Here's a tabulated comparison between cybersecurity and information security:

Aspect	Cybersecurity	Information Security
Definition	Protects digital systems, networks, and data	Protects information in any form (digital or physical)
Scope	Primarily focuses on digital assets and systems	Encompasses all aspects of information, including physical documents, data, and systems
Focus	Prevents unauthorized access, attacks, and threats in the cyberspace	Ensures confidentiality, integrity, and availability of information assets, regardless of location
Measures	Includes measures such as firewalls, antivirus software, intrusion detection systems (IDS), encryption, etc.	Encompasses policies, procedures, technologies, and physical security measures
Threats	Addresses threats such as malware, phishing, ransomware, hacking, DDoS attacks, etc.	Addresses threats such as unauthorized access, data breaches, theft, espionage, social engineering, etc.
Application	Applicable to digital environments, networks, and online activities	Applicable to both digital and physical information assets, as well as organizational processes and practices
Importance	Vital for protecting digital infrastructure, data privacy, and maintaining trust in online transactions and communications	Essential for safeguarding sensitive information, maintaining compliance with regulations, and preserving organizational reputation and trust

Pnem: def—>focus-> threat->measure->appli->imp.

2. Cybersecurity principles are fundamental guidelines that organizations and individuals should follow to protect digital assets, systems, and data from cyber threats. Here are some key principles of cybersecurity: CIA AAA

1. **Confidentiality**: Ensure that sensitive information is accessed only by authorized individuals or systems. Use encryption, access controls, and secure communication channels to protect data from unauthorized access.

2. **Integrity**: Maintain the accuracy and reliability of data and systems. Implement measures such as data validation, checksums, and digital signatures to prevent unauthorized alterations or modifications to data.

3. **Availability**: Ensure that systems and data are available and accessible when needed. Implement redundancy, backups, and disaster recovery plans to mitigate the impact of cyber attacks, system failures, or natural disasters.

4. **Authentication**: Verify the identity of users and systems to prevent unauthorized access. Use strong passwords, multi-factor authentication (MFA), and biometric authentication to ensure that only authorized individuals can access sensitive information or systems.

5. **Authorization**: Grant appropriate permissions and privileges to users based on their roles and responsibilities. Implement access controls, least privilege principles, and segregation of duties to limit access to sensitive data and systems.

6. **Accountability**: Hold individuals and entities accountable for their actions in cyberspace. Implement logging, auditing, and monitoring mechanisms to track user activities, detect anomalies, and investigate security incidents.

7. **Resilience**: Build resilience against cyber threats by implementing proactive security measures, conducting risk assessments, and continuously monitoring and updating security

controls. Develop incident response plans and conduct regular security training and awareness programs to prepare for and respond to cyber attacks effectively.

8. **Defense-in-Depth**: Implement multiple layers of security controls to create a robust defense against cyber threats. Use a combination of technical, administrative, and physical controls to protect against various attack vectors and minimize the impact of security breaches.

9. **Privacy**: Respect individuals' privacy rights and protect their personal information from unauthorized access or disclosure. Comply with privacy regulations and standards, such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act), to ensure the lawful and ethical handling of sensitive data.

10. **Continuous Improvement**: Adopt a mindset of continuous improvement in cybersecurity practices. Stay informed about emerging threats and vulnerabilities, conduct regular security assessments and penetration tests, and update security policies and procedures to adapt to evolving cyber risks.

By adhering to these cybersecurity principles, organizations and individuals can enhance their security posture and better protect themselves against cyber threats and attacks.

face.# CHALLENGES OF CYBER SECURITY

- For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system.**Elements of cyber** encompass all of the following:
- **Network security**
- **Application security**
- **Endpoint security**
- **Data security**
- **Identity management**
- **Database and infrastructure security**
- **Cloud security**
- **Mobile security**
- **Disaster recovery/business continuity planning**
- **End-user education**

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves.

- Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats.
- Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (**NIST**) issued guidelines in its risk assessment **framework** that recommend a shift toward **continuous monitoring** and real-time assessments, a data-focused approach to security

as opposed to the traditional perimeter-based model.

I'd be glad to explain the Normal System Development Life Cycle (SDLC) and the Security System Development Life Cycle (SSDLC):

Normal System Development Life Cycle (SDLC)

The SDLC is a structured approach for planning, creating, deploying, and maintaining information systems. It ensures the system meets user needs, functions as intended, and delivers value. Here's a breakdown of the typical SDLC phases:

1. **Planning and Requirement Analysis:**
    - Define project goals and objectives.
    - Gather user requirements, focusing on what the system needs to do.
    - Identify constraints, such as budget and timeline.
    - Determine feasibility (can it be built? is it worth it?).
2. **Design:**
    - Translate user requirements into a system architecture.
    - Design the user interface (UI) for ease of use.
    - Choose appropriate data structures and algorithms.
    - Create a detailed system blueprint.
3. **Development and Implementation:**
    - Code the system based on the design specifications.
    - Develop unit tests to verify individual components work as expected.
    - Integrate components into a working system.
    - Deploy the system to the production environment.
4. **Testing:**
    - Perform system testing to ensure the entire system functions as designed.
    - Conduct user acceptance testing (UAT) to get user feedback and identify usability issues.
    - Fix bugs and defects identified during testing.
5. **Deployment and Maintenance:**
    - Train users on how to use the system.

- Provide ongoing maintenance to fix bugs, add new features, and address changing user needs.

Security System Development Life Cycle (SSDLC)

The SSDLC incorporates security best practices into the entire SDLC, resulting in more robust and secure systems. It builds upon the SDLC by proactively addressing security throughout the development process. Here's how it enhances each SDLC phase:

1. **Planning and Security Requirements Analysis:**
    - In addition to user needs, identify security risks, threats, and vulnerabilities.
    - Define security controls (e.g., access controls, encryption) and compliance requirements (e.g., HIPAA, PCI DSS).
    - Conduct security threat modeling to identify potential attack vectors.
2. **Secure Design:**
    - Integrate security considerations into the system design.
    - Implement secure coding practices to minimize vulnerabilities (e.g., input validation, buffer overflow prevention).
    - Use secure authentication and authorization mechanisms.
    - Design for data protection (e.g., encryption at rest and in transit).
3. **Development and Secure Coding:**
    - Developers follow secure coding practices to write code that is resistant to attacks.
    - Use code review processes to identify and fix security vulnerabilities.
    - Conduct static and dynamic application security testing (SAST and DAST) to identify potential security flaws.
4. **Security Testing:**

- In addition to functional testing, perform penetration testing (pen testing) to simulate real-world attacks and identify security weaknesses.
- Conduct vulnerability scanning to identify known security vulnerabilities in system components.
- Address security vulnerabilities identified during testing before deployment.

5. **Deployment and Security Maintenance:**

   - Deploy the system with security best practices in mind (e.g., secure configuration, patch management).
   - Implement ongoing security monitoring to detect and respond to threats promptly.
   - Conduct regular security audits and vulnerability assessments to identify and address emerging risks.
   - Provide security awareness training for users to identify and avoid cyberattacks.

Key Differences:

Feature	SDLC	SSDLC
Focus	Functionality, usability, meeting user needs	Security, protecting data and systems
Security Consideration	Addressed in later stages (sometimes)	Integrated throughout the entire development process
Security Testing	May occur, but not the primary focus	A crucial phase, with specialized security testing
Coding Practices	Standard coding practices	Secure coding practices to minimize vulnerabilities
Maintenance	Bug fixes, new features	Includes ongoing security monitoring and updates

Benefits of SSDLC:

- Reduced risk of cyberattacks and data breaches
- Increased system reliability and uptime
- Enhanced compliance with security regulations
- Improved user confidence in the system's security

Choosing between SDLC and SSDLC depends on the specific project's security requirements. However, in today's security-conscious world, incorporating security considerations throughout the development process using SSDLC is generally recommended for most systems that handle sensitive data.

