International Journal of Management, IT & Engineering
Vol. 10 Issue 09, September 2020
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Cyber-risk management: identification, prevention, and mitigation techniques

Naveen Kunnathuvalappil Hariharan

Sr. Hyperion SME & Department of Information Technology, United States

Abstract

Cyber-attacks on critical infrastructure, as well as the possibility of cyber-terrorism and even cyber-warfare, pose a threat to societies on a larger scale. Stakeholders are vulnerable to information theft, service disruptions, privacy and identity theft, fraud, espionage and sabotage. This article provides a brief overview of risk management, with a particular emphasis on cyber security and cyber-risk assessment. This article provides an overview of risk management, with a particular emphasis on cyber security detection, prevention, and mitigation techniques. We showed how organizations could mitigate their cyber risk with careful management.

Keywords:*Cyber-risk, cyber security, Cyber risk identification, Cyber risk mitigation, Cyber risk prevention*

Introduction

Over the course of several decades, information and communication technologies (ICT) have provided tremendous benefits to businesses, individuals, and society as a whole. This is evident when we consider the internet's broad and profound impact on so many aspects of our daily life. The internet, and more broadly cyberspace, has evolved into a foundation for a wide range of services and activities that we now take for granted (Eling and Schnell 2016. People and businesses now have access to more and better services than ever before, thanks to cyberspace and its underlying infrastructure. Banking and finance, communication, entertainment, health, power supply, social relations, transportation, trade, and social engagement are some instances where this is true. As a result, the smooth operation of ICT is critical to our daily lives, fundamental rights, economy, and social security Gordon et al. 2003.

Simultaneously, cyberspace has introduced and continues to present a slew of new risks and flaws. Stakeholders are exposed to a wide range of cyber security incidents with varying degrees of severity. Information theft, service disruptions, privacy and identity theft, fraud, espionage, and sabotage are just a few examples Bouveret 2018. On a bigger scale, cyber-attacks on key infrastructure, as well as the prospect of cyber-terrorism and even cyber-warfare, pose a threat to societies Radanliev et al. 2018. In addition to the numerous opportunities for cyber-crime and harmful assaults, there are several non-malicious dangers that can result in cyber security breaches. Indeed, the pervasiveness of cyberspace has led to a situation where a huge number of hazards that we were previously exposed to in the physical world now exist in cyberspace and have become cyber-risks.

Due to its potentially disastrous consequences on organizational information systems, reputational risk, and the loss of consumer and stakeholder confidence, cyber risk is becoming an ever-growing concern to both public and private institutions. With the advent of the internet and the resulting proliferation of information technology, businesses, non-profit organizations, and government entities were generally unprepared to identify and address this risk. However, the threat has increased in frequency and intensity over time, and the nature of attacks has also altered (Biener et al. 2015). In many early cases, cyber-attackers and information-disruption campaigns disrupted business operations for no other reason than to amuse themselves or because they saw getting into a company's information technology (IT) infrastructure as a challenge. They would deface websites or takedown servers to irritate or simply challenge other cyber specialists to prove they could do it, not for financial gain. However, as the internet and e-commerce have developed, employee access to firm data has raised, and internal computer systems are increasingly accessible via remote access, cyber attackers have evolved, becoming more adept, and their impacts have gotten more destructive (Leuprecht et al. 2016)

Current cyber threats and attackers are increasingly focused on profiting from the repercussions of their attacks, either by exploiting the data, they illegally obtain for personal benefit or by requiring payments from the damaged organization to restore service, access, or website functionality.

Stakeholders must understand the nature of cyber risk and what distinguishes it from other types of risk to provide a suitable degree of cyber security, and they must have adequate methodologies and strategies for cyber-risk management McQueen et al. 2006.

Risk management

Essentially, a "risk" is the possibility that something will go wrong and cause injury or loss. A risk's seriousness is determined by its likelihood of occurrence and its consequences. The influence on an asset is the consequence, and an asset is a valuable object that we wish to protect.

Risk management entails a set of coordinated efforts aimed at directing and controlling an organization's risk exposure. A risk management framework should be used to ensure that a risk management process is adequate, efficient, and effective. This framework, in turn, should adhere to risk management's fundamental principles (Borghesi and Gaudenzi 2012.

