Study Unit Four

Cybersecurity Risks and Controls

This study unit covers **Section A. Engagement Planning, subsection 3.c.-d.**, in The IIA's Part 2 CIA Exam Syllabus. This section is 50% of Part 2.

The **learning objective** of Study Unit 4 is

- Plan the engagement to assess key risks and controls

As the third of eight study units on engagement planning and the second focusing on information technology systems, this study unit underscores the need for internal auditors to understand the expanding cybersecurity landscape when planning engagements to assess key risks and controls. The risks posed by mobile and Internet of Things (IoT) devices, cloud computing platforms, various forms of malicious software, and the imperative for effective incident response strategies significantly broaden an organization's threat landscape. These interconnected vulnerabilities necessitate a careful assessment of security controls, policies, and governance processes.

By comprehending how these emerging technologies and threats interrelate, internal auditors can identify potential vulnerabilities during the planning phase. Mastering these subjects enables internal auditors to enhance the organization's security posture, safeguard critical data and systems, and maintain stakeholder trust throughout the engagement planning process.

4.1 Cybersecurity Risks

Author's Note

Understanding the cybersecurity risks associated with mobile and Internet of Things (IoT) devices, as well as cloud computing platforms and services, is crucial for an internal auditor because these technologies significantly expand an organization's threat landscape. As organizations increasingly integrate these devices and services into their operations, they introduce vulnerabilities such as weak authentication, poor password management, inconsistent security standards, and unique cloud-specific risks. Internal auditors must be able to assess these risks to ensure that effective controls are in place to protect the organization's information assets and to maintain compliance with relevant regulations.

By being knowledgeable about these emerging cybersecurity challenges, internal auditors can provide critical insights and recommendations that enhance the organization's security posture, ensuring the integrity, confidentiality, and availability of vital data and systems.

Cybersecurity is the prevention of damage to, protection of, and restoration of (1) computers, (2) electronic communications systems and services, (3) wire communication, and (4) electronic communication, including information contained therein. The purpose is to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. This definition identifies the challenges of protecting information assets and systems.

- Nonrepudiation refers to the assurance that someone cannot deny the validity of his or her actions or the receipt of a specific message or transaction. This concept is crucial in ensuring accountability and authenticity in digital communications and transactions.

Many technologies, platforms, and services have related risks. The following sections describe some of their vulnerabilities and risks.

Mobile and Internet of Things (IoT) Devices

IoT devices are nonstandard computing devices that connect wirelessly to a network and have the ability to transmit data. Traditional cell phones, tablets, laptops, and other devices were designed to be wireless. But smart watches, health devices, home security systems, and even thermostats now may be wireless. Cybercriminals can gain unauthorized access to a network through security flaws in these devices. Many of these risks are briefly described below and on the following pages because of the broad categories of risks related to devices connected to the Internet.

- **Weak authentication** – Lack of authentication for verifying the identity of a user, process, or device, often as a prerequisite to allowing access to system resources.
- **Poor password management** – Users repeating the use of combinations of usernames and passwords. Many passwords are subject to password cracking techniques.
- **Lack of encryption** – IoT devices typically fail to employ encryption.

- **Low processing power** – IoT applications typically have a smaller data footprint and require less data storage, preventing them from using security features such as firewalls, virus scanners, and end-to-end encryption.
- **Use of legacy assets** – Applications that were not initially designed for web connectivity may not be compatible with newer encryption and other security safeguards, despite attempts at updates.
- **Shared network access** – IoT devices may rely on the same network as other end-user devices and may be used to access sensitive data or other applications.
- **Inconsistent security standards** – No single security standard exists for IoT devices. The lack of consistent protocols and guidelines makes machine-to-machine communication riskier.
- **Patch management deficiency** – A common challenge for both IoT and mobile devices is maintaining a consistent and effective process for applying necessary updates to firmware, operating systems, and security patches. This deficiency leads to increased security vulnerabilities because these devices often fail to receive timely updates that address various bugs and potential exploits.
  - Addressing this deficiency is critical to ensuring the security and optimal performance by implementing structured and frequent patch management practices.
- **Gaps between mobile networks and the cloud** – IoT devices typically interact with cloud-based applications. They reside on mobile networks and, although the mobile network and the cloud application may be secure, transmissions may still be vulnerable to interception and malware attacks. Messages must flow from the mobile network, through the public Internet, and to the cloud application and vice versa.
- **Limited device management** – Organizations lack the visibility and control required to determine whether individual devices have been compromised. For detection of anomalous activity, they rely on end users who may not recognize whether their devices have been compromised, thus exposing the organization to a security risk.
  - A related concern is **shadow IoT**, the deployment of devices without any knowledge or official support of the organization.
- **Physical vulnerabilities** – IoT devices and hardware that are in regular contact with people may be exposed to increased risk of tampering and unauthorized access. One risk is theft of physical assets, such as SIM cards or data storage devices.
- **Growth of IoT environment** – The exponential growth rate of IoT connected devices, coupled with limited device management and inconsistent IoT device security standards, creates a higher risk security environment.
- **IoT ransomware vulnerabilities** – Ransomware can affect all types of organizations. Hackers infect devices with malware to gain unauthorized access to sensitive data and threaten to keep, delete, or expose the data unless ransom is paid.
- **Data leakage** – When an application (riskware) requires mobile users to grant broad permissions for its use, data leakage may occur. Users typically do not review security concerns prior to granting these permissions. The result is that the application developer is capable of injecting code native to mobile operating systems to surreptitiously transfer data across networks.

