 2012)<br>• ([ITU-T], 2014c)<br>• ([ITU-T], 2014b)<br>• (Rutkowski et al., 2010) |
| MITRE Corporation | • Common Event Expression (CEE)<br>• Common Result Format (CRF)<br>• Common Weakness Scoring System (CWSS)<br>• Cyber Observable eXpression (CybOX)<br>• Common Platform Enumeration (CPE)<br>• Common Configuration Enumeration (CCE)<br>• Common Attack Pattern Enumeration and Classification (CAPEC) | • ([MITRE], 2014b)<br>• ([MITRE], 2014c)<br>• ([MITRE], 2014d)<br>• ([MITRE], 2014e)<br>• (Buttner, A., & Ziring, 2009)<br>• ([MITRE], 2014a)<br>• (S. Barnum, 2008) |

| | | |
|---|---|---|
| | • Structured Threat Information eXpression language (STIX)<br>• Trusted Automated eXchange of Indicator Information exchange (TAXII)<br>• Malware Attribute Enumeration and Characterization (MAEC)<br>• Common Weakness Enumeration (CWE) | • (Sean Barnum, 2012)<br>• (Connolly, Davidson, & Schmidt, 2016)<br>• (Kirillov, Beck, Chase, & Martin, 2010)<br>• (Martin, 2007) |
| Int. Standards Organization (ISO) / Int. Electro-technical Commission (IEC) | • Software Identification (SWID) | • ([IOS-IEC], 2009) |
| Industry Consortium for Advancement of Security on the Internet (ICASI) | • Common Vulnerability Reporting Framework (CVRF) | • (Mike Schiffman, 2011) |
| Internet Engineering Task Force (IETF) | • Incident Object Description Exchange Format (IODEF) | • (Danyliw, Roman, Jan Meijer, 2007) |
| Institute of Electrical and Electronics Engineers (IEEE) | • Malware Metadata Exchange Format (MMDEF) | • ([IEEE ICSG], 2014) |
| Open Grid Forum | • Web Services Agreement Specification (WS-Agreement) | • (Andrieux, Alain, Karl Czajkowski, Asit Dan, Kate Keahey, Heiko Ludwig, Toshiyuki Nakata, Jim Pruyne, John Rofrano, Steve Tuecke, 2007) |
| Organization for the Advancement of Structured Information Standards (OASIS) | • eXtensible Access Control Markup Language (XACML) | • (Moses, 2005) |
| Forum of Incident Response and Security Teams (FIRST) | • Common Vulnerability Scoring System (CVSS) | • (Schiffman, M., Wright, A., Ahmad, D., & Eschelbeck, 2004) |
| Industry Consortium for Advancement of Security on the Internet (ICASI) | • Common Vulnerabilities Reporting Framework (CVRF) | • (M. Schiffman, 2011) |

| | | |
|---|---|---|
| European Network and Information Security Agency (ENISA) | • European Information Sharing and Alert System (EISAS)<br>• Cyber Defense Data Exchange and Collaboration Infrastructure (CDXI) | • (Pawlinski, P., Jaroszewski, P., Urbanowicz, J., Jacewicz, P., Zielony, P., Kijewski, P., & Gorzelak, 2014)<br>• (L. Dandurand, 2010) |
| MANDIANT | • Open Indicators of Compromise Framework (OpenIOC) | • (Pawlinski, P., Jaroszewski, P., Urbanowicz, J., Jacewicz, P., Zielony, P., Kijewski, P., & Gorzelak, 2014) |
| Verizon | • Vocabulary for Event Recording and Incident Sharing (VERIS) | • (Pawlinski, P., Jaroszewski, P., Urbanowicz, J., Jacewicz, P., Zielony, P., Kijewski, P., & Gorzelak, 2014) |
| United States Computer Emergency Readiness Team (US-CERT) | • Traffic Light Protocol (TLP) | • (Pawlinski, P., Jaroszewski, P., Urbanowicz, J., Jacewicz, P., Zielony, P., Kijewski, P., & Gorzelak, 2014) |
| European Telecommunications Standards Institute (ETSI) | • Information Security Indicators (ISI) | • (Pawlinski, P., Jaroszewski, P., Urbanowicz, J., Jacewicz, P., Zielony, P., Kijewski, P., & Gorzelak, 2014) |
| Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) | • Collective Intelligence Framework (CIF) | • (Pawlinski, P., Jaroszewski, P., Urbanowicz, J., Jacewicz, P., Zielony, P., Kijewski, P., & Gorzelak, 2014) |

### 2.1.2 Structure of Information Sharing Models

The ISAO standards organization and MITRE has described three basic cybersecurity information sharing models ([ISAO], 2016; Bruce J. Bakis, 2017) hub-and-spoke, peer-to-peer and hybrid models. In the peer-to-peer sharing model, any member of the community can interact and share information with any or all other members without passing through a central hub. The information dissemination is faster and inexpensive because there is no cost involved related to central hub. This sharing model is beneficial for small communities where the trust relationship is asymmetrical and sharing of

information is based on dynamic conditions such as contents, current threat, and so on. There are no value addition services available centrally in peer-to-peer sharing model. This model is more suitable for information flow scenarios where information is directly collected and analyzed by the members.

The hub-and-spoke sharing model incorporates a central hub which collects information from members (spokes) and disseminate it to the community. The hub can either redistribute the information directly or after value addition more useful information is disseminated to community members. The hub receives information from members at central location which makes it easy to process, filter, analyze and correlate relevant information for greater analytic insights. The entire sharing model is based on the central hub which makes the system vulnerable to delays and system failures. In some scenarios, the timeliness of information is very important therefore delays in distribution can reduce the benefits of the information-sharing mechanism. The costs incurred by the value addition services make this model expensive than peer-to-peer information sharing model. If the community members have to bear these costs than it precludes several members to join the information sharing community. In addition, hub-and-spoke model requires a high level of trust of members on the hub.

In addition to above discussed sharing models, the characteristics of above two sharing models are combined together in one model and is named as hybrid model. The hybrid sharing model is useful in scenarios where some time-sensitive information needs to be disseminated instantly to all members or some of the members and trying to avoid the delays at central hub. While in scenarios,

when some value addition or vetting of information is required than sharing information through hub is more feasible.

### 2.1.3 Methods for Information Exchange

The cybersecurity information exchange methods are usually based on unidirectional or bidirectional information sharing schemes. In unidirectional information exchange method, one entity produces information and shares with other stakeholders in the ecosystem e.g. open source threat intelligence. While in bidirectional information exchange the intelligence is consumed as well as produced and shared with other stakeholders in the ecosystem for instance joining ISAC or government sharing program. The methods of exchange are mostly directed by community requirements and concepts of operations. The ISAO standards organization describes publish-subscribe and crowdsourcing as two methods for information exchange ([ISAO], 2016). These information exchange methods can be applied to any of information sharing models. In the publish-subscribe information exchange method, a producer publishes information on a regular or irregular basis, and its publications are individually subscribed to by one or more community members. The crowdsourcing information exchange method is suitable when participants collectively contribute to a discussion thread, or an automated cyber threat information sharing repository, or other systems to transform granular threat data into more coherent threat intelligence.

### 2.1.4 Mechanisms for Sharing Information

The cybersecurity information is shared in the ecosystem using the formal and informal information sharing mechanisms. The formal sharing mechanisms

include the automated sending and receiving of information using specialized tools such as Threat Intelligence Platforms (TIPs) and Security Information and Events Management systems (SIEM). In the automated mechanisms, threat intelligence information is represented in structured manner and is shared among trusted partners and communities in a machine processing structure ([ISAO], 2016). The automated mechanisms also include the notification services, which generate and send messages to users or other applications that have subscribed to the service ([ISAO], 2016).

Most of the organizations are still using the informal mechanisms such as phone calls, email, chat, social media platform or in person meetings, to enable collaboration and information sharing. These sharing mechanisms are suitable for ad-hoc participants because of its minimal cost. Many organizations are using the information sharing mechanisms including in person meetings, tele-conferencing, email (general, encrypted message, list servers), messaging services, websites and secure portals.

The information sharing mechanisms are selected based on requirements of the stakeholders and communities in the ecosystem such as timeliness, quality and sensitivity of information.

### 2.1.5 Information Types

Cybersecurity information consists of information related to cyber threats that might help enterprises to protect themselves and detect malicious activities (Johnson et al., 2016). Several types of information are being shared and each type of information is used for its specific purpose. It is necessary to have sufficient information for planning and analyzing the cybersecurity, and

offering incentives for enhanced security. Different types of cybersecurity information are required by stakeholders in government and private sectors to assess the risk to cybersecurity at organizational level or at national level, including the risk to critical infrastructures (Goodwin et al., 2015). Several other types of information can be used for incident identification & analysis, detection of cyberattacks, and analysis of incidents to determine the objectives of attackers (Goodwin et al., 2015). Major types of cybersecurity information include security alerts, best practices, list of vulnerabilities & mitigations, security tools configurations, tactics-techniques and procedures (TTPs), indicators, threat intelligence reports, incidents, situational awareness, and strategic analysis (Goodwin et al., 2015; Johnson et al., 2016; Luiijf & Klaver, 2015).

#### 2.1.5.1 Indicators of Cyber Threats

Indicators are utilized to defend, analyze and detect potential cyber threats and vulnerabilities. Indicators are observables (malicious events on a system or network) or technical artifacts that can forecast about the potential upcoming or currently ongoing cyber-attacks. It consists of information such as malicious file hashes, command and control IP addresses, phishing e-mails, malicious email message's subject text, suspicious domain names, uniform resource locator (URL) refereeing to malicious contents and others ([ISAO], 2016; Johnson et al., 2016). In addition, the indicators may also include the contextual information which help end users to determine whether an indicator is relevant to them or not. The context information answers the questions such as how to

handle the indicator? what is the valid time window of the indicator? what are the related incidents, threat actors, and campaigns ([ISAO], 2016)?

#### 2.1.5.2 Tactics, Techniques and Procedures (TTPs)

Tactics, techniques, and procedures (TTPs) represent a broad set of information that is used to describe the behavior and capabilities of the attackers or attack campaigns ([ISAO], 2016; Johnson et al., 2016). The tactics are high-level descriptions of behavior of attackers or actors. Detailed descriptions about the malicious actor's behavior contextualized with their tactics are called techniques. In addition, detailed descriptions (at low level) in the context of their techniques are called procedures (Johnson et al., 2016). TTPs includes the information such as specific adversary behaviors, actor's propensity to use a particular variant of malware, resources leveraged, attack tools, delivery mechanism or exploit, order of operations, target victim information, and the vulnerabilities or weaknesses being targeted ([ISAO], 2016; Johnson et al., 2016). The aggregated information related to campaigns are strategic in nature which are used to inform situational awareness and support decision making activities ([ISAO], 2016).

#### 2.1.5.3 Security Alerts and Advisories

Security alerts are human readable high level briefs, technical notifications and other relevant information related to security issues (Johnson et al., 2016). Some other terminology also being used for security alerts such as vulnerability notes, security advisories and security bulletins. The sharing of security alerts and advisories are providing immediate, tactical, and strategic information to impact decision making and support in taking protective measures ([ISAO],

2016). The security alerts are issued by several organizations in public and private sectors for instance CERTs, ISACs, cybersecurity research organizations and commercial security service providers ([ISAO], 2016; Johnson et al., 2016).

#### 2.1.5.4 Cyber Threat Intelligence Reports

Cyber threat intelligence reports contain information ranging from high-level trending reports to detailed analysis of specific campaigns ([ISAO], 2016). These reports provide greater situational awareness to stakeholders by describing indicators, TTPs, threat actors, campaigns, targeted systems & information, and other relevant information. The cyber threat intelligence reports provides the necessary contextual and enriched information that support the decision-making processes (Johnson et al., 2016). Some reports are the result of several years of analysis and tracking of cyber threats ([ISAO], 2016). Government organizations and commercial vendors publish various reports regularly and contains information about specific incidents and describe the updated state of cyber threat landscape.

#### 2.1.5.5 Cybersecurity Tools Configurations

Sharing of operational cybersecurity practices is an important way to collaborate and build trust, learn from each other's experience and collect feedback on cybersecurity practices ([ISAO], 2016). Operational cybersecurity practices include effective (recommended) configurations and settings for cybersecurity related systems (Johnson et al., 2016). It may also contain information such as effective architectures, effective or ineffective system

configurations, manning strategies and other similar type of information ([ISAO], 2016).

#### 2.1.5.6 Incidents Information

The incidents information is detailed information about the attempted or successful attacks which are discovered while investigating or responding to a cybersecurity incident ([ISAO], 2016; Goodwin et al., 2015). Incident information sharing can enable large scale analysis to uncover adversary trending across the cybersecurity ecosystem ([ISAO], 2016). The details of information in incident information sharing varies and depend on sensitivity of information which have financial and reputational impact as well as other concerns. In majority of scenarios the incidents information may include: description of information lost, impact assessment, temporal information, relevant indicators, TTPs, suspected intents, response actions, log of actions taken and other ([ISAO], 2016; Goodwin et al., 2015).

#### 2.1.5.7 Vulnerabilities

Vulnerability information include details about the vulnerabilities in software, hardware, business process, specific systems or infrastructure, or general classes of vulnerabilities that can be exploited for malicious purposes ([ISAO], 2016; Goodwin et al., 2015). Several organizations and vendors are regularly publishing vulnerability information related to their products and services. The vulnerability information provides the situational awareness and suggests the immediate response actions in the case of recently discovered high-severity vulnerabilities in exposed systems ([ISAO], 2016).

#### 2.1.5.8 Information related to Courses of Action

Courses of actions are specific methods & measures for responding to cyber-attacks, mitigating threats, vulnerabilities and procedures for recovering from incidents. The course of actions include several types information such as software patches, antivirus updates, specific IP address for blocking, and instructions to block malicious activities on the networks ([ISAO], 2016; Goodwin et al., 2015; Johnson et al., 2016).

#### 2.1.5.9 Information about Campaigns

The information about campaigns relates intended effects of an adversary or group including employed tools, related threat actors, associated incidents, and other relevant campaign's information ([ISAO], 2016). These types of information have a key role in developing a comprehensive understanding about the potential threats as well as specific objectives and capabilities an adversary or group has employed. The information about campaigns is strategic in nature and used to inform situational awareness and decision making activities ([ISAO], 2016).

#### 2.1.5.10 Information about Threat Actors

Malicious individual (s) or group (s) who are responsible for malicious activities, events or incidents that has potential impact on the safety and security of other stakeholders are termed as "threat actor". Threat actors can be categorized or grouped on the basis of their goals, intentions, motivation, and capabilities. Commonly, four groups of threat actors are mentioned in the literature: cybercriminals, hacktivists, cyberterrorists, and state-sponsored actors (Ablon, 2018).

Characteristics and the specific objectives of threat actors are very important to understand for all the stakeholders of the ecosystem. The information such as name, affiliation, region of operation, description, relationship, capability, motives, intentions, target asset, target victim, and objectives helps to understand the characteristics of threat actors (Irwin, 2014). The sharing of threat actor's information among stakeholders can help to establish a complete picture and understanding of the potential threats.

#### 2.1.5.11 Threat Data Analysis

The cyber threat data is converted into threat intelligence by passing through several steps such as collection, aggregation, normalization, transformation, enrichment, contextualization, de-duplication, correlation, prioritization, data analytics, machine learning algorithms, visualization, privacy preserving and sharing. Several available threat intelligence platforms provide these types of functionalities for processing of threat intelligence data received from several sources ([A], 2019; [TC], 2018; [TQ], 2019b, 2019a; Wagner, Dulaunoy, Wagener, & Iklody, 2016).

### 2.1.6 Information Processing

The data science can play an important role in automation of analyses, pattern detection, or prediction during the threat intelligence generation. The size of threat data is growing very rapidly having millions of indictors, therefore, big data analytics techniques are highly suitable for automated analysis. The most commonly used data science techniques in threat intelligence includes the probability & statistics, supervised & un-supervised techniques, natural language processing and knowledge graph representation.

### 2.1.7 Standards and Protocols

Standards and protocols have a key role in automation of cybersecurity information sharing and enable information exchange between different implementations of open source and vendor products. The use of standards and protocols augment information processing, transformation, correlation, enrichment and analysis (Johnson et al., 2016). The use of standard processes and procedures makes the cybersecurity information sharing more effective among the communities from different geographical regions. The commonly used recommendations, specifications, protocols and guidelines in the area of cybersecurity information sharing is summarized in ***(Table 1)***.

### 2.1.8 Legal Framework

Several countries have already established the legal framework in order to promote the cybersecurity information sharing. For Instance, the United States has issued the "Cybersecurity Information Sharing Act (CISA)" along with the guidance document to assist enterprises that share information with the federal government ([C], 2015; [DHS], 2016). In addition to CISA act, Executive Orders such as ([TWH], 2013, 2015) also provide the legal basis for the sharing of cybersecurity information sharing.

The European Union cybersecurity strategy ([EC], 2013) and network and information system directive ([NIS], 2016) laid the foundations to encourage the cooperation to improve the cybersecurity at public and private sector organizations at national & international level. These documents ensure that all the relevant stakeholders should share the cybersecurity information among themselves.

The South Korean government also issued an act ([KCC], 2001), which encourage the promotion of cooperation related to cybersecurity information sharing.

Similarly, the government of Japan has issued the cybersecurity Act ([CD], 2015a) and strategy ([CD], 2015b) which give the basic legal infrastructure for the cybersecurity information sharing.

## 2.2 Cybersecurity Information Management Systems

The role of information security is becoming more significant due to swift increase in the spectrum of cyber threats in the enterprises. To achieve high level of information security, it is not enough for enterprises to rely only on traditional security solutions to mitigate specific threats, perimeter and end point security controls (Bhatt, Manadhata, & Zomlot, 2014). In the area of information security, working in silos drives significant gaps in detecting & preventing exploitation. Therefore, several attacks remained unobserved until substantial harm has already been occurred. To effectively mitigate security threats, enterprises must combine dispersed security efforts into a consolidated and cohesive effort.

For the prevention, detection, monitoring and mitigation of the sophisticated threats, enterprises are investing in the advanced cybersecurity information management and sharing technologies which can enhance their capabilities of securing data and networks infrastructure. For this study, we selected the two types of cybersecurity information management systems based on the mostly used systems mentioned in the market surveys (Barahona, 2017; D Shackleford, 2018). Specifically, we will investigate how "Security Information and Event Management - (SIEM) (Bhatt et al., 2014; Di Sarno, Garofalo, Matteucci, & Vallini, 2016)" and "Threat Intelligence Management and Sharing Platforms - (TIP) (Sauerwein, Sillaber, Mussmann, & Breu, 2017)" bring values and increase the obtained benefits to the enterprises.

### 2.2.1 Security Information and Event Management Systems (SIEM)

In the enterprises, huge amount of security related information is generated in the form of log files during the monitoring of IT assets (such as networks, application servers, database servers and user accounts management), perimeter security controls (such as intrusion detection systems (IDS), firewalls & intrusion prevention systems (IPS)) and endpoint security controls (such as antiviruses). The security information originating from multiple sources has different formats because each security control is using their vendor-specific schema. It is very difficult to correlate security information and events in the presence of large number of IT assets and security controls from different vendors (Bhatt et al., 2014; Di Sarno et al., 2016; Inns, 2014). SIEM systems were designed for collection, normalization, correlation, and storing the normalized security related information into the enterprise's centralized system (Bhatt et al., 2014; Di Sarno et al., 2016). It is a combination of formerly two heterogeneous systems - security event management system (SEM) and security information management system (SIM) (Di Sarno et al., 2016). The SEIM system utilizes the research from several fields such as data warehousing, data mining, statistics, distributed data, behavioral analytics, intelligent systems and machine learning (Dorigo, 2012; Warnecke, 2013). In addition to commercial, several open source SIEM systems are also available in the market for instance, ([OSSIM], n.d.).

The information received into the SEIM system from log files of the installed software and hardware devices in the enterprises network infrastructure is

utilized for monitoring, regulatory compliance confirmation and to evaluate the level of security. The SIEM system collects the information i.e. event and logs in real time from the assets being protected in the network. There are several protocols available (such as OPSEC, SNMP and Syslog) for transferring log data from information sources to a SIEM system. Agents are used to translate the different formats of log information into a common data format that is recognized by a SIEM system (Di Sarno et al., 2016). The agents can also provide the functionality to filter the log information to prevent the transfer of irrelevant information into the SIEM system to optimize the storage space, network bandwidth, and processing resources of SIEM system (Di Sarno et al., 2016). The received information is aggregated, normalized, enriched, indexed, correlated and stored permanently into the SIEM system (Bhatt et al., 2014; Coppolino, D'Antonio, Formicola, & Romano, 2016; Di Sarno et al., 2016; Dorigo, 2012; Miller, 2011). The historical data in combination with the real time network data is utilized for several other features or use cases (Williams, 2006). The SIEM system provides the added knowledge and situational awareness of the enterprise's network and all the devices connected to it (Warnecke, 2013). This knowledge can be utilized for real-time detection and elimination of threats, security posture improvement, trend visualizations, regulations compliance monitoring and reporting (e.g. HIPAA, PCI/DSS, HITECH, ISO, SOX, GDPR and others), information security policy management, assist in forensic or diagnostic investigation, automation of security operation centers (SOC) and other security operations (Warnecke, 2013). One of the major benefit of centralized SIEM systems is the centralized

management of security information, and leverage automation by reducing the burden of manual data sharing, compliance reporting and audits.

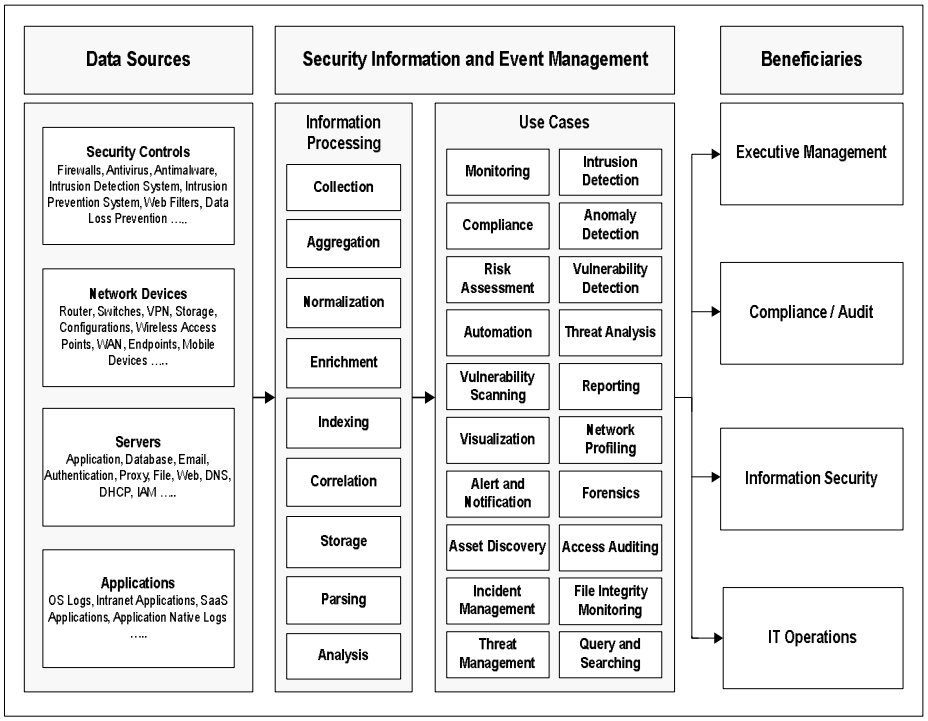



**Figure 3. Security Information and Event Management System**

This approach reduces the mean time to identify threats near to real time as well as reducing the mean time of remediating threats. The other benefits of properly adopting the SIEM systems include the comprehensive visibility of enterprise' security posture, network, endpoints, data and applications. SIEM systems can provide the actionable contextual intelligence by correlating the events across the end points and applications. In addition, the SIEM systems has the potential to reduce the IT security operation costs and optimize the existing security investment. Furthermore, investments in the SIEM system exhibits the potential to enhance the efficiency of the security teams and can significantly improve the return on security investment (RoSI) due to advanced offerings of

capabilities (Warnecke, 2013). ***(Figure 3)*** represents the detailed illustration about the SIEM systems.

The stakeholders in the enterprises which can directly getting benefits from the SIEM systems includes the executive management, audit and compliance teams, security operation teams and IT operations department. The managers of the enterprises can get real time automated generated reports from the SIEM system consisting of executive summaries and other valuable information for decision making. These types of features significantly increase the knowledge of the managers about their enterprises regarding the devices, tools and services available on the network (Warnecke, 2013). The management of enterprises can assure the regulatory compliance and evaluate the return on investment (ROI) by utilizing the knowledge produced by the SIEM systems (Warnecke, 2013). The SIEM systems can assist the audit teams and compliance monitoring teams to assess the real time situations (Dorigo, 2012; Warnecke, 2013).

The information security tasks in enterprises are becoming difficult due to swift increase in advanced cyber threats, complexity of IT systems, as well as adoption of emerging technologies such as cloud, IoT, mobile, and social media. In this situation, the efficiency of security operation teams heavily depends on security data analytics, behavior analytics, forensic capabilities, advanced visualizations, access to actionable cyber threats intelligence, enterprise networks and systems awareness, and effective procedures to coordinate response in the enterprises (Bhatt et al., 2014). The SIEM systems provide necessary features to information security teams which can leverage their capabilities to analyze security information and strength the discovery

of security breaches (Bhatt et al., 2014; Di Sarno et al., 2016). The use of SIEM systems brings several benefits to IT operation teams including quick root cause analysis, reduced mean time to recover, enterprise level operational visibility and IT resources and applications monitoring.

The enterprises invest in the SIEM systems depending on their requirements. Some enterprises implement the SIEM system because of the regulatory requirements while others are required to develop and maintain a SIEM solution to enhance the security of their data and IT infrastructure. Even though, the SIEM solutions offer several benefits, yet many organizations fail to get the best value from these systems because of its implementation cost, time, complexity, operational & maintenance challenges, limited security budget, limited skilled manpower and total cost of ownership (Bhatt et al., 2014; Warnecke, 2013).

### 2.2.2 Threat Intelligence Management and Sharing Platforms (TISP)

In enterprises, the information security teams are gathering cybersecurity information internally as well as from external information sources to protect their IT infrastructure from the potential cyber threats and attacks (Brown et al., 2015). The information security teams are also sharing the cybersecurity information in the communities to exploit the collaboration opportunities (Luc Dandurand & Serrano, 2013). The exchange of cybersecurity information is becoming necessary for supporting timely decision-making and automated response to cyber-attacks. Further, the exchanged cybersecurity information can also be utilized for the management of vulnerabilities, threats, incidents,

and other relevant information security activities (Luc Dandurand & Serrano, 2013).

The trend of cybersecurity information exchange pushed the enterprises to formulate and implement their threat intelligence programs with the goals to generate cyber threats intelligence for embedding into enterprise's workflows which can serve decision makers ([ENISA], 2017). The threat intelligence programs support the enterprises to collect cybersecurity information, analyze, transform into actionable intelligence and integrate it with external intelligence ([ENISA], 2017).

Efficient information management and sharing systems are required that can support the utilization of cybersecurity information in an effective manner (Brown et al., 2015). In year 2000, (Edwards, Migues, Nebel, & Owen, 2002) first proposed such a system to collect, analyze, and distribute cybersecurity information. It was proposed that this type of system will be in place among other existing systems of the enterprise. This system will store data feeds from several sources, filter, categorize and eliminate redundant data. This information will be prioritized, and finally distributed to different stakeholders (Edwards et al., 2002). (Luc Dandurand & Serrano, 2013) also presented the concept of TISPs, they also describe the major requirements which includes: (a) facilitate information sharing and collaboration, (b) enable and promote automation, and (c) facilitate the generation, refinement and vetting of data. (Serrano, Dandurand, & Brown, 2014) discussed the issues of the existing cybersecurity information sharing systems and proposed solutions that meets the specific requirements in this domain including legal framework, privacy,

data ownership, mapping among different formats of data, data protection policies and controlled sharing of information in the communities. Considering these requirement a new technology discipline of TISPs were emerged for improving their cyber threat intelligence capabilities and provide supports to enterprise's threat intelligence programs ([ENISA], 2017). For instance, Splunk enterprise security developed a threat Intelligence framework which provide different mechanisms for generating and consuming of cybersecurity related information as well as for managing threat feeds, detecting threats, and alerting ([SPLUNK], n.d.). This framework enables the exploration of incidents data in real time, providing the capabilities of incident investigations, leverage the proactive defense and quick reports generation.

A variety of information sources provide the cyber threats intelligence such as open-source intelligence (OSINT), commercial sources, public websites, repositories and blogs which contain information at different levels and covering multiple timescales (Brown et al., 2015). The cybersecurity information feeds are streams of data (i.e. indicators or artifacts), threat actor's information, motivations of attackers, methods of attacks, characteristics and other relevant human intelligence. The cybersecurity information can also be collected through a variety of devices over the network such as sensors and other network log information. In addition, several sources in the deep web also provides relevant information about the cybersecurity. All this information is utilized in sense making about the updated cybersecurity situation by learning from others experiences with the ultimate goal of strengthen the security and preparation for actionable responses (Brown et al., 2015). The cyber threats

intelligence feeds are available from both types of sources i.e. free and paid. Free intelligence feeds are generated by non-profits organizations while paid feeds are from the security vendors.

The trusted communities are also an important sources of highly relevant cybersecurity information that complements existing threat information capabilities such as National Detection Network (NDN) from the National Cyber Security Center (NCSC) in Netherlands (Fransen et al., 2015), and Financial Services Information Sharing and Analysis Center (FS-ISAC) ([FS-ISAC], 2019). These communities or networks of organizations exchange threat intelligence amongst each other with the major role of connecting relevant stakeholders. The communities collectively put efforts to enhance the cyber resilience by taking suitable measures to reduce damages and prevent their assets (Fransen et al., 2015). By participating in different cybersecurity information sharing communities and forums (i.e., public, private sharing communities, government repositories), the end users can get highly relevant information that can meet their operational needs (Johnson et al., 2016).

The organizations internal information sources such as telemetry, IDS or SIEM also provide valuable information which is contextualized by comparing and correlation with the information received from other sources. The Information and Security Analysis Centers (ISAOs), Computer Emergency Response Teams (CERTs), CSIRTs, security operations center (SOCs) and ISACs are also issuing advisories and threat reports which are important sources of cybersecurity information. The other sources of cybersecurity information include human intelligence, honeypots, malware processing, scanning,

crawling, and darknets. ***(Figure 4)*** represents the different types of the cyber threat intelligence sources, features of TIPs and target audience of TIPs.

The threat intelligence platforms composed of several functional areas that realize the intelligence driven cyber security approach (Winkler & Gomes, 2016). It is an enterprise level software system in which different functional areas collaborate by automated workflows for threat management, detection, analysis, defensive processes and track them until completion (Winkler & Gomes, 2016). The threat intelligence platforms offer several features for processing of incoming cybersecurity information such as collection, correlation, ingestion, categorization, enrichment, data mapping, association, normalizing, indexing and others features as shown in ***(Figure 4)***.

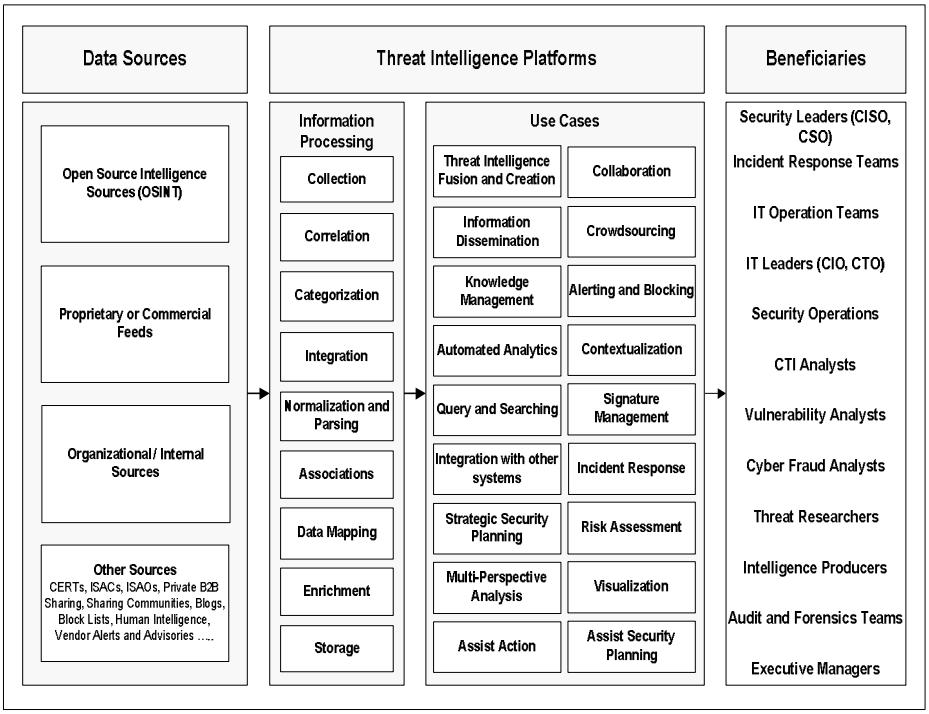



**Figure 4. Threat Intelligence Management and Sharing Platform**

The information received in TIPs can be utilized for providing different capabilities or use cases as shown in ***(Figure 4)***. The basic feature of TIPs is to leverage the utilization of threat intelligence in configuring the security devices to block the malicious activities over the organization's network ([TC], 2015). The TIPs enable actions on threat intelligence by offering APIs & connectors for integrations with SIEM systems, endpoint protection devices, next-generation firewalls, IDS/IPS, and other security solutions. The cyber threat intelligence in machine-readable and structured standard format (such as STIX Structured Threat Information eXpression) leverage the accurate alerts generation and blocking ([TC], 2015). The knowledge management capabilities of TIPs enable the advanced searching, contextualizing, linking data together, and making associations with the incidents, threats, or adversaries ([TC], 2015; Winkler & Gomes, 2016). The signature management in TIPs make the signatures more useful and assist the security teams in decision making based on adversary's known tactics, techniques and procedures (TTPs). Further, it can help in establishing confidence, prioritization of activities, and selection of appropriate step for strengthening the security ([TC], 2015). TIPs enables the multi-perspective analysis by assessing the threat intelligence from multiple types of information sources. It supports in the provision of threat relevance by covering and fusion of internal and external intelligence sources and allows threat assessments comprehensively.

Cyber threat intelligence sharing is considered as the basic requirements of TIP as mentioned in ([ENISA], 2017; [TC], 2015; Brown et al., 2015; Luc Dandurand & Serrano, 2013; Fransen et al., 2015; Sauerwein et al., 2017;

Serrano et al., 2014). TIPs enable the dissemination of threat intelligence and other relevant information for internal consumption or in the larger security community, thereby strengthening cyber defense ([TC], 2015). The TIPs can enable crowdsourcing by bringing the intelligence analysts, security operations, incident response, and risk management teams into one platform which can work jointly for the common mission to defend the enterprise from advanced cyber threats. Several other uses of TIPs are also mentioned in ***(Figure 4)***.

The information available in the TIPs are usable for different use cases by different roles such as IT operation teams, SOCs, incident responders, threat analysts, audit and forensics teams, risk analyst, fraud analysts, malware analysts, decision makers, and other types of roles depending on the structure of enterprises ([TC], 2015; Winkler & Gomes, 2016).

Enterprises have to face several challenges during the successful implementation of TIPs. The selection of the most relevant information sources is one of the biggest challenge for the organizations. The gathering, combining and enriching of intelligence from the multiple sources also require greater knowledge about schemas of the information (Brown et al., 2015).

### 2.2.3 Benefits of Adopting Cybersecurity Information Management Systems

In the enterprises, security teams are dealing with more advanced cyber-attacks than ever before. Therefore, collaboration at larger extent is required to secure the information and network assets (D Shackleford, 2018). The survey conducted by SANS institute in 2018 (D Shackleford, 2018), show that 68% of the responders already utilize threat intelligence for detection and response,

while 81% of them affirmed that cyber threat intelligence is helping to improve their security and response capabilities. In order to collect, aggregate, analyze, and generate cyber threat intelligence, security teams are using different types of tools in their enterprises. The surveys shows that, SIEM systems and TIPs are the mostly used information management systems which are gaining significant traction during the recent years (D Shackleford, 2018). There is an increasing trend of using of cyber threat intelligence by the security teams. The same survey by SANS institute (D Shackleford, 2018) reveals that the enterprises are using threat intelligence mainly for security operations tasks such as blocking threats (70%), detecting threats (79%), threat hunting (62%) and incident response (71%), and so on.

The activities related to the information security are usually spread throughout the enterprise. Therefore, the cybersecurity information management systems should have enterprise wide scope. These systems result in several types of benefits at multiple levels of enterprise. The cybersecurity information management systems can be comparable with other enterprise wide systems such as enterprise resource planning systems (ERP) in terms of the benefits that they bring to the enterprise.

As discussed in the literature, the ERP systems can bring two major types of benefits into the enterprises: tangible benefits such as faster processing, cost savings; and intangible benefits that include customized processes, improved information visibility and improved customer responsiveness (Shang & Seddon, 2004). Several other frameworks are also presented in the literature to identify and classify the benefits of enterprise systems and relevant IT/IS

investments (Irani & Love, 2002; Mirani & Lederer, 1998; Shang & Seddon, 2002). These frameworks consider the benefits either tangible or intangible based on the organizational activities such as management control, financial management, strategic planning, operation control and other activities. Some other studies also recognize the several kinds of benefits that enterprises can achieve by adopting ERP systems (Esteves, 2009; Poston & Grabski, 2001; J. W. Ross & Vitale, 2000). (Chand, Hachey, Hunton, Owhoso, & Vasudevan, 2005) mentioned the increased profits, organizational growth, reduced operational cost and customer satisfaction as the benefits which can be achieved by implementing the ERP system in an enterprise. Furthermore, (Davenport, 2000) and (Markus, Axline, Petrie, & Tanis, 2000) mentioned about some other benefits of ERP systems such as information availability, consistent information, reduced errors and productivity improvement. They also made further recommendations, that the benefits from the ERP systems should also be measured from diverse perspectives. Similarly, (Shang & Seddon, 2002) has presented a framework for assessing and managing the benefits of ERP systems. They classify the benefits of enterprise systems into five major dimensions: strategic, managerial, organizational, infrastructure, and operational. Each dimension of organizational benefits is further divided into sub-dimensions providing a comprehensive framework to analyze the organizational benefits.

In the area related to the information security in enterprises, (Ezingeard, McFadzean, & Birchall, 2005) presented a four-layer model of organizational benefits discussing the justifications in the information assurance (IA)

investments. They discussed that the IA is mainly consider the availability, confidentiality, integrity, identification and authentication, and non-repudiation (Ezingeard et al., 2005). The similarities between the information security and assurance with few differences were also stated. They further mentioned that, IA is mandatory for business continuity, customer trust, effective decision-making, and good governance in the enterprises. The presented IA benefits model consists of four layers: Organizational, Operational, tactical and strategic.

In another study, (Stewart, 2012) investigated the weaknesses and strengths of information security spending in various strategies that are useful for enterprises. A taxonomy was constructed, which can be used by the enterprises to select a rational approach for information security spending. The taxonomy is structured considering the perspective of the potential benefit obtained by the enterprises. The taxonomy is classified into three main themes; enhance efficiencies, , create future gains and avoid future losses.

(Huang, Behara, & Goo, 2014), argued that most of the enterprises are investing in the information security because of the risk reduction (primary reason) as well as business benefits (secondary reason). They further compare the benefits of information security investments and the economic costs. It was stated, that the conceived benefits by the enterprise are due to security risks reduction in the firms. They also highlighted that, security investments can generate direct business benefits as well as reduces the security risks.

**Table 2. Framework for Assessing the Benefits of Cybersecurity Information Management Systems**

| Dimensions | Benefits |
|---|---|
| **Operational** (Ezingeard et al., 2005; Shang & Seddon, 2002) | Resilient Business Processes<br>Improved Productivity<br>Improved Responsiveness<br>Better Information Usage<br>Improved Customer Service |
| **Managerial** (Shang & Seddon, 2002) | Better Resource Management<br>Improved Planning and Decision Making<br>Performance Improvement<br>Improved Monitoring of Operations |
| **Tactical** (Ezingeard et al., 2005; Stewart, 2012) | Building Business Flexibility for Current and Future Changes<br>Better Understanding of Business Opportunities<br>Easier Regulatory Compliance<br>Better Control<br>Improved IT Infrastructure Capability |
| **Strategic** (Ezingeard et al., 2005; Shang & Seddon, 2002; Stewart, 2012) | Better Governance<br>Support for Business Growth<br>Cheaper Equity<br>Cost Reduction<br>More Sales and Stock Value<br>Building External Linkages |
| **Organizational** (Ezingeard et al., 2005; Shang & Seddon, 2002; Stewart, 2012) | Improved Shareholder Value<br>Enable Organizational Learning<br>Facilitate Knowledge Management<br>Competitive Advantage<br>Reputation<br>Building Common Vision |

The benefits of risk reduction involve the avoidance of future potential or expected adversarial events. While, business benefits include the positive effects on financial outcomes or overall business operations of the host enterprise.

