Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Acknowledgement

- Google Cyber Security

Certified Information Systems Security Professional (CISSP):

Security Domains for Cyber Analyst

CISSP: Security Domains for Cyber Analyst

- D 1: Security and risk management
- D 2: Asset security
- D 3: Security architecture and engineering
- D 4: Communication and network security
- D 5: Identity and access management
- D 6: Security assessment and testing
- D 7: Security operations
- D 8: Software development security

D1: Security and risk management

- All organizations must develop their **security posture**.

- Security posture is an organization's ability to manage its defense of critical assets and data and react to change.

- **Elements** of D1 that impact an organization's security posture include:
  - Security goals and objectives
  - Risk mitigation processes
  - Compliance
  - Business continuity plans
  - Legal regulations
  - Professional and organizational ethics

D1: Security and risk management

- **InfoSec** (related to D1) refers to a set of processes established to secure information.
- An organization may use playbooks and implement training as a part of their D1 program,
  - based on their needs and perceived risk.

InfoSec **design processes** include:

- Incident response
- Vulnerability management
- Application security
- Cloud security
- Infrastructure security

For example, a security team may need to alter how **PII** is treated in order to adhere to the European Union's General Data Protection Regulation (GDPR).

D2: Asset security

- It involves managing the cybersecurity processes of organizational assets,
  - including storage, maintenance, retention, and destruction of physical and virtual data.
- As **loss or theft** of assets can expose an organization and increase the level of risk,
- keeping track of assets and the data they hold is essential.
- **Conducting** a security impact analysis, **establishing** a recovery plan, and **managing** data exposure
  - will depend on the level of risk associated with each asset.
- **Security analysts** may need to store, maintain, and retain data by creating backups to ensure ability to restore environment
  - in case a security incident places the organization's data at risk.

D3: Security architecture and engineering

- D3 focuses on managing **data security**.
- Ensuring effective **tools, systems, and processes** are in place helps protect assets and data.
  - Security architects and engineers create these processes.
- **Shared responsibility** aspect of D3 means all individuals involved take an active role in lowering risk during the design of a security system.

Additional design principles related to D3

- Threat modeling
- Least privilege
- Defense in depth
- Fail securely
- Separation of duties
- Keep it simple
- Zero trust
- Trust but verify

Example: the use of a security information and event management (**SIEM**) tool

- to monitor for flags related to unusual login or user activity to access private data

D4: Communication and network security

- D4 focuses on managing and securing **physical networks** and wireless communications.
  - includes on-site, remote, and cloud comm.
- Organizations must ensure data remains secure
- **Challenge:** managing external connections to make certain that remote workers are securely accessing its networks

Designing network security controls (like restricted network access)

- can help protect users and ensure network remains secure when employees travel or work outside of the main office.

D5: Identity and access management

- D5 focuses on **keeping data secure** by ensuring
  - user identities are trusted and authenticated and
  - that access to physical and logical assets is authorized.
- This helps prevent unauthorized users, while allowing authorized users to perform their tasks.

- D5 uses the principle of **least privilege**,
  - i.e., granting only the minimal access and authorization required to complete a task.

Example: a cybersecurity analyst might be asked to ensure that for private data of a customer

- customer service representatives can only view
  - such as their phone number, while working to resolve the customer's issue;
- then remove access when the customer's issue is resolved.

D6: Security assessment and testing

- D6 focuses on **identifying and mitigating** risks, threats, and vulnerabilities.
- Security **assessments** help organizations determine whether their internal systems are secure or at risk.
- Organizations might employ pen testers to find **vulnerabilities** that could be exploited by a threat actor.
- D6 suggests that organizations **conduct** security control testing, as well as **collect** and **analyze** data.
- it also emphasizes the importance of conducting security audits to monitor for and reduce the probability of a data breach.
- cybersecurity professionals may be **tasked** with auditing user permissions to validate that users have the correct levels of access to internal systems.

D7: Security operations

D7 focuses on the

- **investigation** of a potential data breach and
- Applying **preventative measures (**using strategies, processes, and tools) after occurrence of a security incident.
- This includes
  - Training and awareness
  - Reporting and documentation
  - Intrusion detection and prevention
  - SIEM tools
  - Log management
  - Incident management
  - Playbooks
  - Post-breach forensics
  - Reflecting on lessons learned

The cybersecurity professionals involved in D7

- work as a team to manage, prevent, and investigate threats, risks, and vulnerabilities.
- are trained to handle active attacks, such as large amounts of data being accessed from an organization's internal network, outside of normal working hours.

Once a threat is identified, the team works diligently to keep private data and information safe from threat actors.

D8: Software development security

- D8 focuses on using **secure** programming practices and **guidelines** to create secure applications.
  - Which help deliver secure and reliable services, to protect organizations and their users.
- Security must be added into each element of SDLC, from design and development to testing and release.

