Course Details

Course Title:
Attack, Reporting and Documentation

- **Course Code**: CSF4042B
- **Course Category**: Program Elective - IV

Course Layout

- Introduction to Cybersecurity Attacks, Reporting, and Documentation
- **Incident Response Frameworks**
- Cybersecurity Policy Documentation
- Cybersecurity and Contracting
- Incident Reporting Templates

Chapter Overview

- Introduction to incident response
- NIST Cybersecurity Framework
- SANS Incident Handling Process
- Role of law enforcement and regulatory bodies
- Business Continuity Planning (BCP)
  - Crisis management plans
  - Disaster recovery plans

Introduction to incident response

- Incident Response and Its Importance
  - Why it's essential
  - How it is crucial for any organization

Definition of Incident Response

- **Incident response** refers to the process of identifying, managing, and addressing security incidents within an organization.
- An incident could be a data breach, malware attack, system compromise, or other cybersecurity event that disrupts normal operations.
- **Importance of Having a Structured Incident Response Plan**
  - Risk management:
  - Compliance:
  - Operational continuity:
  - Reputation management:

Goals of Incident Response

- **Minimize Damage and Recovery Time:**
  - **Limit Scope & Impact:** Stop the incident from spreading.
  - **Ensure Fast Recovery:** Minimize downtime to keep business running smoothly.
- **Mitigate Exploited Vulnerabilities:**
  - **Address Root Cause:** Fix issues (e.g., unpatched systems, weak credentials) to prevent future incidents.
  - **Analyze & Fix Vulnerability:** Understand how it was exploited, resolve it, and put preventive measures in place.
- **Prevent Future Incidents:**
  - **Post-Incident Analysis:** Implement lessons learned, improve defenses, and prevent similar threats.
  - **Continuous Improvement:** Enhance security measures, tools, and employee awareness after every incident.

Phases of Incident Response

- **Preparation:**
- **Incident Response Plan (IRP):**
  - Clear communication channels.
  - Defined roles and responsibilities.
  - Contact information for stakeholders (e.g., security vendors, legal teams).
  - Incident response tools and resources (e.g., forensics tools, log analysis).
- **Training & Mock Drills:** Ensure team preparedness.

Phases of Incident Response

- **Detection and Analysis:**
  - **Detection:** Identify an incident via automated alerts, employee reports, or external notifications.
  - **Analysis:** Assess severity, identify affected systems, determine attack method, and prioritize response actions using log analysis, network traffic review, and forensic tools.
  - **Goal:** Quickly gather information to understand the full scope and nature of the incident.

Phases of Incident Response

- **Containment, Eradication, and Recovery:**
  - **Containment:** Stop the incident from spreading by isolating affected systems or disabling network access.
  - **Eradication:** Remove the root cause (e.g., remove malware, patch vulnerabilities, change compromised credentials).
  - **Recovery:** Restore systems and services to normal, ensure systems are clean, verify backups, and apply patches to prevent recurrence.

Phases of Incident Response

- **Post-Incident Activity:**
  - **Post-Mortem/Retrospective:**
    - What went well?
    - What could be improved?
    - Document lessons learned and adjust the IR plan.
  - **Update Policies:** Revise policies, procedures, and defenses based on findings.
  - **Reporting:** Notify stakeholders and regulatory authorities as required (e.g., GDPR, HIPAA).

Incident Response Team

- **Roles and Responsibilities of the IR Team:**
  - **Incident Response Manager:** Oversees the process, ensures the plan is followed, and coordinates with teams and leadership.
  - **Security Analysts:** Analyze, investigate, and identify the incident's nature and scope.
  - **Forensics Experts:** Collect evidence and data for analysis and legal purposes.
  - **IT Staff:** Handle containment, recovery, and system restoration.
  - **Legal and Compliance:** Ensure legal obligations are met and communicate with external parties.
  - **Public Relations:** Manage communication with customers, partners, and the public to maintain trust.

Incident Response Team

- **Coordination with Other Departments:**
  - **Key Departments Involved:**
    - IT, Legal, Management, and HR.
  - **Cross-Departmental Communication:**
    - Ensures effective incident management, protects reputation, legal standing, and operations.
  - **Clear Communication:**
    - Clear lines of communication, especially in a crisis.

