Security training –
Is it a Requirement or boondoggle(Unnecessary)?

Abstract

Cybercrime is moving at high speed. A few years ago, cybercriminals used to specialize in identity theft, but now they take the control over organization's network, hack into our bank accounts, and steal tens or hundreds of thousands of dollars. Organizations of every size and type are at risk.

So, are you the next cyber-heist victim? Before becoming a victim, you really need a strong human firewall as your last line of defence. And the only solution to it is Cyber Security and it can only be obtained by "Security Training".

Before exactly coming to the conclusion whether security training is a requirement or boondoggle for the society, let's check out its pros or cons foremostly and then judge it.

Definition

Security awareness training is a form of education that seeks to equip members of an organization with the information they need to protect themselves and their organization's assets from loss or harm.

For the purposes of any security awareness training discussion, members of an organization include employees, temps, contractors, and anybody else who performs authorized functions online for an organization. Security training allows organizations to influence behaviour, mitigate risk, and ensure compliance. There are countless benefits of initiating security awareness training in your company.

Security awareness training is a way to achieve a level of knowledge that gives us control over security threats – but how effective is this type of training? Or it can be no beneficial to us. Let’s check this out in our next part.

Why Security Awareness Training

1. To be **aware of the organization's safety**, we must develop ourselves to be able to confront (face things as they are). Security training helps employees/ developers confront the fact that unwanted guys are trying to trick them and hack the data illegally. Once they confront that, they become aware and able to detect these scam emails and can take appropriate action like deleting the email or not clicking a link.

2. Security awareness training helps **people win more high-profile contracts**. This isn't conjecture. During CybSafe's recent survey of 250 IT decision makers, more than half said a business customer had made cyber security precautions part of either an existing contract or part of the RFP process in order to win the contract. More than two thirds said at least one customer had required the achievement of a recognised cyber security standard.

3. To be clear, compliance alone is no reason to introduce security awareness training. But more and more regulators are demanding specific industries implement security awareness training. **Compliance can be a happy offshoot of security awareness training.** Those who introduce compliance become more secure and, in many industries, meet a regulatory requirement.

4. The absence of security awareness training in one organisation makes other organisations vulnerable. It's a little like leaving our house door unlocked – with the keys to next door waiting inside. Security awareness training doesn't just benefit you. **It gives us the platform to behave in a socially responsible manner.** It benefits our customers, our suppliers and everyone else interlinked with our network.

5. Security awareness training doesn't just keep people safe at work. It keeps them safe in their personal life, too. For the most part, this particular benefit remains unseen. If security awareness training does what it's supposed to do, it isn't just an employer benefit. **It's an employee benefit, too**.

Benefits of Security Training

There’s really no question that training yields benefits. Let’s take a look at the some of the benefits of security awareness training.

1. Develop a Security-Focused Culture: When we offer any sort of training to our employees on a topic, it becomes an indirect message to them that it’s important. Regular training instills better habits and finally, when something becomes a habit, people will continue to follow it like it’s second nature. So, it helps to develop a security focussed work culture within the organization.

2. Empower Employees: As said, human make mistakes but it cannot be excused at all situations mainly when it speaks about the security system. To reduce the chance of human error and empower our staff, security awareness training is the solution. This training will teach them how to protect the company when using technology so there’s no guessing about what security steps should be taken.

3. Prevent Downtime: Whenever a breach or incident occur, it takes huge considerable time to investigate and repair it which is likely to wreck our workflows and deadlines. Downtime, even for only a few hours, can cause severe disruption. So, security training helps employees to save this precious time.

4. Increase Adoption: We can’t expect our employees to adopt security practices on their own by reading the policy from the very first day. Training leads our employees towards adoption as they are well-informed and understand risks once they’ve been through training. With more training comes greater adoption and a workforce-wide awareness, thus enhancing security throughout our organization.

5. Collect Risk Data by Driving Awareness: With more awareness of security risks, employees become a good source of great insight for collecting risk data. Gaining better knowledge of what types of risk employees are encountering, informs us of our security strategy.

Detriments of Security Training

1. Behaviour changes aren't guaranteed: Awareness doesn't always translate to changes in behaviour – at least not right away. Because old habits are hard to break, real change requires ongoing education, hands-on training, setting measurable objectives and offering rewards when goals are met.
2. Time and Resources Required: As we've gathered by now, cyber security awareness is a marathon, not a sprint. Awareness campaigns must be ongoing to drive home the message and reach new employees. Even if we're not spending a lot, creating and executing an effective campaign requires significant staff time and resources to create program materials, set goals, organize and execute training sessions, and measure progress.
3. Information Overload: We have to cut through a lot of noise to reach employees with our message. Work that seems more pressing and time-sensitive is thrown on their way. Cyber security news and advertisements compete with our information for head space. Even outside of work, we're up against the plethora of distractions that make up our digital world – texts, emails, blogs, social posts and more.

Summarizing

Cybercriminals take advantage of our natural human behaviour. By doing so, they have made phishing the most successful of cyber-attack methods. One of the reasons that we, as individuals, can be tricked by cybercriminals and trapped in their bags is that because our awareness of security is poor and we hardly bother about it. Let's prove this with the help of some statistical data and world records.

- In a Risk IQ report, it was found that poor security awareness is putting consumers at risk of data and identity theft. This poor security awareness also enters the workplace.
- For mobile users, it is an even worse condition. In studies, users clicking on mobile phishing links has increased by 85 percent since 2011.
- In the last few years, 76 percent of companies reported being a victim of a phishing attack.
- Verizon showed that 30 percent of phishing emails are opened and 12 percent of them are activated, i.e. the links are clicked on or the attachments opened.
- Understanding of secure password use is still poor. A report by Last Pass on password hygiene found that, on average, an employee will share a password with 6 other co-workers.

Cybersecurity threat reduction has come down to us at every field and their head throbbing problem. Many modern cyber threats use our own behaviour as part of the attack method. This behaviour needs to be changed to turn the tables on the cybercriminal. We have to use our best defence, our people, to help us protect our castle. By using a fun, engaging, and effective security awareness training program we can make sure our organisation and its people are prepared. Let the Defence Works help our business avoid cyber security breaches. Get employees fired up and ready to battle back.