Unit 4 Cybersecurity Policy Drafting

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**January 3, 2023**

**Part 1**

**What are the major considerations of organizational security policies?**

There is much at work when regarding cyber security policies. In today’s cybersecurity landscape, many factors could impact a business in an innumerable number of ways. Additionally, not every business runs the same way as each other. Because of this, cybersecurity policies have a few major considerations that serve as benchmarks for each policy and the business to be served by it. The National Institute of Standards and Technology outlines some key considerations in this matter; they are broken down into five categories (The National Institute of Standards and Technology, 2024). Firstly, come on the identify function details preliminary strategies and preventative measures to mitigate malicious actors. This function can detail many categories from asset management, to risk management strategies. This function is particularly important due to the initial strategy that may be provided from this policy’s outlook. A proper risk management strategy may ensure that employees understand exactly what is to be expected at all times. Additionally, further communication on the matter may serve to heighten a sense of cohesion for all employees serving within the business. Secondly, the Protect function details the security of a business’s network and the data contained there within. In the protect function employees are trained in order to identify potential risks in their daily job functions and routine maintenance is scheduled to ensure current and up to date security measures. Imperatively, this function details with employee behavioral mechanisms such as risks associated with an employee’s misunderstanding regarding the networks that they utilize throughout their job functions. Proper adherence to this policy function may mitigate the potential risk factors of malicious attacks such as phishing scams. As an organization is only a strong as each of their team members, a proper policy outline may bolster the individual strength of each member of the team to help them succeed on a greater level. The third function details the detection of security threats and potential malicious actors by way of network and physical anomalies. This key function helps root behavior as it is happening in the field. It may be easy for a business to be lost in the imperative nature of vulnerabilities, and as such a certain organization may be lost to the frantic nature of an event. Having a well-documented outline of how to act in such an event may bolster both response programs, and mitigate further disasters caused by disorganization. The fourth Function is attributed to actions of response. This can be the groundwork that is to be laid for a communications basis in the event of a security breach. During this function it is important to identify who needs what information, how often, and of what frequency. Finally, the recover function details planning on how employees in the business should act after an event has occurred. This function details the hindsight of the event, and how to streamline or improve the response going forward (The National Institute of Standards and Technology, 2024). These key functions are an important foothold to develop an effective cyber security strategy. Policies that utilize these outlines can serve to be more well-rounded and encompass a wide variety of topics that may serve as a vulnerability for other policy outlines.

**Create two possible policies regarding risk assessment and analysis.**

Policies drafted from the NIST Cybersecurity Framework (The National Institute of Standards and Technology, 2024).

Policy 1: Large-Scale Business

1. Security Categorization

The IT Department will be upheld to:

* Maintain security controls on physical and digital levels for confidential data as designated by system owners and executive personnel.
* Document security controls both physical and digital in a security plan to be reviewed by associated stakeholders with security control rationale and use-case.

1. Risk Assessment

The IT Department will be upheld to:

* Oversee or conduct a proper assessment of risk from logical factors malicious or otherwise related to proper use-cases of the organization and their materials.
* Document the Risk Assessment and the findings annually in respective organization.
* Review Risk Assessment findings with associated executive stakeholders minimum once per quarter, or when new potential security risks become known; whichever is soonest.
* Update the Risk Assessment regularly with new factors and disciplines that could impact the organization’s well-being.

1. Vulnerability Scanning

The IT Department will be upheld to:

* Employ vulnerability scanning tools and techniques to identify key factors such as software flaws, mis-aligned configurations, and back-end design philosophies that may provide additional vulnerabilities to the organization and its assets.
  + This scan should be done quarterly with documentation on the temporal data, and findings recorded to be reviewed by executive stakeholders.
* Report results of the vulnerability scan to associated executive stakeholders, and answer clarification information with insights and automation no less than 31 days after each scan is done.
* Action upon threatening vulnerabilities within 31 days of the stakeholder briefing.
* Employ regular system updates to handle security vulnerabilities that are highlighted in such briefings.
* Ensure security controls are upheld at each stage in the vulnerability scan, and that controls remain active throughout the lifetime of the organization.

Policy 2: Small-Scale Business

1. Security Categorization

The IT Department will be upheld to:

* Maintain security controls on physical and digital levels for confidential data as designated by the system owner, or chief security personnel.
* Document security controls both physical and digital in a security plan to be reviewed by associated stakeholders with security control rationale and use-case.
* Document learned disciplines while researching security threats while developing this action plan.

1. Risk Assessment

The IT Department will be upheld to:

* Utilize a third-part risk assessment to probe for risks associated to the business and its operations.
* Document the Risk Assessment and the findings annually in respective organization, or when new risks are identified.
* Review Risk Assessment findings with associated executive stakeholders or business management at minimum once per quarter, and when new potential security risks become known.
* Update the Risk Assessment regularly with new factors and disciplines that could impact the organization’s well-being.