Summary

- **Importance:** Incident response protects organizations from cyber threats.
- **Structured Plan:** Minimizes damage, reduces recovery time, and prevents future incidents.
- **Four Phases of IR:** Preparation, Detection & Analysis, Containment & Recovery, Post-Incident.
- **Clear Roles:** Effective coordination is essential.
- **Key Takeaway:** Incident response focuses on crisis management and continuous improvement to strengthen security posture.

Introduction to incident response

NIST Cybersecurity Framework

NIST Cyber Security Framework

- **National Institute of Standards and Technology (NIST): Promoting Innovation**
  - Non-regulatory agency
  - Advances measurement science, standards, and technology
- **NIST Cybersecurity Framework (NIST CSF): Flexible Security Framework**
  - Integrates with any organization's existing security processes
  - Suitable for any industry
  - Excellent starting point for information security and cybersecurity risk management in Organizations

History of the NIST CSF

- **Executive Order 13636**:
  - Issued on February 12, 2013, this order tasked NIST with developing a framework to reduce risks to critical infrastructure
- **Framework Development**:
  - NIST engaged with stakeholders from government, industry, and academia
  - involved workshops, requests for information (RFI), and extensive outreach
- **Initial Release**: **Framework Version 1.0**
  - CSF was first published in February 2014
  - Main focus was on critical infrastructure sectors

History of the NIST CSF

- **Framework Version 1.1**
  - Published in April 2018
  - added supply chain risk management
- **Framework Version 2.0**
  - Published in Feb 2024
  - Expanded applicability to Small Businesses
  - Added new guidance on cybersecurity governance and continuous improvement

NIST CSF core structure

- **Framework Core**:
- **Includes functions, categories, subcategories and informative references.**
- **Functions:** Identify, Protect, Detect, Respond, Recover
  - General overview of security best practices
  - Not procedural steps
  - Performed concurrently and continuously
  - Aims to create an operational culture that adapts to dynamic cybersecurity risks
- **Categories & Subcategories**
  - Offer specific action plans
  - Tailored for departments or processes within an organization

NIST CSF core structure

- **Implementation Tiers: (Partial, Risk-Informed, Repeatable, Adaptive)**
  - Describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework.
- **Profiles**:
  - Represent the alignment of an organization's cybersecurity activities with the desired outcomes of the Framework Core.

NIST functions and categories

- **Identify:**
- **Protect:**
- **Detect:**
- **Respond:**
- **Recover:**

Identify: Understanding Key Assets

- Asset Management (ID.AM):
  - Identifies physical and digital assets (e.g., hardware, software, data, personnel, devices).
  - Ensures critical assets are prioritized based on their importance to business operations.
- Business Environment (ID.BE)
  - Understands the organization’s role in the supply chain and critical functions.
  - Defines mission objectives, stakeholders, and dependencies.

Identify: Understanding Key Assets

- Governance (ID.GV):
  - Establishes cybersecurity policies, procedures, and roles to align with business objectives and regulations.
  - Ensures accountability for risk management decisions.
- Risk Assessment (ID.RA):
  - Identifies potential threats and vulnerabilities that could impact the organization.
  - Evaluates the likelihood and impact of various risks.

Identify: Understanding Key Assets

- Risk Management Strategy (ID.RM):
  - Defines the organization's tolerance and approach to risk management.
  - Guides decision-making based on risk appetite and business objectives.
- Supply Chain Risk Management (ID.SC):
  - Identifies risks associated with third-party vendors and partners.
  - Ensures supply chain resilience and security considerations in procurement processes.

Key Purpose of the Identify Function in CSF 1.1

- To provide a clear understanding of the organization's cybersecurity posture.
- To align cybersecurity priorities with business objectives and regulatory requirements.
- To lay the groundwork for effective risk management and incident response planning.

Protect: Implement Safeguards

- Identity Management and Access Control (PR.AC):
  - Focuses on ensuring access to physical and digital assets is limited to authorized users, processes, or devices.
- Awareness and Training (PR.AT):
  - Ensures that personnel and stakeholders are aware of cybersecurity risks and their roles in protecting organizational assets.
- Data Security (PR.DS):
  - Protects information through appropriate measures such as encryption, data classification, and integrity controls.