The goals of the risk management process must be determined as part of the organization's overall management. This is why a risk management framework should be used to implement the risk management process in the firm. The framework establishes the risk management mission and commitment, as well as risk management policies and duties, risk management integration into organizational activities, and internal and external communication and reporting methods Arnold 2017. The risk management framework should be evaluated, reviewed, and enhanced on a regular basis. The risk management framework, in turn, must adhere to risk management's fundamental principles. The principles apply to all types of risk management, but companies must understand what they mean to them and how they apply to their own risk management framework Hunziker 2021).

Cyber-risk

Cyberspace is an interconnected network of computerized networks that include services, computer systems, embedding processors, and controllers, and also information in storage or transit. A cyber-system is one that operates in cyberspace Camillo 2017.

Information infrastructures, as well as people and other entities involved in the system's business processes and other behavior, are all examples of cyber-systems. As a result, most firms' cyber-systems are a component of their organizational structure. Furthermore, cyber-systems are becoming more and more common in society. Software systems and Internet connectivity are used by citizens, businesses, governments, and a variety of other stakeholders to provide and consume services. Welfare, health, finance, entertainment, social networks, trade, energy, transportation, and so on are examples of such services. Many of the vital systems that affect society as a whole, known as critical infrastructures, are also cyber-systems. Telecommunications, transportation, finance, power, water, and emergency services are examples of such infrastructures.

The protection of cyber-systems against cyber-threats is known as cyber security. The protection of cyber-systems against cyber-threats is known as cyber security.

Malicious or non-malicious cyber-threats are both possible. Denial of service (DoS) assaults and injection attacks, for example, are examples of harmful threats. Systems that crash due to code faults or loss of Internet connection owing to wear and tear of communication cables or other hardware are examples of non-malicious risks Kendrick 2010.

Importantly, what characterizes cyber security is not what we want to protect it from, but what we want to defend it from; it is characterized not by the types of assets to be secured but by the types of threats to assets.

Safety can be described as the preservation of life and health through the avoidance of physical harm caused by property or environmental damage. One of the most significant distinctions between safety and cyber security is that while safety focuses on system mishaps that may cause harm to the environment, cyber security focuses on threats that inflict harm through cyberspace. Another difference is that when it comes to safety, the assets evaluated are usually confined to the life of human, as well as environmental assets. However, when it comes to cyber security, the assets of concern can be anything that needs to be secured (Newsome 2013).

Cyber risk is a hazard brought on by a cyber threat. Cyberspace has a significant impact on the types and forms of threats and dangers that may arise, as well as risk management and risk assessment procedures and techniques Rohmeyer and Bayuk 2018. The potential for cyberspace to be extraordinarily far-reaching is one of its most striking features. This indicates that prospective threat sources could be located anywhere in the world but have the capability of causing damage deep within our concern's cyber-system. Another important consideration is that a significant portion of cyber-threats is malevolent; they are perpetrated by adversaries with specific goals and objectives. Non-malicious cyber-threats, on the other hand, exist.

Cyber risk is considered malicious if it is caused (at least in part) by a malicious threat and non-malicious otherwise. Importantly, some cyber-risks are both harmful and non-malicious under this definition. These are cyber-threats that can come from either a malicious or non-malicious source Antonucci 2017. Consider the case of illegal access to confidential information. A malicious cyber-risk is one that occurs as a result of a hacker, whereas a non-malicious cyber-risk is one that occurs as a result of data being accidentally posted on an open website. There are other situations that occur just as a result of the coexistence of malicious and non-malicious threats. An intrusion that happens when the intrusion detection and prevention system is down owing to an unintentional failure is an example of this Trim and Lee 2016. These are classified as harmful cyber-risks since they can't happen without a malicious threat.

Risk Identification Techniques

Because cyber-systems are computer-based, there is typically a wealth of data and information accessible from event logs, intrusion detection systems and other monitoring tools, vulnerability scanners, the results of penetration testing and other types of security assessments, source code inspections, and so on. We attempt to fully leverage such information when identifying risk. As a result, we conduct a thorough review of the target description, including the attack surface and assets, in order to discover any potentially useful information sources. These sources are mapped to the target's relevant part(s), which will be beneficial later in the risk analysis stage. This is generally performed in close collaboration with maintenance staff, technical managers, security managers, or those who are familiar with the technical infrastructure in depth. Any test findings relating to the metering terminal's Internet interface, for example, are mapped to this section of the attack surface. The results of these tests then assist us in identifying vulnerabilities and dangers to assaults via this interface Coburn et al. 2018.