1. Vulnerability Scanning

The IT Department will be upheld to:

* Employ vulnerability scanning tools and techniques to identify key factors such as software flaws, mis-aligned configurations, and back-end design philosophies that may provide additional vulnerabilities to the organization and its assets.
  + This scan should be done quarterly with documentation on the temporal data, and findings recorded to be reviewed by executive stakeholders.
  + Document design philosophies that contributed to vulnerabilities, and the rationale behind potential fixes. This fix is to be implemented no later than 31 days after the scan findings, at the discretion of security management.
* Report results of the vulnerability scan to associated executive stakeholders, and answer clarification information with insights and automation no less than 31 days after each scan is done.
* Action upon threatening vulnerabilities within 31 days of the stakeholder briefing.
* Employ regular system updates to handle security vulnerabilities that are highlighted in such briefings.
* Ensure security controls are upheld at each stage in the vulnerability scan, and that controls remain active throughout the lifetime of the organization.

**Part 2**

**What should the acceptable use policy cover and why?**

Many different acceptable use policies cover quite a number of topics today. In today’s digital landscape, existing tools have a myriad more different use cases thanks to the ingenuity of modern technology. However, this also invents new issues that may arise with Unintended use of those existing tools. Acceptable use policies cover these scenarios as best as they can. Content to go over in acceptable use policies may include the intended use case of a tool being covered in the policy, intended deviations of that use case regarding that tool, and other creative uses for the tool within reasonable and professional bounds that one could utilize (Brown University Office of Information Technology, 2021). It is important to cover these scenarios not only to manage risk in case of an accident, but also to help the user understand exactly how to engage with the organization and the tools that are provided. Additionally, it is important to go over acceptable deviations in tool usage in order to Accommodate alternate use factors that certain users may need in order to overcome more personal challenges. Utilizing intended use cases, and deviations, can provide a more inclusive and understanding atmosphere well keeping object manipulation within reasonable tolerances. This will reinforce the safety of the atmosphere within the organization to both personnel and assets alike.

**What types of information should be covered in a commercial organization’s data classification policy and why?**

A data classification policy may help an organization to keep bounds on how exactly the organizations data is shared, and how it is used. This further increases the safety of all of those that interact with the organization by proxy. To such an extent data classification policies are a helpful tool to keep actors in line with intended methods of thought. The type of information that should be covered in a commercial organization’s data classification policy may not be reasonable to include all data that an organization has access to but should reasonably include sensitive data, or data that may become sensitive given certain factors. Such data may include private information of users, information regarding to employees in payroll, important information relating to the organization’s associates, impossible monetary investment portfolios (The University of Kansas, January). It may be quite difficult to cover commercial organizations data classifications correctly, but with the cybersecurity landscape of today informational security is more important than ever. A leak of the wrong information can completely devastate an organization with no way to recuperate. Not only is a monetary cost of such a situation intense, but it may also cost an organization a great amount of opportunities in the future. Additionally, having all of this information documented in a policy—rather than just having executive personnel ensure that they will classify data correctly—upholds certain standards for send security personnel along with documentation to keep further transparency throughout the organization. This transparency helps bolster organization, and will ensure that each and every employee remains on the same page to mitigate risks of nonconformance.

**What are some effective ways to get user buy-in of security policies?**

The effectiveness of cybersecurity policies is only as good as the conformity of users. A well drafted cybersecurity policy may be useless if no one adheres to it. Because of this, user-buy in is incredibly important to the longevity of a policy and the organization that it serves. One way to boast user conformity would be education (Biros, 2016). Disseminating information regarding the policy, and why it is important to adhere to may further increase enthusiasm towards the policy, and thus the users that conform to it. Should users understand exactly how a policy may solve certain issues that may run rampant in the cybersecurity landscape of today, they may be more likely to adhere to the policy that they can trust. Another way to ensure users follow a policy would be motivational incentive (Biros, 2016). Should a policy be attributed to an organization with employees, certain incentives may be leveraged in order to ensure employee compliance. Reports, reviews, and talks may all be effective strategies to ensure that employees remain vigilant about a policy with regards to their daily job functions. With these strategies in mind, there is no one single way to ensure that individuals stick to a policy as it is outlined. A careful eye must be kept to ensure that employees are properly adhering to policies and understanding must be measured to ensure that issues with the policy are dealt with as they arrive.

# **References**

Biros, D. S. (2016, July). *Motivating Employees to Comply with Information Security Policies*. Retrieved from Journal of the Midwest Association for Information Systems: https://www.metrostate.edu/sites/default/files/2022-03/V2I2.A1.pdf

Brown University Office of Information Technology. (2021, July 18). *Acceptable Use of Information Technology Resources Policy*. Retrieved from Brown University Policies: https://policy.brown.edu/policy/acceptable-use-it-resources

The National Institute of Standards and Technology. (2024, February 17). *Policy Template Guide*. Retrieved from The NIST Cybersecurity Framework: https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/img/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online.pdf

The University of Kansas. (January, 26 2022). *Data Classification Handling Procedures Guide*. Retrieved from Kansas University Policy Library: https://policy.ku.edu/IT/data-classification-handling-procedures