Protect: Implement Safeguards

- Information Protection Processes and Procedures (PR.IP):
  - Defines security policies, procedures, and processes to protect information systems.
- Maintenance (PR.MA):
  - Ensures that maintenance activities on systems are performed securely and appropriately.
- Protective Technology (PR.PT):
  - Implements technical security solutions to protect systems and assets from cybersecurity threats.

Key Purpose of the Protect Function in CSF 1.1:

- To safeguard assets, limit exposure to threats, and support the organization's ability to continue operations safely.
- To ensure a proactive security posture by implementing appropriate safeguards and controls.

Detect: Alert Measures

- Anomalies and Events (DE.AE):
  - Ensures that cybersecurity events and anomalies are detected, analyzed, and addressed in a timely manner.
- Security Monitoring (DE.CM):
  - Implements continuous monitoring solutions to detect cybersecurity threats and unauthorized activities.
- Continuons Détection Processes (DE.DP):
  - Establishes processes to continuously test and evaluate detection capabilities to ensure effectiveness.

Key Purpose of the Detect Function in CSF 1.1:

- To ensure timely discovery of cybersecurity events and anomalies.
- To provide actionable intelligence to respond effectively to threats.
- To maintain situational awareness through logging, monitoring, and alerting systems.

Respond: Appropriate Reactions

- Response Planning (RS.RP):
  - Ensures that response processes and procedures are established, communicated, and executed during and after an incident.
- Communications (RS.CO):
  - Establishes coordination and communication protocols with internal and external stakeholders during incidents.
- Analysis (RS.AN):
  - Ensures cybersecurity incidents are analyzed to determine their impact and guide response actions.

Respond: Appropriate Reactions

- Mitigation (RS.MI):
  - Ensures that activities are performed to contain and eradicate incidents effectively.
- Improvements (RS.IM):
  - Focuses on lessons learned from incidents to enhance response strategies and prevent future occurrences

Key Purpose of the Respond Function in CSF 1.1:

- To ensure an organized and effective response to cybersecurity incidents.
- To minimize the impact of an incident and facilitate a return to normal operations.
- To foster continuous improvement in incident management capabilities.

Recover: Ensure Continuity

- Recovery Planning (RC.RP):
  - Ensures that recovery processes and strategies are in place and executed after an incident to restore business operations.
- Improvements (RC.IM):
  - Focuses on applying lessons learned to improve recovery processes and ensure stronger resilience in the future
- Communications (RC.CO):
  - Ensures coordinated communication with internal and external stakeholders during and after recovery efforts to maintain trust and transparency

Key Purpose of the Recover Function in CSF 1.1

- To ensure rapid restoration of critical business functions after an incident.
- To minimize downtime and associated costs.
- To foster a culture of continuous improvement and resilience.

CSF Tiers in 1.1

- Levels of cybersecurity maturity
- Assess cybersecurity risk management practices
- Help identify areas for improvement
  - **Tier 1 (Partial)**:
  - **Tier 2 (Risk-Informed)**:
  - **Tier 3 (Repeatable)**:
  - **Tier 4 (Adaptive)**:

CSF Tiers in 1.1

- Tier 1 (Partial)
  - Informal risk management practices
  - Limited cybersecurity awareness
  - Ad-hoc approach to cybersecurity
- Tier 2 (Risk-Informed)
  - Some cybersecurity risk awareness
  - Inconsistent risk management practices
  - Policies exist but aren't fully integrated

CSF Tiers in 1.1

- Tier 3 (Repeatable)
  - Integrated risk management
  - Formal processes in place
  - Repeatable and proactive security practices
- Tier 4 (Adaptive)
  - Adaptive risk management practices
  - Continuously improving processes
  - Anticipates and responds to cybersecurity risks

NIST CSF Profiles in 1.1

- Used to tailor the framework to an organization's specific needs
- **Current Profile**:
  - Represents the organization's current cybersecurity activities and practices.
- **Target Profile**:
  - Defines the desired cybersecurity outcome based on business needs, risk tolerance and resources.
- **Gap Analysis:**
  - Helps identify the difference between Current and Target Profile, highlighting area’s of improvement.