- **Network spoofing** – Fake network access points are established in high-traffic public locations. These connections appear to be legitimate Wi-Fi connections. But cybercriminals can obtain account login credentials, including usernames and passwords, to further hacking efforts.
- **Improper session handling** – Mobile applications use tokens to avoid repeated identity access verification for usage of applications. Users can perform multiple actions without having to reauthenticate their identity. If a mobile application unintentionally shares session tokens, improper access could result from malicious agents impersonating legitimate users.
- **Spyware** – This software is surreptitiously installed into an information system or mobile device to gather information on individuals or organizations without their knowledge.
- **Physical vulnerabilities** – These result from mobile devices and hardware that are subject to regular contact with people. This exposure increases the risks of tampering and unauthorized access. The results may be theft of physical assets, such as SIM cards or data storage devices, and physical penetration to access a network.

Cloud Computing Platforms and Services

Cloud computing is the on-demand provision of IT services over the Internet with the ability to pay for services on an as-needed basis. Instead of owning and managing physical servers and data centers, an organization can use a cloud provider to access technology services such as computing power, storage, and databases on an as-needed basis.

The three main types of cloud computing are as follows:

- **Infrastructure as a service (IaaS).** Access to (1) networking capabilities, (2) virtual or dedicated hardware, (3) operating systems, and (4) data storage capabilities is provided so that an organization can deploy infrastructure for its own requirements.
- **Platform as a service (PaaS).** An organization's hardware and operating systems (infrastructure) are managed as a service, thus freeing the organization to deploy and manage its software.
- **Software as a service (SaaS).** An organization's infrastructure and applications are managed by the cloud service provider. Entities using SaaS are solely interested in the actual use of the underlying applications and seek efficiencies from not having to oversee or deploy and manage infrastructure or the applications.

The following are risks generally applicable to cloud computing platforms and services:

- Data security is a risk for **cloud service providers (CSPs)**. They store data in remote servers, and data leakage may occur due to unauthorized access or other inadequate data security practices.
- Identity and access management (IAM) risk results from improper management of user identities and access permissions on a computer system, enabling improper unauthorized access to sensitive data or systems and applications.

- Application security is a cloud computing risk similar to applications in a traditional, non-cloud environment. These security concerns include, but are not limited to, Structured Query Language (SQL) injection, cross-site scripting (XSS), and challenges related to the conversion of legacy systems for use in the cloud.
- Compliance is a risk for organizations that operate in particular industries or across state and national borders. General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS) are just a few examples of regulations and standards that pose compliance challenges for data management and security.
- Compatibility risks occur when applications and operating systems may not support cloud computing protocols.
- Public key infrastructure (PKI) management risk includes lack of segregation of duties over the issuance and use of certificates, exposing an organization to internal threats. Also, the use of self-signed certificates can be error prone.
- The Domain Name System (DNS) is an integral part of the Internet that allows users to access websites and other online resources by translating domain names into IP addresses. DNS security risks include spoofing, hijacking, amplification, and tunneling.

Cloud-Unique Cybersecurity Risks

The following are risks applicable only to a CSP's implementation of a cloud computing environment. They are not vulnerabilities in a traditional IT data center.

- **Consumer transparency.** Organizations lose some visibility and control over assets and operations that have been moved to the CSP.
- **Unauthorized use.** The on-demand self-service provisioning cloud capability offered via CSPs enables an organization's personnel to deliver services without organizational IT's consent.
- **Compromise of Internet-accessible management application programming interfaces (API).** CSPs typically provide a set of APIs that customers use to manage and interact with cloud services. Organizations use these APIs to deliver, manage, and monitor their assets and their users. However, these APIs contain the same software vulnerabilities as APIs for operating systems. Unlike on-premises computing, CSP APIs are accessible via the Internet, which exposes them more broadly to exploitation.
- **Failure of tenant separation.** Exploitation of system and software vulnerabilities within a CSP's infrastructure, platforms, or applications that support multi-tenancy can lead to a failure to maintain separation among other CSP customers.
- **Incomplete data deletion.** Consumers' reduced awareness of the physical location of their data storage in the cloud reduces their ability to verify secure deletion of their data.

