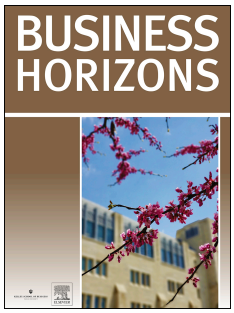

Cybersecurity: Risk management framework and investment cost analysis

In Lee, Ph.D.

PII: S0007-6813(21)00024-0

DOI: https://doi.org/10.1016/j.bushor.2021.02.022

Reference: BUSHOR 1735

To appear in: *Business Horizons*

Please cite this article as: Lee I., Cybersecurity: Risk management framework and investment cost analysis, *Business Horizons*, https://doi.org/10.1016/j.bushor.2021.02.022.

Cybersecurity: Risk management framework and investment cost analysis

In Lee, Ph.D.
Cecil P. McDonough Endowed Professor in Business
School of Computer Sciences
College of Business and Technology
Western Illinois University Macomb, IL 61455
Email: I-Lee@wiu.edu

Cybersecurity: Risk management framework and investment cost analysis

ABSTRACT

As organizations accelerate digital transformation with mobile devices, cloud services, social media, and the Internet of Things (IoT) services, cybersecurity has become a key priority in enterprise risk management. While improving cybersecurity leads to higher levels of customer trust and increased revenue opportunities, rapidly evolving data protection and privacy regulations have complicated cybersecurity management. Against the backdrop of rapidly rising cyber breaches and the emergence of novel cybersecurity technologies such as machine learning and artificial intelligence, this paper introduces a cyber risk management framework and discusses a cyber risk assessment process. This paper illustrates a continuous improvement of cybersecurity performance and cyber investment cost analysis with a real-world cybersecurity example.

Keywords: Cybersecurity, Cyber Threats, Risk Management, Risk Assessment, Cyber Investment, Data Security, Cybercrime, Cyberattack, Cybersecurity Breach

1. Introduction

According to ISO/IEC 27032:2012, cybersecurity is defined as preservation of the confidentiality, integrity, and availability of information in complex environments resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it. Along with the advances of IT, the domains of cybersecurity have constantly faced up to new threat methods and techniques aiming to take advantage of IT and human vulnerabilities. Currently, cybersecurity is considered one of the critical components in enterprise risk management, as the ever-growing cyber breaches cause a wide range of critical damages to organizations and people. These damages include penalties, reputational harm, decrease in stock value, compliance breaches, privacy breaches, and disruption of operations, to name a few.

The average number of security breaches grew by 11 percent from 130 in 2017 to 145 in 2018 per organization. The average cost of cybercrime for an organization increased US$1.4 million to US$13.0 million (Accenture, 2019). The exponential growth of smartphones, cloud services, social media, and the Internet of Things (IoT) applications has motivated cybercriminals to innovate penetration tools and techniques and increase cyberattacks. Cybercriminals not only steal data, but also disrupt operations and services. Improving cyber defense leads to higher levels of customer trust and increased revenue opportunities.

The annual cyber security spending worldwide grew by 64% from $75.6 billion in 2015 to $124 in 2020 (statista.com, 2020). Worldwide spending on security solutions will achieve a compound

annual growth rate (CAGR) of 9.2% over the 2018-2022 period and $133.8 billion in 2022. The fastest growing technology categories include managed security services (14.2% CAGR), security analytics, intelligence, response and orchestration software (10.6% CAGR), and network security software (9.3% CAGR) (IDC, 2019). The 'Top 7 security and risk trends for 2020' include creating pragmatic risk appetite statements, implementing security operations centers (SOCs), establishing a data security governance framework to prioritize data security investments, and investing in their cloud security competency (Gartner, 2020).

Installing firewall, antivirus software, and encryption technologies serves basic security functions in safeguarding organizations' computing resources from cyberattacks and intrusions, but is not sufficient in meeting the current cybersecurity needs. As a growing number of organizations use public cloud and mobile services, the scope of cybersecurity management goes beyond organizational boundaries as in the Capital One data breach case where a former Amazon cloud service employee gained access to more than 100 million Capital One customers' accounts and credit card applications early in 2019 (Bloomberg.com, 2019).

With more and more enterprises adopting cloud services to accelerate their business and promote collaboration, the importance of securing apps and data managed by public cloud services is growing. While cloud services are economical, the cloud users must assess security risks and the degree to which new human behaviors are required (Cusack & Ghazizadeh, 2016). Forrester's 2019 report estimated that by 2023 the global market for cloud security technologies will reach $12.7 billion, up from $5.6 billion in 2018, and a demand for the public cloud is driving the overall market for cloud security (eWEEK.com, 2019).

Various cybersecurity regulations have been enacted to safeguard computer systems and protect data in organizations with the primary purpose of protecting public interest. One of the major goals of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is to protect the privacy and security of healthcare information by creating national standards and improving the efficiency and effectiveness of the nation's health care system (U.S. Department of Health and Human Services, 1996). The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 expanded the scope of privacy and security protections available under HIPAA by increasing the potential legal liability for non-compliance and providing for more stringent enforcement (U.S. Department of Health & Human Services, 2009). The General Data Protection Regulation (GDPR), considered to be the toughest privacy and security law in the world, established minimum levels of organizational cybersecurity requirements for the collection and use of personal data, as well as the rights of data owners. The GDPR entered into force in 2016 after passing European Parliament and all organizations were required to be compliant in the European Union and the European Economic Area (GDPR.eu, 2018). While government regulations have been are instrumental in safeguarding personal data and computer resources, they have significantly increased compliance burden and the cyber investment costs for organizations.

Against the backdrop of the current cybersecurity issues and existing cybersecurity frameworks, this paper discusses the trends of cyberattacks and breaches. Then, this paper presents a four-layer cyber risk management framework. An illustration-based discussion with a real-world scenario follows on the cyber risk assessment and investment cost analysis.

2. Cybersecurity Trends

Cybersecurity started to gain wide attention of the public with the introduction of microcomputers. The arrival of microcomputers in the late 1970s shifted highly centralized mainframe-based computing to end-user-based decentralized computing where end-users started to develop their own applications with various office tools. However, compared to mainframe computers which were tightly controlled and protected by professional developers, end-user-developed applications on microcomputers became a fertile ground for numerous security attacks such as the Brain virus, Michelangelo virus, and Morris worm.

