CHAPTER 8

Creating a Security Culture

Every organization across every industry should take information security seriously. Security attacks can take place nearly every day and can result in exposing applications to the outside world. By establishing a strong culture of cybersecurity, enterprise organizations lay a foundation that leads to decreased number of threats in the long run.

The previous chapter covered automated security monitoring, including setting up a security policy using Azure Monitor and Azure Sentinel.

This chapter covers the following topics:

- Leadership support
- Training

Leadership Support

Organizations need a leader, someone who is responsible for creating a culture of security. Building a security culture must be handled as a project, with support from the highest level of executives. Enterprise organizations can start by executing these steps:

- Recruiting the right people to run the program
- Determining the project scope
- Measuring the security awareness and interests in the organization
- Creating actions of execution to reach goals
- Creating deadlines for different actions to determine the start and end dates

S. Lad, *Azure Security For Critical Workloads*, https://doi.org/10.1007/978-1-4842-8936-5_8

- Defining metrics
- Creating success factors

Establishing a security culture across an enterprise organization creates an environment where management and employees speak the same language and have a common understanding of their own business and strategy. A security culture must be built together with the employees.

People, processes, and technologies are often seen as the three pillars of information security. Although a proper balance between the three is essential, the aspects of internal culture and training as they relate to the "people" pillar are often overlooked. Not focusing on the people in an organization leads to reduced effectiveness of processes and technologies. See Figure 8-1.

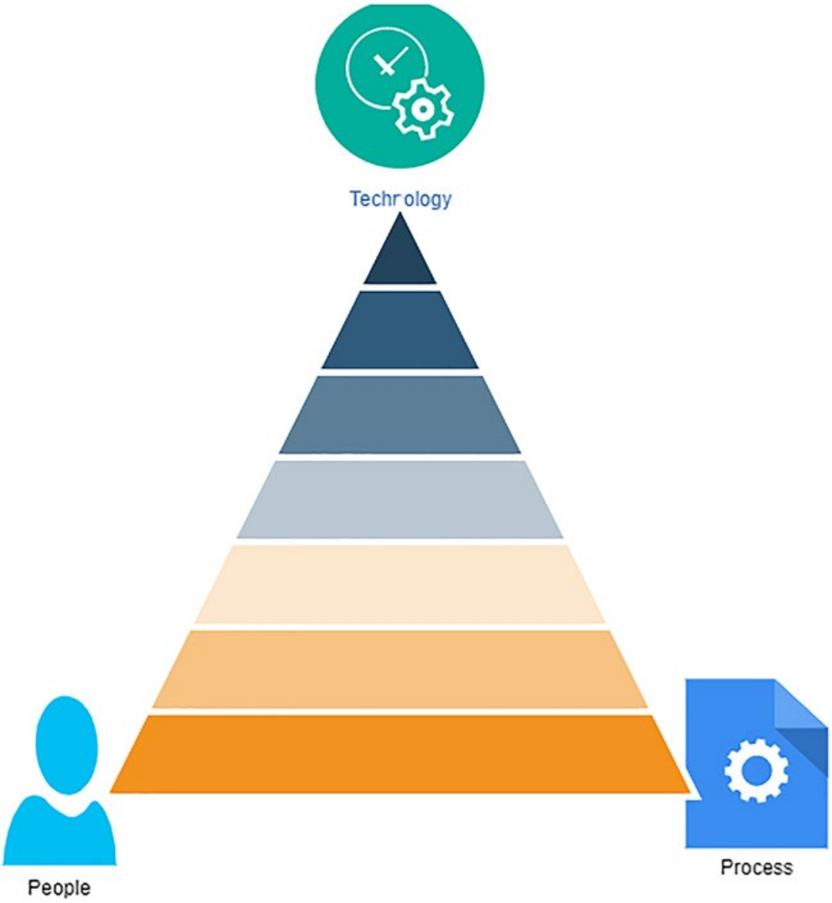

Figure 8-1. *Security culture: people, processes, and technologies*

Organizations should seek to establish a culture where employees understand the importance of cybersecurity and define policies, procedures, and controls. Modifying the existing corporate culture to incorporate security awareness will require support from the leaders of the following items:

- Encourage the initiative to create security culture: Stakeholders within the organizations should promote a security awareness culture to maintain a positive attitude toward information security. Support for security measures expected by the enterprise will help the company achieve their goals. In addition to that, business managers should look for employees who are not working with the right attitude and help create a positive and proactive environment.
- Lead by example: Regardless of what leaders tell employees, if they don't follow the defined processes, policies, and controls then it will create the wrong impression among the employees and they will become less serious about the security culture.
- Fundamental understanding of the information security: Stakeholders in the organization may not be security experts, but they should be provided with additional training to get a foundational understanding and knowledge of security. Having basic knowledge of security among the employees and between the leaders can mitigate the possibility of individuals involved in security incidents.
- Proactive leadership involvement: Stakeholders in the organization should create a proactive plan for an incident response plan, business continuity plan, and other key procedures. Every stakeholder might not be aware of the procedures, but being aware about such information allows leaders to contribute to the organization.