In this study, we will utilize the components of the frameworks presented in the (Ezingeard et al., 2005; Shang & Seddon, 2002; Stewart, 2012). It is argued that the scope of cyber security information management systems are enterprise wide, therefore the framework presented in (Shang & Seddon, 2002) can provide solid foundation to discuss the benefits of these systems. Similarly, the model presented in (Ezingeard et al., 2005) offers a relevant basis to analyze the benefits of high level of information security through information assurance. We proposed a framework for assessing the benefits of cybersecurity information management systems and is mentioned in ***(Table 2)***. In our proposed framework, we group the enterprise's benefits into five dimensions: Operational; Managerial; Tactical; Organizational and Strategic.

### 2.2.4 Operational Benefits

The day-to-day activities of enterprises are the operational activities which comprise of acquiring and consuming the resources and repeated periodically i.e. monthly, weekly or daily. Enterprise systems are used to reduce the costs of operational activities and improves output by automating the basic routine activities and repetitive operations (Shang & Seddon, 2002). The operational benefits have instant positive effect on the enterprise's capability to deliver services and products more efficiently and effectively (Ezingeard et al., 2005).

The cybersecurity information management systems have direct effect on the performance of security and IT operations teams of enterprises and have indirect effect on the overall performance of enterprises. The activities related to detection of cyber security incidents are supported by these systems and are carried out continually by the security teams of enterprises. These systems can enhance the capabilities of security teams and greatly enhance their effectiveness in detecting the security incidents in the early stages which can reduce the potential losses as well as increase the uptime of their IT infrastructure. In addition, these type of enterprise systems enable security teams to become more productive, by moving from repeated activities (such as log file analysis) to a more proactive role in enterprises. This effectiveness can help decrease the whole information risk profile and enable enterprises to save time and money (Dorigo, 2012; Hernandez, 2010; Inns, 2014; Miller, 2011; D Shackleford, 2018; Warnecke, 2013).

The capability of long time retention of cybersecurity information is helpful in forensic analysis, incidents investigations and detection of stealthy attacks (such as advanced persistent threats (APTs)) which enhances the performance of the security teams in organizations. The cybersecurity information management systems have the capabilities of automate the report generation process using multiple report formats, which can significantly improve the productivity and performance of security managers of enterprises (Hernandez, 2010).

The cybersecurity information management systems can better utilize the internal and external information to improve the information assurance in the

enterprises and therefore pulling the information security and ensure the business continuity (Ezingeard et al., 2005). These systems enable the flow of cybersecurity information in the enterprises, which in turn ensures the continuity of day-to-day activities, availability of services to customers as well as supports to achieve the operational excellence. In addition, information security is key to effective operational controls and procedures of enterprises, which rely on accurate and timely information for effectiveness and business continuity (Ezingeard et al., 2005).

Effective security capabilities are utilized to improve the IT operations (Stewart, 2012). In addition, security and operational concerns are inclusive of these activities. This can be explained with the examples such as inventory management tells us, what needs to be defended and what security efforts need to be prioritized. Authorized or malicious changes to a systems is difficult to determine without change management control. Similarly, control of configuration management ensures that, the configurations of systems are according to their security needs and functional requirements. Examples from the information security area are as follows: security technology that protects against DoS attacks (Denial of Service) can have valid applications also in other IT areas such as traffic monitoring, bandwidth & service level monitoring, and shaping. The deployed IDS (Intrusion Detection System) in an enterprise can be beneficial for assisting investigations, regardless of negative or positive value realization from it (Cavusoglu, Mishra, & Raghunathan, 2005). In summary, the enterprises can gain security as well as other functional benefits

by investment in the security. All of these benefits are tangled with each other and cannot be untangled.

Conclusively, these systems can potentially offer the organizational benefits in terms of the resilient business process, improved productivity, improve responsiveness, better information usage and ultimately improved customer services (Ezingeard et al., 2005; Hernandez, 2010; Shang & Seddon, 2002).

### 2.2.5 Managerial Benefits

The managerial activities involve the control & allocation of available resources, support for strategic decision making and monitoring of overall operations in the enterprises. The managerial activities are heavily relying on summarized reports and information which can provide the overall picture of enterprises (Shang & Seddon, 2002). The enterprise wide cybersecurity information management systems are important source of information about the security posture and can provide decision and planning benefits to management ([ENISA], 2017; [TC], 2015; Brown et al., 2015; Dorigo, 2012; Miller, 2011; Shang & Seddon, 2002; Williams, 2006). These systems also have the capabilities to produce detailed reports. Enterprises can utilize this information to demonstrate the due diligence or compliance during the audits and investigations (Hernandez, 2010). These reports allow enterprise managers to identify the weak security points, where further investment might be required.

The enterprise wide cybersecurity information management systems can support enterprises to have better planning, effective resource management, improved decision making, enhanced monitoring of operations, and better

performance in multiple operating divisions of the enterprises (Shang & Seddon, 2002).

### 2.2.6 Tactical Benefits

The enterprises can derive several tactical benefits due to the availability of information through the cybersecurity information management systems. The enterprises are investing more and more into their IT infrastructures to improve their productivity and reduce operation costs. The standard architecture of enterprise wide cybersecurity information management systems can offer the features of automated IT resource discovery and implementation of information security policies. These systems enable the enterprises to have reduced information security costs, flexible and robust business processes for current and future changes, better control on IT infrastructure and enhanced capabilities for prompt implementation of security policies on newly installed or discovered IT resources (Ezingeard et al., 2005; Shang & Seddon, 2002).

The cybersecurity information management systems enable the availability of accurate and trusted information. This information is valuable for the shareholders and can increase their trust on the enterprise which is ultimately helpful in better understanding of business opportunities (Ezingeard et al., 2005). Some regulations such as Payment Card Industry Data Security Standard (PCI DSS) and the Health Information Portability and Accountability Act (HIPAA) requires log management including log retention and daily log review. There are some other regulatory requirements that require enterprises to submit compliance reports to various regulatory and assurance entities which is a time consuming task for security managers. So, the cybersecurity

information management systems provide support for complying the different regulatory requirements without extra expenditure on technology. The processes can remain compliant and compliance is monitored through these systems (Bhatt et al., 2014; Dorigo, 2012; Ezingeard et al., 2005; Hernandez, 2010; Inns, 2014; Miller, 2011; Warnecke, 2013; Williams, 2006).

Another benefit of adopting the cybersecurity information management systems is that they help in building and standardizing the processes & mechanisms to address the security concerns. Also, these systems enhances the ability to respond to changes. For instance, if standard security mechanisms are established than, merging of different IT infrastructures as a result of merger or acquisition is faster, smoother and easier. The cybersecurity information management systems provide the flexibility in these types of scenarios as well (Stewart, 2012).

Conclusively, the enterprise wide cybersecurity information management systems can offer benefits such as building business flexibility for current and future changes, enterprises can better understand the business opportunities, easier regulatory compliance (Huang et al., 2014), better control and improved IT infrastructure capabilities (Ezingeard et al., 2005; Shang & Seddon, 2002).

### 2.2.7 Strategic Benefits

Strategic benefits that are associated with the ability of enterprise to perform better than its competitors and achieve its strategic objectives (Ezingeard et al., 2005). In an enterprise, the cybersecurity information management systems can directly or indirectly support the high level strategic decisions and activities regarding long term planning. The strategic activities in an enterprise include

the activities such as acquisition and business merging, marketing competition, product planning, customer retention and capital sourcing (Shang & Seddon, 2002).

The cybersecurity information management systems have the capabilities to provide the holistic information security picture of the enterprise as well as the utilization of the IT infrastructure to the executive management. The executive management can make better decisions based on the available information regarding IT and security investment, also provision of assurance concerning the enterprise's security to other relevant stakeholders (Ezingeard et al., 2005).

These systems enhance the confidence in IT systems, that enable enterprise to effectively leverage the offered business value from their IT systems. The increase in confidence on IT systems is due to the increased system protection which improves the IT systems availability (Warnecke, 2013). However, the ultimate value that cybersecurity information management systems can offer, is the increased continuity in business with minimal operational and financial impact on offered services (Butler, 2009). Another benefit of having properly implemented these systems are leveraging the opportunity of collaboration and attraction of external funding. In several scenarios, the enterprises solicit collaboration and external financing to fund their upcoming project, innovative ideas or for extending their existing business. The information security history is one of the factors that investors analyze before realizing any contract. For instance, investors believe that enterprises that had already faced the security breaches or vulnerable to cyber attacks in the past can be exposed to financial damage in the future as well (Ettredge & Richardson, 2003; Ezingeard et al.,

2005; Garg, Curtis, & Halper, 2003; Hovav & D'Arcy, 2003; Spanos & Angelis, 2016).

The readiness of enterprises for investing in cybersecurity information management systems will give the assurance that they are serious about their business reputation which will have positive impact on all the relevant stakeholder including customers and investors. In addition, an enterprise will be more trusted among its stakeholders, if they ensure the privacy of the collected information as well as ensure the secure exchanges with its business partners (Ezingeard et al., 2005).

Overall, these system improves the information security posture of the enterprise due to which several other benefits can be achieved such as obtaining more businesses which results in direct business benefits in terms of higher revenues, maintenance of customer retention and stock market share. The higher information security level enables the capability to launch additional value-added services such as secure interactions with clients and suppliers, and consequently generating growth opportunities for the enterprises. It works as business enabler for the enterprises. The literature suggest that the enterprises must have to invest in security to achieve a certain level of information security. This makes them eligible to capture new businesses by obtaining new customers. In addition, they become eligible for bidding on different types of projects, as several companies are insterested to evaluate the security audit reports to investigate whether the security practices are acceptable. For instance, organizations in the healthcare industry have to comply with HIPPA rules in order to qualify for Medicaid and Medicare payments (Huang et al.,

2014). Furthermore, several evidences have been observed, in which the stock market value of the enterprise boosted after the announcements related to investments in information security (Huang et al., 2014).

In summary, the cybersecurity information management systems can monitor the overall IT infrastructure of the enterprise which can also be integrated with the internal and external information sources have the potential of attaining the following strategic benefits: better governance, support for business growth, cheaper equity, cost reduction, more sales and collaboration by building the external linkages (Ezingeard et al., 2005; Shang & Seddon, 2002).

### 2.2.8 Organizational Benefits

The organizational benefits are those which are required by the main stakeholders of the enterprises. Organizational benefits emerge when the use of cybersecurity information management systems offer benefits to an enterprise in terms of learning, cohesion, focus and smooth implementation of its strategies (Shang & Seddon, 2002). The operational, managerial, tactical, strategic benefits discussed in the previous sections result in the better value of the stakeholders of enterprise and also offer competitive advantage. In several industries, measures to maintain the information security and privacy of the information is posed as a necessary condition by the regulators, entities and other authorities for issuing the operating license which is ultimately an organizational benefit to enterprises (Ezingeard et al., 2005).

The enterprise wide cybersecurity information management system enables the enterprises to have more cohesive and focused approach towards the information security. These systems leverage the enterprise level learning and

better at executing its chosen strategies. Additional evidences of organizational benefits comprise of improved employees' satisfaction & morale, better accountability, and conversion of employees from doers to planners with widened skills sets.

Some enterprises are investing in these systems (e.g. SIEM for log management) considering their major focus on regulatory compliance. But these systems can also help to gain better control over business, letting them to increase efficiency, enhance enterprise learning, meet the challenges of emerging information security issues and potentially can offer competitive advantage. Organizational benefits also appear when the enterprise wide cybersecurity information management systems are supporting in establishing a common vision for the future of enterprise. These systems enable the proper communication among the employees about the current and potentially fore coming issues which in turn improves the overall mutual understanding between the management and the employees. Security teams can use the cybersecurity information management systems for knowledge generation based on wide range of activities specifically beneficial for security and IT operation teams, IT management, finance and human resource (Warnecke, 2013).

The cybersecurity information management systems involve a wide range of stakeholders, they must have to work together, regularly in multiple cross-functional teams, to assess security events, generate reports and take actions to address incidents and other identified issues. These activities promote the

overall risk management and security culture in the organizations and helps to diminish the organizational silos (Hernandez, 2010).

The high level of information security achieved through appropriately placing the security tools can have several organizational benefits. (Jennex & Zyngier, 2007) argued that the overall security of an enterprise is an important success factor for enterprise's process of knowledge management, enhanced confidence in an enterprise's reputation and brand (Univesity, 2007), and customers prefer those enterprises who have better reputation regarding the protection of their data (Wang, 2004).

In the enterprises, cybersecurity information management systems are expected to offer the organizational benefits such as improved stakeholders value, facilitate organizational learning, competitive advantage (Huang et al., 2014), reputation (Huang et al., 2014) and building common vision across the enterprise and, promotion of enterprise level security culture (Hernandez, 2010).

# Chapter 3: Values of Stakeholders in Cybersecurity Information Sharing Ecosystems

## 3.1 Summary

The market of cybersecurity information is growing with more number of end users, cybersecurity solutions and information providers (Dey et al., 2014). Specifically, the market is highly attractive for new entrants i.e. solution and information providers, but their survival rate is very low and most of them disappear within couple of years (Dey et al., 2012). It has been observed that, existing literature mostly covers special aspects such as technological aspects of cybersecurity (i.e., information sharing, quality of information, automation, standards and protocols (Skopik et al., 2016)), cybersecurity investments, incentives, public-private collaboration in cybersecurity information sharing (He et al., 2018; Praditya & Janssen, 2015; Zheng & Lewis, 2015). But, there is a gap in determining value creation and values obtained by stakeholders in cybersecurity information sharing ecosystem for formulation of business strategies and policies. Therefore, this study has been performed to determine the values that these offerings actually generate for the involved stakeholders.

The objectives of this research essay is to model structure of value creation and distribution among stakeholders in cybersecurity information sharing ecosystem. This study will help in investigating whether all stakeholders gain sufficient value when participating in cybersecurity information sharing ecosystems. On the basis of the research objective, four research questions are defined: (1) How value is created in cybersecurity information sharing

ecosystem? (2) How value is distributed among stakeholders? (3) How do the value parameters affect the values obtained by stakeholders? (4) How distribution of value changes in different situations?

The research questions have been answered by identifying the stakeholders and value parameters in the cybersecurity information sharing ecosystem. Three types of stakeholders are identified i.e. cybersecurity solution providers, cybersecurity information providers and end users. Seven value parameters are also identified including install base (number of end users), trusted communities, quality of services (QoS), quality of information (QoI), timeliness of information, trust on information sources and cost. These value parameters are used for explaining net value of stakeholders generated from cybersecurity solution and information providers in cybersecurity information sharing ecosystems. The value parameters are integrated into three additive utility functions, representing values generated for respective stakeholders. The utility functions enable the evaluation of value creation and value distribution in cybersecurity information sharing ecosystem.

In this study, relative changes of values of stakeholders in cybersecurity information sharing ecosystem has been analyzed by simulation technique using system dynamics methodology. Vensim software of Ventana Systems is utilized for simulation which supports the system dynamics methodology ([VS], 2015).

Our simulation results imply that the value obtained by information providers is quite low in comparison to the cybersecurity solution providers. The high usage fee slightly impacts the values of end users while it has significant impact

for the cybersecurity solution and information provider. In the saturated market (i.e., in a market, in which the number of new end users slows down), cybersecurity solution provider and information provider even experience a negative value allocation. This indicates more potentials risks for information providers as compared to the cybersecurity solution providers.

Consequently, this study can make a number of contributions in the area of value creation in cybersecurity information sharing. From the theorectical perspectives, this research provides a framework to evaluate the values of stakeholders in the cybersecurity information sharing ecosystem. To the best of our knowledge, analysis of the values of all the stakeholders in cybersecurity information sharing ecosystem is not well known, in fact there are several studies on the incentives and return on security investment (Gordon et al., 2015c; Gordon, Loeb, Lucyshyn, & Zhou, 2015a, 2015b) but these studies do not cover the overall picture of the cybersecurity information sharing ecosystem. If sufficient revenues are generated for the cybersecurity solution and information providers, they will leverage innovation in the area of cybersecurity, which ultimately have positive impact on the overall cybersecurity situation.

The results of this research will help in specifying sustainable cybersecurity information sharing ecosystems in which all the stakeholders can generate sufficient values. Furthermore, the business managers can improve the value exchange methods among the end users, cybersecurity solution and information providers.

The outline of rest of the essay will proceed as follows: ***Section 3.2*** gives a literature survey, gap analysis and overview of area of economics of cybersecurity. The theoretical frameworks related to our research are given in the ***Section 3.3***. ***Section 3.4*** presents the description of proposed value model, value parameters and utility functions for the stakeholders. This is followed by the discussion about the simulation model description and different scenarios in ***Section 3.5***. ***Section 3.6*** of the paper presents the presentation of simulation results and sensitivity analysis. The ***Section 3.7*** concludes the research with a discussion, summary, limitations along with directions for future research.

## 3.2 Literature Survey and Gap Analysis

From the last few decades, security researchers realized that the technological solutions alone are not sufficient to solve the cybersecurity problems and started to explain it in economic perspectives (Anderson, 2001; Anderson & Schneier, 2005; Gordon & Loeb, 2002b, 2006; A. Ross & Moore, 2006; Schneier, 2011). Several streams of literature in the area of economics of cybersecurity emerge which consists of study of economic incentives for information security investment decisions, appropriate budgeting, network effects from cybersecurity investments, economics of cybersecurity information sharing, determining the economic impacts of cyberattacks, cybersecurity risk modeling, and cybersecurity policy.

Investments in cybersecurity activities is an import aspect to help mitigate the cybersecurity challenges in organizations. It has been observed in the literature that, there is a trend of underinvestment in the cybersecurity which is hardly ever reach to its optimum level (Gordon et al., 2015c, 2015a). The consequences of cybersecurity underinvestment include the increased cyber risks, economic costs due to incidents, social welfare losses, reduced level of individual and national security (Campbell, Gordon, Loeb, & Zhou, 2003; Gordon et al., 2015a). Several types of economic models and frameworks are also presented in the literature related to decision-making of cybersecurity investments. (Gordon & Loeb, 2002b) developed an economic model considering the investment decisions for security of information systems and evaluates the cost of cybersecurity against the expected loss from cyber-attacks. In a subsequent work, (Gordon & Loeb, 2006) explained empirically that this

type of economic analysis is widely used in practical scenarios for security investment decisions. (Gordon et al., 2015b) presented an economics-based analytical framework for evaluating the impact of regulations and incentives designed by the government to improve the situation of investments in cybersecurity by the firms in private sector. They describe that investments in cybersecurity at private firms depend on the utilization of optimum combination of inputs to cybersecurity and willingness to rise their investments in cybersecurity activities. (Garvey, Moynihan, & Servi, 2013) argue that the economic decision making plays an important role in securing globally distributed information repositories. Thus, for evaluating economic-benefits and returns on cybersecurity investments, a macro-analytic method was presented termed "Table Top Approach" which allows and explains the selection of competing choices that suggest the greatest cost-benefit gains in cyber defense. (Weishäupl, Yasasin, & Schryen, 2018) conducted the theory based exploratory multiple case study to optimize the future IT security investments and selection of security measures based on the past decisions.

The game theory has been extensively used in the recent literature to discuss the incentives which leads to more effective security investment decisions making. (Cavusoglu, Raghunathan, & Yue, 2008) studied the mangers view of security investment and argue that traditional decision-theoretic risk management techniques to define investments in security are not appropriate because of the strategic nature. The hackers have dynamics strategies and they alter their attacking and hacking strategies considering firm's investment strategies in security. They proposed the game theoretic model to determine

information security investment levels and compared it with decision theory approaches considering the factors of vulnerability, levels of investment, and payoff from investments. (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2014) addressed the challenge of how do we make better security decisions, and proposed techniques and algorithms that optimally allocates cybersecurity resources according to different tasks to support well-founded human decision making using the game theory. (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016) suggested that effective decision-making strategies should be used by security managers when investing in cybersecurity resources. They considered the combinatorial optimization, game theory, and a hybrid of these two for making the cybersecurity decision making more effective. (Panaousis, Fielder, Malacaria, Hankin, & Smeraldi, 2014) uses the non-cooperative control games to investigates the optimal investment in the cybersecurity controls in the organizations specifically the cases in which organizations faces the problems of underinvestment or inefficient spending on cybersecurity.

Some other techniques have also been utilized to study the cybersecurity investments. (Kjell Hausken, 2006) presented the economic model using the logistic function to assess the relationship between the optimum cybersecurity investments level and the vulnerabilities of information sets that exhibits increasing returns and then decreasing return of investment. (Dor & Elovici, 2016) used the grounded theory to present the model that support the decision-making practices regarding organizational investments in information security in several industries. (Herath & Herath, 2008) developed the integrated real options analysis (ROA) model using Bayesian statistics that includes learning

and post-auditing analysis technique for evaluating the information security assets value for optimal level of investments in cybersecurity.

In the organizations, the decision makers are interested to know that the investments in any product or service is justified or not. The financial justification in case of cybersecurity investments is difficult because high level of cybersecurity delivers non-financial benefits, rather than direct increase in revenue or a reduction in costs. In the cybersecurity investments literature, several metrics have been presented to quantify the return on security investments (ROSI), e.g., (Gordon & Loeb, 2002a) and (Anderson, Böhme, Clayton, & Moore, 2008); cybersecurity decision making e.g., (Dor & Elovici, 2016; Fielder et al., 2016; Huang & Behara, 2013; Mayadunne & Park, 2016); net present value (NPV), e.g. (Eisenga, Jones, & Rodriguez, 2012; Sheen, 2010); the Internal Rate of Return (IRR), e.g., (Buck, Das, & Hanf, 2008; Wawrzyniak, 2006); Annual Loss Expectancy (ALE), e.g., (Cremonini & Martini, 2005; Tanaka, Matsuura, & Sudoh, 2005).

Another research direction in cybersecurity is the network externalities which also have effect cybersecurity investments levels. (A. Ross & Moore, 2006) explains that externalities play an important role in cybersecurity underinvestments, similarly (Lelarge, 2012) emphasized that network externalities always resulted in inefficient cybersecurity investments.

Further, the economic incentives in cybersecurity information sharing has been extensively studied in the literature. There are majorly eight different categories of information sharing incentives have been discussed in the literature (Koepke, 2017). The sharing of cybersecurity information has been studied at four

different levels: within governments, among governments, among companies in the private sector, and between the government and the private sector (Cavelty, 2015; Dunn-Cavelty & Suter, 2009; Gal-Or & Ghose, 2005; Prieto, 2006). The cybersecurity information sharing between private and the government organizations is difficult to achieve. The companies are reluctant to share information about the cybersecurity breaches and vulnerabilities because of negative incentives associated with the information dissemination and negative correlation with the market value of the targeted firms (Campbell et al., 2003; Cavusoglu, Mishra, & Raghunathan, 2004b; Koepke, 2017). In addtion, (Koepke, 2017) divided the shortcomings that hinder information sharing of cyber threats into eight categories; (1) constitutional / legal, (2) technological, (3) informational, (4) collaborative, (5) managerial, (6) organizational, (7) performance, and (8) Cost. Some other reasons of hindering the cybersecurity information sharing includes, violation of privacy protection laws, loss of reputation and the potentials of more exploits by hackers can be possible due to the public dissemination of cybersecurity information (Branscomb & Michel-Kerjan, 2006; Cavelty, 2015). Further, (Naghizadeh & Liu, 2016) investigated the incentives that enterprises have in security information sharing agreements for information disclosure.

In a study conducted by (Mermoud, Keupp, Huguenin, K., Palmié, & David, 2018) presented an incentive based model for cybersecurity information sharing among the human agents, and tested it with the empirical data collected by online survey from participants (Information Sharing and Analysis Centers (ISAC) for critical infrastructures). Similarly, (Vakilinia & Sengupta, 2017)

studied the rewarding and participation fee allocation mechanisms in order to encourage the information sharing behavior. (Khouzani, Pham, & Cid, 2014) investigated the incentives behind investments by competing companies in discovery of their security vulnerabilities and sharing of their findings. The studies in these areas, are mostly focusing on the adjustment of incentives for all the stakeholders to have win-win situation, resolve trust issues (Branscomb & Michel-Kerjan, 2006) and understanding the conditions which are conductive to an optimal involvement of the state level networks of cybersecurity cooperation (Suter, 2012, 2016).

Several other aspects of sharing of cybersecurity information have also been investigated in the literature; such as market values of firms in the private sector in response of publically announcing security breaches (Gordon, Loeb, & Sohail, 2017), economic issues and welfare in general (Gal-Or & Ghose, 2005; Gordon, Loeb, & Lucyshyn, 2003) and cooperation among individuals, private organization and governments (Gordon et al., 2015c; Hausken, 2015; Laube & Böhme, 2016). (Gordon et al., 2003, 2015a) explained that when cybersecurity related information is shared, the firms can reduce the spending and can achieve increased level of cybersecurity with lesser cost. They provided the sufficient and necessary conditions for sharing of cybersecurity information which can lead to decreased or increased level of cybersecurity. They also highlighted the issue of free riding and mentioned the importance of appropriate incentive mechanisms for firm-level profits as well as for social welfare.

In our research, we have considered the commercial cybersecurity information sharing ecosystem. In the private sector, the most powerful incentive for an

organization to invest in cybersecurity activities, is the motivation to increase the value of their organization. In order to understand the values of stakeholders in the cybersecurity information sharing ecosystem, there exist a gap in the literature related to determining the value creation, evaluating and distribution of the values obtained by stakeholders. Therefore, in this paper a framework is provided to determine the values which are actually generated for the involved stakeholders due to the offered cybersecurity solution and information. We identify that there must be an economic evaluation of values of stakeholders, in order to avoid cost and risks of a security breach. For this study, we surveyed literature from different disciplines i.e. cybersecurity information sharing, value creation and value co-creation and network effects. The overview of our research is given in ***(Figure 5)***.

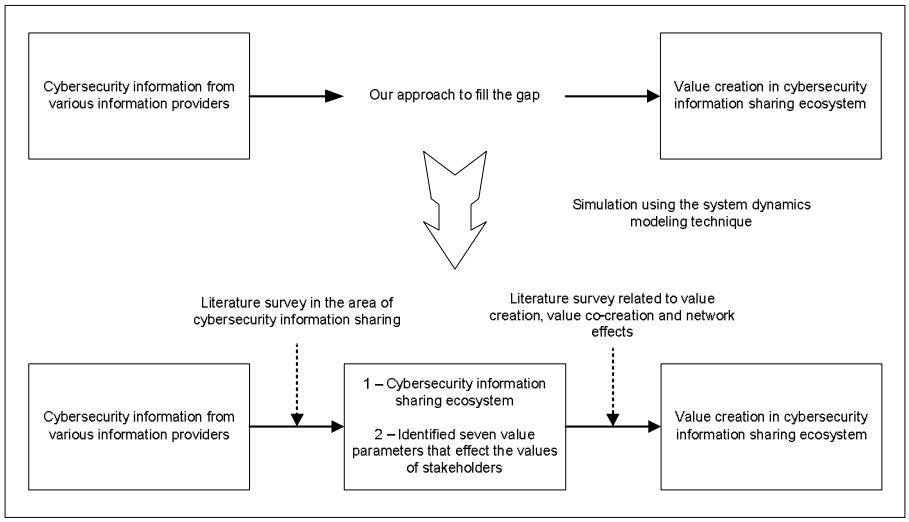



**Figure 5. Research Overview of Value Creation in Cybersecurity Information Sharing Ecosystems**

## 3.3 Theoretical Frameworks

### 3.3.1 Values of Stakeholders in Cybersecurity Information Sharing Ecosystems

The stakeholders in cybersecurity information sharing ecosystems have different values, we will study the values obtained by end users, cybersecurity information providers and solution providers. Stakeholders work together to collect and share cybersecurity information, which can give broader visibility of the threat landscape. The information-sharing ecosystem produces more values as a whole, than the sum of the values of individual stakeholders acting independently.

Value creation is a networked process that creates outputs that are more valuable than its inputs instead of linear value creation. Generally, values are the benefits that consumers are expecting to have by using the products or services. The definition of value creation is different among the stakeholders, which has its own contextual meaning. Similarly, the process of value creation is also different among the stakeholders. It is subjective and depend on the individuals who receives it and is not necessarily the same for everyone. It is essential to understand the drivers and sources of value creation within the enterprises, industry, and marketplace. It has been observed in the literature, that value creation vary in different industries based on multiple intangible factors. Major categories of intangible factors include technology, innovation, management capabilities, intellectual property, alliances, employee relations, customer relations, community relations and brand value.

In cybersecurity information sharing ecosystem, the value can be defined as the benefits and the sense of security obtained by end users from using the cybersecurity solutions and information. It is very difficult in case of end users to directly identify and quantify all the benefits and utilities obtained from high level of cybersecurity, and translate them into economic terms to show the potential profitability from the point of view of cybersecurity investments (Magnusson, Molvidsson, & Zetterqvist, 2007).

The major factors that increase the utility of end users include the efficiency, satisfaction, productivity, consumer privacy, secure e-commerce, secure partnerships, increased level of comfort on business transactions, reduced liability and meeting regulatory compliance ([ITGI], 2006; [S], 2002). Another study provides the categorization of benefits that can be achieved from the cybersecurity are: (a) operational benefits considering the effectiveness of delivering services and goods; (b) strategic benefits related to competitive advantages; (c) tactical benefits considering trading partners; and (d) organizational benefits including shareholders value (Ezingeard et al., 2005). The other benefits obtained by end users includes: retain and acquire customers; market valuations; business resilience; performance improvements; protection of digital assets; accountability; financial management; increased trust and public confidence; prevent potential financial and reputation losses; and enhanced ability to deliver services & products electronically. Conversely, the lower utility causes several risks such as productivity, loss of revenue, competitive advantage, privacy violation, reputation, survival business continuity.

In order to analyze value, one way is to determine the financial benefit of implementing a strong cybersecurity posture and determining of the quality of that posture through assessing cyber-risks and their mitigating control processes. Another way of calculating financial benefits is the cost-avoidance in terms of avoiding cost of cyber-attacks. The cybersecurity information increases awareness of cyber-attacks which provides to companies the necessary information to evaluate such costs. Therefore, to some extent, the financial benefits of cybersecurity can be determined by evaluating the cost of a cyber-attack.

In this study, we are considering the increase in effectiveness, efficiency and productivity as the potential benefits for end users in the cybersecurity information sharing ecosystem. The cybersecurity posture of end users is improved by the utilization of cybersecurity information. The high level of cybersecurity enhances value by improving the efficiency, effectiveness and contributing economically to the end user's goals of maximizing their utility.

For cybersecurity solution and information provider, value can be defined as the profit, which they get from end users and the number of end users getting attached to them i.e. installed base. The cybersecurity solution providers and information providers provide services to end users and in return receives usage fee from them. The satisfaction of the end users results in the network externalities and increases the number of users in their installed base. The increase of the cybersecurity posture of end users is the common and inextricably linked interest of all stakeholders in the ecosystem. Therefore, the value creation can be sustainable, if it is created for all types of stakeholders in

the ecosystem. The main focus should be on creating values for end users, but this cannot be attained unless cybersecurity solution and information provider receive consistently attractive returns.

The value creation in cybersecurity information sharing ecosystem is important for all stakeholders. The characteristics of cybersecurity information sharing ecosystems influence the value creation of all the stakeholders. There is a distinction between the usage value (i.e. individually evaluated by the customers), and the exchange value (i.e. only realized at point of sales). Therefore, proper identification of competitive advantages of cybersecurity solution and information providers these characteristics should be considered in measuring the values of stakeholders. Specifically, we will give answers to the following questions in our research: What is the value of each stakeholder? How value is created for each stakeholder? How value is captured by the stakeholders? How value is created through the interrelationship among the stakeholders? We identified the value parameters that affects the values and concludes sources of utilities and profits and proportion of value captured by the stakeholders.

### 3.3.2 Values Creation in Cybersecurity Information Sharing Ecosystems

The value creation has been studied extensively in different areas such as e-business (Amit & Zott, 2001; Lee, Kim, Noh, & Lee, 2010), platform business model (Baek, Kim, & Altmann, 2014; Haile & Altmann, 2012, 2016; K. Kim, Altmann, & Hwang, 2010, 2011; Smedlund, 2012), these literatures identified several dimensions of value creation and also evaluated different business

models. (Aviad, Węcel, & Abramowicz, 2018) define cybersecurity value as to quantify the benefits that cybersecurity knowledge can bring to those who use it. The utilization involves consumption of knowledge or identifying missing links in the existing knowledge that needs to be added. The evolution of big data triggers several information-intensive services, where value creation is extremely effected by the information interactions. (C. Lim et al., 2018) studied the factors and mechanisms that affect value creation based on information in the current data rich economies. Information is recognized as a valuable resource and an asset that has a significant value (Thompson & Kaarst-Brown, 2005). In information-intensive services, value is generated mainly through information interactions. These information interactions are different than the traditional interpersonal and physical interactions among the service providers and customers (Karmarkar & Apte, 2007; C.-H. Lim & Kim, 2014). The value creation phenomenon is carried out by multiple actors of enterprises to jointly create value (Merrilees, Miller, & Yakimova, 2017). The consumers and producers work jointly and reciprocally to co-create value through resources integrations and applying the competences (C. Lim et al., 2018). This is similar to the case of cybersecurity information sharing ecosystem, where all the stakeholders work together to improve the overall security posture.

Another definition of value is given by (Barney, 1991), he defined value as the resource of a firm, and it becomes valuable if it leverage the opportunities to defuses the threats from the environment of firm. The cybersecurity information is a firm's resource, utilized by the end users against the cyberattacks, and creates value for them. The cybersecurity information interactions facilitate the

value creation thereby contributing in improvement and innovations in cybersecurity. Accordingly, value creation based on cybersecurity information sharing needs an understanding of value creation in the ecosystem. However, there is a gap in the existing literature between value creation and cybersecurity information sharing. While in other environments (such as big data), the value creation based on data has already been extensively studied (C. Lim et al., 2018). He also explained the data-based value creation in information intensive services, which is similar to the process of utilization of cybersecurity information sharing.

The process of value creation through information can be explained as: first, the firm provides the value propositions to support customers. The customers utilize the firm's offering for the fulfilment of their goals (Bettencourt & Ulwick, 2008). During these interactions, the firm collects the customers and service operations relevant data from several sources (C. H. Lim, Kim, Hong, & Park, 2012). This collected data is provided to other entities (C.-H. Lim & Kim, 2014), they perform data analytics to convert it into more useful information (George, Haas, & Pentland, 2014). Finally, the relevant entities and customers utilize this information to create value and also for generating more data (Saarijärvi, Grönroos, & Kuusela, 2014). The value is generated only when the users of the information utilize it for their intended purposes (Heinonen et al., 2010; Vargo & Lusch, 2004).

In area of cybersecurity, the information related to cyberattacks and involved risks have the potential to contribute in creation of value. The firms can reduce the level of risk by evaluating and determining the available information and

can attain positive value (Philip & Salimath, 2018). For example, the availability of cybersecurity information makes it possible to identify high-level risks that can have multiple impacts (e.g. regulatory, reputational, financial etc.). Based on the available information about the risks, different strategies and controls can be suggested for improving the security of information assets and can reduce the potential damage (Luo, Shenkar, & Nyaw, 2002).

The available frameworks to evaluate the value creation and distribution are not suitable for the cybersecurity information sharing ecosystem. It is important to analyze the value distributions for the stakeholders of cybersecurity information sharing ecosystems for taking effective business decisions. Therefore, measurable value parameters are required to identify for the cybersecurity information sharing ecosystems. Conclusively, we can state that the existing research works did not fully explain the value creation and exchange for all the involved stakeholders in cybersecurity information sharing ecosystems. Our paper, however, addresses this research gap by introducing a new value creation framework for cybersecurity information sharing ecosystem, which can be a useful tool for policy makers and business managers. Besides, the framework assist in explaining the value of end users, cybersecurity solution and information providers. This framework can be used as a decision support tool for investments in development of cybersecurity solution and information generation, design of business models, service bundling, and market structure evolutions.

### 3.3.3 Cybersecurity Value Co-creation

The cybersecurity information sharing ecosystems become increasingly complex, with networks of information and solution provider interacting with the end users network. The value creation in cybersecurity information sharing ecosystem can be perceived as value co-creation. To understand these ecosystems, a systematic methodology is vital to allow a complete view that considers different parts along with their interconnections within the ecosystem. This methodology also have to enable analysis of value networks at multiple levels (i.e. from ecosystem to the individual stakeholder level).

Value co-creation can be described as the configurations of resources of the service systems that interact and cooperate with other service systems to create value (Maglio, Vargo, Caswell, & Spohrer, 2009; Spohrer, Maglio, Bailey, & Gruhl, 2007). The co-creation of value was initially focusing on the value from business assets, but these days it tends to cover multiple aspects including the privacy and security of information assets. In the cybersecurity information-sharing ecosystem, all the stakeholders interact and share cybersecurity information among each other to co-create value. The stakeholders in the ecosystem increasingly collaborate and co-create value by the combination of service offerings and information from multiple stakeholders. As similar to the case of service system, stakeholders in the cybersecurity information sharing ecosystem establish many-to-many relationships through the interactions, and thus forming a value network (Patrício, Fisk, e Cunha, & Constantine, 2011). The ordering of resources (such as organizations, information, people and technology) are linked with in the system as well as externally to other systems

through value propositions (Maglio et al., 2009; Spohrer et al., 2007). The approach of analyzing the service systems enables understanding of the parts of system without losing the overall context (Gummesson, 2007). The value is co-created by integration of available resources of a service system, with the resources of other systems (Vargo & Lusch, 2008). A multilevel view was proposed for distinguishing the organizational level service system and constellations of customer value at the network level (Patrício et al., 2011). In addition, these value constellations can also be seen a service systems, that cooperate together for the provision of integrated support to customer activities (Patrício et al., 2011).

The dyadic perspective of a single customer and single supplier is shifted to a many-to-many perspective, in which the network of end users work together with solution and information provider networks. (Pinho, Beirão, Patrício, & Fisk, 2014) investigated the value co-creation concept in complex value networks having many actors. The actors or stakeholders can be active or passive having varying role in network. In the complex systems contexts, the actors or stakeholders collaborate in interactive and mutual exchange configuration to create value (Vargo & Lusch, 2008). From the perspective of value networks in cybersecurity information sharing ecosystem, all stakeholders collaborate and share information (i.e. integrate resources) for value creation which is beneficial to everyone in the ecosystem. This case of value co-creation is similar to value networks or system of service systems described by (Vargo & Lusch, 2008) where value co-creation moves beyond the customer and firm dyad to a much broader perspective. In this scenrio, all

the involved stakeholders (e.g. employees, customers, companies, suppliers, stockholders, and other partners in the network) leverage value creation for themselves and others. According to (Grönroos, 2008), the interaction for co-creation of value is defined through scenarios where service provider and customers are involved in each other's practices. Similarly, in cybersecurity information sharing ecosystems, the end users share information in the trusted communities which is also utilized by the solution and the information provider.

The cybersecurity value co-creation is twofold as described by (Vicini et al., 2016), first, to extract the value from huge volume of information available in distributed environments. Second, to improve the customer's perception about the privacy issues and believes that the data is stored on secured systems. These issues becomes more important especially when end-users are directly involved in value co-creation process (Prahalad & Ramaswamy, 2004). In another study conducted by (Feltus & Proper, 2017a, 2017b), investegated the the security and privacy as an instance of value co-creation. Further, a collaborative security approach is proposed in the study conducted by (Garrido-Pelaz et al., 2016). It was argued that, information sharing could support to establish the early prevention mechanisms. They proposed a model of cybersecurity information sharing among dependent organizations that are affected by different cyber-attacks.

The role of customers is changing from proactive to active participation during the process of value creation (McColl-Kennedy, Vargo, Dagger, Sweeney, & Kasteren, 2012; Payne, Storbacka, & Frow, 2008). In the value creation process, the customers executes a series of activities to attain an anticipated

outcome (Payne et al., 2008). This study offers detail about how value is co-created in many-to-many value networks, disclosing the complex and dynamic interconnections among the involved stakeholders. Similarly, in the cybersecurity information sharing environments, the role of end users is also changing towards proactive information sharing.

There are several forms of value co-creation including informal, formal, online and offline. In most of the scenarios, a platform is needed to leverage the process of value co-creation. Most of the cybersecurity solutions such as "Threat Intelligence Management Platforms (TIPs)" and "Security Information and Event Management (SIEM)" system provide appropriate tools that supports communication and information sharing between involved stakeholders, which ultimately engages in value co-creation in the cybersecurity information-sharing ecosystem. We will focus the value co-creation in many-to-many context related to the cybersecurity information sharing where multiple stakeholders (end users or cybersecurity solution or information provider) simultaneously interact to co-create value.

### 3.3.4 Network Effects

The key issues related to the success of cybersecurity information sharing ecosystem includes the gaining of huge mass of end users, scalability and achieving self-sustainable growth. In some cases, the initial development of cybersecurity solutions can be supported by third party (i.e. in terms of finances, promotion, or otherwise subsidized using external funding). However, the long term the sustainable success depends on a practical business model and the capability to attract the new end users. In the early phases, a common issue is

the growth of the installed base of end users. The allocation of development resources should be planned properly to attract a large number of end users. In the presence of several non-interoperable and competing cybersecurity solutions, there can be the risk that no solution provider achieves a critical mass. In cybersecurity information sharing ecosystem, achieving a large number of end users depends crucially on network effects created in the ecosystem.

