Cybersecurity Training

Ryan Coon

CYB-690

Dr. Kimberly Ford

October 8, 2025

**Culture of Security Awareness**

Creating a culture of security awareness through a Christian worldview perspective emphasizes the importance of stewardship, integrity, and community, fostering an environment where all members—management, staff, clients, and stakeholders—are engaged in safeguarding information and resources.

From a Christian perspective, security awareness is not merely a technical requirement but a moral obligation. It encourages individuals to act responsibly and ethically, recognizing that their actions can impact the broader community. For instance, training programs can be designed to reflect biblical principles, promoting ethical behavior and vigilance in cybersecurity practices. This includes understanding the significance of protecting sensitive information and the potential consequences of negligence.

Collaboration is essential in this framework. By fostering open communication and teamwork, organizations can ensure that everyone is on the same page regarding security protocols. Management must demonstrate commitment to security initiatives, which can inspire buy-in from staff and stakeholders. When leaders model ethical behavior and prioritize security, it creates a ripple effect throughout the organization, encouraging all members to take ownership of their roles in maintaining a secure environment.

Moreover, involving clients and stakeholders in security discussions reinforces the idea that security is a shared responsibility. By educating them about potential risks and the importance of cybersecurity, organizations can build trust and enhance their overall security posture.

**Physical and Information Security Risks**

Physical security risks pose tangible threats to an organization's assets, encompassing dangers like theft, vandalism, and unauthorized access to physical spaces. For instance, a break-in at a data center could result in the loss of critical hardware and sensitive data. To mitigate these risks, organizations should implement robust access control measures, such as key card systems or biometric scanners, to restrict entry to sensitive areas. Surveillance systems, including cameras and alarm systems, can act as a deterrent and provide evidence in the event of an incident. Furthermore, secure storage solutions, like locked cabinets and safes, are crucial for protecting valuable items and confidential documents. Employee training plays a vital role, educating staff on recognizing suspicious behavior and the importance of maintaining physical security protocols.

Information security risks involve threats to digital assets, including data breaches, malware infections, and phishing attacks. These threats can originate from both internal and external sources, potentially leading to data loss, financial damage, and reputational harm. To protect against these risks, organizations should prioritize data encryption to safeguard sensitive information both during transit and while stored. Regular software updates are essential to patch vulnerabilities and prevent exploitation by malicious actors. Strong password policies and multi-factor authentication enhance security by making it more difficult for unauthorized individuals to access systems and data. Moreover, an incident response plan is critical, outlining steps to be taken in the event of a security breach, including containment, investigation, and recovery.

**Phases of System Development Life Cycle**

The System Development Life Cycle (SDLC) is a structured approach to software development that encompasses several key phases, each with its own security-related concerns. Understanding these phases is crucial for integrating security measures effectively throughout the development process.

Initiation: This phase involves defining the project scope and objectives. Security concerns at this stage include identifying potential threats and vulnerabilities that could impact the system. Stakeholders should assess risks and establish a preliminary security framework to guide the project. Engaging security experts early can help in recognizing critical security requirements.

Requirements: During this phase, detailed functional and non-functional requirements are gathered. Security-related issues include defining security requirements such as authentication, authorization, and data protection. It’s essential to involve security professionals to ensure that all potential threats are considered, and appropriate security measures are documented.

Design: In the design phase, the system architecture is created based on the requirements. Security concerns here focus on designing secure system components and interfaces. This includes implementing security controls like encryption, secure coding practices, and access controls. Threat modeling can be beneficial to identify and mitigate potential security risks in the design.

Development: This phase involves actual coding and building the system. Security issues during development include ensuring that developers follow secure coding standards to prevent vulnerabilities such as SQL injection or cross-site scripting. Regular code reviews and static code analysis can help identify security flaws early in the development process.

Testing: The testing phase is critical for identifying and fixing security vulnerabilities. Security testing should include penetration testing, vulnerability assessments, and security audits to ensure that the system is resilient against attacks. It’s important to validate that all security requirements are met and that the system behaves as expected under various threat scenarios.

Deployment: Once testing is complete, the system is deployed to a production environment. Security concerns during deployment include ensuring that the deployment process is secure and that sensitive data is protected during transfer. Additionally, access controls should be enforced to limit who can deploy and manage the system.

Operations and Maintenance: After deployment, the system enters the operations and maintenance phase, where it is monitored and updated. Security issues here involve ongoing monitoring for security incidents, applying patches, and updating security measures as new threats emerge. Regular security assessments and user training are essential to maintain a strong security posture.

