TERMINOLOGIES: Topic #1 - #6

Information Assurance Security

BSCS | PROF. Kawabata | SEM 2 , 2023

TOPIC #1: UNDERSTANDING SECURITY CONCEPTS

THE MANY AREAS OF INFORMATION SECURITY

★ **Application Security** - security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.

★ **Access Control** - method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.

★ **Business Continuity and Disaster Recovery (BCDR or BC/DR)** - set of processes and techniques used to help an organization recover from a disaster and continue or resume routine business operations.

★ **Governance, Risk and Compliance (GRC)** - strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations.

★ **Legal, Regulations, Investigations and Compliance** - addresses ethical behavior and compliance with regulatory frameworks. It includes the investigative measures and techniques that can be used to determine if a crime has been committed, and methods used to gather evidence.

★ **Security Architecture and Design** - looks at how information security controls and safeguards are implemented in IT systems in order to protect the Confidentiality, Integrity, and Availability of the data that are used, processed, and stored in those systems.

★ **Network Security** - consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible.

★ **Physical Security** - security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm.

★ **Operations Security (OPSEC)** - a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, and determines if information obtained by adversaries could be interpreted to be useful to them.

★ **Cryptography** - the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents

THE MANY AREAS OF INFORMATION SECURITY

★ **Confidentiality** - Access Controls restrict users from accessing sensitive Information without permission, encryption protects information at rest or in transit, steganography hides information within images or other files.

★ **Integrity** - ensure that information is not altered without authorization; protects an organization's information from accidental or intentional tampering that may come as the result of many different issues.

★ **Availability** - ensures that information and systems remain available to authorized users when needed.

DIFFERENT CONTROLS THAT PROTECT THE AVAILABILITY

★ **Redundant Components**
- protect system against failure of a single part.

★ **High Availability**
- protects services against the failure of a single server.

★ **Fault Tolerance**
- protects services against disruption from a small failure.

★ **Digital Signatures** - provide authenticity and non-repudiation.

★ **Authenticity** - achieved when the recipient of a message can be confident that the message actually came from the purported sender.

★ **Non-repudiation** - achieved when the recipient of a message can prove to an independent third party that the message actually came from the purported sender.

PRIVACY

★ **Personally Identifiable Information (PII)**
- any information that can be traced back to an individual.

★ **Protected Health Information (PHI)**
- individually identifiable health records governed under HIPAA.

★ **Segregation of Duties** - no individual should possess two permissions that, in combination, allow them to perform a highly sensitive action.

★ **Accountability** - the ability to trace every action taken on a system back to an individual user without any ambiguity and without allowing the user to deny responsibility for that action.

★ **Need to Know** - limits information access.

★ **Least Privilege** - limits system permissions.

★ **Privilege Aggregation** - jeopardizes least privilege to implement Least Privilege can be in Group, Account Standardization, Account Management Processes & Procedures.

★ **Defense in Depth** - implementing several layers of protection.

★ **Implicit Deny** - indicates that unless something is explicitly allowed it is denied.

★ **Due Care** - is often called the "Prudent Man" rule, which is doing what any responsible person would do, in other words, this is implementing a security measure to mitigate against certain risk.

★ **Due Diligence** - it is essentially the management of due care. In other words, ensuring the implemented security measure was done correctly.

★ **Gross Negligence** - is the opposite of due care; if you're not performing due care, what a prudent man would do, and you suffer a negative loss, you could be held legally liable.

▲ ▼ ▲ ▼ ▲ ▼ ▲ ▼ ▲ ▼ ▲ ▼ ▲

TOPIC #2: IDENTIFY AND IMPLEMENT SECURITY CONTROLS

★ **Authentication Basic** - authentication is used to prove identity through the use of some type of credential that is previously known by the authenticator.

★ **Technical Controls** - include any measures taken to reduce risk via technological means.

OTHER SECURITY CONTROLS

★ **Preventive Controls**
- prevents actions.

★ **Detective Controls**
- sends alert during or after an attack.

★ **Corrective Controls**
- "correct" a damaged system or process.

★ **Deterrent Controls**
- deter users from performing actions.

★ **Compensating Controls**
- add additional security by compensating other control's weaknesses.

★ **Physical Controls**
- includes implementing different access control methods with

technology you can touch.

★ **Logical Controls**
- include elements that are implemented through technological means.

★ **Administrative Controls**
- it defines the human factors of security; it involves all levels of personnel within an organization and determines which users have access to what resources and information.

SECURITY MANAGEMENT PRACTICES

★ **Security Policy** - policies are the top tier of formalized security documents.

★ **Standards** - much more specific than policies; standards are tactical documents because they lay out specific steps or processes required to meet a certain requirement.

★ **Baselines** - minimum level of security that a system, network, or device must adhere to.

★ **Guidelines** - points to a statement in a policy or procedure by which to determine a course of action.

★ **Procedures** - the most specific of security documents; a procedure is a detailed, in-depth, step-by-step document that details exactly what is to be done.

TOPIC #3: ASSET MANAGEMENT LIFECYCLE

★ **Asset** - anything deemed valuable to a company.

