

This is a continuation of the INFO 101 course which you have probably completed. In this course we will cover the remaining 5 CISSP information security domains.

Overview

- **Topics covered in this course**

1. Information Security and Risk Management
2. Security Architecture and Design
3. Legal, Regulations, Compliance and Investigations
4. Physical (Environmental) Security
5. Business Continuity and Disaster Recovery Planning

Narrative:

This course is divided into five sections:

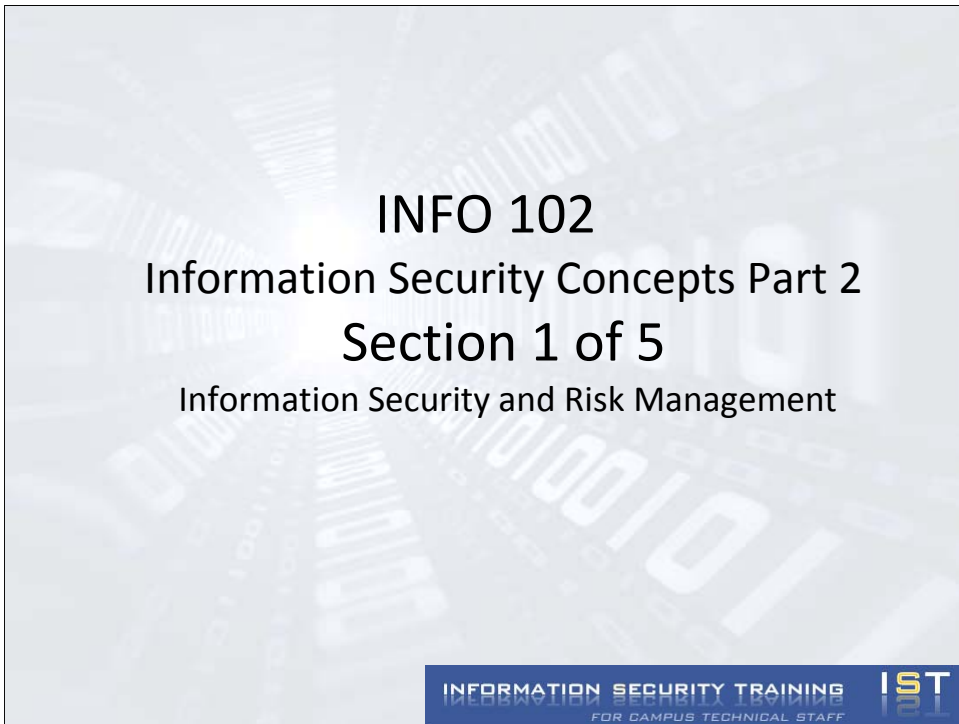
Information Security and Risk Management

Security Architecture and Design

Legal, Regulations, Compliance and Investigations

Physical (Environmental) Security

Business Continuity and Disaster Recovery Planning



Narrative:
Information Security and Risk Management

Objectives

- Protect organization's ability to carry out its mission
- More than an IT function



INFORMATION SECURITY TRAINING
FOR CAMPUS TECHNICAL STAFF

IST

Narrative:

The objective of risk management is to protect the organization's ability to carry out its mission. This is much more than just an IT function. Risk management involves the assessment of risks to the organization's assets, then taking action to reduce the risks. Actions taken to manage and reduce risk include installation of additional hardware and software, promotion of good security practices, organization of an emergency response team, mitigation of the risk in other ways, or acceptance of the risk.

Risk

- A quantifiable measure
- The probability a negative event will occur
- A measure of the impact of such an occurrence



Narrative:

Risk is a quantifiable measure calculated from the probability that a particular negative event will occur and an estimate of the impact of such an occurrence. The impact is usually measured in dollars, but in some circumstances it could be measured in terms of injury to humans or lives lost.

Risk Management Steps

- Risk assessment
- Risk mitigation
- Evaluation and assessment

Narrative:

There are three stages of risk management - risk assessment, risk mitigation, and evaluation and assessment of the mitigation.

Risk Assessment



- Identify assets
- Estimate value of assets
- Identify threats to assets (STRIDE)
- Analyze existing security safeguards
- Analyze vulnerabilities
- Estimate probability and frequency of attacks
- Estimate impact of losing assets

Narrative:

The assessment of risks is a methodical process. The first step is the identification of all of the organization's assets. They include hardware, software, data, facilities, and people. A value is assigned to each asset. Obviously some assets are more important than others. For example, the accounts receivables data is more valuable than the copy machine.

The potential threats to each asset are then identified. There are a number of different threat classification schemes to choose from. The STRIDE scheme is popular now.

In the next step of risk assessment, the existing security safeguards are identified and evaluated for each asset.

Weaknesses in access and storage procedures, physical protection and other vulnerabilities are analyzed and the consequences of losing all or part of that asset are estimated during impact analysis.