Disposal: Finally, when the system is no longer needed, it must be disposed of securely. Security concerns include ensuring that all sensitive data is properly deleted or destroyed to prevent unauthorized access. Organizations should follow data sanitization standards to mitigate risks associated with data breaches during disposal.

**Critical Electronic Device Proper Use**

The proper use of critical electronic devices and communication networks is essential for maintaining the integrity, availability, and confidentiality of information systems. These devices, which include routers, switches, and servers, must be managed with a focus on security and efficiency. First and foremost, organizations should implement strong access controls to ensure that only authorized personnel can interact with these devices. This includes using secure authentication methods such as multi-factor authentication and regularly updating passwords to mitigate unauthorized access.

Moreover, it is crucial to employ encryption protocols for data transmission across communication networks. This protects sensitive information from interception during transit. Regular software updates and patches are also vital, as they address vulnerabilities that could be exploited by cyber threats. Additionally, organizations should conduct routine security assessments and audits to identify potential weaknesses in their infrastructure.

Training staff on best practices for using these devices and networks is equally important. Employees should be aware of the risks associated with phishing attacks and social engineering tactics that could compromise network security. Furthermore, implementing a comprehensive incident response plan ensures that organizations can quickly address any security breaches or failures in communication networks.

**Critical Information Proper Handling**

The proper handling of critical information is essential for safeguarding sensitive data and ensuring compliance with legal and ethical standards. This process begins with identifying and classifying information based on its sensitivity and the potential impact of unauthorized access. Organizations should implement strict access controls to ensure that only authorized personnel can access critical information, utilizing methods such as multi-factor authentication and regular password updates to enhance security.

Additionally, it is crucial to maintain a clear inventory of where sensitive information is stored, whether in physical files, electronic devices, or cloud storage. This practice not only aids in data management but also facilitates compliance with data protection regulations. When it comes to data disposal, organizations must adopt secure methods to prevent unauthorized access to personally identifiable information, such as shredding physical documents and using data-wiping software for electronic files.

Training employees on the importance of information security and best practices for handling sensitive data is vital. This includes educating them about potential threats like phishing attacks and social engineering tactics. Furthermore, organizations should establish a comprehensive incident response plan to address any breaches swiftly and effectively, minimizing potential damage.

References:

Andrews, L. (2024, May). *Handling Sensitive Information and Confidentiality in Security Operations*. Agsprotect.com; AGS Protect. https://www.agsprotect.com/blog/handling-sensitive-information

CISA. (n.d.). *Protect the Physical Security of Your Digital Devices | CISA*. Www.cisa.gov; U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices

CISA. (2024, December 3). *Enhanced Visibility and Hardening Guidance for Communications Infrastructure | CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

Department of Homeland Security. (2024). *Secure Cyberspace and Critical Infrastructure | Homeland Security*. U.S. Department of Homeland Security. https://www.dhs.gov/archive/secure-cyberspace-and-critical-infrastructure

Federal Trade Commission. (2016). *Protecting Personal Information: A Guide for Business*. Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

Gowing, G. T. (2023). *Cybersecurity from a Christian Worldview*. Www.letu.edu. https://www.letu.edu/academics/arts-and-sciences/story-cybersecurity-glyn-gowing.html

Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., & Gulick, J. (2008, October 16). *Security Considerations in the System Development Life Cycle*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/64/r2/final

Palo Alto Networks. (n.d.). *What Is Secure Software Development Lifecycle (Secure SDLC)?* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-secure-software-development-lifecycle

Poteete, P. (2020). *The Value of Christian Principles in Cybersecurity Education*. Geneva.edu. https://www.geneva.edu/blog/program-spotlight/the-value-of-christian-principles-in-cybersecurity-education

Red Hat. (2022, September 30). *Security in the software development lifecycle*. Www.redhat.com. https://www.redhat.com/en/topics/security/software-development-lifecycle-security

SANS. (2022). *Critical Controls for Effective Cyber Defense*. Sans.org. https://www.sans.org/media/critical-security-controls/cag4-1.pdf

Scrut Automation. (2022, October 13). *Creating a Cyber Security Mindset*. Scrut Automation. https://www.scrut.io/post/cyber-security-culture-csc

SentinelOne. (2025, July 30). *Information Security Risks: Impacts and Best Practices*. Sentinelone.com; SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/information-security-risks

Turn-key Technologies Staff. (2024, July 8). *Guide to Physical Security: Common Physical Security Threats and How to Mitigate Them*. Turn-Keytechnologies.com; Turn-Key Technologies. https://www.turn-keytechnologies.com/blog/guide-to-physical-security-common-physical-security-threats-and-how-to-mitigate-them