The network effects play an important role in determining the economic values of stakeholders in the cybersecurity information-sharing ecosystems. The network externalities affect the values of stakeholders (i.e. indirect and direct network effects). The generation of value due to the availability of complementary services or products is known as indirect network effects. While direct network effects is explained as values created from the number of existing users (Katz & Shapiro, 1985). Further, cross-side or indirect network effects refer to situations where the value for an actor group depends on the size of another actor group therefore reflect a pre-existing underlying interdependency. For example, with more number of users, the value of mobile phones operating system platform will be high for the application developers and vice versa. The interdependency fuels a self-reinforcing feedback loop of adoption "from both sides", that has the supporting effect to attract installed base at the earlier stages. Two-sided network effects explain the double impact of both types of network effects. In the traditional markets of software products, the major part of value is conceived through the two-sided network effects. Specifically, the network effects have effect on market competition, equilibrium, compatibility decisions, and adoption pace of new technologies

(Clements, 2004; Katz & Shapiro, 1985, 1986; Liebowitz & Margolis, 1994). Comparable to traditional markets, the cybersecurity information sharing ecosystems can be viewed as a two-sided market place (Rochet & Tirole, 2006). In the cybersecurity ecosystems, the information providers attracts solution providers and end users. Similarly, solution providers attract end users and information providers. This scenario is analogous to the markets of autos. The autos market can be seen as two-sided market because auto manufacturers must attract both expert mechanics and consumers (Rysman, 2009). Several studies have extensively investigated the impact of positive network effects in the markets of technology and software products (Haile & Altmann, 2012, 2016; Katz & Shapiro, 1985). It is recognized that the large market share offers an additional utility to the vendors. The cybersecurity information and solution providers are not only relying on comparison of features, capabilities functionalities, and prices of their services and products. However, some additions factors also play role in increasing the size of the end user network. These factors include the timeliness of information, availability of trusted communities and trust on the information sources. The trusted community affects the value of solution providers and end users, because end users can get valuable tools and tips from there for improving responses to cyber-attacks and increase their level of cybersecurity.

### 3.3.5 System Dynamics

Several stakeholders are interacting with each other in cybersecurity information sharing ecosystem makes the value creation a complex interdependent system. The complex nature of ecosystem makes it necessary to

have sophisticated analytical tools to help decision makers to analyze interactions of among the stakeholders as well as for developing business models to increase the value of involved stakeholders. The benefits of using cybersecurity information can only be realized by utilizing for long time period and through a trusted relationship among the stakeholders, only a dynamic model is a suitable option to show the nature of value creation for end users, cybersecurity solution and information providers. Such a dynamic model can capture interdependencies among the stakeholders and real life interactions within the ecosystem. Considering these characteristics of the cybersecurity information sharing ecosystems, system dynamics methodology has been chosen for this study. System dynamics provide the necessary tools for the analysis of interactions among the stakeholders and for modelling the value creation over time for each of the stakeholders.

System dynamics is an aspect of system theory, which deals with understanding the behavior of complex systems over time, by considering feedback loops and time delays (John D Sterman, 2000). It is a modelling technique, which can be used for investigating the mutual interaction, interdependence, information flow, circular causality, feedback loops, and other dynamic issues that can arise in complex social economical systems. Currently the system dynamics methodology is being used for policy design and analysis in multiple domains such as value creation in software service platforms (Baek et al., 2014; Haile & Altmann, 2012, 2016; K. Kim et al., 2010, 2011), information security and cybersecurity (Baek et al., 2014; Dutta & Roy, 2008; Nazareth & Choi, 2015). The basis of the system dynamics methodology consider that, relationships

among the components of a system are very important in investigating the behavior of a system.

## 3.4 Proposed Value Creation Model for Cyber Security Information Sharing Ecosystems

The proposed value creation model in this section, includes the interrelationship among the stakeholders, value parameters which are utilized to determine the values of stakeholders, and a methodology for measuring the values. The proposed model is structured into three parts: interrelationship among stakeholders and their value exchange, effects of value parameters on stakeholders in cyber security information sharing ecosystem, and mathematical model that measure the generated values through the value exchange.

### 3.4.1 Interrelationship Among Stakeholders and their Value Exchanges

The identification of stakeholders is necessary for organizations to meet their targets, fulfill their missions and create value (Bryson, 2004). The stakeholder theory (Mitchell, Agle, & Wood, 1997) suggests to identify the stakeholder's groups, who are affected by and can affect other stakeholders in cybersecurity information sharing ecosystem through their roles. Five types of stakeholders have been identified in the cybersecurity information sharing ecosystem: cybersecurity solution providers, information providers, end users, government agencies and standardization organizations. The roles of these stakeholders are described in detail in ***Section 2.1.1***. In the cybersecurity information sharing

ecosystems: cybersecurity solution providers, information providers and end users are involved directly in value creation and exchange. Therefore, we consider them as the main actors of the value exchange system of the cybersecurity information-sharing ecosystem. The literature on cybersecurity information sharing primarily focus on the public-private collaborations, however, other types of relationships also exist such as one-to-one partnerships and groups solely comprised of private organizations (Harkins, 2016). The relationship among the stakeholders is given the ***(Figure 6)***.

The cybersecurity information sharing ecosystem provides an environment, in which stakeholders collaborate with each other and share information to improve the cybersecurity posture and enables the value exchange among the groups of stakeholders. The cybersecurity solution offer an intermediary role between the information sources and end users, which enables the information processing, utilizing and dissemination. For this study, we are not considering the competition between cybersecurity solution providers. Therefore, the additional interactions (such as brand name) compared with other cybersecurity solution providers are also does not considered. The end users can receive the cybersecurity information from different information sources i.e. the same information from different information sources helps end users to verify it and build their confidence on the authenticity of the information. The end users may be subscribed to multiple information sources and receive information in different formats. In some scenarios, one stakeholder executes all the roles simultaneously in the cybersecurity information sharing ecosystem i.e. cybersecurity solution provider, information provider and end user. While in

some other cases one stakeholder can play the roles of cybersecurity solution provider and information provider. The end users are stakeholders, who are not only end users of cybersecurity solution and information but also the producers of cybersecurity information and cybersecurity solutions and tools. The end users are basically utilizing the cybersecurity information in their own context but they are also generating some information which they are sharing within the trusted communities. Similarly, the end users are also developing tools or solutions in response to some vulnerabilities and sharing it in the trusted communities from where other end users are benefiting from those solutions. Some cybersecurity solution providers also offer the development tools or kits to the end users.

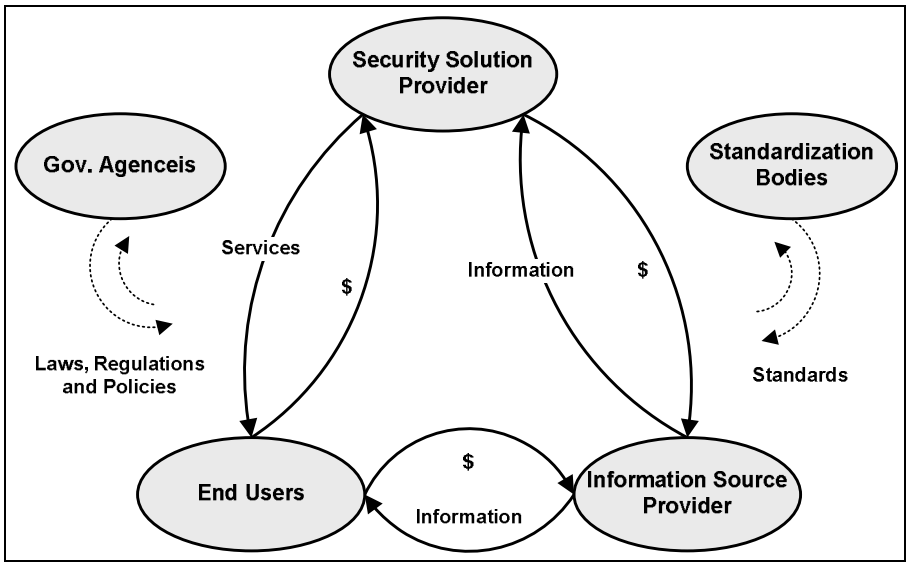



**Figure 6. Interrelationship among the Stakeholders of Cybersecurity Information Sharing Ecosystem**

These tools are used by the end users to develop some small solutions, which can be deployed on the platform which is provided by the cybersecurity solution

provider. However, in the context of this research work we are considering that all the stakeholders are separate and are treated as independent entities.

There is a direct value exchange among the stakeholders (i.e. direct payment of offered services), resulting in net utility for end users, utility (profit or loss) for the cybersecurity solution provider, as well as utility (profit or loss) for cybersecurity information provider. The value exchange among the stakeholders of cybersecurity information sharing is depicted in ***(Figure 6)***. The value exchanged between a cybersecurity solution provider, information provider and end users includes the provisioning of cybersecurity software solutions or services and cybersecurity information in exchange for fees or a share of the cybersecurity solution provider's revenue obtained from their end users. The share of cybersecurity solution revenue happens when the cybersecurity solution provider sells the bundles i.e. bundle of cybersecurity solution and cybersecurity information from some information sources. In this case, the revenue generated by the cybersecurity solution provider is shared with the cybersecurity information as per their agreement. The cybersecurity solution and information providers provide their products to end users either as a software solution, pre-packaged software product, a premium threat feed or as a customer-specific report. To both, cybersecurity solution provider and information provider, the end users are the main source of revenue in the cybersecurity information sharing ecosystems.

### 3.4.2 Value Parameters and their Effects on Stakeholder's Values

This section described the value parameters that determine the values obtained by stakeholders in the cybersecurity information sharing ecosystem. These parameters are directly affecting the values of stakeholders in the ecosystem. They indicate the sources of value generation and are used for quantifying stakeholder's values in the ecosystem. The impact of these parameters is important to understand for cybersecurity solution providers and information providers for effectively formulating strategies and policies for their businesses.

The existing literature provides value creation framework in e-business (Amit & Zott, 2001), success factors and their relationship in web 2.0 service business (Amit & Zott, 2001), and parameters of value creation related to software service platforms (Haile & Altmann, 2012, 2016). In this work we identified a set of value parameters and presented a value creation model in which the effect of these parameters on the stakeholder's value can be measured in different scenarios of cybersecurity market. In the proposed value creation model, seven value parameters have been identified based on the literature survey in the area of cybersecurity information sharing. This set of value parameters considers quality of information (QoI), quality of service (QoS), installed base (i.e. number of end users in the ecosystem), timeliness, trust, cost and trusted communities. These value parameters are utilized in constructing value creation model and for quantifying values of stakeholders. The value parameters and their interrelations as observed in cybersecurity information sharing ecosystem are shown in ***(Figure 8)***.

As shown in ***(Figure 7)***, the values of stakeholders are affected by the parameters in positive or negative manner and are represented by (+) and (-) symbols on arrows heads respectively.

The number of end users (i.e. installed base) and the cost (i.e. cost of utilizing cybersecurity solution or services and information) are the two parameters which affect the values of all the stakeholders. The value of cybersecurity information provider is effected by three more parameters i.e. timeliness, QoI and trust. While the value of cybersecurity solution provider is effected by two additional parameters i.e. trusted communities and QoS. However, the value of end users is effected by all the parameters.

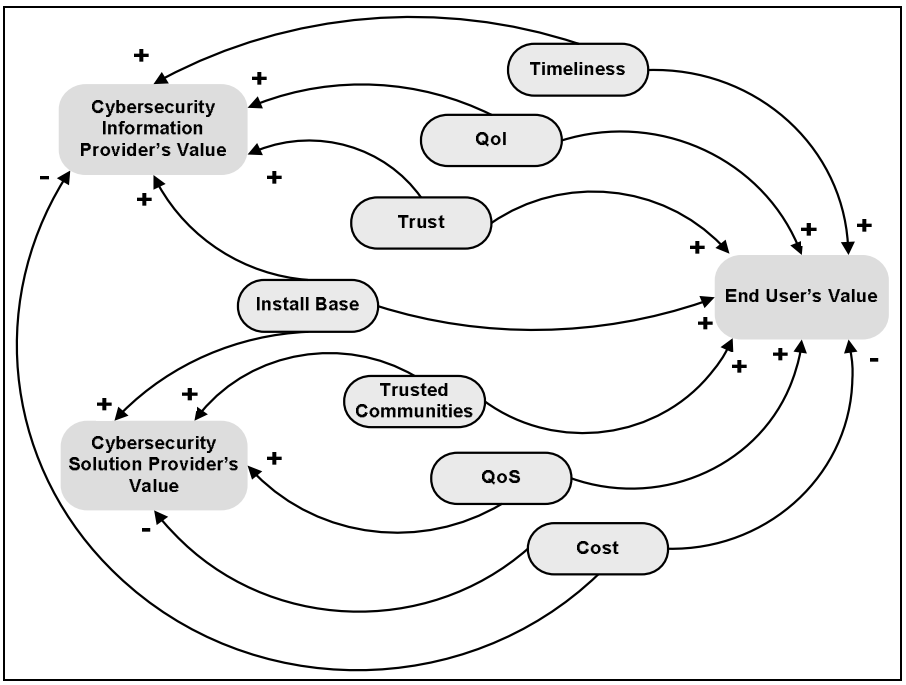



**Figure 7. Effects of Value Parameters on the Values Obtained by the Stakeholders**

The installed base has a positive effect on the values of stakeholders and it attracts more end users (Amit & Zott, 2001; Haile & Altmann, 2012, 2016). The cybersecurity solution provider and information provider can gain a competitive advantage by leveraging the network of a large number of users. In such scenarios, network effects also play an important role in attracting more end users and are considered as the business strategy (Haile & Altmann, 2012). The installed base enables the value co-creation and has positive impact on values of all the stakeholders in the cybersecurity information sharing ecosystem. We consider the installed base is same for both cybersecurity solution provider as well as information provider.

Cost negatively impacts the values of all stakeholders in the cybersecurity information sharing ecosystem. For end users, there are majorly two types of cost involved in using cybersecurity information i.e. cost of cybersecurity solution and cost of cybersecurity information. Increase in one stakeholder's cost increases the value of another stakeholder. For instance, if the cost of cybersecurity solution is high than the value gained by cybersecurity solution provider increases while the end user's value decreases. The higher cost of improving the QoS of cybersecurity solution indirectly affects the installed base. The cybersecurity information providers are separate entities but in some scenarios, the cybersecurity software solution providers bundle the information from the information provider with their solutions and sell the complete bundle to the end users.

The QoI, QoS, timeliness, trust and trusted communities are the parameters that positively drives the values of all the stakeholders in the ecosystem and attracts

more end users to the installed base (Haile & Altmann, 2012, 2016). All these parameters impact the decisions of end users to join the cybersecurity information sharing ecosystem. The parameters also impact other parameters as shown in ***(Figure 8)***, which enables the value creation in the ecosystem. As shown in ***(Figure 8)***, the installed base of end users impacts the other parameters i.e. QoS, QoI, trust and cost. It determines the revenue that can be used towards improving QoS and QoI. The cost of the cybersecurity solution and information provider can be compensated with the large size of installed base. QoI and QoS impacts the trust of installed base of end users i.e. more end users can be attracted if the existing installed base have trust on cybersecurity solutions and available information. The benefits of end users are also impacted by the size of installed base, as more number of end users increases the size of trusted communities that determines the potential information exchange.

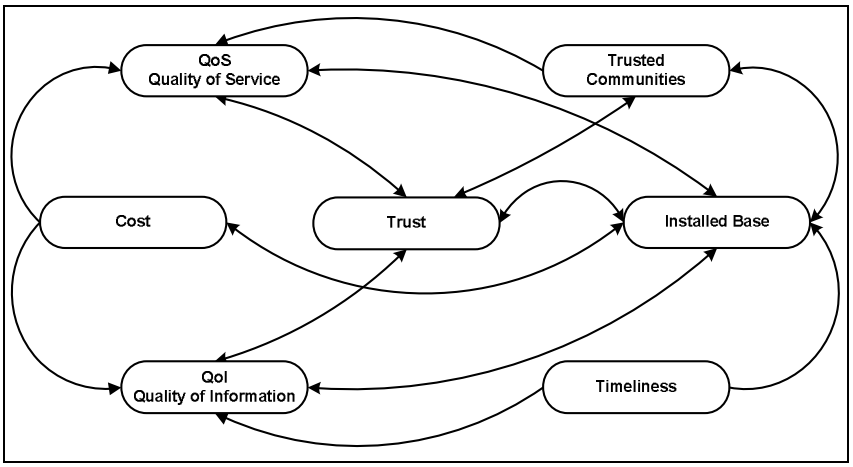



**Figure 8. Interrelationship among the Value Parameters**

This information exchange due to the trusted communities increases the QoS of the cybersecurity solution provider because the solution provider is providing the platform for creation of trusted communities. The QoI is

improved with the timeliness of cybersecurity information which can improve the trust of end users on the information provider. The parameters of trust, QoS, QoI and timeliness positively impacts the size of installed base of end users. Cost has a major impact on the growth of the installed base and it also determines the level of QoS and QoI that can be implemented cybersecurity solution and information providers.

In the following subsections, the above discussed value parameters will be described in detail and an explanation is also given on how they impact each of the three stakeholder values.

#### 3.4.2.1 Quality of Service (QoS)

The QoS is related to the cybersecurity solutions and is used to measures the functional and non-functional capabilities of cybersecurity solutions. It majorly indicates whether functionality, interoperability with different types of information (described in ***Section 2.1.5***), and performance of cybersecurity solutions are up to the requirements of end users and meet the intended objectives of improving the cybersecurity. The main functionalities provided by the cybersecurity solution includes information collection, searching & querying, correlation, pattern matching, data enhancement & contextualization, reports generation, information distribution & dissemination, automation and integration with existing systems (Appala, Cam-Winget, McGrew, & Verma, 2015; Brown et al., 2015; Sauerwein et al., 2017; Sillaber, Sauerwein, Mussmann, & Breu, 2016). ***(Figure 7. Effects of Value Parameters on the Values Obtained by the StakeholdersFigure 7)*** shows the positive impact of QoS on the values for solution provider and end users, and offered QoS is also

used to determine the obtained values of these stakeholders. Better QoS also have impact on the installed base and trust which enables to attract more end users that ultimately increases the size of installed base ***(Figure 8)***.

Achieving the high level of security posture is a complex activity, thus the requirements of end users are dynamic in nature. Therefore, cybersecurity solution providers invest in new functionalities to improve the QoS of their solutions to fulfill the dynamic requirements of end users (Rashid, Noor, & Altmann, 2019) and make their solutions more valuable to end users. The QoS of cybersecurity solutions can be constant or dynamic, if solution providers do not invest the QoS remains at constant level while investing in the new functionalities or improving the existing one results in improved QoS i.e. dynamic QoS. The cybersecurity solution providers can manage the market leadership by providing the dynamic QoS to the end users. In this work, we assume that an increase in revenue is the benefit obtained by cybersecurity solution providers due to high QoS.

#### 3.4.2.2 Quality of Information (QoI)

High quality cybersecurity information is essentially required by end users to take proactive actions in response of potential cyberattacks and achieve high level of cybersecurity (Al-Ibrahim, Mohaisen, Kamhoua, Kwiat, & Njilla, 2017; Appala et al., 2015; Sauerwein et al., 2017; Sillaber et al., 2016). Security managers considered quality information as an important tool in making the tactical, operational and strategic decisions. The reduced uncertainty in security issues due to access to quality information improves the cybersecurity planning which reduces the cost, improve the effectiveness and drives value creation in

the ecosystem. Scarce information sharing and poor quality of cybersecurity information seems to have an impact on the effectiveness and efficiency of the end users. The QoI of cybersecurity information considers the issues of correctness, relevance, completeness, accuracy, uniqueness, consistency, specific, actionable, prioritization and integration of information from several information providers (Dave Shackleford, 2018). ***(Figure 7)*** shows the positive impact of QoI on the values for information provider and end users. High level of QoI also impact the installed base and trust which enable to attract more end users which ultimately increase the size of installed base ***(Figure 8)***. The low level of QoI ultimately negatively affect the values of information providers and end users.

#### 3.4.2.3 Installed Base

The installed base is represented by the number of active end users in the cybersecurity information sharing ecosystem. The values of all the stakeholders are effected by the installed base and is considered as a main source of revenue and end user's utility in the ecosystem. ***(Figure 7)*** shows the positive effects of installed base on the values of all the stakeholders in the ecosystem. The positive effects of installed base can be explained trough the network effects (Clements, 2004; Haile & Altmann, 2012, 2016; Katz & Shapiro, 1985, 1986; Liebowitz & Margolis, 1994). The network effect is beneficial for all the stakeholders and attracts even more end users. The cybersecurity solution and information providers can leverage their user network to gain a competitive advantage. The cybersecurity market analysis shows that the cost of cybersecurity solutions and information is very high (Robb, 2007) (i.e. from

hundreds to thousands of USD). Therefore, end users are very cautious to adopt the new cybersecurity solutions and are less likely to switch to other solutions. The size of installed base also impacts the other parameter i.e. QoI, QoS, trust and cost which enable to attract more end users which ultimately increase the size of installed base ***(Figure 8)***. The network effects due to large number of end users in the installed base is the business strategy of the cybersecurity solution and information providers. The cybersecurity and information providers can compensate their costs with the more number of end users in the installed base. Therefore, cybersecurity solution and information provider have the advantage to stay competitive among the competitors, if they have critical mass of end users. In the cybersecurity information sharing ecosystem, the direct and indirect network effects come into play (Rashid et al., 2019). The increase in the number of end users reinforced by the installed base is explained by the phenomena of direct network effect. The indirect network effect can be explained as the increase in QoS, QoI, timeliness and trust due to the increase installed base, which enables more end users to join the cybersecurity ecosystem.

#### 3.4.2.4 Cost

Cost has negative effect on the values obtained by all the stakeholders in the cybersecurity information sharing ecosystem ***(Figure 7)*** and it also impacts the other parameters i.e. QoI and QoS ***(Figure 8)***. In this model, cost is used to represent all types of costs incurred by the stakeholders. The end users have to incur majorly two types of costs: cost of cybersecurity solution and the cost of cybersecurity information. The end users have to pay the usage fee based on

pricing model such as monthly or annual subscriptions. The subscription fee also considers the factors such as number of users and deployment models of the solution. The deployment models can be web based applications, API interfaces, cloud based systems, distributed application and premise-dependent models. Similarly, end users have to pay for cybersecurity information depending on pricing model i.e. free with limited records, annual or monthly based subscriptions.

On the other side, the cybersecurity solution and information providers face costs for solutions and services offered such as maintenance cost and end users support. The net value of cybersecurity solution and information providers increases due to reduction in the cost of service offering through improved efficiency (Amit & Zott, 2001). In the cybersecurity information sharing ecosystem, increase in the values of solution and information providers might result in a decrease in the value of end users. For instance, if the price of cybersecurity solution or information is set high, the end user's utility will be negatively affected while the revenue of other stakeholder's increases.

#### 3.4.2.5 Trusted Communities

To improve the cybersecurity level, organizations having common interest collaborate and share information among each other and are referred as trusted communities (Serrano et al., 2014). Trusted communities play important role by disseminating up to date information in the cybersecurity information sharing ecosystem. End users can get valuable information from different types of communities such as public and private cybersecurity information sharing communities (Harkins, 2016; Serrano et al., 2014). The cybersecurity

information shared in trusted communities enable end users to have better awareness about the cyber threats and their mitigations (Zhang, Patwa, & Sandhu, 2016). Communities can be open, formal, self-organizing or informal groups that drive through voluntary cooperation and serve as a forum to value exchange (Serrano et al., 2014). Most of the cybersecurity solutions offer the platform to enable the community collaboration among common interest entities ([TC], 2018; Wagner et al., 2016) and allow voluntary contribution from which other member of community can extract value. The size of communities is proportional to the size of the installed base and also proportional to the amount of value co-creation activities in the ecosystem. Trusted communities positively impact the values obtained by cybersecurity information providers and end users as shown in ***(Figure 7)*** and also drives the QoS and installed base as shown in ***(Figure 8)***.

#### 3.4.2.6 Timeliness

Cybersecurity information is effective only if it holds the characteristics of timeliness. It is a measure of how cybersecurity information remains valid, current, and allow sufficient time for recipient to take appropriate action against emerging cyberattacks. Timely sharing of cybersecurity information gives early signals for corrective actions and is valuable in the cybersecurity information sharing environment (Appala et al., 2015). For instance, if an organization receives an alert after security breach is already done the damage is already done i.e. the received information does not remain current and does not allow sufficient time to respond. Delayed information results in end user's dissatisfaction, increase in damage costs in case of cyberattacks and ineffective

decision making. Several surveys such as (Dave Shackleford, 2018) mentioned that lack of timely information is the biggest concern of cybersecurity professionals. In order to make effective and efficient decisions in the area of cybersecurity, the decision makers should have access to quality information in timely manner (Serrano et al., 2014; Sillaber et al., 2016). The timeliness of cybersecurity information positively impact the values obtained by cybersecurity information providers and end users as shown in ***(Figure 7)*** and also drives the QoI and installed base as shown in ***(Figure 8)***.

#### 3.4.2.7 Trust

(Jøsang, Ismail, & Boyd, 2007) defined trust as the degree to which one party is ready to depend on somebody or something in a situation with a feeling of relative security, with the possibility of negative consequences. The key concepts in this definition are reliability and dependence. The level of reputation can be one metric to measure the trust. In other words, it can said that trust can be developed using the high level of reputation. Furthermore, it can be concluded that the major goal of reputation systems is the establishment of trust between unfamiliar parties.

Trust plays an important role to enable the collaboration in cybersecurity information sharing ecosystem, the collaboration does not materialize unless trust exists among different stakeholders. All the participants in the trusted communities will not share cybersecurity information if no trusts exist among the peers because of factors such as damage of reputation or assumption that this information can be used by attackers.

As shown in the ***(Figure 7)***, trust has positive impact on the values of all the stakeholders. It also influences the other parameters: QoS, QoI, trusted communities, timeliness and installed base as shown in ***(Figure 8)***. In cybersecurity information sharing ecosystem, trust can be defined as the effectiveness, efficiency, reliability or the perception of the desire to depend on cybersecurity solution and information (Safa & Von Solms, 2016). In the literature, the dimensions of verifiability, reputation, believability and provenance that are highly relevant in the cybersecurity information sharing ecosystem (Sillaber et al., 2016). It can be attributed as the relationship among the stakeholders in the ecosystem, specifically trust is the most significant factor to enable value co-creation through information sharing in trusted communities. Several cybersecurity solutions support establishment of trust through internal vetting processes and others techniques that rely on stakeholders to manually build up trust (Sillaber et al., 2016). In this work, we consider trust among the stakeholders as the facilitator in enabling the value creation and co-creation in the cybersecurity information sharing ecosystem.

### 3.4.3 Utility Functions to Quantify Values of Stakeholder

The functioning of an economic system can be understood by establishing the relationship among the variables of the system which are to be analyzed using mathematical models. This section describes the utility functions which we constructed to quantify the values obtained by the stakeholders in cybersecurity information sharing ecosystems. The value parameters (described in ***Section 3.4.2***), their interrelationships and relationships with stakeholders are the basis

of utility functions. These utility functions take the value parameters as input and quantify the profits and utilities of the stakeholders in the ecosystem.

In this work, we consider one cybersecurity solution provider, a variable number of information providers and a variable number of end users collaborate with each other to form the cybersecurity information sharing ecosystem. There is a fixed pool of potential users at any time, who may adopt existing cybersecurity solutions and information sources and then added to installed base of end users. The security solution providers and information providers may enter the market at any time and start to offer their services and sell their products. The end users according to their needs make decisions based on seven parameters for adopting the available cybersecurity solutions and information sources. We will use the system dynamics approach to analyze the model which is based on dimensionless values of value parameters ranging from 0 to 1. Modeling the economic system using the dimensionless approach, helps to decide the relevant variables and how they are related to the system. We have followed the approach used in (Ginevičius, 2008; Haile & Altmann, 2016) to assess the relative importance of value-determining parameters in the model.

#### 3.4.3.1 End User's Value

The net utility function $U_{s,i_{1..n},a}(t)$ of end user is defined based on the value model shown in ***(Figure 7)*** of ***Section 3.4.2***. The utility function $U_{s,i_{1..n},a}(t)$ receives all the functional and non-functional benefits obtained by the end user $(a)$ at a given time $(t)$ towards achieving effective cybersecurity level by utilizing cybersecurity solution $(s)$ and information source(s) $(i_{1..n})$ in the ecosystem. The net utility of end user is the sum of all the positive benefits

minus the cost incurred in utilizing the cybersecurity solution and information sources:

$$U_{s,i_{1..n},a}(t) = \begin{bmatrix} u1_{s,a}(QoS(t)) + u2_{i_{1..n},a}\left(QoI_{i_{1..n}}(t), TL_{i_{1..n}}(t), T_{1..n}(t)\right) + \\ u3_{i_{1..n},a}(IS(t), D_a(t)) + u4_{s,a}(IB_{s,i_{1..n}}(t), TC_s(t)) \end{bmatrix} - [C_{s,a}(t) + C_{i_{1..n},a}(t)] \quad (1)$$

The utility functions $u1$, $u2$, $u3$ and $u4$ represent the perceived values of parameters by end users and are accumulated in the net utility $U_{s,i_{1..n},a}(t)$ of end users. These utility functions are generating values in the range between 0 and 1. The minimum utility is represented by 0 while a value of 1 represents the maximum utility. The values of these utility functions increases to maximum number but always will remain below the value 1 (i.e. maximum utility) showing the asymptotic shape as described in (McDougall & Levesque, 2000), a similar approach has been used in (Ginevičius, 2008). A simple justification for the asymptotic behavior is that the improvement in value parameter perceived by the end user depends on the actual level of value of parameter i.e. less marginal utility is perceived if the actual level of parameter value is high.

The end users obtain the maximum utility is constrained by the end user's capacity to utilize the cybersecurity solution and information. This phenomenon is also explained in the case of service platforms in (Ginevičius, 2008; Varian, 2014). The obtained utility of end users in the cybersecurity information sharing ecosystem can always be maximized by improving the factors such as quality of service, quality of information, or other factors. The value co-creation in the trusted communities can be maximized further even its already at maximum level by enabling volunteer information sharing in the trusted communities.

In equation (1), the utility function $u1_{s,a}(QoS(t))$ represents the utility of user $(a)$ obtained due to exchange of value through the quality of service (QoS), which are the functional and non-functional benefits of adopting the cybersecurity solution $(s)$ at time $(t)$. It is assumed that the value of QoS can never be 0, we consider that the lowest value of QoS is starting from 1 and it can be maximized to highest value (i.e., ∞) by investment in the QoS of cybersecurity solution. Based on this assumption, there is no limit on how much improvement in the QoS can be made, and the improvement in QoS follows the dynamic needs of end users in the ecosystem. As discussed in ***Section 3.4.2***, the increase in QoS also increases the utility of end users. The asymptotic behavior can be chosen for the utility function $u1_{s,a}(QoS(t))$ and can represented by equation $(1.a)$. This representation has the property that if QoS increases from 1 to ∞ it can increase from to 0 to close to but below 1.

$$u1_{s,a}(QoS(t)) \rightarrow \left(1 - \frac{1}{(QoS(t))}\right) \qquad (\mathbf{1.a})$$

The utility function $u2_{i_{1..n},a}\left(QoI_{i_{1..n}}(t), TL_{i_{1..n}}(t), T_{1..n}(t)\right)$ in equation (1) represents the utility of end user $(a)$ obtained due to exchange of value through the quality of information (QoI), timeliness (TL) of information and trust (T) on the information providers. These utilities are the functional and non-functional benefits obtained by using cybersecurity information from information providers $(i_{1...n})$ at time $(t)$. Similar to the case the QoS, the value of QoI can never be 0, we consider that the lowest value of QoI is starting from 1 and it can be maximized to highest value (i.e., ∞) by investment in the QoI of cybersecurity information sources. This assumption allows to improve the QoI to very high level (i.e., ∞), which follows the needs of dynamic needs of end

users in the ecosystem and the current status of the cyber threats and attacks. The ***Section 3.4.2*** gives a brief description about the positive impact of QoI, TL and T on the values of end users in the cybersecurity information sharing ecosystem. The same logic of asymptotic behavior of that we use for the QoS can be applied to $u2_{i_{1..n},a}\left(QoI_{i_{1..n}}(t), TL_{i_{1..n}}(t), T_{1..n}(t)\right)$ and is represented in equation $(1.b)$. This representation has the property that if QoI, TL, and T increases from 1 to $\infty$ it can increase from 0 and close to but below 1 i.e. asymptotic behavior (McDougall & Levesque, 2000). In the cases where end users are using cybersecurity information from more than one the individual values of each information source is summed up to calculate the utility $u2()$.

$$u2_{i_{1..n},a}\left(QoI_{i_{1..n}}(t), TL_{i_{1..n}}(t), T_{1..n}(t)\right) \rightarrow \left(1 - \frac{1}{\left(\sum QoI_{i_{1..n}}(t) + \sum TL_{i_{1..n}}(t) + \sum T_{i_{1..n}}(t)\right)}\right) \qquad (\mathbf{1.b})$$

The third term i.e., $u3_{i_{1..n},a}\left(IS(t), D_a(t)\right)$ in equation $(1)$ represents the value obtained by end users from adopting or utilizing a certain number of available different information sources. The variable $D_a(t)$ denotes the average number of the information sources that an end user utilize at time period $(t)$, whereas $IS(t)$ represents the total number of information sources available in the cybersecurity information sharing ecosystem. In other terms, $u3_{i_{1..n},a}\left(IS(t), D_a(t)\right)$ represents the utility obtained by the end users by adopting the $D_a(t)$ information sources at time $(t)$ from the total available information sources $IS(t)$. The asymptotic behavior of $u3()$ is represented in the equation $(1.c)$:

$$u3_{i_{1..n},a}\left(IS(t), D_a(t)\right) \rightarrow \left(1 - \frac{1}{\left(IS(t) * D_a(t)\right)}\right) \qquad (\mathbf{1.c})$$

The utility $u4_{s,a}\left(IB_{s,i_{1..n}}(t), TC_s(t)\right)$ in equation $(1)$ is the utility that end users obtain from the number of active end users present in the cybersecurity information sharing ecosystem. We consider one cybersecurity solution provider, which has provided the platform to enable end users to create trusted communities. The first form of utility from $u4()$ is due to the variable $IB_{s,i_{1..n}}(t)$, which are the direct network effects that comes from the installed base of the cybersecurity information sharing ecosystem (***Section 3.3.4***).

The second form of utility through $u4()$ is due to the variable $TC_s(t)$ which represents the trusted communities. Majorly these are the benefits that end users obtain due to value co-creation i.e. the end users share cybersecurity information or solutions related to trivial issues or cyber threat in the trusted communities. Mostly these information sharing in trusted communities are on voluntarily basis or any other incentive based sharing mechanism defined by the cybersecurity solution provider. Other end users in the trusted communities take the functional and non-functional benefits. The utility obtained by end users through the value exchange in trusted communities can be described through the value co-creation (***Section 3.3.3***).

In order to limit the value of end users obtained through the utility function $u4()$, we use the asymptotical functional form (McDougall & Levesque, 2000) by applying the same logic as in $(1.a), (1.b)$ and $(1.c)$. The asymptotic behavior of $u4()$ is represented in the equation $(1.d)$:

$$u4_{s,a}\left(IB_{s,i_{1..n}}(t), TC_s(t)\right) \rightarrow \left(1 - \frac{1}{(IB\,(t) + TC\,(t))}\right) \qquad (\mathbf{1.d})$$

The last term $C_{i_{1..n},a}(\mathrm{t}) + C_{s,a}(t)$ in equation $(1)$ is related to the cost that the end user faces in the cybersecurity information sharing ecosystem. We assume that the end users will adopt one cybersecurity solution such as threat intelligence management platform or security information and event management platforms. The first variable is $C_{s,a}(t)$ in $u4()$, which mainly consist of the costs of selecting, purchasing, training and utilizing (i.e., the average usage fee of cybersecurity solution). The second variable $C_{i_{1..n},a}(\mathrm{t})$ represents all the costs incurred by end users during the selection, purchase, processing and using the cybersecurity information for different information providers (i.e., the average usage fee of cybersecurity information). It also includes the cost of time that end users spend to retrieve cybersecurity information from open source information providers, blog or other internal and external information sources. Accordingly, we can consider the linear cost function as shown in $(1.e)$:

$$C_{s,a}(t) + C_{i_{1..n},a}(\mathrm{t}) \rightarrow \left(C_{s,a}(t) + \sum C_{i_{1..n},a}(t)\right) \qquad (\mathbf{1.e})$$

Based on the $(1.a), (1.b), (1.c), (1.d)$ and $(1.e)$ we can rewrite the equation $(1)$ as follows:

$$U_{s,i_{1..n},a}(t) = \left[\left(1 - \frac{1}{(QoS\,(t))}\right) + \left(1 - \frac{1}{\left(\sum QoI_{i_{1..n}}(t) + \sum TL_{i_{1..n}}(t) + \sum T_{i_{1..n}}(t)\right)}\right) + \left(1 - \frac{1}{(IS\,(t) * D_a(t))}\right) + \left(1 - \frac{1}{(IB\,(t) + TC\,(t))}\right)\right] - \left(C_{s,a}(t) + \sum C_{i_{1..n},a}(t)\right) \qquad (\mathbf{2})$$

### 3.4.3.2 Cybersecurity Information Provider's Value

The net value function $U_{i,k}(t)$ of a cybersecurity information provider is defined based on the value model described in ***Section 3.4.2*** is as follows:

$$U_{i,k}(t) = \left[\left(1 - \frac{1}{(QoI_{i,k}(t) + TL_{i,k}(t) + T_i(t))}\right) + \left(F_{i,a}(t) * D_a(t) * \frac{IB(t)}{IS(t)}\right) + RS_s(t)\right] - C_{i,k}(t) \quad (3)$$

where the first term of $U_{i,k}(t)$ describes the utility of the information provider $(i)$ providing the information source $(k)$ received through the quality of information $QoI(t)$, timeliness $TL(t)$ and trust $T(t)$. This term is identical to the one described for the utility of end users, but that was only representing the utility of information provider due to its own $QoI(t)$, timeliness $TL(t)$ and trust $T(t)$. As discussed in ***Section 3.4.2***, the value of information providers also increases with the increase in the utility of end users.

The second term in $U_{i,k}(t)$ represents the revenue of the information provider. The variable $F_{i,a}(t)$ represents the average fee, which an end user $(a)$ pays for using the cybersecurity information to information provider $(i)$ at time period $(t)$. The variable $D_a(t)$ represents the average number of the information sources that an end user utilizes at time period $(t)$. The average number of end users per information source is calculated by the total end users $IB(t)$ in the ecosystem divided by the $IS(t)$ i.e. which represents the total number of information sources available in the ecosystem. It is assumed here, without losing validity of our results, the number of information sources to be equal to the number of information providers. This assumption does not change the results, as our model assumes that the costs of producing information are same for all the information providers.

The third term $RS_s(t)$ is the share of revenue that is shared by the cybersecurity solution provider $(j)$ i.e., the information provider $(i)$ receives the shared revenue. There can be several cases, we are considering that the cybersecurity solution and information provider as separate entities. If the information

provider has an alliance with the cybersecurity solution provider for selling the bundles to the end users than there is a need to consider the effect of revenue sharing on their utilities. The bundle contains the complete package (i.e. cybersecurity solution and information), the end users can buy the complete package from either solution provider or information provider. If the cybersecurity solution is selling the bundles than it will share the revenue with the information provider based on the agreed percentage and information provider will receive the shared revenue and vice versa.

The last term denotes the cost $C_{i,k}(t)$ that an information provider incurs for producing the cybersecurity information. It includes all the costs that information provider faces for supporting end users, new information generation, information storage and processing, maintenance services and the amount of back-end processing needed. The cost $C_{i,k}(t)$ linearly increases with the size of installed base and new information.

#### 3.4.3.3 Cybersecurity Solution Provider's Value

Based on the model described in ***Section 3.4.2***, the net value of $U_{\mathrm{s,j}}(t)$ obtained by the cybersecurity solution provider $(s)$ from offering the cybersecurity solution $(j)$ at a given time $(t)$ is defined as given below:

$$U_{\mathrm{s,j}}(t) = \left[\left(1 - \frac{1}{(QoS(t))}\right) + \left(F_j(t) * IB_j(t)\right) + \sum RS_{i_{1..n}}(t)\right] - C_{s,j}(t) \qquad (4)$$

where the net value $U_{\mathrm{s,j}}(t)$ of cybersecurity solution provider $(s)$ is defined as the utility generated due to the $(QoS)$ and the revenue generated from the end users and sharing of revenue minus the cost for offering the cybersecurity solution $(j)$. With higher utility of cybersecurity solution provider, there are

more incentives for a solution provider to improve QoS of its services or solution to meet the expectations and requirements of end users and also offer more incentives to end users to join the ecosystem and trusted communities.

The first term of $U_{\mathrm{s,j}}(t)$ describes the utility of the cybersecurity provider through the quality of service $QoS(t)$. This term is included based on the discussion in ***Section 3.4.2*** i.e. the value of cybersecurity solution provider increases with the improvement in the utility of end users.

