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.

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**

RC Cybersecurity relies on a critical infrastructure of electronic devices and communication networks to function effectively. These essential components enable communication, data storage, and the protection of consumer information, ensuring smooth and optimal operations. This infrastructure encompasses a range of devices, including network servers (application, database, and web servers), routers, firewalls, landlines, mobile phones, switches, computer systems, and Intrusion Detection and Prevention Systems (IDPS).

These devices are interconnected through the company's segmented network. This network segregation is designed to limit the impact of potential cyber intrusions by controlling the flow of incoming and outgoing traffic to RC Cybersecurity's critical infrastructure.

The use of these electronic devices and communication networks is governed by a set of standards established by regulatory bodies such as PCI-DSS, NIST, HIPAA, FISMA, and ISO 27001. Compliance with these regulations is paramount for RC Cybersecurity to maintain full compliance, mitigate data breaches, and defend against cyberattacks. Building upon these regulatory standards, RC Cybersecurity has also developed its own internal standards and rules to further govern the usage of its critical devices and communication networks.

**Critical Information Proper Handling**

As a compliant organization, RC Cybersecurity adheres to a comprehensive framework of rules and standards derived from HIPAA, PCI-DSS, GDPR, FISMA, NIST, and ISO 27001 in the management of consumer data. We prioritize the secure storage of Protected Health Information (PHI) and other sensitive consumer data, implementing robust controls aligned with these regulatory requirements.

For example, RC Cybersecurity strictly adheres to the required controls when processing consumer credit and debit card information and all related financial records. We utilize a dedicated server with integrated PCI-DSS APIs to facilitate credit/debit card transactions, ensuring secure processing. Similarly, all medical patient records are stored on a separate, secure server, with comprehensive HIPAA controls in place. This multi-layered approach is designed to safeguard PHI and prevent data breaches.

Furthermore, RC Cybersecurity maintains vigilant monitoring of incoming and outgoing network traffic within its critical information infrastructure. Our systems undergo regular audits to ensure optimal performance, identify necessary updates, and proactively address any required patching or routine maintenance. In addition, all data belonging to European consumers is managed in strict compliance with the guidelines and regulations of GDPR

**Action Plans and Procedures to Recover or Reestablish Critical Electronic Devices and Communication Networks**

Creating a robust Information Technology Disaster Recovery Plan (IT DRP) is essential, and it should be developed in partnership with your Business Continuity Plan. The process begins with a Business Impact Analysis, which helps establish the priorities and Recovery Time Objectives (RTOs) for your IT systems. These objectives are crucial for determining how quickly you need to recover your systems. Technology recovery strategies are then developed to ensure the swift restoration of hardware, applications, and data, aligning with the needs of business recovery.

Consider the vast amounts of electronic information RC Cybersecurity manages; much of it is important, and some is critical for survival. The potential impact of data loss or corruption due to hardware failures, human error, cyberattacks, or malware can be severe. Therefore, a comprehensive plan for data backup and restoration is indispensable.

Recovery strategies should encompass all aspects of Information Technology (IT) systems, including applications and data. This involves your entire IT infrastructure: networks, servers, desktops, laptops, wireless devices, and connectivity. The priorities for IT recovery must mirror the priorities established during the Business Impact Analysis for business functions and processes. It's also vital to identify the IT resources needed to support time-sensitive business functions. The recovery time for any IT resource should directly correspond to the recovery time objective for the business function or process that relies on that resource.

IT systems rely on a combination of hardware, software, data, and connectivity. The failure of any single component can disrupt operations. Consequently, recovery strategies must account for potential losses in various areas, such as the computer room environment (including security, climate control, and backup power), hardware (networks, servers, computers, and peripherals), connectivity to service providers (fiber, cable, wireless), software applications (like email and enterprise resource management), and, of course, data and the restoration process itself. A well-prepared IT DRP is fundamental to safeguarding your data and ensuring the continued success of your business.

**Risks Resulting from Insecure Behavior of Employees**

Insider threats pose a particularly significant risk to organizations. Unlike external attackers who must breach security perimeters, insiders already possess legitimate access to computer systems and networks, essential for their daily work. This inherent access, however, creates a vulnerability. If misused or exploited to harm the organization, the consequences can be devastating and financially crippling.

Insiders often have a strategic advantage when attempting to compromise an organization. They are typically familiar with the company's data structure, including the location of sensitive intellectual property. Furthermore, they may understand how information is protected, potentially enabling them to bypass security measures more easily. Because insiders already have direct access to the organization and its network, they don't need to overcome external barriers. This makes insider threats more challenging to defend against than external attacks. Their actions can also be difficult to detect, as their activities often blend seamlessly with normal business operations.

The potential risks associated with insider threats are substantial, including the loss of sensitive consumer data, a decline in consumer trust and confidence, and the imposition of substantial fines from regulatory bodies such as HIPAA, GDPR, and PCI-DSS, potentially costing millions of dollars.

**Certification and Accreditation for IT Professionals**

Certifications and accreditations play a crucial role in validating the skills and knowledge of IT professionals. These credentials not only enhance career prospects but also demonstrate a commitment to ongoing professional development. Among the most recognized certifications is the CompTIA A+, which serves as an entry-level credential for IT support professionals, covering essential skills in hardware, software, and troubleshooting. For those focusing on cybersecurity, the Certified Information Systems Security Professional (CISSP) is highly regarded, showcasing expertise in designing and managing an organization's security posture. Additionally, the Certified Information Systems Auditor (CISA) certification from ISACA is pivotal for IT auditors, emphasizing the importance of auditing, control, and security of information systems.

The Cisco Certified Network Associate (CCNA) certification is essential for networking professionals, validating their ability to install, configure, and troubleshoot networks. As cloud computing continues to grow, certifications like the AWS Certified Solutions Architect and Microsoft Certified: Azure Solutions Architect Expert are increasingly sought after, reflecting proficiency in cloud services and architecture.

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