CSF3404 Cyber Security

Chapter 8 Implementing Compliance and Operational Security

Lecturer:
Waheed Ghanem
Fakhrul Adli bin Mohd Zaki
Aalim Rozli

Faculty of Ocean Engineering Technology and Informatics,
Universiti Malaysia Terengganu

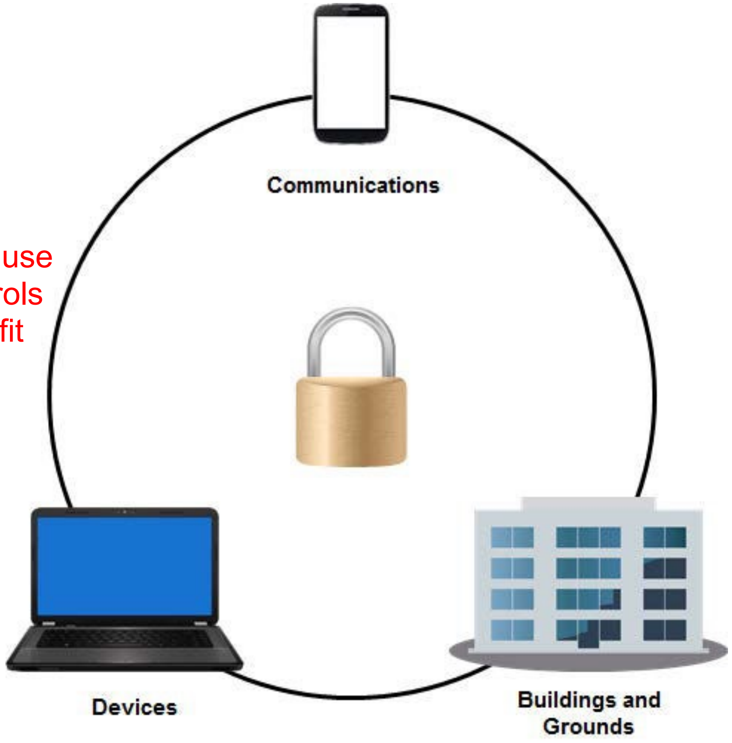
Physical Security

- To verify your company's compliance with internal and external policies on an ongoing basis.
- To begin maintaining a complete security infrastructure.
- Make sure that the physical components of your company's security plan are in place.
- Explore the security measures used to ensure the physical security of the organization.

Physical Security Controls

- Security measures that restrict, detect, and monitor access to specific physical areas or assets.
- They can control access to;
  - Building.
  - Equipment.
  - Specific areas.
    - Such as
      - Server rooms.
      - Finance.
      - Legal areas.
      - Data centers.
      - Network cable runs.
      - In any other area that has hardware or information that is considered to have important value and sensitivity.

Determining where to use physical access controls requires a risk/benefit analysis.



Physical Security Controls

- There are various ways to categorize the different physical security controls:
  - **Deterrent controls** discourage attackers from attacking in the first place.
  - **Preventive controls** stop an attack before it can cause damage.
  - **Detective controls** identify attacks in progress.
  - **Compensating controls** support other physical controls.
  - **Technical controls** are hardware or software that aid in protecting physical assets.
  - **Administrative controls** leverage security policies and are used to train personnel.

Physical Security Control Types

- There are a number of physical access controls available to ensure the protection of an organization's physical environment.
  - ✓ Locks
  - ✓ Logging and visitor access
  - ✓ Identification systems
  - ✓ Video surveillance
  - ✓ Security guards
  - ✓ Signs
  - ✓ Bonded personnel
  - ✓ Mantrap doors
  - ✓ Physical barriers
  - ✓ Alarms
  - ✓ Motion detection
  - ✓ Protected distribution

Environmental Exposures

- Environmental exposures must be considered when evaluating the overall security of a building.
- Exposures can include:
  - Lightning
  - Hurricanes
  - Earthquakes
  - Volcanic eruptions
  - High winds
  - Extreme weather conditions.
- As a result of any of these exposures, a number of issues may arise:
  - Power fluctuations and failures.
  - Water damage and flooding.
  - Fires.
  - Structural damage to the building leading to unauthorized access

Environmental Controls

- There are certain environmental controls that can be implemented to help control a facility's physical environment.
  - HVAC systems
  - Hot and cold aisles
  - EMI shielding
  - Alarm control panel
  - Fire prevention
  - Fire detection
  - Fire suppression

Environmental Monitoring

- Regularly monitoring the environmental conditions and controls surrounding a building and the hardware stored inside **it is important to properly secure and prevent damage to resources.**

- Conditions that can threaten security should be monitored regularly, **along with the implementation of necessary security controls**.