The second term $U_{\mathrm{s,j}}(t)$ represents the revenue of the cybersecurity solution provider. The variable $F_{s,j}(t)$ represents the average fee, which an end user pays to cybersecurity solution provider $(s)$ for using the solution $(j)$ at time period $(t)$. The $F_{s,j}(t)$ is multiplied with the $IB_j(t)$ to get the total revenue of the cybersecurity solution provider.

The third term represents the sum of revenue that has been receive from the information providers in case of alliances for the cybersecurity solution bundles. The fourth term is the sum of the revenues that are shared by the cybersecurity information providers $(i_{1..n})$ as discussed in ***Section 3.4.3.2***. Without losing validity of our results, we are not considering the case of deduction of revenue share that is given to information providers in case of bundling of cybersecurity solution and information sources.

The last term $C_{s,j}(t)$, all the costs that are faced by the cybersecurity solution provider to provide support to end users, development of new functionalities, maintenance of trusted communities, recurring costs and payment of third party services (if any).

## 3.5 Simulation Model Description

### 3.5.1 Implementation

The mathematical value creation utility functions proposed in ***Section 3.4.3***, the relationship of value creation parameters and stakeholders described in ***Section 3.4.2*** are implemented using system dynamics technique and implemented in Vensim software (McDougall & Levesque, 2000). Vensim supports the implementation of system dynamics models and has the capabilities to handle all the scenarios that are discussed in ***Section 3.5.4*** (shown in ***Figure 9***). System dynamics has the capabilities to model the complex interactions among the stakeholders. Our simulation model considers one cybersecurity solution provider, multiple information providers and multiple end users and consider three scenarios with different setting.

In cybersecurity information sharing ecosystem, it helps in understanding the impact of value parameters on the stakeholders, interrelationship among the stakeholders, impact of different strategies for value addition, and the impact of business policy adjustments in response to dynamic cybersecurity market conditions. The cybersecurity solution and information providers can model how improved QoS and QoI results in increased profits, or they can evaluate the needs of investments in infrastructure to improve their quality of services. This type of modeling can help the stakeholders to establish a sustainable cybersecurity information sharing ecosystem.

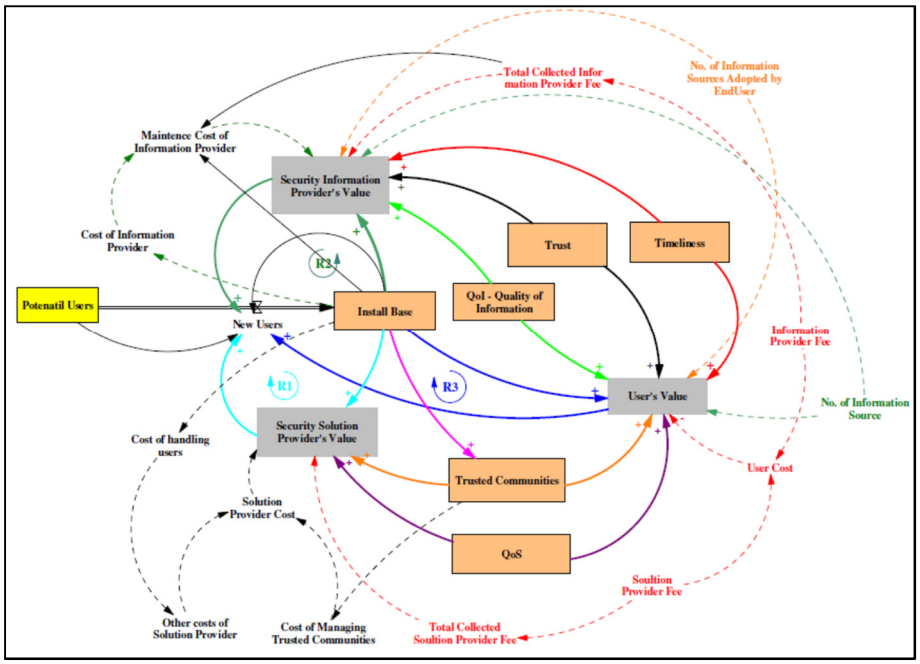



**Figure 9. System Dynamics Model of the Stakeholder's Value Creation (Implementation)**

With respect to QoS, QoI and timeliness, the higher the utilities of cybersecurity solution and information providers are, the more incentive for them exist to improve their products and serveries, so that the expectations and dynamic requirements of end users are fulfilled. The trust on information providers will be established based on the utilities and beliefs of existing end users, and to improve the trust, information providers have to take appropriate measures. The market coverage of cybersecurity market is very low as described in (McDougall & Levesque, 2000), therefore there exists always attractions for the new entrants i.e. information providers joining the cybersecurity information sharing ecosystem. With respect to end users, all these value parameters increase the utility of end users, the higher the end user value is, the more end users will join the ecosystem.

Based on these relationships, we implemented our simulation model and is shown in ***(Figure 9)***. The implementation of our proposed value creation model reveals three positive feedback loops (R1, R2 and R3). The feedback loop (R1) demonstrated that higher the number of end users in the installed base, the more value of solution provider is created, and attracts more end users to join the installed base. Regarding the feedback loop (R2), higher the number of end users in the installed base, the more value of information provider is created, which attracts more end users to join the installed base. According to third feedback loop (R3), higher the number of end users in the installed base, the more value of end user is created through trusted communities, and more users will be attracted to join the installed base.

### 3.5.2 Simulation Settings

The cybersecurity security market has special characteristics of very low market coverage, highly competitive and the survival rate of vendors are very low (McDougall & Levesque, 2000). Therefore, it is necessary to observe the dynamics of value creation and distribution in the cybersecurity information sharing ecosystem for longer time period. Hence, the number of time periods was set to 120 months (i.e., 120 time periods). In our simulation model we are not considering the outflows of solution providers, information providers and end users. The installed base $IB(t)$ is cumulative value increasing through new adoptions over time.

| Table 3. Settings of Variables for Simulation Model of Cybersecurity Information Sharing Ecosystem | | | | | |
|---|---|---|---|---|---|
| **Model Variables** | **Description** | **Reference** | **Scenrio-1: Base Values** | **Scenrio-2: Growing Market** | **Scenrio-3: Saturated Market** |
| $QoS(t)$ | Variable indicates the level of QoS | Assumption based on (Haile & Altmann, 2016) | [1……∞] | [1……∞] | [1……∞] |
| $QoI(t)$ | Variable indicates the level of QoI | Assumption | [1……∞] | [1……∞] | [1……∞] |
| $TL(t)$ | Variable indicates the timeliness of information | Section 3.4.2.6 | 5 | 5 | 5 |
| $T(t)$ | Variable indicates the level of trust on the information provider | Section 3.4.2.7 | 5 | 5 | 5 |
| $IB(t)$ | Variable indicates the size of the installed base | Initial Value | 1 | 1 | 1 |
| $PU$ | Constant representing potential end users | Assumption | 500,000 | 500,000 | 500,000 |
| $F_j(t)$ | Variable indicates average usage fee of cybersecurity solutions | (Robb, 2007) and Scaling | 0.1 | 0.1 | 0.1 |
| $F_i(t)$ | Variable indicates average usage fee of cybersecurity information sources | (Robb, 2007) and Scaling | 0.1 | 0.1 | 0.1 |
| $D_a(t)$ | Variable indicates average number of the information sources that an end user utilizes | Assumption based on (Barahona, 2017; Dave Shackleford, 2018) | 5 | 10 | 2 |
| $IS(t)$ | Constant describes the total number of information sources available in the ecosystem | Market Research | 100 | 100 | 150 |
| $TC_s(t)$ | Variable indicates average size of trusted communities | Assumption | 70% of $IB(t)$ | 70% of $IB(t)$ | 70% of $IB(t)$ |
| $C_{i,k}(t)$ | Variable indicates average cost of information provider for generating cybersecurity information | Assumption (Details are in Section 3.6.2) | 5 % of Revenue | 5 % of Revenue | 5 % of Revenue |
| $C_{j,s}(t)$ | Variable indicates average cost of solution provider for generating cybersecurity solution | Assumption (Details are in Section 3.6.2) | 5 % of Revenue | 5 % of Revenue | 5 % of Revenue |
| $RS(t)$ | Constant describes the percentage of share of revenue that is shared by the cybersecurity solution or information provider | Assumption based on (Haile & Altmann, 2016) | 0.7 | 0.7 | 0.7 |
| ***Rate of growth of new end users per month*** | | | | | |
| • | Linear Growth | Scenario 1 | 200 | 200 | 100 |
| • | Exponential Growth | Scenario 2 | 10 % of existing $IB(t)$ | 10 % of existing $IB(t)$ | 05 % of existing $IB(t)$ |
| • | Logistic Growth | Scenario 3 | LN ($PU$ / $IB(t)$ ) * ( $IB(t)$ * 0.03 ) | LN ($PU$ / $IB(t)$ ) * ( $IB(t)$ * 0.03 ) | LN ($PU$ / $IB(t)$ ) * ( $IB(t)$ * 0.03 ) / 2 |

The ultimate goal of improving cybersecurity level describe the behavior of end users, it is assumed that an end user is utilizing more than one different types of information from multiple information sources. One information provider may offer multiple types of information. In our simulation scenario, we are considering only commercial cybersecurity solution and information provider. This means that end users have to pay in return for using solutions and information.

In our scenarios, the value parameters are implemented to dynamically show an increase in values as utilities of end users, cybersecurity solution and information providers increases. The ratio of revenue share is set to 70%, similar to the implementation of (McDougall & Levesque, 2000). The details of the values of variables is mentioned in ***(Table 3)***.

### 3.5.3 Model Validation

A system dynamics model is usually validated using two approaches i.e. behavioral validation and structural validation.

The behavioral assessment emphases on the behavior of model during execution and evaluates the confidence that can be put in the results (Barlas, 1989; John D Sterman, 2000). For behavior assesment we conducted the extreme condition testing and sensitivity analysis. The extreme condition analysis evaluates whether the model's parameters are appropriately behaving under extreme conditions (Barlas, 1989; John D Sterman, 2000). The results were inspected for any strange behaviors and also evaluated for expected logical consistency. Sensitivity analysis enquires whether variation in assumptions over the plausible range of uncertainty have impacts on the

conclusions that are important to the purpose (John D Sterman, 2000). The values of parameters are systematically changed to evaluate whether, the functioning of the model is as per expectations. Further, behavior of each the construct of the model is traced over time. The temporal behavior is examined for fluctuations and tendencies toward extreme values. Any abnormal behavior triggers a deeper examination of all the relevant constructs and may need to restructure and recalibration of the proposed model. In case of any abrupt response, the constructs were adjusted or introduced new constructs to stabilize the behavior of model. The relevant equations were also recalibrated to address the existing anomaly accordingly.

While, in the structural validation it is determined that the model reflects the real world accurately (Barlas, 1989, 1996; Senge & Forrester, 1980; John D Sterman, 2000). For structral validation of the mdoel we perfrom three assesments i.e. structrual assessment, parameter assesment and dimensional consistency. Structural assessment determines whether the structure of model is consistent with available descriptive knowledge of problem in real world which is being modeled. The model consists of constructs including (i.e., vulnerability, attacks, risk, damages, and costs) are all drawn from the existing literature of information security area. The parameter assessment evaluates whether any parameters takes on value outside the prescribed limits, e.g., probabilities greater than 1.

### 3.5.4 Simulation Scenarios Description

The adoption of cybersecurity solutions is described by negative network effects, as if more number of users are using cybersecurity solutions (such as

antivirus, anti-spyware, encryption software or firewalls) then the overall network is secure and consumers are not willing to pay for expensive solutions (McDougall & Levesque, 2000). But in the information sharing ecosystems, the role of cybersecurity information is critical. In addition, the functionalities of cybersecurity solutions particularly used in information sharing ecosystems (such as threat intelligence platforms or security information and event management) are completely different than the normal cybersecurity solutions (such as antivirus, encryption software or firewalls). In addition to commercial information providers, the end users are also participating in information generation through trusted communities and the phenomena can be explained through the concept of value co-creation (***Section 3.3.3***). In this case, the installed base drives the positive network externalities.

In order to analyze the values of stakeholders in the cybersecurity information sharing ecosystem, it is reasonable to choose the following three scenarios: (Scenario 1) the base values for all parameters i.e. reference scenario; (Scenario 2) large size of the install base and increased values for other parameters i.e. high network; (Scenario 3) variation in adoption rate of end users after market saturation starting from time period t = 50. In our simulation model, we selected these three scenarios based on their potentially significant impact on the values of the stakeholders. It is assumed that there is one cybersecurity solution provider, multiple number of information providers and a limited number of potential end users. All these stakeholders are separate entities and their value is created through different utilities. The results of the three scenarios are

compared with each other to evaluate the value implications of all the stakeholders.

#### 3.5.4.1 Scenario-1: Base Values

This scenario uses the base values to generate the reference values of the stakeholders that will be used for comparative analyses of the three scenarios. The scenario settings are given in the ***(Table 3)***. These settings are based on the technical reports, market surveys, vendor's reports and cybersecurity solution provider's web blogs ([A], 2019; [ETSI], 2017; [S], 2002; [TC], 2018; [TQ], 2019b, 2019a; Haile & Altmann, 2016; Irwin, 2014; Johnson et al., 2016; Dave Shackleford, 2018; Wagner et al., 2016). These literature has been use for settings such as size of installed base $IB(t)$, the average usage fee of cybersecurity solution $F_j(t)$, The average fee for the use of information source $F_i(t)$, average number of the information sources that an end user utilizes $D_a(t)$, total number of information sources available in the ecosystem $IS(t)$, the size of trusted communities $TC_s(t)$, the cost of information provider for generating information $C_{i,k}(t)$ and the cost of solution provider for generating solution $C_{j,s}(t)$. The base values of quality of service of cybersecurity solution $QoS(t)$, quality of information $QoI(t)$ and are assumed to start from the satisfactory level and slowly increases based on the other factors approaching the maximum value of 1. There are open source cybersecurity solutions and information sources are available, but these are not providing high level of quality and services. Therefore, we are assuming that most of the utility of end users are generated through the use of commercial solutions and information and they have to pay the fee in return of utilizing their products.

It is assumed that the utility of end users $U_{s,i_{1..n},a}(t)$ is always greater than 0. The adoption rate of end users is varying depending upon the utility of end user $U_{s,i_{1..}a}(t)$, and its increase or decrease is directly proportional to value of existing installed base.. If $U_{s,i_{1..n},a}(t)$ becomes zero, no new end users will join the ecosystem. On the other hand if $U_{s,i_{1..n},a}(t)$ greater than 0, then a certain number of new end users will be added to installed base at time period t + 1. This process will be continued until market saturation; we consider that market is becoming saturated when the size of installed base is becoming equal to 1. The number of new end users is determined at each time period and they are constant or dynamic portion of the potential end users in the ecosystem. In the linear growth rate, it is assumed, that at every time period t, a constant number of new end users join the ecosystem. The other growth scenario i.e. logistic growth rate (Lekvall & Wahlbin, 1973), in which the number of new end users first slowly increases in the beginning but then grows exponentially until a possible maximum. After that point, there will be a decrease in the number of new end users due to market saturation i.e. exponential decrease. The factors such as network effects and market saturation are the theoretical bases behind the logistic growth rate functions. Market saturation occurs as soon as the pool of potential users in a certain market segment decreases, the rate of growth of install base also deceases. This scenario is also implemented in the (Haile & Altmann, 2016) for software service platform using the Gompertz logistic function which grows slowly in the beginning and at the end (Lekvall & Wahlbin, 1973). The second scenario is very rare in the cybersecurity, because the market coverage for the cybersecurity products is very low (around 50%)

and their cost is very high (Dey et al., 2012). So until the reasonable high market coverage of cybersecurity products, it is very rare that the second scenario will appear in the cybersecurity information sharing ecosystem. But the comparison of the two scenarios of adoption rates of new end users is important, as it helps understanding the impact of the number of new end users on the values of stakeholders. we are considering the cybersecurity information sharing ecosystem with one solution provider and n number of information providers. However, in real cybersecurity market, there may be *n* number of cybersecurity solution providers and their numbers increases following a linear growth. The cybersecurity market is highly attractive for new entrants but most them are disappearing within couple of year because the market is highly competitive (Dey et al., 2012). We are not considering the case in which the solution and information providers are becoming out of market.

#### 3.5.4.2 Scenario-2: Growing Market

In this scenario, the size of installed base is large and the average number of information sources at a given time $(t)$ is also increased. The value parameters such as trusted communities and trust is considered as the motivations for attracting more end users and increase of cybersecurity market growth. The improvement in the value parameters such QoS, QoI and timeliness by the cybersecurity solution and information provider also highly contributing in the growth of the market. The growth of the market is implemented in the simulation by the increased size of installed base and the average number information source adoption from 1 source to 10 sources ***(Table 3)***. The impact

of market growth on the values of stakeholders is analyzed by comparing the results of scenario 1 and scenario 2.

#### 3.5.4.3 Scenerio-3: Saturated Market

The adoption rate represents the number of new end users in the cybersecurity information sharing ecosystem, who joins the ecosystem in each time period. This adoption rate of the new end users increases until the point of market saturation and then starting to decrease. The increased adoption rate is considered in the scenario 2 while in this scenario case of decreasing adoption rate of end users has been considered. There can be several causes of decreased adoption rate e.g. high competition, lower QoI & QoS, trust breach or bad performance of timeliness. In the implementation of this scenario, the negative growth rate is assumed to happen at time period t = 100. From this time period onwards, the growth rate (adoption rate) is half of the original growth rate of scenario 1.

## 3.6 Simulation Analysis

In this section, we present the simulation results showing the value creation dynamics for all the stakeholders in the cybersecurity information sharing ecosystem. The results of these scenarios are compared to have better insights about the impact of parameters on the values of the stakeholders. In order to check the reliability of the simulation results, we did the sensitivity analysis to explore the effects of the value parameters on the values of the stakeholders.

### 3.6.1 Comparison of Scenarios

The impact of value parameters on the values of stakeholders has been calculated using the mathematical value creation model proposed in the ***Section 3.4.3***. The dynamics of value creation for the value of end users $U_{s,i_{1..n},a}(t)$, the value of information provider $U_{i,k}(t)$, and the value of cybersecurity solution provider $U_{\mathrm{s,j}}(t)$ has been calculated based on the three scenarios discussed in ***Section 3.5.4***. The simulation results obtained through the three scenarios give insights about the impact of different values of the parameters. The comparison of simulation results of the three scenarios gives indications about the relative importance of the different variables. The number of adopted information sources by end users vary in each of the three scenarios. In the base scenario, it is considered that the end users are utilizing 5 information sources. The growing market scenarios considers that the end users are using 10 information sources while in the case of saturated market the end users are using 2 information sources.

The value obtained by end users in the three cases of base scenario is shown in ***(Figure 10***, ***Figure 11***, and ***Figure 12).***

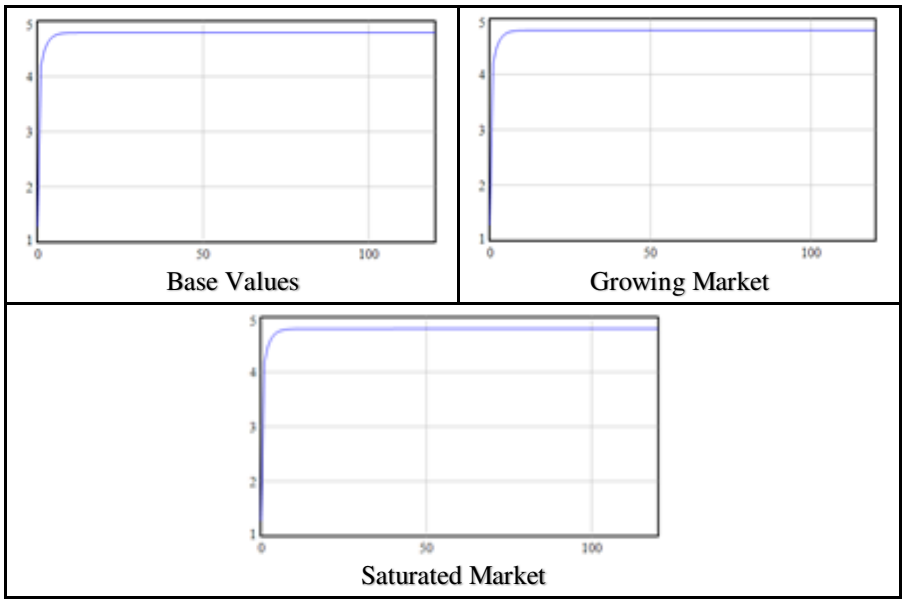



**Figure 10. Values of End Users for the Three Scenarios Using Linear Growth Rate**

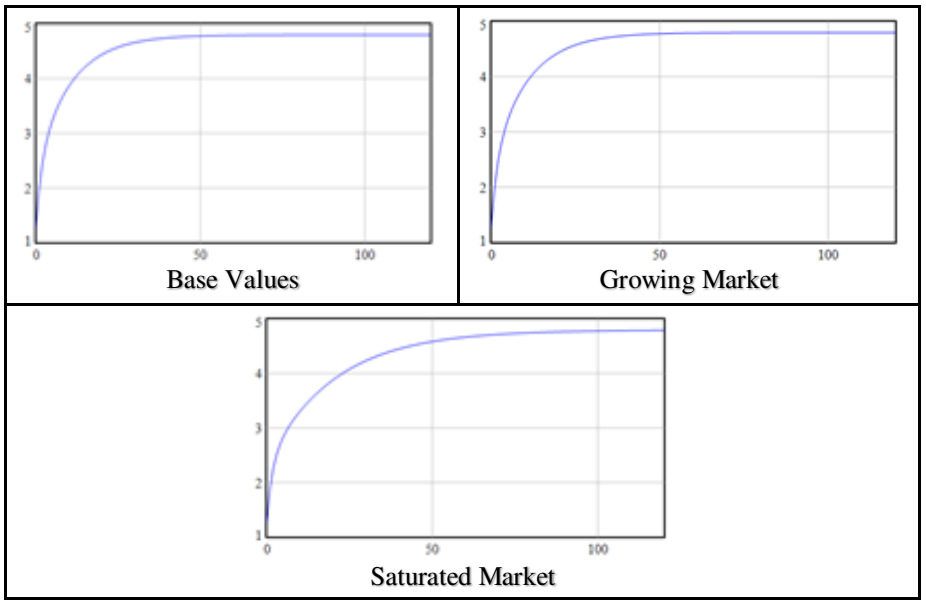



**Figure 11. Values of End Users for the Three Scenarios Using Exponential Growth**

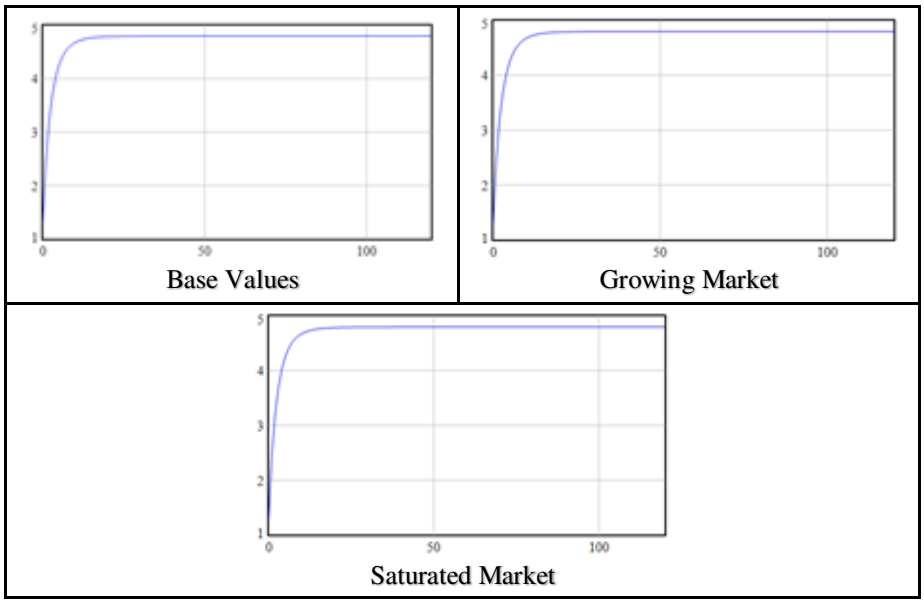



**Figure 12. Values of End Users for the Three Scenarios Using Logistic Growth Rate**

It has been observed that the value of end user at $t = 0$ is $U_{s,i_{1..n},a}(t) > 0$ in three types of growth rates of all the scenarios, because it is necessary to maintain the positive utility for end users in order to keep them in cybersecurity information sharing ecosystems. In the linear growth rate ***(Figure 10)***, the utility of end users grows very fast and reaches of maximum utility at t = 10 irrespective of the market scenario, because there is a linear increase in the install base at each time period. The linear increase in number of end users in the install base make it possible to have sufficient size of install base in few time periods. This is the ideal case, where at each time a fixed number of end users will be added to the install base, but in real case there is no surety of linear growth of market.

In the case of exponential growth rate ***(Figure 11)*** there is slight difference in the value obtained by the end users in different scenarios of market especially in the scenario of saturated market. In the case of exponential growth rate of base and growing market scenario, the value of end user reaches to maximum at t = 60 while in saturated market scenario it takes more time periods i.e. t = 100 to reach to the maximum. The growth of end users in the install base is dependent on the existing size of install base i.e. at starting time period the size of install base is very small and after that it starts to increase slowly. This is the main reason that the end users reach to maximum utility as compare to the base value scenario.

In the logistic growth rate, the growth of utility of end users is independent of the three scenarios ***(Figure 12)*** which is similar to the linear growth rate. If we compare it with the linear growth rate, there is slight difference in increasing pattern during the starting time periods i.e. at t = 40 the end user's utility reaches to its maximum value.

In all the three market scenarios, the install base is very small at the starting time period therefore, at that time the value of end user comes from the QoS, QoI, timeliness and trust. The trusted communities have also no impact on the values of end users in the initial time period because the size of trusted communities are directly proportional to the size of the install base i.e. small size install base leads to small size of trusted communities. Therefore, the cybersecurity solution providers have to keep the QoS from the very beginning to attract more end users to their install base. Similarly, the information

providers have to keep the QoI, timeliness and trust at very high level from the start so that they can attract more end users to their install base.

The utility of end users $U_{s,i_{1..n},a}(t)$ increases and reaches up to almost maximum possible value during the starting time periods. After this point, the growth of end users value becomes very slow and reaches to highest possible utility for all scenarios in the presence of different information sources and network effects. From this time period onwards, there is very little increase in the value of end users, because of the increased costs of utilizing information from more information sources. Further, advanced cyberattacks are also emerging continuously making cyber defense a complex and resource intensive activity. In addition, the utilization of cybersecurity information that is available due to trusted communities also increases the utilization costs of end users. The additional utility obtained is compensated with the additional cost incurred therefore the utility of end users cannot grow further.

The values of information providers $U_{i,k}(t)$ described in (***Equation 3***) for different market growth rates are shown in ***(Figure 13***, ***Figure 14*** and ***Figure 15)*** for all the three scenarios. The information providers can enter at any time into the cybersecurity information sharing ecosystem and offer their services to the end users. We are considering that each information provider offers information that is different from the information of other information providers. For the three scenarios, the growth rates i.e. linear, exponential and logistic show different behaviors. In the case of end users, their values are growing very rapidly and reaches to maximum utilities very quickly, but the situation for the growth of values of information providers is not similar. The

difference in the behavior of the growth of values is due to the initial investment of the end users and the information providers. The cost of one information feed is in the range from hundreds to thousands of dollars per years which are incurred by the end users while in its comparisons the initial investment of information provider is relatively very high. The information providers have to develop the algorithms and technology to gather and process the cybersecurity information. Even in some case they have to put their services on the cloud and have to pay for the cloud infrastructure they are using for offering their services. Therefore, the information provider's initial cost is higher than the cost faced by the end users. The information provider cannot recover their costs of information offering $C_{i,k}(t)$ until they generate sufficient revenue from attracting a large number of end users.

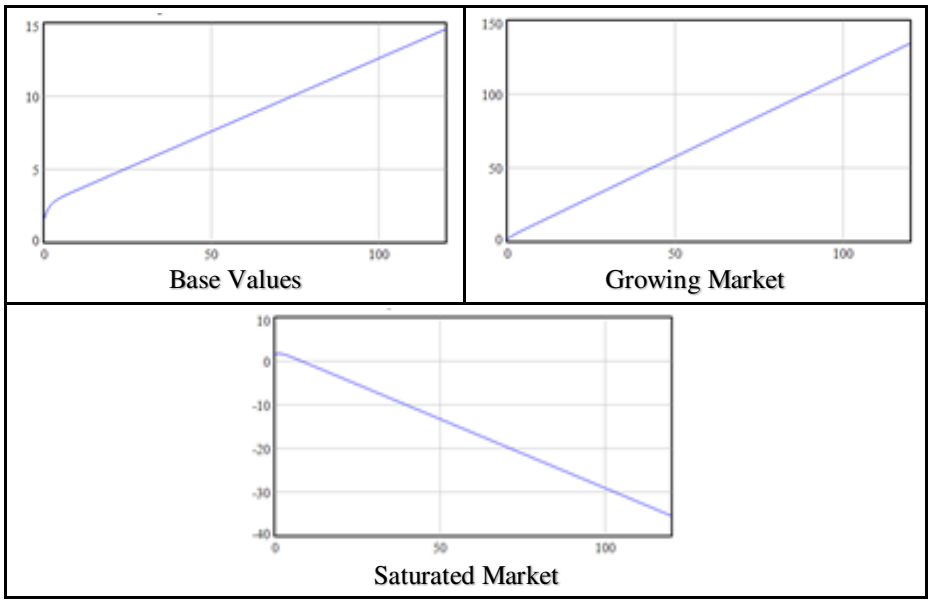



**Figure 13. Values of Information Provider for the Three Scenarios Using Linear Growth Rate**

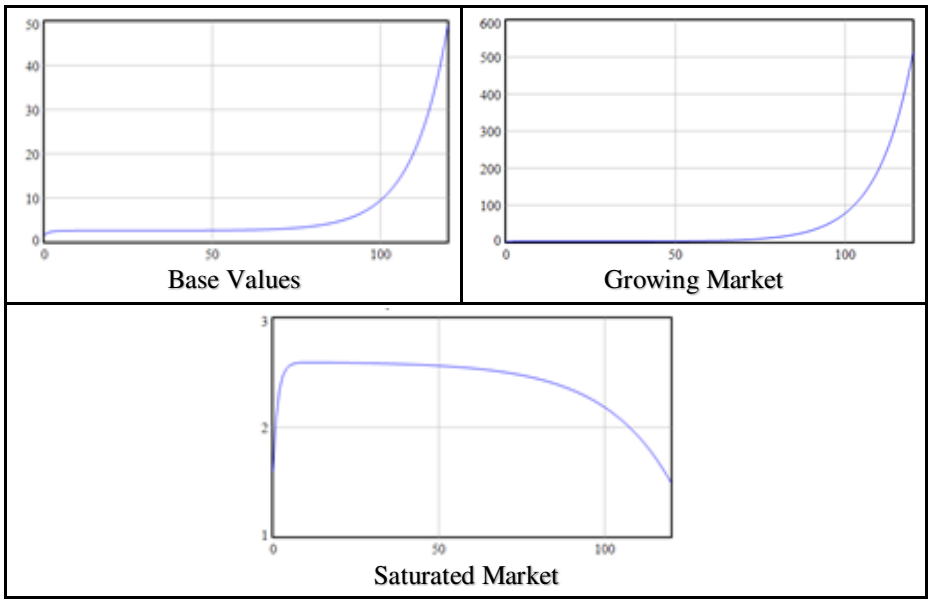



**Figure 14. Values of Information Provider for the Three Scenarios Using Exponential Growth Rate**

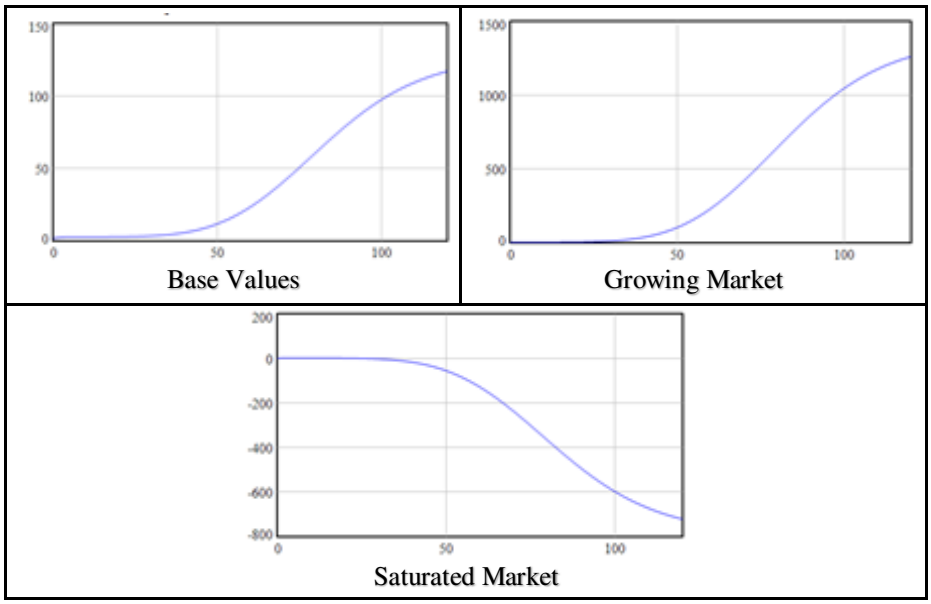



**Figure 15. Values of Cybersecurity Information Provider for the Three Scenarios Using Logistic Growth Rate**

In the case of linear growth rate ***(Figure 13)*** the value of information provider in the base value scenario is starting from the positive side, the growth is little faster in start and after that it grows linearly. The growth is rapid in the beginning because a fixed number of new end users are joining the ecosystem. In the growing market scenario, the adoption of information sources by end users is increased and new end users are dynamically joining the ecosystem based on the existing installed base. The growth of the utility of information provider is linear and reaches to very high value as compared to the base value scenario. This is because in contrast to base value scenario the number of end users increases very rapidly at the later time periods. In the case of saturated market scenario, the number of information sources adopted by end users $D_a(t)$ are reduced to 2 from 10 (as compared to growing market scenario), new users per month reduced to 100 from 200 (as compared to base value and growing market scenario) and also the number of information sources $IS(t)$ increases from 100 to 150 (as compared to growing market scenario). Therefore, in the saturated market scenario of the linear growth rate the value of information decreases linearly, because the number of information sources increases and also adoption of information sources per users also decreased. At each time period, the information provider does not able to generated sufficient revenue and its costs are higher and thus the utility starting to decrease.

In the case of exponential growth rate ***(Figure 14)***, the value of information provider in the base value scenario is starting from the positive side, the growth is little faster at the beginning and after that it grows linearly until t = 50. Afterwards, it starts to grow again and at t = 100 the rapid growth in the value

of information provider has been observed. This behavior is due to that the size of the install base becomes reasonably large and the information providers are generating sufficient revenue. The growing behavior of the utility of the information provider in the growing market is slightly different than the base value scenario. The value of information remains very low near to zero and remained at this level until t = 60. Because the install base is growing at very slow pace, and after achieving the sufficient size of the install base it grows rapidly and reaches to very high level as compared to base value scenario. In the case of saturated market scenario, the values of the variables information sources adopted by end user $D_a(t)$, $IS(t)$ and new users per month is changed to 2, 150, 5% of install base from the values 10, 100, 10% of install base respectively. In this case the value of information provider slightly grows and reaches around 2.3 in the first few time periods, and after maintaining this level for few more time periods is started to decrease. At time period t = 120, the value of information provider decreased to only 0.5. In this case, the value obtained by information provider is very low as compared to base value and growing market scenario. The information provider is not generating sufficient revenue, and it becomes extremely impossible to improve the quality of information (QoI) and timeliness.

In the case of logistic growth rate ***(Figure 15)***, the value of the information provider follows the S-shaped curve on the positive side for the base value and growing market scenario but in the saturated market scenario it follows the negative S-shaped curve. The value of information provider reaches very high (i.e. 1250) in the growing market scenario as compared to the base value

scenario (i.e. 115). In the base value scenario, the value of information started slightly above zero (i.e. 02) and remains at this level at time period t = 25 and after that it started to grow slowly. At t = 100 the growth in the value become slow as compared to growth between time periods between t = 60 to t = 100. In the growing market scenario, the value of information remains at the zero up to t = 35, because at start, the size of install base increases very slowly. But after getting sufficient install base the value of information provider grows rapidly and supersede the value of information provider in the base value scenario. In the scenario of saturated market, the value of information provider stays at zero level up to t = 35 as compared to growing market scenario. But afterwards, because of the saturated market the information providers are not able generate sufficient revenue and its values is decreasing and moves towards the negative side. This situation clearly shows that the reduced number of new end users affects the value for information providers more significantly than the value for end users. The reason is that information provider are mainly generating revenue from new end users. Existing end users can only consume a limited number of information sources, covering the overall capacity of market. The information provider in this scenario is not able to improve the quality of information (QoI) and timeliness due to the insufficient revenue generation. Therefore, the survival of the information provider in the market becomes very difficult.

The values of information providers $U_{j,s}(t)$ described in (Equation 4) for different market growth rates are shown in ***(Figure 16***, ***Figure 17*** and ***Figure 18)*** for all the three scenarios. For the three scenarios, the growth rates i.e.

linear, exponential and logistic show different behaviors. The cybersecurity solution providers can enter at any time into the cybersecurity information sharing ecosystem and offer their solutions and services to the end users. For simplicity, we are not considering the situations of competitions and competitive cybersecurity markets. The behavior of value of solution provider is similar in the linear growth rate for all the three scenarios of market. The only difference is that the value of cybersecurity solution provider is reached at lower level in the saturated market scenario as compared to other two scenarios of the market. The value for the solution provider $U_{j,s}(t)$ at time period t = 0 is 0. The value only increases, if the solution provider starts attracting end users, generating revenue from getting usage fee $F_j(t)$ from end users. The costs $C_j(t)$ that have to be covered by cybersecurity solution providers includes the cost for supporting end users, maintenance cost and the cost of maintaining the trusted communities. The other two market scenarios i.e. growing market and saturated market show different behavior than the base value scenario. In the exponential growth rate ***(Figure 17)***, the value of solution is same and at very high level (i.e. 8200) for the base and growing market scenario but the value of solution provider is very low as compared to other two scenarios. The logistic growth ***(Figure 18)***, follows the s-shaped curve which clearly reflects the different number of new end users joining the information sharing ecosystem at each time period. It highlights the cybersecurity solution provider's strong dependency on end users. In the saturated market scenario, the value of solution provider is nearly to half of the value of the solution provider in the other two scenarios.

