The Measure of a Successful CISO: Reliance on Frameworks and Planning

Eric K. Corpus

Old Dominion University

CYSE 200: Cybersecurity, Technology and Society

Ms. Hind Aldabagh

April 23, 2023

Abstract

Figure 1

#3 – 100% Secure

Note. Graphic of the comic strip *The Adventures of CISO Ed & Co.* from #3 – 100% Secure.

A CISO must rely upon frameworks and plans to ensure the security and resilience of an organization's information systems. Effective protections and prevention against threats doesn't happen by luck or chance. I believe that by implementing established cybersecurity frameworks, develop comprehensive risk management plans, and utilize predictive analytics, these processes can be effective in identifying and mitigating potential risks. These comic strips from Balbix see Figures 1 & 2, while humorous, capture a snapshot of the difficulties CISOs encounter. It is imperative that CISOs continuously evaluate and update these frameworks and plans to adapt to evolving cyber threats and business needs.

Figure 2

#25 - Going By Gut Feeling?

Note. Graphic of the comic strip *The Adventures of CISO Ed & Co.* from #3 – 100% Secure.

Cybersecurity Framework: A guide for overall cyber resiliency

On April 16, 2018, version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity was made available to the public. The novice to cybersecurity or a seasoned CISO will hear or has heard reference to the Framework time and again, so it begs the question, "What is the Framework?" Taken directly nist.gov website, it is defined as follows:

> "The Framework is a voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders."

Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013, directed the NIST to work to develop this framework. Matthew Barrett the credited author of version 1.1, emphasizes that the Framework is rooted in its "collaborative effort involving, industry, academia, and government" (Barrett, 2018). This thoughtful approach ended up being a comprehensive document that allows organizations, both big and small to implement cybersecurity to the level that best works for them.

The framework is globally recognized as well. Business' and/or organizations will be able to interact with not only international business partners but also confidently with international customers. The framework also provides a means for coordination at all levels of an organization. Whether at the Senior Executive level, the business/process level, or the implementation/operations level, the individuals working at these levels have the ability to focus on what's appropriate at their respective levels, they then can action what's appropriate at their level. An additional key factor with this framework is that it is "designed to complement existing business and cybersecurity operations" (Barrett, 2018). Organizations can significantly benefit from using this framework as it ultimately can "reduce and better manage cybersecurity risks" (Barrett, 2018).

If a CISO or any cybersecurity professional joins an organization, and they were not already implementing the framework or not education of the framework, there would be immediate benefits with incorporating the framework into its current cybersecurity practices. Taking the time to educate management that the framework is scalable to its specific needs as well as determining what's most important is a win-win for any business. It should be stressed that the framework must be revisited frequently and evolve as needed. There may be new threats or other reasons to evolve and improve. The five framework core functions which are Identify, Protect, Detect, Respond, and Recover should be implemented and reviewed frequently. Most CISOs should look to enact the seven steps to either establish or improve a cybersecurity program too. These seven steps result in an Action Plan that can be implemented for use in an effective cybersecurity program. From a business prospective, the most important takeaway that should be stressed to any employer is that the framework can help in determining how both time and money can be best spent in regards to cybersecurity. Any business owner or organization leader would appreciate any mechanism that results in success.

Physical and Logical Protections - Ensuring Availability

A critical measure for success of a CISO is his or her ability to ensure availability of systems and data 24/7 for customers. Leveraging the best practices and advancements is technology, a solid approach to address issues and bin efforts is to focus protections as either physical protections or logical protections. Physical protections encompass the things that can be physically touched. A CISO should take a holistic approach to the physical components of the network. This would include implementing redundant systems for the equipment that the network works off of. There could be additional switches, servers, firewalls, to name a few critical components. Ensuring power is maintained no matter the situation is another consideration as well. Critical components would require the utilization of UPS and other backup power solutions. An additional consideration would be to potentially have a secondary off-site that could be used if the primary site becomes unusable. Generally speaking, this secondary site

would be physically located well outside from where the primary site is. For example, if the primary site is in Florida and experiences a hurricane, the off-site may be located outside of the state. This secondary site could be used as a data backup and storage facility as well.