- **Constant video monitoring** is used to look for environmental issues such as overheating, water, or electricity issues.

Safety

- Affects both personnel and property.
- Deter intruders with fencing and CCTV.
- Protect employees with locks and proper lighting.
- Formulate an escape plan/route and perform drills.
- Test your controls to verify they are up to standard

Legal Compliance

- The **security professional** is responsible for meeting the security needs of outside legal authorities as well.

- **Security professionals** will determine the security requirements your company may be legally required to meet.

- Legal security compliance requirements can affect your company in a variety of situations.

Compliance Laws and Regulations

- Compliance is the practice of ensuring that the requirements of legislation, regulations, industry codes and standards, and organizational standards are met.
- Several controlling authorities need to be recognized to achieve compliance:
    - Governmental legislative entities such as national congresses or parliaments and state, provincial, or regional senates or other law-making bodies.
    - Governmental regulatory agencies that promulgate rules, regulations, and standards for various industries.
    - Industry associations that promulgate rules, regulations, and standards for individual industries.

Legal Requirements

- All organizations must consider their overall or general legal obligations, rights, liabilities, and limitations when creating security policies.
- All organizations must be prepared to work with civil authorities when investigating, reporting, and resolving each incident.
- Information security practices must comply with legal requirements that are documented in other departmental policies, such as human resources.
- Observe legal limitations and civil rights.
- Consider legal issues for different groups

Types of Legal Requirements

Legal issues can affect different parties within each organization.

- Employees
  - Who is liable for the misuse of email and Internet resources? The organization, the employee, or both?
  - What is the extent of liability for an organization for criminal acts committed by its employees?
  - What rights to privacy do employees have regarding electronic communications?
- Customers
  - What customer data is considered private, and what is considered public?
  - How will a company protect the privacy and confidentiality of customer information?
- Business partners
  - Who is liable if data resides in one location (country) and the processing takes place in another location?
  - Who is responsible for the security and privacy of the information transmitted between an organization and a business partner? The sender or the receiver?

Types of Legal Requirements

Information security professionals must observe generally accepted forensic practices when investigating security incidents.

Evidence Collection

Evidence Preservation

Chain of Custody

Jurisdiction

Forensic requirements

Types of Legal Requirements

- **Evidence collection:**
  - Collecting evidence from floppy disks, hard drives, smart cards, and other media ensures the integrity of the evidence and prevents tampering.
  - Evidence that is improperly collected may not be admissible in court.
- **Evidence preservation:**
  - Criminal cases or even internal security incidents can take months or years to resolve.
  - The company must be able to properly preserve all gathered evidence for a lengthy period of time.
- **Chain of custody:**
  - Whoever gathers and preserves the evidence must also maintain a complete inventory that shows who handled specific items and where they have been stored.
  - If the chain of custody is broken, it can be difficult, if not impossible, to prosecute a technology crime.
- **Jurisdiction:**
  - Determining exactly who has the right to investigate and prosecute an information technology criminal cases can be extremely difficult due to overlapping laws for copyright, computer fraud, and mail tampering.

Security Awareness and Training

- You need to keep your security infrastructure healthy.
- Security is the responsibility of all the individuals in the organization.
- Attackers are smart and will take advantage of employees that may not be savvy enough to know they are being solicited for information.
- Security professional is responsible to educate or coach your users about their individual security responsibilities.
- An educated user is the security professional's best partner in preventing security breaches.

Security Policy Awareness

- An organization's security policy is created to ensure that all system users comply with the security guidelines and procedures enforced by management.
- Security professionals should verify that the security policy is accessible and that users are trained in the importance of security awareness within an organization.
- Regular training sessions and security policy documentation will ensure that users follow the correct procedures when accessing and using system resources and services

Role-Based Training

- The organization implements training based on job roles and organizational responsibilities.

- For instance,
  - End users might not need training about how to keep budget or personnel information secure.
  - Managers would definitely need to know about restrictions on sharing that sort of data.

- May establish or encounter role-based training relates to incident reporting and response.