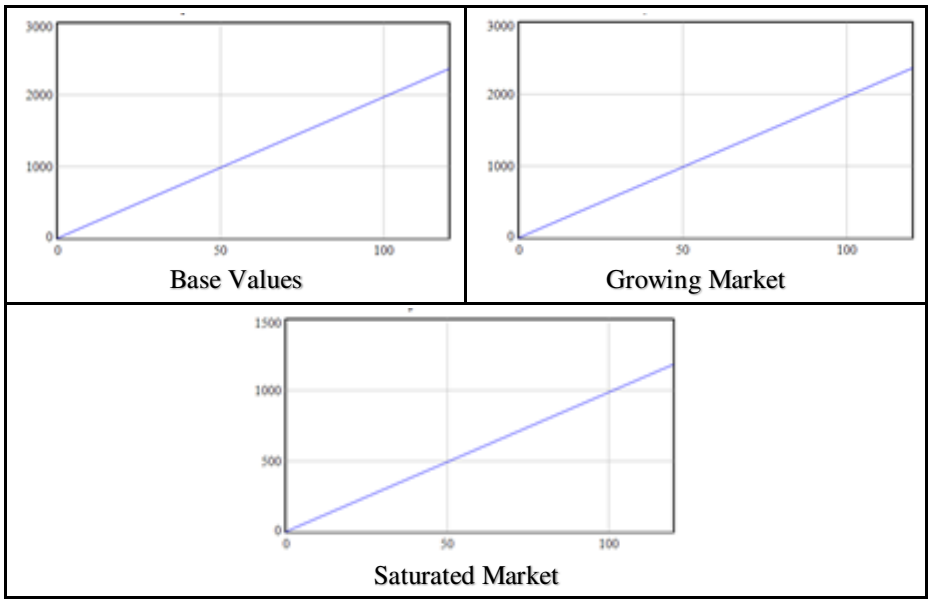



**Figure 16. Values of Cybersecurity Solution Provider for the Three Scenarios Using Linear Growth Rate**

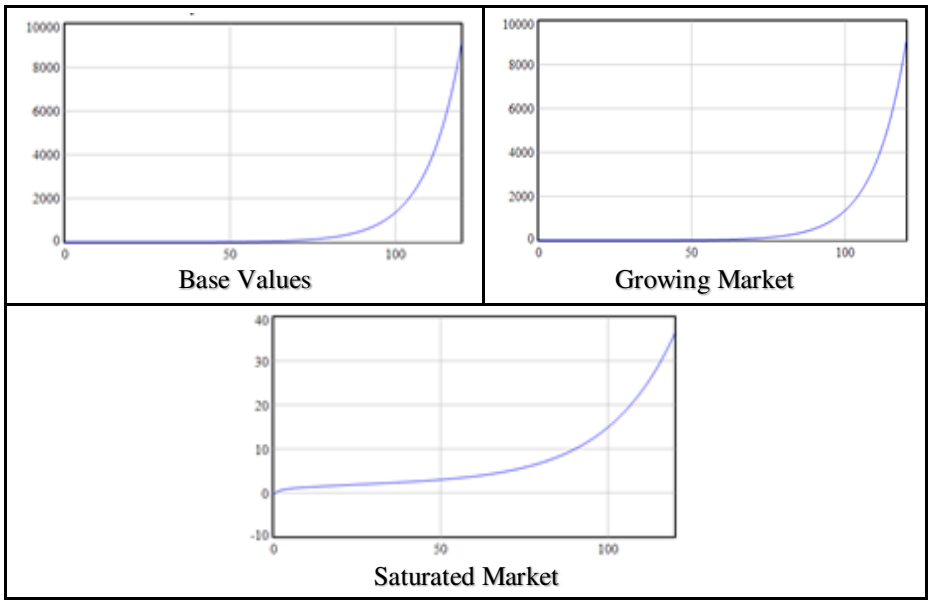



**Figure 17. Values of Cybersecurity Solution Provider for the Three Scenarios Using Exponential Growth Rate**

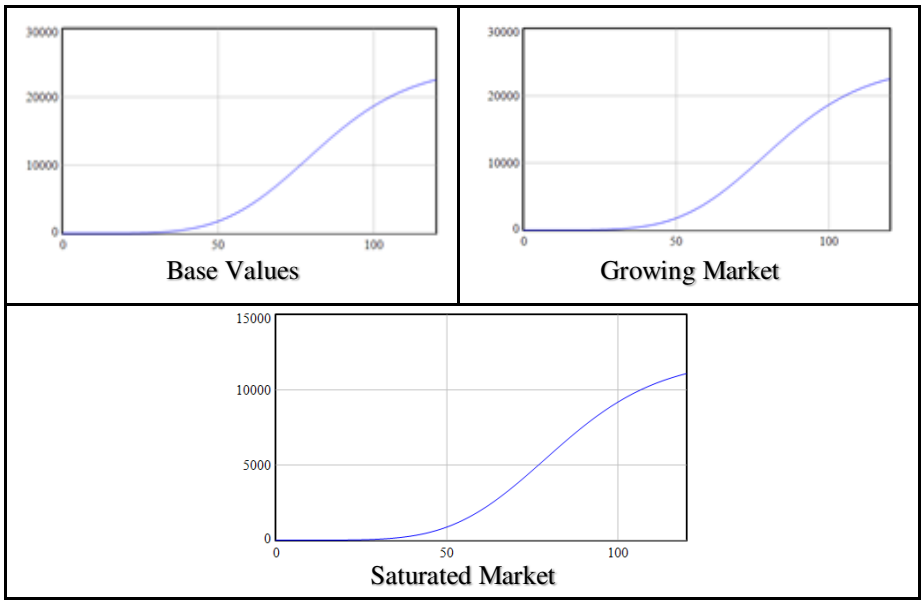



**Figure 18. Values of Cybersecurity Solution Provider for the Three Scenarios Using Logistic Growth Rate**

### 3.6.2 Sensitivity Analysis

Sensitivity analysis determines how varying values of input variables will affect the output of particular dependent variables under a given set of assumptions. In our simulation, we conducted the sensitivity analysis to explore detailed insights about the values obtained by stakeholders in cybersecurity information sharing ecosystem. The sensitivity analysis is conducted with respect to the cost of solution providers for offering their services, usage fee of cybersecurity solutions for end users, cost of information providers for offering information and the usage fee of cybersecurity information sources for end users. We considered 10 different values for each of these simulation variables, which shows the pricing decisions of solution and information providers. All other simulation variables are kept the same, except the variables used for the

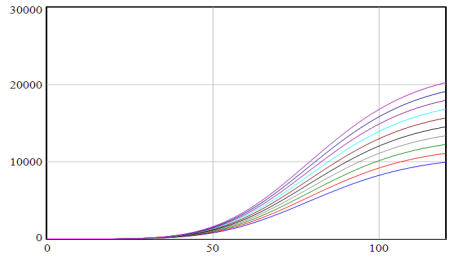
sensitivity analysis. We have considered the variable settings of base scenario (Scenerio-1) with logistic growth rate for the simulation of sensitivity analysis.

#### 3.6.2.1 Sensitivity Analysis of Solution Provider and End Users (with respect to cost incurred by solution provider and fee paid by end users)

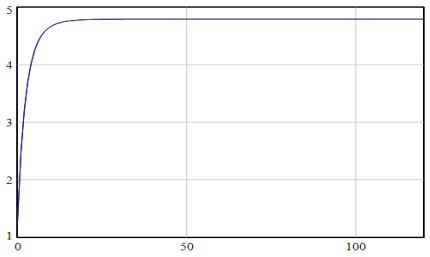
The monthly cost incurred by the solution provider $C_{s,j}(t)$ for offering their solutions and services include the cost of support to end users, development of new functionalities, maintenance of trusted communities, recurring costs (maintenance costs) and cost of acquiring third party services (if any). The cybersecurity solution provider receives the monthly fee $F_{s,j}(t)$ that is paid by end users for utilizing the cybersecurity solution. The monthly fee $F_{s,j}(t)$ (i.e. purchasing prices) for cybersecurity solutions are set by the solution provider depending on their business model. The value of information providers will not be impacted by different values of $C_{s,j}(t)$ and $F_{s,j}(t)$.

For the sensitivity analysis, we used the different values of $C_{s,j}(t)$ and $F_{s,j}(t)$ to analyze the their impact on the utilities of the stakeholders. These variables only effect the values of cybersecurity solution providers and end users. For the first case, the values of $C_{s,j}(t)$ are chosen in the range from 5% to 50% (i.e. 5%, 10%, 15%, 20%, 25%, 30%, 35%, 40%, 45%, 50%), of the total revenue generated per month by the solution provider. The values of $F_{s,j}(t)$ are chosen in the range from 0.1 to 1.0 (i.e. 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0). These values of $F_{s,j}(t)$ are scaled as ( $0.1 \rightarrow 1{,}000$, $0.2 \rightarrow 2{,}000$,……., $1.0 \rightarrow$

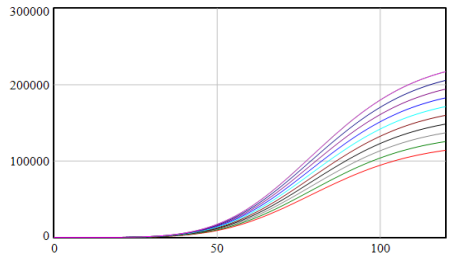
10,000) based on the market survey of the prices of the different cybersecurity solutions (Dey et al., 2012).



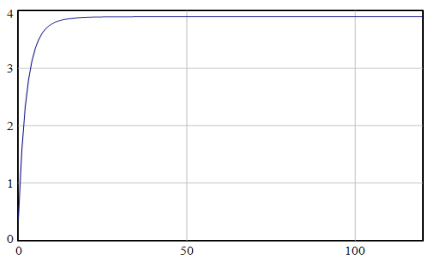

$F_{s,j}(t)$ = 0.1, $C_{s,j}(t)$ = 5%, 10%, ....., 50%




$F_{s,j}(t)$ = 0.1, $C_{s,j}(t)$ = 5%, 10%, ....., 50%




$F_{s,j}(t)$ = 1.0, $C_{s,j}(t)$ = 5%, 10%, ....., 50%

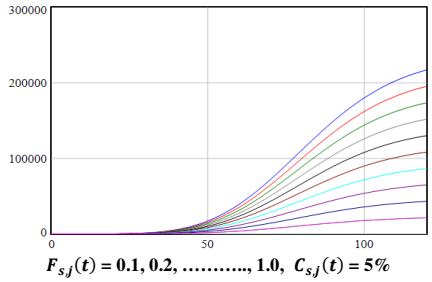



$F_{s,j}(t)$ = 1.0, $C_{s,j}(t)$ = 5%, 10%, ....., 50%

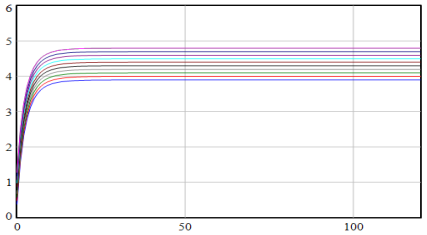
**Figure 19. Sensitivity Analysis of Solution Provider's Value Based on $C_{s,j}(t)$ and $F_{s,j}(t)$**

**Figure 20. Sensitivity Analysis of End User's Value Based on $C_{s,j}(t)$ and $F_{s,j}(t)$**

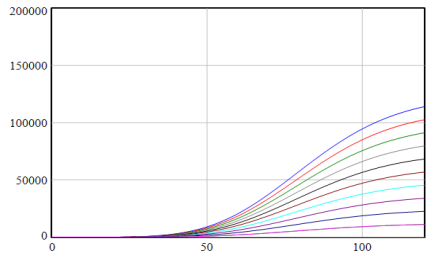
Each value of $F_{s,j}(t)$ is simulated for 10 values of $C_{s,j}(t)$ and the results of boundary values are shown in ***(Figure 19*** and ***Figure 20)***. If we keep the lower boundary value of $F_{s,j}(t) = 0.1$ the value of solution providers remain between 10,000 and 20,000 and the value of end users reaches near 5. For the upper boundary value of $F_{s,j}(t) = 1.0$, the value of solution provider increases and remains between 12,000 and 22,000, while the value of end users decreases below 4. The $C_{s,j}(t)$ has no impact on the value of end users while high value of $F_{s,j}(t)$ decreases the value of end users and vice versa.



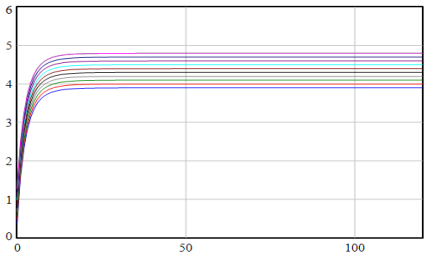

$F_{s,j}(t)$ = 0.1, 0.2, ……., 1.0, $C_{s,j}(t)$ = 5%




$F_{s,j}(t)$ = 0.1, 0.2, ……., 1.0, $C_{s,j}(t)$ = 5%




$F_{s,j}(t)$ = 0.1, 0.2, ……., 1.0, $C_{s,j}(t)$ = 50%




$F_{s,j}(t)$ = 0.1, 0.2, ……., 1.0, $C_{s,j}(t)$ = 50%

**Figure 21. Sensitivity Analysis of Solution Provider's Value Based on $C_{s,j}(t)$ and $F_{s,j}(t)$**

**Figure 22. Sensitivity Analysis of End User's Value Based on $C_{s,j}(t)$ and $F_{s,j}(t)$**

The comparison of the changes in the values of the two stakeholders i.e. solution providers and end users are shown ***(Figure 19*** & ***Figure 20)*** and ***(Figure 21*** & ***Figure 22)***. From these figures the intuitive observations are that, the higher the average cybersecurity solution usage fee is, the less value is generated for the end users ***(Figure 22)*** and the more value is generated for the cybersecurity solution providers ***(Figure 21)***. The value for the end users is the highest for $F_{s,j}(t) = 0.1$ and lowest when $F_{s,j}(t) = 1$. Inversely, the cybersecurity solution providers achieve the lowest revenue at $F_{s,j}(t) = 0.1$ and maximum revenue at $F_{s,j}(t) = 1$. The value of solution provider remains at zero up till time period t = 35, for all the values of $C_{s,j}(t)$ from 5% to 50%, in both the cases of boundary values of $F_{s,j}(t)$ i.e. 0.1 and 1.0. The value of

cybersecurity solution provider started to rise at time period t = 35, because at this stage the install base has sufficiently increased. From this observation we can argue that the value of cybersecurity solution provider does not largely impacted by the cost incurred by them but sufficiently large install base is necessary for significant growth in the revenue. The end users are the most important source of value creation for the solution providers in the cybersecurity information sharing ecosystem.

Similarly, for the second case, each value of $C_{s,j}(t)$ is simulated for 10 values of $F_{s,j}(t)$ and the results of boundary values are shown in ***(Figure 21*** and ***Figure 22)***. The variable values of $F_{s,j}(t)$ have impact on the values of both the stakeholders i.e. cybersecurity solution provider and end users. If the value of $C_{s,j}(t)$ is kept at lower boundary (i.e. cost equals to 5% of the total revenue generated), the value of solution provider will remain with the range of 2,000 to 22,000 and value of end users will remain in the range 3.9 to 4.9. For the upper boundary value of $C_{s,j}(t) = 50\%$ (i.e. cost equals to 50% of the total revenue generated), the value of solution provider decreases significantly and remains between 2,000 and 12,000, while there is no change in the range in the value of end users i.e. between 3.9 to 4.9. If the solution providers, keeps the fee at very low level, and their cost become high than there is no significant attraction for them to keep improving the QoS and introduce new services and solutions. For all the values of $C_{s,j}(t)$ and $F_{s,j}(t)$, the curves of the valued of solution providers and end users shows the similar behaviors as logistic growth in different scenarios mentioned in ***Section 3.6.1***.

#### 3.6.2.2 Sensitivity Analysis of Values of Information Provider and End Users (with respect to cost incurred by information provider and fee paid by end users)

The monthly cost incurred by the cybersecurity information provider $C_{i,k}(t)$ for offering information which includes the cost of support to end users, generation of new information, recurring costs (maintenance costs) and cost of acquiring third party services (if any). The information provider receives the monthly fee $F_{i,a}(t)$ that is paid by end user for utilizing the cybersecurity information. The monthly fee $F_{i,a}(t)$ (i.e. purchasing prices) for information sources or feeds are set by the information provider depending on their business model. The value of cybersecurity solution providers will not be impacted by different values of $C_{i,k}(t)$ and $F_{i,a}(t)$.

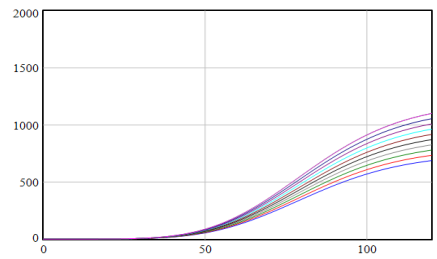
For the sensitivity analysis, we used the different values of $C_{i,k}(t)$ and $F_{i,a}(t)$ to analyze the their impact on the utilities of the stakeholders. These variables only effect the values of information providers and end users. For the first case, the values of $C_{i,k}(t)$ are chosen in the range from 5% to 50% (i.e. 5%, 10%, 15%, 20%, 25%, 30%, 35%, 40%, 45%, 50%), of the total revenue generated per month by the information provider. The values of $F_{i,a}(t)$ are chosen in the range from 0.1 to 1.0 (i.e. 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0). These values of $F_{i,a}(t)$ are scaled as ( $0.1 \rightarrow 1{,}000$, $0.2 \rightarrow 2{,}000$,……., $1.0 \rightarrow 10{,}000$) based on the market survey of the prices of the different cybersecurity solutions and information feeds (Dey et al., 2012). Each value of $F_{i,a}(t)$ is simulated for 10 values of $C_{i,k}(t)$ and the results of boundary values are shown in ***(Figure 23. Sensitivity Analysis of Information Provider's Value Based on $C_{i,k}(t)$***

***and $F_{i,k}(t)$Figure 23*** and ***Figure 24)***. If we keep the lower boundary value of $F_{i,a}(t) = 0.1$ the value of information providers remains between 700 and 1,200 and the value of end users reaches near 5. For the upper boundary value of $F_{i,a}(t) = 1.0$, the value of solution provider increases and remains between 8,000 and 12,000, while the value of end users decreases below 4. The $C_{i,k}(t)$ has no impact on the value of end users while high value of $F_{i,a}(t)$ decreases the value of end users and vice versa.

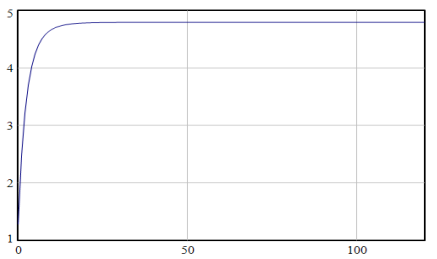
The comparison of the changes in the values of the two stakeholders are shown ***(Figure 23*** and ***Figure 24)***. The intuitive observations are that, higher the average information utilization fee is, the less value is generated for the end users ***(Figure 24)*** and the more value is generated for the information providers ***(Figure 23)***. The value for the end user is highest when the $F_{i,a}(t)$ is set to 0.1 and the lowest $F_{i,a}(t)$ is set to 1. Inversely, the information providers achieve the lowest revenue at $F_{i,a}(t) = 0.1$ and maximum revenue at $F_{i,a}(t) = 1$. The value of information provider remains little above the zero, for all the values of $C_{i,k}(t)$ from 5% to 50%, in both the cases of boundary values of $F_{i,a}(t)$ i.e. 0.1 and 1.0. The value of information provider started to rise at time period t = 40, because at this stage the install base has sufficiently increased.

From this observation we can argue that the value of information provider is not impacted by the cost incurred $C_{i,k}(t)$, but sufficiently large install base is necessary. This behavior clearly represents that the end users are the most important source of value creation in the cybersecurity information sharing ecosystem. The value creation for all the stakeholders come from the number of end users in the cybersecurity information sharing ecosystem only. From

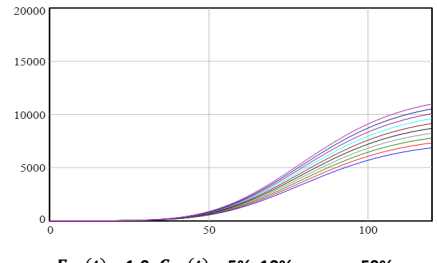
these observations, we can elucidate that these types of cybersecurity information sharing ecosystems needs to have a balanced value exchange between different types of involved stakeholders. Only then, bootstrapping and sustainability of the value exchange is possible.



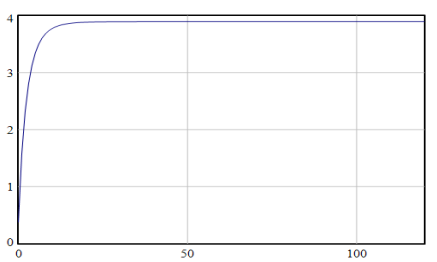

$F_{i,k}(t)$ = 0.1, $C_{i,k}(t)$ = 5%, 10%, ....., 50%




$F_{i,k}(t)$ = 0.1, $C_{i,k}(t)$ = 5%, 10%, ....., 50%




$F_{i,k}(t)$ = 1.0, $C_{i,k}(t)$ = 5%, 10%, ....., 50%



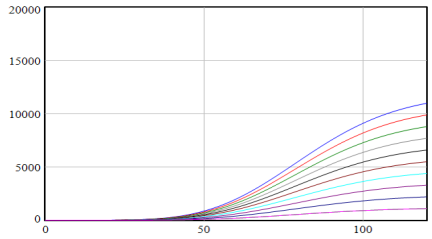

$F_{i,k}(t)$ = 1.0, $C_{i,k}(t)$ = 5%, 10%, ....., 50%

**Figure 23. Sensitivity Analysis of Information Provider's Value Based on $C_{i,k}(t)$ and $F_{i,k}(t)$**

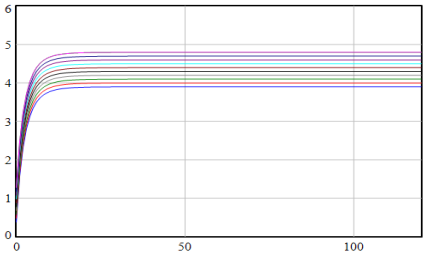
**Figure 24. Sensitivity Analysis of End User's Value Based on $C_{i,k}(t)$ and $F_{i,k}(t)$**

Similarly, for the second case, each value of $C_{i,k}(t)$ is simulated for 10 values of $F_{i,a}(t)$ and the results of boundary values are shown in ***(Figure 23)*** and ***(Figure 24)***. The variable values of $F_{i,a}(t)$ have impact on the values of both the stakeholders i.e. information provider and end users. If the value of $C_{i,k}(t)$ is kept at lower boundary (i.e. cost equals to 5% of the total revenue generated), the value of information provider will remain with the range of 1,000 to 11,000 and value of end users will remain in the range 3.9 to 4.9. For the upper

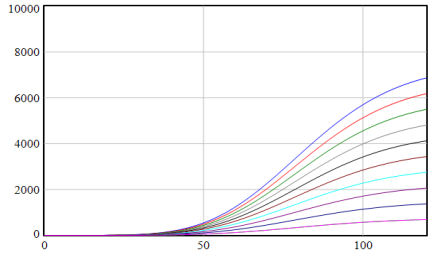
boundary value of $C_{i,k}(t) = 50\%$ (i.e. cost equals to 50% of the total revenue generated), the value of information provider decreases significantly and remains between 400 and 6,400, while there is no change in the range in the value of end users i.e. between 3.9 to 4.9.



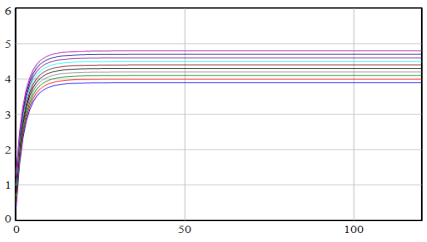

$F_{i,k}(t)$ = 0.1, 0.2, ……., 1.0, $C_{i,k}(t)$ = 5%




$F_{i,k}(t)$ = 0.1, 0.2, ……., 1.0, $C_{i,k}(t)$ = 5%




$F_{i,k}(t)$ = 0.1, 0.2, ……., 1.0, $C_{i,k}(t)$ = 50%




$F_{i,k}(t)$ = 0.1, 0.2, ……., 1.0, $C_{i,k}(t)$ = 50%

**Figure 25. Sensitivity Analysis of Information Provider's Value Based on $C_{i,k}(t)$ and $F_{i,k}(t)$**

**Figure 26. Sensitivity Analysis of End User's Value Based on $C_{i,k}(t)$ and $F_{i,k}(t)$**

If the information providers, keeps the fee at very low level, and their cost become high than there is no significant attraction for them to keep improving the QoI, trust and timeliness of information as well as introducing new types of information and intelligence will not be much attractive. For all the values of $C_{i,k}(t)$ and $F_{i,a}(t)$, the curves of the values of information providers and end

users shows the similar behaviors as logistic growth in different scenarios mentioned in ***Section 3.6.1***.

## 3.7 Discussion and Conclusion

### 3.7.1 Discussion

The simulation results show that the values of stakeholders are interdependent and change in the value of end users affects the values of other two types of stakeholders i.e. cybersecurity solution provider and information provider. More specifically the value of end users is dependent on cybersecurity solution provider and information provider. In the case of cybersecurity solution provider or information provider, their values are not directly interdependent on each other, but depends on the values of end users. The results of the three scenarios (***Section 3.6.1***) and the sensitivity analysis (***Section 3.6.2***), the install base $IB(t)$ (i.e. the number of end users) is emerged as the common determinant that positively effects the values of the stakeholders. It is a necessary condition that end users have positive values for sustainability and bootstrap in the cybersecurity information sharing ecosystem. The positive value of end users is the basis and is necessary for cybersecurity solution provider and information provider to generate revenue. The survival of cybersecurity solution provider and information provider is possible only when they can recover their costs and generate profits, which is only possible if sufficiently large number of end users joined the cybersecurity information sharing ecosystem.

The growth rate assumptions in the three scenarios, reveal that the values of cybersecurity solution providers are much higher than the cybersecurity

information providers (***Figure 13***, ***Figure 14***, ***Figure 15***) and (***Figure 16***, ***Figure 17***, ***Figure 18***). This is because the cybersecurity solutions enable the management of cybersecurity information, in addition quality of information is more useful than the large quantities of cybersecurity information. More cybersecurity information does not directly relate to the higher cybersecurity level information (Johnson et al., 2016; Tounsi & Rais, 2018), instead cybersecurity solution becomes more important for processing and management of cybersecurity. The life of cybersecurity information is short and out dated information adds no additional value to the end users (Tounsi & Rais, 2018). These facts reveal that, the cybersecurity information providers have to put more efforts for collecting, processing and sharing for every newly generated information. Conversely, the cybersecurity solution providers are adding or improving the existing functionalities of their solutions. There is no direct dependency among the cybersecurity solution provider and information providers. Several open source cybersecurity solutions such as MISP (Dey et al., 2012) are available, similarly cybersecurity information is also available as open source such as FS-ISAC ([FS-ISAC], 2019). But, the commercial cybersecurity solutions and information sources adds value in terms of QoS and QoI respectively to achieve higher level of cybersecurity. The end users can use the combination of open source and commercial solution and information sources.

For the information providers, it is more important to fulfill the dynamic requirements of end users and also follow the standard formats and methods for information sharing to survive in the cybersecurity information sharing

ecosystem. The survivability of solution provider and information providers depends upon the values they obtain in the cybersecurity information sharing ecosystem. The assumption of a growing number of new information sources, an upper limit on the average number of information sources that a single end user can use (Scenario 2) and a decrease in the number of new adopters (i.e. end users) because of saturated market or abnormal behavior (Scenario 3) also indicate a sustainability problem for the cybersecurity information sharing ecosystem. It has been observed that, value of cybersecurity solution provider increases in all the scenarios with values of end users greater than zero. While, in case of cybersecurity information providers, their marginal value decreases in the case of saturated market scenario (***Figure 13***, ***Figure 14*** and ***Figure 15***) i.e. the number of new end users joining the cybersecurity information sharing ecosystem starts to decline. This behavior raises the question that whether sufficient value is created for cybersecurity information providers to survive and stay in the ecosystem.

The sensitivity analyses (***Section 3.6.2***) is conducted with respect to the average fee that end users pay in return of utilizing the cybersecurity solution and information, and with respect to the cost of offering cybersecurity solution and information which are to be bear by the solution and information provider. The sensitivity analysis reveals the negative impact of high usage fee on values of end users, while the high costs have negative impact on the values of the cybersecurity solution and information providers. The high average fee reduces the attractiveness of the cybersecurity solution and information and results in

less adoption rate and also the values of end users are significantly decreased (***Figure 22*** and ***Figure 26***).

It has been observed from the market survey (e.g. (Robb, 2007)), the prices of the cybersecurity solution and information is very high i.e. from hundreds to thousands of dollars per year. The implication of the simulation results for the cybersecurity market is that solution and information providers need to focus on finding suitable and flexible pricing scheme that should allow them to sustain for longer time periods in the market and bootstrapping the value creation and distribution between the stakeholders. This results in a sustainable value creation model, that enable innovation in the dynamic cybersecurity information sharing ecosystem. Furthermore, the cybersecurity solution providers and information providers will be able to sustain their services for relatively longer time periods.

### 3.7.2 Concluding Remarks

In this study, we studied the value creation, value distribution and the interdependency among the stakeholders of cybersecurity information sharing ecosystem. We answered the four research questions raised in ***Section 1.4.1***. The ***Section 3.4.1*** discusses the interrelationship among the stakeholders of the ecosystem. Further, this section also explain the sources of value and distribution of value in the ecosystem. The ***Section 3.4.2*** explain the effect of value parameters on the values obtained by different stakeholders. The values of the stakeholders vary in varying scenarios and is explained in ***Section 3.6.1***. In particular, we developed a value creation model for the different types of stakeholders using the additive utility functions. For our study we consider the

three major types of stakeholders i.e. cybersecurity solution providers, cybersecurity information providers and end users. This study is important because previous researches showed that the cybersecurity solution providers can survive for only a couple of years in the cybersecurity markets. Further, the emergence of information providers in the cybersecurity market is not too much old, so this is appropriate and timely to study the value creation and distribution in the cybersecurity information sharing ecosystems.

For using the additive utility functions, seven value parameter have been identified from the literature includes installed base, quality of service (QoS), quality of information (QoI), trusted communities, trust timeliness, and cost. The number of end users are represented by the installed base who are generating the monetary benefits by paying the usage fee to solution providers and information providers in the cybersecurity information sharing ecosystem. The utility of end users is enhanced through the network effects and value co-creation (i.e. value created by the end users through the trusted communities). With respect to cybersecurity solution, QoS represent the functional and non-functional capabilities, which end users uses for improving the level of security and also for managing the cybersecurity information. The QoI represents the benefits which end users have in managing the cybersecurity activities. Majorly, the QoI of cybersecurity information includes the correctness, relevance, completeness, accuracy, uniqueness, consistency, trust and integration of information from several information providers. Trusted communities are the group of organizations having common interest, collaborate and share information among each other and are referred as trusted

communities. Timeliness is a measure of how cybersecurity information remains valid, current, and allow sufficient time for recipient to take appropriate action against emerging cyberattacks. The parameter of trust represents the willingness of end users to depend on the information provider with a feeling of relative security. With respect to cost, each type of stakeholder bear different types of cost. The different cost types include the cost of cybersecurity solution and information usage for end users, the cost of service offering for cybersecurity solution and information provider (e.g., maintenance cost, cost of managing services, cost to supports end users, cost of improving QoS and QoI). All these seven value parameters can simultaneously impact the values of stakeholders, forming a complex interdependency in the value creation model among the stakeholders.

The value creation model reveals that the major value is generated by the number of end users (i.e. install base) in the cybersecurity information sharing ecosystem. More specifically, an increase in the number of end users triggers the increase in the value for the end users due to the availability of larger trusted communities and more potential connections to other end users. Further, it also increases the benefits for the cybersecurity solution providers and information providers due to income from service sales. The simulation results show that in the current value creation model, the value cyber security solution provider is higher than the information provider. The results of our simulation shows that in the saturated market scenario there is a risk of potential unsustainability of the value creation and distribution in the cybersecurity information sharing ecosystem. The risk is due to the high prices of the cybersecurity solutions and

information sources and it becomes more eminent with the market saturation. The end users can utilize the cybersecurity solution and information sources depending on their limited purchase power, and under the saturated market conditions the number of new end users joining the ecosystem decreases, which ultimately increases the potential risk of instability of the cybersecurity market. Thus, the demand is negatively affected, and the information providers specifically unable to recover their total costs ***(Figure 13***, ***Figure 14***, and ***Figure 15)***.

The findings of this study can have implications for the business manager to make policy decisions related to the business models and pricing schemes for the cybersecurity solution providers and information providers. The solution and information providers have to devise strategies that support the values of each other, in order to survive for a long time period and make the market stable. The strategies related to the bundling of cybersecurity solution and information sources in one package will be attractive strategy for suitability in the cybersecurity information sharing ecosystem. Further for bundling options, attractive revenue sharing schemes is vital for sustainability of value generation for all the stakeholders as well as for the growth of the cybersecurity information sharing ecosystem.

In future, our study will be extended by including more factors such as the detailed market structures, competitive environments, detailed pricing models, and the structure of trusted communities, to establish a fine-grained value creation model in cybersecurity information sharing ecosystems.

### 3.7.3 Limitation

The research method which we have used for this study inherits the limitations that exists in the simulation methodologies. In order to represent the interdependence among the stakeholders and to model the assumptions of the presented value creation model, we use the relative values for some variables but for the other variables we use the real values (such as $F_{i,a}(t)$ and $F_{s,j}(t)$). Therefore, this technique can only depict the inclinations of results and the nature of the impacts on the values (i.e. positive or negative impacts). There is a need to validate the interdependency through the real data from the cybersecurity information sharing ecosystem.

# Chapter 4: Investing in Cybersecurity Information Management and Sharing Systems

## 4.1 Summary

Enterprises are employing a portfolio of security strategies to enhance their level of information security. These security strategies include the cybersecurity information sharing, attack detection, prevention, vulnerability reduction, risk assessment, threat deterrence, education and training. Each of these security strategies have different payoffs, effectiveness and costs in the complex environment of information security. The enterprises have to deploy their resources on a set of security strategies for effective management of information security. Different security tools, controls and measures are being used to implement the security strategies.

In the enterprises, along with several tasks, the security managers are also responsible for security technology selection and establishing the appropriate justifications for investment in the selected security (Nazareth & Choi, 2015; Whitman & Mattord, 2011). These justifications of investment are then communicated to executive management for their approval and release of funds. The information security investments are difficult to justify because it is not always possible to proof returns on the security investments. The traditional approaches to calculate the return on information security investments (such as ROI, ROSI, ALE, NPV and ROA) are difficult to apply, because the security investments are not directly generating revenues or profits. Instead, the information security investments address the loss prevention and mitigation of

potential threats to the enterprise's assets (Robert Putrus & CFE, 2016). Further, the traditional methods of calculating return on information security investments are unable to quantify the intangible benefits such as organizational, strategic, operational, managerial and tactical benefits that it brings to enterprises.

Additionally, another major challenge that security managers have to face in enterprises, is the difference of the perceptions and views of non-IT management towards the information security. This phenomenon of difference in perceptions can be explained using the agency theory. Often, there is a lacking of quantifiable understanding of how information security technologies, applications, controls, measures and services may contribute to the enterprise's business objectives. Further, the security managers are also not realistic in linking the information security technologies to the interests of enterprises to increase the profits and revenue, expanded market share, enhance customer satisfaction and resource allocation. Due to these lacking, the executive management of enterprises consider the information security investments as merely a sunk cost. The existence of differences in perceptions, a communication gap emerged between the security managers and executive management that leads to under investments in the information security. The highly technical nature of information security makes it more difficult for the security managers, to justify the security project proposals as well as how these proposals might be beneficial to the enterprises. Because of these issues, it becomes more difficult for security managers to establish information security investment justifications in the enterprises (Robert Putrus & CFE, 2016).

The information security investments are totally different than the traditional business investments because security investments deal with the attack prevention, detection, trouble shooting, risk mitigation and risk management. Even after considerable information security investments, there is no technical guarantee of the complete immunization of enterprises assets from the cyberattacks. All these scenarios contribute in increasing the complexity of the issue and making it more difficult for security managers to establish the justification for information security investments. Furthermore, it is difficult for enterprises to implement the standardized information security investment decision making processes due to complex nature of the area of information security (Weishäupl et al., 2018). Therefore, for the availability of sufficient funds for information security, enterprises must have to decide at strategic level that how much resources should be invested in this area to minimize the losses due to cyber-attacks and maximize the cumulative benefits (Oosthuizen, Molekoa, & Mouton, 2018).

The security managers need appropriate tools and methodology to fill these types of the gaps. In this research work, we will propose a system dynamics based model which can be utilized by the security managers to quantify the benefits that cybersecurity information management systems bring to enterprises and help them to communicate with the executive management. Specifically, in this paper, we are trying to answer the research question: (1) how investment in cybersecurity information management systems impact the security level of enterprise? (2) How these systems enhance network security

and mitigate the risk of advanced cyber threats? and (3) how these systems are contributing to cumulative benefits to the enterprises?

To answer this question, we first did the literature survey to analyze the use cases of the cybersecurity information management systems. After that, based on the existing literature, we proposed a framework to analyze the benefits that these systems bring to the enterprise. The framework is majorly consisting of five main categories of benefits: organizational, strategic, operational, managerial and tactical benefits. Subsequently, we developed a system dynamics based model incorporating the use cases of the cybersecurity information management systems and the cumulative benefits that they bring to the enterprise. Based on the utility maximization theory, the results of our model suggest that the cybersecurity information management systems bring threefold benefits to enterprises: (1) increasing the level of information security, (2) reduction in operating cost of enterprise, and (3) significantly increase the cumulative benefits. Convincingly, this model can be used to establish the foundation of business justification for investment in the cybersecurity information management systems and other security tools.

The remainder of the chapter is organized as follows; ***Section 4.2*** gives the review of the different streams of information security literature as well as provides a brief discussion about the security investment justification problem which is modeled in the later sections. A theoretical framework is given in the ***Section 4.3***, that establishes the foundation for building the model. A system dynamics based model is presented in ***Section 4.4,*** that accumulates the major user cases of cybersecurity information management systems along with the

enterprise wide benefits of these systems. It describes the level of investments in security tools in terms of detection ability, prevented attacks, successful attacks and cumulative benefits of enterprise. The description about the simulation settings and different scenarios are presented in ***Section 4.5***. The next ***Section*** discusses about the implications of this research work. Finally, the paper is concluded with discussion about limitations and future extensions.

## 4.2 Literature Survey and Gap Analysis

### 4.2.1 Literature Survey

Enterprises are greatly relying on the Information Technology (IT) for their day to day activities and business operations; and failure of these IT systems could even lead to bankruptcy (Kearns & Lederer, 2004). To protect the IT infrastructure, enterprises are implementing a portfolio of information security strategies including vulnerability reduction, deterrence, detection, education & training to counter vast variety of security threats (Nazareth & Choi, 2015). Each of these strategies needs investment and each of them have different costs, and effectiveness which are difficult to quantify. The potential benefits that are being derived from investments in information security are undeniable but realistically difficult to quantify and estimate. There are several factors which are difficult to quantify including numerous types of threat manifestation, the ability to recover from successful attacks, the extent of damage incurred, damage of reputation, and effects of the successful attacks on the enterprises (Nazareth & Choi, 2015). The successful attacks have the potential to burden enterprises with corporate liability, monetary damage and undermine credibility (Cavusoglu, 2002; Cavusoglu, Mishra, & Raghunathan, 2004a). The evolving threats and complexity of countermeasures generates confusion in the strategies of information security investments and several enterprises have to adjust their security investment strategy to alleviate fear, uncertainty and doubt (FUD). In order to deal with FUD, the implementation of security measures costs less than the costs of recovering from security attacks. But this strategy provides a very high level indictions and offers no insight on the investments

in security measures to ehnacement of security capabilities (Warnecke, 2013). The enterprises are of different nature e.g. organizations in defense and entertainment industry may be facing different types of cyber threats. Therefore the strategy of investments in information security for each type of organizations should be customized considering the specific requirements, rather than availability of funds (Warnecke, 2013).

The multidimensional nature of issue of information security investments in enterprises can be summarized into three main streams: 1) optimal amount of investments in security; 2) which are the appropriate security technologies, measures or tools worth investment; 3) how to make security investments effective (Huang et al., 2014).

Several studies were conducted to address these issues independently.

#### 4.2.1.1 Optimal Level of Information Security Investments

The optimum level of investments in security is usually addressed using the decision analysis and comparing it with the risk and return of investments. Contrary to return of IT investments, the return of security investment (ROSI) does not derive from increased revenues or decreased costs like IT investments do. Instead, it comes from reducing and managing the security risk that an enterprise is facing (Alter & Sherer, 2004; Yue, Çakanyıldırım, Ryu, & Liu, 2007). Among the existing strategies, the risk management is the most progressive strategy to justify the information security investments. It depends on determining the likelihood of occurring a specific security incident and the associated costs with this specific incident. The profiling of potential risks that an enterprise can be exposed to, offer an understanding of needed security

capabilities. It is useful in determining the optimal investment in security controls considering the potential losses that can be associated with a security breach (Cavusoglu, 2002; Cavusoglu et al., 2004a; Warnecke, 2013). But have inherent limitations due to the estimation of the cost and likelihood of occurring security incidents (Warnecke, 2013).

Information security Investments is an important aspect to help mitigate the security challenges in the enterprises. In a study conducted by (Böhme & Moore, 2016), they derived and compared optimal investments in security over multiple time periods. Further, they explore the delicate balance between reactive and proactive security investments.

The issue of underinvestment in information security has been extensively discussed in the literature and pointed out that it is hardly ever reach to its optimum level. The consequences of cybersecurity underinvestment include the increased cyber risks, economic costs due to incidents, social welfare losses, reduced level of individual and national security (Campbell et al., 2003; Gordon et al., 2015c, 2015a). Several frameworks and economic models are proposed in the literature related to decision-making of information security investments. Gordon et al. (Gordon & Loeb, 2002b) developed an economic model considering the investment decisions for security of information systems and evaluates the cost of cybersecurity against the expected loss from cyber-attacks. In a subsequent work, (Gordon & Loeb, 2006) explained empirically that this type of economic analysis is broadly used in practical scenarios for security investment decisions. In another work, Gordon et al. presented an economics-based analytical framework for evaluating the effect of regulations and

incentives designed by the government to improve the situation of cybersecurity investments by the private sector firms (Gordon et al., 2015b).

It was explained that the cybersecurity investments at private firms depend on the utilization of optimal mix of cybersecurity strategies and willingness to increase their investments in cybersecurity activities. In another work, (Garvey et al., 2013) argued that the economic decision making plays an important role in securing globally distributed information repositories within the organizations or outside the organizations. Thus, to measure economic-benefits and returns on security investments a macro-level analytic method was presented called "Table Top Approach" which allows and explains the selection of competing choices that offer the maximum cost-benefit gains in cyber defense (Garvey et al., 2013).

#### 4.2.1.2 Selection of Appropriate Information Security Technology

The second stream of information security investments is connected to the selection of appropriate controls, security technologies, measures or tools worth investment. It has been observed, that the selection of security investments is supported by traditional management tools such as return on investment (ROI), return on security investment (ROSI), net present value (NPV), analytic hierarchical process (AHP) and others. In the enterprises, the decision makers are interested to know that the investments in any product or service is justified or not. The financial justification in case of cybersecurity investments is difficult because information security delivers non-financial benefits, rather than direct increase in revenue or a reduction in costs. For instance, the value

of firewall can be evaluated by the damages related with a security breach, which was mitigated due to the availability of firewall. However, it is difficult to differentiate a mitigated attack from an attack that never occurred. Therefore, the value resulting from an attack that never experienced is inherently ambiguous (Warnecke, 2013). Similarly, (Warnecke, 2013) in his work argued that, we can say that "no one buys a SIEM or TIP systems to generate revenue".

