6.7: The Human Element

Technical controls provide the first line of defense, but employees also make or break an organization's security posture.

Definition: Social Engineering

Social engineering refers to psychological manipulation tactics that cybercriminals use to trick people into divulging confidential information or performing actions that compromise security.

Human errors, whether intentional or not, contribute to a large portion of security incidents. Here are some statistics:

- The 2023 Verizon Data Breach Investigations Report found that 74% of all breaches include the human element, with people involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering. (Verizon, 2023)
- An IBM study found that 95% of cybersecurity breaches are due to human error. (IBM, 2022)

Organizations need to create a strong security culture that engages all personnel is vital. Key elements include:

- Security Awareness Training - Regular training ensures employees are mindful of threats and equipped with best practices. This guards against risky behavior like password reuse or phishing susceptibility. Training should cover malware, social engineering, sensitive data handling, incident reporting, and more.
- Security Policies - Policies codifying expected behaviors, asset management, access controls, and incident response help govern actions and promote accountability. Employees should affirm their knowledge of policies.
- Organizational Buy-In - Management must spearhead security and exhibit commitment.
- Employees are more attentive to policies when leaders endorse their significance. A top-down culture of vigilance permeates the firm.
- Empowered Security Team - Security staff should have executive backing, resources, and visibility. This empowers them to enforce controls, audit processes, and guide strategic decisions. Their expertise steers the ship.
- Security-Minded Hiring - Personnel choices matter. Screening candidates reduces insider threat risks. Those valuing security and ethics are preferable.

A strong security culture that engages all personnel, at all levels, is a key approach to reconcile human strengths and fallibility to combat human errors and social engineering.

References:

Verizon. (2023). 2023 Data Breach Investigations Report. Retrieved on August 6, 2023, from verizon.com

IBM (2022). Cost of a Data Breach Report 2022 from ocedic.com