Facing Issues with Proper Cyber Policy

Robert Sullivan Timmons

School of Cybersecurity, Old Dominion University

CYSE300: Introduction to Cybersecurity

Dr. Joseph Kovacic

January 25th, 2023

In the digital age, with threats from seemingly every angle, organizations must have a cybersecurity policy. While creating a proper policy, there are many issues that need to be addressed. On top of covering all issues a corporation may face, cyber policy should be dynamic and scalable. This paper will cover five issues that should be tackled in a cybersecurity policy. The topics covered will include the classification of threats, the education of employees, data protection policies, and employee access privileges. The paper will conclude by addressing the upkeep of the cyber policy. Without a proper cyber policy covering key issues, a company will face countless threats.

Cyber policy should begin by defining and approaching threats concisely and efficiently. Outlined within a policy, there should be the organization's cyber requirements, risks, and needs. Lackluster policy breeds problems. The chief information security officer, or CISO, should take stock of company resources and decide what threats the company is most likely to face. As reported by Security Scorecard, "Teams should start with a cybersecurity risk assessment to identify the organization's vulnerabilities and areas of concern that are susceptible to a data breach." (Security Scorecard, 2021). Employee education should be emphasized within a policy as well. Insider threats and social engineering can easily destroy an organization from the inside. Proper employee training would include understanding the risks of free public Wi-Fi or leaving your computer unlocked while you step away. Training shouldn't be a one-and-done situation, instead, as reported by CNBC's Reinicke, "Training and awareness should be dynamic and ongoing to foster a company culture of good security practices." (Reinicke 2018) Outlining policy as well as educating employees are two firsts that must be tackled in a cyber security policy.

Another issue to tackle in cyber policy would be data protection. In traditional protection schemes, there is usually a disconnect between data protection and cybersecurity. Data protection revolves around protecting data in a system, while cybersecurity focuses on defending the system itself. Forbes writes "…cybersecurity covers safety against cyberattacks, while data protection covers a set of issues related to data storage, management, and access." (Forbes 2020). A separation of infrastructure leads to there being less standardization across the business and more resources dedicated to managing the two teams. Continuing into the article, Forbes explains "Having a single pane of glass ISMS allows you to control your data better than with separate infrastructure for data protection and cybersecurity." (Forbes 2020). Uniting these types of security through cyber policy causes fewer issues for information security teams down the line. Building upon this, implementing proper privileges within an organization is something a policy needs to address. Two of the best ways to go about privilege management is through the cybersecurity principles of least privilege and zero trust. The 'least privilege' principle as described by the National Institute of Standards and Technology, or NIST, is "The principle that a security architecture should be designed so that each entity is granted the minimum resources and authorizations that the entity needs to perform its function." (NIST 2023) Users are only granted enough information to complete their daily jobs and tasks, allowing sensitive data to be reserved only for those who need it. Zero trust architecture on the other hand "…mandates the creation of micro-perimeters of control…". (CPA, 2019). as Using both these principles in tandem reduces employee access to sensitive material as well as quarantines their actions, stopping potential insider threats or employee accidents.

The final issue that needs to be addressed in the cybersecurity policy is maintaining the policy itself. After outlining, drafting, and implementing policy, one of the largest hurdles, in the long run, is policy upkeep. With threats evolving, everchanging, and companies growing and shrinking, cyber policy should always be revisable and adaptable. To tackle this issue, every six months there would be a cyber evaluation, covering recent cyber threats to the organization, changes to the organization's physical or logistical structure, and a review of regulatory requirements. As the infosec institute aptly states "Cybersecurity policies should be living documents that grow and evolve with your organization." (Mallory 2020) Maintaining cyber policy should be one of the top priorities to be handled after implementation.

Cybersecurity is a complex subject, requiring policy authors to attempt to solve numerous issues. Addressing what issues a company has and organizing the cyber needs of the organization are paramount. With the organization's needs understood and documented in the policy, tackling employee education is the next step. The policy should clearly state that cyber safety is engrained into the company culture through dynamic education. Folding data protection and cybersecurity teams into one group should also be addressed in the policy, bringing greater efficiency and communication. Lastly, upkeep should be outlined in the cyber policy, making sure the business doesn't fall behind in the world of cyber threats. With threats from all around, one of the greatest counters to cyber threats is a well-rounded cyber policy that covers numerous issues.

REFERENCES

Security/Scorecard. (2021, August 11). *How to design an effective cybersecurity policy*. SecurityScorecard. Retrieved January 27, 2023, from https://securityscorecard.com/blog/cybersecurity-policy-examples

Csreinicke. (2018, June 21). *The biggest cybersecurity risk to US businesses is employee negligence, study says*. CNBC. Retrieved January 27, 2023, from https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html

Yec. (2021, December 10). *Council post: Why data protection and cybersecurity can't be separate functions*. Forbes. Retrieved January 27, 2023, from https://www.forbes.com/sites/theyec/2020/11/25/why-data-protection-and-cybersecurity-cant-be-separate-functions/?sh=3638e5b217cc

Direnpramodacumar. (2022, July 27). *Zero trust and least privilege: What a cybersecurity mindset looks like*. CPA Practice Advisor. Retrieved January 27, 2023, from https://www.cpapracticeadvisor.com/2019/02/06/zero-trust-and-least-privilege-what-a-cybersecurity-mindset-looks-like/

Editor, C. S. R. C. C. (2019, February 6). *Least privilege - glossary: CSRC*. CSRC Content Editor. Retrieved January 27, 2023, from https://csrc.nist.gov/glossary/term/least_privilege

Mallory, P. (2021, March 24). *Time to update your cybersecurity policy?* Infosec Resources. Retrieved January 27, 2023, from https://resources.infosecinstitute.com/topic/time-to-update-your-cybersecurity-policy/