Classification of Threats to Assets (STRIDE)

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

Narrative:

If a large number of threats can be sorted into categories, it should be possible to design cost-effective countermeasures for classes of threats rather than focusing on individual threats. There are a number of useful ways to classify threats.

The STRIDE classification stands for spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege.

Spoofing occurs when one party successfully pretends to be someone else. For example, an outside party might call the Help Desk pretending to be an employee while requesting that her password be reset.

Tampering indicates that data has been altered in an unauthorized way.

Repudiation, as mentioned previously, implies that the receiver of a good or service could get away with not paying for it.

Information disclosure means that sensitive information was revealed inappropriately.

Denial of service prevents legitimate users from using computer resources effectively.

Elevation of privilege means that an intruder, once having gained access to a system as an ordinary user, manages to obtain superuser privileges or administrative rights. This threat class also includes legitimate users who inappropriately gain superuser privileges or administrative rights.

Risk Mitigation



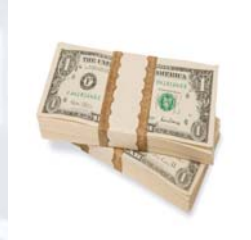
- Estimate costs
- Reduce risks
 - To an acceptable level
 - Balance value of asset with the cost of protection

Narrative:

After risks to each asset have been identified and the impact of losing that asset has been predicted, risk mitigation begins. A cost value is assigned to each risk attempts are made to reduce the risk to an acceptable level at a reasonable cost. If the cost of protecting the asset is higher than the value of the asset, it is not to the advantage of the business to protect that asset in that way.

Costs

- Costs of protection
 - Equipment and software
 - IT support staff
 - User and IT staff training
- Costs due to losses
 - Intrinsic value of the asset
 - System downtime
 - Fines or penalties
 - Loss of face
- Balance security and productivity



Narration:

The cost of protecting an asset can include adding equipment and software such as firewalls and intrusion detection systems. Additional IT support staff may be needed to monitor systems, install virus checking software or perform backups. It may be necessary to invest in training IT staff to use security tools. User security awareness and training programs may be necessary to protect data and hardware assets.

In addition to the upfront price of protecting an asset, the cost of recovering from a security incident must be included in the assessment of risk. The expense of a security incident includes not just the replacement of hardware or the employee time spent recovering the data, they also include the cost of system downtime. This price can be substantial for online retail businesses, financial institutions, credit card companies and many other businesses. In addition to the cost of lost equipment, employee time and lost business opportunities, the organization may face fines or penalties and loss of credibility.

And yet, all of these costs must be balanced against the lost productivity of employees if overly restrictive security measures are employed to reduce risks.

Risk Mitigation

- Countermeasures
- Change security policy or procedures
- Hardware, software or personnel
- Improve backups
- Redundant systems
- Purchase insurance
 - (risk transference)
- Accept the risk



Narrative:

After a thorough evaluation of the threats to assets and the costs of both losing and protecting each has been estimated, countermeasures may be put into place. This is called risk mitigation.

Based on the value of the asset to the organization and the potential cost of instituting countermeasures, the company may choose to make changes to security policy or procedures, add hardware, software or personnel, provide additional training for personnel, improve backup procedures or invest in redundant systems.

Sometimes the assessment process indicates that it is not financially sensible to invest in infrastructure changes. An organization may instead choose to purchase insurance. Or in some cases when the risk is low or the cost of countermeasures is prohibitive, the organization may accept the risk and take no further action.

Residual Risk

- Some risk always remains



INFORMATION SECURITY TRAINING
FOR CAMPUS TECHNICAL STAFF

IST

Narrative:

No matter what you do, some risk of failure always remains. We refer to this as residual risk. With time, money, and attention, risk can be reduced. But it cannot be completely eliminated.

Evaluation and Assessment

- Change is normal
- Repeat risk assessment every 2 to 3 years
- Identify new threats
 - Survey users
 - Monitor logs
 - Track security incidents

Narrative:

But the job is not done after risk assessment and risk mitigation steps have been completed. Risk management is an ongoing activity. Change in IT infrastructure is normal. Hardware is added to the network, software is upgraded or replaced by new products, staff come and go and security policies are updated. As the environment and people evolve, risk assessment and mitigation activities must be done on a periodic basis.

As a matter of good practice, security incidents should be tracked, logs should be monitored and users should be surveyed to identify emerging threats.

People



- Developers
- Operations
- Users
- Managers
- Other staff

Narrative:

Security cannot be assigned to someone else and forgotten. All employees and users must be vigilant in order to prevent security breaches.

Developers are responsible for writing secure code, testing thoroughly and following other best software development practices.

Operations staff must correctly install software, monitor logs, and recover from intrusions.

Users prevent intrusions by avoiding malicious web sites, checking for viruses and spyware frequently and being suspicious of strangers.

Managers are responsible for allocating resources for security. They keep security as a priority for the organization.