★ **Data Retention** - the long-term storage of valuable assets, typically driven by: Legal and Regulatory Compliance Requirements and Organizational Requirements.

ASSET LIFECYCLE

★ **Identify and Classify**
- new assets should be identified and classified.

★ **Secure**
- secure assets based on the classified value.

★ **Monitor**
- regularly monitor for changes in value and the effectiveness of our security controls.

★ **Recovery**
- if an asset is adversely impacted, recovery measures should be in place.

★ **Disposition**
- once the usefulness of an asset has been reached and it is to be disposed, there are two primary methods: archiving the asset for long-term storage or defensible destruction, ensuring there is no data remanence.

DATA STATES

★ **Data at Rest** - data that's stored on media of any form (hard drive, USB stick, tape, CD). It's considered at rest because it's not being transmitted over the network or in use. Data at rest is commonly protected by disk and file encryption.

★ **Data in Motion** - data that's currently moving across a network from one device to another. Data in motion is commonly protected by network encryption, such as SSL, TLS, and VPN connections with IPSec encryption.

★ **Data in Use** - data that's being used by a system process, application or user. It's data that's being created, updated, appended, or erased. Data in use is the hardest to protect because it's not encrypted while in use. Proper access control, integrity checks, and auditing measures can help protect data in use.

TOPIC #3: DATA SECURITY

★ **Data** - the most valuable asset held by many organizations.

★ **Big Data** - the use of data sets much larger than those that may be handled by conventional data processing and analytic techniques

★ **Data Classification Policy** - describes security levels; classification programs establish the basis for other information and asset handling requirements

DATA STATES

★ **Data in Rest** - data stored for later use on storage media.

★ **Data in Motion** - data being sent over a network between two systems.

★ **Data in Use** - data being actively used in a system's memory.

DATA SECURITY ROLES

★ **Data Owners**
- business leaders with overall responsibility for data. They set policies and guidelines for their data sets.

★ **Data Steward**
- handle the day-to-day data governance activities. They are delegated responsibility by data owners. .

★ **Data Custodians**
- actually store and process information and are often IT Staff Members.

★ **Data Users**
- work with information in their jobs on a daily basis.

TOPIC #4: PARTICIPATE IN CHANGE MANAGEMENT LIFECYCLE

★ **Change Management** - the process that businesses and organizations use to implement changes through building and delivering effective change strategies.

★ **Configuration Management** - tracks specific device settings.

★ **Baseline** - provides a configuration snapshot.

★ **Automation** - improves the efficiency and effectiveness of configuration management.

★ **Versioning** - assigns number to each version.

TOPIC #5: IMPLEMENTING SECURITY AWARENESS AND TRAINING & COLLABORATE WITH PHYSICAL SECURITY OPS

★ **Security Impact Analysis** - the analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

★ **Security Training** - provides users with the knowledge they need to protect the organization's security.

★ **Security Awareness** - keeps the lessons learned during security training top of mind for employees.

★ **Training Frequency** - initial training for new employees; update training for employees with new roles.

★ **Compliance Programs** - ensure that an organization's information security controls are consistent with the laws, regulations and standards that govern the org's activities.

★ **Compliance Obligations** - laws, regulations, and standards.

★ **Social Engineering** - presents serious risks to cybersecurity; manipulating people into divulging information or performing an action that undermines security.

COMMON TYPES OF SOCIAL ENGINEERING

★ **Spear Phishing** - targeting specific organizations or individuals.

★ **Vishing** - using mobile phones or telephones.

★ **Smishing** - SMS or text messages.

★ **Whaling** - targeted attack aimed at high-profile individuals, such as CEO.

OTHER TYPES OF SOCIAL ENGINEERING

★ **Pretexting**
- gains a victim's trust, typically by creating a backstory that makes them sound trustworthy.

★ **Tailgating**
- physical security attack that involves an attacker following someone into a secure or restricted area.

★ **Shoulder Surfing**
- occurs when the Threat actors directly observes information like log-in credentials, ATM, PINs by hovering over the shoulder of the user.

★ **Eavesdropping**
- someone is secretly listening to confidential information while others are conversing.

▲ ▼ ▲ ▼ ▲ ▼ ▲ ▼ ▲ ▼ ▲ ▼ ▲

TOPIC #6:
ACCESS CONTROLS

★ **Access Controls** - single/multi factor authentication, single sign-on (SSO), device authentication and federated access.

★ **Multifactor Authentication** - combines authentication techniques from two or more of the authentication categories: Something you know, something you and something you are.

★ **Security Assertion Markup Language (SAML)** - allows single sign-on (SSO) within a web browser across a variety of systems.

★ **Federated Identity Management** - individuals may have accounts across multiple systems, federated identity management systems share identity information; this reduces the number of individual identities a user must have.

★ **Single Sign-On (SSO)** - authentication system that shares a single authentication session across multiple systems, avoiding asking users to log in multiple times.

★ **Active Directory Federation Services (ADFS)** - supports integrating Active Directory SSO with other services.