CYBERSECURITY: A HUMAN ERROR

Name: Abdulaziz Aljebrin

Course: IT-120-A

Date: 03/9/21

**Abstract**

The increased usage of the internet has made organizations, businesses and individuals to be vulnerable to outside attacks. The increasing levels of internet insecurity are increasingly becoming a worry for almost everyone to the extent of the internet world being untrustworthy. Studies form the Computer crime and Security Survey indicate that there has been an upward trend in cyber crime attacks with different types of malicious attacks including spyware, viruses, social engineering, etc. As much as there has been tremendous results in updating of software and machines, the issue on attacks still stands to be a menace. More individuals and organizations are still being attacked. In this paper, I provide an overview of cybercrime, identify tools being used by the perpetrators to push their agenda. This paper seeks to establish how human activity has increased the possibilities of vulnerability all over the world. I will focus on the extents that machine and software security has been developed and how the human factor still stands to be the weak-link in creating a secure internet world. The paper will also include a personal reflection on the extents that cyber crime has thrived under human supervision.

Cybersecurity: A Human Error

**Introduction**

This paper is about cybersecurity and the circumstances revolving around human error that directly influence cyber-attacks. Cybersecurity or information technology security is the protection of computer systems and networks from malicious attacks or unauthorized access. In the current world, criminals have shifted their attack methods to now manipulating human behavior to inflict cyberattacks. Businesses have the fear of being put at risk because top security fears are related to human factors and employee behavior. Most businesses are wary about employees sharing inappropriate data via their resources or devices. We as human beings want to achieve much in a short span that we accept technology derived to suit our desires to lead us. This perception is on an individual basis and at the organizational level. Most businesses will trust software to run their errands and have a few individuals run them.

Altogether, businesses have a good reason to be worried about employees assisting in cybersecurity risks. Employees may make mistakes that put their businesses’ data or systems at risk which could mean that they do not have the required training to teach them how to behave properly and to protect the company they work for. Other than employee carelessness, cyberattacks on businesses could be from the internal employees, working against their employer. Potentially, this could mean attacks by viruses and malware. Businesses will have to undertake new security policies which will focus on balancing human engagement and machines. Most businesses have the best firewalls but still find themselves attacked due to the carelessness and ignorance from staff members and other employees.

**Literature Review**

According to Kaspersky, global cyber-attacks continue to evolve at a rapid pace, with new cases being recorded every year. Governments across the world have responded to the rising cyber threats with guidance to help companies and everyone else implement effective cybersecurity practices (Schwab, & Poujol, 2018). In 2019 alone, over 7.9 billion data breaches were recorded which was almost double the number recorded over the same period in 2018. The international data corporation analysis shows that such breaches could result in a massive expenditure of over $133 billion by the year 2022 (Jouini, & Rabai, 2020). With over 57% of businesses operating through the online space, internet security will continually be compromised. Initially, businesses strengthened their systems with the latest technologies but still ended up being attacked.

According to IBM, human error has been greatly overlooked to the extent that we make mistakes as our ways of growing and learning rather than the pathways to the losses we achieve. The study indicates that if we eliminated human error in cybers security, we can eliminate over 95% of these attacks (Gillam, & Foster, 2020). When security incidents happen at businesses, more so with the current online structure, employees are supposedly directly involved or are in a position to mitigate the risks unknowingly. All the same, businesses fail to take serious action when they are hit by security incidents. Over 40% of businesses in the world will hide information regarding attacks happening due to human error emanating from the fear of being reprimanded (Gillam, & Foster, 2020). The thought of trusting such systems could lead to extensive damage and breach of the entire organization's infrastructure. All the same, the implications could have a far-reaching damaging impact all through the market environment (Thames, & Schaefer, 2017).

Businesses using the BYOD policy (Bring Your Own Device) to work ultimately allows business data to be carried and worked on via personal devices. However, the devices may land on unauthorized personnel or may get stolen exposing company data. In such situations, the company may have to install security systems on the devices, employee carelessness may expose data. Over half of data exposed by employees happens after they lose their devices placing them as crucial components of attacks (Evans, Maglaras, & Janicke, 2016).

**Reflection**

Many electronic security software programs are available to detect malware and remove them from machines. Security programs are there to help confine programs that may be potentially malicious to the system and separate them from the user’s network to prevent new infections and attacks. Moreover, security programs are continually under improvement with new threats evolving every other day. However, there are no mechanisms to isolate human mistakes from leading to attacks unless through putting data protection policies. There is more that businesses will have to do to secure their systems from employees who might act irresponsibly. Until then, when organizations and individuals realize that we cannot completely trust systems and humans to develop security solutions.

It is common knowledge that cybercriminals are into social engineering aspects to develop and propel their scamming tactics. The rise of social media has made the process much easier with criminals imitating businesses or personnel from well-known brands. The ease of access and the aspect of manipulation facilitate cyber-attacks. For example, an individual may imitate to be the CEO from a given brand company requesting transfer of funds from the business’ accounts. The same individual may create malware emails, create profiles with the credentials and finally succeed in getting the money. It may take months before the company realizes that they may be losing money, and even after knowing, it may take time to rectify the situation.

Businesses are in constant danger of threats both internally and externally. However, what we should be wary of is the danger from within happening with due advantage from careless or uninformed staff who are more likely to cause a security breach. There could be individuals who could intentionally be malicious enough to carry out attacks for their purpose or to settle old scores with the company employing them (Streeter, 2013). Therefore, companies should advocate for an easier mechanism for identifying cases of attacks no matter how small they may be and differentiate between legitimate and malicious activities.

**Conclusion**

While putting security policies in place and adhering to them is important for a business, we also need to understand that the policies cannot cover all the risks. We need to have everyone strictly follow the policies. It is evident from the discussion above that if only individuals were more careful with what they do on the internet and through their devices, we can eliminate almost every other cyber-attack possibility for the respective company. Moreover, there is a need to implement solutions that are more visible and centralized with the operations of the company, so that employees can be more aware of their actions and mitigate any scenario that would jeopardize the security of company data. By understanding that most cyberattacks are human-centered, we can focus on mechanisms and defense systems that will account for an organizational system rather than a technological system.

**References**

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667-4679.

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. *Computers in Human Behavior*, *108*, 106319.

Jouini, M., & Rabai, L. B. A. (2020). Towards New Quantitative Cybersecurity Risk Analysis Models for Information Systems: A Cloud Computing Case Study. In *Handbook of Computer Networks and Cyber Security* (pp. 63-90). Springer, Cham.

Schwab, W., & Poujol, M. (2018). The state of industrial cybersecurity 2018. *Trend Study Kaspersky Reports*, *33*.

Streeter, D. C. (2013). The effect of human error on modern security breaches. *Strategic Informer: Student Publication of the Strategic Intelligence Society*, *1*(3), 2.

Thames, L., & Schaefer, D. (2017). *Cybersecurity for industry 4.0*. Heidelberg: Springer.