Module 7 Journal

Joshua Lane

03/03/19

Advances in cyber technology have created opportunities for workplace deviance. Human beings will always, to a certain extent, accidentally cause cybersecurity incidents or purposely cause cybersecurity incidents. Employees specifically are the weakest links in the cybersecurity chain, so to speak. Human behavior is considered to be “cybersecurity’s biggest, most persistent threat” (Blau, 2017). A lot of companies are trying to throw more technology-oriented fixes at the human behavioral problem, and it just is not working (Blau, 2017). The way to significantly reduce financial costs to companies due to cybersecurity incidents in the long run is to put employees through proper training. When training and leading employees, these companies must account for common human behavior when addressing how to get employees not to deviate from secure practices.

Technological cyber advances have given the end user a false sense of security. While better software and hardware with less vulnerabilities may make a cyber system more secure, they do not prevent employees from using the system improperly. Companies in the past had been focusing more on the software and hardware side of cybersecurity, so a lot of hackers target the employees in an attempt at easier access (Blau, 2017). IBM reported more than 95% of security incidents were due to humans making mistakes (Blau, 2017). This includes any of the most common attacks such as phishing, brute force password attacks due to weak passwords, or not installing security updates in time (Blau, 2017). Accounting for human behavior when engineering a cyber system and making policies to keep employees in check is one of the most effective cybersecurity measures that a company can take.

One way is to remove certain options for the employees that would make them procrastinate updates. Automatic update features remove the employee's choice to procrastinate because they are not authorized to stop the update when it is a default software feature (Blau, 2017). You can keep track of policy compliance levels with software for each employee and send them a monthly report of how well they are doing compared to others, and this of course must go through a deidentification process. It encourages employees to step it up to the level of their peers if they are lacking when compared (Blau, 2017). This appeals to the human want to be competitive or not be left behind by people they consider their equals (Blau, 2017). In these and other ways, behavior can be nudged in the right direction to make the cyber environment more secure.

Influencing human behavioral patterns through software and adaptive policies is the best way to mitigate workplace deviance. Human behavioral patterns are relatively predictable, so this is not such a difficult task when thought about in the grand scheme of cybersecurity. There are mountains of information on manipulating human behavior, one just needs to know where to look.

References

Blau, A. (2017, December 11). Better Cybersecurity Starts with Fixing Your Employees' Bad Habits. Retrieved March 03, 2019, from https://hbr.org/2017/12/better-cybersecurity-starts-with-fixing-your-employees-bad-habits