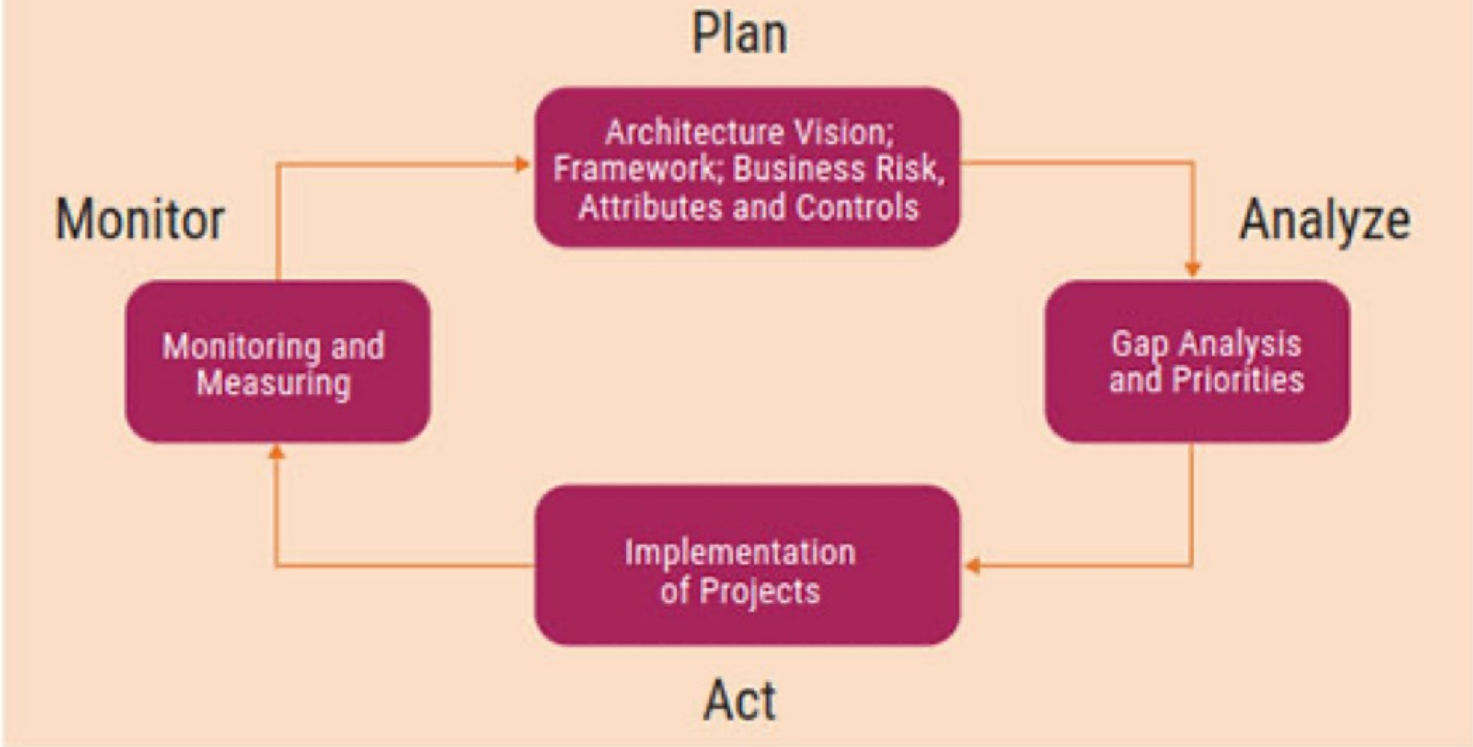
The Best Framework for Security Architecture

- Several frameworks exist for security architecture, the most important ones are SABSA, O-ESA and OSA. They complement and overlap each other.
- The challenge is to develop a security architecture that is effective.
- If you look at the existing frameworks, you may find that they never fit exactly in your situation. The concept of security architecture has many faces, and each framework has its own focus and strengths.
- How to make the best security architecture out of

Security architecture

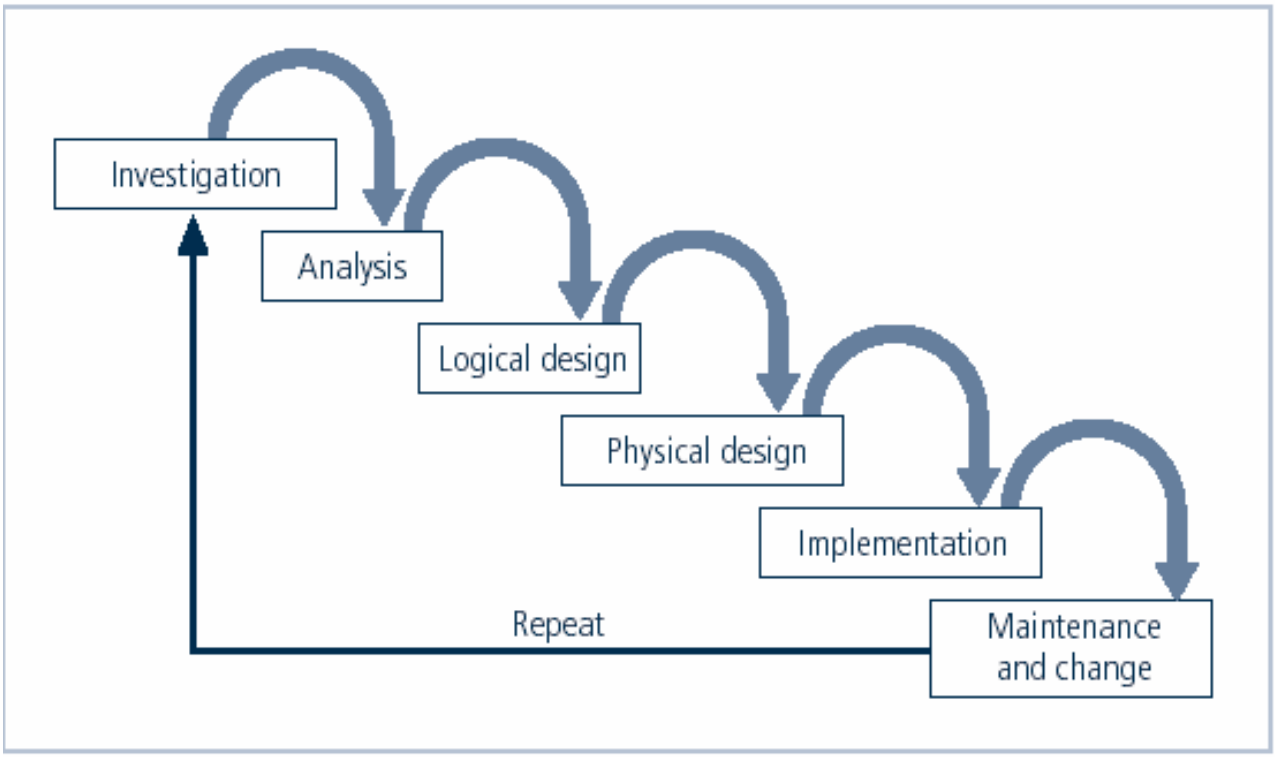
- A top-down approach to enterprise security architecture can be used to build a business-driven security architecture.1
- An approach to prioritizing the security projects that are identified as part of architecture assessment while ensuring business alignment follows.
- Business risk and attributes can be used to identify relevant security controls and a maturity assessment can be performed to identify the current and desired maturity level of those controls and

Figure 1—Security Architecture Life Cycle



The Systems Development Life Cycle

- Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization
- Methodology is formal approach to problem-solving based on structured sequence of procedures
- Using a methodology
  - ensures a rigorous process
  - avoids missing steps
- Goal is creating a comprehensive security posture/ program
- Traditional SDLC consists of six general phases



SDLC Waterfall Methodology

Investigation

- What problem is the system being developed to solve?
- Objectives, constraints and scope of project are specified
- Preliminary cost-benefit analysis is developed
- At the end, feasibility analysis is performed to assesses economic, technical, and behavioral feasibilities of the process

