Principles of IS

Emilio Cress

University of Advancing Technology

NTS201-Security Essentials

Professor Mason Galatas

March 16th, 2021

**Principle 1: There is no such thing as absolute security.**

Now this may come as a shock to some, but to believe that anything is completely impenetrable is a fool’s folly (image 1 in references). If someone is dedicated enough, no amount of security measures, passwords and usernames, or encryption can stop them from their goal. But that is not to say that we cannot be as secure as possible. Consider for example this department has the latest state of the art security system, but an administrator mistakenly clicks on a bad link, then everything is compromised. One slip up is all it takes, so to take this principle to heart does not mean “if we are never secure, what is the point of trying” it is quite the opposite. If we are never secure let us do our best to make it as hard as possible for threats to compromise us.

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

In a perfect world, our data would be protected from those who would steal it, our data verified and pure, and our data available to those who should need it. It is not a perfect world however, but that should not mean a perfect world is not the aim. If we were to have a folder filled with private user information, we would want to keep that out of the hands of competitors (confidentiality), constantly monitored for trojans or unexpected changes (integrity), and backed up on a separate server in case of natural disaster, system failure, or any other disruption (availability). (IMAGE 2)

## **Principle 3: Defense in Depth as Strategy**

A security network should be likened to an onion. Both have layers. While not convenient, many layers of security should be given and assigned to sensitive data, each layer securing the next, and hopefully addressing the shortcomings of other layers. With both physical security measures and automated measures we try to strike a balance between each one’s strengths and weaknesses. Even the smartest security agent in the world has a chance to fall for one of the simplest phishing scams, and one of the most elaborate security AI can be tricked into letting a malicious program slip through it’s fingers. When used in conjunction however, weaknesses become minimized, and the strengths have been maximized.

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

 Human nature is to trust. No matter how many security measures are in place, all it takes is one person to slip up and reveal a little too much about sensitive information, and boom the whole system is compromised. Janice in HR can click an email link that she thinks will take her to a website filled with cute puppy pictures, but instead it scans her system for usernames and passcodes. Constant security meetings, and reminders to the people we are trying to protect go a long way in keeping the company, and it’s employees safe.

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

 Computers are one of the most complicated and finicky things on this planet. Computer software is no different either. When looking at both hardware and software you need to ask yourself, “Is this functional? Is this working the way I intended it too?” and then (especially with software), “Are there any vulnerabilities with the implementation for this?” Maybe the accounting software just got an update overhaul, and corporate wants us to install it properly for them. Once we get everything installed, up and running, it is revealed the new update has several backdoors and vulnerabilities that hackers can exploit and gain access to our accounting information with, but it is too late to roll back the update. Computers are complicated, so our approach to their security should be thorough and meticulous.

## **Principle 6: Security Through Obscurity Is Not an Answer**

 When securing a system, hiding how the security works is not even remotely close to a solid security measure. It should not be your goal to keep mechanisms a secret, as like we said in Principle 1, someone will always be out to find those secrets out, and if given enough time and resources, they’ll eventually find out those secrets. If our entire security system relies on a password that we do our utmost to keep secret, and only that password, but we convince ourselves it is secure because no one on the outside knows that secret, the second someone finds it out (and they will) the whole system becomes compromised.

## **Principle 7: Security = Risk Management**

 Risk analysis and risk management are the two integral to securing information services. An IS practitioner should ask themselves if the security measures justify the damage done if that system was to be compromised. If a system is at high risk for exposure then immediate action should be taken, but if it is a low risk then our efforts or resources should be focused on more pressing matters. Our job is to figure out who might want to attack our systems, their level of expertise, how they might go about exploiting our systems, and which systems they might want to target. Systems that carry sensitive information about our customers, or systems that are integral to keeping our company up and running, are far more at risk than a system that carries a company employee list or other smaller systems such as that.

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

 These three types of security system, and the proper combination of these 3 make our systems that much harder to exploit. If we have measures to prevent an attack before they happen (Firewalls, IPS etc.), catch an attack or see anomalies in our systems (Human monitors, IDS etc.) and measures to respond to these attacks (kill switches, alarms to notify humans of the attack etc.) then our system will be well protected. (IMAGE 3)

## **Principle 9: Complexity Is the Enemy of Security**

 The more complex a system becomes the harder it is for a security team to defend it. A small family owned business is a lot easier to secure and defend than the White House for example. As the web of networking expands over systems, with more programs, systems, and people being added to it, the more complex and difficult our job becomes at securing and protecting each and everyone of them. If all we had to do was defend HR’s master terminal it would be a pretty simple job and wouldn’t require a security team, but one we start adding other departments computers, different routers, and locations our job starts getting infinitely harder.

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

 Scare tactics only work in politics and pushing propaganda, not security. When we need to ask for more resources from management, we justify our means to our end. IT Management is a lot smarter about technology nowadays, as most other people are, and we cannot blame the hacker boogieman on why we need more money and resources than we realistically do. If we were to want more security and higher wages we would go to management and provide evidence and reasoning as to why it is justified, not try to scare them with big words and fake threats to push them into approving it.

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

 When attempting to properly secure anything, there should not be an over reliance on any single thing, people, process, or technology. Instead a balance, with cohesive synergy should be striven for (IMAGE 4). Imagine a table. That table needs multiple legs if it needs to be able to stand up tall, if built on one leg, or even only two, it will be wobbly and unstable, ready to tip at a moment's notice. But if a balance is struck with 3 legs each supporting the table equally, the table will stand strong even when pushed around. In a secure system people should be monitoring network traffic, and the technology implemented (firewalls, IDS/IPS, detection algorithms) with each person with their own jobs to fill in the network (preventing just one person from being totally in charge) with a process such as the separation of duties.

## **Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!**

 When it comes to dealing with users, and even sensitive information with coworkers, secrets are never good. If you see something, say something. Our users have a right to know that we might have been compromised, whereas if we had kept that from them, chances are it’ll get out anyway, and our reputation will have taken a bigger hit. When monitoring a system if any one of you should see something out of the ordinary, no matter how small, tell a superior. Secrecy, especially in something as complicated as IS, generally leads to that situation becoming that much more complicated. If we are compromised, being open with the public does more good than harm.

References:

*Information security principles of success*. (2014, July 4). Pearson IT Certification: Videos, flash cards, simulations, books, eBooks, and practice tests for Cisco, CompTIA, and Microsoft exams. https://www.pearsonitcertification.com/articles/article.aspx?p=2218577

IMAGE 1



IMAGE 2



IMAGE 3



IMAGE 4

