1. No matter how much security or where you hide stuff at, people will always find their way around it. It doesn’t matter if it’s the best of the best, people will still find a way around it. Unauthorized access happens with people not even knowing it.
2. The three security goals are Confidentiality: Being or keeping secret or private, Integrity: Truthfulness and Availability: Which is What is available and what can be obtained. All these are important for the triangle because they all work together to make sure everyone is safe and secure and know what they’re doing and keeps hacker and attackers out of the network.
3. Defense in Depth as Strategy: Layered security help have layers in the security which includes 2FA so that systems are harder to get into without the authorization. These Detect, Protect and responds to attacks so that if someone is not monitoring it then it can take care of itself.
4. People make the worse security decisions: Some people don’t understand why security is so important and don’t realize the damage that can be done. people always need to keep their passwords secret and only high up personnel need to know it.
5. Functional and Assurance: The most important thing about your software is, is it functional? Having your software work efficiently is super important so that you don’t have to keep checking on it and having to worry about an attack. Assurance is there so that just incase it does fail there will be a backup that is there to make sure the attacks or hacks don’t get into the system.
6. Security through Obsecurity is not an answer: When the first hacker finds out how to crack your security, then the whole mechanisms of the security is broken down and will no longer work until improved or fixed. Also with this information they can probably go through the whole system and break it down piece by piece to know how it works.
7. Security = Risk Management: Security is concerned not with eliminating all threats within a system or facility, but with eliminating known threats and minimizing losses if an attacker succeeds in exploiting a vulnerability. Risk analysis and risk management are central themes to securing information systems.
8. Three types of security: Controls must be implemented as one or more of these previous types, or the controls are not there for the purposes of security. Detective: Tells the system wether or not there is a virus. Responsive: how the system Reacts to the attacks and what it does.
9. Complexity Is the Enemy of Security: More complex systems= the harder it is to secure which can lead to more attacks and different ways hackers could get in.
10. Fear and Uncertainty: The tactic of fear, uncertainty, and doubt (FUD) no longer works: Information security and IT management is too mature. Now IS managers must justify all investments in security using techniques of the trade.
11. Process and Technology are Adequately Secure: Process controls are implemented to ensure that different people can perform the same operations exactly in the same way each time. Processes are documented as procedures on how to carry out an activity related to security. The process of configuring a server operating system for secure operations is documented as one or more procedures that security administrators use and can be verified as done correctly.
12. Open disclosure of Vulnerabilities is good for security: Some white-hat hackers hack into businesses, not for harm, but to make sure that the company knows about these weak points and to make sure they are able to keep everything safe.

Gil, A., & Clemson University. (2019, December 3). Data Security - Confidentiality, Integrity & Availability: kVA. Retrieved from <https://www.kvausa.com/data-security-confidentiality-integrity-and-availability/>.

Shah, N. (2018, May 1). The Security Risks Presented by Complex Networks. Retrieved from <https://www.fortinet.com/blog/business-and-technology/decrease-your-customers--network-complexity-for-increased-securi.html>.

Tittel, E., & Follis, E. (2019, June 17). Top Tips For Becoming a White Hat Hacker. Retrieved from https://www.businessnewsdaily.com/10713-white-hat-hacker-career.html.