Name: Ean N. Miller

Date: 4-2-2023

OLD DOMINION UNIVERSITY

CYSE-200 CYBERSECURITY TECHNOLOGY AND SOCIETY

WRITE-UP #3: The Human Factor

Table of Contents

BLUF

There are many ways that the human factor has played a role in our society, not only in scientific, medical, artistic, and social advancements but also in cyber technology. Throughout the history of cyber technology and its creation, there have been many different contributions to improve various technology and systems that have made technology reliable and used in almost every facet of life. But with grants and improvements, there also come issues, which sometimes involve the human factor. Although there are many different cyber threats to technology, there are also many methods to defend against those threats. However, as mentioned, the human factor will make these defensive methods obsolete unless people have the proper training and knowledge to not give in to these cyber threats.

The Human Factor:

As mentioned, the human factor and the various contributions people have made to improve technology have vastly improved society. Not only that, but because of the human factor, society has been able to implement cyber technology into nearly every facet of life. Although there have been contributions due to the human element, many methods have been used to turn these contributions into disadvantages or weapons to use against people. Many ways were created to infiltrate, steal, and use data and information against various companies and organizations to get more, whether money or personal data. As cyber technology and the internet advanced cyber threats also advanced through the creation of techniques and methods such as the Trojan Horse, worms, viruses, zombies, malware, phishing, etc. Due to human interaction with the internet and cyber technology, these methods of attack and cyber threats were created. However, another human factor issue is that if people are not adequately trained or know how to identify or defend against these threats, they can and will fall victim to these attacks. Fortunately, many companies and organizations implement this sort of cyber technology training to ensure that their employees can identify and defend themselves against these cyber threats.

Various Human Contributions & Cyber Threats:

Human Contributions:

The human factor and its vast contributions stretch far and wide, from the humble brick house phone or landline to the vast world known as the internet that we have today. These contributions improved human life and society, such as the ability to secure, categorize, catalog, and gather data safely. This made things like taking inventory and collecting data to find social trends that companies can adjust their algorithms to fit the trends and make more money from. For instance, relevant and everyday use of this is seen in social media today. Social media sites like Instagram, Facebook, and others use advertisements and surveys to gather data. Companies and organizations then use this data to determine what promotions are working and whether or not they should keep up with their usual advertisements or switch things up that may entice more people to buy what they are selling. Another contribution is the creation of the smartphone; these devices are probably the most common piece of cyber technology in the 20th century. They are seen in almost every person in the world, and every person is attached at the hip to these devices in an almost addictive way. Nearly everyone is on these devices and always has them on hand. With these smartphones, information has been made that much easier to access, and communications worldwide have become more reliable and available. Someone could be here in the U.S., out on the street, contacting someone in another country, beforehand this feat was only possible through the use of payphones and various other less reliable methods. Still, with these advancements, some tradeoffs and disadvantages will arise.

Cyber Threats:

As with improvements, issues will always arise to be the counterbalance with various cyber threats that have been created. Multiple techniques or methods that one may use to break into a system include malware, phishing, and other practices that a hacker or attacker may use to tamper or steal information from a company or an organization. Much like human contributions, these cyber threats are also due to the human factor; human intervention has made it possible for cyber threats to be used often and created constantly. Although the human factor also plays a role in these cyber threats in more than just its creation, without proper training, these threats can significantly affect technology and systems. One such impact the human factor can have is that with phishing, a person may receive an email from a legitimate-looking source. The person will then click on the link it may be provided, which may have a payload of malicious code or malware that may lead to a possible breach in security or worse. Another issue would be if someone were to use random hardware that may be found on a university or college floor. Then use said hardware without realizing it is harboring malware or programs, such as keyloggers, that can steal your info to get money or other valuable things. There are also things like trojan horses, where someone can download seemingly harmless open-source code but then become infected by the trojan breaching their security. There are many ways to infiltrate these systems, but more often than not, these methods are only effective due to people's lack of knowledge of cyber threats and lack of training in identifying them.

Training & Cyber Technology & Fund Allocation:

Although, at first glance, it should be common sense and most people should have some background knowledge of cyber technology, most of a company's funds should be put into training people to identify cyber threats. However, some companies and organizations must pay more attention to this training and invest more in their cyber training. What these companies need to realize, however, is that proper funding for their training can lead to drastic consequences for their company and profits. Firstly, many schools and other educational institutes should require at least one online and technology safety class simply because of how common cyber threats and human errors occur with their technology. Aside from that, companies should put a good portion of their money and funds into cybersecurity training because of how vital this training will be in securing the sensitive information a company may have. Companies should allocate about 45% or 50% of their funds to cyber training. However, this should not be a necessary investment simply because most companies have top-notch security systems and software. However, these fancy and high-end security systems are nothing in the face of the human factor that can invite various cyber threats into a company. One person with no proper or zero training in cyber awareness is a substantial cyber threat to a company and needs to be taken care of before the danger is even given a chance to put the company at risk. If I were to be in charge of the cyber training, I would start with the basics, such as not clicking on suspicious links, do not go to sites that are not company-sanctioned on company computers, you can get viruses on your own time with your computers, and one of the most significant issues I have found with many people that I know, do not use simple passwords, use complex ones with a lot of various characters, numbers, and no specific phrases or words, make it as random as possible. Although these seem like relatively simple concepts, most need to realize or learn not to do these things and are often vulnerable to attack and infiltration. Not only that but if the company were to introduce some new system or hardware, I would balance this out immediately after it has been implemented or before having cyber awareness or training sessions to train employees on these

systems and show them what not to do. However, if unable to host a meeting or training session, I would send emails about the other cyber technology, give the employees the rundown, and then do a follow-up meeting or session.

Conclusion:

In conclusion, due to the many advancements and contributions that humanity has made in the cyber technology field, we should emphasize and implement more training in our companies and institutions. With the human factor issue, while it did provide many advantages to our society, it also causes too many problems and disadvantages that cyber training is a necessity. A quarter or nearly a quarter of funding should be put toward cyber training to defend against cyber threats. Not only that, but if a company introduces new systems or cyber technology to their employees, they should host some sort of meeting or training session before its implementation to give their employees ample time to get used to the new technology and prevent security breaches. Without proper training, a company's most secure and high-end security will fail simply because of the human factor.

Sources Cited

No sources used