Analysis

- Consists of assessments of the organization, status of current systems, and capability to support proposed systems
- Analysts determine what new system is expected to do and how it will interact with existing systems
- Ends with documentation of findings and update of feasibility analysis

Logical Design

- Main factor is business need; applications capable of providing needed services are selected
- Data support and structures capable of providing the needed inputs are identified
- Technologies to implement physical solution are determined
- Feasibility analysis performed at the end

Physical Design

- Technologies to support the alternatives identified and evaluated in the logical design are selected
- Components evaluated on make-or-buy decision
- Feasibility analysis performed; entire solution presented to end-user representatives for approval

Implementation

- Needed software created; components ordered, received, assembled, and tested
- Users trained and documentation created
- Feasibility analysis prepared; users presented with system for performance review and acceptance test

Maintenance and Change

- Consists of tasks necessary to support and modify system for remainder of its useful life
- Life cycle continues until the process begins again from the investigation phase
- When current system can no longer support the organization's mission, a new project is implemented

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC may be adapted to support specialized implementation of an

IS project

- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

Investigation

- Identifies process, outcomes, goals, and constraints of the project
- Begins with enterprise information security policy
- Organizational feasibility analysis is performed

Analysis

- Documents from investigation phase are studied
- Analyzes existing security policies or programs, along with documented current threats and associated controls
- Includes analysis of relevant legal issues that could impact design of the security solution
- The risk management task begins

Logical Design

- Creates and develops blueprints for information security

- Incident response actions planned:
  - Continuity planning
  - Incident response
  - Disaster recovery
- Feasibility analysis to determine whether project should continue or be outsourced

Physical Design

- Needed security technology is evaluated, alternatives generated, and final design selected
- At end of phase, feasibility study determines readiness of organization for project

Implementation

- Security solutions are acquired, tested, implemented, and tested again
- Personnel issues evaluated; specific training and education programs conducted
- Entire tested package is presented to management for final approval

Maintenance and Change

- Perhaps the most important phase, given the ever-changing threat environment
- Often, reparation and restoration of information is a constant duel with an unseen adversary
- Information security profile of an organization requires constant adaptation as new threats emerge and old threats evolve

Security Professionals and the Organization

- Wide range of professionals required to support a diverse information security program
- Senior management is key component; also, additional administrative support and technical expertise required to implement details of IS program

Senior Management

- Chief Information Officer (CIO)
  - Senior technology officer
  - Primarily responsible for advising senior executives on strategic planning
- Chief Information Security Officer (CISO)
  - Primarily responsible for assessment, management, and implementation of IS in the organization
  - Usually reports directly to the CIO

5)
The Best Framework for Security Architecture

- Several frameworks exist for security architecture, the most important ones are SABSA, O-ESA and OSA. They complement and overlap each other.
- The challenge is to develop a security architecture that is effective.
- If you look at the existing frameworks, you may find that they never fit exactly in your situation. The concept of security architecture has many faces, and each framework has its own focus and strengths.
- How to make the best security architecture out of this diversity?

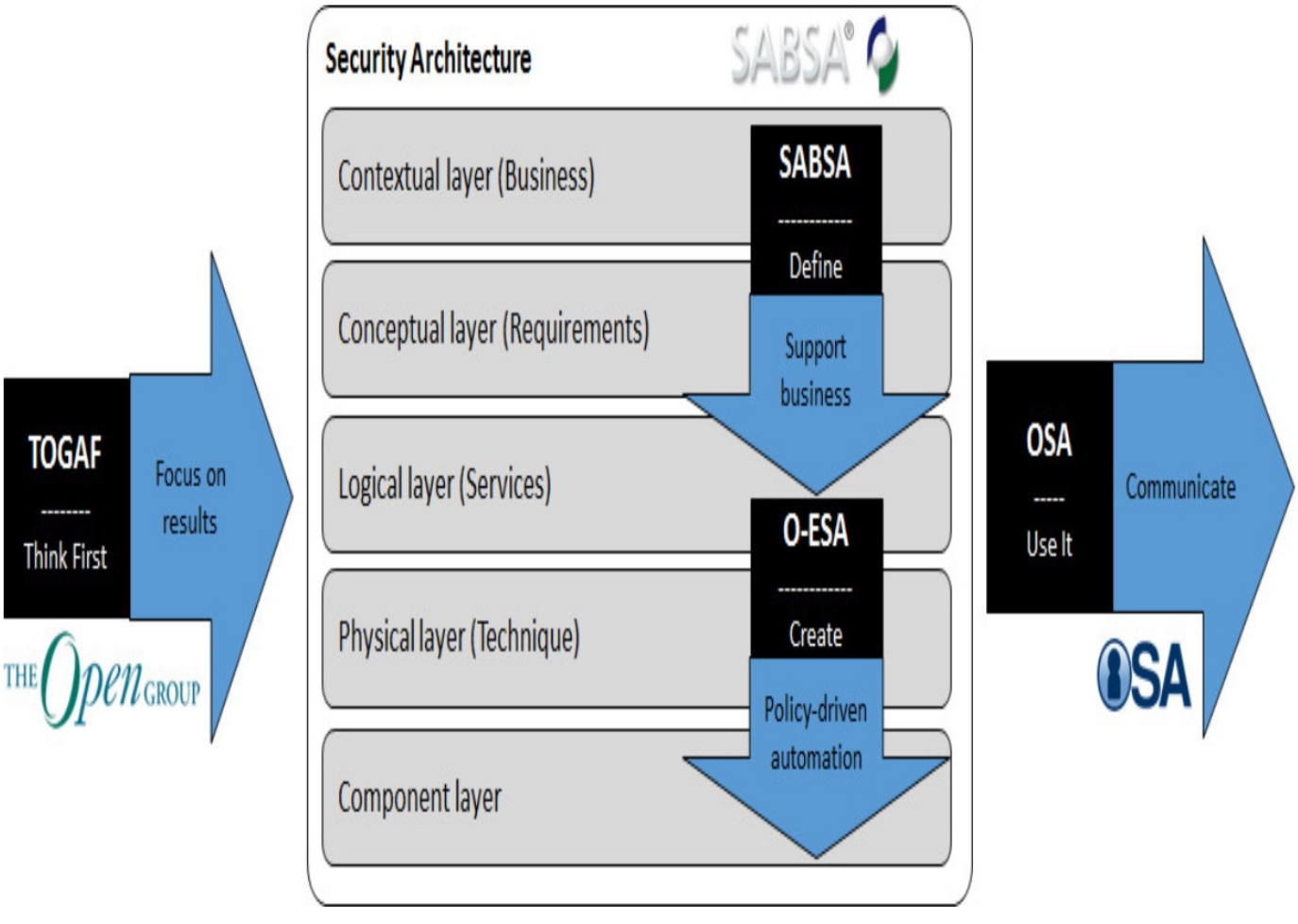


Figure 1. Various architecture frameworks put in perspective, based on their strengths.

- SABSA (Sherwood Applied Business Security Architecture):
  - SABSA is a framework and methodology for developing enterprise security architectures and aligning security objectives with business goals. It emphasizes a holistic approach to security that integrates with business processes and enables organizations to manage risk effectively. SABSA provides a structured approach to security architecture development, incorporating business attributes, security attributes, and operational requirements.
- O-ESA (Open Enterprise Security Architecture):
  - O-ESA is an open framework for designing and implementing enterprise security architectures. It aims to provide a common language and structure for discussing security architecture concepts and principles. O-ESA emphasizes the importance of aligning security with business objectives and focuses on creating flexible, adaptable, and scalable security solutions.
- OSA (Open Security Architecture):
  - OSA is a community-driven initiative aimed at developing open standards and best practices for security architecture. It provides a set of guidelines, templates, and reference models to help organizations design, implement, and manage security architectures effectively. OSA promotes collaboration and knowledge sharing among security professionals and encourages the use of open standards and interoperable technologies.

