Old Dominion University

School of Cybersecurity

Five Important Issues for Every Information Security Policy

Kerina Drummond

Introduction to Cybersecurity, CYSE 300

Malik Gladden

September 15, 2024

What do passwords, face Id, and fingerprint recognition all have in common? They are all forms of security. According to Merriam-Webster, security is “the quality or state of being secure or being free from danger, safety,” (Merriam-Webster, 2019). Security can mean a plethora of things to different people, but all can agree it is vital in our day-to-day lives. With our deep emergence into the world of technology it is crucial that we secure our systems but more importantly our information. Most people do not realize how much personally identifiable information (PII) is stored in our devices, and if that information gets into the wrong hands, it can leave any one person or organization vulnerable any range of malicious attacks from identity theft to fraud. To combat this horrible scenario most businesses create an information security policy (ISP).

An information security policy (ISP) is a “a set of rules, guidelines, and procedures that outline how an organization should manage, protect, and distribute its information assets,” (HackerOne, 2024).” These polices are created to protect a business' data confidentiality, integrality, and availability (C-I-A). For a business to run at optimal levels these three components must be protected. An information security policy will aid in breach prevention and prevent any of the (C-I-A) elements from being compromised. An information security policy should cover a list of policies all authorized team members and external parties are required to follow targeted toward protection of sensitive information a company holds. A few critical issues that should be covered in every ISP include data classification levels, security awareness, data backup, authorization and accessibility, and a clean desk policy.

Organization's data is extremely vital to the business's success and reputation. To ensure only authorized members access data an ISP should include data classification levels where data is ranked from least sensitive and where a low rank member can access files to most sensitive. The ranking should be based on document contents and the damage that can be done to a company if the information were to be breached. Our U.S. government, on the federal level, uses Top secret, Secret, and Confidential to classify government secrets (Kim & Solomon, 2023 pg.# 42). Top secret being the most sensitive and Confidential being the least. Although a business's secrets may not have the ability to destroy a nation, using the same structure or altered version of data classification can protect an organization's data.

To protect an organization from internal and external threats, security awareness training for all employees needs to be included in the ISP. To protect from and prevent Cyber-attacks an organization must inform employees ways to avoid creating a vulnerability in the system. According to Mimecast, "Research suggests that human error is involved in more than 90% of security breaches (Mimecast, 2022)," to reduce the possibility a breach can happen from human error, employees needed to be retrained periodically to keep up with new threats. The training must also align with company policies to target company specific risks as well. For example, a organization with a receptionist needs to be aware of social engineering to ensure they do not let anyone without proper authorization in, while a simple remote job without a physical location will not have this specific problem.

Data backup for obvious reasons needs to be included in an information security policy to ensure important information remains available at all times. In case of a breach, natural disaster, or a system failure, data backup satisfies the availability requirement of the C-I-A triad. Backup

must be done regularly to ensure files are up to date. Storage locations and roles of those involved in the back up process should be included in policy (Harvey, 2020).

Fighting unauthorized users from entering a system is a difficult, 24/7 task, which is why a policy specifically designed for authorization and accessibility is important. Who a company has in their system is important to keep track of, especially for large corporations that may have 200 or more people under their supervision, to keep unauthorized users from accessing vital company secrets. The policy needs to include protocols of identification based on a company's systems. For example, if a company uses keycards, they need name, employee card number, a log of swipe ins and swipe outs, what computer was accessed, what level clearance this employee has, and a photo that is updated periodically for second step verification.

Finally, a clean desk policy should be included in an ISP to protect data as well as hardware. The clean desk policy should include procedures to properly discard physical documents, locking computers, logging off, etc. This policy should also require a literal clean desk, a space that is tidy and free from liquids, which can damage a computer or food that can lead to critters. Require use of a break room or require cups with lids. Simple procedures like this should be stressed to further reduce a breach or system failure from human error. A leak of sensitive information because a file was not shredded is an organizations nightmare.

In conclusion, there are many different policies a company can create and add to their ISP to fit their needs of prevention, and protection. Five important policies that should be in every ISP regardless of an entity are data classification levels, security awareness, data backup, authorization and accessibility, and a clean desk policy. An information security policy is vital to an organization to outline ways policies and procedures to follow to prevent attacks and failures. ISPs must have policies that abide by the C-I-A to ensure the functionality of an organization.

This policy is ever changing with the times and must be updated to match to continue ensuring the security of any entity.

References

HackerOne. (2024). *Information Security Policy: Examples & 11 Key Elements*. Www.hackerone.com. https://www.hackerone.com/knowledge-center/information-security-policy

Harvey, S. (2020, January 15). *15 Must-Have Information Security Policies I KirkpatrickPrice Resources*. KirkpatrickPrice Home. https://kirkpatrickprice.com/blog/15-must-have-information-security-policies/

Kim, D., & Solomon, M. (2023). *Fundamentals of information systems security* (4th ed.). Jones & Bartlett Learning.

Merriam-Webster. (2019). *Definition of SECURITY*. Merriam-Webster.com. https://www.merriam-webster.com/dictionary/security

Mimecast. (2022). *What is Security Awareness Training and Why is it Important? | Mimecast*. Www.mimecast.com. https://www.mimecast.com/content/what-is-security-awareness-training/