Alexander Moore

CEG 6422

Vance Saunders

10/28/21

Understanding Cyber-Risk Management

A cyber risk is often considered “the risk of damage to an organization through its information systems” [10]. This is to say that it is the risk of any loss or disruption that may come to a person or organization as a result of a single or multiple failed cyber security systems. This loss can come in the form of monetary loss, data loss, or possibly both. Because this loss severely weakens organizations, costing some into the millions of dollars, a new method has been used to minimize the risk. “Cybersecurity risk management is an ongoing process of identifying, analyzing, evaluating, and addressing your organization’s cybersecurity threats.” [1]. In general, this management process is comprised of four steps: Planning, Assessing, Handling, and Monitoring. A large part of risk planning consists of risk and vulnerability identification and may consist of group meetings and brainstorming. “The risks facing you will always depend on what you are trying to protect … Then you will need to identify your vulnerabilities to the threats facing you” [2]. The goal of risk planning is to manage the risk proactively instead of reactively. Risk assessment involves identifying the most significant and likely risks to an asset and determining the impact of those risks. “This balance between impact and likelihood is at the heart of risk assessment” [2]. Additionally, it is useful to determine the risk control, or the degree to which the organization can change the outcome. If the risk control is low, it may be useful to spend the company’s resources elsewhere. Handling risks involves mitigating the risks that have already been identified and assessed in the previous steps. “There are two main categories of measures. Some risks can be mitigated with technological solutions, like having the latest equipment. Others can be mitigated with best practices” [2]. The final step, risk monitoring, is used to assess whether the predicted risks actually occur and to collect information that may be useful for future risk analysis and management.

The first, and one of the largest challenges facing organizations in their attempt to implement cyber risk management is that it is considered an issue for information technology specialists or the IT team. “IT can lead cybersecurity efforts, but cyber risk needs to be incorporated into the overall enterprise risk management framework” [4]. This means that all departments of the organization need to work together cooperatively in order to implement and execute the cyber risk management framework and have it be successful. This enterprise-wide management is best done when the people in leadership roles are also involved in integrating the framework. “It is the leadership of an organization, the C-Suite, which has the most influence on the behavior and culture of an organization” [4]. Adapting the overall behavior and culture of the organization to be more aware of cyber risks and managing them with the framework will help the organization with safer cyberspace navigation. The reason that this challenge has not been resolved yet is because most people working in miscellaneous departments at organizations don’t believe that cybersecurity is something that they need to worry about. Because they are not educated on the cyber threats that they may be vulnerable to, they simply think that their online safety is in the hands of the cybersecurity professionals. Instead, every single employee of an organization needs to be vigilant for cyber threats and should adopt the cyber risk management framework to help themselves and their organization as they navigate cyberspace.

The second challenge organizations face when attempting to integrate the cyber risk management framework is sharing the cybersecurity risk information. Just as the information needs to be shared with the people of all departments in the organization, it also “must be communicated to all the appropriate stakeholders, especially those involved in your company's decision-making. You need to make it clear to all appropriate parties the potential business impact of relevant cyber risks” [5]. Any parties that may be affected by the vulnerabilities in the organization’s cybersecurity should be aware of the potential risks. This includes constantly updating these parties as the risks increase, decrease, or change in general. If this challenge is not conquered, it could cause major failures to the immediate organization, as well as any of the affected third parties. The reason that this has not been resolved yet is similar in reasoning to the previous challenge; Most people consider cyber risks to be a concern of only the technology professionals, when instead it should be something communicated with all affected parties.

Another challenge that comes with the implementation of a cyber-risk management framework is that the details of the framework need to be established by the organization that is implementing it. Instead of a step-by-step guide for enabling the framework, the descriptive approach allows the organization to figure it out themselves. This can be a challenge for companies that don’t have experience with risk management frameworks and are unsure about how to enact such a plan. This challenge has not been resolved yet because this standard “is by design, since if the government had prescribed a set of cybersecurity practices, there would have been vigorous protests” [3]. This challenge impacts those organizations that are not experienced with integrating risk management, especially cyber risks. This means that, while some companies will be able to use the framework to navigate more safely through cyberspace, other companies may be left behind. Additionally, this challenge implies that the government will have less regulation over the safety of these organizations.