Cloud and On-Premises Cybersecurity Risks

The following are risks applicable to both cloud and on-premises IT data centers. Some of these overlap other descriptions of risks related to technology.

- **Stolen credentials.** An attacker attempts to gain unauthorized access to user accounts by stealing login credentials for the purpose of obtaining additional resources.
- **Vendor dependence.** Dependence on a single provider for a specific purpose makes it difficult to transition to a different vendor due to increased costs, compliance concerns, and technical obstacles.
- **Technical complexity.** IT staff may not have the capacity or skill level to manage, integrate, and maintain the migration of assets and data to the cloud in addition to their responsibilities for on-premises IT.
- **Reduced forensic capabilities.** IT administrators and staff for both the CSP and the organization may abuse their authorized access to the organization or the CSP's networks, systems, and data. The ability to monitor, log, or review the perpetrator's activities may be constrained in a cloud environment.
- **Data loss.** Data loss can occur due to malicious activity, physical catastrophe, or accidental deletion by the CSP. The result may be permanent data loss of sensitive information. The burden of data loss does not solely reside with the CSP. The organization may use encryption technology and be responsible for maintaining its encryption key. This risk is magnified for organizations using multiple CSPs.
- **Compromise of CSP supply chain.** The CSP may outsource part of its infrastructure, operations, and maintenance. If these third parties fail to support the CSP's requirements, services for the organization may cease to function. This risk is magnified for organizations with multiple CSPs.
- **Insufficient due diligence.** Organizations receiving cloud services may perform insufficient due diligence about (1) the security protocols employed by the CSP and (2) their own responsibilities to provide security measures.

4.2 Cybersecurity Related Policies and Controls

Author's Note

Understanding cybersecurity and related policies and controls is crucial because internal auditors are responsible for evaluating and ensuring the effectiveness of an organization's risk management, control, and governance processes. By understanding these topics, an internal auditor has the ability to assess whether the organization is adequately protecting its information assets.

This knowledge enables an auditor to identify potential vulnerabilities, ensure compliance with laws and regulations, and recommend improvements to strengthen the organization's overall security posture. In an era with increasingly sophisticated cyber threats, such expertise is vital for safeguarding an organization's critical data and maintaining stakeholder trust.

Cybersecurity is information security applied to computer hardware, software, and networks.

- The Committee on National Security Systems (CNSS) in the United States defines **information security** as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information.

Three Goals

1. **Confidentiality** is assurance of the secrecy of information that could adversely affect the organization if revealed to unauthorized persons.
2. **Integrity** is ensuring that information accurately reflects the business events underlying them and preventing the unauthorized or accidental modification of programs or information.
3. **Availability** is the ability of the intended and authorized users to access information resources to meet organizational goals.

Policies are the foundation of effective information security and cybersecurity measures.

- Senior management is responsible for risk assessment, including identification of risks and consideration of their significance, the likelihood of their occurrence, and how they should be managed.
  - Senior management is also responsible for establishing organizational policies regarding computer security and implementing a compliance structure.
- The successful planning, design, and implementation of security procedures are initiated by strong policies and management support.
- Policies govern how to resolve issues, including the use of IT infrastructure. Effective policy must be
  - In compliance with laws and regulations
  - Communicated and explained to applicable personnel
  - Accepted by applicable personnel
  - Enforced

IT Control Frameworks

An IT control framework is a structured set of policies, procedures, and guidelines that organizations use to manage IT risks. The benefits of using an IT control framework are that it provides a structured approach to identifying and assessing IT risks and the controls that are necessary to mitigate those risks. An example is the COBIT framework.

Data Governance

Data governance is the process of ensuring the availability, integrity, and security of an organization's data through policies, standards, and practices. Organizations need to know that their data are secure, are high quality, and are available for analysis when needed. Good data governance means that the owners of data and the uses of that data are documented, and that data security measures and data privacy policies are in place.

Data Privacy Principles

For legal and business reasons, organizations must protect personal data from unauthorized access, disclosure, or misuse. In principle, individuals should be able to control how their personal data are used. Principles of data privacy include lawfulness, fairness, transparency, accuracy, integrity, confidentiality, accountability, and limitations on the use of the data.

Governmental data protection laws regulate the collection and use of personal data. Different countries take different approaches, but all have the goal of preventing harm to the individual whose data are collected. The European Union's GDPR (General Data Protection Regulation) is one prominent law, and the U.S., the U.K., China, and other countries have their own similar laws.

Data Integrity

The difficulty of evaluating data integrity is a significant challenge in a computer-based auditing environment.

- Electronic evidence is difficult to authenticate and easy to fabricate.
- Internal auditors must be careful not to treat computer printouts as traditional paper evidence. The data security factors pertaining to electronic evidence must be considered.
- The degree of the auditor's reliance on electronic evidence depends on the effectiveness of the controls over the system from which such evidence is taken.