UNIT–III: Incident Response-Incident categories, Incident response, Incident recovery, Operational security protection-Digital and data assets, ports and protocols, Protection technologies

Incident response

• Incident response is a key component of an enterprise business continuity and resilience program.

• The increasing number and diversity of information security threats can disrupt enterprise business activities and damage enterprise information assets.

• A sound risk management program can help reduce the number of incidents, but there are some incidents that can neither be anticipated nor avoided.

• Therefore, the enterprise needs to have an incident response capability to detect incidents quickly, contain them, mitigate impact, and restore and reconstitute services in a trusted manner.

• This white paper examines incident response from security, risk, privacy and assurance perspectives; identifies some key issues to be considered in an incident response program; and outlines where the COBIT 4.1 framework can be applied to the development of an effective incident response capability.

• Incident: a security event which requires action from the internal security team. This does not include events which do not become incidents. Events can also be logged, as an addition.

• Event: An alert or log from a system that indicates that an attempted attack has happened (for example a firewall log entry log for an SSH brute force attack).

• Entity: an institution / company which collects metrics for incidents on the network that they control.

3.1 Incident categories

AN INCIDENT CLASSIFICATION FRAMEWORK

❖ Creating an incident classification framework is an important element in enabling the proper prioritization of incidents.

❖ It will also help you to develop meaningful metrics for future remediation.

❖ We recommend a two-tiered scheme that focuses on classifying the incident at the highest level (category, type, and severity) to prioritize incident management.

❖ Incident classification may change frequently during the incident management lifecycle as the team learns more about the incident from the analysis being performed.

Category:

• Unauthorized access of the network
• Malware
• Denial of Service
• Improper Usage by an IT administrator (accidentally or intentionally)
• Unsuccessful Access Attempt

Type:

• Targeted vs Opportunistic Threat
• Advanced Persistent Threat
• State Sponsored act of Espionage
• Hacktivism Threat
• Insider Threat

Severity

• Critical Impact- Threat to public safety or life

• High Impact- Threat to sensitive data
• Moderate Impact- Threat to Computer Systems
• Low Impact- Disruption of services

INCIDENT TAXONOMY

❖ The second tier of this framework is incident taxonomy.

❖ Taxonomy focuses on detailing additional information about an incident that you need to identify root cause and trends.

❖ It can also provide you with information that is essential for incident response metrics.

❖ Classifying incidents for each of the following six criteria can give you detailed information on the incident that will be crucial in helping to find the best way to resolve the incident and prevent repeated incidents in the future.

❖ It is much easier to contain an incident when there is an understanding of that incident, and the correct protocol in handling it.

Direct Method
• End User
• 3rd Party Service Provider
• Law Enforcement such as the FBI
• Data Loss Prevention system, Firewall, Anti-Virus, Proxy, and Netflow

Attack Vector
• Viruses
• Email attachments
• Web pages
• Pop-up windows
• Instant messages

Impact
• Employee Dismissal
• HR/ Ethics Violation
• Loss of Productivity
• Unauthorized Privileges
• Brand Image
• Lawsuit
• Denial of Service

Intent
• Malicious
• Theft
• Accidental
• Physical Damage
• Fraud
• Espionage

Data Exposed
• Public
• Confidential
• Export Control
• Financial Reporting
• Unknown

Root Cause
• Unauthorized Action
• Vulnerability Management
• Theft
• Security Control Failure/Gap
• Disregard of Policy
• User Negligence
• Non-Compliance to Standards such as PII, PCI, HIPPA
• Service Provider Negligence

3.2Incident response

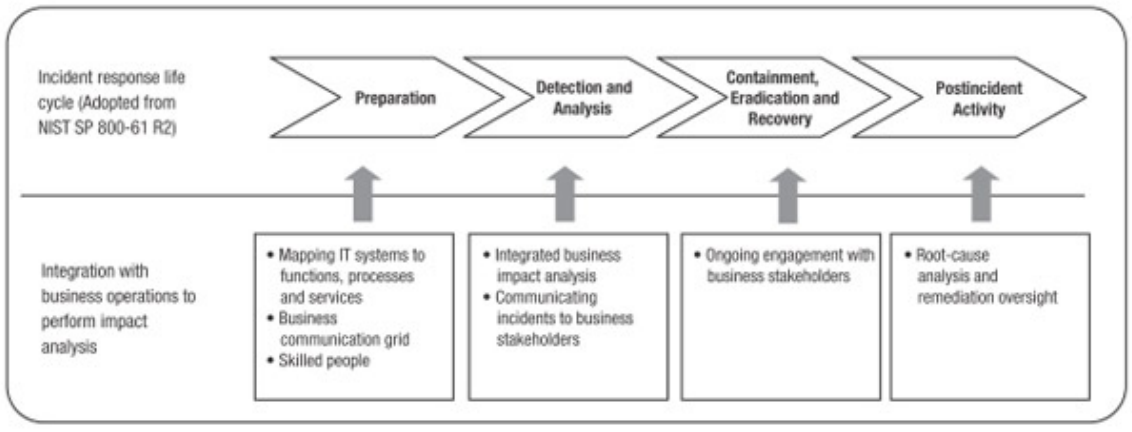
https://www.isaca.org/Journal/archives/2015/volume-6/Pages/a-business-integrated-approach-to-incident-response.aspx?utm_referrer=

An Integrated Approach to Incident Handling

❖ The US National Institute of Standards and Technology (NIST) "Computer Security Incident Handling Guide"[4] has been leveraged to emphasize the potential integration points between the security incident management process and operational risk management process and to provide a framework for incident managers and business managers to engage each other effectively.

❖ This article reviews each phase of the NIST process flow guide, identifies the integration points with business stakeholders and provides guidelines on how to operationalize those in a practical way (**figure 1**).

Figure 1—Incident Response Life Cycle and Business Integration



Source: Hari Mukundhan. Reprinted with permission.

Incident Preparation Phase

1. An unfolding security incident, depending upon its scope, could create confusion and panic to both staff and customers.
2. To proactively mitigate such confusion, incident managers should provide clear, precise, relevant and targeted information to various audiences.
3. For the business stakeholders, the message should be as nontechnical as possible and must point to potential business impacts so that stakeholders can calibrate the responses on their side.
4. The incident manager role in the information security organization has the best vantage point to provide such information.
5. The incident manager should be prepared up front with the communication grid, i.e., what information should be communicated to which business stakeholders and during which life cycle stage of the incident.
6. Appropriate templates, email distribution lists and call trees should be created up front in partnership with the business.
7. Where possible, a dry run should be performed to fine tune the effectiveness of the communication channels and vehicles.

Figure 2 is an example of a communication grid.

Figure 2—Example of a Communication Grid

Information required for the communication grid:
1. Identify relevant stakeholders associated to various key processes and systems in the organization.
2. Pre-establish communication channels and contact details:
   a. Identify audio and video conference numbers. Preferably, maintain a separate conference line for senior management.
   b. Create email distribution lists.
   c. Create call tree(s) to broadcast message to business users.
   d. Where possible, obtain dedicated rooms with both video and audio conferencing facilities.
   e. Maintain key stakeholder official contact information.
3. Create email, call tree, etc., communication templates.
4. Create a communication grid to determine 'what should be communicated to whom' with clarity on what MUST (mandatory) vs. what SHOULD (recommended) be communicated to whom. In other words, mandatory vs. recommended.

Key Incident Management Actions	Relevant Stakeholders					Communication Channel
	Technology and IT Security Managers	Business Manager	Senior Management	Functional Heads (Business and Administrative)	Business Users	
Complete initial notification of potential business-impacting incidents.	Must	Must	–	Should	–	Email distribution list
Evaluate business impact on a continuous basis.	Should	Must	–	Should	–	A/V conference/contact list/ In-person
Perform periodic executive updates.	–	–	Must	Should	–	Senior management A/V conference lines
Communicate business impact.	Should	Must	Must	Must	Should	Email distribution list
Evaluate and finalize containment, eradication and recovery options.	Must	Must	Should	Should	–	Email distribution list
Communicate actions and relevant information around the finalized option.	Must	Must	Must	Must	Must	Call tree
Perform periodic recovery updates.	Must	Must	Must	Must	Must	Call tree

Source: Hari Mukundhan. Reprinted with permission.