How NIST CSF 1.1 Can Helped:

- **Identify: Understanding Key Assets**
- **Protect: Implement Safeguards**
- **Detect: Alert Measures**
- **Respond: Appropriate Reactions**
- **Recover: Ensure Continuity**

NIST CSF 1.1

NIST CSF 2.0

The Journey from 1.1 to 2.0

- The NIST Cybersecurity Framework was designed to be a living document that is refined, improved, and evolves over time (to keep pace with technology and threat trends, integrate lessons learned, and move from *best practice* to *common practice*).

- The NIST Cybersecurity Framework (CSF) 2.0 was created to handle new cybersecurity issues and make it easier to use for different types and sizes of organizations. The changes from CSF 1.1 to CSF 2.0 were driven by several key factors.

Why the Change

- Growing Cybersecurity Risks & Threat Landscape
  - Cyber threats are getting more complex, with an increase in ransomware, supply chain attacks, and AI-driven threats.
  - Organizations need a more strategic and governance-focused approach to cybersecurity, not just operational measures.
- Need for Stronger Cybersecurity Governance
  - CSF 1.1 didn't have a specific governance function to align cybersecurity with business goals.
  - CSF 2.0 introduces the "Govern" (GV) function, which focuses on cybersecurity risk management at the leadership level, highlighting accountability and decision-making.

Why the Change

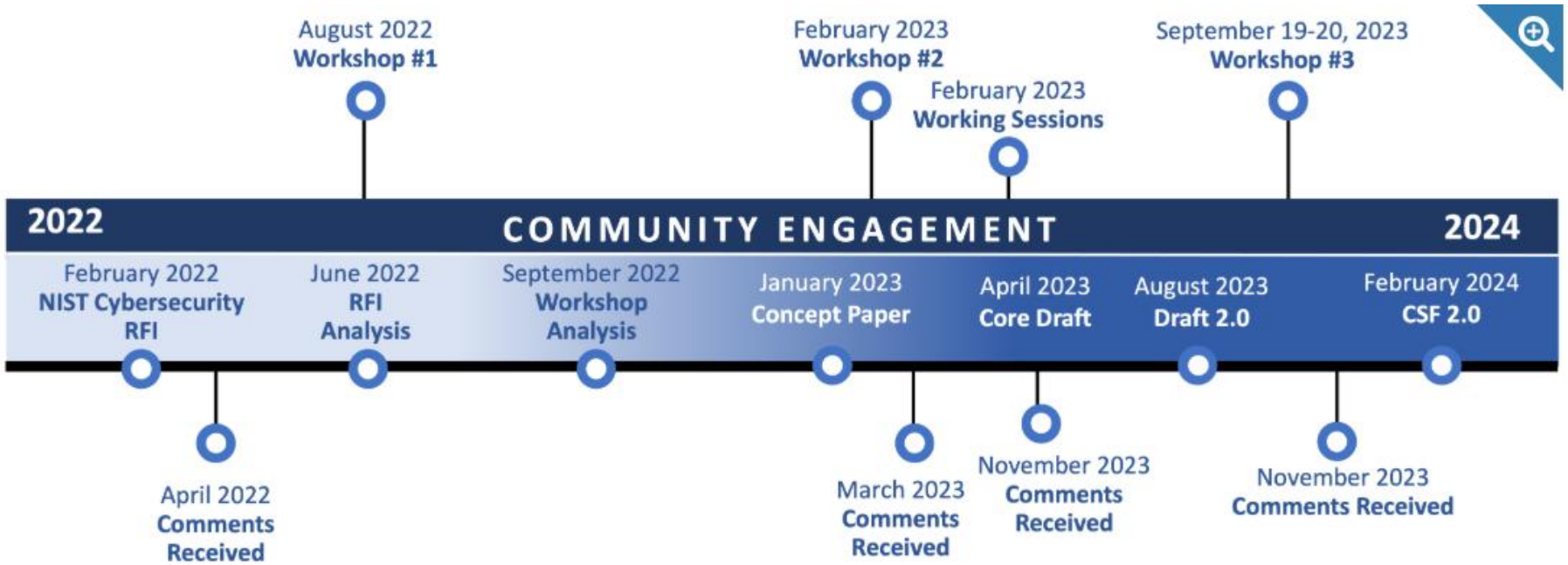
- Increased Focus on Supply Chain Security
  - High-profile supply chain attacks like SolarWinds and Log4j showed the need for better supply chain risk management.
  - CSF 2.0 now includes more guidance on managing risks from third-party vendors and assessing their security.
- Broader Applicability Beyond Critical Infrastructure
  - CSF 1.1 was mostly used by critical infrastructure sectors like energy, healthcare, and finance.
  - CSF 2.0 is designed for all types of organizations, including small businesses, government agencies, and international entities.