Several metrics have been presented in the literature related to information security investments to quantify the return on security investments (ROSI), e.g., (Gordon & Loeb, 2002a) and (Anderson et al., 2008); cybersecurity decision making e.g., (Dor & Elovici, 2016; Fielder et al., 2016; Huang & Behara, 2013; Mayadunne & Park, 2016); net present value (NPV), e.g., (Eisenga et al., 2012; Sheen, 2010); the Internal Rate of Return (IRR), e.g., (Buck et al., 2008; Wawrzyniak, 2006); Annual Loss Expectancy (ALE), e.g., (Tanaka et al., 2005), (Cremonini & Martini, 2005). (Herath & Herath, 2008) developed the integrated real options analysis (ROA) model using Bayesian statistics that incorporates learning and post-auditing analysis technique for assessing the value of information security assets for optimal level of investments in cybersecurity.

(Viduto, Maple, Huang, & LóPez-PeréZ, 2012) uses the optimization and allocation of limited security investment for selecting and prioritizing security technologies. They proposed an optimization and risk assessment model to minimize the risk and costs of selecting the security countermeasures.

(Huang & Behara, 2013) in his work proposed an analytical model for allocation of security investments by considering attacks that are occuring

simultaneously from various threat agents having distinct characteristics. They concluded that if the security budget is small than it is better for an organization to allocate almost all of the investments to preventing one type of attacks. Also, in the existence of highly connected information systems the organizations have to focus on the technologies against some specific types of attacks.

(Sawik, 2013) uses the bi-objective trade-off model for the selection of security controls and measures. This model is based on the probabilities of occurring attacks, associated costs and effectiveness of security measures. He suggested that, selection of security measures portfolio depends heavily on confidence level, costs and acceptance of risk level by the decision makers.

(Weishäupl et al., 2018) conducted the theory based exploratory multiple case study to optimize the future IT security investments and selection of security measures based on the past decisions. (Panaousis et al., 2014) uses the non-cooperative control games to investigates the optimal investment in the cybersecurity controls in the organizations specifically the cases in which organizations faces the problems of underinvestment or inefficient spending on cybersecurity. (Cavusoglu et al., 2008) studied the mangers view of security investments, and argued that the traditional techniques of decision-theoretic risk management for determining the security investments are not appropriate. Because the strategic nature of hackers allow them to alter their hacking strategies by considering the security investments strategies of the organization. They proposed a game theoretic model to determine information security investment levels and compared it with decision theory approaches considering the factors of investment levels, vulnerability, and payoff from investments.

(Fielder et al., 2014) addressed the challenge of how do we make better security decisions, and proposed techniques and algorithms that optimally allocates cybersecurity resources according to different tasks to support well-founded human decision making using the game theory. (Fielder et al., 2016) suggested that effective decision-making strategies should be used by security managers when investing in cybersecurity resources. They considered the game theory, combinatorial optimization, and a hybrid of these two for making the cybersecurity decision making more effective.

#### 4.2.1.3 Making the Security Investments Effective

The third stream of security investments is related to the security performance. Enterprises are relying on security technologies (such as intrusion detection systems (IDSs), anti-malware and firewalls) to manage the information and network security risks. The value of IDs in the firm's IT security architecture of an enterprise has been assessed and studied by applying different IDS configurations (Cavusoglu et al., 2005). It was illustrated that, the IDS configuration, represented by detection (true positive) and false alarm (false positive) rates, determines whether an enterprise realizes a negative or positive value from the IDS.

The attackers are using different hacking strategies and altering their strategies in response of enterprise security investment strategies (Cavusoglu et al., 2008). Thus the enterprises have to take measures to make their security investment more effective. For effective security investment, an important issue is the ability to configures and adopt to the adversarial conditions that an enterprise

faces besides the several other technological, operational and procedural issues of security technology deployment (Huang et al., 2014).

The game theory has been extensively used in the literature to discuss the incentives which leads to more effective security investment decisions making as well as it is well suited to model the performance of a specific security technology (Huang et al., 2014). (Cavusoglu et al., 2008) studied the mangers view of security investment, and argued that traditional decision-theoretic risk management techniques to determine security investments are not appropriate. Because, the hackers alter their hacking strategies in response to the modification of enterprise's investment strategies. They proposed the game theoretic model to determine information security investment levels and compared it with approaches of decision theory by considering the factors of vulnerability, level of security investments, and security investments payoffs. (Cavusoglu et al., 2005) used the game theory to evaluate the performance of the intrusion detection systems (IDS). It was suggested that the enterprises could get the positive return on investments from these types of technologies, only when these technologies improves the detection capabilities. They further expanded the results by considering the other technologies related to information security and proposed a model based on the game tree approach for making strategic decision in information security (Cavusoglu et al., 2005). Security managers in any enterprise can use their methodology, with their own context specific parameters, to evaluate and examine the various types of their adopted security controls and measures (Huang et al., 2014).

### 4.2.2 Gap Analysis and Problem Description

In the enterprises, security managers have several responsibilities, but the most important tasks include the selection of security tools & technologies, risk management, threat assessment, information security policy and planning (Whitman & Mattord, 2011). The selection of information security tools and technologies is a difficult task because their costs are usually very high and enterprises are always facing with the budget constraints. In addition, several other factors also affect the selection of the information security tools and technologies such as prevailing vulnerabilities, the perceived attractiveness of targets (both at IT infrastructure and at applications level), the number of attackers, sophistication of attacks and the availability of attack tools (Nazareth & Choi, 2015).

In order to secure the IT infrastructures, a significant number of enterprises are already utilizing the cybersecurity information in their security procedures (D Shackleford, 2018). Similarly, some surveys also reveals that the use of cybersecurity information management tools have also been increased than the previous year's (Barahona, 2017; D Shackleford, 2018). Among different available cybersecurity information management tools, SIEM systems are mostly used tools and standalone TIPs are also gaining significant traction during the recent years (Barahona, 2017; D Shackleford, 2018). In order to implement the new security tools and technologies, the security managers have to convince the executive management for seeking the required investments for the information security i.e. for the procurement of selected security tools and technologies. The information security requires considerably significant investments, and the enterprises seek methodologies to determine whether the

investment is appropriate and justified (Robert Putrus & CFE, 2016). Some arguments proposed that information security should be considered at the same necessity level as any other required infrastructure i.e. as accounting, operations and IT functions to enable enterprises to do business because of the severity of impact of incidents of security breaches (Robert Putrus & CFE, 2016).

The information security investments are difficult to justify and it is not always possible to proof returns on the security investments. The traditional approaches to calculate the return on information security investments (such as ROI, ROSI, ALE, NPV and ROA) are difficult to apply in the information security area, because these investments are not directly generating revenues or profits. Instead, the information security investments address the loss prevention and mitigation of threats to the enterprise's assets (Robert Putrus & CFE, 2016). Further, the traditional methods of calculating return on information security investments are unable to quantify the intangible benefits such as organizational, strategic, operational, managerial and tactical benefits that it brings to enterprises.

In addition, one of the major challenges that security managers face in the enterprises is the difference of the perceptions and views of non-IT management towards the information security. Often, there is a lacking of quantifiable understanding of how IT applications, technologies and services may contribute to the enterprise's business objectives. Further, the security managers are also not realistic to links the information security and technology solutions to the interests of the enterprise to increase the profits and revenue, expansion in market share, enhance customer satisfaction and resource

allocation. Due to this lacking, the enterprises considers the investment in information security as merely a suck cost. Due to the differences in perceptions, a communication gap emerged between the security managers and executive management that leads to under investments in the information security. The highly technical nature of information security makes it difficult for security managers, to justify the security proposals and how they might be beneficial to the enterprises.

This communication gap makes it more difficult for security managers to establish the justifications of information security investments in the enterprises (Robert Putrus & CFE, 2016). Another challenge, information security is a risk mitigation, management and prevention investment which is totally different than the traditional business investment. Even after considerable investments in information security, there is no technical guarantee to immunize the enterprises from the cyberattacks. In these situations, it becomes much more difficult for security managers to establish the justification for the information security investments. Furthermore, it is difficult for enterprises to implement the standardized information security investment decision making processes due to complex nature of the area of information security (Weishäupl et al., 2018). Therefore, for the availability of sufficient investment for information security, enterprises must have to decide at strategic level that how much resources should be invested in this area to minimize the losses due to cyber-attacks and maximize the cumulative benefits (Oosthuizen et al., 2018).

In these situations, the security managers need appropriate tools and methodology to fill these types of the gaps. In this research work, we will

propose a system dynamics based model which can be utilized by the security managers to quantify the benefits that information security brings to enterprises and help them to communicate with the executive management. Furthermore, this model can be used to establish the foundation of business justification for investment in the information security tools and systems.

## 4.3 Theoretical Background

### 4.3.1 Agency Theory

Agency theoretic view is used to explain and resolve the issue among different cooperating stakeholders of an enterprise, who have conflicting goals (Eisenhardt, 1989; Hill & Jones, 1992; S. A. Ross, 1973).

The agency theory explains that the investors and managers have different preferences majorly due to varying goals and / or differences in risk aversion behaviors. For instance, executives of an enterprise decide to explore the new markets and expand the scope of their existing business. This decision can reduce the profitability of enterprise in short-term, but with the expectation of more profits in the long-term. However, this type of decision may have opposition from the shareholders because they may prioritize the capital growth in short-term. In the case of risk aversion, one example can be the approval of loans from bank on very low limits; the shareholders can oppose the decision of the bank in terms of taking high risks of defaults.

From the information security perspective, security managers and executive management have different preferences and priorities in terms of allocation of investments. They have to make investment allocation decesions between the reveneue generation, assets development or activities related to enhancing

information security (Srinidhi, Yan, & Tayi, 2015). Productive assets can improve cash flows and decrease the vulnerability of the enterprise from the financial distress which also reduces the security issues in the long-term. On the other side, investment in security activities and assets can reduce the security breaches in the short-term at the expense of cash flow over the long run (Srinidhi et al., 2015). The executive management have to select the mix of security and productive investments in the enterprises, making the decision subject to the agency problem (Hart, 1995). (Weill & Ross, 2004) also described the IT governance perspective using the agency theoretic view. IT governance specifies accountabilities and supports an enterprise to align its IT investments (e.g. security improvements) with the firm's strategic objectives. The agency theory can effectively support the IT governance decision making in terms of prioritization and investment (i.e. decisions about how much and where to invest in IT). Using the agency theory view of the enterprise, we identified and explained the misalignment of the perception of the security managers and the executive managers of the enterprise in terms of investments in information security. The security managers can establish the justification and can communicate to the executive management about the priority and importance of the information security investments.

### 4.3.2 Utility Theory

Utility theory is useful for explaining the behavior of the decision makers, who have to decide among the available services or goods to consume, and obtain the maximum possible level of overall utility considering the budget and cost of the goods or services. This theory provides the methodological framework

based on the utility maximization principle to evaluate the alternate choices made by the decision makers. Several researchers have used this theory to answer the question that; what is the optimal amount of investment for information security which have justified returns on investment (Gordon & Loeb, 2002b; Hoo, 2000)? (Huang, Hu, & Behara, 2008) used the expected utility theory to determine the optimal security investment level that maximizes the utility of the investment. Their results discuss the management of information security investment based on different system configurations and characteristics of threat environments. In another research, (Huang et al., 2014) presented a model for health care information exchanges based on the scale free network principles and applied the risk reduction and utility maximization to determine the optimal level of information security investments. In addition, they also consider the business benefits that security investments would bring to an enterprise and how they would affect the security investments decision. The results of this study shows that the security events in which potential loses reaches a critical value must be protected, and enterprises would spend only a fraction of essential security risks on security measures. (Huang, Hu, & Behara, 2006) adopted the expected utility theory and derive the optimal security investments by considering simultaneous attacks from various external agents having diverse characteristics. They showed how enterprises have to allocate the limited security budgets to protect themselves against distributed and targeted attacks simultaneously. They also discussed that it is better for enterprises which have small security budget to allocate most or all of the security investment to measures against one type of attack. Further, they discussed that enterprises have to allocate most of its security budgets for

defending the targeted attack which have large potential losses. (Huang et al., 2008) also used the expected utility theory to analyze the behavior of risk-averse decision makers. They discussed that for non-zero optimum security investment there exists a minimum potential loss and above it optimal investment increases with potential losses. Furthermore, they suggest that the risk-averse decision maker might continue to do security investment until the expenditures are near to the potential loses.

In a study, conducted by the (Mayadunne & Park, 2016) used the expected utility approach to analyze the decisions of information security investments of the risk taking small and medium enterprises (SMEs) and compared these decisions made by the risk neutral firms. They discussed that, risk takers SMEs are prioritizing the information set's vulnerability in making security investment decisions. They further showed that the risk taking SMEs make large investments in protecting information sets, with less effectiveness of the investment in lowering breach probability. Further, they compare the security investments decisions of risk neutral and risk taking SMEs and discuss about the diversification of investments considering the value of information sets and varying vulnerabilities.

### 4.3.3 System Dynamics

System dynamics methodology has been widely used by the research community to investigate different aspects of information security. The system dynamics methodology uses a combination of first-order differential equations to relate quantitative and qualitative factors within and across time periods (J D Sterman, 2000). Its basic principles were established by the Forrester to

investigate managerial and dynamic decisions using control principles (Forrester, 1961).

The information security management and security investments decision making is a complex area, which involve a range of quantitative and qualitative factors across time periods. Therefore, system dynamics is considered as an appropriate methodology for creating models and better understanding of information security management and decision making (Nazareth & Choi, 2015). System dynamics is currently being employed for information security management, security resources deployment, security investment decision making, security policy design and analysis.

The increasing information security breaches making it confusing for security managers in making best investment decisions to defend against cyberattacks. (Agular Rodriquez, 2017) in his research, employed system dynamics to understand the dynamic interaction between defenders and attackers for security investment decisions. He studied the dynamic interaction between a defender and attacker in two strategies of investment. The first is "wait and see" and other is the "weakest link strategy". He suggested that both of these strategies are not effective under uncertainty. He discussed that instead of coping with attacks, it is rational for defender in the presence of uncertainty to underinvest in information security. Further, he proposed two policy options to improve defenders' financial performance over time, 1) information sharing among defenders and 2) higher dismissal time of attacks. He observed that, combination of implementation of higher dismissal time and information

sharing depends on enterprise's size and the available budget to invest in information security (Agular Rodriquez, 2017).

(Nazareth & Choi, 2015) employed system dynamics to evaluate the alternate security management strategies based on the security investment and security costs. The results provide guidance to managers for security decision making, and suggests that investing in detection tools has a higher payoff than investing in deterrence strategy. In another study, (Behara, Huang, & Hu, 2007) presented an information security life cycle model to observe the effect of investments in multiple aspects of information systems security. There model analyzes the impact of investment in intrusion detection, HR policy, value reduction, deterrence and vulnerability reduction on the overall number of attacks faced. It was observed, that investments in all security areas are more effective as compared to traditional investment strategies, which focus only on high-profile areas. (Sarriegi et al., 2007) investigated the impact of investments in security controls implementation, and showed that different types of controls headed to variable levels of total security with technical security controls being the most effective.

In the area of information security management, another stream is the study of the impact of threats posed by the security attacks. (Melara, Sarriegui, Gonzalez, Sawicka, & Cooke, 2003) used the system dynamics to study the effect of insider threats and analyzed the impact of motivation, technical workplace discontent, security controls, and time-bomb attacks. They suggested the policies to minimize the risk of security failures or at least to reduce the extent of damages which can be potentially occur due to insider

attacks. (Yang & Wang, 2011) studied the insider threats utilizing system dynamics based on illegal insider corporate stock sale as a case study using achievement, disgruntlement, and unmet expectations to model illegal behavior. (Gonzalez & Sarriegui, 2004) performed modeling of outsider and insider threats based on the motivation for attacks, deterrence, trust and detection ability.

Another other stream is the risk based security analysis where system dynamics have been utilized extensively. A model was presented in (Trček, 2006) to study the risk management by analyzing the effect of security policy, threats and security intrusions detection. In another research, impacts of risk on security investments and asset vulnerabilities were studied. The results disclosed that vulnerabilities and security investments start to stabilize, after an initial period of oscillatory behavior of the risks (Trček, 2008). (A. C. Kim, Lee, & Lee, 2012) studied the financial impact of different information security risk strategies. They discussed that the strategies (such as risk acceptance and risk reduction) have different behavior when confronted with decreasing and increasing risks. The system dynamics has also been used in several other areas of information security such as vulnerability pricing on the black market (Radianti & Gonzalez, 2006), the effect of incident reporting and frequency over different circumstances (Olav Sveen, Sarriegi, Rich, & Gonzalez, 2007), and personnel forecasting for information security (Park, Lee, No Yoon, & Yeon, 2008).

## 4.4 Information Security Investment Model

The model proposed in this section, investigates the organizational benefits of adopting the cybersecurity information management systems as well as financial implications of security decisions on an enterprise's information asset base. The model integrates concepts from several facets of information security including organizational benefits, attacker's value, security investments, security decision making, deterrence, risk assessment, threat detection, attacks, attack motivation and target attractiveness. The proposed model intends to relate these concepts to the security costing and the overall sustained damage. Using this model, the managers are able to explore the organizational benefits and impact of security investments decisions into multiple security channels under a varying range of conditions. It is not possible to cover all the scenarios and security attacks in the proposed model, still it can provide managers with insights into relative risks and tradeoffs. The model is depicted in ***(Figure 27)***. The rest of this section provide the detailed description about the proposed model.

The notations used to explain the model include the rectangles, double arrow, valve symbols, clouds and connectors. The rectangles are used for stock items that can deplete or accumulate over time. The double arrows and valve symbols represent the flows, which effect the stocks. These flows come from or empty into the reservoirs which are shown by the cloud symbols in the proposed model. The simple arrows or connectors represent the effect of one item on another item. The arrows are marked with the "+" or "-" signs which shows that it has positive and negative effect i.e. whether an increase in one will lead to an

increase in another. The other items or variables are represented by the converters in the proposed model. The values of converters are specified for a given time period and are determined by other converters through connectors. The signs on connectors also help in characterizing the loops in the model. Two types of loops can exist in the model; reinforcing loops (all positive signs) and balancing loops (at least one negative sign). The unchecked reinforcing loops can eventually lead to zero or infinite values of involved converters. While the balancing loops will possibly lead to equilibrium and will show the oscillatory behavior.

The proposed model is comprised of several segments addressing organizational benefits, capabilities of cybersecurity information management systems, attacks, attackers value, risk assessment, vulnerability, recovery, and economic considerations. The model is slanted at the enterprise level instead of individual and perceptual levels. During accumulation of the model it was specifically emphasized to make it quantifiable and easy to verify. However, for some constructs quantification of values proves a challenging task. The values of the organizational benefits are considered at the enterprise level. The motivations of the attacks are assessed at the individual level instead of considering groups of the attackers (Gonzalez & Sarriegui, 2004; Melara et al., 2003; Nazareth & Choi, 2015). The proposed model is inclined toward understanding the economics perspectives, security investment decision and obtained organizational benefits form security tools altogether in a single model which is very useful for security managers to establish negotiable justification related to security investments for the executive management.

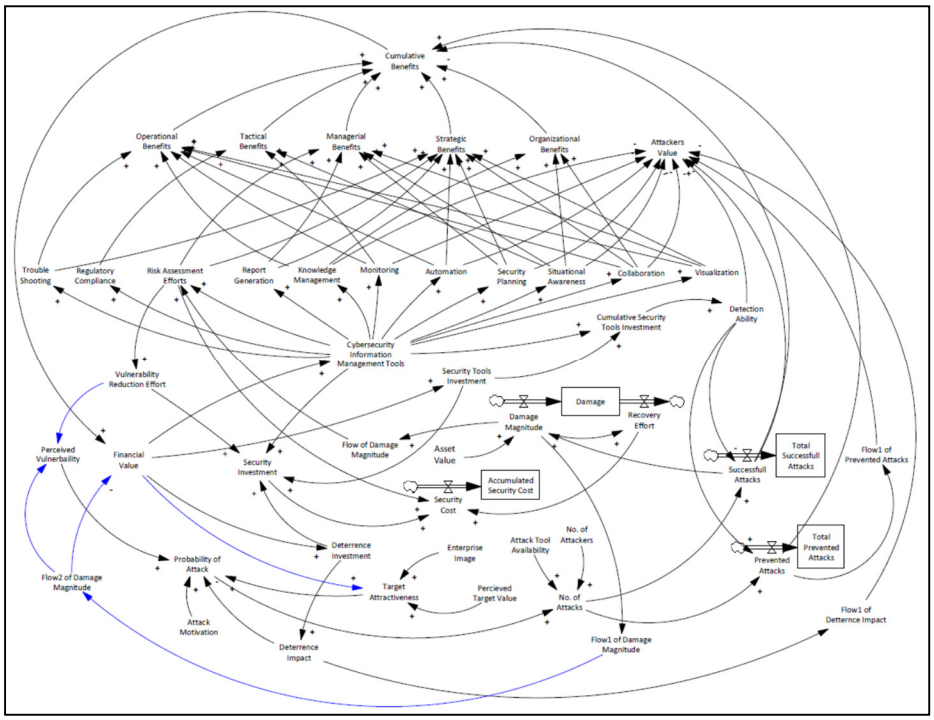



**Figure 27. Information Security Investment Decision Making Model**

We have selected the organizational benefits offered by the cybersecurity information management systems. The motivation of selecting these type of the systems for this study is that apparently they provides absolutely no additional security (Dorigo, 2012; Warnecke, 2013). But the stimulus of implementing these systems comes from the added knowledge about the networks as well as, devices, and applications connected to it. In this situation, it is challenging for security managers to establish justification of investment in cybersecurity information management systems based on indirect and intangible benefits. The proposed model can be used to cover this gap.

The model proposed in (Nazareth & Choi, 2015) is discussing the information security management based on the security investments. For the literature support to our model we have adopted some of the parts of their model with

some modifications and including some additional constructs wherever required. The protection of assets in enterprises from the threats and attacks are the main reasons for information security investments. We considered that enterprises are investing in vulnerability reduction efforts, security tools and deterrence. Previous studies mentioned that investment in security tools have higher pay off than investing in other security areas (Nazareth & Choi, 2015). In our study, we categorize the security tools into two groups i.e. cybersecurity information management tools and security tools. The detailed discussion on the former systems are available in ***Section 2.2***.

It is common practice that enterprises are implementing some type of security tools (e.g., malware detection programs, anti-virus programs, intrusion detection systems and firewalls). These security tools are useful in preventing different types of the attacks. But the evolving complexity and new emerging types of the attacks makes the situation worse because even in the presence of the implemented security tools a lot of attacks are gone undetected and when detected they have already done the damage. Also these security tools are working in silos and are not capable of providing the overall security picture of the enterprise. In order to provide the integrated view, another type of security tools called the cybersecurity information management tools are used for improving the security posture of the enterprise. These tools integrate all the existing device of an enterprise in a centralized system and also collect security information from external and internal sources, which is then used for improving the security level.

As discussed in ***Section 2.2*** and (Nazareth & Choi, 2015), the investments in security tools and cybersecurity information management systems enhances the attack detection abilities of enterprises. The attackers value is inversely related to the detection ability of the enterprise. With the increased detection abilities, the enterprise can prevent more attacks, with the reality that it is not possible to prevent all the incoming attacks. Therefore, some attacks become successful, that can appear in several capacities and have considerably different effects.

It has been observed from the security practices that investments in security tools is a gradual and step wise procedure. It does not need to be continuous because of an existing investment in security tools will allow the enterprise to detect some of incoming attacks. Therefore, our model uses the cumulative security tools investments to assess the detection ability of an enterprise. As discussed in (Nazareth & Choi, 2015), this behavior was modeled as negative exponential function. The increase in the security tools investment increases the detection ability, but eventually, at a diminishing rate. The successful attacks will cause varying damage; some has small while the others may have prominent impact. The damage magnitude construct is used in the model to capture the impact of damage caused by the successful attacks.

As discussed in (Nazareth & Choi, 2015), investments in the security tools is likely to have a more prominent effect on the overall security posture of the enterprise. We categorize the security tools into two types i.e. cybersecurity information management systems (e.g. SIEM and TIP) and traditional security tools (e.g., firewalls, anti-virus software, malware detection systems and intrusion detection systems). The later types of tools are directly involved in the

adding the value of the security i.e. attack detection and prevention while the former are more related to cybersecurity knowledge management and sharing as discussed in ***Section 2.2***. The investments in security tools improves the detection ability of the enterprise. Increased detection ability reduces the attacker's value and have positive impact on the cumulative benefits of the enterprise. Attackers also have to invest for buying attack tools and putting efforts for launching the attacks. The successful attacks increase their value while the prevented attacks reduce their value.

The cybersecurity information management systems are considered separately because of their specially offer capabilities. We have considered only the major capabilities such as trouble shooting, regulatory compliance, risk assessment efforts, report generation, knowledge management, monitoring, automation, security planning, situational awareness, collaboration and visualization. These capabilities offer several benefits, which are grouped into five major types of benefits that an enterprise can perceive i.e. operational, tactical, managerial, strategic and organizational benefits (discussed in detail in ***Section 2.2.3***). The relationship between the capabilities of the cybersecurity information management systems and the organizational benefits are drawn in the model based on the discussion of ***Section 2.2.3***. All these five types of the benefits become the input to calculate the cumulative benefits of the enterprise due to the all types of the security investments. In addition, the successful attacks on an enterprise have negative impact while the prevented attacks pose positive impact on the cumulative benefits (Oosthuizen et al., 2018).

The value of attackers are effects by the collaboration, knowledge management, monitoring, automation, security planning and situational awareness. These variables represent the major functionalities of the cybersecurity information management systems. The functionalities are negatively effecting the value of the attackers. Similarly, the investment in the security tools enhances the attack detection abilities, which ultimately decreases the value of attackers. The improved detection abilities result in reduction in the successful attacks and increases the rate the of prevented attacks. The successful attacks variable is the only one which increases the value of attackers. In addition, the investments in the deterrence increases the impact of deterrence which ultimately decreases the value of attackers.

Now we describe the segment of financial value of an enterprise. The increased benefits will ultimately have positive impact on the overall financial value of the enterprise. With more financial value, the enterprise will be able to invest more in the vulnerability reduction efforts, deterrence, and security tools and hence the security level can be increased. In addition, the financial value is input into the target attractiveness and with increased financial value of an enterprise will also have positive impact on the increasing the target attractiveness (Oosthuizen et al., 2018). The target attractiveness is calculated by the combination of the perceived target value, enterprise's image and the financial value of enterprise.

The motivation of the attack on an enterprise depends on the financial consideration, monitory gain or the perceived notoriety of a successful attack. The attack probability is formulated by the attack motivation, perceived

vulnerability of enterprise's information assets and target attractiveness in conjunction with the impact of deterrence. All factors positively impact the attack probability except the deterrence impact which has a negative influence. The target attractiveness and attack motivation is modeled using a negative exponential approximation function, although the impact of former is pronounced. Conversely, the impact of deterrence on attack probability can be modeled as a simple decreasing convex function because the two constructs have an inverse characteristic relation (Nazareth & Choi, 2015). The actions related to deterrence results in a variety sanctions and most of time these sanctions are targeted to internal attackers. It has been observed that, deterrence has very less impact for external attackers (Nazareth & Choi, 2015).

The perceived vulnerability is having the same concave relation and is modeled using the negative exponential approximation function, because it has a steadily increasing effect at a diminishing rate on the probability of attack. The probability of attack is modeled by considering the fact that the cumulative effect of all the constructs on it will remain in the 0-1 range. In order to have the values of attack probabilities in the expected range, extensive testing of the function was done to avoid unexpected results.

Now we discuss the segment consisting of number of attacks that can be originated from inside or outside of the enterprise. But in our model we are not differentiating between the external or internal attacks and attackers. In reality the attacks can be described into several types such as hacking, denial of service (DOS), malware attacks, phishing and social attacks. Also, the model does not differentiate the impact of attacks on different types of information assets of the

enterprises. Similarly, we are also not considering the individual success rate of internal and external attackers. In real situations, their impact on different assets vary depending upon different scenarios and the level of security in the enterprises. These assumptions are considered to provide the aggregate picture by encapsulating the low level details; also keeping the model understandable and useable for the managers. The two main factors i.e. availability of attack tools and number of attackers are used to determine the number of attacks on an enterprise (Nazareth & Choi, 2015).

In our model, the attacks which are detected and prevented are called the "prevented attacks" and the rest will be called "successful attacks". The stocks of total prevented attacks, total successful attacks and accumulated security costs accumulating the respective values but are not determinant of other variables in the model.

The damage magnitude shapes the perceived vulnerability and with the increased vulnerability reduction efforts will lessen the perceived vulnerability. The recovery efforts will be initiated after damage is sustained due to successful attack. Based on the extent of the damage, the recovery efforts may be involving complex or trivial activities and needs a substantial amount of time. The recovery efforts may include the re-installation of servers or restoring the data from backups. After some damage occurred, based on the damage magnitude the enterprise triggers the incremental risk assessment efforts. In this incremental risk assessment process, focus is on the unaddressed vulnerabilities and also it activates the vulnerability reduction efforts. The higher vulnerability

reduction efforts have negative impact and it can lessen the value of perceived vulnerability.

In order to improve the level of security, enterprises are investing in the security related activities such as security tools and deterrence actions which results in increase in the security costs. The investments in the security tools are already discussed above. Further, the model uses the security investments, recovery efforts and risk assessment efforts as input for calculating the total cost incurred for the security activities in an enterprise. Investing continuously in these areas usually have a cumulative effect (Nazareth & Choi, 2015). During the simulations, the cumulated security cost is calculated using the stock only for convenience purposes. The security investments and cost are directly related to each other. The security controls and software i.e. security tools require significant investments because of the higher market price, and therefore have a pronounced impact on the total security cost. The deterrence actions are normally focusing the internal attackers that are implemented using permissions and sanctions. As shown in the model the deterrence impact is inversely related to the attacker's value. As we already mentioned that, our model does not differentiate among different types of attackers.

## 4.5 Simulation Model Description

In this research work, system dynamics has been used as a simulation methodology having capabilities to correlate several constructs of the comprehensive model to track the progression across time periods. The simulation of the model is implemented using the Vensim® PLE of Ventana Systems, Inc. (Harvard, MA, USA), and provides functionalities to implement the system dynamics based simulations.

### 4.5.1 Simulation Setting

For simulation iterations, the selected unit of time is month and it runs for 36 months which represents a short to medium term security planning horizon.

As per definition of stocks in system dynamics, it is the accumulation of the values starting from the zero. But in the scenario of security tools investment and deterrence investments the initial values are not starting from zero because it is assumed that enterprises has already did some investments in these areas which is in accordance to the values used in (Nazareth & Choi, 2015). Almost all the values in the simulation are normalized on a 0-1 scale, with middle values chosen to represent the balanced scenario. It allows further exploration of conditions including reduced or greater security threats. The value of asset base is set to USD 5 million and number of attackers are set to 100 for initiating the simulation. From the market survey, it has been observed that cybersecurity information management tools require to have annual license renewal, therefore we set our simulation to incorporate this scenario. While the investment on deterrence is based on every six months (Nazareth & Choi, 2015). The

simulation was run under different scenarios, to investigate the cumulative benefits, value of attackers, security investments, security costs and damages.

Two approaches are used for the validation of system dynamics models, structural validation and behavioral assessment (Barlas, 1989, 1996; Senge & Forrester, 1980; John D Sterman, 2000). The congruence of system dynamics model with the real world scenarios is confirmed through the structural validation. The behavior assessment is performed during the executions, assesses the degree of confidence that can be placed in the results. The model was analyzed by applying extreme conditions for its behavior validation. Similarly, the congruous behavior of the model was also assessed under extreme conditions via examining the results. All the constructs utilized in the model are drawn from the existing literature in the areas of information security and organizational benefits realization. The same procudre has been utilized for model validation as discussed in (***Section 3.5.3***).

### 4.5.2 Settings of Variables

The section describes the equations and utility funtions of all the constructs, used to implement the simulation of the model are presented in ***(Table 4)***.

**Table 4 - Settings of Variables for Information Security Investments Simulation Model**

| Variables | Initial / Base Value | Utility Function | Reference |
|---|---|---|---|
| **Financial Value** | 0.5 Million (USD) | - | Assumption |
| **Asset Base** | 5 Million (USD) | - | Assumption |
| **Population of Attackers** | 10 | - | (Nazareth & Choi, 2015) |
| **Attack Tool Availability** | 0.5 (0-1value range) | - | (Nazareth & Choi, 2015) |
| **Deterrence Expenses** (every six months) | 2,000 USD | - | Assumption |

| | | | |
|---|---|---|---|
| **Deterrence Impact** | Negative Exponential Function | *1 - EXP( -1 * 0.125 * Deterrence Investment / 100 )* | - |
| **Investments in security tools** (every year) | 5,000 USD | - | (Nazareth & Choi, 2015; Robb, 2007) |
| **Investments in cybersecurity information management tools** (every year) | 10,000 USD | - | (Robb, 2007) |
| **Existing Investment in Security Tools** (It is assumed, that the enterprise already has done some initial investment in security tools) | 5,000 (USD) | - | Assumption based on (Nazareth & Choi, 2015) |
| **Existing Investment in Security Information Management Systems** (It is assumed, that the enterprise already has done some initial investment in cybersecurity information management tools) | 2,000 (USD) | - | Assumption based on (Nazareth & Choi, 2015) |
| **Attack Tool Availability** | 0.5 | - | (Nazareth & Choi, 2015) |
| **No. of Attackers** | 100 | - | (Nazareth & Choi, 2015) |
| **Enterprise Image** | 0.5 | - | (Nazareth & Choi, 2015) |
| **Percieved Target Value** | 0.5 | - | (Nazareth & Choi, 2015) |
| **Target Attractiveness** | - | *2.5 * ((Enterprise Image) / (Enterprise Image + 1)) * ((Perceived Target Value + 0.2)/(Perceived Target Value + 0.5)) * (( 1 - 1 / Financial Value))* | - |
| **No. of Attacks** | - | *SMOOTHI( RANDOM UNIFORM(2.5 * (Probability of Attack * "No. of Attackers") * (Attack Tool Availability^1.1), 7.5 * (Probability of Attack * "No. of Attackers") * (Attack Tool Availability^1.1) , 0 ) , 1 , 10 )* | - |
| **Risk Assessment Efforts** | Negative Exponential Function | *(1 - EXP( - 0.001 * (Cybersecurity Information Management Tools/20)) ) + (1 - EXP( - 0.001 * (Flow of Damage Magnitude/20)))* | - |
| **Detection Ability** | Negative Exponential Function | *1 - EXP( - 0.001 * (Cumulative Security Tools Investment/20))* | - |
| **[Regulatory Compliance], [Report Generation], [Trouble Shooting], [Knowledge Management], [Monitoring,** | Negative Exponential Function | *1 - EXP( - 0.001 * (Cybersecurity Information Management Tools/20))* | - |

| | | | |
|---|---|---|---|
| **Automation], [Security Planning], [Situational Awareness], [Collaboration], [Visualization]** | | | |
| **Damage Magnitude** | 1 | *IF THEN ELSE( RANDOM UNIFORM ( 0 , 1 , 0 ) > 0.5, 0.0002 * Asset Value * Successfull Attacks * RANDOM EXPONENTIAL( 0 , 1 , 0 , 1 , 0 ) , 0 )* | - |
| **Damage Magnitude** | - | *RANDOM UNIFORM( Damage Magnitude * 0.5 , Damage Magnitude * 1.5 , 0 )* | - |
| **Cumulative Security Tool Investment** | | *Cybersecurity Information Management Tools + Security Tools Investment* | - |
| **Successfull Attacks** | 10 | *(1 - Detection Ability) * "No. of Attacks"* | - |
| **Prevented Attacks** | - | *Detection Ability * "No. of Attacks"* | - |
| **Vulnerability Reduction Efforts** | - | *RANDOM UNIFORM ( Risk Assessment Efforts * 0.5 , Risk Assessment Efforts * 1.5 , 0 )* | - |
| **Security Cost** | - | *Security Investment + Recovery Effort + Risk Assessment Efforts* | - |
| **Overall Security Investments** | - | *Vulnerability Reduction Effort + Deterrence Investment + Security Tools Investment + Cybersecurity Information Management Tools* | - |
| **Operational Benefits** | - | *(Automation + Collaboration + Knowledge Management + Monitoring + Trouble Shooting + Visualization) / 6* | - |
| **Tactical Benefits** | - | *( Monitoring + Regulatory Compliance + Situational Awareness) / 3* | - |
| **Managerial Benefits** | - | *( Report Generation + Risk Assessment Efforts + Security Planning + Situational Awareness + Visualization ) / 5* | - |
| **Strategic Benefits** | - | *( Automation + Collaboration + Report Generation + Risk Assessment Efforts + Security Planning + Trouble Shooting + Visualization ) / 7* | - |
| **Organizational Benefits** | - | *(Collaboration + Knowledge Management + Situational Awareness) / 3* | - |
| **Cumulative Benefits** | - | *( Managerial Benefits + Operational Benefits + Organizational Benefits + Strategic Benefits + Tactical Benefits + (1 - 1 / Prevented Attacks) - (1 - 1 / Successfull Attacks) ) / 7* | - |

| | | | |
|---|---|---|---|
| **Attackers Value** | 1 | *( ( (1 - 1 / Successfull Attacks) - (1 - 1 / Automation) - (1 - 1 / Collaboration) - (1 - 1 / Detection Ability) - (1 - 1 / Flow1 of Detternce Impact) - (1 - 1 / Flow1 of Prevented Attacks) - (1 - 1 / Knowledge Management) - (1 - 1 / Monitoring) - (1 - 1 / Security Planning) - (1 - 1 / Situational Awareness)) / 10 )* | - |

### 4.5.3 Simulation Scenarios Description

#### 4.5.3.1 Base Scenario

The base scenario is established using values for dimensionless and other constructs to depict the case of small and medium scale enterprises. The value of financial value and the assets base is set to USD 5 million to initialize the simulation. The population of the attackers is set to 10 along with the attack tools availability is set to 0.5 on a 0-1 value range (Nazareth & Choi, 2015). The variables including the attack motivation, enterprise image and perceived target value are also set at 0.5 on a 0-1 value range. The investments in security tools and cybersecurity information management tools are set to 5,000 USD and 10,000 USD respectively at the start of every year. As it is assumed that the enterprise has already done some investment in security tools and cybersecurity information management tools. Keeping in this view, we initialize the security tools and cybersecurity information management tools as USD 2,000 and 5,000 USD respectively. In addition, the deterrence expenses of $2,000 are considered for every six months. The details of the variables initialization and base values along with utility functions are mentioned in ***(Table 4)***.

#### 4.5.3.2 Alternate Scenarios

The simulation is executed for varying investment decisions to track the behavior of different constructs of the model. Several cybersecurity information security management systems are available in the market with varying functionalities and features. Based on the offered functionalities their prices are also different. The enterprises choose the cybersecurity information management system considering their security budgets. Therefore, to incorporate the different scenarios we are considering the cost of cybersecurity information management systems in the range from 3000 USD to 7000 USD per month. These scenarios are categorized as very low, low, base scenario, high and very high. Starting from 3000 USD and with the increment of 1000 USD we established five scenarios for executing our simulation model as shown in ***(Table 5)***.

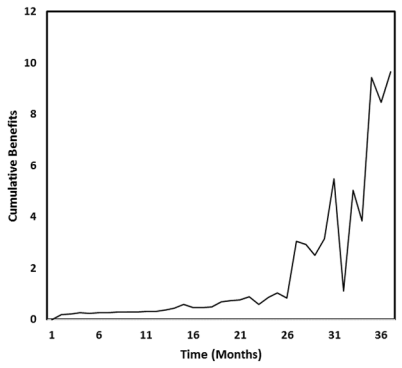
**Table 5. Simulation Settings of Alternate Scenarios for Cybersecurity Information Management System**

| | **Cybersecurity Information Management Systems (USD) - Varying** | **Security Tools (USD) - Fixed** |
|---|---|---|
| **Very low** | 3,000 | 5,000 |
| **Low** | 4,000 | 5,000 |
| **Base Scenario** | 5,000 | 5,000 |
| **High** | 6,000 | 5,000 |
| **Very High** | 7,000 | 5,000 |

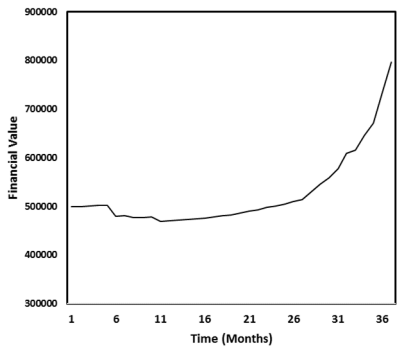
## 4.6 Simulation Analysis

### 4.6.1 Base Scenario

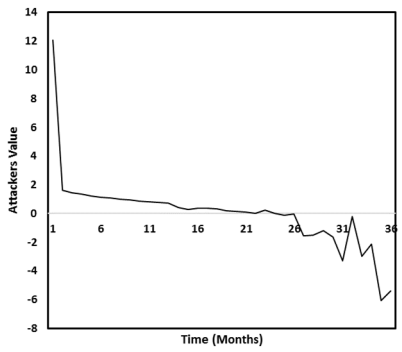
After establishing the base case, the model is executed to track the values of the cumulative benefits, financial value, detection ability, attackers value, security costs and damage magnitude. The results for the base scenario is shown in ***Figure 28***. The cumulative benefits include the detection ability, organizational benefits, tactical benefits, managerial benefits, strategic benefits and organizational benefits.