It is important to recognize that while analyzing historical data like event logs, it is important to avoid assuming that tomorrow will be the same as yesterday. Even though a danger has not materialized in the past, this does not rule out the possibility that it will do so in the future. The absence of related events in the logs does not rule out a threat or occurrence from being evaluated. This is especially crucial to recognize in the case of rare but severe catastrophes, like a large-scale coordinated attack on the metering system. Likewise, just because a vulnerability isn't found by a security test doesn't mean it doesn't exist. We don't need to think about the severity of vulnerabilities or the possibility of threats and incidents while identifying risks; at this point, we just document everything that might be relevant and leave the deeper study for later.

We make sure to thoroughly assess whether there are portions of the target that require extra security testing, logging/monitoring, or other probing throughout the risk identification process, as well as later during the risk analysis. However, there is also a question of time and resources available. It also relies on whether the relevant data can be gathered through other sources.

In addition to the target-specific information sources mentioned above, open sources such as international standards, online repositories, and numerous studies on cybersecurity, threats, and vulnerabilities can provide useful input to risk identification Shetty et al. 2018. Our key challenge when utilizing such data is to determine the exact sources of relevance and to choose only those aspects that are relevant to our assessment from these sources. Here's an easy four-step process to follow Ruan 2017; (Antonucci 2017; Refsdal et al. 2015):

1. Establish relevance criteria depending on factors such as the sort of system or domain we are working with, the assets we are dealing with, or the type of risk we are dealing with. 2. Use the stated criteria to identify information sources. 3. Take only the elements from these sources that are relevant to our assessment. 4. Rephrase the selected elements, which must be expressed in broad terms by necessity, so that they apply precisely to our evaluation objective and assets.

Even when dealing with cyber-systems, extracting information not just from system logs, security tests, and other sources but also from people who are intimately familiar with the object of assessment from their unique perspectives is critical for risk identification. These individuals may include the creators of the central system or metering nodes, the central system's maintenance team and operators, the distribution system operator's information security officer and managers, and possibly some of their power customers, according to our evaluation (Nagaraju et al. 2017).

Although they may not be familiar with the specific target of the assessment, external experts may be able to provide basic information on typical threat sources, vulnerability and attack types, and trends. When communicating with external experts, we must, of course, take great care not to reveal confidential information unless the party on whose behalf we do the evaluation has given their approval.

Interviews may be used to collect information from people. Interviews might follow a rigid framework with all questions set in advance, or we can adopt an open style with major themes to be covered but a lot of room for the interviewee's additional contribution. The best option is frequently a hybrid strategy, in which we prepare questions but are prepared to follow up on unexpected but important subjects raised by the interviewee. Interviews can be quite useful, but they must be utilized with caution. Interviews, however, take a lot of time and effort, and they rely on the appropriate people being willing and available. The risk assessors must also be skilled in conducting interviews as well as organizing and aggregating data Coburn et al. 2018.

Questionnaires are another method for gathering information and knowledge from people. This is easier to plan than interviews because we don't have to agree on a date with the subject. On the negative side, we lose the ability to ask follow-up questions or clarify points. Furthermore, the subject has limited opportunities to expound on topics not addressed by the questionnaire, potentially resulting in the omission of critical information.

For risk identification, we can also employ brainstorming and other comparable strategies. In plenary meetings, key stakeholders and individuals with first-hand knowledge of specific areas or components of the goal are gathered to contribute to the identification process. This method has the advantage of allowing participants to discuss and follow up on each other's ideas. If one person, for example, discovers a weakness that no one else has considered, the rest of the group might brainstorm ways to exploit it. This has the potential to be highly effective if we can gather the appropriate folks.

Unfortunately, there are several disadvantages to brainstorming that we should be aware of. One is that the personalities of the participants are important, and there is a risk that the more outspoken individuals will dominate while others would barely contribute, resulting in a lack of diversity of viewpoints. Individual participants can also use this time to pursue their own agenda and focus solely on themes that are relevant to them. Other hazards include the possibility that the debate will veer off subject and that the limited time will not be distributed evenly among the issues to be discussed (Reuvid 2016).