The invention of WWW in 1989 led to the explosive growth of web applications created new opportunities for cybercriminals. Most cyberattacks came through web systems as well as the Internet and other networks. A host of cyber threats developed to take advantage of WWW include spyware, adware, spam, spim, phishing, Denial-of-Service Attack (DoS Attack), ransomware, and eavesdropping. Cybercriminals started to apply a variety of social engineering techniques for cybercrime victims to perform certain actions or divulge confidential or personal information. Cybercriminals often exploited security flaws of Internet-connected computers to steal millions of credit card data and personal data of millions of customers from major corporations such as TJX, Target, Marshalls, and Adobe.

Recently, mobile devices and the IoT became popular targets of cybercriminals. Bring Your Own Device (BYOD) policies related to the rapid diffusion of mobile devices has introduced mobility security risks to the organizations. Employees bring their own smartphones, tablets, and laptop computers to routinely access corporate computer systems via wireless public/private networks. Many of these devices are fraught with security risks as users are less concerned about authentication and data encryption for most mobile devices and less concerned about protecting their devices from cyberattacks. Fake public Wi-Fi networks and text-message phishing scams are also some of the growing mobile security threats.

The IoT has brought about a new paradigm in which a global network of machines and devices capable of interacting with each other is driving digital innovation in enterprises (Lee, 2019). As the growing number and variety of connected devices are introduced into the IoT networks, the potential cyber threats grow exponentially. A lack of security in the IoT systems open up opportunities for cybercriminals to access sensitive customer data related to privacy and business transactions. For example, when medical IoT devices such as remote patient monitoring systems are left unprotected, the entire network can be exposed and patients become extremely vulnerable to potential attacks (Abraham, Chatterjee, Sims, 2019). Wearable devices also are also susceptible to cyberattacks that can not only compromise data, but also physically harm the wearer (Mills et al., 2016).

3. A Cyber Risk Management Framework

Cyber risk management needs to holistically address both technical and human aspects. Currently, there is a plethora of cybersecurity frameworks (e.g., NIST Cybersecurity Framework, ISO/IEC 27001, Control Objectives for Information and Related Technology (COBIT), ANSI/ISA-62443-3-3 (99.03.03)-2013). The NIST Cybersecurity Framework is voluntary guidance created through collaboration between industry and government for organizations to better manage and reduce cybersecurity risk (NIST, 2018). However, risk management issues are tangentially addressed in the NIST Cybersecurity Framework where risk management specifically relevant to supply chain with external parties was discussed.

The seven stages/chains Cyber Kill Chain® framework is also a widely used framework in cybersecurity. The model identifies what the cyber attacker must complete in order to achieve their objective and helps the defender break the chain at an early stage as well as each stage to stop the cyber attacker's malicious actions (Hutchins, Cloppert, & Amin, 2011). The framework focuses mainly on the technological side of cybersecurity involving attackers and defenders, informing stage-by-stage activities defenders can take against organized cybersecurity attacks. However, it did not fully reflect human aspects of cyber risks such as human mistakes and internal threats as witnessed in the case of Capital One - Amazon cloud data breach (Bloomberg.com, 2019).

While these well-known frameworks provide high-level qualitative guidelines for managers, none of these frameworks present a balanced view of cyber risk management. They do not explicitly address the cybersecurity ecosystem and its impacts on risk management. Furthermore, the frameworks do not provide any guide on how risk is measured quantitatively and how

cybersecurity investment can be justified. Therefore, managers are left to develop cybersecurity projects without understanding macro-level cybersecurity issues occurring in the cyber ecosystem and without quantitative risk assessment methods for adequate financial investment analysis.

This paper proposed a Cyber Risk Management Framework with a focus on the cyber ecosystem and cyber risk quantification in order to complement existing frameworks such as the NIST Cybersecurity Framework and Cyber Kill Chain® framework. The proposed framework categorizes factors affecting cyber risk into four layers, each of which is dedicated to specific functions and responsibilities related to cyber risk management. Figure 1 shows the proposed framework, which consists of the Cyber Ecosystem Layer, the Cyber Infrastructure Layer, the Cyber Risk Assessment Layer, and the Cyber Performance Layer.

The Cyber Ecosystem Layer focuses on understanding its stakeholders in the organizational environment. The Cyber Infrastructure Layer focuses on an understanding of the intraorganizational elements such as organization, employees/internal users, and cyber technologies that interact with elements of both the cyber ecosystem and the cyber risk assessment. At the Cyber Risk Assessment Layer, cyber risks are identified, quantified, and investment/spending decisions are made with the purpose of mitigating cyber risks. At the Cyber Performance Layer, investment plans are executed, prioritized cyber threats are monitored and continuous improvements are made. The elements of the Cyber Ecosystem are exogenous variables in that the values of the elements in the layer are determined outside the organization. The elements of the Cyber Infrastructure Layer, the Cyber Risk Assessment Layer, and the

Cyber Performance Layer are endogenous variables whose values are determined by the organization. Each layer is detailed below.