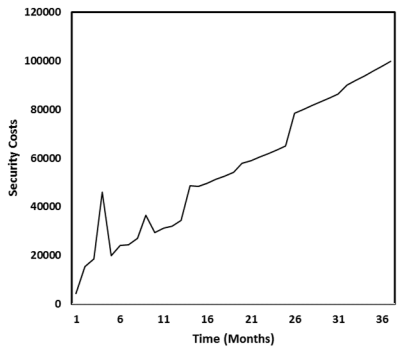

**(a) - Cumulative Benefits**



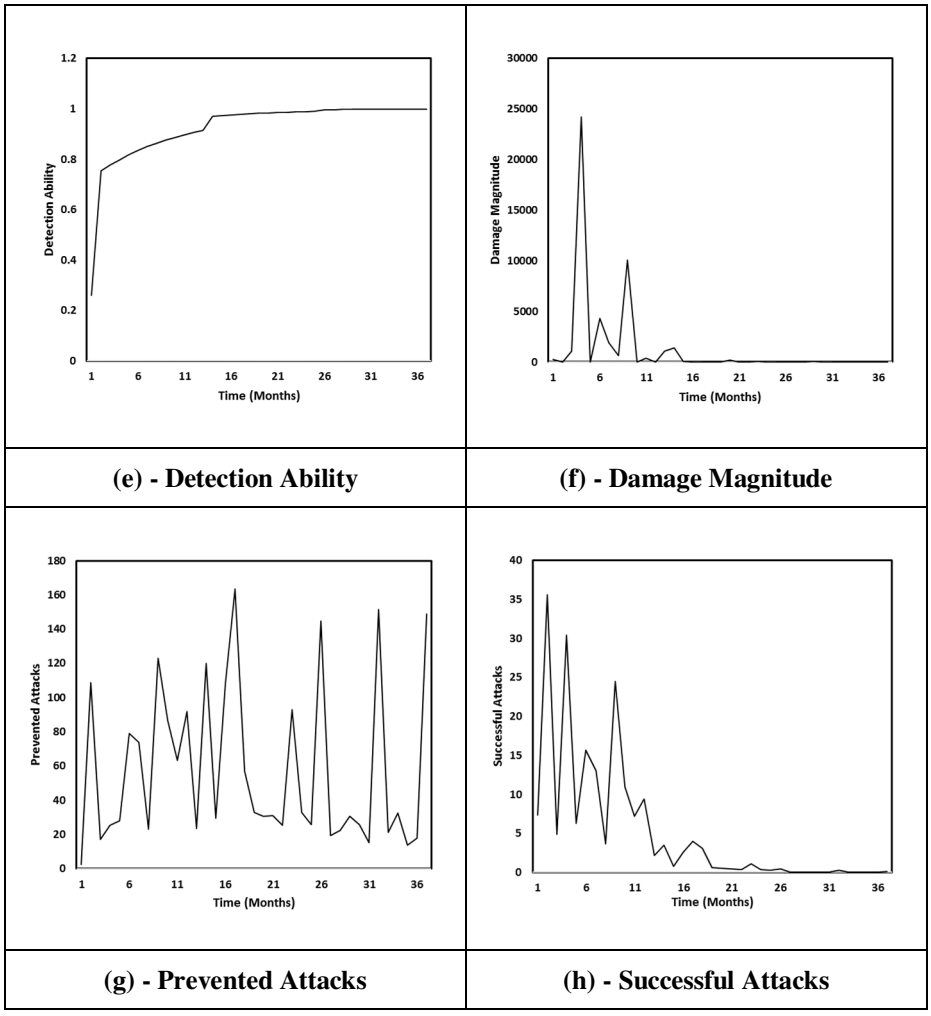

**(b) - Financial Value**




**(c) - Attackers Value**




**(d) - Security Costs**




**(e) - Detection Ability** | **(f) - Damage Magnitude**

**(g) - Prevented Attacks** | **(h) - Successful Attacks**

**Figure 28. Base Scenario**

The ***Figure 28(a)*** depicts the cumulative benefits of the enterprise. It can be observed that until 18th iterations, the cumulative benefits are slightly higher than 0. As mentioned in the simulation settings that the initial investment on the security tools is at the start of every year. It has been observed, that the first investment into the security tools (i.e. cybersecurity information management tools and security tools) there is no significant increase in the cumulative benefits. But after 18th iteration, the benefits starting to increase and represents

a significant increase in the later iterations of the simulation. This behavior can be explained by that fact that with the passage of the time the enterprise got experience and develop expertise on the security tools. The better utilization of the security tools results in significant increase in the cumulative benefits of the enterprise. The more cumulative benefits bring more financial value to enterprise and this behavior is described by the ***Figure 28(b)*** and is similar to the behavior discussed in (Nazareth & Choi, 2015).

***Figure 28(c)*** shows the value of the attackers. It is argued that the value of attackers decreases with sufficient security controls in place and security investments. In the presence of these measures the attackers have to put more efforts to achieve successful attacks. This behavior results in the negative value of attackers specially in the later iterations of the simulations. The variables i.e. security investments, recovery efforts, and vulnerability reduction efforts cumulatively impact the security costs and shows an increasing trend as shown in ***Figure 28(d)***.

The number of attacks depends upon the no. of attacker, availability of attack tools in the market and the probability of the attacks. Based on these variables, there may be different number of attacks at different times as shown in ***Figure 28(g)***. The successful attacks are higher at the starting iterations of the simulation as compared to the later iterations and is shown in the ***Figure 28(h)***. At the starting iterations, the attack detection ability of the enterprise is low ***Figure 28(e)*** which increases with in the later iterations of the simulation. The increase in detection ability is due to the security investments which ultimately results in reduction of number of successful attacks. In concurrence to the

successful attacks the damage magnitude also shows the similar behavior shown in ***Figure 28(f)***. As we can observe from ***Figure 28(g)*** and ***Figure 28(h)*** that number of attacks are higher but the successful attacks are less in number. Previous research also shows the similar behavior of successful attacks, and from these only some can cause damage (Nazareth & Choi, 2015). In addition, the attack severity variation elucidates the variation in the incurred damage magnitude. As described in out model, the incurred damage magnitude activates the risk assessment efforts which further triggers the vulnerability reduction efforts. Both of these activities contributes to the increase of the security costs and tend to mirror the damage.

The behavior of all the constructs of the simulation is observed, and found that they were performing as per our expectations. Further, the sensitivity of the key input variables is also analyzed to validate the behavior of our model. This was done by systematically altering key input parameters. The expected behavior during the sensitivity analysis build our confidence on the acceptable behavior of the model. After that the simulation was ready to utilize for the alternate scenarios.

### 4.6.2 Alternate Scenario

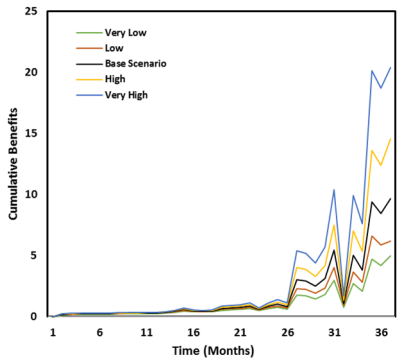
During the execution of simulation, we track the impact of these varying investments and investigated the behavior of cumulative benefits, financial value, attackers value, security costs, detection ability, damage magnitude, number of attacks and successful attacks. The behavior of results of the simulation are according to the expectations with moderate variations. ***Figure***

***29*** depict the results of the varying investments in cybersecurity information management systems.

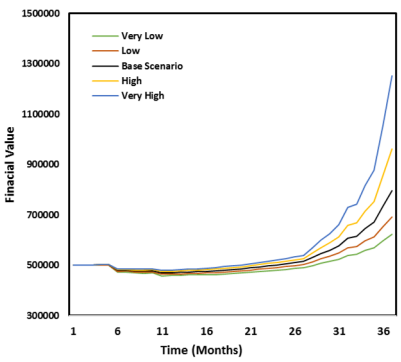
The investment in the cybersecurity information management systems (i.e., alternate scenario) have a significant impact on the cumulative benefits to an enterprise. The enterprise level benefits in terms of operational, tactical, managerial, strategic and organizational are collectively represented by the cumulative benefits.

In the start of the simulation, the impact of cybersecurity information management systems investments on the cumulative benefits to an enterprise based on the different cases (i.e. very low, low, base, high and very high) and not pronounced as shown in ***Figure 29(a)***. All the different cases show the same behavior up to 26$^{th}$ month, but after that there is significant increase in the cumulative benefits of the enterprise. The increasing behavior of cumulative benefits is proportional, based on different cases of investments in cybersecurity information management systems. The results also reveal that in the last iterations (i.e. months), there is a significant increase in the cumulative benefits with the high and very high investments as compared to the base scenario. While, in the case of low and very low investments, the increase in the cumulative benefits are considerably less pronounced.

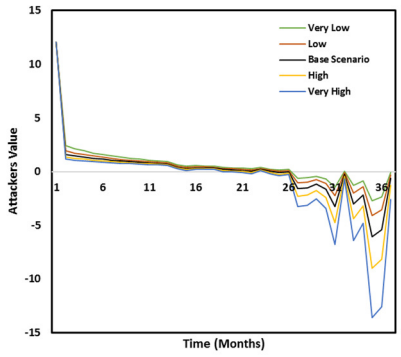
These results suggest that, the enterprise level benefits realization from the investments in the cybersecurity information management system is a time taking process. While for investing in the cybersecurity information management system, the enterprises have to plan for relatively longer time frames.



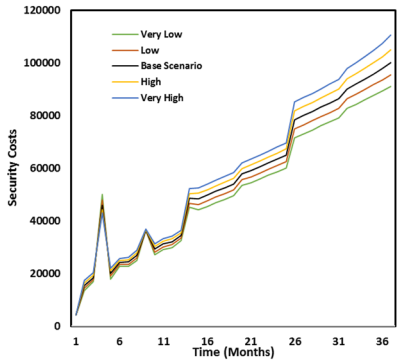

(a) - Cumulative Benefits



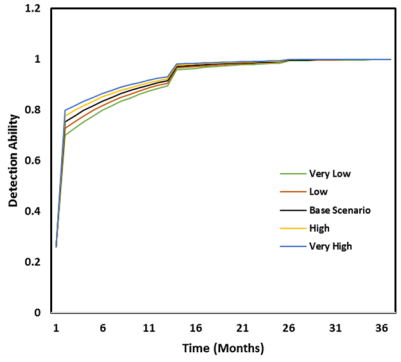

(b) - Financial Value



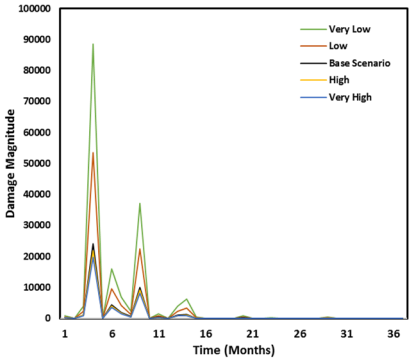

(c) - Attackers Value



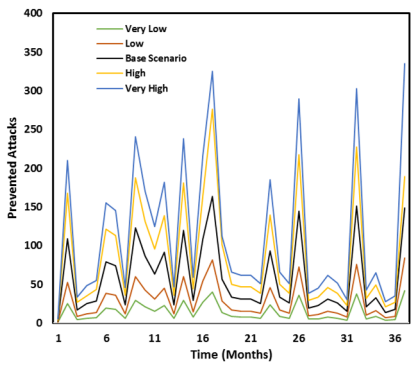

(d) - Security Costs



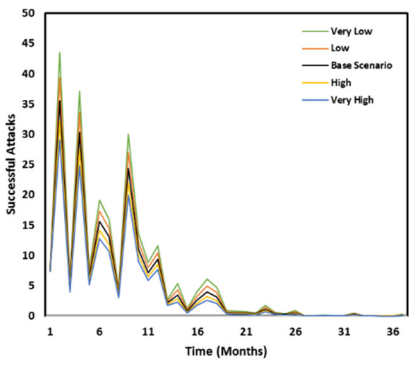

(e) - Detection Ability




(f) - Damage Magnitude




(g) - Prevented Attacks




(h) - Successful Attacks

**Figure 29. Varying Investment in Cybersecurity Information Management Systems**

In addition to increasing behavior of cumulative benefits due to the investment in cybersecurity information managent systems, the detection ability also conceives a positive impact. Security tools investment enhances the detection abilities which help to reduce the number of successful attacks. The detection ability shows a positive impact due the cumulative security tools investments, in which both the cybersecurity information management system and security tools investments are accumulated. So the detection ability increases in any case of the cumulative security tools investment and its behavior is shown in ***Figure 29(e)***. It is assumed that the enterprise has already has some investment in security tools which provide some level of detection ability. At the start of simulation, the detection ability is very low, but there is a pronounced increase after the first iteration. The investments in the cumulative security tools are made on annual bases, due to reasons discussed in ***Section 4.5.1***. Thus after first iteration we can observe a significant growth in the detection ability. The sudden increase in the detection ability can be explained by the fact that, in the

presence of basic security controls or tools several types of basic attacks can be easily detected. But, the increasing complexity of cyberattacks makes the situation worse and requires more investments in cumulative security tools.

It is observed that a significant reduction in successful attacks can be achieved through added investment in cumulative security tools. Further, it is also observed that the number of successful attacks is nearly double for low investments in cumulative security tools. In summary, the reduction in cumulative security tools investment have a significant impact on the number of successful attacks, whereas added investments considerably reduce that number ***Figure 29(h)***. ***Figure 29(g)*** presents the behavior of the prevented attacks. It also follow the similar behavior to the successful attacks ***Figure 29(h)***. The prevented attacks due to the added investments (i.e. high and very high) are significantly higher (about double in number) than the lower investments. But the fact is that the number of prevented attacks is not a reliable measure to present the performance of security controls. Because, the severity of the attacks is not similar and may be one successful attack is more damaging than the collective prevented attacks.

After first iteration, the growth in detection ability is very slow and after $12^{th}$ iteration we can observe another major increase. The value of detection ability is normalized on 0-1 scale range (0 = minimum and 1=maximum). We observed that, the detection ability reaches to maximum after $26^{th}$ iteration but it always remains below the value 1. This asymptotic behavior is due to the emergence of zero day vulnerabilities which have higher chances of exploitation because their remedies and detection capabilities take some time to develop. The

difference in the emergence time of zero day vulnerabilities and the time at which the remedies become available is one of the reason that keeps the value of detection ability always less than 1 (i.e. not all the attacks can be detected). Conclusively, it is argued, that with the decreased level of cumulative security tools investments, the number of successful attacks increases and, correspondingly, the damages incurred and the overall security cost also increases. The overall security cost also includes the recovery cost, cost of risk assessment efforts and cost of vulnerability reduction efforts.

The impact of cybersecurity information management systems investments on the financial value of the enterprise is shown in ***Figure 29(b)***. For all the cases of alternate scenario, the value of variable "financial value" is initialized similar to the base scenario. The financial value is the profit margins, market capitalization, current stock price and the brand image of the enterprise (Oosthuizen et al., 2018). In the simulation results, we can observer that the financial value shows the similar behavior as of cumulative benefits because the later has a positive impact on the former variable. The financial value shows an increasing trend but the growth rate is much pronounced after $26^{th}$ iteration. The increased financial value results in increased target attractiveness and ultimately the probability of attack will be increased. In this case, the successful attacks on the enterprise also increases which have the potential to cause huge damage. Further, more financial value can trigger increased efforts to reduce the vulnerabilities of the enterprise and also triggers enhanced investments in the deterrence. Conclusively, we can argue that the increased financial value of an enterprise will increase the overall security investments.

The impact of different level of deterrence investments has also analyzed. In comparison with the cumulative security tools investment, the impact of deterrence investment on the attacker's value is negligible. This behavior can be explained that the deterrence strategy is mostly effective for the insider attacker, while the external attackers are at lower priority in this strategy (Nazareth & Choi, 2015). Additionally, the deterrence practices are not successful against the experienced external attacker, because the probability of trace-back is often low and also prosecution thereafter is extremely unlikely.

The results of the overall security costs are also providing insightful behavior of the security investments. The overall security cost includes the security investments, cost of risk assessments, and cost of recovery efforts and cost of vulnerability reduction effort. The damage magnitude triggers the recovery efforts, risk assessment / reassessment efforts and ultimately vulnerability reduction efforts. These costs represent a relatively smaller component and are also driven by the extent of the incurred damage. The cumulative effect of these costs is shown in ***Figure 29(d)***. We observe a sudden increase in the security at the $4^{th}$ iteration of the simulation. This is because at the initial iterations the security investments is low and the number of successful attacks are high which can be observed ***Figure 29(h)***. The damage due to the successful attacks triggers the security cost. With a little lag, this behavior can be comparable in ***Figure 29(g)*** and ***Figure 29(h)***. Overall, an increasing trend of the security cost is observed. The same may not be argued for cumulative security tools investment, i.e. more investment leading to a considerable lessening in overall costs, and decreases in investment leading to larger security costs. The impact

of investment in cybersecurity information management systems and security tools is pronounced and can be observed in ***Figure 29(g)***.

The security investments massively impact the value of attackers, and it decreases considerably with the availability of sufficient in place security controls. It can be observed from ***Figure 29(c)***, that at the initial iterations of the simulation the value of attacker is high and it suddenly decreases when the first security investments has occurred. This can be interpreted as with security investment, the enterprise can achieve the basic defensive capabilities which are sufficient for detecting and preventing a large number of non-sophisticated attacks. After, the third iteration, the value of the attacker is decreasing very slowly until 26$^{th}$ iteration. This behavior can be explained based on the fact that, with the passage of time the complexity of attacks is increasing and depends on the types of the attacks launched on the enterprise. We are not considering different types of attackers in our model, but in the real scenarios there are several types of the attackers exists with different motivations. Thus after 3$^{rd}$ iteration, there no dramatic decrease in the value of attackers. But after the 26$^{th}$ iteration (i.e. after the 3$^{rd}$ annual security investment), the value of attacker remains below 0. The justification of this behavior, is that after 26$^{th}$ iteration, the enterprise has established sufficient capabilities to protect their assets. In this scenario, the attackers have to put more efforts and have to invest more in the attacker's tools. In this situations, most of the attackers just shift to another target. But the attackers with have specific motivations, they will continue to launch the attack even with very negative value (e.g. state sponsored attacks or rival sponsored attacks). In any case, the enterprises have to invest sufficient in

the area of security. In addition, we can observe from the ***Figure 29(c)***, that in the last iterations of the simulation, the impact of high and very high investments is more pronounced on the value of attackers as compared to base scenario. Conclusively, the high investment in security have negative impact on the value of attacks but it does not mean that the assets in the enterprise are totally protected from the attacks.

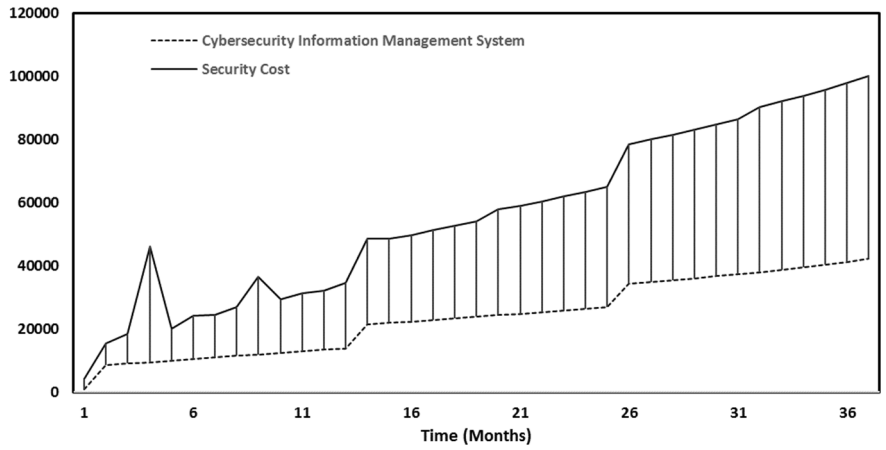



**Figure 30. Contribution of Cybersecurity Information Management System's Investment in Overall Security Cost**

In our model we have not considered all types of security costs such as professional training of security staff, training of all employees related to information security, management of information security procedures, and varying deterrence investments. We considered the security cost in terms of cybersecurity information management systems, security tools investment, risk assessment efforts, recovery efforts, vulnerability reduction effort and fixed deterrence investment. The contribution of cybersecurity information management system in the overall security cost is mentioned in ***Figure 30***. The contribution in the overall cost due to cybersecurity information management

systems is significant. On the other side, these systems are reducing the operational costs of enterprise such as regulatory compliance, report generation, monitoring, support in automations security planning and collaborations. A detailed investigation is required for investigating the impact of cybersecurity information management systems on the overall operational cost of enterprise.

## 4.7 Discussion and Conclusion

### 4.7.1 Discussion

The main focus of the model is to provide security managers with clear guidelines regarding the impact of security investments, specifically the impact of investment in cybersecurity information management systems in terms of benefits to the enterprise, financial value and attackers value. The security managers can utilize these impacts for establishing the justifications in the cybersecurity information management systems and can overcome the communication gap with the executive management.

The investment in cybersecurity information systems has twofold benefits. These systems are useful in improving the level of information security as well as several other benefits can also be achieved from them. These benefits mainly include the regulatory compliance, reports generation, monitoring, security planning, situational awareness, information security knowledge management, collaboration and trouble shooting. These benefits ultimately reduce the overall operation cost of the enterprise and specifically develops the confidence of the enterprise on its IT infrastructure. The presented model reveals that varying security investments have different implications for the costs associated with implementing the security tools specifically cybersecurity information management systems for providing security to information assets of an enterprise. Several key implications can be inferred, some of these were expected, while others provide different inference and insights. The most intuitive are that the investment in the cybersecurity information management systems increases the overall security costs but at the same time increase the

cumulative benefits and decreases the attackers value. The decreased value of attacker has plus point for enterprises because, in this situation the attacker requires more efforts to launch a successful attack. Similarly, a significant reduction in the security damages has been observed due to the investment in cumulative security tools. It has also been observed that there is not an unbounded relation because at some point, the security costs due to security investments will outweigh any achieved benefits. As evident from the literature, there exist an inverse relation between security investment and attacks (Nazareth & Choi, 2015). Further, it can be stated that even very high security investments cannot eliminate all successful attacks. In the case of additional investment in cybersecurity information management systems have the potential to increase the overall the overall cumulative benefits of the enterprise. But, in the presence of high level of security tools investment, additional investment in security tools does not bring additional security and cannot reduce the successful attacks to zero. However, a strong justification of investing in the cybersecurity information management can be established by considering the operational benefits of the enterprise as well as the enhancement in the level of security.

It has been evident from the literature, that appropriate level of security investments is necessary for an enterprise (discussed in detail in ***Section 4.2***). In order to prevent the reinforcing loop of security attacks, it is mandatory to have sufficient security investment in appropriately scrutinized security controls and measures. If the reinforcing loop on the security attacks are not checked, then it may result in increase in the number of attacks. In this case, if

an attack become successful then a perception can be established that the target enterprise system is vulnerable and eventually leading to untenable situations regarding the protection of information assets (Nazareth & Choi, 2015).

The assets of an enterprise are more likely to scattered at multiple locations and among several platforms. Therefore, a combination of security strategies is required to protect all the dispersed assets of an enterprise. For improving the information security, the enterprises have to invest in different strategies such as security tools, deterrence and vulnerability reduction. All these strategies jointly take part in improving the information security of enterprise. Investment in different strategies have varying payoffs. Our model considers mainly the investment in the security tools, which is further categorized into cybersecurity information management system and other security tools. In the cybersecurity information management systems, we mainly considered the "Security Information and Event Management – SIEM" and "Threat Intelligence Management and Sharing Platform - TIP". While, the security tools include the anti-malware programs, spyware detection programs, firewalls, intrusion detection systems and anti-virus programs. It is a common practice, that enterprises are deploying a combination of security tools to prevent from the attacks and secure the information assets. Previous researches established that, among the security strategies the investments in security tools have greatest benefits by preventing more attacks. While, cutback on security tool investment is most damaging effect. The results of our model shows that the portfolio of security tools i.e. combination of cybersecurity information management systems and other security tools are providing the balance approach to protect

the enterprise from different types of attacks. Any prevented attack has definite payoff in terms of cumulative benefits, reduced damage potential, detection ability, recovery effort, and subsequent risk assessment and vulnerability reduction effort.

The strategy of cybersecurity information sharing for improving the enterprise level security is getting importance. The attackers are using innovating ways for launching the sophisticated attacks. In this scenario, the utilization of cybersecurity information becoming more effective to protect the assets of the enterprise. The cybersecurity information is available in different forms with varying formats. It can be obtained within the enterprise from different types of security controls as well as from outside the enterprise in the form of threat feeds, active vulnerabilities information and intelligence reports.

The cybersecurity information management systems having enterprise wide scope are being used to manage the internal and external information. These systems show the potential of having two way benefits; first these systems provide additional support to the detection ability and secondly these systems help to reduce the security as well as general operation costs of the enterprises. In the former case, it can be argued that the monitoring of logs, received information through external collaborations, sophisticated trend analysis and visualizations, and knowledge management can provide additional detection abilities and insights to the overall enterprise's security situation. Hence, improved detection ability can potentially lead to less successful attacks and less damage to information assets. This information can be useful for adjusting the configurations of the security tools according to the severity and urgency of

security threats. In the latter case, these systems have the potential to effectively support the regulatory compliance in several areas which is mandatory due to existence of several regulations such as HIPAA, PCI/DSS, HITECH, ISO, SOX and GDPR. The investment in the cybersecurity information management systems is valuable and hence, security managers must have to consider this area for investment.

The previous researches indicates that investing in certain areas of information security has some certain payoffs i.e. investing in some area is more beneficial than the others (Nazareth & Choi, 2015). Most of the researches who used the system dynamics are focusing the costs and attacks. While, the model proposed in this research is more focused towards understanding the benefits of investing in the security tools (i.e. costs in security tools).

There are several implications for researchers. This research can be used for structural analysis and understanding the cumulative benefits that the investment in security tools brings to the enterprise. The results indicate that the investment in cybersecurity information management systems has twofold benefits. These benefits have impact on recuing the operational cost of the enterprise as well as increasing the security of the information assets. The investment in security tools results in increase in the security cost but at the same time it decreases the operational cost of the enterprise. A detailed investigation needs to be initiated to analyze the phenomenon of equilibrium between the enterprise security and operational cost. It is likely that at some point, the marginal cost will outweigh the marginal benefit; this introduces the notion of an optimal investment level. The model can also be used to investigate

the cumulative benefits and level of information security for different tools and systems under a varying conditions.

### 4.7.2 Concluding Remarks

Enterprises put a lot of efforts and investment to secure their critical information assets and network infrastructure. Several security strategies and security tools are used to improve the security posture of the enterprises. Even in the presence of sufficient security investment and security tools, it is unlikely that all assets can be made absolutely secure. After a certain security level, it become prohibitively expensive for enterprises to achieve an absolute security level. For achieving the appropriate level of information security, the security mangers have to communicate suitable justifications of investment in security endeavors to their executive management for the sanction of security budget.

This research provides a tool to security managers for establishing the justifications for investment in cybersecurity information management systems which are aligned with the overall goals of the enterprise. We answered the three research questions that we raised in ***Section 1.4.2***. The ***Section 4.6.1*** and ***Section 4.6.2*** uses different scenarios to explain the security level in the presence of varying level of investments in the cybersecurity information management systems. It is also explained that varying level of investments directly affect the detection abilities and also have strong impact on the other benefits that enterprises obtain from high level of security.

The model proposed in this research can be used in several capacities by security researchers and practitioners. The model can serve as a decision support tool, justifying the information security investments specifically for the

cybersecurity information management systems. It can also serve as a design tool, where regulatory compliance and monitoring of IT infrastructure can be evaluated under a variety of different situations with a view to identifying best practices. The model can be used for systematic explanation of relationship between the enterprise's cumulative benefits, level of information security and overall security costs.

The system dynamics based model incorporates many information security aspects of an enterprise such as detection ability, attacker's value, successful attacks, prevented attacks, security investments and security costs. In addition, the model also analyzed the impact of investing in cybersecurity information management systems on the cumulative benefits to an enterprise in terms of operational, tactical, managerial, strategic and organizational benefits. Simulation using the model indicate that investment in cybersecurity information management systems has threefold benefits: (1) increasing the level of information security, (2) reduction in operating cost of enterprise, and (3) significantly increase the cumulative benefits. In addition, the results also suggest that these systems enhance the detection ability of enterprises which has a significant impact on the value of attackers. In addition, it can be concluded that investment in multiple area of information security needed to effectively protect the information assets of the enterprise.

### 4.7.3 Limitations

The research method which we have used for this study inherits the limitations that exists in the simulation methodologies. We use the values of the initial values of the variables from the literature and some are taken from market

surveys. This technique can only depict the inclinations of results and the nature of the impacts on the values (i.e. positive or negative impacts). There is a need to validate the interdependency through the real data from the real users of cybersecurity information management systems.

More variable can also be added to extend the depth of the study. Further, varying conditions may include the level of investment, target attractiveness, higher number of attackers, probability of attacks, differently motivated attackers, different types of attacks and cutbacks in the investment in security tools, level of collaboration with peer enterprises, and availability of updated information. These extensions will require systematic exploration of the search space and detailed structural analyses to ensure that intermediate variables are behaving appropriately.

# Chapter 5: Conclusion

## 5.1 Summary

In this research work, we studied two important ressearch problems related to cybersecurity information sharing ecosystems (i.e., stakeholder's value creation and security investment justifications).

In the first essay, we studied the value creation, value distribution and the interdependency among the stakeholders of cybersecurity information sharing ecosystem. Related to the value creation, distribution and the interdependency among the stakeholders of cybersecurity information sharing ecosystem, we developed a value creation model for the different types of stakeholders using the additive utility functions. For our study, we consider the three major types of stakeholders (i.e., cybersecurity solution providers, cybersecurity information providers and end users). The emergence of information providers in the cybersecurity market is still pretty new, so this is appropriate and timely to study the value creation and distribution in the cybersecurity information sharing ecosystems.

For using the additive utility functions, seven value parameter have been identified from the literature, including installed base, quality of service (QoS), quality of information (QoI), trusted communities, trust, timeliness, and cost. The number of end users are represented by the installed base, who are generating the monetary benefits by paying the usage fee to solution providers and information providers in the cybersecurity information sharing ecosystem. The utility of end users is enhanced through the network effects and value co-

creation (i.e., value created by the end users through the trusted communities). With respect to cybersecurity solution, QoS represent the functional and non-functional capabilities, which end users uses for improving the level of security and also for managing the cybersecurity information. The QoI represents the benefits, which end users have in managing the cybersecurity activities. Majorly, the QoI of cybersecurity information includes the correctness, relevance, completeness, accuracy, uniqueness, consistency, trust and integration of information from several information providers. Trusted communities are the group of organizations having common interest, collaborate and share information among each other and are referred as trusted communities. Timeliness is a measure of how cybersecurity information remains valid, current, and allow sufficient time for recipient to take appropriate action against emerging cyberattacks. The parameter of trust represents the willingness of end users to depend on the information provider with a feeling of relative security. With respect to cost, each type of stakeholder bear different types of cost. The different cost types include the cost of cybersecurity solution and information usage for end users, the cost of service offering for cybersecurity solution and information provider (e.g., maintenance cost, cost of managing services, cost to supports end users, cost of improving QoS and QoI). All these seven value parameters can simultaneously impact the values of stakeholders, forming a complex interdependency in the value creation model among the stakeholders.

The value creation model reveals that the major value is generated through the number of end users (i.e., install base) in the cybersecurity information sharing

ecosystem. More specifically, an increase in the number of end users triggers an increase in the value for end users due to the availability of larger trusted communities and more potential connections to other end users. Further, it also increases the benefits for the cybersecurity solution providers and information providers due to income from service sales. The simulation results show that in the current value creation model, the value for cyber security solution provider is higher than that for the information provider. The results of our simulation shows that, in the saturated market scenario, there is a risk of potential unsustainability of the value creation and distribution in the cybersecurity information sharing ecosystem. The risk is due to the high prices of the cybersecurity solutions and information sources, and it becomes more eminent with the market saturation. The end users can utilize the cybersecurity solution and information sources depending on their limited purchase power, and, under the saturated market conditions, the number of new end users joining the ecosystem decreases, which ultimately increases the potential risk of instability of the cybersecurity market. Thus, the demand is negatively affected, and the information providers specifically unable to recover their total costs.

In the second essay, we studied the impact of security investments, specifically, the impact of investments in cybersecurity information management systems in terms of benefits to the enterprise, financial value and attackers' value. The security managers can utilize these impacts for establishing the justifications in the cybersecurity information management systems and can overcome the communication gap with the executive management.

Enterprises put a lot of efforts and investments to secure their critical information assets and network infrastructure. Several security strategies and security tools are used to improve the security posture of the enterprises. Even in the presence of sufficient security investment and security tools, it is unlikely that all assets can be made absolutely secure. After a certain security level, it become prohibitively expensive for enterprises to achieve an absolute security level. For achieving the appropriate level of information security, the security mangers have to communicate suitable justifications for investment in security endeavors to their executive management for the sanction of security budget. We provide a tool to security managers for establishing the justifications for investment in cybersecurity information management systems, which are aligned with the overall goals of the enterprise. The system dynamics based model incorporates many information security aspects of an enterprise such as detection ability, attacker's value, successful attacks, prevented attacks, security investments and security costs. In addition, the model also analyzed the impact of investing in cybersecurity information management systems on the cumulative benefits of an enterprise in terms of operational, tactical, managerial, strategic and organizational benefits. Simulation using the model indicate that investment in cybersecurity information management systems has threefold benefits: (1) increasing the level of information security, (2) reduction in operating cost of enterprise, and (3) significantly increase the cumulative benefits. In addition, the results also suggest that these systems enhance the detection ability of enterprises, which has a significant impact on the value of attackers.

## 5.2 Implications

The findings of the value creation model can have implications for the business manager to make policy decisions related to the business models and pricing schemes for the cybersecurity solution providers and information providers. The solution and information providers have to devise strategies that support the values of each other, in order to survive for a long time period and make the market stable. The strategies related to bundling of cybersecurity solutions and information sources in one package will be attractive strategy for suitability in the cybersecurity information sharing ecosystem. Furthermore, for bundling options, attractive revenue sharing schemes are vital for sustainability of value generation for all the stakeholders as well as for the growth of the cybersecurity information sharing ecosystem.

Similarly, there are several implications for researchers in analyzing the impact of investments in security strategies. This research can be used for structural analysis and understanding the cumulative benefits that the investment in security tools brings to the enterprise. The results indicate that the investment in cybersecurity information management systems has twofold benefits. These benefits have impact on recuing the operational cost of the enterprise as well as increasing the security of the information assets. The investment in security tools results in an increase in the security cost, but, at the same time, it decreases the operational cost of the enterprise. A detailed investigation needs to be initiated to analyze the phenomenon of equilibrium between the enterprise security and operational cost. It is likely that at some point, the marginal cost will outweigh the marginal benefit; this introduces the notion of an optimal

investment level. The model can also be used to investigate the cumulative benefits and level of information security for different tools and systems under a varying conditions.

## 5.3 Limitations of Study

The research method, which we have used for these studies, inherits the limitations that exists in simulation methodologies.

Regarding the first essay, in order to represent the interdependence among the stakeholders and to model the assumptions of the presented value creation model, we use the relative values for some variables, but, for other variables, we use the real values. Therefore, this technique can only depict the inclinations of results and the nature of the impacts on the values (i.e., positive or negative impacts). There is a need to validate the interdependency through the real data from the cybersecurity information sharing ecosystem.

Regarding the second essay, the results of the simulation needs to be verified with real data from enterprises, who have already adopted a cybersecurity information management system. Furthermore, more variable can also be added to extend the depth of the study. Further, varying conditions may include the level of investment, target attractiveness, higher number of attackers, probability of attacks, differently motivated attackers, different types of attacks and cutbacks in the investment in security tools, level of collaboration with peer enterprises, availability of updated information. These extensions will require systematic exploration of the search space and detailed structural analyses to ensure that intermediate variables are behaving appropriately.

## 5.4 Suggestions for Further Research

In the future, it is proposed that the study in the first essay will be extended by including more factors such as the detailed market structures, competitive environments, pricing models, and the structure of trusted communities, to establish a fine-grained value creation model in cybersecurity information sharing ecosystems.

For the future research related to the second essay, it is proposed that a emprical study is needed, in which data and experiences of actual users from enterprises will be analyzed, who have already adopted the cybersecurity information management systems. This type of data will be helpful to identify the most important benefits that can be achieved from these systems and dependency among the different factors.

# References


[A]. (2019). Threatstream, Anomali, Security intelligence and information sharing strategy. Retrieved from threatstream.com

[APCERT]. (2019). Asia Pacific Computer Emergency Response Teams (APCERT). Retrieved from http://www.apcert.org

[C]. Congress, Cybersecurity Information Sharing Act of 2015 (2015). USA. Retrieved from https://www.cisecurity.org/newsletter/cybersecurity-information-sharing-act-of-2015/

[CD]. Cabinet Decision, The Government of Japan, The Basic Act on Cybersecurity (2015). Retrieved from http://www.loc.gov/law/foreign-news/article/japan-cybersecurity-basic-act-adopted/

[CD]. Cabinet Decision, The Government of Japan, The Cybersecurity Strategy (2015). Retrieved from https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

[CSIRT]. (2019). National Computer Security Incident Response Teams (CSIRTs). Retrieved from https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/index.cfm

[DHS]. Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015, The Department of Homeland Security [DoHS], The Department of Justice (2016). USA. Retrieved from https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec 105%28a%29%29.pdf

[EC]. European Commission. Cybersecurity strategy of the European Union: an open, safe and secure cyberspace. (2013). Europe. Retrieved from http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[ECSO]. (2018). Industry 4.0 and ICS Sector Report - Cyber security for the industry 4 . 0 and ICS sector. Retrieved from https://www.ecs-org.eu/documents/uploads/industry-40-and-ics-sector-report-032018.pdf

[ENISA]. (2017). Exploring the opportunities and limitations of current Threat Intelligence Platforms. Retrieved from https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

[ETSI]. (2017). Technical Report, CYBER; Global Cyber Security Ecosystem,

ETSI TR 103 306 V1.2.1 (2017-03). Retrieved from http://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.02.01_60/tr_103306v010201p.pdf

[FIRST]. (2019). Forum of Incident Response and Security Teams. Retrieved from https://www.first.org/

[FS-ISAC]. (2019). Financial Services Information Sharing and Analysis Center (FS-ISAC). Retrieved from https://www.fsisac.com/

[G]. (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[IBM]. (2018). The Average Cost of a Data Breach. Retrieved from https://www.ibm.com/security/data-breach

[IEEE ICSG]. (2014). IEEE ICSG Malware Metadata Exchange Format Working Group. Malware metadata exchange format version 1.2. IEEE ICSG Malware Metadata Exchange Format Working Group,. New Jersey, USA.

[IOS-IEC]. (2009). ISO/IEC 19770-2: Software Asset Management—Part 2: Software Identification Tag. International Organization for Standardization/International Electro-Technical Commission. Geneva, Switzerland.

[ISAO]. (2016). The ISAO Standards Organization, ISAO 300-1: Introduction To Information Sharing. Retrieved from https://www.isao.org/products/isao-300-1-introduction-to-information-sharing/

[ITGI]. (2006). Information security governance: Guidance for boards of directors and executive management, IT Governance Institute. Chartered Accountants Journal. ISACA.

[ITU-T]. (2011). ITU-T X.1521, Common Vulnerability Scoring System. International Telecommunications Union. Geneva, Switzerland.

[ITU-T]. (2012). ITU-T X.1524, Common Weakness Enumeration. International Telecommunications Union. Geneva, Switzerland.

[ITU-T]. (2013). ITU-T X.1544, Common Attack Pattern Enumeration and Classification. International Telecommunications Union. Geneva,

Switzerland.

[ITU-T]. (2014a). ITU-T X.1520, Common Vulnerabilities and Exposures. International Telecommunications Union. Geneva, Switzerland.

[ITU-T]. (2014b). ITU-T X.1526, Language for the Open Definition of Vulnerabilities and for the Assessment of a System State. International Telecommunications Union. Geneva, Switzerland.

[ITU-T]. (2014c). ITU-T X.1546, Malware Attribute Enumeration and Characterization. International Telecommunications Union . Geneva, Switzerland.

[JPCERT]. (2014). JPCERT/CC and IPA, Japan Vulnerability Notes. Retrieved from http://jvn.jp/

[KCC]. Korea Communications Commission. Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (2001). South Korea.

