# Security Evaluation

Shweta A. Chawla
Founder & Investigator
SC Cyber Solutions

SC
Cyber Solutions

# Security Evaluation

- The examination of a system to determine its degree of compliance with a stated security model, security standard, or specification.
- The evaluation may be conducted
  - by analyzing the detailed design, especially of the software, often using verification and validation
  - by observing the functional behavior of the system
  - by attempting to penetrate the system using techniques available to an attacker



shweta@sccybersolutions.com

SC
Cyber Solutions




shweta@sccybersolutions.com

SC
Cyber Solutions

# Why are Security Evaluations Important

- Identify assets
- Enable the IT team to identify areas of weakness and opportunities for growth in security protection
- Identify and secure sensitive data
- Understands where current vulnerabilities exist
- Prioritise these vulnerabilities
- Make informed decisions about security and training expenses
- Build contingency plans
- Meet compliance requirements
- Update, improve cybersecurity policies and procedures



shweta@sccybersolutions.com

SC
Cyber Solutions

- Access control and user account management
- Information security governance and risk management
- Improved workstation and device security
- Business continuity and disaster recovery planning
- Cryptography
- Physical (environmental) security
- Network and operations security
- Security architecture and design



shweta@sccybersolutions.com

SC
Cyber Solutions

# Asset Management

- Asset management is the process of identifying, on a continuous, real-time basis, the IT assets that your organization owns and the potential security risks or gaps that affect each one

- An asset is anything of value to a business
- And /or anything of value that supports the business and its operations

- In the case of security audits, this asset is one that relates to information services



shweta@sccybersolutions.com

SC
Cyber Solutions

- Information asset
  - Information stored in any form
  - A dataset of information arranged and managed as a single, valuable entity
- Physical asset
  - Equipment that add value
- People asset
  - People working within the organization with access to information
- Critical asset
  - Any of the above
  - Important to maintain functioning of the business



shweta@sccybersolutions.com

SC
Cyber Solutions

# Importance of Asset Management

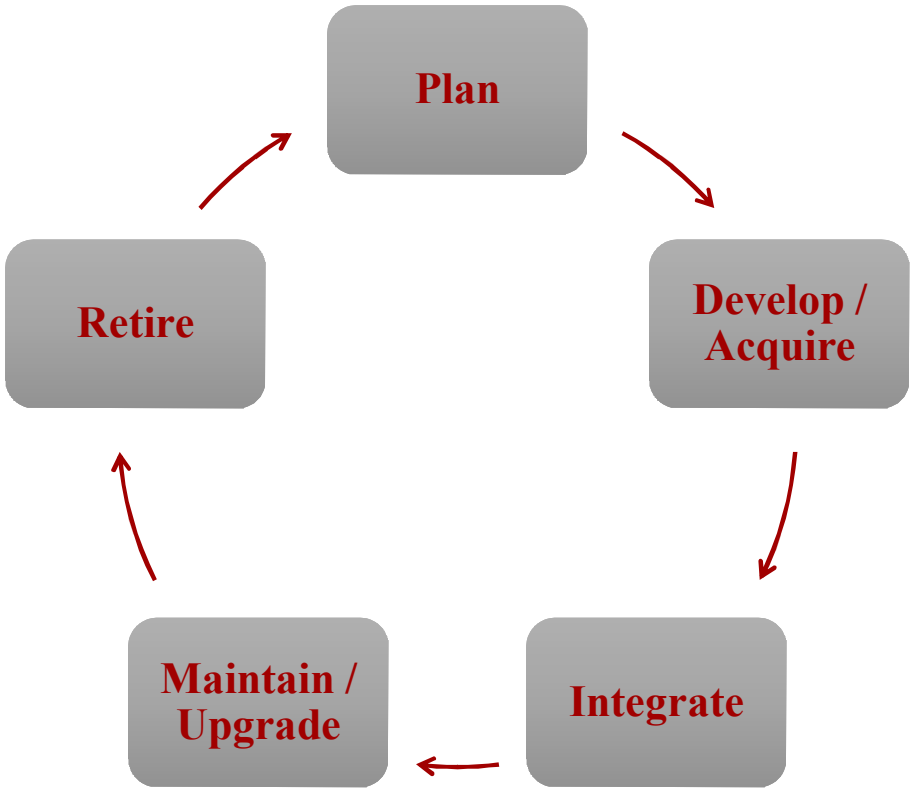
- Identify the assets and the threats they face
- Manage the risks associated with threats
- Streamlines asset security
- Create faster incident response processes