Yet another challenge of implementing the risk management framework is determining which risks are more important to consider than others. When considering the scope of an organization, there are many different types of risks that need to be assessed. For example, business risks could include compliance risk, financial risk, reputation risk, operational risk, and competition risk. Compliance risk suggests the difficulty business owners face when they “face an abundance of laws and regulations with which they need to comply” [6]. Financial risks consider the debts that a company may owe, or the possibility of monetary theft. Reputation risk is the “risk that an unhappy customer, product failure, negative press or lawsuit can adversely impact a company's brand reputation” [6]. Operational risk refers to a risk that could result in the impedance of internal company operations. Competition risk, otherwise known as comfort risk, is a result of “a company leader becoming so comfortable with their success and the status quo that they don't look for ways to pivot or make continual improvements” [6]. Those are just a few of the larger list of risks that a business must consider when integrating a risk management framework. Additionally, each of these general risk categories have specific possible risks within them. In total, there are likely well over one hundred different risks that must be considered. Therefore, it is important that the CEO and/or other executives are familiar with all the potential risks so that they can make the decision on which are most important to mitigate, and which can be disregarded as less important. This challenge has not been resolved because a large extent of risks are inherent to any business, and the number of risks only increase as the organization grows to include multiple departments.

The fifth challenge that comes with implementing a cyber risk management framework is that cyberspace is extremely complex and ever-changing. Complex systems are described by “circumstances in which relatively small differences in initial conditions or relatively small perturbations are associated with very large changes in the resulting patterns of behavior and/or strategic outcomes” [8]. Cyberspace is considered an ever-changing complex system because it is “thought of as a self-organizing social system: individuals, with little or no central oversight, perform simple tasks” yet the world has witnessed as “the Internet has grown exponentially with no visible end in sight as to its size or complexity” [8]. But this expansion is not only limited to the internet. Cyberspace consists of all interconnected technology, which includes physical electronics as well. “The blurring line between digital and physical domains indicates that nations and organizations will only be secure if they incorporate cybersecurity features, principles and frameworks are a necessity for all organizations, especially those with high-value assets.” [7]. The reason that this challenge has not been resolved and will almost certainly not be in the foreseeable future, is because of the monstrous growth that cyberspace has already undergone. Furthermore, the widespread use across the globe and the increasing speed at which it grows means that it is unlikely that it will stop, or even slow, any time soon. This only makes the challenge of managing risks more difficult as more threats will emerge.

A sixth challenge that comes with implementing cyber risk management is getting past the abundant number of laws and regulations that are set in place in an attempt to govern cyberspace. As a result of the ever-changing and complex cyberspace mentioned earlier, the government attempts to control it to the best of their ability. The more that cyberspace grows and changes, the more laws and regulations will be established to continue managing this cyberspace. Additionally, because “U.S. businesses and consumers have become increasingly reliant on computer technology, insurers and regulators are trying to catch up with the ensuing cyber-risks” [9]. Not only are the policymakers trying to keep up with the everchanging terrain of cyberspace, but the laws and regulations between different countries do not always match up. “Cyber adversaries do not stop at countries’ borders, nor do they comply with different jurisdictions.” [7]. On the other hand, organizations are required to adhere to those rules, and must modify their risk management assessments accordingly. While these regulations may make it safer to navigate cyberspace, it also makes keeping up with risk management more difficult. This challenge has not been resolved yet because of the exponential growth of cyberspace and the need of the government to regulate that. Because cyberspace is continuing to grow and the government will continue to grasp as much control as possible, this challenge is likely not going to be mitigated in the foreseeable future.