Personally Identifiable Information

- PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

- What constitutes PII will vary depending on the legal jurisdiction?
- PII can include a user's
  - Full name
  - Fingerprints
  - License plate number
  - Phone number
  - Street address
  - Driver’s license number

Classification of Information

- To adequately protect information from disclosure and other threats.
  - We need;
    - To understand the risks associated with the release or modification of the information.
- The risk of information loss or modification is often measured by labeling (**classifications**) the information.
- The classifications will depend on the type of business and how the data is stored.
- Classified data can be either hard or soft.
  - Hard data refers to concrete information.
  - Soft data refers to the organization's ideas.

Classification of Information

- Information is categorized according to the level of sensitivity in the information:
  - High, Medium, and Low
  - Restricted, Private, and Public
  - Confidential, Restricted, and Public

Classification of Information

- **Corporate Confidential:**

  Information that should not be provided to individuals outside of the enterprise.
- **Personal and Confidential:**

  Information of a personal nature that should be protected.
- **Private:**

  Correspondence of a private nature between two people that should be safeguarded.
- **Trade Secret:**

  Corporate intellectual property that, if released, will present serious damage to the company's ability to protect patents and processes.
- **Client Confidential:**
  - Client personal information that, if released, may result in the identity theft of the individual.
  - Client corporate information or intellectual property. You may need to sign a non-disclosure agreement (NDA) to keep an organization's information about a client confidential.