A security awareness culture will encourage employees to question skeptical activities, become more resilient to social engineering attacks, and adhere to the defined policies, procedures, and controls. See Figure 8-2.

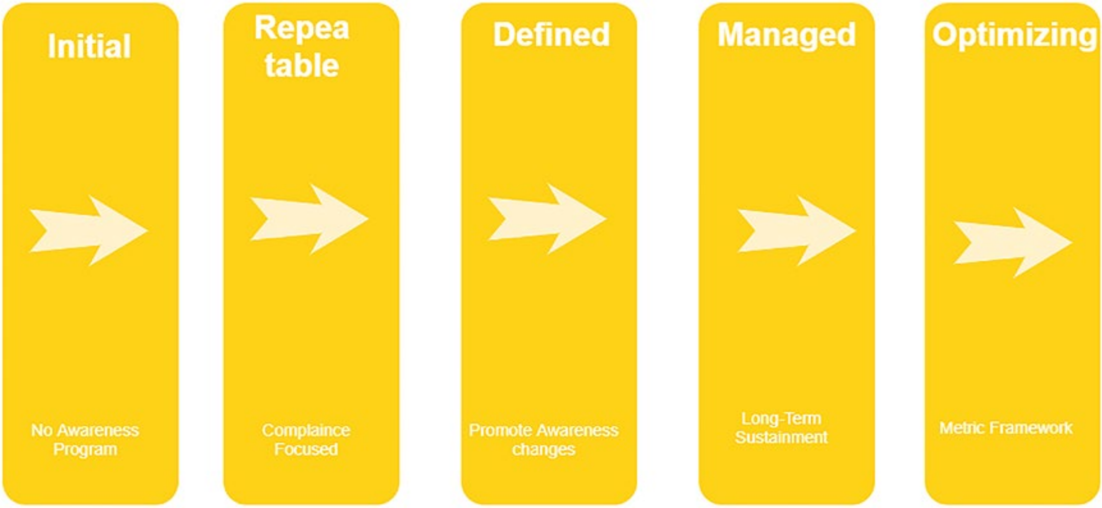

Figure 8-2. *Security culture: people, processes, and technologies*

All the teams in the enterprise organization can run a mix of technical, administrative, and professional programs to improve overall security. Let's look into a few of the possible initiatives that enterprise organizations can follow:

- Gap Analysis: First, you need to understand the existing gap analysis, which is where the organization stands today. By performing the gap analysis, you can easily find what needs to be done and when.
- Needs differ for each department: Different departments and disciplines have different needs as per their knowledge and skills. It is also advised to run the safety program to create an iterative culture building process across the departments so that it is easier to see if such a safety program has the desired effect.
- Improve security competence: You can perform many activities to spread awareness across the organization to improve the overall security. Metrics should be defined for each activity to understand if the goal has been achieved or not and to improve the overall security competence.
- Games: Cost and complexity of developing games today is lower than ever. We can create both computer games as well as board games related to security awareness and quiz to improve security awareness.

- Ethical hacking: Hire a company that can test physical security, employee goodwill, and your public-facing systems to avoid phishing attacks.

Training

In order to improve the overall security culture and security awareness, you should train employees and keep them up-to-date about possible security issues and how to avoid them.

- Be flexible to the corporate culture: Creating a security culture differs not only from organization to organization but also within the departments and management levels.
- Instead of creating a fixed path to drive security training across the organization, it is better to sit together with senior stakeholders and employees and create a security awareness program.
- Validate training to achieve organizational goals: Phishing attacks, data breaches, and CEO fraud attacks are the major concerns by most practitioners across the world. Undertrained employees lack the ability to detect security threats and don't have a correct understanding of a security attack. Be ready to focus not only on the best training but also to train for all possible scenarios.
- Replicate phishing scenarios at random intervals: Phishing simulation techniques are really important for maintaining the workforce's phishing defense. Simulating phishing scenarios will enable organizations to understand and predict employee behavior against the attack and track behavioral changes over time.
- Frequency of the training: Security training should happen often, to keep security a top priority for everyone. Although there is no magic frequency for such training, short trainings distributed frequently are most effective and best able to create a security culture across an organization. See Figure 8-3.