As a result, a highly skilled risk assessor is required to lead the brainstorming sessions. It also necessitates that we anticipate ahead of time how we will structure and guide the discussion. Assets, threat source kinds, vulnerability types, or sections of the target description or attack surface can all be used to build the structure.

It is up to us how we organize the brainstorming, but it generally depends on the assessment aim, any participant preferences, and which step of the risk identification process we are working with. It may also be difficult to do on-the-fly documentation of the proceedings. As a result, we'll need to recruit a dedicated secretary to handle this task. We could use video or audio recordings if all participants agree, but we don't suggest it because it is likely to impede the participants. On a more practical level, getting all of the participants together for a brainstorming session can be tough.

The risk identification information sources and methodologies to utilize are determined by a number of factors, including available resources and information sources, as well as the type of target. For example, a suitable risk identification for a standard web application or service of a non-critical system can most likely be based to a great extent on general standards and libraries of cyber-threats and vulnerabilities. Risk identification, on the other hand, is far more difficult when dealing with a highly specialized critical system like the AMI Trim and Lee 2016. As a result, we attempt to combine methodologies in order to obtain a fuller picture and to confirm the results. If, for example, interviews reveal apprehension about the presence of specific vulnerabilities or the feasibility of assaults, vulnerability scanning, and security testing might help to alleviate the apprehension.

Cyber threat risk prevention techniques

If an enterprise's financial transaction over the internet is hijacked and dollars or information are taken, it may take a long time (if at all) for the theft to be discovered. Furthermore, the proceeds are unlikely to be recovered, and the thieves are unlikely to be captured. It is much better to avoid theft or cyber-crime in the first place, and the first line of defense is to purchase a good suite of security software from a reliable vendor that includes anti-spyware, adware detection, malware, and antivirus protection.

It's also necessary to have an automated update option, as well as an automated routine check of the system, and software patches should be loaded as soon as they become available. Obtaining assistance from advisers such as cyber risk insurers, lawyers, accountants, and risk managers is also a good business practice.

When it comes to internal money cyber theft, there are some basic best practices that businesses should implement to reduce the cyber risk associated with financial accounts, such as password-protecting checking accounts, accounts receivable checks, vendor and payroll checks, and credit card receipts Nagaraju et al. 2017. Because many cyber breaches go undiscovered for lengthy periods of time, extra measures such as segregating check writing and account reconciliation activities, as well as undertaking unannounced periodic audits of accounts payable and checks paid, can help avoid continuous cyber theft. Over a particular threshold, the company should impose a dual signature requirement for checks written out, as well as credit card spending limits on staff credit cards. As checks and fund transfers cannot be done in secret on a regular basis, this prevents (or mitigates) huge losses if a cyber-thief joins the system. Similar measures should be used to protect intellectual property and valuable information like databases, such as barring access or requiring verification to obtain copies, or keeping an automatic log of who has accessed a specific record or data set. Because businesses and non-profits do not have the same legal protection as individuals when it comes to cyber theft of bank accounts (the bank must reimburse the individual but not the company), proactive diligence is especially important for transactions involving financial transfers over the internet. While cyber theft insurance can provide a loss control mechanism against such risks, it usually comes with a deductible and so still carries the risk of a loss for the company Korstanje and E. 2016.

Furthermore, many cases of internal cyber (or just employee) theft may have been avoided if employees, potential employees (and even board members and trustees) had their criminal records checked. A refusal to agree to such checks should be regarded as a red signal. Employees (regardless of tenure) should also be subjected to a criminal history and credit check every five years or like, especially if they have access to financial accounts or check signing authority. Disgruntled personnel should be inspected more closely if they have access to critical information, as previously stated Kendrick 2010.

Encrypting signals at both ends of the communication channel, as well as higher-level authentication of identification before enabling access to cyber places with the potential for breach and data loss, are examples of further preventative methods. Before enabling access to accounts, certain banks, for example, will apply a secondary verification method each time. When attempting to log in to an account, the individual receives a text or email message containing a specific code that must be entered along with the password. Many types of unwanted access to company computer systems can be prevented using similar ways, preventing losses before they occur.