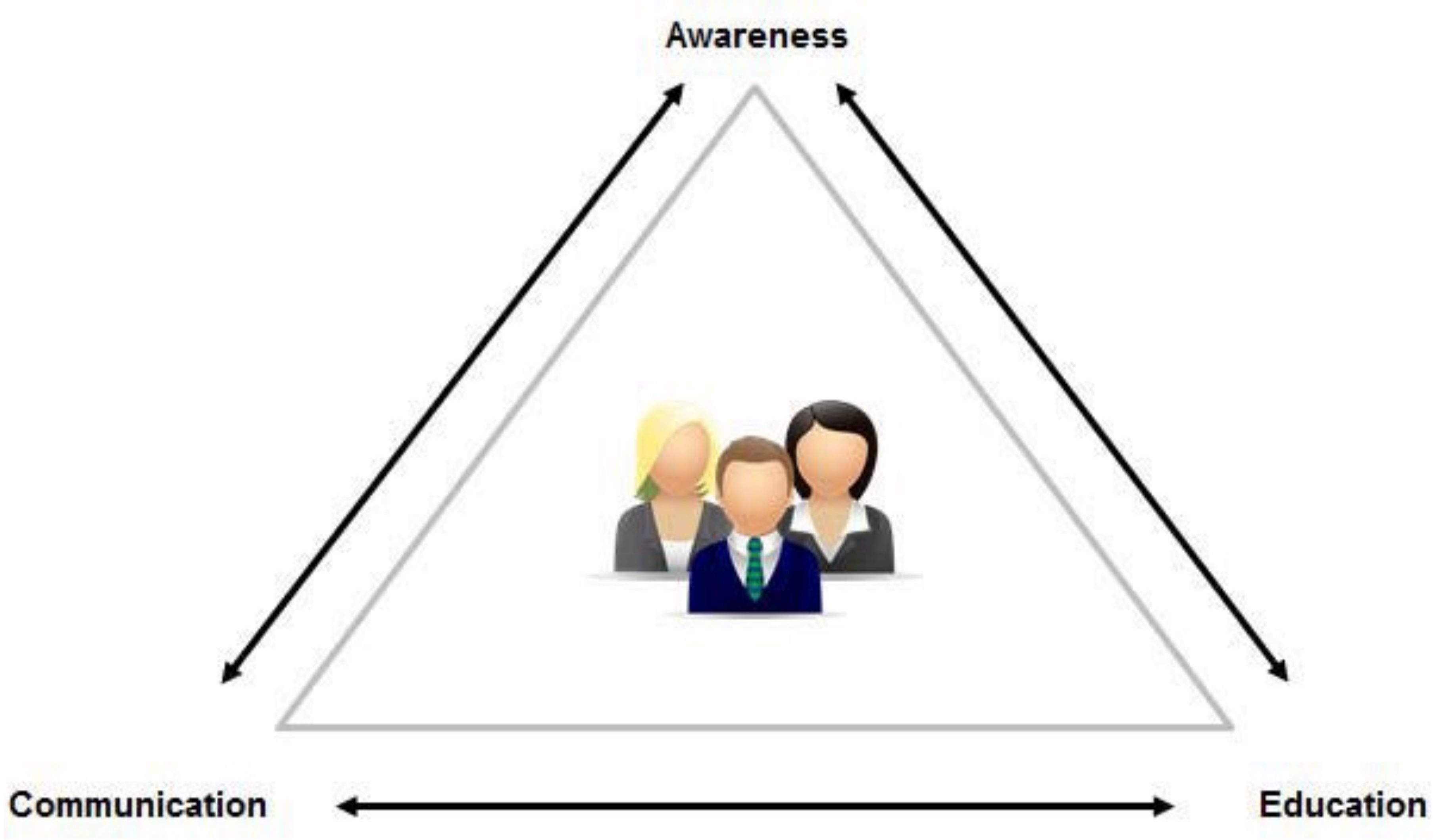
Employee Education

- Information security is not the exclusive responsibility of information professionals.

- A comprehensive security plan can only succeed when all members of an organization understand the necessary security practices and comply with them.

- Security professionals are often the ones responsible for educating employees and encouraging their compliance with security policies.

The employee education process



The employee education process

- **Awareness:**
  - Employees must understand the importance of information security and security policies, and have an awareness of the potential threats to security.
  - Employees also need to be aware of the role they play to protect an organization's assets and resources.
  - A security professional can create awareness through seminars, email, or information on a company intranet.

- **Communication:**
  - The lines of communication between employees and the security team must remain open.
  - Security professionals can accomplish this by encouraging employees to ask questions and provide feedback on security issues.

- **Education:**
  - Employees should be trained and educated in security procedures, practices, and expectations.
  - Employees are responsible for organizational security the second they join an organization and have access to the physical building and resources, and the intellectual property inside.
  - Education should continue as technology changes and new information becomes available.
  - Educated users are one of your best defenses against social engineering attacks.

Online Resources

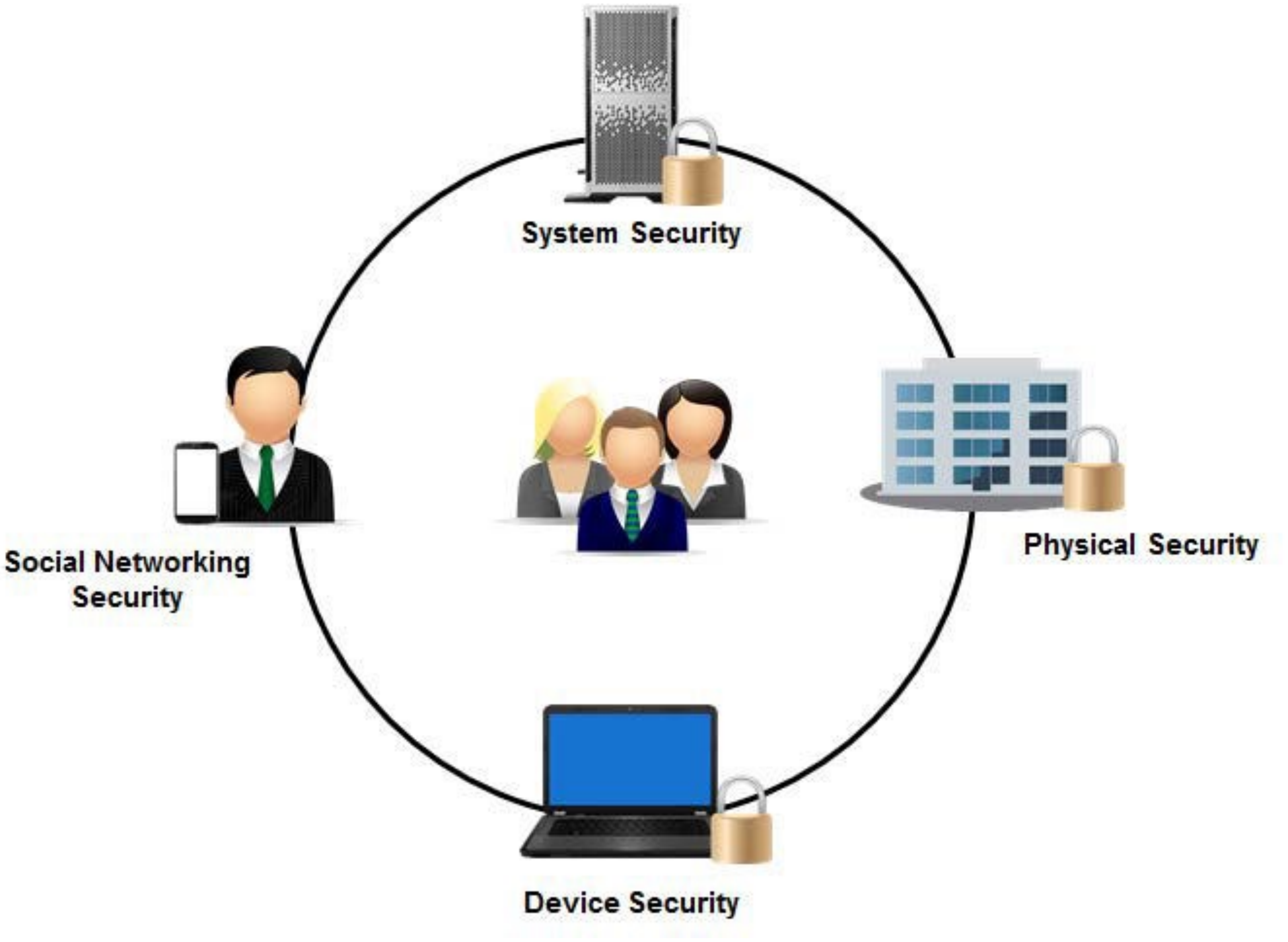
- A common way to promote employee awareness and training is to provide employees with online access to security-related resources and information.
- You can provide proprietary, private security information, such as your corporate security policy document, through an organization's intranet.
- You can also point employees to a number of reputable and valuable security resources on the Internet.
- Both you and the employee should be cautious whenever researching information on the Internet.
  - Just because the information is posted on a website does not mean it is factual or reliable.