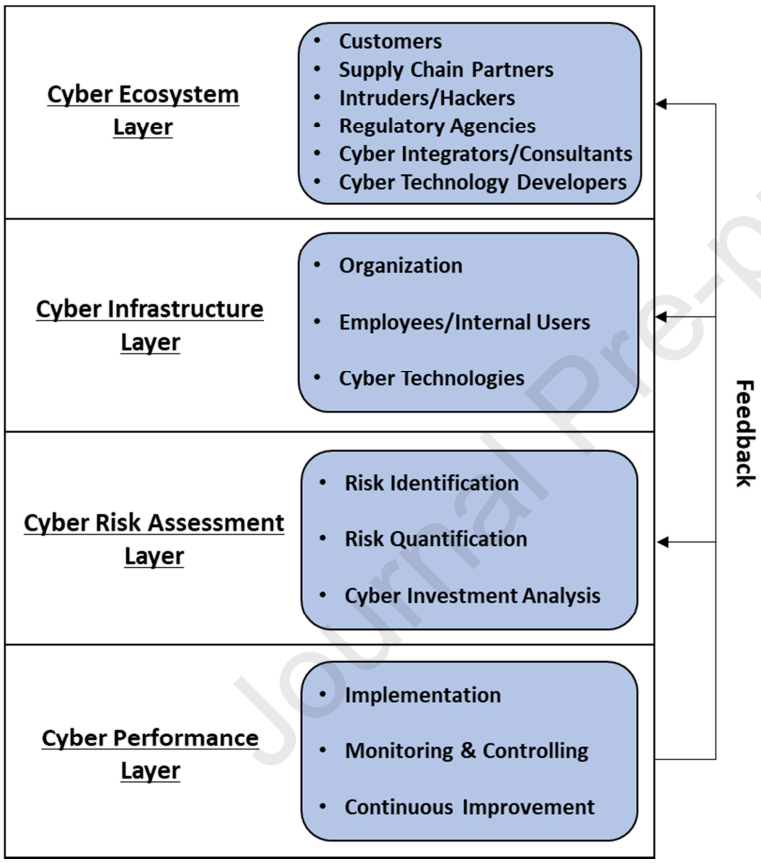

Figure 1. The Proposed Cyber Risk Management Framework

3.1 Cyber Ecosystem Layer

The Cyber Ecosystem Layer is the top layer of the Cyber Risk Management Framework. Cybersecurity involves largely independent or interdependent stakeholders whose interests and goals may not be compatible with each other. Understanding how specific stakeholders of the

cyber ecosystem interact with IT assets and services such as applications, networks, and data is a prerequisite for an organization to be able to develop defense strategies and protect the IT assets from cyberattacks. An organization's cyber ecosystem also helps them work cooperatively and competitively with stakeholders to support cybersecurity activities. An organization needs to continuously monitor and evaluate the cyber ecosystem and communicate any changes detected from the ecosystem to the other layers.

Major players in the cyber ecosystem include supply chain partners, customers, intruders/hackers, regulatory agencies, technology developers, and integrators/consultants. It is crucial to understand how and why supply chain partners and customers interact with the IT systems of an organization to conduct business transactions. It is essential to identify technology developers and integrators/consultants and to understand how they help organizations develop cybersecurity policy and technologies. It should be noted that the cyber ecosystem also includes adversaries such as intruders and hackers who commit cyberattacks for economic gains or other nefarious purposes. It is important to identify those intruders/hackers and analyze how they penetrate the organization's IT systems, steal data, install malware, and/or intercept communications. Regulatory agencies are responsible for establishing cybersecurity laws, rules, and guidelines, and overseeing compliance. Once the cyber ecosystem is evaluated, the cyber infrastructure layer is analyzed to understand the state of the internal infrastructure needed to support cyber risk management.

3.2 Cyber Infrastructure Layer

The Cyber Infrastructure Layer is the middle layer of the Cyber Risk Management Framework, which plays an active role in safeguarding the current IT assets and services of an organization. Organizations, employees/internal users, and cyber technologies are the three key elements of the Cyber Infrastructure Layer. The Cyber Infrastructure Layer focuses on both the technological and human aspects of cybersecurity management and reflects the current cybersecurity capability of an organization. The organization element defines roles, responsibilities, policies, and processes for cybersecurity management. The employee/internal users element focuses on employee awareness, morale, job satisfaction, and cyber training. The cyber technologies are deployed to detect and counter cyberattacks, mitigate the risk of threats, and ensure data confidentiality and user authentication.

The organization element plays the central role in defining their strategies for cyber defense and mitigation. A large-scale survey shows that positive attitudes toward cybersecurity policies are related to more secure behaviors (Choong & Theofanos, 2015). Sustained support from senior management is crucial to ensure that action plans are in place to mitigate the risk of cyberattacks (Esteves, Ramalho, & De Haro, 2017). Establishing the best-practice cybersecurity policy and overseeing compliance strengthen and reinforce the security practices.

The employees/internal users, also called the people element, focuses on awareness, motivation, and behavior about cybersecurity risk. The employees/internal users interact with the cyber ecosystem and presumably support organizational goals. According to a study conducted by Shred-it (2018), more than 85% of senior executives and 515 small business owners admit employee negligence is one of their most serious information security risks. In many

organizations, the people aspect of cybersecurity is one of the weakest links (Esteves, Ramalho, & De Haro, 2017). Raising cybersecurity awareness and training are critical to promoting cybersecurity best-practices and integrating them into daily tasks. It is also necessary to develop people-centric security workplaces where desirable security behaviors are disseminated amongst the employees (Dang-Pham, Pittayachawan, & Bruno, 2016).

The cyber technologies are used to protect three broad categories of IT assets and services from cyber threats: applications, networks, and data. Cyber technologies are critical for protecting organizations from threats due to the use of wireless communication technologies used in various systems, unknown security holes of IT assets and services, and connectivity to the Internet. For successful cybersecurity management, organizations need to continuously assess cyber threats towards the IT assets and services to commission and decommission various cyber technologies.

To deploy cyber technologies for applications and networks, an organization needs to analyze how the technologies are used and what the threats are to vulnerabilities of the applications and networks. Data is another important consideration in cyber technology deployment. The explosive growth of unstructured distributed data increases cyber vulnerabilities threats to organizations. To understand what data are generated, how the data are used, and what data are targets of cyberattacks is important to the adoption of specific cyber technologies for data security. Recently, machine learning technologies have been receiving growing attention, as they showed better results in some scenarios than traditional cybersecurity technologies (Lezzi, Lazoi, & Corallo, 2019).

3.3 Cyber Risk Assessment Layer

The cyber risk assessment layer plays a central role in the cyber risk management framework. Abraham, Chatterjee, and Sims (2019) present a three-stage approach to understanding, valuing, and mitigating cybersecurity risks. Similarly, this layer involves three steps: (1) risk identification, (2) risk quantification, and (3) cyber investment analysis. The risk identification step focuses on identifying potential cybersecurity threats, vulnerabilities, and attacks. The risk quantification step focuses on quantifying the magnitude and frequencies of cyberattacks and prioritizing attack types. The cyber investment cost analysis step focuses on analyzing cyber investment cost-benefit and making investment decisions in the cyber infrastructure.

3.3.1 Risk Identification

Identifying cyber risks requires understanding the preferred approaches intruders and hackers take. Taxonomies of cyber risk represent the prior knowledge that the organization has regarding the types of assets to be protected, and also the type of vulnerabilities and threats (Rea-Guaman et al., 2020). The taxonomies corresponding to assets, cybersecurity vulnerabilities, and cybersecurity threats need to be established and updated by the organization over time to facilitate risk identification (Rea-Guaman et al., 2020). The organization must be aware of the importance of establishing and maintaining updated taxonomies to address the ever-changing cybersecurity environment and ongoing or periodic cyber risk identification.

