Humans in Cybersecurity

Amani Almutairi

Marymount University

Abstract

In this Digital Age, securing technology against attacks from outsiders and insiders has never been more critical. Securing technology entails ensuring that the system is immune to cyberattacks from malware. At least, this is what most organizations focus on. Most times, organizations pay a hefty amount of money to develop new technology to keep the systems safe. Human beings are often forgotten in this cybersecurity conversation. They have proven to be the weakest link in the war against cyberattacks—Cyber attackers prey on human beings for naivety, ignorance, or slip-ups. Therefore, human resource needs to be informed on their role in this whole fight and what can be done to better security.

Some of the keywords in this report are:

1. i) Cybersecurity – This is the process of defending the technology and data in an organization against attacks.
2. ii) Cyberattack – Deliberate actions are taken to bypass the security protocol of an organization.

Introduction

Cybersecurity calls for organizations to be vigilant in the measures they take up to protect themselves against external and internal attacks of a malicious kind. One mistake in clicking open an email or a website could prove to be too costly for organizations in this day and age. Hackers have developed new and improved methods of attacking. Therefore, it is up to these organizations to be more vigilant in protecting their data and technology. Measures taken could be subjective to each organization. Oversight boards could also be established to create policies for organizations to follow.

Literature Review

This report reviews three different articles written by credible authors by their mastery. The consensus in each of these articles is that human beings still pose the biggest threat to cybersecurity in terms of liability, thus earning the title "weakest link." This implies that the solution to minimizing cyberattacks lies in the human resource.

Robert Kress, the managing director of a company specializing in assessing risk, highlights how human beings are centered on the problem. "Phishing and social engineering attacks, up 16%; ransomware, up 15%; and stolen devices, up 13 percent in just one year" shows only part of the problem (Kress, 2019). The author insists on the importance of holding employees accountable. He argues that employees are often neglected in the process of solidifying against attacks such as new products and technology. As such, employees are not aware of the loopholes that could be exploited. Some of the ways an organization can be accountable are fostering safe behavior, creating a culture of cybersecurity champions, incentivizing "security-first" behavior, and informing the people on what to expect (Kress, 2019).

Lance Spitzner echoes the point that human beings are often neglected in his article. He argues that organizations spend up to 20 times more on computers than "humanOS" (Spitzner, 2019). Mus Huseyin argues that companies using "$2000 per full-time employee on cybersecurity" yet corporations are losing $12.5 billion to business email compromises aimed at tricking employees into thinking that they are corresponding with their CEOs, shows the need for a change in direction. Humans are failing against technology. Therefore, he argues that it is time for organizations to rethink how cybersecurity is approached in organizations.

In my opinion:

The fast developing in the computer machines. Make our life more comfortable and help us in most things, such as shopping, education, and communication. This means we must be more aware. The interaction with others might be necessary and with attention. You cannot give yourself to the one you don't even know him you may see his outlooking without knowledge.

Reflection

Cybersecurity is pivotal in this day and age. Any slight loss in concentration or simple security measures could prove to be too costly a mistake to the organization. The gravitas of the issues at hand could be assigned a value, which would be the estimated $31 billion in the loss that banks experienced in 2018 (Huseyin, 2019). It is, therefore, a severe issue – having the human resource as the loose end.

Having identified that as a pressing problem, it is also essential to figure out the next possible steps in redefining the cybersecurity space. Is it time for a change in my way of thinking? This question prompts subjective answers based on the organizational culture. Some organizations have thrown money at training the human resource in issues cybersecurity. Often, these are large organizations. In such a scenario, while teaching the human resource on matters cybersecurity is essential, an automated cybersecurity system is paramount. The bigger the organizations, the more complex the cyberattacks. Pitting the human being against the computer is not a good idea; it is only a matter of time before the computer beats man.

For organizations that barely invest in training the human resource on cybersecurity issues, they ought to invest.

For organizations that barely invest in training the human resource on cybersecurity issues, they ought to invest.

The tough balance lies in balancing this graph:

Figure 1

Figure 2

65%: Security pros who expect to be responding to a major breach in the next year	20,373: Number of complaints the FBI received last year involving business email compromise (BEC) attacks	68%: Share of pros who said skills shortages were impacting their security operations
52%: Share of data breaches caused by external hacks	80%: Number of security pros who find it harder in 2019 to find people with security skills	90%: Share of security pros who believe their personal data is at risk

Table 1

References

Huseyin, M. (2019). Why humans are the weakest link in cybersecurity. *ACT*. Retrieved from https://www.treasurers.org/hub/treasurer-magazine/why-humans-are- the%E2%80%93weakest-link-in- cybersecurity#:~:text=Hackers%20prey%20on%20humans'%20psychological,efficiency%22%20makes%20us%20particularly%20vulnerable.

Kress, R. (2019). Why humans are still security's weakest link. *Accenture*. Retrieved from https://www.accenture.com/us-en/blogs/security/humans-still-securitys-weakest-link

Spitzner, L. (2019). This is why the human is the weakest link. *Security Awareness*. Retrieved from https://www.sans.org/security-awareness-training/blog/why-human-weakest-link

Vijayan, J. (2020, September 21). 31 cybersecurity stats that matter. Retrieved February 08, 2021, from https://techbeacon.com/security/31-cybersecurity-stats-matter