Detection and Analysis

8. Risk is typically a function of the adverse impact that arises if the circumstance or event occurs and the likelihood of occurrence.[6]
9. Therefore, if the impact to business is unclear, the risk due to the incident is also unclear.
10. This situation can potentially lead to incident response teams incorrectly prioritizing incidents. That is, it may outwardly appear that one incident is more critical than another, but, in fact, this may not be the case.
11. For example, an externally facing web site that is being impacted by a denial-of-service (DoS) attack may appear more critical than the unavailability of a single sign-on (SSO) server that services many internal applications.
12. But in the case of a web site with a commonly used SSO server, for example, its unavailability could cripple business operations.
13. Obviously, in such a case, the SSO server incident needs to be prioritized ahead of the DoS attack incident.
14. Because of situations such as this, quickly understanding the business impact in partnership with business managers is vital.

The following are some of the business impacts that require analysis:
15. **Financial impact**—Both a financial loss and an inappropriate financial gain to an organization due to an incident should be considered when determining the financial impact. Based on the capital requirements and the risk appetite, organizations should identify a threshold value beyond which a formal chief financial or risk office review is required. An inappropriate financial gain is still considered a financial impact that requires investigation, analysis and eventually corrective action. For example, a man-in-the-middle attack on an end-of-day net transaction file sent by a client may show that the client owes money to the firm rather than the other way around.
16. **Legal and regulatory impact**—The impacts regarding legal concerns, such as contractual issues, regulatory fines and penalties, and breach of service level agreements (SLAs), must also be considered. Given the heightened regulatory environment after the global financial crisis, the potential impact to statutory and regulatory requirements needs to be given special attention.
17. **Operational impact**—A partial or full inability to run the day-to-day business operations of an organization needs to be considered. Depending on the type and scope of the incident, an impact to business operations may or may not impact customer service. It may or may not impact finances. It can be organizationwide or can be limited to a certain section. However, a sustained impact to operations typically leads to a cascading financial, regulatory and/or reputational impact.
18. **Reputational impact**—Reputational impact occurs when negative publicity regarding an institution's business practices leads to loss of revenue or litigation.[7]

Typical incident documentation tends to delve deep into the technical details related to the incident (e.g., the IP addresses impacted, details of the system log files, the network layer in which the incident occurred).

However, as noted in the incident preparation stage, the incident manager should keep the message nontechnical and focus on the potential impacts to the business in a plain and simplistic fashion.

The communication templates created during the incident preparation stage can be utilized to get the key messages out as soon as possible via email distribution lists, call trees or conference calls.

The following are some of the key aspects to be taken into consideration while documenting and communicating the incident:

19. Determine the incident types and the severity level at which business engagement is required. Note that not every incident warrants a business engagement. Also take into consideration the sensitivity of the information before sharing.
20. Develop templates and guidance to create a high-level, nontechnical executive summary articulating the scope and depth of the incident. Target this toward the executive business leaders.
21. Develop templates and guidance to create a detailed, nontechnical write-up articulating the impact to IT systems and, thereby, the potential processes and services that could be impacted. Such communication is typically targeted toward the function heads, managers and staff.
22. Maintain email distribution lists, call trees and other possible communication channels that can be used for communication during the incident.
23. As required, train incident managers on the important aspects of business communication.

Containment (controlling), Eradication (removal) and Recovery

24. For incidents that have a business impact, the incident manager and the business manager have to work closely to ensure that business response is timely and adequately calibrated.
25. If the incident and the business impact is an evolving one, the incident manager may have to invite the business manager to brief, periodic touch-point meetings to appraise the current state of the incident's scope and depth and how it is being contained and eradicated.
26. The business manager, depending upon the evolving state of the incident and its containment or eradication success rate, would, in turn, be expected to constantly reassess the impact and respond accordingly.
27. For example, if a network worm has brought down only a small number of desktops used by operations staff and the incident response teams are able to successfully contain, eradicate and restore services quickly, then the impact to customers may not be significant and the business may have to simply wait for the rest of the desktops to be up and running.
28. On the other hand, if the network damage is spreading fast and is outpacing the incident response team, the business managers may have to consider other options, such as activating a disaster recovery site, transferring work to a different location or shifting to a manual option.

Periodic engagement with the business manager during this phase has the following advantages:

29. Provides a constant feedback mechanism to the incident managers on the priority level of an incident
30. Provides feedback on the effectiveness of the business continuity plan, thereby improving the resilience of the organization and its functions
31. Assists in proactively managing news media, social media, regulators, vendors and other third partiesManages client expectations accordingly
32. Prepares the business proactively for legal and other contractual impacts
33. On a long-term basis, aligns the cybersecurity agenda with the business strategy

Postincident Activity

The postincident activity section of the NIST guide provides excellent insights on how to arrive at lessons learned and how to improve the incident response process in general.

Performing a root-cause analysis for impactful incidents and following it up with remediation measures is important.

In simple terms, the incident manager should be able to document the relationship between the incident's root causes and the business impact and how the incident was contained, eradicated and recovered.

A joint lessons-learned session should, at a minimum, focus on the following:

Identifyaccountable parties to the incident root cause and assign ownership to remediate.

Determine if the incident has recurred along with a recurring financial impact. If the probability of the incident occurring in the future is also high, consider whether additional capital needs to be allocated to cover for future potential losses.

Update the system's function-process-service map and other documentation, if required.

Determine whether the businessimpact was calculated accurately and what needs to be done to improve the calculation.

If the disaster recovery site was activated, check whether the recovery plan requires an update. Interface with business continuity managers to carry forward the update.

Constant oversight should be provided by business managers to ensure that root-cause owners are remediating the root causes on time and business management is kept updated.

Conclusion

To help keep the cybersecurity agenda consistently aligned with business priorities and to provide a practical and effective mechanism for prioritizing incidents, an integrated approach to incident management is vital. Response and recovery can be more targeted and more efficient. Additionally, incident managers may find themselves in a better position to obtain resources to invest in skills and technologies that are required to deal with future incidents.

Improving Efficiency of Security Incident Response Using SOAR

- Managing IT is a fairly complicated task due to its complexity. Complexity arises due to the need to use various products from different vendors to meet ever-evolving business requirements.
- Similarly, managing security is as complex as managing IT, if not more so, due to the Internet enabling various different paradigms of enabling technology to meet business requirements better.
- The increasing complexity of IT coupled with the ever-increasing use of the Internet has resulted in a spate of new threats.
- This makes the security manager role more difficult as managers now need to coordinate multiple technologies and varied security products.
- To combat growing threats, organizations have invested in multiple security solutions such as security information and event management (SIEM) systems, user and entity behavior analytics (UEBA), threat intelligence platforms, incident response platforms, intrusion detection and prevention systems (IDPS), etc.
- These solutions help the organization combat security incidents more effectively and, at times, proactively take action against security incidents.

- This helps the organization develop an improved security posture. However, this leads to more alerts for security personnel to investigate, which can be time consuming and may result in a delayed response.
- With the introduction of the EU General Data Protection Regulation (GDPR) and other similar compliance requirements, delayed response is something that is becoming untenable.

The challenge faced by security managers is how to integrate all these tools, people and processes to enable the common objective of providing protection for information assets.

Security orchestration, automation and response (SOAR) is a term used to describe the integration of different technologies used for effective security.

SOAR technologies enable organizations to collect and aggregate vast amounts of security data and alerts from a wide range of sources. This assists human and machine-led analysis. It enables standardization and automation of threat detection and remediation.

