Name: Tay Lamell

Date: March 24, 2024

The Human Factor in Cybersecurity

BLUF

When it comes to securing information in the rapidly evolving digital world, there is no one method that will guarantee safety 100% of the time. However, there are steps that can be taken to ensure that the best efforts are being made around the clock, regardless of a company's size or available resources.

Introduction

One of the most common challenges about surviving the digital age, is how to keep up with the latest advances while on a budget. No matter if you're just someone trying to keep up with the latest phone model while still being able to pay rent, or a media company trying to figure out how to make a profit in the era of streaming, everyone is trying to figure out how to stay up to date with technological trends while not breaking the bank. While the challenge may be universal, there is no area in which it is more important, in my opinion, than cybersecurity. When it comes to cybersecurity, not keeping up with new advancements goes beyond being behind on trends, because being behind the times can put at risk the safety of employees and customers alike.

Background

In order to best answer the question of how I would allocate my funds if I had a limited budget to dedicate towards human training or cybersecurity technology proper, I first want to paint a brief picture of the impact cyber attacks have on businesses. In 2022, IBM published a

report which detailed the impacts cybersecurity breaches had on 550 organizations worldwide. According to the report, of the 550 organizations studied, 80% had experienced more than one data breach (IBM Security, 2022), costing on average $4.35 million per breach. The report also shared that 19% of the data breaches that were experienced by the companies had occurred due to stolen user credentials, and 45% of the total data breaches had occurred due to issues in cloud cybersecurity (IBM Security, 2022).

Per the article “2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics” from Cybercrime Magazine, 43% of reported cyber attacks are experienced by small businesses, more than half of whom go out of business in the months following (Morgan, 2023). Despite their difference in size, a report from tech company Cisco showed that small businesses aren’t too far behind large businesses in terms of their cybersecurity practices (Morgan, 2023). Still, small businesses face many of the same threats as larger corporations. Cyberattacks such as malware, phishing, and data leaks happen to all companies regardless of the number of employees and resources they have, and will likely increase in occurrence due to the various applications of artificial intelligence softwares.

The Human Factor

So what would I do if I were the Chief Information Security Officer (CISO) of a corporation with limited resources trying to navigate the sea of digital dangers? Where and how would I implement resources to help my organization mitigate the cyber threats that we will face even if we were to expand? Were I the CISO of an organization, I would focus primarily on ensuring that our number one resource, our employees, were trained as consistently as possible to ensure the best practices are being put into place. Without a strong foundation, even the most

advanced structures can crumble, and in terms of a company, this means making sure that the "human factor" to our cybersecurity measures are well-versed in secure practices.

The website Expert Insights took a look at the most pressing cyber threats faced by small businesses, and all five dealt in some way with the human user itself (Witts, 2024). Threats such as password breaches, the downloading of malware to company devices, and the exploitation of patch updates to devices all occur because the actual human using the device isn't doing what they should to help ensure such vulnerabilities don't get taken advantage of. The largest threat faced by smaller organizations remains email-based phishing attacks, and despite their increase in recent years, only 20% of small businesses worldwide give anti-phishing trains beyond once a year (Jones, 2023). Although humans will always make a mistake here and there, the chances of them occurring lessen with increased reinforcement or practice. Were I the CISO of one of these companies, I would hold trainings twice a fiscal quarter if for nothing else than to refresh employees on doing four simple things: update your passwords every two months, make sure said password is not something that can be easily guessed, update any and all company devices as soon as the updates are available, and never open or download anything that's coming from a source not pre-approved by the company.

Although more training could be costly, according to Sean Harris, the senior vice president for Intelligent Technical Solutions, "If you look at the cost of not doing security awareness training, it's pretty astronomical… the soft targets or the people are the weakest point (Mindanao, 2023)." With Intelligent Technical Solutions, via a 2022 summary of findings report from Verizon (*Summary of Findings,* 2022), going on to state that roughly 82% of data breaches are the result of human error (Mindanao, 2023), placing more resources in proactive

cybersecurity rather than in reactive measures is an easy decision to make. As the old saying goes: “The best defense is a good offense.”

The Digital Factor

The best trained soldiers can only last so long without the right equipment to back them up. No matter how much I would dedicate to training employees in cybersecurity practices, if the technology or softwares at their disposal wasn’t up-to-date, the training would be next to useless. Especially in a world where artificial intelligence is predicted to increase the amount and impact of existing cyber attack methods (*The Near-Term Impact of AI on the Cyber Threat*, 2024), the importance of up-to-date technological cybersecurity measures will only continue to grow. While there is a growing trend to cloud-based cybersecurity measures, the misconfiguration of an organization’s cloud-based infrastructure continues to be one of the top weaknesses of this approach (Brown, 2024). Keeping this in mind, I wouldn’t completely write off the merits of use of the cloud in my organization’s cybersecurity measures, but it wouldn’t be a priority.

Instead, if I were the CISO of an organization, I would once again turn my attention to tried and true foundational methods. By this I mean making use of two-factor authentication, the latest firewall models for company devices, continuous software patches to go hand-in-hand with efforts to ensure said updates are installed on company devices as soon as possible, and implementing efficient malware detection and protection software. Especially where more sensitive data is concerned, the use of biometric authentication to ensure only authorized users were accessing the information would not only help ensure that the data wasn’t falling into the wrong hands, but also help track who accessed what should a breach occur.

Conclusion

While I do not believe that any one method will ever be enough to guarantee the security of information in today's world, I do believe that there exist a plethora of ways for the best efforts to be made in attempting. Technology and knowledge of its use are far too common today to allow for a lack of resources to be a reason for any shortcomings in proactively defending against cyber threats. If anything, a restriction in resources should make organizations get creative in the ways they secure their data, even if said creativity must first present itself as a reinforcement of the basics.

References

Brown, S. (2024, February 6). *14 Cloud Security Issues, Challenges, Risks, and Threats*. StrongDM. https://www.strongdm.com/blog/cloud-security-issues-risks

IBM Security. (2022). *Cost of a Data Breach: Report 2022*. https://www.ibm.com/downloads/cas/3R8N1DZJ

Jones, C. (2023, December 8). *50 Phishing Stats You Should Know in 2024*. Expert Insights. https://expertinsights.com/insights/50-phishing-stats-you-should-know/

Mindanao, K. (2023, November 17). *How Much Does Security Awareness Training Cost (& Is It Worth It?)*. Intelligent Technical Solutions. https://www.itsasap.com/blog/cost-security-awareness-training

Morgan, S. (2023, May 24). *2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, and Statistics*. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-almanac-2023/

Summary of Findings. (2022). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

The Near-Term Impact of AI on the Cyber Threat. (2024, January 24). National Cyber Security Centre. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

Witts, J. (2024, February 15). *The Top 5 Biggest Cybersecurity Threats That Small Businesses Face and How to Stop Them*. Expert Insights.

https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/