Esteves, Ramalho, and De Haro (2017) suggested two stages typical hackers take: exploration and exploitation. During the initial stage of an attack, hackers typically take on an exploration that combines deliberate and intuitive thinking and relies on intensive experimentation. Once

access to a system is gained, hackers depend on exploitation to achieve their goals. On the other hand, the Cyber Kill Chain® framework classified cyberattacks into seven stages (Lockheed Martin, 2009). Each of the seven stages from 'reconnaissance' to 'act on objective' present unique threats and vulnerability. Every intruder and hacker exploit vulnerabilities of an applicable asset type and launch attacks. For the cyber risk assessment, risk identification requires two major activities: (1) identify the types of assets to be protected and the type of vulnerabilities and threats from external actors, and (2) identify the types of assets to be protected and the type of vulnerabilities and threats from internal actors. To facilitate reader's understanding, imagine that an organization identified major cyber vulnerabilities and threats regarding network servers and email systems arising from external hackers and cyber vulnerabilities and threats related to laptop/desktop mishandling arising from internal users.

3.3.2 Risk Quantification

Risk quantification is being increasingly adopted in most industry sectors (Allodi & Massacci, 2017). Risk quantification is a critical step toward a more efficient allocation of resources and a more secure overall environment (Chen, Kataria, & Krishnan, 2011). Risk quantification requires measuring frequencies of cyberattack types, magnitude of consequences of cyber breaches arising from the attacks, and prioritizing cyberattacks using a risk matrix. Keeping track of the frequencies of cyber breaches and the number of individuals/financial losses affected helps an organization quantify the risk in the future.

Cyberattacks arrive in certain probability distributions. For example, cyberattacks can be modeled as a random process of arrival with a Poisson probability density function which is

commonly used for a variety of arrival applications (Kuypers & Maillart, 2018). Hence, the expected arrival rate of cyberattacks per period is an essential parameter in quantifying the frequency of a certain cyberattack type. An organization may also identify how the frequency of cyberattacks changes over time from their cybersecurity monitoring system and use the trend data to continuously adjust their cybersecurity action plans.

Risk quantification involves estimating the cost associated with different attack types and breach scenarios. The cost of a cyber breach for the individual or organization responsible is dependent upon three things: (1) statutory fines, (2) cost of experts or lawyers needed to resolve the breach, and (3) value of the data released (Draper & Raymond, 2020). For a healthcare organization, negative consequences include ransomware payment, sending patients/customers to alternative sites for care services, reputation damage, government penalties and sanctions, and the costs of recovering data, replacing equipment, and implementing various security measures (Abraham, Chatterjee, & Sims, 2019). Risk quantification would require sophisticated and comprehensive analyses to determine frequencies of the different cyberattack types and the breach costs.

The construction of a cyber risk matrix facilitates risk quantification. The use of a cyber risk matrix helps the assessment team members facilitate the quantification process. The cyber risk matrix has two dimensions. One dimension is the frequency of cyberattack types per period and the other dimension is the expected financial loss per cyber breach. A cyber breach refers to a penetrated cyberattack as not all cyberattacks lead to cyber breaches. Through the analysis of the risk matrix, risk priority of attack-breach can be determined. In general, an attack type with a higher expected financial loss and more frequent cyberattacks and/or frequently penetrated

cyberattacks will have a higher priority. With modified real-world data, Figure 2 shows a cyber risk matrix of the three attack types. In this scenario and subsequent discussion, we assume that the decision horizons under consideration is one year. Depending on the decision horizon an organization chooses, a proper numeric adjustment may be needed for a shorter or longer decision horizon than one year. The dotted lines are drawn to divide a high, medium, and low risk area. The network server attack is in the high-risk area with 250 attacks per year and $20,000 of expected financial loss/per breach. Email is in the medium risk area with 100 attacks per year and $20,000 expected financial loss/per breach. Finally, laptop/desktop is in the on the border of the medium and low risk area with 100 attacks per year and $10,000 of expected financial loss/per breach.

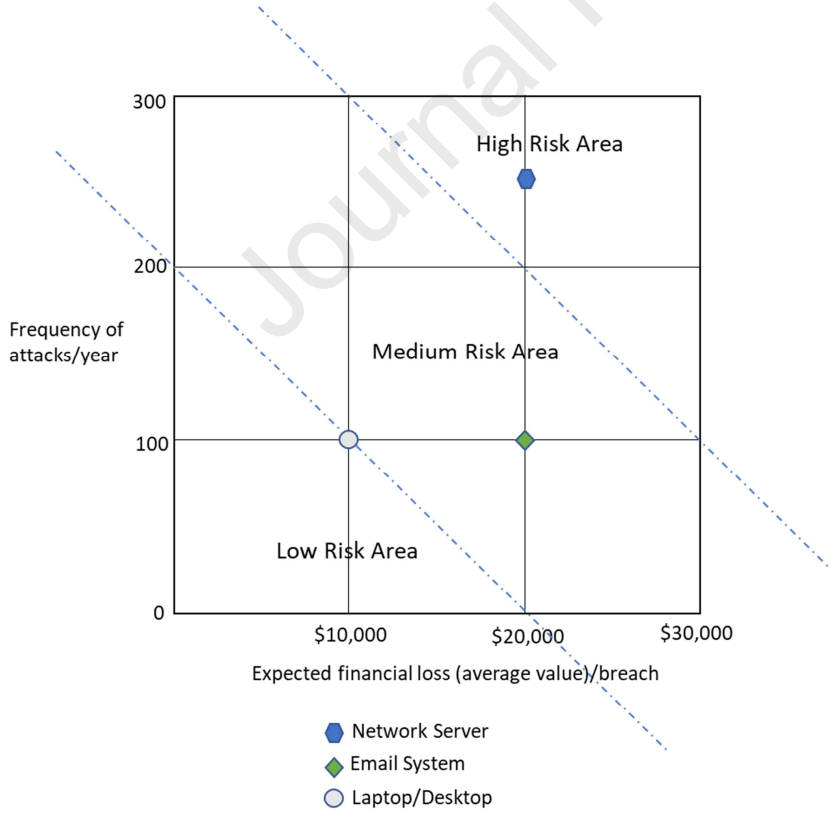

Figure 2. A Cyber Risk Matrix for Three Cyberattack Types

The second step in the risk quantification is to derive an expected financial loss function for each cyberattack type and for the entire cyberattack. The highest expected financial loss comes from the defense probability of zero from cyberattacks (i.e., all cyberattacks results in cyber breaches) and the lowest expected financial loss from the defense probability of 1.0. The expected financial loss of cyberattack type *i* at varying degree of defense probability, *r*, is given as:

$$FL_i = (f_i * l_i)(1 - r) \quad (1)$$

where f_i is an estimate of the frequency of cyberattack type, *i*, which is a constant, l_i is an estimate of the financial loss of each breach of cyberattack type, *i*, which is also a constant, and *r* is a defense probability. *r* depends on cybersecurity investment. It is assumed that the decision horizon is one year. Note that the estimate of the frequency of cyberattack is a constant and is independent of the defense probability, since the cyberattacks come from adversaries and are not under the organization's control. It is assumed that the organization achieves the target defense probability with certain cyber investment to reduce the number of penetrated attacks (i.e., realized cyber breaches). The cyber investment will be discussed in the next section. The number of penetrated cyberattacks is affected by the defense probability, r, and is $f_i * (1 - r)$.