shweta@sccybersolutions.com

SC
Cyber Solutions

# IT Asset Lifecycle






shweta@sccybersolutions.com

SC
Cyber Solutions

# Asset Management


http://www.thegti.com/FckImages/image/gasset%20picture.png



shweta@sccybersolutions.com

SC
Cyber Solutions

# Asset Management

- A sample list of information to gather per asset
  - Software
  - Hardware
  - Data
  - Interfaces
  - Users
  - Support personnel
  - Mission or purpose
  - Criticality
  - Functional requirements
  - IT security policies
  - IT security architecture
  - Network topology
  - Information storage protection
  - Information flow
  - Technical security controls
  - Physical security environment
  - Environmental security



shweta@sccybersolutions.com

SC
Cyber Solutions

# Risk

- The possibility that something bad might happen
- Effect, impact of this is usually uncertain
- The nature of risk is generally subjective



shweta@sccybersolutions.com

SC
Cyber Solutions

# Cyber Risk

- The potential for an unplanned, negative business outcome involving the failure or misuse of IT
- Risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems
- Types of risk
  - Strategic
  - Operational
  - Financial
  - External

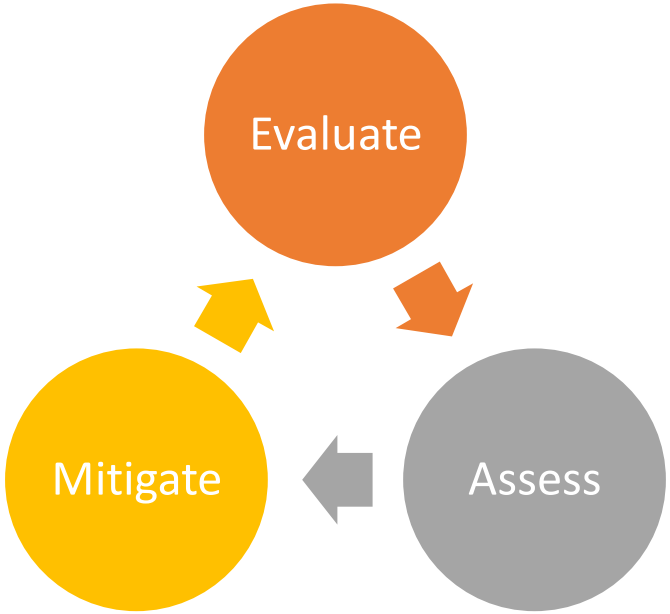


shweta@sccybersolutions.com

SC
Cyber Solutions

# Risk Management Components

- Evaluation, to identify assets and evaluate their properties and characteristics
- Risk assessment, to discover threats and vulnerabilities that pose risk to assets
- Risk mitigation, to address risk by transfer-ring, eliminating or accepting it






shweta@sccybersolutions.com

SC
Cyber Solutions

# Risk Management

- Process of identifying, assessing and controlling threats
- Studies the relationship between risks and impacts



