The 12 Principles of Information Security

Emily Kellogg

University of Advancing Technology

Training Plan

Principle 1: There Is No Such Thing as Absolute Security

This principle explains that security is never perfect, and no matter how secure something is, it still has vulnerabilities. “Given enough time, tools, skills, and inclination, a malicious person can break through any security measures” (Pearson, 2014).

Principle 1 could be achieved by an organization through the hiring of network administrators and a network security team to monitor the organization’s network. This way, if any malicious person(s) tries to compromise the network, the team will be there to defend it.

Network administrators and their team are very important because they are the backbone of security for organizations. Without them, there would not be anyone to monitor and secure the organization’s network and educate employees on computer safety.

Principle 2: The Three Security Goals are Confidentiality, Integrity, and Availability

Confidentiality, Integrity, and Availability, the CIA Triad:

Confidentiality means to prevent unauthorized access. Integrity means to keep data pure and unchanged. Availability means to keep data available for authorized use (Fenwick, 2012).

The CIA Triad could be implemented into an organization with the use of basic security measures like password-protected documents and folders, encryption, authorized users, and cloud syncing. Password-protected documents keep confidential information away from people who are not allowed to see it. Encryption makes data unreadable unless an authorized password is used. Authorized users are those with the privilege of viewing confidential information. Cloud syncing backs up data to different locations.

All the examples listed above are extremely important because without them, unauthorized users can view, manipulate, and delete confidential data. The CIA Triad is an important component of information security in an organization because it ensures that confidential data is protected, unchanged, and available only to authorized users.

Principle 3: Defense in Depth as Strategy

Layered security is “…implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response” (Pearson, 2014). Instead of securing one layer and leaving the others vulnerable, layered security overlaps and protects all layers.

Layered security could be carried out in an organization by creating multiple points of protection for a network rather than solely relying on one. For example, instead of a network administrator only installing a firewall, they could install multiple firewalls and an antivirus software.

Layered security is a need for any organization because each layer is protected by the next. This creates a sort of fail-safe, preventing total failure if one layer were to become compromised.

Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

This principle suggests that people are terrible at making security decisions on their own. “Examples include falling for scams and taking the easy way” (Fenwick, 2012). A great example of this is when employees receive suspicious emails and click on links/download attachments from them. Tip #3 in the *Top 10 Secure Computing Tips* says “phishing scams are a constant threat… cyber-criminals will attempt to trick you into divulging personal information…” (UC Berkeley, n.d.).

Principle 4 could be solved by educating employees on internet safety through a training course provided by the organization.

This principle is important to consider because networks are intertwined. If even one computer within the network gets compromised, the entire network becomes vulnerable. Hence why internet safety courses for employees are so important.

Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance

Functional requirements “…describe what a system should do” (Pearson, 2014). Assurance requirements “…describe how functional requirements should be implemented and tested” (Pearson, 2014). Take software development as an example. During the creation of software, the functional requirements describe how the software runs, while the assurance requirements ensure the security of the software.

Computer security could be implemented by the organization’s cybersecurity team. Cybersecurity professionals ensure that systems are secure and functioning how they are supposed to. It is important to have a strong sense of computer security in the workplace because without it, computers can malfunction, and the organization can be vulnerable to cyberattacks.

Principle 6: Security Through Obscurity Is Not an Answer

The incorrect idea that hiding the details of how software is secured makes it more secure. “The only problem is that if that secret ever gets out, the whole system is compromised” (Fenwick, 2012). This idea is very similar to what Coca-Cola does with their recipe. They believe that by telling very few people the recipe, the secret is safe from the public. But at any time, if that recipe gets released, their whole company can crumble.

One way to implement this idea into an organization is to have multiple methods of securing data. That way, if an attacker finds out one method, they cannot infiltrate the organization. For example, an organization could enable two-factor authentication for their employees’ company emails. Two-factor authentication requires the employee to input their password and a one-time verification code to access their account. This method disables attackers from accessing an account if they find out the password.

It is crucial for an organization not to operate under the idea that ambiguity creates security because it is so easy for confidential information to get out. It’s better to be safe than sorry.

Principle 7: Security = Risk Management

“Effective risk management means attempting to control, as much as possible, future outcomes by acting proactively rather than reactively” (Corporate Finance Institute, n.d.). Instead of waiting for the worst thing to happen, its important to eliminate the possibility of it occurring.

This principle can be applied to an organization through the proactive use of risk management; planning, organization, cost control, and budgeting (Corporate Finance Institute, n.d.). For example, it would not make sense for a mid-sized organization to spend $2 million on all its tech assets but spend nothing to protect the assets. Rather, the organization should mitigate the risk of its tech assets being compromised by buying insurance and security.

Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive

“…a security mechanism serves a purpose by preventing a compromise, detecting that a compromise or compromise attempt is underway, or responding to a compromise while it’s happening or after it has been discovered” (Pearson, 2014). Like the CIA Triad, this principle indicates that prevention, detection, and response are all important aspects of security that should be used collectively within an organization.

Prevention, detection, and response can be applied to an organization by using antivirus software on workplace computers. If used correctly, Antivirus software can successfully prevent, detect, and respond to compromises along with the organization’s cybersecurity team.

Prevention, detection, and response are vital aspects of an organization’s computer security because without proper security measures, organization’s risk losing assets and time.

Principle 9: Complexity Is the Enemy of Security

Although complex systems seem like a great concept, the more complex something is, the less simple it is to secure. For example, say a company requires workers to use multiple applications at the same time while remaining logged into all of them. This makes it difficult for the security team to ensure the ultimate protection for every application at once.

An organization could minimize the complexity of its system by reducing the amount of data centers it uses and moving its data to the cloud (Baldwin, 2015).

It is important for an organization to have a less-complex system because it makes the system more productive, it costs less, and it makes the process of securing the system smoother.

Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security

Essentially, scaring a company into buying security has become an immature tactic for information security teams. The best way to get management to invest in better security is to explain why it is needed and how vital it is.

One way this principle could be used: the IS team could create a PowerPoint to educate management on the importance of new technology and how said technology could benefit the organization.

With how far the IT world has come, using scare tactics to get management to spend money on new technology is seen as immature and pointless as it does not place importance on new technology or educate management. That is why taking the time to educate and inform management is crucial to the success of IT.

Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

What this means is that by themselves, people, processes, and technology can all fail, but together they are successful. “For example, it takes a person to install and configure (processes) a firewall (technology)” (Fenwick, 2012).

An organization’s IT department is a great example of how the triad could be used in the workplace. Through the hiring of information security, network administration, and other IT professionals, an organization ensures that processes and technology are put in place, followed, and monitored. Therefore, the triad is successfully balanced and carried out.

This triad is so important because on their own, each of the three aspects are subject to failure. People can make the wrong decisions, processes can be ignored without controls put in place, and technology can become vulnerable or fail.

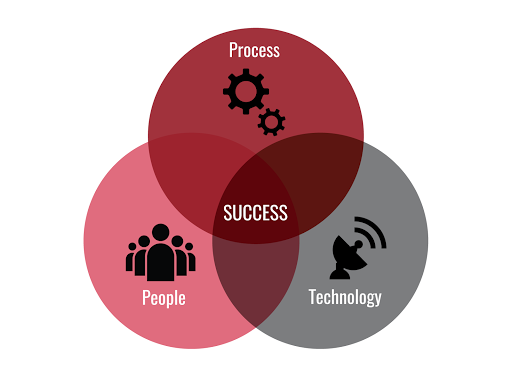


Figure 1. The people, process, technology triad

Principle 12: Open Disclosure of Vulnerabilities is Good for Security!

Principle 6 tells us that security through obscurity is not an answer. In fact, not disclosing a vulnerability to workers leads to a false sense of security (Pearson, 2014).

As an example, say an organization’s IT department finds a new vulnerability in the system that affects the workplace email application. Instead of keeping the vulnerability a secret among the IT department, they could hold a meeting with management and employees to discuss the vulnerability and an action plan.

It is important to be open with employees and management about a new vulnerability or possible attack because everyone has the right to know about something that affects them. Even if they cannot do anything about it in the moment.

# Bibliography

Corporate Finance Institute. (n.d.). *What Is Risk Management?* Retrieved from Corporate Finance Institute: https://corporatefinanceinstitute.com/resources/knowledge/strategy/risk-management/

Fenwick, T. (2012, March 19). *Twelve Information Security Principles of Success*. Retrieved from Ezine Articles: https://ezinearticles.com/?Twelve-Information-Security-Principles-of-Success&id=8846855

Pearson. (2014, July 4). *Information Security Principles of Success*. Retrieved from Pearson IT Certification: https://www.pearsonitcertification.com/articles/article.aspx?p=2218577&seqNum=2

UC Berkeley. (n.d.). *Top 10 Securing Computing Tips*. Retrieved from Berkeley Information Security Office: https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips

Dolfing, H. (2020). [People, process, technology triad]. People, Process, Technology (In Exactly That Order!). Retrieved from https://www.henricodolfing.com/2020/05/people-process-technology-in-exactly.html.