SOAR technologies help organizations as follows:

- **Speeds the response to security events**—SOAR tools speed up response time by integrating all the tools in the security operations center's (SOC) arsenal including threat intelligence sources—both internal and external to organization. Instead of using a dozen or more different tools, security personnel can refer to one data source to get all information and indicators of compromise very quickly.
- **Simplifies the investigation process**—In many cases, SOAR tools can investigate low-level alarms and escalate only important ones to security personnel. Also, they provide a consolidated view that makes it easier to correlate alarms from different tools and determine root cause.
- **Minimizes the damage from attacks**—Automation capabilities may help initiate action such as blocking an IP address or isolating a compromised system or endpoint, which can help to minimize damage and provide important information about the attack faster.
- **Reduces time spent reacting to false positives**—False positive alarms require unnecessary effort and waste security personnel's time, reducing their productivity. SOAR helps reduce false alarms.
- **Improves the efficiency and effectiveness of IT and security operations**—SOAR integrates cybersecurity and IT operations so that they can work together and provide a comprehensive view of the environment and improve the efficiency and effectiveness of IT and security operations.
- **Prevents and manages security threats**—SOAR enables knowledge capture to further improve an organization's capabilities to prevent and manage security threats.
- **Provides meaningful and insightful dashboards**—SOAR provides these dashboards so that enterprises can understand and appreciate the efforts put in by the security team.
- **Lowers costs of operations**—All of the previously listed points also result in lowering the costs of operations.

Many organizations today outsource security operations to managed security service provider (MSSP) vendors. When selecting an appropriate vendor for MSSP, organizations should include SOAR services in their requirements to achieve maximum benefits from outsourcing arrangements.

10.INCIDENT RECOVERY:

Incident recovery in cybersecurity refers to the process of restoring affected systems, data, and services to their normal state following a security incident. This phase of incident response is crucial for minimizing the impact of the incident on the organization's operations and reputation. Incident recovery typically involves the following key steps:

1. **Assessment of Damage**: Before beginning the recovery process, it's essential to assess the extent of the damage caused by the security incident. This may involve identifying affected systems, determining the scope of data loss or corruption, and understanding the impact on critical business operations. Conducting a thorough assessment helps prioritize recovery efforts and allocate resources effectively.
2. **Data Restoration**: One of the primary goals of incident recovery is to restore any lost or corrupted data to its pre-incident state. This may involve restoring from backups, recovering data from unaffected sources, or utilizing data recovery tools and techniques. It's important to ensure the integrity and consistency of restored data to prevent further issues down the line.
3. **System Rebuild or Repair**: Depending on the nature of the incident, affected systems may need to be rebuilt or repaired to remove any traces of malicious activity or vulnerabilities. This may involve reinstalling operating systems, applying security patches, and reconfiguring system settings to ensure they are secure and functional. In some cases, it may be more efficient to rebuild systems from scratch rather than attempting to repair them.
4. **Service Restoration**: Once data and systems have been restored, the focus shifts to restoring affected services and applications to their normal functioning state. This may involve restarting services, reconfiguring network settings, and testing applications to ensure they are working as expected. It's important to prioritize critical services to minimize downtime and disruption to business operations.

---

5. **Validation and Testing**: After recovery efforts are complete, it's essential to validate that systems, data, and services have been successfully restored and are functioning correctly. This may involve conducting thorough testing and verification procedures to ensure that all components are operational and that security controls are effectively mitigating any remaining risks.
6. **Documentation and Lessons Learned**: Throughout the incident recovery process, it's important to document all actions taken, including steps followed, decisions made, and outcomes achieved. This documentation serves as a valuable resource for future reference and helps improve incident response capabilities. Additionally, conducting a post-incident review allows organizations to identify lessons learned, root causes, and areas for improvement to enhance their overall cybersecurity posture.

By following a structured incident recovery process, organizations can effectively restore operations following a security incident, minimize downtime and disruption, and mitigate the impact on their business and stakeholders. Continuous refinement and improvement of incident recovery capabilities are essential for building resilience against future incidents.

Incident recovery

GUIDE FOR CYBERSECURITY INCIDENT RECOVERY

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=922797

Recovery

➢ This is the process of restoring and returning affected systems and devices back into your business environment. During this time, it's important to get your systems and business operations up and running again without the fear of another breach.

➢ Determine how to bring all systems back into full production after verifying that they are clean and free of any nastiness that could lead to a new security incident.

Questions to address

• When can systems be returned to production?

• Have systems been patched, hardened and tested?

• Can the system be restored from a trusted back-up?

• How long will the affected systems be monitored and what will you look for when monitoring?

• What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc)

Operational security protection

Cyber-security:

Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

• **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
• **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
• **Information security** protects the integrity and privacy of data, both in storage and in transit.
• **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
• **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
• **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Digital and data assets:

An information asset is a component related to provision of accurate data or information for decision making purposes by an entity. It is considered to hold value to that particular organization and should therefore be protected by ensuing Confidentiality, integrity and availability. (CIA)

Examples of information Assets are Information (or Data), Computer Application Systems, Computers (Personal Computers (PCs) laptops , PDAs, phones) , Networks (Local Area Network (LAN), Wide Area Network (WAN), Wireless Networks), Human Resources, Facilities (Main Distribution Facilities (MDFs), data centers, server room) and Other Technologies such as database technologies among others

common types of cyber threats:

1. ****Malware**: Malware, short for malicious software, is a broad category of software designed to damage or gain unauthorised access to computer systems. Common types of malware include. * viruses, * worms, * Trojans, * ransomware, * spyware, and *. adware.**

2. ****Phishing**: Phishing is a form of social engineering attack where cybercriminals use deceptive emails, websites, or messages to trick individuals into revealing sensitive information such as login credentials, financial details, or personal data.**

3. ****Man-in-the-Middle (MitM) Attack**: In a MitM attack, an attacker intercepts communication between two parties to eavesdrop, modify, or impersonate the communication. This allows the attacker to steal sensitive information or manipulate data exchanges.**

4. ****Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks**: DoS and DDoS attacks aim to disrupt or overwhelm a target system or network by flooding it with a large volume of traffic or requests. This can lead to system slowdowns, downtime, or service unavailability.**

5. ****SQL Injection**: SQL injection is a type of attack where attackers exploit vulnerabilities in web applications or databases to inject malicious SQL code. This can allow attackers to access, manipulate, or delete data stored in the database.**

6. ****Cross-Site Scripting (XSS)**: XSS attacks involve injecting malicious scripts into web pages viewed by other users. When unsuspecting users visit the compromised pages, the malicious scripts execute in their browsers, allowing attackers to steal cookies, session tokens, or other sensitive information.**

7. ****Ransomware**: Ransomware is a type of malware that encrypts files or locks users out of their systems, demanding a ransom payment in exchange for restoring access. Ransomware attacks can cause significant data loss, financial damage, and operational disruptions.**

8. ****Insider Threats**: Insider threats occur when individuals within an organization misuse their access privileges to steal sensitive information, commit fraud, or sabotage systems.**

Insider threats can be intentional or unintentional and may involve employees, contractors, or partners.

9. **Social Engineering: Social engineering attacks manipulate individuals into divulging confidential information or performing actions that compromise security.**

***pretexting,**

*** baiting,**

*** tailgating, or/. impersonation techniques to gain trust and deceive victims.**

10. **Zero-Day Exploits: Zero-day exploits target vulnerabilities in software or hardware that are unknown to the vendor or have not been patched yet. Cybercriminals exploit these vulnerabilities to launch attacks before security patches or updates are available, making them particularly dangerous.**

These are just a few examples of the diverse range of cyber threats that organizations and individuals may face. Staying informed about emerging threats, implementing robust cybersecurity measures, and practicing good security hygiene are essential for mitigating the risk of cyber attacks.

Certainly! Here's a classification of cyber attacks into web-based attacks and system-based attacks:

****Web-Based Attacks**:**

1. **SQL Injection (SQLi):**

- Web-based attack where attackers exploit vulnerabilities in web applications to execute malicious SQL commands and gain unauthorized access to databases or manipulate data.