Other staff members, including janitorial and support staff, maintain physical security by locking doors and shredding documents.

What to do When a Breach Occurs?

- Security response team responds
- Employees must report security breaches
 - Who to contact
 - How to contact them
 - What incidents to report
 - What information to report

Narrative:

But security incidents may still occur. What should employees do when a security breach occurs?

Every organization should have a security response team trained to deal with security breaches. All employees must know how to report security breaches including
who to contact
how to contact them
what incidents to report and
what information to report

Security Response Team - Incident Response

- Triage
 - interpret and prioritize reports
 - verify scope of incident
- Coordinate
 - Document event
 - Notify others
- Resolve the incident
 - Analyze problem
 - Eliminate cause
 - Restore systems



Narrative:

The security response team's first responsibility is to respond to incidents. During the triage stage, the team interprets reports of incidents and prioritizes them. They verify the scope of the incident and determine whether it actually occurred. Most organizations have a Help Desk to perform initial aspects of incident response.

The security response team also coordinates activities as events unfold. They document and categorize the nature of the event and notify others as appropriate.

The response team also resolves the incident. They analyze the problem and eliminate its immediate cause. If necessary, they restore systems to correct operation.

Security Response Team - Reporting

- Report to management
- Report to users
- Communicate with external response teams
- Collect statistics



Narrative:

Once the immediate security incident has been resolved, the response team is obligated to report to management. The report may include an assessment of damages as well as recommendations for mitigating future incidents of a similar nature.

The security response team may also report the resolution of the incident to users if they have been affected.

Of equal importance is communication with response teams at other organizations. The Morris Worm brought the Internet to its knees in 1988. From that we learned the importance of communication and coordinated incident responses to Internet threats.

A number of formal CERT (Computer Emergency Response Team) networks have been established including Carnegie Mellon's CERT project and the US government's US-CERT program. Members ask one another for advice, share information and cooperate with other organizations to resolve incidents.

Security response teams also collect statistics on incidents. When incident information is analyzed over time and shared with other organizations, emerging trends can be detected and early responses can be made.

Security response team – Other Activities

- Evaluate new products
- Recommend purchases
- Perform security audits
- Educate and train users

Narrative:

When not responding to emergencies, the security response team performs preventative maintenance. They evaluate new products from a security perspective, recommend security-related tools for purchase or installation, perform security audits and educate and train users.

Training and Awareness

- Train users to
 - Prevent intrusions
 - Understand why security is important to the organization
 - Understand why security is important to the individual



INFORMATION SECURITY TRAINING **IST**
FOR CAMPUS TECHNICAL STAFF

Narrative:

All employees must be made aware of security policies and the consequences of violating them. Users can prevent many intrusions when they understand why security is important to the organization and how to practice good security hygiene.

Users circumvent security measures and create breaches when security measures interfere with productivity. For example, server room doors are propped open when workers have to find the only person with a key in order to gain entrance many times a day. Informed users are more apt to suggest compromises and less apt to create breaches.

Sometimes users do not know how to employ good security. For example, many users do not know how to create strong passwords. Again, training can be useful.

Obviously, IT workers need ongoing, specialized training as they continue to fight the battle against cybercrime. SANS and CERT are two of the leading security training organizations. The SANS Institute provides information security training and certification. CERT courses focus more heavily on network computing security.

Best Practices for Users



- Beware of social engineering
- Passwords are private
- Limit access to secured areas
- Reporting incidents

INFORMATION SECURITY TRAINING **IST**
FOR CAMPUS TECHNICAL STAFF

Narrative:

As part of a layered defense approach to security, users can be the organization's biggest liability – or its first defense.

Social engineering remains one of the largest causes of security incidents. However, users can be trained not to give out sensitive information without proper authentication.

Passwords sharing can be discouraged through good policies and procedures followed by awareness programs. Humor usually works well to remind folks about good practices.

Limiting access to secure areas is another best practice. If the goal is to interfere with a business, stealing a server is as effective as running a rootkit. A locked door can be an effective deterrent – as long as it stays locked.

Finally, users need to be trained to report incidents. The users are usually the first to notice problems with performance or outages. If the problems are not reported, it simply takes much longer for them to be resolved.

Summary

- Risk management
 - Risk assessment
 - Risk mitigation
 - Evaluation and assessment
- Security response teams
- Training and awareness

Narrative:

Risk management starts with risk assessment. Appropriate countermeasures to threats are designed based on the value of the asset and the probability that a threat will occur. We refer to this as risk mitigation. Ongoing evaluation of risks and countermeasures is necessary in IT environments which change frequently over time.

Security response teams interpret and prioritize reports of incidents, notify others, provide coordination and resolve the incidents. They also share information with national computer emergency response groups to promote the security of the entire Internet.

Training and awareness can prepare users to prevent social engineering attacks and reduce acts of subversion.