Cyber risk mitigation techniques

While not all risks may be avoided, the negative consequences can be reduced with careful planning. Risk management frameworks and methodologies that uncover information security vulnerabilities are commonly used by companies aiming to mitigate their cyber risk OECD 2017.

The organization (or a third party) conducts a security audit to identify risks and vulnerabilities in the company's systems as the first stage. This step normally entails looking over the physical computer environment for external dangers as well as looking over electronic networks (including offsite access by employees and customers). Companies also interview IT managers to acquire information on current risk profiles and determine the financial implications of the risk management process. Before consulting with insurers or security professionals, many businesses take the suggested steps to organize their own in-house response, such as setting up access controls and installing firewalls. Data encryption, which encrypts each document so that it cannot be read even if stolen or hijacked during mobile transmission, is a critical risk mitigation approach for businesses to use. Third parties will find it nearly impossible to attack databases or mobile devices if communication and/or documents are encrypted.

Encryption can be used in different ways. Encryption can be done on individual files or entire archives. Encryption comes in a variety of shapes and sizes. The private key cryptography method and public-key cryptography method are the most common ways of encryption. Encryption and decryption are both done using the same key in private key encryption Siegel et al. 2002. Private key algorithms are generally relatively fast and easy to implement in hardware. Hence they are often employed for bulk data encryption. Private Key encryption is primarily used to encrypt files, directories, and partitions that are only known by the data's owner. Stream ciphers algorithm and block ciphers algorithm are the two main types of private key algorithms.

A stream cipher encrypts each byte of data independently and is often used in wireless communications. Block ciphers, on the other hand, encrypt one block of data at a time and are mostly used for data encryption. In public-key cryptography, two distinct but related keys are used: a public key and a private key. Anyone can have access to the public key, and it's used to encrypt data intended for the private key's owner. The private key remains confidential and is used to decrypt data encrypted using the public key. Email messages, file attachments, digital signatures, and other transaction-related activities all require public-key cryptography. In order to avoid cyber danger, monitoring and detection are also essential Newsome 2013.

Many times, businesses are unaware of or respond insufficiently to a potential breach that could have been avoided. The performance rate of the affected firms would greatly improve if they implemented current monitoring and intrusion techniques to detect attacks or threats in real-time. Security consultants can assist in defining risk, detailing risk mitigation measures, estimating the financial ramifications of such risks, completing and monitoring risk audits, and identifying cyber vulnerabilities (as the environment is always changing).

Conclusion

Cyber-attacks on key infrastructure, as well as the prospect of cyber-terrorism and even cyber-warfare, pose a threat to societies. Cyber risk is becoming an ever-growing concern to both public and private institutions. This article provides a brief overview of risk management, with a focus on cyber security identification, prevention, and mitigation techniques.

The risk of cyber-systems being hacked exists, but it is critical not to fall into the trap of believing that tomorrow will be the same as yesterday. It's critical to remember this in the event of a rare but severe disaster, such as a large-scale coordinated attack on a metering system. Risk assessors must establish relevant criteria for the type of system or domain under consideration, as well as the type of risk. Interviews can be beneficial, but they should be used with caution. The best option is a hybrid strategy in which we prepare questions while also being prepared to follow up on subjects.

We can also use brainstorming and other similar strategies to identify risks. This method has the benefit of allowing participants to discuss and build on each other's ideas. However, there are a few drawbacks to brainstorming that we should be aware of. The personalities of the participants are important because the more outspoken individuals run the risk of dominating.

Businesses can prevent the risk of data loss by encrypting signals at both ends of the communication channel. Higher-level authentication of identification before enabling access to cyber places with the potential for breach and data loss is also a preventative method. Some banks will apply a secondary verification method each time an account is accessed. It is a type of encryption that encrypts each byte of data sent by an internet service provider (ISP) to prevent data from being intercepted.

Businesses can mitigate their cyber risk with careful planning. Data encryption, which encrypts each document so that it cannot be read even if stolen or hijacked, is a critical risk mitigation approach for businesses to use. Companies can also set up access controls and install firewalls before consulting with security professionals. Businesses are unaware of or respond insufficiently to a potential breach that could have been avoided. Security consultants can assist in defining risk, detailing risk mitigation measures, and estimating the financial ramifications of such risks. The performance rate of the affected firms would greatly improve if they implemented current monitoring and intrusion techniques.