The total expected financial loss of all cyberattacks at a defense probability, *r*, is given as:

$$TFL = \sum_{i=1}^{n} (f_i * l_i)(1 - r) \quad (2)$$

Continuing from the previous scenario, Figure 3 shows the linear relationship between the expected financial loss from cyberattack types and the defense probability. According to Equation (1), the network server's expected financial loss is $5 million per year when the

defense probability is zero. i.e., (250*$20,000)*(1-0.0). The network server's expected financial loss is $2.5 million per year when the defense probability is 0.5. i.e., (250*$20,000)*(1-0.5). The total expected financial loss of all three cyberattack types is $8 million per year when the defense probability is zero. i.e., $1 million + $2 million + $5 million. The total expected financial loss of all three cyberattack types is $4 million per year when the defense probability is 0.5.

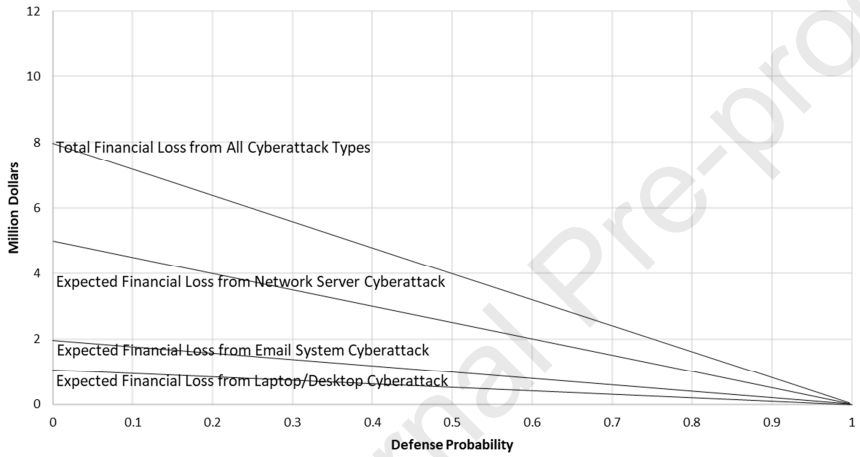

Figure 3. Relationship between Financial Loss from Cyberattack Types and Defense Probability

3.3.3 Cyber Investment Analysis

The financial losses that may happen due to cyberattacks and other information system failures in an organization can be prevented with investment in different security measures and purchase of data protection systems (Bojanc & Jerman-Blažič, 2008). A cyber investment cost analysis needs to take into account two opposing forces of the cybersecurity equation: cyber attackers and cyber defenders. In general, the stronger the cyber defense is, the more deflected the cyberattacks are, and vice versa. A cyber defense plan involves cost-benefit analyses of various

defense options. In this paper, *cyber investment cost* is defined as any money spent to enhance cybersecurity within a given period with the expectation of certain benefits. The cyber investment cost analysis uses a simple, but methodically sound technique for practitioners. The output of the risk quantification, the quantified relationship between financial loss from cyberattack types and defense probability, becomes an input for the cyber investment cost analysis.

As in many other new IT projects, one of the barriers to the investment in cyber risk management is the difficulty in justifying the investment benefits due to a lack of proper analysis models and techniques. Without a good justification for investment, organizations may overlook opportunities to achieve significant benefits obtainable from cybersecurity investment. The cyber investment cost analysis aims to provide convincing financial justification to managers with quantification of tradeoffs between financial loss from cyber breaches and cyber investment cost. The goal of the cyber investment cost analysis is to minimize the total cost of both financial loss from cyber breaches (i.e., penetrated cyberattacks) and cyber investment cost for target cyber defense. The cyber investment analysis needs to take into account all three elements of the cyber infrastructure layer (organization, employees/internal users, and cyber technologies) in order to maximize the benefits of the investment. Traditional financial methods such as NPV, ROI, and payback methods can be easily integrated into the cyber investment cost analysis.

The objective function given as Equation (3) is to minimize the total cyber cost, *TC*. Cyber investment cost, *D*, is a function of the defense probability, *r*.

$$Min\ TC = D(r) + (1 - r)\sum_{i=1}^{n}(f_i * l_i) \quad (3)$$

The cyber defender's cyber investment influences the defense probability. The probability of the cyber defense is modeled as a binomial probability distribution (i.e., either success or no success). The number of successful cyber defense against attacks in a given period is f_i *r. The financial loss due to unsuccessful cyber defense at a given defense probability is the second term in Equation (3). The achievement of a successful defense probability requires a certain investment cost, *D*, which trades off the decrease of the financial loss.

Continuing the previous scenario, Figure 4 shows the tradeoff between the decrease of financial loss and the increase of cyber investment cost (and the increase of the defense probability). The horizontal axis represents the defense probability against cyberattacks from 0.0 to 1.0 and the vertical axis represents the financial loss and cyber investment cost over the varying defense probability. The linear financial loss curve represents the financial loss from cyber breaches due to unsuccessful defense. The total cost minimization is achieved at the point where the marginal increase of the cyber investment cost is equal to the marginal decrease of the financial loss. Therefore, the point of the minimum total cost depends on both the shape of the cyber investment cost curve and the shape of financial loss curve.