In the first video, Steve Culp presents his main suggestions and thoughts on businesses taking a risk-based approach to cyber security. The first point that he drives home is that not all segments of an organization hold the same value and attempting to construct a perfect solution for every aspect of the organization, especially a large one, is implausible. However, you still need a minimum threshold for the resources you spend on the technology, controls, and employee training since attackers will always find the weakest link. I choose to synopsize this point because it is one of the major key points to implementing risk management and executing risk assessment. Another point that he discusses is that the targets that companies often choose to focus on are misunderstood. I think that this point is very important because it makes sense to spend company resources on the assets that are most important. Finally, he mentions the fact that attackers are using social engineering to manipulate people to gain access. According to Culp, people are most often the failure point. I wanted to synopsize this point because it reveals that organizations need to increase their employee training when concerning cybersecurity and protection against malicious hackers/attackers.

The second video mostly follows the dialogue of Dr. Ronald Sugar, as he talks about managing cyber-risk and gives his point of view on risk management from the boardroom. The first point that Dr. Sugar mentions is that most board members likely did not even know what cybersecurity meant a decade ago, and while more have started to realize that it is important and that they could find severe trouble if they don’t address it seriously, most still do not have a firm understanding on the concept. I want to synopsize this point because it is fairly revealing as to how little the executives of companies are aware of cybersecurity. It shows that even the people in charge may need to be taught or trained so that the rest of the organization can integrate a culture of cybersecurity. Another point that Dr. Sugar brings up is that a board is responsible for managing risks within a tolerance that is appropriate for the shareholders of a company. I bring this point up because it reveals the power that the board has and the necessity that the board members should be knowledgeable about cyberspace and cyber risks. It also reveals to me that the board does what is in the best interest of the stockholders and the company, not necessarily themselves or other entities. The third point that Dr. Sugar mentions is that, while he puts trust in his security team, he knows that attacks will happen. He is more concerned about how quickly the response to the attacks will occur, and what processes and actions will take place to counter those attacks. Additionally, he uses each attack as an opportunity to learn and increase protections in the future. I want to synopsize this point because I like that he is realistic about the inevitability that attacks will happen but is more focused on how the team responds to those attacks, if they can mitigate the issues quickly, and if they learn from the experience so that the same attack hopefully does not occur again.

References

[1] Knowles, Mark. “Cybersecurity Risk Management: Frameworks, Plans, & Best Practices.” *Hyperproof*, 8 Sept. 2021, https://hyperproof.io/resource/cybersecurity-risk-management-process/.

[2] “DEMYSTIFYING THE CYBER RISK MANAGEMENT PROCESS.” *Cyberwatching.eu*, European Union’s Horizon 2020, https://cyberwatching.eu/demystifying-cyber-risk-management-process.

[3] Stroud, Andrea. “Improving Cybersecurity and the Challenge of Implementing the NIST Framework.” *APQC*, 27 Mar. 2015, https://www.apqc.org/blog/improving-cybersecurity-and-challenge-implementing-nist-framework.

[4] Riggi, John. “Why & How to Incorporate Cyber Risk Management Into Enterprise Risk Management.” *American Hospital Association*, https://www.aha.org/center/cybersecurity-and-risk-advisory-services/why-how-incorporate-cyber-risk-management-enterprise-risk-management.

[5] Hewitt, Kasey. “11 Considerations of Effective Cybersecurity Risk Management.” *SecurityScorecard*, 19 Aug. 2019, https://securityscorecard.com/blog/10-considerations-for-cybersecurity-risk-management.

[6] Boitnott, John. “Types of Business Risks to Plan For.” *American Express*, 6 Aug. 2021, https://www.americanexpress.com/en-us/business/trends-and-insights/articles/7-business-risks-every-business-should-plan-for/.

[7] Pipikaite, Algirde. “These Are the Top Cybersecurity Challenges of 2021.” *World Economic Forum*, 21 Jan. 2021, https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/.

[8] Phister, Paul W. “Cyberspace: The Ultimate Complex Adaptive System.” *DODCCRP*, The International C2 Journal, 9 Apr. 2010, http://www.dodccrp.org/files/IC2J\_v4n2\_03\_Phister.pdf.

[9] “Managing the Risks in Cyberspace.” *American Academy of Actuaries*, https://www.actuary.org/node/13793.

[10] Fasulo, Phoebe. “What Is Cyber Risk? Definition & Examples.” *SecurityScorecard*, 17 Mar. 2021, https://securityscorecard.com/blog/what-is-cyber-risk-definition-examples.