shweta@sccybersolutions.com

SC
Cyber Solutions

# Risk Threshold

Risk Appetite

Risk Tolerance

Unacceptable Risk



shweta@sccybersolutions.com

SC
Cyber Solutions

# Risk Management Process





shweta@sccybersolutions.com

SC
Cyber Solutions

- Risk
  - Potential for loss, damage, destruction of assets
- Vulnerability
  - Weakness in the system, asset, procedure
- Threat
  - Exploits a vulnerability
  - Can destroy, damage or disrupt an asset
- Exploit
  - Use something for an advantage
  - A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic



shweta@sccybersolutions.com

SC
Cyber Solutions

# IT Security Risk Assessment

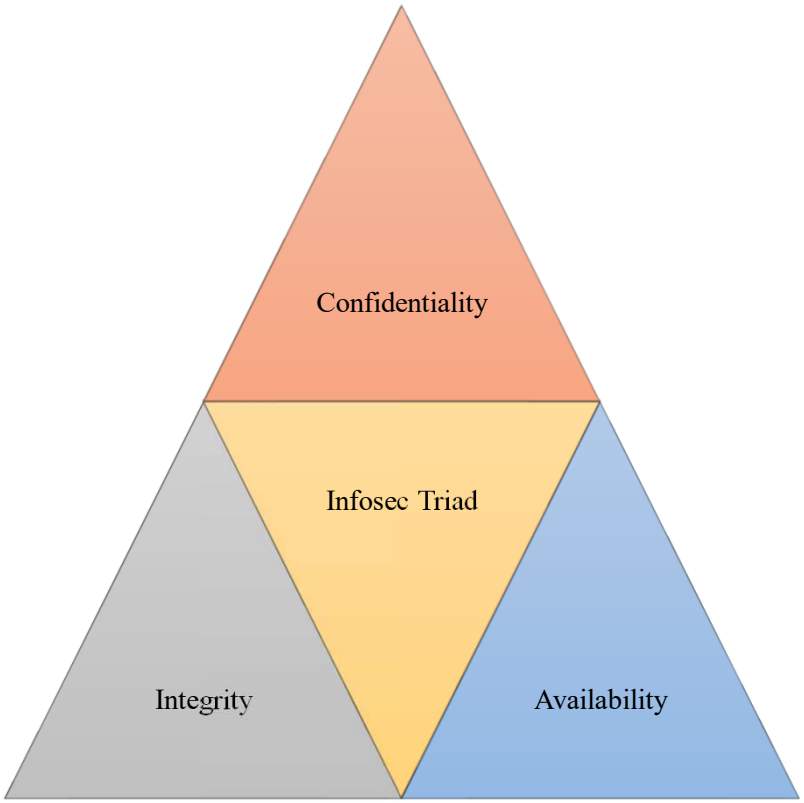
- Identify assets
- Identify risks
- Identify threats
  - Threat => Vulnerability => Risk realized
- Identify vulnerabilities
- Develop metrics
  - Asset X Threat X Vulnerability = Risk
- Consider historical breach data
- Calculate cost
- Perform risk to asset tracking



shweta@sccybersolutions.com

SC
Cyber Solutions

# Assessment Parameters






shweta@sccybersolutions.com

SC
Cyber Solutions

| Methodology | | | |
|---|---|---|---|
| Threat | Likelihood | Impact | Risk |
| Loss of confidentiality | | | |
| Loss of integrity | | | |
| Loss of availability | | | |
| | | Overall Risk | |

Risk level = Likelihood X Impact



shweta@sccybersolutions.com

SC
Cyber Solutions

# Calculate Risk Level

| Likelihood \ Impact | Negligible | Minor | Moderate | Significant | Severe |
|---|---|---|---|---|---|
| Very Likely | Low | Moderate | High | High | High |
| Likely | Low | Moderate | Moderate | High | High |
| Possible | Low | Low | Moderate | Moderate | High |
| Unlikely | Low | Low | Moderate | Moderate | Moderate |
| Very Unlikely | Low | Low | Low | Moderate | Moderate |