Figure 4 shows that when the defense probability is 0.0, the expected financial loss is $8,000,000 from cyber breaches. Assume that an organization is likely to receive 400 cyberattacks per year and each breach (which is not defended successfully) costs $20,000. A defense probability of 0.5

is equivalent to 200 breaches out of the 400 cyberattacks. The potential financial loss at a defense probability of 0.5 is $4 million per year (i.e., 0.5*400*$20,000). There is a wide range of positive net benefit between the defense probability of 0.28 and 0.99 in which the cyber investment is beneficial to the organization due to the greater decrease of financial loss compared to the cyber investment cost.

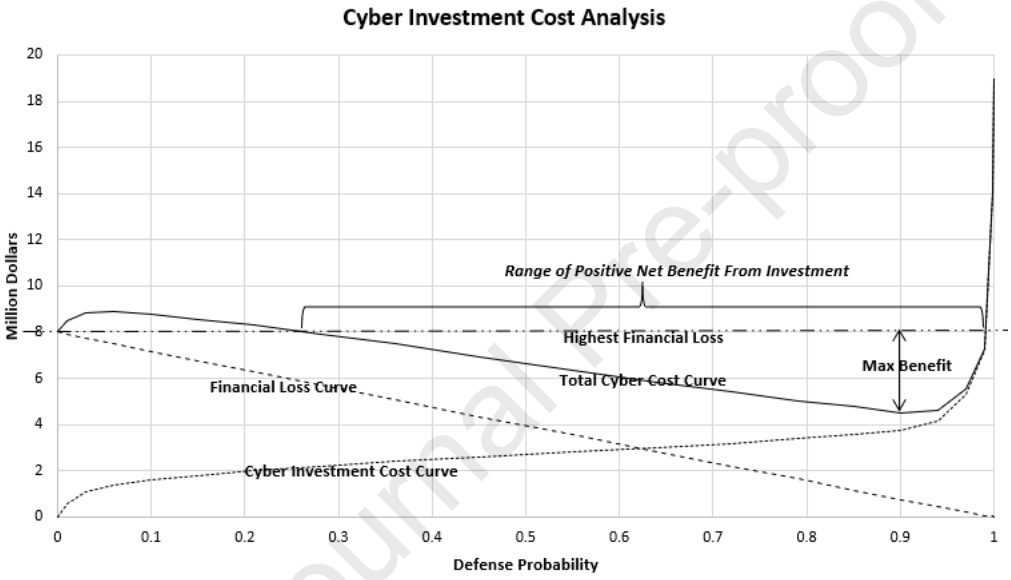

Figure 4. Cyber Investment Cost Analysis

In this cybersecurity scenario, the cyber investment curve is assumed to be s-shaped, which is a typical investment cost curve widely used for cost estimation of technology projects. The s-shaped function suggests that a rapid diminishing return occurs at the point of cyber investment cost beyond the defense probability of 0.99. While the minimum total cost occurs at the defense probability of 0.9, senior management may want to choose a higher defense probability of over 0.9 up to 0.99, if they are cyber risk averse.

3.3.4 Estimating Costs for Cyber Investment Analysis

Estimating costs is the basis of the cyber investment analysis. The specific cost function may vary by industries and scale of business operations. This section discusses general starting points for a manager to plot a rudimentary cost curve for their own situation. The IT asset owners (e.g., managers of network servers) should have a primary responsibility for estimating financial loss and the investment cost curve. Well-known expert judgement techniques such as three-point cost estimates (e.g., pessimistic, optimistic, and most likely) and a Delphi method may be used to facilitate the estimation process and derive more reliable and efficient estimates.

First, the IT asset owners need to identify different types of attacks to the asset and their potential financial losses such as penalties, compensations, replacement, upgrade, and reputation damages. When internal data about financial losses from cyber breaches do not exist, they may look for data from the industry or from similar organizations. Estimates of potential financial losses of different types of attacks on the asset are summed and the estimate of the average of the financial loss per breach for the asset is calculated. For example, a financial loss from cyber breaches arising from the attacks to the network servers must take into account all different types of cyberattacks to the network servers.

The average of the financial loss can be calculated by dividing the total financial loss of the various types of attacks to the network servers by the frequency of the attacks to the network servers. For example, the sum of the expected financial loss from ten attacks is $200,000. The average of the financial loss is $20,000 while different attack types may result in different amounts of financial loss. While this kind of estimation is rudimentary, it can reduce the problem

space and simplify the cost function development. A more precise approach with the use of occurrence probability of each attack type could be taken to derive the expected financial loss of a cyber breach to the network servers. This approach may be useful when certain attack types occur more frequently than other attack types.

Next, they need to plot the cyber investment costs for varying degrees of countermeasures against the cyber threats on the IT assets and services. Cyber investment costs are identified in various countermeasure activities such as policy development, tool development, training, monitoring and control activities. For a theoretical purpose, the previous section illustrated the continuous investment cost curve. However, in practice, the cyber investment cost curve may take a discrete cost curve and a specified defense probability range, not the entire range between 0 and 1. A good starting point for estimating cyber investment costs is the current cybersecurity expense level and defense performance for each IT asset and service. For example, the organization may have operated at the 90% defense probability with the cybersecurity expense of $200,000 for the network server operations. For future cyber investments, the organization may consider defense probabilities of 96%, 97%, 98%, 99% and estimate the corresponding investment costs.

3.4. Cyber Performance Layer

Once the investment decision is made at the cyber assessment layer, cyber performance activities follow. The cyber performance layer focuses on the actual development and operation of the cybersecurity systems based the performance goals set at the risk assessment layer. Three major

activities at the cyber performance layer are implementation, monitoring and control, and continuous improvement.

3.4.1 Implementation

Implementation of the cybersecurity include cyber technology development, testing, deployment, new policy development, training, and a user acceptance study. The new cyber infrastructure should build on the existing infrastructure of organizations, employees/internal users, and cyber technologies. A variety of security tools identified at the cyber ecosystem layer should be sourced for the implementation of the cyber technologies. Organizations also need to develop selection criteria to evaluate and choose among commercially available cyber technologies and vendors. The implementation activities must take into account ease, usability, and usefulness of monitoring and control systems.

3.4.2 Monitoring and Control

During the risk monitoring and control stage, the organization needs to monitor cyberattacks and respond to them timely. Prevention, detection, and recovery are the core activities and conducted concurrently. Detection activities focus on the real-time tracking of external cyberattacks, abnormal user activities, and illegal access to data and applications. Recovery activities deliver a solution in real time. Monitoring and control need to keep a log of types and sources of cyberattacks, frequencies and magnitude of the attacks in terms of penalty, lost sales, ransom paid, the amount of data stolen, and recovery for future cyber investment cost analysis.