2. **Cross-Site Scripting (XSS):**

- Web-based attack where attackers inject malicious scripts into web pages viewed by other users, allowing them to steal cookies, session tokens, or personal information.

3. **Phishing:**

- Web-based attack where attackers use fraudulent emails, websites, or messages to trick individuals into revealing sensitive information such as login credentials, financial details, or personal data.

4. **Drive-By Downloads:**

- Web-based attack where malware is automatically downloaded and installed onto a user's system without their consent, usually through malicious websites or compromised web advertisements.

5. **Formjacking:**

- Web-based attack where attackers inject malicious code into web forms on e-commerce websites to steal payment card details and other sensitive information entered by users.

6. **Credential Stuffing:**

- Web-based attack where attackers use automated tools to systematically test stolen username and password combinations (obtained from previous data breaches) on various websites to gain unauthorized access.

****System-Based Attacks**:**

1. **Malware:**

- System-based attack where malicious software is deployed to infect and compromise computer systems, networks, or devices. This includes viruses, worms, Trojans, ransomware, spyware, and adware.

2. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:**

- System-based attacks where attackers flood a system, network, or service with excessive traffic or requests, causing disruption or downtime and rendering the service unavailable to legitimate users.

3. **Insider Threats:**

- System-based attacks initiated by individuals within an organization who misuse their privileges to steal data, commit fraud, or sabotage systems. This includes employees, contractors, or partners acting maliciously or unintentionally.

4. **Zero-Day Exploits:**

- System-based attacks exploiting vulnerabilities in software or hardware that are unknown to the vendor or have not been patched yet. Zero-day exploits allow attackers to launch attacks before security patches or updates are available.

5. **Rootkits:**

- System-based attacks where attackers install malicious software (rootkits) on compromised systems to gain unauthorized access and maintain control over the system while evading detection by security measures.

6. **Brute Force Attacks:**

- System-based attacks where attackers systematically guess passwords or encryption keys through trial and error until they find the correct combination, gaining unauthorized access to systems or accounts.

These classifications provide an overview of the different types of cyber attacks targeting web-based platforms and computer systems. It's essential for organizations and individuals to be aware of these threats and implement appropriate cybersecurity measures to protect against them.

Certainly! Here are the types of cyber attackers and insider threats:

****Types of Cyber Attackers**:**

1. **Hackers:**

- Individuals or groups with advanced technical skills who exploit vulnerabilities in computer systems, networks, or software for various purposes, including financial gain, activism, espionage, or sabotage.

2. **Script Kiddies:**

- Inexperienced individuals who use pre-written scripts or tools to launch cyber attacks without fully understanding the underlying technology or techniques involved. Script kiddies often engage in cyber attacks for fun or to gain notoriety.

3. **Nation-State Actors:**

- Government-sponsored or affiliated groups that conduct cyber attacks against foreign governments, organizations, or critical infrastructure to achieve political, economic, or military objectives. Nation-state actors often have advanced capabilities and resources at their disposal.

4. **Cybercriminals:**

- Individuals or groups who engage in cyber attacks for financial gain, such as stealing sensitive information, committing fraud, extorting ransom payments, or conducting identity theft. Cybercriminals may operate independently or as part of organized crime syndicates.

5. **Insiders:**

- Individuals within an organization who misuse their privileges to steal data, commit fraud, sabotage systems, or leak confidential information. Insiders may include employees, contractors, partners, or trusted third parties.

6. **Hacktivists:**

- Individuals or groups who engage in cyber attacks for ideological or political reasons, aiming to promote social or political change, raise awareness about specific issues, or

protest against perceived injustices. Hacktivism often involves defacing websites, disrupting services, or leaking sensitive information.

7. **Cyber Espionage Groups:**

- State-sponsored or independent groups that conduct cyber attacks to gather intelligence, steal proprietary information, or conduct espionage activities against governments, corporations, or organizations. Cyber espionage groups often target high-value targets for strategic or economic purposes.

****Types of Insider Threats**:**

1. **Malicious Insiders:**

- Employees or trusted individuals who intentionally misuse their access privileges to steal sensitive information, sabotage systems, commit fraud, or disrupt operations for personal gain, revenge, or ideological reasons.

2. **Careless Insiders:**

- Employees or individuals who inadvertently pose a security risk through negligent or careless behavior, such as clicking on suspicious links, sharing passwords, mishandling sensitive data, or failing to follow security policies and procedures.

3. **Compromised Insiders:**

- Employees or individuals whose credentials or systems have been compromised by external attackers, allowing adversaries to exploit their access privileges to infiltrate networks, steal data, or carry out malicious activities.

4. **Untrained Insiders:**

- Employees or individuals who lack awareness or understanding of cybersecurity risks and best practices, making them vulnerable to social engineering attacks, phishing scams, or other forms of manipulation by cyber attackers.

5. **Disgruntled Insiders:**

- Employees or individuals who become disillusioned, resentful, or disgruntled due to workplace grievances, conflicts, or dissatisfaction. Disgruntled insiders may engage in malicious behavior as a form of retaliation or protest against their employers.

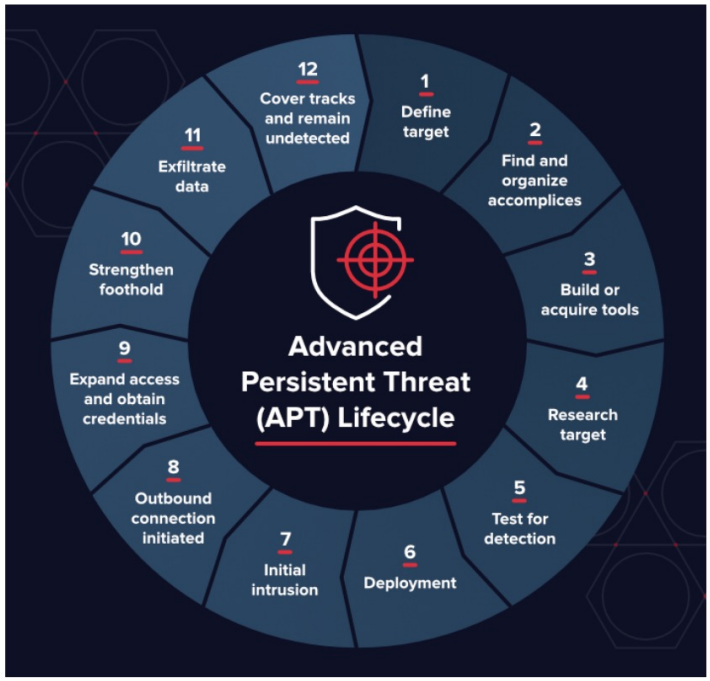
6. **Inadvertent Insiders:**

- Employees or individuals who inadvertently cause security incidents or breaches through innocent actions or mistakes, such as misconfiguring systems, falling victim to social engineering attacks, or mishandling sensitive data without malicious intent.

These classifications provide insight into the various motives, capabilities, and behaviors of cyber attackers and insider threats, highlighting the diverse range of threats organizations may face in cyberspace. It's essential for organizations to implement comprehensive security measures and training programs to mitigate these risks effectively.

The lifecycle of an APT is much longer and
more complicated than other kinds of attacks.

Virus attacks
Advanced Persistent Threat (APT) Lifecycle



- Define target: Determine who you're targeting, what you hope to accomplish – and why.
- Find and organize accomplices: Select team members, identify required skills, and pursue insider access.
- Build or acquire tools: Find currently available tools, or create new applications to get the right tools for the job.
- Research target: Discover who has access you need, what hardware and software the target uses, and how to best engineer the attack.
- Test for detection: Deploy a small reconnaissance version of your software, test communications and alarms, identify any weak spots.
- Deployment: The dance begins. Deploy the full suite and begin infiltration.

Initial intrusion: Once you're inside the network, figure out where to go and find your target.

