The Role of Employee Awareness in Preventing Business Cyber Risks

N. Arvinth, Research Associate, National Institute of STEM Research, Coimbatore, Tamil Nadu, India.
nagarajanarvinth@gmail.com, https://orcid.org/0009-0000-9798-9828

Introduction

The issue of cybersecurity is often presented from a technical standpoint – as something related to firewalls, encryption algorithms and intrusion detection systems. But there is substantial amount of evidence that shows a completely different picture. Namely, the majority of successful attacks utilize human behavior rather than purely technical flaws. It should be understood that employees, on all levels, are the key element in the cyber risk assessment of any organization. They may be considered the first line of protection, people able to detect and report suspicious activities before it turns into a disaster – but if not properly trained, these very same people may unintentionally become the way in for attackers to penetrate into the company's information systems.

The issue of employee awareness as a tool for reducing business cyber risks will be discussed in the current article. Understanding the Human Risk Factor

With growing popularity, cyber-attacks become more dependent on social engineering – the use of psychology to manipulate people into taking certain actions or disclosing confidential information. The reason why attackers choose such tactic is very simple: it is easier and more effective to convince a person rather than try to penetrate into a secure defense system. Why bother trying to break through the well-protected firewall when one carefully crafted email can do everything to get the user's login data?

There are several psychological techniques which social engineering uses in order to convince people to cooperate. In many cases, social engineers use authority, posing as executives or legitimate organizations and exploiting the employees' natural tendency to obey authorities. They also create a sense of urgency to prevent the users from analyzing the emails properly. They use familiarity, impersonating known colleagues, partners or companies to reduce the user's suspicions. Moreover, attackers use helpfulness targeting the customer support specialists who are trained to assist their customers.

Understanding these psychological mechanisms is necessary for building effective awareness campaigns.

The Relevance of Awareness for Today's Employees

There are a number of factors that increase the relevance of employee awareness today.

The level of sophistication of phishing scams has risen considerably. Unlike their predecessors, modern phishing attacks use sophisticated language free of errors, accurate branding, and a high level of personalization based on publicly available data or information from previous cyber-attacks, which makes them much harder to discern from genuine e-mails or phone calls.

Hybrid and remote working has broadened the scope of potential attacks. Employees who are not at the corporate office will have to deal with a different set of security threats, including unsecured internet connection, personal devices, and lack of physical availability of IT professionals.

Generative AI technologies have made it much easier to produce convincing scams. With help of generative AI software, an attacker can create convincing e-mails and even fake audio and video messages, undermining one's ability to recognize a phishing scam.

The cost of business email compromises continues to rise. These kinds of attacks rely exclusively on social engineering, which makes them impossible to protect against without raising employees' awareness.

The Cost of Inadequate Awareness

The organizations which ignore the creation of employee awareness put themselves at great risk. One single successful phishing attack will lead to credential theft, ransomware implementation, large-scale financial frauds, and data leakage of their customers or business operations. In addition to the cost of such an incident, the organization could face regulatory fines, legal consequences, and reputational issues that will take many years to repair.

However, it is worth noting that the expense of creating adequate employee awareness is only a tiny part of the possible costs of the incident, which is prevented by this process.

Building Effective Employee Awareness

Going Beyond Compliance-Focused Training

The traditional perspective in most companies has been that security awareness training is compliance-oriented training — a one-time yearly video and quiz, which is done mainly for compliance purposes. This is not an effective strategy, as behavior change is a process that requires constant reinforcement and development of skills rather than a one-time annual activity.

Phishing Simulation Exercises

Phishing simulation exercises can help employees identify phishing emails in a safe environment. Careful implementation,

which includes constructive feedback without negative repercussions, has been proven to significantly increase the capability of employees in recognizing actual phishing attempts.

Role-Based Training

There are various job roles in an organization that are exposed to risks. Hence, training for each role needs to be role-specific. For instance, finance and accounting personnel need training regarding verification of requests for payments, and invoice frauds that are common with them. For executives, training would focus on the techniques used in "whaling" attacks. The IT and help desk personnel need role-based training because of the threat of pretexting calls.

Fostering a Blame-Free Reporting Environment

One of the most important, but also the most overlooked aspects of any good awareness program is the creation of a culture that enables people to feel free from the threat of punishment or embarrassment when reporting mistakes or anything suspicious. The fear of punishment in case an employee becomes a victim of phishing, or clicks on something harmful, discourages people from reporting actual incidents, which delays the whole process of detection and response. A blame-free environment promotes quicker reports that are essential in minimizing the damage caused by real security breaches.

Ensuring the Practicality and Relevance of Security Training

Awareness training should be practical, applicable to the daily work of an employee, and provide practical guidelines, not just warnings. Practical information on how to identify a potential breach or what to do before clicking on something suspicious can help the employees to act immediately.

Multiple Channel Reinforcement

Awareness programs that effectively raise the level of employee security awareness should utilize multiple channels for their implementation – such as the use of short video presentations, emails, the display of posters and other signs in common areas, team meetings, and gaming elements. It is essential to have diverse channels used in order to keep the interest of employees up and provide them with continuous reinforcement of certain ideas through different ways of communication.

Role of the Management

Employees' awareness can be made much more effective if it is actively supported by the management of the organization. Participation of top executives in security training, discussion of security concerns in organizational communication channels, and even following security procedures themselves will help

demonstrate that security is an important element of organizational life, not just a necessary procedure.

Measuring the Effectiveness of Awareness Programs

In order for companies to verify that awareness activities have actually helped reduce their risks, it is important for them to measure behavior over time, not simply the rate of completion of awareness training. Such behavior metrics may include click rate on phishing simulations and its dynamics across repeated tests, the reporting rate of suspicious emails or activity in general, the amount of time that passes between occurrence of suspicious activity and reporting it, and qualitative data received from employees regarding the usefulness of training material. Measuring these metrics over time helps organizations determine where they need more emphasis and prove the worth of their efforts to the management.

Conclusion

Employee awareness cannot be regarded as something tangential to business cybersecurity; instead, it should be viewed as an essential pillar without which effective cybersecurity risk mitigation is simply impossible. As cyberattacks grow more sophisticated in terms of using various social engineering techniques, the awareness of individual employees becomes a very important factor affecting organizational security. An organization can turn its employees into its best defense mechanism by ensuring that they participate in continuous and practical awareness programs and that there is no blaming culture within the company.