3.4.3 Continuous Improvement

Continuous improvement uses data collected over time to discover trends of attacks and long-term performance. The continuous improvement activities need to establish the measurable goals and generate periodic performance reports. It is also important to prioritize key performance metrics for the continuous improvement. In order to establish performance goals of various security dimensions, the industry's and competitors' best practices can be benchmarked.

Continuous improvement allows organizations to improve and revise future cyber investment and cyber strategies according to changing patterns of cyber threats and financial losses. The industry data indicates this evolving nature of cyber threats. During 2018, there was a 350% increase in ransomware attacks, a 250% increase in spoofing or business email compromise attacks and a 70% increase in spear-phishing attacks in companies overall (Garrett, 2018). Identifying new cyber threat types and adversaries involved and updating the cyber risk matrix will shed light on the direction the cyber ecosystem is taking. Timing of the periodic performance evaluation depends on types of organizations and IT systems. For example, a more frequent periodic performance evaluation will be needed for organizations using the complex high-connectivity systems (e.g., hospitals, logistics services, transportation services, and smart factories).

4. Illustration of Continuous Improvement

As an illustration, Figure 5 shows the evolution of the risk profile over two-year periods with directed arrows. This risk matrix utilized real-world data with modification. For "Network Server" and "Email System" threats, both the frequency of attacks and the expected financial loss per breach increase. Email System moves from the medium risk area to the high-risk area.

"Laptop/Desktop" moves to the medium risk area. However, the frequency of attacks decreases and the expected financial loss per breach increases.

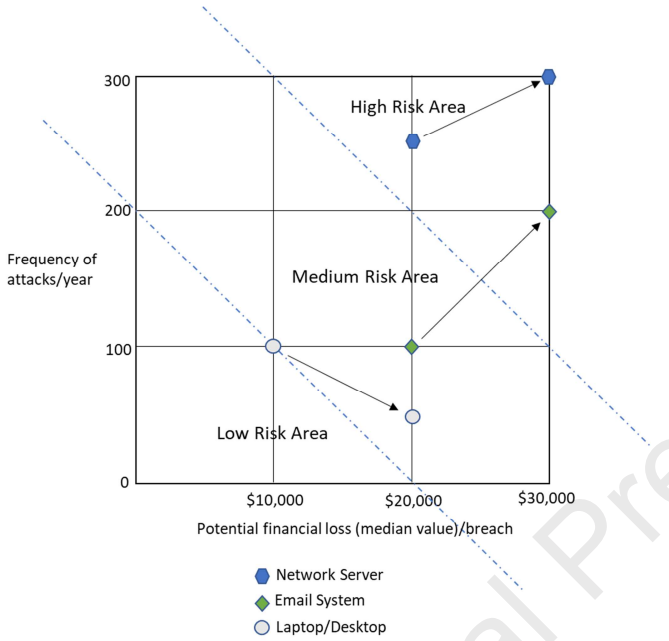

Figure 5. Evolution of Risk Profile over Two-Year Periods

Figure 6 shows the updated risk quantification. When the defense probability is 0%, the expected financial loss is $16,000,000 from cyber breaches. The financial loss curve is steeper than in Figure 4. Figure 6 show the maximum benefit shifted to the defense probability of 0.94 from the defense probability of 0.9, assuming the cyber investment cost curve is the same. The range of positive net benefit is between 0.1 and 0.998, which is wider than in Figure 4. The change of risk profile is highly likely across industries with frequent changes in the IT field, and timely periodic cyber risk assessment and continuous improvement will align the cyber investment with the cybersecurity needs.

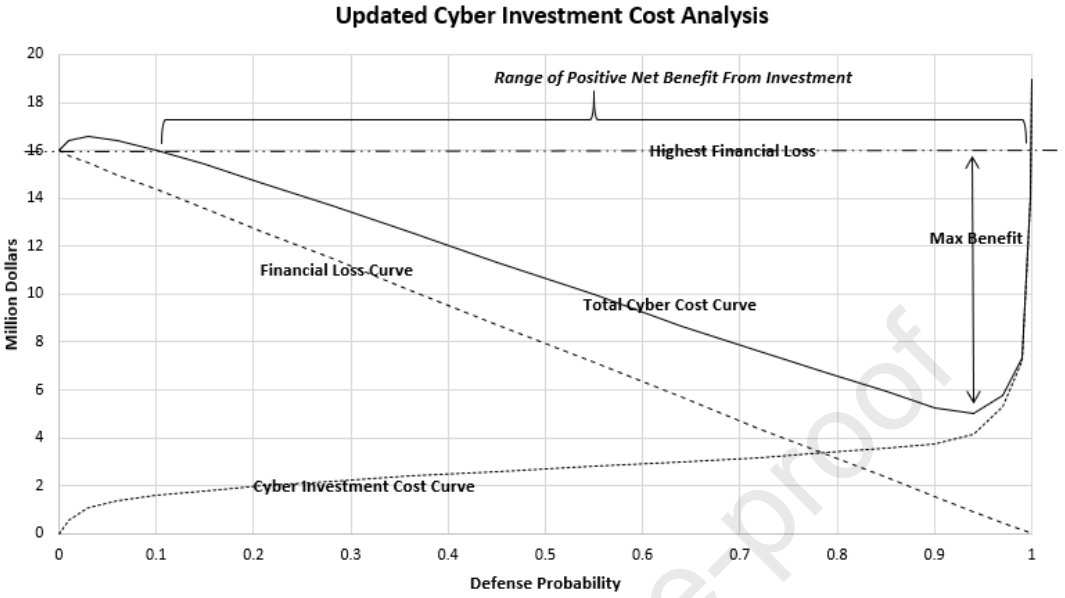

Figure 6. Updated Cyber Investment Cost Analysis

5. Conclusion

With the increased cybersecurity risks posed by cybercriminals and adversaries, it became imperative for organizations to increase their awareness of the change of the cybersecurity landscape and timely response to the change. This paper discussed cybersecurity trends coinciding with technological paradigm shifts. This paper also developed the Cyber Risk Management Framework in which risk management activities are organized and evaluated in four layers. As in many other IT projects, one of the barriers to the investment in cyber risk management is difficulty in measuring the benefits and costs of cybersecurity risk management. The organization is responsible for identifying the need for cyber acquisition and the best technology to meet that need. By prioritizing technologies that improve cybersecurity protection,

organizations can reduce the consequences of cybercrime and unlock future economic value as higher levels of trust encourage more business from customers (Accenture, 2019).

