Chad Holm
cholm017@odu.edu

Leverage Psychological factors Associated with Lapses in Cybersecurity in Organizational Management

With computers being a standard part of life now with the evolution of the internet, many aspects of our lives have changed, and new ways of thinking must come. One of the biggest challenges in most cyber security problems is not related to the software or the hardware; it is the people that are using the computers to access the data and communicate with others, where the hackers could simply find a weak entry point that naturally exists and a weak link caused by human hands. The human factor as an "insider threat" will affect unauthorized access, credentials stealing, and computer systems with malware. It is important to adopt user-centered methods and organizational management involved perspective and leverage the human factors as an integrated methodological approach to cultivate a better cyber-security culture. The centerpiece of the solutions comes down to the investigation of the rationale and psychological factors that why the people make these choices, how the user feels with the added security involved, and why people choose not to follow these guidelines? Even though in most cases, the added cyber hygiene practices required for many of these computers' users are simple and easy to understand. However, this failure occurs at all levels. This paper it will address some of these issues and looks at possible solutions to the problems.

As in a report done by ProofPoint inc. [1], the key findings are that individuals and lower-level management account for about 60% of the targeted malware and phishing attacks for user credentials [1]. Workers in operations and production roles are the most exposed, and they account for 23% of targeted malware and phishing attacks credentials [1]. Management was the

second-most exposed job function, followed closely by the R&D and engineering departments. Executives and upper-level managers are targeted and receive more of these attacks even though they represent a smaller portion of the workforce [2]. Phishing and spear-phishing may seem trivial and straightforward when looked at by general users, but when the attackers know what to look for, these users can be easily deceived by phishing attacks. There is a rise in phishing attacks in the workplace based on social media. These type of cyber-attacks have gained popularity in recent years, with the amount of time people spend on social media constantly increasing. This leads to another avenue of an attack at the workplace with people logging on to their social media accounts on the companies' networks and hardware. People forming an addiction to these social networks make it difficult to prevent the employees from logging on while at the workplace. When at the workplace, many employees do not feel that they are doing anything wrong by not following proper cybersecurity procedures. Many think that the structure implemented at the workplace works and the simple things that they do wrong will not hurt anything. This can lead to significant problems in the workplace atmosphere. There are many ways that people have tried to fix this problem, and some of the solutions do work within reason. One way is to make the employees at a company feel as though they are a part of the big picture and make them feel as though they belong. This creates the need for the upper management to change the ways that they run the day-to-day operations [3]. One solution is to give weekly or monthly briefings and training to let the employees know about all the new security risks that have surfaced and the damages caused by cybercrimes. This simple approach can make the employees feel as though they are a part of the defense of the cybercrimes and their part in the big picture makes a difference.

Another perspective to consider is to provide incentives to motivate employees to follow proper cyber security procedures is to give them incentives. This approach tries to make people more aware of what they are looking at when they read their emails. During the briefings, there can be some examples of phishing emails or other typical cyber-attacks examples to show to the employees to help them notice the minor flaws that are usually included in the phishing emails and these attacks. Games and other activities can also gain good employee morale when it comes to cybersecurity by allowing the users to interact and make the training easier to understand, as noted in a securityscorecard.com story [4]. There are cybersecurity based games available to assist with the training, such as Anti Phishing Phil, a mobile app designed to help train people to notice phishing emails [5]. This general approach will make everyone more aware of the problem at hand.

There are many reasons for the failures of proper cybersecurity practices within organizations. They can be like what has been mentioned above, but they can also go much deeper than that. Many companies have created training programs to help strengthen their approach to cyber security. In paper [6] (Reeves A, January 2021), many people who participate in these programs have a negative feeling about participating in the training sessions that are held to train the users about cybersecurity. For example, employees may find that the actions required to maintain cyber security are overwhelming and tiresome, and as a result, they disengage from security-related behavior that leads to fatigue [7]. There is a four-component model [6] that explains this fatigue. The fatigue type is classified as cognitive or attitudinal. These are the two ways that individuals will experience and manifest cybersecurity fatigue. The cognitive type of fatigue refers to an individual's limited capacity to make decisions. When this fatigue starts, people fall back to being impulsive, intuitive, and biased decision making or avoid making

decisions at all. This can lead to problems with people ignoring security warnings while they are on the corporate network. The other type of fatigue: attitudinal is where an individual has a negative effect relating to cybersecurity. This can be a result of emotional exhaustion, moral disengagement, and cynicism. If they are suffering from this type of fatigue, they may not feel that the cybersecurity procedures are of much value. With burnout being such a problem, it can be tough to get the employees to follow the proper procedures. Many employees feel that cyber security programs at their workplace make their lives harder and will inherently make things worse.