Online Resources

- Here are just a few of the information security resources that you can find on the Internet:
  - www.microsoft.com/security/default.mspx
  - /www.oracle.com/technetwork/topics/security/whatsnew/index.html
  - http://tools.cisco.com/security/center/home.x
  - www.sans.org
  - www.openssh.org
  - www.emc.com/domains/rsa/index.htm
  - /www.cert.org
  - searchsecurity.techtarget.com/
  - www.securityfocus.com
  - www.entrust.com
  - www.ruskwig.com
  - www.symantec.com/security_response/index.jsp
  - www.mcafee.com
  - http://project.honeynet.org
  - http://web.mit.edu/kerberos
  - http://hoaxbusters.org
  - http://vmyths.com
  - http://snopes.com

User Security Responsibilities

- Because security is most often breached at the end-user level, users need to be aware of their specific security responsibilities and habits.



Security Area & Employee Responsibilities

- **Physical security:**
  - Employees should not allow anyone in the building without an ID badge.
  - Employees should not allow other individuals to tailgate on a single ID badge.
  - Employees should be comfortable approaching and challenging unknown or unidentified persons in a work area.
  - Access within the building should be restricted to only those areas an employee needs to access for job purposes.
  - Data handling procedures of confidential files must be followed.
  - Employees must also follow clean desk policies to ensure that confidential documents and private corporate information are secured and filed away from plain sight.

Security Area & Employee Responsibilities

- **System security:**
  - Proper password behaviors can be crucial in keeping systems resources secure from unauthorized users.
  - Employees must use their user IDs and passwords properly and comply with the ID and password requirements set forth by management.
  - Password information should never be shared or written down where it is accessible to others.
  - All confidential files should be saved to an appropriate location on the network where they can be secured and backed up, not on a hard drive or removable media device.

Security Area & Employee Responsibilities

- **Device security:**
  - Employees must use correct procedures to log off all systems and shut down computers when not in use.
  - Wireless communication and personally owned devices must be approved by the IT department and installed properly.
    - ✓ These devices can be a gateway for attackers to access corporate information and sensitive data.
  - Portable devices, such as laptops and mobile devices, must be properly stored and secured when not in use.

Security Area & Employee Responsibilities

- **Social networking security:**
  - Employees must be made aware of the potential threats and attacks that target social networking and peer-to-peer (P2P) applications and websites.
  - The use of these applications can lead to potential breaches in security on an organization's network.
  - Security policies should include guidelines and restrictions for users of any social networking application or website.