The basic tenet of the four-layer framework is that if we want to make a sound justifiable cyber investment to protect our IT assets and services from threats, we need to understand our external environment through the cyber ecosystem layer, evaluate the organization, employees/internal users, and existing cyber technologies through the cyber infrastructure layer, assess cyber risks through the cyber risk assessment layer, and conduct cybersecurity activities at the cyber performance layer. All the four layers are strongly intertwined and referenced to the cyber risk management framework, so that a holistic cyber risk management is achieved.

The cyber ecosystem layer is concerned with identifying and understanding the roles of its stakeholders under the organization's idiosyncratic cybersecurity environment. The cyber infrastructure layer is concerned with safeguarding IT assets and services of an organization. Organization, employees/internal users, and cyber technologies are the three key elements of the cyber infrastructure layer. The cyber risk assessment layer focuses on the identification of IT assets, cyber vulnerabilities, and cyber threats, risk quantification of cyberattack types, and investment analysis. Each cybersecurity breach can cause financial loss and conversely the prevention of it can generate a reduction of financial loss. Since an investment in the security technologies is a capital expenditure, the investment is likely to be under scrutiny of senior management for budget approval. The optimal investment comes at the point where the marginal increase of the cyber investment cost is equal to the marginal decrease of the financial loss. While it is not a trivial task, continuous improvement should be conducted to respond properly to the rapid development occurring in the cyber ecosystem.

To be better prepared for any emerging cyber threats, organizations need to analyze not only their own organizational cybersecurity risks, but also the industry-wide cybersecurity trends. While our discussion is limited to risk quantification, our framework can be expanded to the qualitative risk assessment (e.g., experts' opinion on cyber risk, nonfinancial strategic decision-making, and multi-criteria decision making), when quantitative historical data are not readily available. While the cyber investment decision uses cost minimization as an objective, it is also possible to combine popular traditional financial methods for project selection such as NPV, ROI, and payback methods in the process of a cyber investment decision. It is also worth mentioning that while this paper focuses on cyber risk management, cyber risk management is part of large organization risk management which involves non-cybersecurity organizational risk issues.

Acknowledgment

I offer special thanks to Associate Editor Dr. Jan Kietzmann and reviewers for their valuable comments and suggestions.

REFERENCES

Abraham, C., Chatterjee, D., & Sims, R.R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*. *62*(4), 539-548.

Accenture. (2019). Ninth Annual Cost of Cybercrime Study. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Allodi, L., & Massacci, F. (2017). Security Events and Vulnerability Data for Cybersecurity Risk Estimation. *Risk Analysis*. *37*(8), 1606-1627.

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*. *28*(5), 413-422.

Bloomberg.com. 2019. Capital One Says Breach Hit 100 Million Individuals in U.S. https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*. *35*(2), 397-422.

Choong, Y.Y., & Theofanos M. (2015) What 4,500+ People Can Tell You – Employees' Attitudes Toward Organizational Password Policy Do Matter. In: Tryfonas T., Askoxylakis I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2015 pp 299-310. Lecture Notes in Computer Science, vol 9190. Springer, Cham

Cusack, B., & Ghazizadeh, E. (2016). Evaluating single sign-on security failure in cloud services. *Business Horizons*. *59*(6), 605-614.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2016). Impacts of security climate on employees' sharing of security advice and troubleshooting: Empirical networks. *Business Horizons*. *59*(6), 571-584.

Draper, C., & Raymond, A.H. (2020). Building a risk model for data incidents: A guide to assist businesses in making ethical data decisions. *Business Horizons*. *63*(1), 9-16.

Esteves, J., Ramalho, E., & De Haro, G. (2017). To Improve Cybersecurity, Think Like a Hacker. *MIT SLOAN MANAGEMENT REVIEW*. *58*(3), 71-77.

eWEEK.com. (2019). Cloud Security Spending Set to Grow, Forrester Forecasts. https://www.eweek.com/security/cloud-security-spending-set-to-grow-forrester-forecasts

GDPR.eu. (2018). What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr/

Garrett, G. (2018). Cyberattacks Skyrocketed in 2018. Are you ready for 2019? IndustryWeek. https://www.industryweek.com/technology-and-iiot/article/22026828/cyberattacks-skyrocketed-in-2018-are-you-ready-for-2019

Gartner. (2020). Top 7 Security and Risk Trends for 2020. https://www.gartner.com/en/conferences/apac/security-risk-management-australia/gartner-insights/security-risk-trends

Hutchins, E.M., Cloppert, M.J., & Amin, R.M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

IDC. (2019). Worldwide Spending on Security Solutions Forecast to Reach $103.1 Billion in 2019, According to a New IDC Spending Guide. https://www.idc.com/getdoc.jsp?containerId=prUS44935119

ISO/IEC. (2012). ISO/IEC 27032:2012(en) Information technology - Security techniques - Guidelines for cybersecurity. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Kuypers, M, & Maillart, T. (2018). Designing Organizations for Cyber Security Resilience. *WEIS 2018*. https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2016/09/WEIS_2018_paper_50.pdf

Lee, I. (2019). The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet of Things*. Vol. 7, 100078.

Lezzi, M., Lazoi, M., & Corallo, A. (2019). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*. 103, 97-110.

Lockheed Martin. (2009). Cyber kill chain®. Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Accessed 13 Aug 2019

Mills, A.J., Watson, R.T., Pitt, L., & Kietzmann, J. (2016). Wearing safe: Physical and informational security in the age of the wearable device. *Business Horizons*. *59*(6), 615-622.

NIST. (2018). Framework Documents. https://www.nist.gov/cyberframework/framework

Rea-Guaman, A.M., Mejía, J., San Feliu, T., &Calvo-Manzano, J.A. (2020). AVARCIBER: a framework for assessing cybersecurity risks. *Cluster Computing*. https://doi.org/10.1007/s10586-019-03034-9

Shred-it. (2018), Security Tracker 2018. https://www.shredit.com/en-us/resource-center/original-research/security-tracker-2018

statista.com. (2020). Annual cyber security and cyber insurance spending worldwide from 2015 to 2020. https://www.statista.com/statistics/387868/it-cyber-securiy-budget/

U.S. Department of Health and Human Services. (1996). HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996. https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

U.S. Department of Health & Human Services. (2009). HITECH Act Enforcement Interim Final Rule. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html