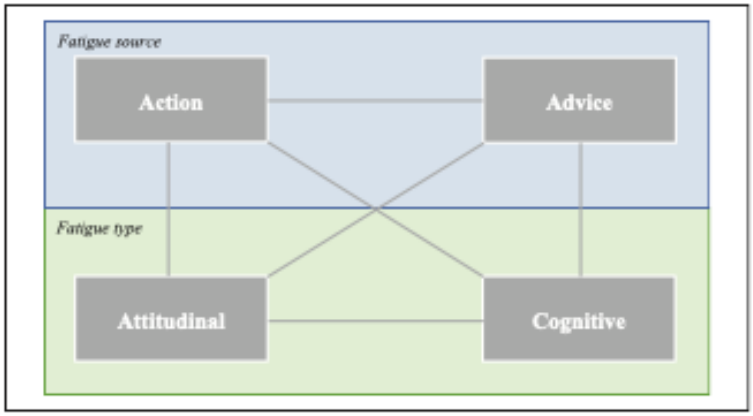

Fig. 1 The Four-component Model of Cyber Security Fatigue [6]

The other two parts of the four-component model of cybersecurity fatigue are the fatigue source. These two can be viewed as a pair; also, they are action and advice. The advice goes with the overload of information that individuals receive about cybersecurity. The users are tired of behaviors that they must comply with to keep up with the policies that are in place. On the other side of this is action fatigue. If an employee is repeatedly asked to change his password or must question every email they receive, these are examples of action fatigue setting in. Many times, employees with find workarounds to the security systems in place when this type of fatigue sets

in within individuals. One such example of this is with the use of multifactor authentication, which leads to an action-related source and leads to cognitive type fatigue. These types of fatigue can come on easily and you can see in Fig 1 that both sources of fatigue can result in each fatigue type [6]. Ultimately, this fatigue can lead to burnout among individuals. The stress of new systems and security measures can trigger a poor attitude if not noticed. This can be referred to as a technostress [8], which refers to stress caused by the use of technology. The relationship between technostress and workplace behaviors has been well researched [9]. Individuals suffering from technostress are far less likely to adopt new technologies, less productive, and less satisfied with their jobs [10].

With the complexity of cybersecurity and the nature of the attacks, it is extremely important for the general workforce to be knowledgeable and trained in cybersecurity to a certain level. Attention must be given to prevent the failure of a good cybersecurity program so that the weakest link is not the employees behind the computer and the company is still in compliance with the requirements they must follow. It comes down to finding compromise the "Security, Functionality and Usability Triangle" [11] and finding a balance between the three. Too much security and it risk burnout with the employees. In many cases, it should be scaled back on security and functionality to move more toward usability [12].

With the number of attacks on government and private computer systems, it has become necessary for the typical user to pay more attention to what they are doing on these systems. Many people do not have the safe cybersecurity habits that they do every day. This can come from many sources, but many times it comes down to a choice the user makes. We need to continue to look at this problem to find solutions to this complex problem. It can come as simple as making sure that the users are comfortable with the software they are using and listening to

complaints, so the problems can be solved. Using new sources of educating the users by conducting the education in an interactive and fun way. We can limit the number of successful attacks by making the users understand what these attacks can be disguised as.

References

[1] Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks | Winter 2019 https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-protecting-people-winter-2019.pdf

[2] https://www.computerweekly.com/news/252448101/People-top-target-for-cyber-attackers-report-confirms

[3] R. Beyer, B. Brummel-Implementing Effective Cyber Security Training for End Users of Computer Networks 2015

[4] https://securityscorecard.com/blog/5-ways-to-engage-employees-during-national-cybersecurity-awareness-month

[5] Hendrix, Maurice & Al-Sherbaz, Ali & Bloom, Victoria. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training?. International Journal of Serious Games. 3. 10.17083/ijsg.v3i1.107.

[6] Reeves A, Delfabbro P, Calic D. Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*. January 2021. doi:10.1177/21582440211000049

[7] Furnell, S., & Thomson, K.-L. (2009). Recognising and addressing "security fatigue." *Computer Fraud & Security*, *2009*(11), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

[8] Brod, C. (1982). Managing technostress: Optimizing the use of computer technology. *Personnel Journal*, *61*(10), 753–757.

[9] Atanasoff, L., & Venable, M. A. (2017). Technostress: Implications for adults in the workforce. *The Career Development Quarterly*, *65*(4), 326–338.

[10] Calic, D., Pattinson, M., Parsons, K., Butavicius, M., & McCormac, A. (2016, July). *Naïve and accidental behaviours that com- promise information security: What the experts think* [Paper presentation]. The Tenth International Symposium on Human Aspects of Information Security & Assurance.

[11] Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K.: Guidelines for usable cybersecurity: Past and present, in The 3rd International Workshop on Cyberspace Safety and Security (CSS 2011) at The 5th International Conference on Network and System Security (NSS 2011), Milan, Italy, 6-8 September.

[12] Bada, M. Sasse, A. Nurse, J. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? January 9, 2019 https://arxiv.org/abs/1901.02672#