Security Team Training

Adalberto Ruiz

University of Advancing Technology

Our department was recently requested to create a training plan for our security team. The training plan must include the 12 principles of information security. If you do not know the 12 principles of information security, they will be highlighted throughout the plan. The first principle is there is no such thing as absolute security. This means that no matter how secure you believe the security is, people will get through. Given enough time, and knowledge, anyone can get through security measures. Never let your guard down, because there have been some of the most secure companies in the world that have claimed that no one will be able to get through their security that have been broken into. The next principle comes along with three security goals. One of the goals is confidentiality. This means everything must be kept a secret and in private. The information must not be disclosed to anyone person or thing. The second goal is integrity. With integrity comes the golden rule that data must be kept pure and trustworthy. None of the information can be changed whatsoever, not even one single character. Availability means that the data and resources are only available for authorized use. Non authorized users are not allowed to access confidential data, only you are responsible for what goes on through your account. The next principle is defense in depth as strategy. With this principle comes human error. As an example, if something gets emailed to you that looks odd, or different than the usual, it’s most likely a phishing attempt. Once this happens, your best bet is to delete the email, and not download anything or enter credentials. This is one security measure that is easily looked over. If you download an executable file and run it or enter a credential from some external source, our security is most likely compromised. From there they have access to all files linked to your account and they can compromise more from there. The next principle is when left on their own, people tend to make the worst security decisions. This means that even when you’re out of the office do not take any bribes. Your security is still at risk since you know inside information with our company. The fifth principle is security depends on two types of requirements: functional and assurance. While functional requirements are explaining what a system should do, assurance requirements tell how a functional requirement should be implemented. The next principle is security through obscurity is never the answer. No matter how obscure you make it to get through the security measures, people will take time out of their day just to get through. It’s like a puzzle, while it’s a tedious task it’s easily accomplishable to finish the task with a bit of time and effort. The seventh principle is security = risk management. This means that you must balance out the budget. It would make sense to protect your $100k house with $2,000 worth of security, but it would not make sense to install a $3,000 alarm system on a car worth $1,000. The following principle has three types of security, controls are preventative, detective, and responsive. This means that our security controls must have a way to prevent, detect, and a way to respond to a compromise in real time. The ninth principle is complexity is the enemy. Making security far too complex will make it much more difficult to implement and it’s usually not worth the time or resources to do so. The tenth principle is fear, uncertainty, and doubt don’t work. Scaring management is a terrible way to get the resources and money needed to be invested into security. Explaining is a more reasonable and honorable way to do this stuff, because then they will have an understanding on what is necessary and what is not. The second to last principle is people, process, and technology are all needed to secure a system or facility. All these are needed to secure a system or facility. Without people how will the process install itself onto a machine? The answer is it does not. The machine does not have self-installing capabilities, while humans are not robots intended to do one thing, and one thing only. Disclosure of vulnerabilities is not good is the last and final principle currently. Telling people about issues or patches is terrible for business and will hurt the industry in the end if kept a secret. These are the 12 principles you must know and follow while working in this company.

Terry F (2014, December 14) Twelve information security principles of success https://ezinearticles.com