In terms of logical protections, backups should be done regularly and software should be kept current. This set alone will help greatly against known vulnerabilities and prevent against other exploits. If an organization utilizes a Security Operations Center, as part of the daily tasks is to monitor logs and events to detect any issues. This work can also be accomplished in a smaller scale with a SIEM, but this will require personnel trained to monitor and detect alerts. The other team that is assembled is an organization, Computer Security Incident Response Team (CSIRT). The SANS Institute publishes a 20-page handbook to lays out a structured 6-step plan for incident response. The steps include, Preparation, Identification, Containment, Eradication, Recovery, and Lessons learned ("SANS Incident Response Plan"). In concert with monitoring and detection, if there is any incident detected, incident handling procedures must be immediately executed. Ensuring that access to critical systems and data are by Authorized Users only which includes multi-factor identification is implemented is a significant logical protection to ensure is completed. It is critical to utilize multiple cybersecurity practices which will ensure there is minimal risk in the disruption of operations, access and availability. This physical and logical protection plan should be assessed regularly and increased as required. This measure of ensuring availability to data and systems is imperative of any CISO.

Predictive Knowledge: Creating an Effective Approach

As a CISO one of the key milestones is to develop an effective cyber-policy and infrastructure. A practical and proactive approach is needed. Typically, a CISO leads this development as well as the process to update it periodically or as required. In a blog post from SecurityScorecard, "A cybersecurity policy is a set of standardized practices and procedures designed to protect a business's network from threat activity" ("How to Design an Effective Cybersecurity Policy"). Risk management, collaboration,

resilience, culture, and adaptability must be prioritized. This means that managing risks, promoting awareness, building backup systems, and sharing responsibility for protecting critical infrastructure is imperative. Internal assessments and collaboration and information sharing with external partners are invaluable for identifying emerging threats and vulnerabilities. These steps to collaborate and partner share are cornerstones to significant advances in Cyber Threat Intelligence. This role within any organization is becoming more and more valuable. Cyber-policy and infrastructure must be flexible and adaptable to keep up with evolving threats. John Giordani Technology Risk Manager, Information Assurance & Cybersecurity Advisor writes, “Predictive analytics is the use of analyses that make predictions and projections about future events or trends to identify risks and better inform security protocols or defenses” (Giordani, 2022). By combining predictive knowledge with a proactive approach, a CISO can develop a strong cyber-policy and infrastructure that can withstand emerging cyber threats.

In Closing

The role and significance of a CISO continues to grow and become more vital each and every day as threats emerge. Ensuring the security and resilience is task number one for all CISOs. A successful CISO maintains a deep understanding of the frameworks and plans they helped develop and implement. They rely on established best practices and standards such as NIST, develop robust incident response plans and a highly effective CISO creates a cybersecurity culture across all levels of the organization. As threats evolve and continually seek out to damage to business and organization around the world, it is extremely important that a CISO stays current and adapts to every changing landscape of information security. A successful CISO will always be proactive, innovative, and maintain a solid grasp on the importance of frameworks and plans to safeguard their organization’s assets and systems.

References

Barrett, M. (2018, April 16). *Cybersecurity Framework v1.1*. National Institute of Standards and Technology. Retrieved from https://www.nist.gov/cyberframework/framework

Giordani, J. (2022, April 30). *How Predictive Analytics Could Change Cybersecurity*. LinkedIn. Retrieved from https://linkedin.com/pulse/how-predictive-analytics-could-change-cybersecurity-john-giordani?trk=articles_directory

How to Design an Effective Cybersecurity Policy. (2021, August 11). SecurityScorecard. Retrieved from https://securityscorecard.com/blog/cybersecurity-policy-examples

SANS Incident Response Plan. (n.d.). Cynet. Retrieved from https://cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth

#3 – 100% Secure. (n.d.). *The Adventures of CISO Ed & Co.* (n.d.). Balbix. Retrieved April 18, 2023, from https://www.balbix.com/ciso-ed

#25 – Going By Gut Feelings?. (n.d.). *The Adventures of CISO Ed & Co.* (n.d.). Balbix. Retrieved April 18, 2023, from https://www.balbix.com/ciso-ed