To achieve security,

- Software development process must have security in mind at each step.
- Security cannot be an afterthought.
- Performing application security tests can help ensure vulnerabilities are identified and mitigated accordingly.

D8: Software development security

- Having a system in place
  - to test the programming conventions, software executables, and security measures embedded in the software is necessary.

- Having quality assurance and pen tester professionals
  - to ensure the software has met security and performance standards.

- For example, an entry-level analyst working for a pharmaceutical company might be asked
  - to make sure encryption is properly configured for a new medical device that will store private patient data.

Managing Threats, Risks and Volunerabilities

Risk management

❖A primary goal of organizations is to protect assets.

- An **asset** is an item perceived as having value to an organization. Assets can be digital or physical.

Examples of **physical assets** include:

- Payment kiosks
- Servers
- Desktop computers
- Office spaces

Examples of **digital assets** include the personal information of employees, clients, or vendors, such as:

- Social Security Numbers (SSNs), or unique national identification numbers assigned to individuals
- Dates of birth
- Bank account numbers
- Mailing addresses

Managing Threats, Risks and Vulnerabilities

Strategies to Mitigate Risks

- **Acceptance**: Accepting a risk to avoid disrupting business continuity
- **Avoidance**: Creating a plan to avoid the risk altogether
- **Transference**: Transferring risk to a third party to manage
- **Mitigation**: Lessening the impact of a known risk

- Additionally, organizations implement risk management processes based on widely accepted **frameworks**
  - to help protect digital and physical assets from various threats, risks, and vulnerabilities.

Example Frameworks

- National Institute of Standards and Technology Risk Management Framework (NIST RMF)
- Health Information Trust Alliance (HITRUST)

Managing Threats, Risks and Vulnerabilities

Most common threats, risks, and vulnerabilities

❖**Threats (**event that can negatively impact assets)

- Insider threats
- Advanced persistent threats (APTs)

•**Risks** (anything that can impact confidentiality, integrity, or availability of an asset)

- Internal risk
- External risk
- Legacy systems
- Multiparty risk
- Software compliance/licensing

▪ **Vulnerabilities** (a weakness that can be exploited by a threat)

Some vulnerabilities include:

- **ProxyLogon:**
- **ZeroLogon:**
- **Log4Shell:**
- **PetitPotam:**
- **Security logging and monitoring failures:**
- **Server-side request forgery:**

Frameworks and Controls

Security frameworks are guidelines used for building plans to help mitigate risk and threats to data and privacy.

- Frameworks support organizations' ability to adhere to compliance laws and regulations.
- **Example:** healthcare industry uses frameworks to comply with United States' Health Insurance Portability and Accountability Act (HIPAA),
  - which requires that medical professionals keep patient information safe.

Security controls are

- safeguards designed to reduce *specific* security risks.
- measures used by organizations to lower risk and threats to data and privacy.
- **Example:** a control used alongside frameworks to ensure a hospital remains compliant with HIPAA
  - requires that patients use MFA to access their medical records **(identity validation).**
- MFA may help mitigate potential risks and threats to private data

Specific Frameworks and Controls

Organizations can use different frameworks and controls to remain compliant with regulations and achieve their security goals.

- **Cyber Threat Framework** (CTF) and
- International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27001.
- Several common security controls are used alongside these types of frameworks

Cyber Threat Framework

According to Office of the Director of National Intelligence,

- the CTF was developed to provide "**a common language** for describing and communicating information about cyber threat activity."
- CTF helps cybersecurity professionals analyze and share information more efficiently.
- This allows organizations to **improve** their **response** to
  - constantly evolving cybersecurity landscape and threat actors' many tactics and techniques.

Specific Frameworks and Controls

ISO/IEC 27001

- An internationally recognized and used framework (a family of standards)
- enables organizations of all sectors and sizes to manage the security of assets (like financial information, intellectual property, employee data, and information entrusted to third parties)
- provides requirements for an IS management system, best practices, and controls
  - that support an organization's ability to manage risks.
- Although it does not require the use of specific controls,
  - it does provide a collection of controls to improve security posture.

Specific Frameworks and Controls

Controls

- Controls are used alongside frameworks to reduce the possibility and impact of a security threat, risk, or vulnerability.
- Controls can be physical, technical, and administrative
- Controls are typically used to prevent, detect, or correct security issues

Examples of physical controls:

- Gates, fences, and locks
- Security guards
- Closed-circuit television (CCTV), surveillance cameras, and motion detectors
- Access cards or badges to enter office spaces

Examples of technical controls:

- Firewalls
- MFA
- Antivirus software

Examples of administrative controls:

- Separation of duties
- Authorization
- Asset classification