shweta@sccybersolutions.com

SC
Cyber Solutions

# Threat Matrix

- Risk assessment matrix
- Probability and Severity risk matrix
- Visual tool that depicts the potential risks affecting a business
- The risk matrix is based on two intersecting factors:
  - the *likelihood* that the risk event will occur,
  - the potential *impact* that the risk event will have on the business
- ∴ it helps visualize probability vs severity of a potential risk



shweta@sccybersolutions.com

SC
Cyber Solutions

# Importance of Threat Matrix

- Prioritisation of risk
- Strategic implementation of risk management
- Realistic view of risk posture



shweta@sccybersolutions.com

SC
Cyber Solutions

# Threat Matrix

| Threat Matrix | | | | | | | |
|---|---|---|---|---|---|---|---|
| Vulnerabilities / Threats | Firewalls | Databases | Application Architecture | Physical Security | Insecure Wireless | Internet-based service (Like VPN) | **Total Score** |
| *Intrusion (Hacking, Password Attacks)* | 9 | 3 | 9 | 9 | 9 | 3 | **42** |
| *Insider Attacks* | 3 | 3 | 3 | 9 | 3 | 1 | **22** |
| *DDoS* | 9 | 0 | 9 | 1 | 3 | 3 | **25** |
| *Theft of Hardware* | 1 | 1 | 1 | 9 | 3 | 1 | **16** |



shweta@sccybersolutions.com

SC
Cyber Solutions

| Threat | Vulnerability | Asset | Impact | Likelihood | Risk | Control Recommendations |
|---|---|---|---|---|---|---|
| System failure — Overheating in server room<br>High | Air-conditioning systems is ten years old.<br>High | Servers<br>Critical | All services (website, email, etc.) will be unavailable for at least 3 hours.<br>Critical | High<br>Current temperature in server room is 40C | High<br>Potential loss of $50,000 per occurrence | Buy a new air conditioner, $3,000 cost. |
| Malicious human (interference) — DDOS attack.<br>High | Firewall is configured properly and has good DDOS mitigation.<br>Low | Website<br>Critical | Website resources will be unavailable.<br>Critical | Medium<br>DDOS was discovered once in 2 years. | Medium<br>Potential loss of $10,000 per hour of downtime | Monitor the firewall. |
| Natural disasters — Flooding<br>High | Server room is on the 3rd floor.<br>Low | Servers.<br>Critical | All services will be unavailable.<br>Critical | Low<br>Last flood in the area happened 10 years ago. | Low | No action needed. |
| Accidental human interference — Accidental file deletions<br>High | Permissions are configured properly; IT auditing software is in place; backups are taken regularly.<br>Low | Files on a file share<br>Medium | Critical data could be lost but almost certainly could be restored from backup.<br>Low | Medium | Low | Continue monitoring permissions changes, privileged users and backups. |



shweta@sccybersolutions.com

SC
Cyber Solutions

# Calculating Cost

- Threat likelihood = medium = 0.5 (scale – 0 to 1)
- Threat impact = high = 1
- Total sensitive records = 1000
- Cost per sensitive record = 20
- Monetary risk = (Threat likelihood X threat impact) X (cost per item x total items) = (0.5 X 1) x (20 X 1000) = 10000



shweta@sccybersolutions.com


Contact details:
Mob: +91 98230 80864
shweta@sccybersolutions.com
www.sccybersolutions.com
@sccs1300

SC
Cyber Solutions

- Some things to look for in an audit
  - Insufficient password complexity
  - Over permissive ACLs on folders
  - Inconsistent ACLs on folders
  - Non-existent or insufficient file activity auditing
  - Non-existent or insufficient review of auditing data
  - Correct security software and security configurations on all systems
  - Only compliant software installed on systems
  - Data retention policies followed
  - Disaster recovery plans updated and tested
  - Incident response plans updated and tested
  - Sensitive data stored and protected correctly with encryption
  - Change management procedures followed



shweta@sccybersolutions.com