- Outbound connection initiated: Target acquired, requesting evac. Create a tunnel to begin sending data from the target.
- Expand access and obtain credentials: Create a "ghost network" under your control inside the target network, leveraging your access to gain more movement.
- Strengthen foothold: Exploit other vulnerabilities to establish more zombies or extend your access to other valuable locations.
- Exfiltrate data: Once you find what you were looking for, get it back to base.
- Cover tracks and remain undetected: The entire operation hinges upon your ability to stay hidden on the network. Keep rolling high on your stealth checks and make sure to clean up after yourself.

Toolbox: Advanced Persistent Threat

- There are a few tried and true tactics that reappear across different APT operations:
- Social engineering
- Spear phishing
- Rootkits
- Exploits
- Other tools

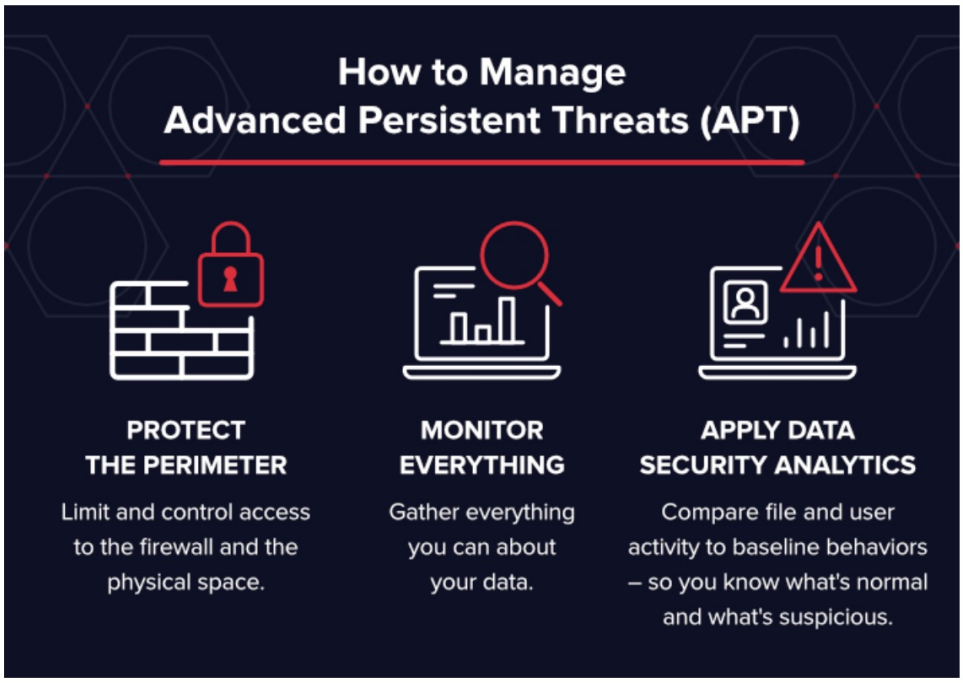
Who is Behind Advanced Persistent Threats (APT)?

- Operators who lead APT attacks tend to be motivated and committed. They have a goal in mind and are organized, capable, and intent on carrying out that goal. Some of these operations live under a larger organization, like a nation-state or corporation. These groups are engaged in espionage with the sole purpose of gathering intelligence or undermining their targets capabilities.
- Some examples of well-known APT groups include:
- APT28 (or Fancy Bear)
- Deep Panda
- Equation
- OilRig

What are Common Targets for Advanced Persistent Threats (APT)?

- Potential targets include:
- **Intellectual property (e.g., inventions, trade secrets, patents, designs, processes)**
- **Classified data**
- **Personally identifiable information (PII)**
- **Infrastructure data (i.e., reconnaissance data)**
- **Access credentials**
- **Sensitive or incriminating communications (i.e., Sony)**

How to Manage Advanced Persistent Threats (APT)?



- Advanced persistent threat attacks can be traced as far back at the 1980s, with notable examples including The Cuckoo's Egg, which documents the discovery and hunt for a hacker who had broken into Lawrence Berkeley National Laboratory. In this early example the hacker, Markus Hess, had been engaged for several years in selling the results of his hacking to the Soviet KGB.
- The extraordinary tactics and lengthy period of hacking mark

this out as a classic early APT. However, APTs as they are understood today are a 21st century phenomena, utilising highly sophisticated tactics and often involving large groups of co-ordinated individuals using complicated technical infrastructure including extensive numbers of command and control (C2) hosts of computers.

Some of the most notable 21st century APT attacks include:

- **Titan Rain (2003)**
- **Sykipot Attacks (2006)**
- **GhostNet (2009)**
- **Stuxnet Worm (2010)**
- **Deep Panda (2015)**

What is Social Engineering ?

➢ As its core it is manipulating a person into knowingly or
unknowingly giving up information; essentially ‘hacking’
into a person to steal valuable information.

It is a way for criminals to gain access to information

systems. The purpose of social engineering is usually to
secretly install spyware, other malicious software or to trick
persons into handing over passwords and/or other sensitive
financial or personal information.

Social Engineering Life Cycle

1. Information Gathering

There could be variety of techniques which is used by
aggressor to gather sensitive information about the target(s). Once these information are gathered, it can be
used to build a relationship either with the target or someone who is important to the success of the attack.
Information that might be gathered includes, but it is not
only limited to:

• A birth date
• A phone list
• An organization’s organizational chart

2. Developing Relationships

An aggressor will first try to build up a good bonding with the target.
He makes sure that he gains the trust of the target which he’ll later exploit.

3. Exploitation

The target could then be manipulated by the ‘trusted’ attacker to reveal
their sensitive information like password to carry out an action (e.g. re-enter
your username pass for reversing facebook policies) this normally occurs. This
action could be at the beginning or end of the attack of the next phase.

4. Execution

Once the target has finished the task requested by the attacker, the cycle is complete.

Social Engineering Attacks

Most popular Social Engineering Attacks are:

➢ Phishing
➢ Pretexting

➢ Baiting
➢ Quid Pro Quo
➢Tailgating

Phishing

➢ Phishing is a type of social engineering attack often
used to steal user data.
➢ They seek to obtain personal information, such as names, addresses and social security numbers.
➢ They use link shorteners or embed links that redirect
users to suspicious websites in URLs that appear legitimate.

Pretexting

➢ Pretexting is defined as the practice of presenting oneself as someone else in order to obtain private information.
➢ Fraudulent Phone Calls.
➢ Attackers focus on creating a good pretext, or a fabricated scenario, that they can use to try & steal the
victims personal information.

Baiting

➢ Baiting is in many ways similar to phishing attacks.
➢ In this attack attacker takes the advantage of human's curiosity or greed by luring the person to do something of what attacker can take benefit to attack or gain confidential information.
➢ e.g: Attacker drops a virus inflected flash drive in common area like lift. Out of curiosity an employee will pick the drive and insert in the machine result a virus spreading in network.

Quid Pro Quo

➢ Quid pro quo means something for something.
➢ Quid pro quo attacks promise a benefit in exchange for information – the benefit usually assumes as a form of service, whereas baiting frequently takes the form of a good.
➢ **Call random numbers** at a company, claiming to be from technical support.

➢ The attacker will help the user, but will really have the
victim type commands that will allow the attacker to **install**
malware.

Tailgating

➢ Another social engineering attack type is known as
tailgating or “piggybacking.”
➢ These types of attacks involve someone who lacks the
proper authentication following an employee into a restricted area.
➢e.g: An unauthorized person wearing a fake ID, follows
an authorized person and enters the secure area through a
door.

Here are a few tips on how users can avoid
social engineering schemes:

- **Do not open any emails from untrusted sources.** Be sure to contact
a friend or family member in person or via phone if you ever receive

an email message that seems unlike them in any way.

- **Do not give offers from strangers the benefit of the doubt.** If they seem too good to be true, they probably are.
- **Lock your laptop** whenever you are away from your workstation.
- **Purchase anti-virus software.** No AV solution can defend against every threat that seeks to jeopardize users' information, but they can help protect against some.
- **Read your company's privacy policy** to understand under what circumstances you can or should let a stranger into the building.