Validation of Training Effectiveness

- If an organization invests in security awareness and training, it should also make sure that the training is effective.
- Effective training helps to ensure compliance and increases the overall security of the organization.
- To validate the effectiveness of your security awareness and training programs:
  - We'll need to identify which components of those programs will have the most impact on overall security.
- The **SANS Securing** the Human Program offers some **free tools** to help organizations **establish metrics** for *measuring impact*, or *behavioral changes* that can be attributed to the training, along with metrics for *tracking compliance* and ways *to assess various risks*.
  - For more information, visit
  - http://www.securingthehuman.org/resources/metrics.

Integrate Systems and Data with Third Parties

- Today's business world is one of partnerships and integration.
  - We will integrate systems and data with third parties.
- Compliance and operational security deal with the sharing of information among organizations.
  - With the advent of so many new technological tools such as social media, more and more organizations find themselves connected to and sharing information with many different entities.
  - The ability to secure these communications while allowing the proper level of access to information is a primary responsibility of any security professional.

Business Partners

- It is a commercial entity that has a relationship of some sort with another, separate commercial entity.
- It can be a supplier, customer, agent, reseller, or vendor of similar products or services.
- It can be formal, such as a contractual agreement, or informal, but no matter what type of partnership exists, there will always be the need to share information among the business partners.
- It should go through an onboarding and off-boarding process when the relationship both begins and concludes, respectively.
  - Proper onboarding involves acclimating partners to the security practices that you expect them to follow.
  - This ensures that there will be a fair balance of responsibility and liability in the partnership.
- Likewise, when the partnership ends, you should establish an off-boarding process.

Social Media Networks and Applications

- Social media networks and applications such as Facebook, Twitter, LinkedIn, and Yammer are being incorporated into more business scenarios than ever before.
- Companies leverage the power of these platforms to connect with a more public-facing audience in order to expand their media presence.
  - The public nature of social media and related apps often presents a risk to an organization's security.
  - Employees may post sensitive information on a social network that has wider-reaching consequences than simple word-of-mouth.
  - Even on its official web page, a company might reveal more than it should.
  - The openness of social media is also a haven for social engineers who will attempt to deceive employees into compromising security.

Interoperability Agreements

- There are various types of agreements that business entities may rely on to facilitate interoperability.
- <u>**Agreement Type:**</u>
  - **Service-level agreement (SLA)**
    - This agreement clearly defines what services are to be provided to the client, and what support, if any, will be provided.
  - **Business partner agreement (BPA)**
    - This agreement defines how a partnership between business entities will be conducted, and what exactly is expected of each entity in terms of services, finances, and security.
  - **Memorandum of understanding (MOU)**
    - This type of agreement is usually not legally binding and typically does not involve the exchange money.
    - They are typically enacted as a way to express a desire for all parties to achieve the same goal in the agreed-upon manner.
  - **Interconnection security agreement (ISA)**
    - This type of agreement is geared toward the information systems of partnered entities to ensure that the use of inter-organizational technology meets a certain security standard.

Risk Awareness

- Awareness of risks includes being always aware of the details of daily interoperability.
- All employees must be trained to detect risks in their departments, no matter how large or small.
  - When employees evaluate the role they play in a partnership or social media integration, they will have a better idea of the risks they are exposed to.
  - Delegating this responsibility will foster a culture of risk awareness and prepare an organization for risk management

Data Sharing and Backups

- Don’t need to give total data access to partners.
- Define clearly who owns what data.
- Implement access control where feasible.
- Let employees know what they should and should not share.
- Consider legal ramifications.
- Control how shared data is backed up.

Guidelines for Securely Integrating Systems and Data with Third Parties

- Develop procedures for on-boarding and off-boarding of partners.
- Draft interoperability agreements appropriate for your situation.
- Follow policies outlined in the agreement.
- Review agreement requirements to verify compliance.
- Exercise discretion with business info on social media.
- Train employees on best social media practices for security.
- Encourage risk awareness in all levels of the organization.
- Clearly define who owns data.
- Control data sharing and discourage unauthorized sharing.
- Set rules for third-party data backups.

Reflective Questions

1. Before attending this course, did you consider environmental issues such as HVAC systems and fire prevention, detection, and suppression as part of your organization's information security initiatives?
2. How do you think security awareness and training can affect an organization?

Thank you