Reference

Antonucci, Domenic. 2017. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. John Wiley & Sons.

Arnold, Rob. 2017. *Cybersecurity: A Business Solution: An Executive Perspective on Managing Cyber Risk*. Threat Sketch, LLC.

Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. 2015. "Insurability of Cyber Risk: An Empirical Analysis." *The Geneva Papers on Risk and Insurance - Issues and Practice* 40 (1): 131–58.

Borghesi, Antonio, and Barbara Gaudenzi. 2012. *Risk Management: How to Assess, Transfer and Communicate Critical Risks*. Springer Science & Business Media.

Bouveret, Antoine. 2018. *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. International Monetary Fund.

Camillo, Mark. 2017. "Cyber Risk and the Changing Role of Insurance." *Journal of Cyber Policy* 2 (1): 53–63.

Coburn, Andrew, Eireann Leverett, and Gordon Woo. 2018. *Solving Cyber Risk: Protecting Your Company and Society*. John Wiley & Sons.

Eling, Martin, and Werner Schnell. 2016. "What Do We Know About Cyber Risk and Cyber Risk Insurance?" *Journal of Risk Finance* 17 (5): 474–91.

Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. 2003. "A Framework for Using Insurance for Cyber-Risk Management." *Communications of the ACM* 46 (3): 81–85.

Hunziker, Stefan. 2021. *Enterprise Risk Management: Modern Approaches to Balancing Risk and Reward*. Springer Nature.

Kendrick, Rupert. 2010. *Cyber Risks for Business Professionals: A Management Guide*. IT Governance Ltd.

Korstanje, and Maximiliano E. 2016. *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities*. IGI Global.

Leuprecht, Christian, David B. Skillicorn, and Victoria E. Tait. 2016. "Beyond the Castle Model of Cyber-Risk and Cyber-Security." *Government Information Quarterly* 33 (2): 250–57.

McQueen, Miles A., Wayne F. Boyer, Mark A. Flynn, and George A. Beitel. 2006. "Time-to-Compromise Model for Cyber Risk Reduction Estimation." In *Quality of Protection*, 49–64. Springer US.

Nagaraju, Vidhyashree, Lance Fiondella, and Thierry Wandji. 2017. "A Survey of Fault and Attack Tree Modeling and Analysis for Cyber Risk Management." In *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, 1–6. ieeexplore.ieee.org.

Newsome, Bruce. 2013. *A Practical Introduction to Security and Risk Management*. SAGE Publications.

OECD. 2017. *Enhancing the Role of Insurance in Cyber Risk Management*. OECD Publishing.

Radanliev, Petar, David Charles De Roure, Razvan Nicolescu, Michael Huth, Rafael Mantilla Montalvo, Stacy Cannady, and Peter Burnap. 2018. "Future Developments in Cyber Risk Assessment for the Internet of Things." *Computers in Industry* 102 (November): 14–22.

Refsdal, Atle, Bjørnar Solhaug, and Ketil Stølen. 2015. "Cyber-Risk Management." In *Cyber-Risk Management*, edited by Atle Refsdal, Bjørnar Solhaug, and Ketil Stølen, 33–47. Cham: Springer

International Publishing.

Reuvid, Jonathan. 2016. *Managing Cybersecurity Risk: How Directors and Corporate Officers Can Protect Their Businesses*. Legend Press Ltd.

Rohmeyer, Paul, and Jennifer L. Bayuk. 2018. *Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions*. Apress.

Ruan, K. 2017. "Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk." *Computers & Security*. https://www.sciencedirect.com/science/article/pii/S0167404816301407.

Shetty, S., M. McShane, L. Zhang, and J. P. Kesan. 2018. "Reducing Informational Disadvantages to Improve Cyber Risk Management." *Geneva Papers on Risk and Insurance Theory*. https://link.springer.com/article/10.1057/s41288-018-0078-3.

Siegel, Carol A., Ty R. Sagalow, and Paul Serritella. 2002. "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security." In *Information Security Management Handbook, Volume 4*, 357–80. Auerbach Publications.

Trim, Peter, and Yang-Im Lee. 2016. *Cyber Security Management: A Governance, Risk and Compliance Framework*. Routledge.

IJMRA