EmergeIT

The Value of User Training in Modern Cybersecurity

Introduction

Modern businesses are comprised of people, processes, and technology. Effectively securing a business requires resiliency in all three areas, as neglecting one creates vulnerabilities, providing easy access for attackers to quickly undo all the hard work and resources invested into the other areas.

Traditionally, IT focused on the process and technology areas of cybersecurity that came naturally to technologists, such as intrusion prevention systems, firewalls, endpoint protection, multi-factor authentication, self-service password resetting, and identity management.

However, the people area, which is based on soft skills such as building user awareness and implementing training curriculums have often lagged in terms of focus and priority. This growing gap between the security of technology, and the resiliency of people has pushed threat actors to focus on human vulnerabilities, with between 85% and 90% of cyber attacks in 2021 beginning with social engineering techniques aimed at exploiting user behaviour[1,2].

Given the changing nature of cyber threats, modern businesses and IT providers alike can no longer afford to put their heads in the sand regarding their users' cybersecurity awareness and skills.

[1]https://www.graphus.ai/blog/91-of-cyber-attacks-come-by-way-of-phishing-know-the-different-types/
[2]https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

Modern threats

The primary cyber threats faced every day by employees are phishing attacks. Phishing is a form of social engineering used to steal data or compromise usernames and passwords of employees. An attacker will send an email, instant message, text message or social media message impersonating a trustworthy source, such as a reputable business or even another employee.

Their intent is to trick the recipient into clicking on a malicious link to either install malware such as ransomware or provide details which would allow the attacker to gain access to corporate data and circumvent other cybersecurity defences. Once access is established, it is generally a matter of time before a data breach occurs, which can be devastating to a business.

In these credential-based attacks, the employee is the first and most effective line of defence, as technical solutions may not identify attackers using legitimate employee credentials to access and steal corporate data.

Similarly, business email compromise attacks, in which attackers appear as legitimate contacts and request for the business to update supplier or employee bank details to divert legitimate payments, are rarely detectable by technical solutions. This leaves the cybersecurity knowledge of employees as the only form of defence for the business. Due to their ability to avoid technical defence solutions, and the low level of cybersecurity training found in many organisations, business email compromise attacks are now the leading cause of cybercrime losses for Australian businesses[3].

[3] https://www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf

Implementing an
Effective training curriculum

Implementing an effective cybersecurity training and awareness program does not have to be a costly endeavour, as security training should only takes a small percentage of the cybersecurity budget and can provide one of the best returns on investment.

Training can be made available to employees in many forms, including digital collateral such as user guides and infographics, interactive platforms like quizzes and gamification, and classroom-based tutoring.

When selecting a training methodology, businesses should consider how many bespoke topics need to be covered. Classroom-based training can be tailored extensively to meet very specific needs of a businesses, while interactive platforms generally provide curated offerings designed to meet regulatory and cyber -insurance requirements, while still allowing custom content to be combined with pre-made content. Off the shelf offerings are also available at low cost for smaller businesses with more generic requirements.

An effective security training curriculum contains four key elements:

1. Onboarding:

In the first few days after joining a company, employees should receive cybersecurity training covering their responsibilities, risks they will face in the job, and how to respond to threats.

2. Retraining:

Simply giving an initial overview during staff onboarding rarely has a lasting impact on habits. For it to be effective, staff should be trained regularly to refresh their knowledge, covering different areas of cybersecurity, as well as newly observed attack techniques.

3. Measuring:

Modern security training programs contain inbuilt mechanisms to test and measure their effectiveness. Regular simulations of phishing, social engineering, or malware outbreaks can highlight areas of strength and weakness in the curriculum. This can also show the ongoing improvements and return on investment of the training program.

4. Targeting:

Not all staff exhibit the same risk level to the organisation, so not all staff should be trained the same. Those with administrative credentials or access to finance systems may require more regular or intensive training, and if they perform poorly in simulations, they may be targeted for additional support.

Evaluating the ROI of cybersecurity training

Evaluating the ROI of any cybersecurity investment can be challenging and viewing it through the same lens as traditional IT investments gives incorrect results. Traditional IT investments, such as a new website, drive business productivity and revenue, so their ROI can be determined based on costs vs. additional sales generated.

Cybersecurity investment, however, provides risk mitigation. It should protect existing productivity and revenue, rather than create it.

Cybersecurity is best viewed similarly to physical security measures. Locks and alarms on a warehouse will not provide a direct revenue increase, but they protect profitability by preventing break-ins and theft.

Cybersecurity investments work in the same way.

Cybersecurity training provides risk mitigation against many forms of cyber threat–business email compromise, ransomware, and data breaches are the three most costly. While average costs are available for each of these types of attack, they heavily depend on business size and revenue. When determining the ROI of cybersecurity training, a business should first work with its IT provider to determine the likelihood and estimated cost of each of these attack vectors.

Example

Acme Co. is trying to determine the value of cybersecurity training for their business. To do this, they plan to determine the cost of ransomware attacks, business email compromise, and data breaches.

Cost of ransomware

Acme Co. has found that, on average, a successful ransomware attack affects 6 in 10 businesses each year[4], and stops them from operating for an average of approximately 20 days[5]. Due to the investment Acme has already made in cybersecurity, they judge their risk to be lower than average, and have estimated the likelihood at 3 in 10. They estimate the impact to be 5 days, or $25,000, of downtime.

Acme Co. also understands that 90% of cybercrime events start with an attack on users, so they attribute 90% of $7,500 to attacks aimed at users. Using these estimates the risk that user activity leads to a ransomware attack can be given a cost of $6,750 per year if no action is taken.

Acme Co. should now conduct a similar analysis of business email compromise attacks and data breaches to determine the full cost of the risk leaving their users untrained.

Improvements from user training

Acme Co. has cited research conducted across 23,400 businesses, which showed an 84% decrease in user susceptibility to cyber attacks after 12 months of security awareness training[6].

They determined that the value of security awareness training is equal to an 84% reduction in the cost of the risk of cybersecurity incidents originating from user poor behaviour.

This means that cybersecurity training will reduce the cost of ransomware risk by $5,670 in the first year.

By determining similar reductions in business email compromise and data breach risks, Acme Co. can determine the full value of cybersecurity training and compare this with the cost of implementing a curriculum.

Conclusion

IT and cybersecurity often focus on implementing new tools and solutions. While these are important, businesses must remember that 90% of modern cyber attacks are conducted against people, and are often not detected by technical solutions.

Fortunately, there is a low cost, high ROI solution to this problem–user security awareness training. While each organisation should conduct its own analysis of the costs and benefits of such a curriculum, given the drastic reduction in the likelihood of very costly risks, there are very few organisations who would not benefit from this investment.

[4] https://www.aic.gov.au/sites/default/files/2021-10/sb35_ransomware_victimisation_among_australian_computer_users.pdf
[5] https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/
[6] https://www.knowbe4.com/hubfs/2021-Phishing-by-Industry-Benchmarking-Report.pdf?hsCtaTracking=5545cbd3-4d37-4ec2-a812-0b2830feefbb%7C753ae012-a008-46ca-ade5-5035e74f6667

Contact Info

1300 348 287

hello@emergeit.com.au

www.linkedin.com/company/emerge-it-solutions-pty-ltd

EmergeIT