[MITRE]. (2014a). The MITRE Corporation, Common Configuration Enumeration (CCE). Retrieved from https://cce.mitre.org

[MITRE]. (2014b). The MITRE Corporation, Common Event Expression. Retrieved from http://cee.mitre.org/

[MITRE]. (2014c). The MITRE Corporation, Common Result Format Specification Version 0.3. Retrieved from http://crf.mitre.org/

[MITRE]. (2014d). The MITRE Corporation, Common Weakness Scoring System. Retrieved from http://cwe.mitre.org/cwss/

[MITRE]. (2014e). The MITRE Corporation, Cyber Observable eXpression. Retrieved from http://cybox.mitre.org/

[MITRE]. (2014f). The MITRE Corporation, Making Security Measurable. Retrieved from http://msm.mitre.org/

[NIS]. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (2016).

[NIST]. (2014a). National Institute of Standards and Technology, Common Configuration Enumeration (CCE). NIST Interagency Report. Retrieved from https://nvd.nist.gov/config/cce/index

[NIST]. (2014b). National Institute of Standards and Technology, National

Vulnerability Database Version 2.2. Retrieved from http://nvd.nist.gov/

[OSF]. (2014). Open Security Foundation, Open Sourced Vulnerability Database. Retrieved from http://osvdb.org/

[OSSIM]. (n.d.). Open Source Security Information and Event Management. Retrieved from https://www.alienvault.com/products/ossim

[RH]. (2014). Red Hat Inc. Security Measurement. Retrieved from https://www.redhat.com/security/data/metrics/

[S]. (2002). Symantec, The value of information security. Retrieved from http://www.softchoice.com/portal/symantec/pdf/whitepaper_value.pdf

[SPLUNK]. (n.d.). Threat Intelligence framework in Splunk ES. Retrieved from https://www.splunk.com/en_us/software/enterprise-security.html

[TC]. (2015). Threat Intelligence Platforms: Everything You've Ever Wanted to Know But Didn't Know to Ask. Retrieved from https://threatconnect.com/download-ebook/

[TC]. (2018). ThreatConnect. Guide to threat intelligence platforms. Retrieved from https://threatconnect.com/

[TQ]. (2019a). ThreatQuotient. Retrieved April 15, 2019, from threatq.com/

[TQ]. (2019b). TopQuadrant, Inc. TopBraid Composer-Maestro Edition (IDE). Retrieved April 15, 2019, from http://www.topquadrant.com/tools/IDE-topbraid-composer-maestro-edition/

[TWH]. Improving Critical Infrastructure Cybersecurity, The White House, U.S. Office of the Press Secretary (2013). USA. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity/

[TWH]. Executive Order - Promoting Private Sector Cybersecurity Information Sharing, The White House, U.S. Office of the Federal Register (2015). Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promotingprivate-sector-cybersecurity-information-shari.

[VS]. (2015). Ventana Systems, Vensim Software Windows Version 7.2 a. Retrieved from http://vensim.com/

Ablon, L. (2018). Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. RAND.

Agular Rodriquez, A. (2017). Understanding the dynamics of Information Security Investments. A Simulation-Based Approach.

Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence.

Alter, S., & Sherer, S. A. (2004). A general, but readily adaptable model of information system risk. The Communications of the Association for Information Systems, 14(1), 35.

Amit, R., & Zott, C. (2001). Value creation in e-business. Strategic Management Journal, 22(6-7), 493–520. https://doi.org/10.1002/smj.187

Anderson, R. (2001). Why information security is hard: An economic perspective. In In ACSAC: Proceedings of the seventeenth annual computer security applications conference (pp. 358–365). Los Alamitos, CA: IEEE.

Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2008). Security economics and the internal market. Report to the European Network and Information Security Agency.

Anderson, R., & Schneier, B. (2005). Guest Editors' Introduction: Economics of Information Security. IEEE Security & Privacy, 3(1), 12–13.

Andrieux, Alain, Karl Czajkowski, Asit Dan, Kate Keahey, Heiko Ludwig, Toshiyuki Nakata, Jim Pruyne, John Rofrano, Steve Tuecke, and M. X. (2007). Web services agreement specification (WS-Agreement). In Open Grid Forum, 128, 216.

Appala, S., Cam-Winget, N., McGrew, D., & Verma, J. (2015). An Actionable Threat Intelligence system using a Publish-Subscribe communications model. In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security - WISCS '15 (pp. 61–70). https://doi.org/10.1145/2808128.2808131

Aviad, A., Węcel, K., & Abramowicz, W. (2018). A Concept for Ontology-Based Value of Cybersecurity Knowledge. International Journal of Management and Economics, 54(1), 50–57.

Baek, S., Kim, K., & Altmann, J. (2014). Role of platform providers in service networks: The case of Salesforce.com app exchange. In 16th IEEE Conference on Business Informatics (CBI ) (pp. 39–45). Geneva, Switzerland: IEEE. https://doi.org/10.1109/CBI.2014.58

Banghart, J., Quinn, S., & Waltermire, D. (2010). Open Vulnerability Assessment Language (OVAL) Validation Program Derived Test Requirements. National Institute of Standards and Technology.

Barahona, D. (Anomali ). (2017). The Second Annual Ponemon Study - The Value of Threat Intelligence. Retrieved from https://www.anomali.com/blog/the-second-annual-ponemon-study-the-value-of-threat-intelligence

Barlas, Y. (1989). Multiple tests for validation of system dynamics type of simulation models. European Journal of Operational Research, 42(1), 59–87.

Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics. System Dynamics Review: The Journal of the System Dynamics Society, 12(3), 183–210.

Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120.

Barnum, S. (2008). Common attack pattern enumeration and classification (capec) schema description. Cigital Inc,.

Barnum, Sean. (2012). Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corporation, 11, 1–22.

Behara, R. S., Huang, C. D., & Hu, Q. (2007). A System Dynamics Model of Information Security Investments. In ECIS (pp. 1572–1583).

Bettencourt, L. A., & Ulwick, A. W. (2008). The customer-centered innovation map. Harvard Business Review, 86(5), 109.

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. IEEE Security & Privacy, (5), 35–41.

Böhme, R., & Moore, T. (2016). The “iterated weakest link” model of adaptive security investment. Journal of Information Security, 7(02), 81.

Branscomb, L. M., & Michel-Kerjan, E. O. (2006). Public–private collaboration on a national and international scale. In Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability (pp. 395–403). https://doi.org/10.1017/CBO9780511509735.024

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security

information sharing to threat management. In Proceedings of the 2nd ACM workshop on information sharing and collaborative security (pp. 43–49). ACM.

Bruce J. Bakis, E. D. W. (2017). Building a National Cyber Information-Sharing Ecosystem, The MITRE Corporation. Retrieved from https://www.mitre.org/publications/technical-papers/building-a-national-cyber-information-sharing-ecosystem

Bryson, J. M. (2004). What to do when stakeholders matter: stakeholder identification and analysis techniques. Public Management Review, 6(1), 21–53.

Buck, K., Das, P., & Hanf, D. (2008). Applying ROI analysis to support SOA information security investment decisions. In 2008 IEEE Conference on Technologies for Homeland Security (pp. 359–366). IEEE.

Butler, J. M. (2009). Benchmarking security information event management (SIEM). A SANS Whitepaper.

Buttner, A., & Ziring, N. (2009). Common Platform Enumeration (CPE) - specification. Retrieved from http://cpe.mitre.org/

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11(3), 431–448.

Cavelty, M. D. (2015). Cyber-security and private actors, Routledge handbook of private security studies.

Cavusoglu, H. (2002). The economics of information technology (IT) security. AMCIS 2002 Proceedings, 344.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004a). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87–92.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. Information Systems Research, 16(1), 28–46.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. Journal of Management Information Systems, 25(2), 281–304.

Chand, D., Hachey, G., Hunton, J., Owhoso, V., & Vasudevan, S. (2005). A balanced scorecard based framework for assessing the strategic impacts of ERP systems. Computers in Industry, 56(6), 558–572.

Cheikes, Brant A., David Waltermire, and K. S. (2011). Common platform enumeration: Naming specification version 2.3. NIST Interagency Report, 7695.8.

Clements, M. T. (2004). Direct and indirect network effects: are they equivalent? International Journal of Industrial Organization, 22(5), 633–645.

Connolly, J., Davidson, M., & Schmidt, C. (2016). Trusted Automated eXchange of Indicator Information (TAXIITM), 2 May 2014.

Coppolino, L., D'Antonio, S., Formicola, V., & Romano, L. (2016). A framework for mastering heterogeneity in multi-layer security information and event correlation. Journal of Systems Architecture, 62, 78–88.

Cremonini, M., & Martini, P. (2005). Evaluating information security investments from attackers perspective: the return-on-attack (ROA). In Workshop on the Economics of Information Security (WEIS).

Dandurand, L. (2010). Cyber Defense Data Exchange and Collaboration Infrastructure (CDXI). In ITU-T Workshop.

Dandurand, Luc, & Serrano, O. S. (2013). Towards improved cyber security information sharing. In Cyber Conflict (CyCon), 2013 5th International Conference (pp. 1–16). IEEE.

Danyliw, Roman, Jan Meijer, and Y. D. (2007). The incident object description exchange format. No. RFC 5070.

Davenport, T. H. (2000). Mission critical: Realizing the promise of enterprise systems. Harvard Business Press.

Dey, D., Lahiri, A., & Zhang, G. (2012). Hacker behavior, network effects, and the security software market. Journal of Management Information Systems, 29(2), 77–108.

Dey, D., Lahiri, A., & Zhang, G. (2014). Quality Competition and Market

Segmentation in the Security Software Market. Mis Quarterly, 38(2).

Di Sarno, C., Garofalo, A., Matteucci, I., & Vallini, M. (2016). A novel security information and event management system for enhancing cyber security in a hydroelectric dam. International Journal of Critical Infrastructure Protection, 13, 39–51.

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. Computers & Security, 63, 1–13.

Dorigo, S. (2012). Security Information and Event Management. Radboud University Nijmegen. Retrieved from https://www.ru.nl/publish/pages/769526/thesissanderdorigo.pdf

Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. International Journal of Critical Infrastructure Protection, 2(4), 179–187.

Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. System Dynamics Review: The Journal of the System Dynamics Society, 24(3), 349–375.

Edwards, C., Migues, S., Nebel, R., & Owen, D. (2002, March 28). System and method of data collection, processing, analysis, and annotation for monitoring cyber-threats and the notification thereof to subscribers. Google Patents.

Eisenga, A., Jones, T. L., & Rodriguez, W. (2012). Investing in IT security: how to determine the maximum threshold. International Journal of Information Security and Privacy (IJISP), 6(3), 75–87.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. Academy of Management Review, 14(1), 57–74.

Esteves, J. (2009). A benefits realisation road-map framework for ERP usage in small and medium-sized enterprises. Journal of Enterprise Information Management, 22(1/2), 25–35.

Ettredge, M. L., & Richardson, V. J. (2003). Information transfer among internet firms: the case of hacker attacks. Journal of Information Systems, 17(2), 71–82.

Ezingeard, J.-N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. Information Systems Management, 22(2), 20–29.

Ezrati, M. (2018). Cybersecurity: A Major Concern And A Great Business Opportunity. Retrieved May 25, 2019, from https://www.forbes.com/sites/miltonezrati/2018/09/05/cyber-security-a-major-concern-and-a-great-business-opportunity/#602f51013e26

Feltus, C., & Proper, E. H. A. (2017a). Conceptualization of an abstract language to support value co-creation. In 2017 Federated Conference on Computer Science and Information Systems (FedCSIS) (pp. 971–980). IEEE.

Feltus, C., & Proper, E. H. A. (2017b). Towards a security and privacy co-creation method. In 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 75–80). IEEE.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2014). Game theory meets information security management. In IFIP International Information Security Conference (pp. 15–29). Springer.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision Support Systems, 86, 13–23.

Fleming, M., & Goldstein, E. (2012). Metrics for measuring the efficacy of critical-infrastructure-centric cybersecurity information sharing efforts. Available at SSRN 2201033.

Forrester, J. (1961). Industrial Dynamics MIT Press. Cambridge, Massachusetts.

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. E & i Elektrotechnik Und Informationstechnik, 132(2), 106–112.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16(2), 186–208.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. Information Management & Computer Security, 11(2), 74–83.

Garrido-Pelaz, R., González-Manzano, L., & Pastrana, S. (2016). Shall we collaborate?: A model to analyse the benefits of information sharing. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (pp. 15–24). ACM.

Garvey, P. R., Moynihan, R. A., & Servi, L. (2013). A macro method for

measuring economic-benefit returns on cybersecurity investments: The table top approach. Systems Engineering, 16(3), 313–328.

George, G., Haas, M. R., & Pentland, A. (2014). Big Data and Management. Academy of Management Journal, 57(2), 321–326. https://doi.org/10.5465/amj.2014.4002

Ginevičius, R. (2008). Normalization of quantities of various dimensions. Journal of Business Economics and Management, (1), 79–86.

Gonzalez, J. J., & Sarriegui, J. M. (2004). System dynamics modeling for information security: An invitational group modeling workshop. Pittsburgh, PA.

Goodwin, C., Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., … Neutze, J. (2015). A framework for cybersecurity information sharing and risk reduction. Microsoft.

Gordon, L. A., & Loeb, M. P. (2002a). Return on information security investments: Myths vs. Realities. Strategic Finance, 84(5), 26–31.

Gordon, L. A., & Loeb, M. P. (2002b). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438–457.

Gordon, L. A., & Loeb, M. P. (2006). Information Security Expenditures. Communications of the ACM, 49(1), 121–125.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 22(6), 461–485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. Journal of Information Security, 6(1), 24.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). Increasing cybersecurity investments in private sector firms. Journal of Cybersecurity, 1(1), 3–17.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015c). The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy, 34(5), 509–519.

Gordon, Loeb, & Sohail. (2017). Market Value of Voluntary Disclosures Concerning Information Security. MIS Quarterly. https://doi.org/10.2307/25750692

Grönroos, C. (2008). Service logic revisited: who creates value? And who co-creates? European Business Review, 20(4), 298–314.

Gummesson, E. (2007). Exit services marketing - Enter service marketing. In The Marketing Book: Sixth Edition (pp. 451–471). Butterworth-Heinemann. https://doi.org/10.4324/9780080942544

Haile, N., & Altmann, J. (2012). Value creation in IT service platforms through two-sided network effects. In 9th International Conference on the Economics of Grids, Clouds, Systems and Services (pp. 139–153). Berlin, Germany: Springer. https://doi.org/10.1007/978-3-642-35194-5_11

Haile, N., & Altmann, J. (2016). Value creation in software service platforms. Future Generation Computer Systems, 55, 495–509. https://doi.org/10.1016/j.future.2015.09.029

Halbardier, A., Waltermire, D., & Johnson, M. (2011). Specification for the asset reporting format 1.1. NIST Interagency Report, 7694.

Harkins, M. W. (2016). External Partnerships: The Power of Sharing Information. In Managing Risk and Information Security (pp. 49–63). Springer.

Hart, O. (1995). Corporate governance: some theory and implications. The Economic Journal, 105(430), 678–689.

Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. Journal of Accounting and Public Policy, 25(6), 629–665.

Hausken, K. (2007). Information sharing among firms and cyber attacks. Journal of Accounting and Public Policy, 26(6), 639–688.

Hausken, K. (2015). A strategic analysis of information sharing among cyber hackers. Journal of Information Systems and Technology Management (JISTEM), 12(2), 245–270. https://doi.org/10.4301/S1807-17752015000200004

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. Risk Analysis, 38(2), 215–225.

Heinonen, K., Strandvik, T., Mickelsson, K. J., Edvardsson, B., Sundström, E., & Andersson, P. (2010). A customer-dominant logic of service. Journal of Service Management, 21(4), 531–548. https://doi.org/10.1108/09564231011066088

Herath, H. S. B., & Herath, T. C. (2008). Investments in information security: A real options perspective with Bayesian postaudit. Journal of Management Information Systems, 25(3), 337–375.

Hernandez-Ardieta, J. L., Tapiador, J. E., & Suarez-Tangil, G. (2013). Information sharing models for cooperative cyber defence. In 2013 5th International Conference on Cyber Conflict (CYCON 2013) (pp. 1–28). IEEE.

Hernandez, J. (2010). Security information and event management: business benefits and security, governance and assurance perspectives. ISACA Journal.

Hill, C. W. L., & Jones, T. M. (1992). Stakeholder-agency theory. Journal of Management Studies, 29(2), 131–154.

Hoo, K. J. S. (2000). How much is enough? A risk management approach to computer security. Stanford University Stanford.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. Risk Management and Insurance Review, 6(2), 97–121.

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. International Journal of Production Economics, 141(1), 255–268.

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. Decision Support Systems, 61, 1–11.

Huang, C. D., Hu, Q., & Behara, R. S. (2006). Economics of Information Security Investment in the Case of Simultaneous Attacks. In WEIS. Citeseer.

Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production Economics, 114(2), 793–804.

Inns, J. (2014). The evolution and application of SIEM systems. Network

Security, 2014(5), 16–17.

Irani, Z., & Love, P. E. D. (2002). Developing a frame of reference for ex-ante IT/IS investment evaluation. European Journal of Information Systems, 11(1), 74–82.

Irwin, S. (2014). Creating a Threat Profile for Your Organization. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. Information Systems Frontiers, 9(5), 493–504.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST Special Publication, 800–150.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2), 618–644.

Karmarkar, U. S., & Apte, U. M. (2007). Operations management in the information economy: Information products, processes, and chains. Journal of Operations Management, 25(2), 438–453. https://doi.org/10.1016/j.jom.2006.11.001

Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. American Economic Review, 75(3), 424–440.

Katz, M. L., & Shapiro, C. (1986). Technology adoption in the presence of network externalities. Journal of Political Economy, 94(4), 822–841.

Kearns, G. S., & Lederer, A. L. (2004). The impact of industry contextual factors on IT focus and the use of IT for competitive advantage. Information & Management, 41(7), 899–919.

Khouzani, M. H. R., Pham, V., & Cid, C. (2014). Strategic discovery and sharing of vulnerabilities in competitive environments. In International Conference on Decision and Game Theory for Security (pp. 59–78). Springer.

Kim, A. C., Lee, S. M., & Lee, D. H. (2012). Compliance risk assessment measures of financial information security using system dynamics. International Journal of Security and Its Applications, 6(4), 191–200.

Kim, K., Altmann, J., & Hwang, J. (2010). Measuring and analyzing the

openness of the Web2.0 service network for improving the innovation capacity of the Web2.0 system through collective intelligence. In Advances in Intelligent and Soft Computing (pp. 93–105). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-14481-3_8

Kim, K., Altmann, J., & Hwang, J. (2011). An analysis of the openness of the Web2.0 service network based on two sets of indices for measuring the impact of service ownership. In Proceedings of the Annual Hawaii International Conference on System Sciences HICSS. Koloa, USA. https://doi.org/10.1109/HICSS.2011.47

Kirillov, I., Beck, D., Chase, P., & Martin, R. (2010). Malware attribute enumeration and characterization. The MITRE Corporation, Tech. Rep.

Kjell Hausken. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Information Systems Frontiers, 8(5), 338–349.

Koepke, P. (2017). Cybersecurity information sharing incentives and barriers. Technical report.

Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. Journal of Cybersecurity, 2(1), 29–41. https://doi.org/10.1093/cybsec/tyw002

Lee, S. M., Kim, T., Noh, Y., & Lee, B. (2010). Success factors of platform leadership in web 2.0 service business. Service Business, 4(2), 89–103. https://doi.org/10.1007/s11628-010-0093-3

Lekvall, P., & Wahlbin, C. (1973). A Study of Some Assumptions Underlying Innovation Diffusion Functions. The Swedish Journal of Economics, 362–377. https://doi.org/10.2307/3439146

Lelarge, M. (2012). Coordination in network security games: a monotone comparative statics approach. IEEE Journal on Selected Areas in Communications, 30(11), 2210–2219.

Liebowitz, S. J., & Margolis, S. E. (1994). Network externality: An uncommon tragedy. Journal of Economic Perspectives, 8(2), 133–150.

Lim, C.-H., & Kim, K.-J. (2014). Information Service Blueprint: A Service Blueprinting Framework for Information-Intensive Services. Service Science, 6(4), 296–312. https://doi.org/10.1287/serv.2014.0086

Lim, C. H., Kim, K. J., Hong, Y. S., & Park, K. (2012). PSS Board: A structured

tool for product-service system process visualization. Journal of Cleaner Production, 37, 42–53. https://doi.org/10.1016/j.jclepro.2012.06.006

Lim, C., Kim, K. H., Kim, M. J., Heo, J. Y., Kim, K. J., & Maglio, P. P. (2018). From data to value: A nine-factor framework for data-based value creation in information-intensive services. International Journal of Information Management, 39, 121–135. https://doi.org/10.1016/j.ijinfomgt.2017.12.007

Luiijf, E., & Klaver, M. (2015). On the sharing of cyber security information. In International Conference on Critical Infrastructure Protection (pp. 29–46). Springer.

Luo, Y., Shenkar, O., & Nyaw, M.-K. (2002). Mitigating liabilities of foreignness: Defensive versus offensive approaches. Journal of International Management, 8(3), 283–300.

Maglio, P. P., Vargo, S. L., Caswell, N., & Spohrer, J. (2009). The service system is the basic abstraction of service science. Information Systems and E-Business Management, 7(4), 395–406. https://doi.org/10.1007/s10257-008-0105-1

Magnusson, C., Molvidsson, J., & Zetterqvist, S. (2007). Value creation and return on security investments (ROSI). In IFIP International Federation for Information Processing (pp. 25–35). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-72367-9_3

Markus, M. L., Axline, S., Petrie, D., & Tanis, S. C. (2000). Learning from adopters' experiences with ERP: problems encountered and success achieved. Journal of Information Technology, 15(4), 245–265.

Martin, R. A. (2007). Common weakness enumeration. Mitre Corporation.

Mayadunne, S., & Park, S. (2016). An economic model to evaluate information security investment of risk-taking small and medium enterprises. International Journal of Production Economics, 182, 519–530.

McColl-Kennedy, J. R., Vargo, S. L., Dagger, T. S., Sweeney, J. C., & Kasteren, Y. van. (2012). Health care customer value cocreation practice styles. Journal of Service Research, 15(4), 370–389.

McDougall, G. H. G., & Levesque, T. (2000). Customer satisfaction with services: putting perceived value into the equation. Journal of Services Marketing, 14(5), 392–410.

Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A., & Cooke, D. L.

(2003). A system dynamics model of an insider attack on an information system. In Proceedings of the 21st International Conference of the System dynamics Society (pp. 20–24).

Mell, P. M., & Grance, T. (2002). Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme| NIST.

Mermoud, A., Keupp, M., Huguenin, K., Palmié, M., & David, D. P. (2018). Incentives for Human Agents to Share Security Information: a Model and an Empirical Test. In 17th Workshop on the Economics of Information Security (WEIS) (pp. 1–22).

Merrilees, B., Miller, D., & Yakimova, R. (2017). The role of staff engagement in facilitating staff-led value co-creation. Journal of Service Management, 28(2), 250–264. https://doi.org/10.1108/JOSM-10-2015-0326

Miller, D. (2011). Security information and event management (SIEM) implementation. McGraw-Hill,.

Mirani, R., & Lederer, A. L. (1998). An instrument for assessing the organizational benefits of IS projects. Decision Sciences, 29(4), 803–838.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. Academy of Management Review, 22(4), 853–886.

Moses, T. (2005). eXtensible Access Control Markup Language (XACML) Version 2.0/Organization for the Advancement of Structured Information Standards (OASIS). OASIS Standard.

Naghizadeh, P., & Liu, M. (2016). Inter-temporal incentives in security information sharing agreements. In 2016 Information Theory and Applications Workshop (ITA) (pp. 1–8). IEEE.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. Information & Management, 52(1), 123–134.

Olav Sveen, F., Sarriegi, J. M., Rich, E., & Gonzalez, J. J. (2007). Toward viable information security reporting systems. Information Management & Computer Security, 15(5), 408–419.

Oosthuizen, R., Molekoa, M. M., & Mouton, F. (2018). System dynamics modelling to investigate the cost-benefit of cyber security investment. In Sixth Annual System Dynamics Conference, Jointly Hosted By The South African System Dynamics Chapter And Eskom Soc.

Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., & Smeraldi, F. (2014). Cybersecurity games and investments: A decision support approach. In International Conference on Decision and Game Theory for Security (pp. 266–286). Springer.

Park, S.-H., Lee, S. M., No Yoon, S., & Yeon, S.-J. (2008). A dynamic manpower forecasting model for the information security industry. Industrial Management & Data Systems, 108(3), 368–384.

Patrício, L., Fisk, R. P., e Cunha, J. F., & Constantine, L. (2011). Multilevel service design: From customer value constellation to service experience blueprinting. Journal of Service Research, 14(2), 180–200. https://doi.org/10.1177/1094670511401901

Pawlinski, P., Jaroszewski, P., Urbanowicz, J., Jacewicz, P., Zielony, P., Kijewski, P., & Gorzelak, K. (2014). Standards and tools for exchange and processing of actionable information. European Union Agency for Network and Information Security. Heraklion, Greece.

Payne, A. F., Storbacka, K., & Frow, P. (2008). Managing the co-creation of value. Journal of the Academy of Marketing Science, 36(1), 83–96.

Philip, J., & Salimath, M. S. (2018). A value proposition for cyberspace management in organizations. Business Information Review, 35(3), 122–127.

Pinho, N., Beirão, G., Patrício, L., & Fisk, R. P. (2014). Understanding value co-creation in complex services with many actors. Journal of Service Management, 25(4), 470–493. https://doi.org/10.1108/JOSM-02-2014-0055

Poston, R., & Grabski, S. (2001). Financial impacts of enterprise resource planning implementations. International Journal of Accounting Information Systems, 2(4), 271–294.

Praditya, D., & Janssen, M. (2015). Benefits and challenges in information sharing between the public and private sectors. In Academic Conferences Limited (p. 246).

Prahalad, C. K., & Ramaswamy, V. (2004). Co-creating unique value with customers. Strategy & Leadership, 32(3), 4–9.

Prieto, D. (2006). Information sharing with the private sector. Seeds of disaster, roots of response: how private action can reduce public vulnerability. Cambridge: Cambridge University Press.

Radianti, J., & Gonzalez, J. J. (2006). Toward a dynamic modeling of the vulnerability black market. In The Workshop on the Economics of Securing the Information Infrastructure (p. 19). Citeseer.

Rashid, Z., Noor, U., & Altmann, J. (2019). Network Externalities in Cybersecurity Information Sharing Ecosystems (pp. 116–125). Springer, Cham. https://doi.org/10.1007/978-3-030-13342-9_10

Robb, D. (2007). Eight Top Threat Intelligence Companies. Retrieved April 19, 2019, from https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html

Robert Putrus, C., & CFE, C. M. C. (2016). A Nontraditional Approach to Prioritizing and Justifying Cybersecurity Investments. MEET THE DEMAND. START TODAY. Capella. Edu/ISACA or 1.866. 933.5836, 46.

Rochet, J., & Tirole, J. (2006). Two-sided markets: a progress report. The RAND Journal of Economics, 37(3), 645–667.

Ross, A., & Moore, T. (2006). The economics of information security. Science, 314 (5799), 610–613.

Ross, J. W., & Vitale, M. R. (2000). The ERP revolution: surviving vs. thriving. Information Systems Frontiers, 2(2), 233–241.

Ross, S. A. (1973). The economic theory of agency: The principal's problem. The American Economic Review, 63(2), 134–139.

Rutkowski, A., Kadobayashi, Y., Furey, I., Rajnovic, D., Martin, R., Takahashi, T., … Hird, M. (2010). Cybex: The cybersecurity information exchange framework (x. 1500). ACM SIGCOMM Computer Communication Review, 40(5), 59–64.

Rysman, M. (2009). The economics of two-sided markets. Journal of Economic Perspectives, 23(3), 125–143.

Saarijärvi, H., Grönroos, C., & Kuusela, H. (2014). Reverse use of customer data: Implications for service-based business models. Journal of Services Marketing, 28(7), 529–537. https://doi.org/10.1108/JSM-05-2013-0111

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. Computers in Human Behavior, 57, 442–451.

Sarriegi, J. M., Santos, J., Torres, J. M., Imizcoz, D., Egozcue, E., & Liberal,

D. (2007). Modeling and simulating information security management. In International Workshop on Critical Information Infrastructures Security (pp. 327–336). Springer.

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI) (pp. 837–851). St. Gallen, S.

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. Decision Support Systems, 55(1), 156–164.

Scarfone, K., & Mell, P. (2010). The common configuration scoring system (ccss): Metrics for software security configuration vulnerabilities. NIST Interagency Report, 7502.

Schiffman, M., Wright, A., Ahmad, D., & Eschelbeck, G. (2004). The common vulnerability scoring system. National Infrastructure Advisory Council, Vulnerability Disclosure Working Group, Vulnerability Scoring Subgroup.

Schiffman, M. (2011). The common vulnerability reporting framework. Tech. Rep.

Schiffman, Mike. (2011). The common vulnerability reporting framework, Tech. Rep.

Schneier, B. (2011). Secrets and lies: digital security in a networked world. John Wiley & Sons.

Senge, P. M., & Forrester, J. W. (1980). Tests for building confidence in system dynamics models. System Dynamics, TIMS Studies in Management Sciences, 14, 209–228.

Serrano, O., Dandurand, L., & Brown, S. (2014). On the design of a cyber security data sharing system. In Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security (pp. 61–69). ACM.

Shackleford, D. (2018). CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey. Retrieved 03/04/2018 from SANS, https://www. sans. org/reading-room ….

Shackleford, Dave. (2018). CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey.

Shang, S., & Seddon, P. (2004). Enterprise systems benefits: how should they be assessed? PACIS 2004 Proceedings, 97.

Shang, S., & Seddon, P. B. (2002). Assessing and managing the benefits of enterprise systems: the business manager's perspective. Information Systems Journal, 12(4), 271–299.

Sheen, J. (2010). Fuzzy economic decision-models for information security investment. Proc. of IMCAS, Hangzhou, China, 141–147.

Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016). Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. In In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (pp. 65–70). ACM. https://doi.org/10.1145/2994539.2994546

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154–176.

Smedlund, A. (2012). Value Co-creation in Service Platform Business Models. Service Science, 4(1), 79–88. https://doi.org/10.1287/serv.1110.0001

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. Computers & Security, 58, 216–229.

Spohrer, J., Maglio, P. P., Bailey, J., & Gruhl, D. (2007). Steps toward a science of service systems. Computer, 40(1), 71–77. https://doi.org/10.1109/MC.2007.33

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems, 75, 49–62.

Sterman, J D. (2000). Business Dynamics: System Thinking and Modeling for a Complex World Irwin McGraw-Hill.

Sterman, John D. (2000). Business dynamics: systems thinking and modeling for a complex world. Irwin McGraw-Hill.

Stewart, A. (2012). Can spending on information security be justified? Evaluating the security spending decision from the perspective of a rational actor. Information Management & Computer Security, 20(4), 312–326.

Suter, M. (2012). The governance of cybersecurity: an analysis of public-private partnerships in a new field of security policy. ETH Zurich.

Suter, M. (2016). Improving information security in companies: How to meet the need for threat information. In In Power and Security in the Information Age (pp. 143–164). Routledge.

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. Journal of Accounting and Public Policy, 24(1), 37–59.

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. Journal of the American Society for Information Science and Technology, 56(3), 245–257. https://doi.org/10.1002/asi.20121

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security, 72, 212–233.

Trček, D. (2006). Using systems dynamics for human resources management in information systems security. Kybernetes, 35(7/8), 1014–1023.

Trček, D. (2008). Using system dynamics for managing risks in information systems. WSEAS Transactions on Information Science and Applications, 5(2), 175–180.

Univesity, E. (2007). Why IT Security Can Instil Confidence in a Company's Reputation and Brand. Knowledge@ Emory (Http://Knowledge. Emory. Edu/Article. Cfm.

Vakilinia, I., & Sengupta, S. (2017). A coalitional game theory approach for cybersecurity information sharing. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 237–242). IEEE.

Vargo, S. L., & Lusch, R. F. (2004). Evolving to a New Dominant Logic for Marketing. Journal of Marketing, 68(1), 1–17. https://doi.org/10.1509/jmkg.68.1.1.24036

Vargo, S. L., & Lusch, R. F. (2008). Service-dominant logic: Continuing the evolution. Journal of the Academy of Marketing Science, 36(1), 1–10. https://doi.org/10.1007/s11747-007-0069-6

Varian, H. R. (2014). Intermediate Microeconomics: A Modern Approach: Ninth International Student Edition. WW Norton & Company.

Vicini, S., Alberti, F., Sanna, A., Notario, N., Crespo, A., & Pastoriza, J. R. T.

(2016). Co-creating security-and-privacy-by-design systems. In Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016 (pp. 768–775). IEEE. https://doi.org/10.1109/ARES.2016.74

Viduto, V., Maple, C., Huang, W., & LóPez-PeréZ, D. (2012). A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. Decision Support Systems, 53(3), 599–610.

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). Misp: The design and implementation of a collaborative threat intelligence sharing platform. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (pp. 49–56). ACM.

Waltermire, D., Schmidt, C., Scarfone, K., & Ziring, N. (2011). Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2. National Institute of Standards and Technology. Gaithersburg, MD, 20899-893.

Waltermire David, Karen Scarfone, and M. C. (2011). Specification for the open checklist interactive language (OCIL) version 2.0. NIST Interagency Report, 7692. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.1031&rep=rep1&type=pdf

Wang, J. (2004). How May IT Security Affect Competitive Advantage?". In The Fourth ABIT Annual Meeting, Monroeville, Pennsylvania.

Warnecke, M. P. (2013). Examining the return on investment of a security information and event management solution in a notional Department of Defense network environment. NAVAL POSTGRADUATE SCHOOL MONTEREY CA. Retrieved from https://apps.dtic.mil/docs/citations/ADA583794

Wawrzyniak, D. (2006). Information security risk assessment model for risk management. In International Conference on Trust, Privacy and Security in Digital Business (pp. 21–30). Berlin, Heidelberg: Springer.

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. Computers & Security, 77, 807–823.

Whitman, M. E., & Mattord, H. J. (2011). Principles of information security. Cengage Learning.

Wilding, N. (2016). Cyber resilience: How important is your reputation? How effective are your people? Business Information Review, 33(2), 94–99.

Williams, A. (2006). Security information and event management technologies. Siliconindia, 10(1), 34–35.

Winkler, I., & Gomes, A. T. (2016). Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies. Syngress.

Yang, S.-C., & Wang, Y.-L. (2011). Insider threat analysis of case based system dynamics. Adv. Comput, 2, 1–17.

Yue, W. T., Çakanyıldırım, M., Ryu, Y. U., & Liu, D. (2007). Network externalities, layered protection and IT security risk management. Decision Support Systems, 44(1), 1–16.

Zhang, Y., Patwa, F., & Sandhu, R. (2016). Community-based secure information and resource sharing in Azure cloud IaaS. In Proceedings of the 4th ACM International Workshop on Security in Cloud Computing (pp. 82–89). ACM.

Zhao, W., & White, G. (2017). An evolution roadmap for community cyber security information sharing maturity model. In Proceedings of the 50th Hawaii International Conference on System Sciences.

Zheng, D. E., & Lewis, J. A. (2015). Cyber threat information sharing. Center for Strategic and International Studies.

Ziring, N., & Quinn, S. D. (2007). Specification for the Extensible Configuration Checklist Description Format (XCCDF): Version 1.1. 3. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

# Abstract (Korean)

기업은 정보 보안의 수준을 향상시키기 위하여 보안 전략 트폴리오를 활용하고 있다. 기업에서 효과적인 보안 수준을 달성하려면 여러 정보 보안 전략에 대한 투자가 필요하다. 이러한 보안 전략은 사이버 보안 정보 공유, 공격 탐지, 예방, 취약성 감축, 위험 평가, 위협 억제, 교육 및 훈련 등을 포함한다.

지난 수십년에 걸쳐 연구자들이 정보 보안 분야를 연구했지만, 정보 보안은 기업에게 여전히 매우 높은 수준의 위험으로 작용할 수 있는 불확실한 분야로 여겨진다. 새로이 증가하고 있는 정보 보안의 복잡성은 기업의 지속적인 보안 상태를 위해 상세히 살펴볼 많은 문제가 존재함을 반영한다. 우리는 정보 보안의 다양한 분야에 대한 기존 문헌을 검토하여 그간 해소되지 못하였고 앞으로도 많은 연구를 필요로 하는 두 가지의 중요한 연구 문제를 확인하였다. 따라서, 본 논문은 이 두 가지 연구 문제에 대한 해결책을 차례로 제시하여 해당 연구 문제들을 해소한다.

첫 번째로 본 논문은 사이버 보안 정보 공유 생태계의 이해당사자를 위한 가치 창출에 대해 조사한다. 조직의 보안 상태를 향상시키기 위한 정보의 활용은 보안 정보 공유 생태계의 진화로 이어진다. 사이버보안 해결책 제공자, 정보 제공자, 최종 사용자, 정부 기관, 그리고 표준화

주체 등이 보안 정보 공유 생태계를 구성하는 다섯 가지 주요 이해관계자다.

이러한 이해관계자들은 서로 다른 가치를 얻고, 그들의 가치 창출은 상호간 연관되어 있으며 복잡한 가치 분배 시스템을 만든다. 해결책과 정보 제공자와 같은 새로운 진입자들에게 해당 시장은 매우 매력적이지만 그들의 생존율은 매우 낮으며 대다수는 수년 내 사라진다. 우리는 이해관계자 사이의 복잡한 상호의존성을 만들어 이해관계자들의 가치에 동시에 영향을 미치는 일곱 가지 매개변수를 확인한다. 비용을 최소화하여 이해당사자의 효용과 이익을 잘 조정하기 위해서는 가치의 창출과 분배를 이해하는 것이 중요하다. 창출되는 가치와 비즈니스 전략 및 정책 수립을 위한 사이버 보안 정보 공유 생태계의 이해관계자가 얻는 가치 사이에는 차이가 존재한다.

본 논문에서는 사이버보안 정보 공유 생태계에 속한 이해당사자들이 충분한 가치를 창출할 수 있는지의 여부에 대해 연구한다. 또한 이해관계자 간의 상호관계를 분석하였다. 그 결과 가치 창출과 이해당사자 사이의 가치 분배의 모형과 가치 매개 변수가 이해당사자가 얻는 가치에 미치는 영향을 결정짓는 모형을 도출하였다. 본 연구의 시뮬레이션 결과는 최종 사용자가 가치의 주요 원천이라는 점과 보안 생태계의 모든 이해당사자들이 최종사용자의 성장하는 설치 기반으로부터 이익을 얻는다는 점을 보인다. 또한, 현재의 가치 창출

모형에서 사이버 보안 해결책 제공자의 가치는 정보 제공자보다 높음을 확인하였다. 포화된 시장에서는 사이버보안 해결책과 정보 원천의 높은 가격으로 인해 가치 창출과 분배의 잠재적 지속 불가능성이라는 위험이 존재한다. 이 연구의 결과는 사업 관리자들에게 사이버 보안 제공자와 정보 제공자에 대한 사업 모형과 가격 제도에 관련된 정책 결정의 측면에 함의를 제공한다.

두 번째 연구 문제와 관련하여 본 논문에서는 사이버 보안 정보 관리 시스템을 위한 기업들의보안 투자 정당성 확립 문제에 대해 연구한다. 공격 보호와 탐지 능력을 향상시키기 위해 여러 종류의 보안 도구가 사용된다. 기업의 보안 상황 인식에 대한 개선을 위해 기업의 내부 및 외부적 사이버 보안 정보를 관리하는데 위 도구들과 함께 사이버 보안 정보 관리 시스템이 활용된다. 기업이 효과적인 수준의 정보 보완을 얻기 위해서는 충분한 양의 자금을 확보할 수 있어야 한다. 따라서, 정보 보안 분야의 투자와 관련하여, 보안 관리자들은 책임 관리자들로부터 자금에 대한 허가를 얻기 위해 적절한 정당성과 편익 분석을 제시해야 한다.

사이버 보안 정보 관리 시스템의 경우, 투자 정당성의 확보에는 성과 평가와 해당 시스템으로부터 얻어지는 기업의 누적 이익을 연결 짓는 체계적 방식이 필요하다. 우리는 시스템 역학 모형을 이용하여 투자가 보안 비용, 탐지 능력, 누적 이익, 공격자의 가치, 성공적 공격, 사전

예방된 공격, 그리고 피해 규모의 측면에서 시스템 보안 정보 관리 시스템에 미치는 영향을 분석하였다. 그 결과, 해당 시스템이 기업에게 1) 정보보안 수준을 증가 2) 기업의 운영 비용 감축 3) 누적 이익의 상당한 증가라는 세 가지 측면의 이익을 제공함을 확인하였다. 보안 관리자들은 사이버 보안 정보 관리 시스템과 기타 보안 도구에 대한 투자를 위한 정당성을 확립하는데 본 모형을 사용할 수 있다.

**키워드:** 정보 공유, 사이버보안, 에코시스템, 이해관계자, 가치, 매개변수, 네트워크 효과, 사이버 보안 정보 관리 시스템, 보안 투자 결정, 시스템 다이내믹스, 시뮬레이션.

**학 번: 2016-38153**