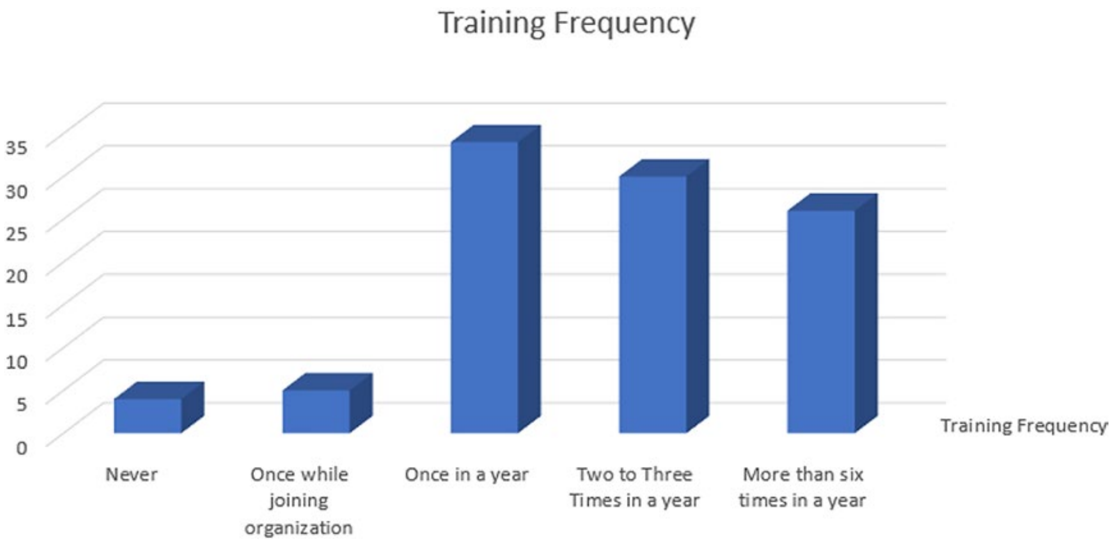

***Figure 8-3.** Security training frequency*

- Focus on employee's behavioral changes: Security professionals view technical infrastructure as a more useful tool for avoiding security incidents rather than creating security-aware training. It is impossible to replace security training with the technical controls. Physical infrastructure is great at preventing security attacks until a phishing email comes into an employee's inbox. It is worth considering security training as the outcome of behavioral changes rather than as a compliance requirement. This behavioral change is not the ultimate goal of the training, but it is measurable. Focus on the phishing rates, number of employees who report to an email, and events blocked by the endpoint protection to back security awareness with data. See Figure 8-4.

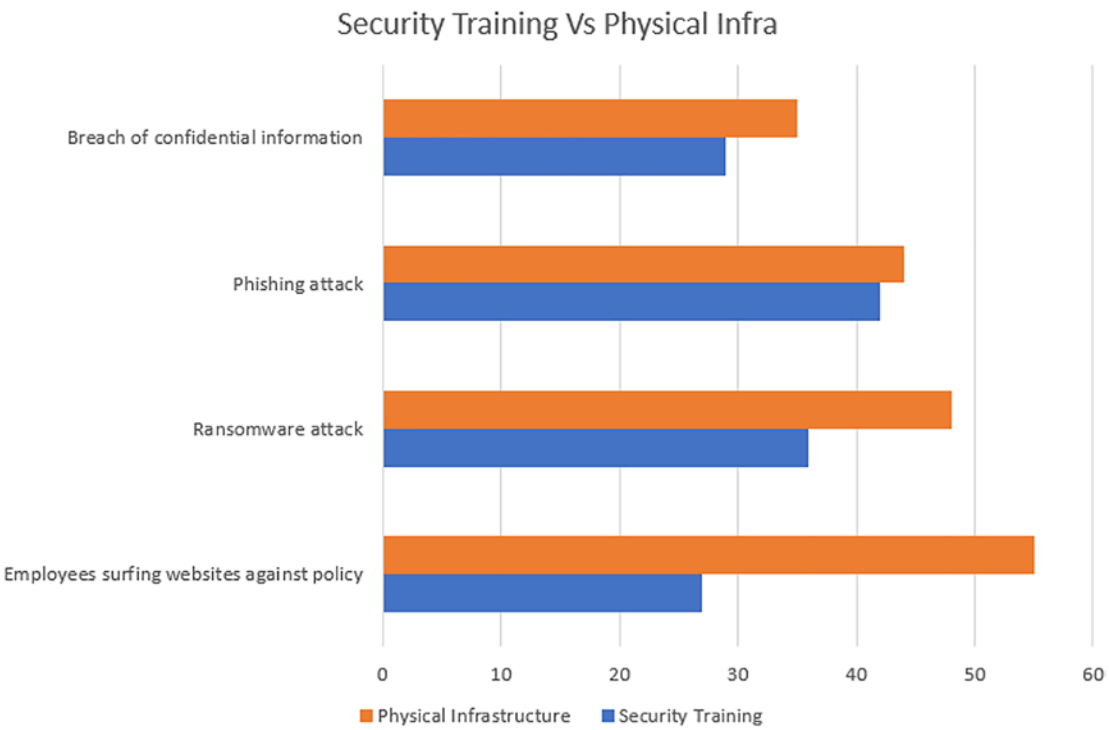

Figure 8-4. *Security training vs physical infrastructure*

- Keep faith in employees to tackle security challenges: Security professionals report low confidence in the company's employees and stakeholders to handle phishing attacks. Having limited confidence in employees' ability to handle security threats makes it important to treat security incidents as an opportunity rather than showcasing them as the inability of employees to tackle security issues.

Conclusion

This chapter explored how to create a security culture across your organization with the support and vision from the stakeholders and organizational leaders. In addition to this, you have to train employees across your organization to be able to recognize and tackle security challenges.