Why the Change

- Alignment with Global and Emerging Regulations
  - Many organizations needed better alignment with various regulatory frameworks, such as:
    - U.S. Executive Orders on Cybersecurity
    - ISO 27001 (International Security Standard)
    - India’s Digital Personal Data Protection (DPDP) Act
    - European NIS2 Directive
    - GDPR

Why the Change

- Emphasis on Continuous Improvement
  - Cybersecurity is an ongoing process, not a one-time task.
  - CSF 2.0 offers more guidance on how to implement this, including maturity models and examples.
- Improved Clarity and Structure
  - Many users found CSF 1.1 hard to understand and apply to their organizations.
  - CSF 2.0 makes the categories and subcategories easier to understand and use.



Credit: Kristina Rigopoulos

NIST CSF 2.0 : Functions

- GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored
- IDENTIFY (ID): The organization's current cybersecurity risks are understood
- PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used
- DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed
- RESPOND (RS): Actions regarding a detected cybersecurity incident are taken
- RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored

Credit : https://www.nist.gov/cyberframework

GOVERN (GV)

- Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood
  - Has 5 Sub-Categories
  - Eg: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
  - We deliver secure and reliable digital solutions, prioritizing data protection and resilience against cybersecurity risks.

Credit : https://www.nist.gov/cyberframework

GOVERN (GV)

- Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions
  - Has 7 Sub-Categories
  - Ex1: Update near-term and long-term cybersecurity risk management objectives as part of annual strategic planning and when major changes occur
  - Near-term update: Implement multi-factor authentication (MFA) across all customer accounts within six months to mitigate rising phishing attacks.
  - Long-term update: Develop a zero-trust architecture over the next three years to align with industry best practices and evolving compliance requirements.

Credit : https://www.nist.gov/cyberframework

GOVERN (GV)

- Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated
  - Has 4 Sub-Categories
  - Ex1: Leaders (e.g., directors) agree on their roles and responsibilities in developing, implementing, and assessing the organization's cybersecurity strategy
  - **CEO**: Ensures cybersecurity aligns with business goals and secures budget approval.
  - **CIO**: Oversees technology implementation and ensures IT infrastructure supports cybersecurity objectives.

Credit : https://www.nist.gov/cyberframework

GOVERN (GV)

- Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced
  - Has 2 Sub-Categories
  - Ex1: Create, disseminate, and maintain an understandable, usable risk management policy with statements of management intent, expectations, and direction
  - **Creation**: The CISO writes the policy, explaining risk assessment, acceptable security practices, and response plans.
  - **Dissemination**: The policy is shared through email, internal portals, and training, making sure all employees know their role in managing risks.
  - **Maintenance**: The policy is reviewed every year and updated after major regulatory changes or security incidents. The IT and compliance teams keep it aligned with new threats and business needs.

Credit : https://www.nist.gov/cyberframework

GOVERN (GV)

- Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy
  - Has 3 Sub-Categories
  - Ex1: Measure how well the risk management strategy and risk results have helped leaders make decisions and achieve organizational objectives
  - Decision Support: After implementing a risk-based vendor assessment process, leadership successfully avoided a partnership with a third-party supplier that had unresolved security vulnerabilities.
  - Objective Achievement: The company's goal was to reduce downtime from cyber incidents by 30%. Post-implementation of enhanced monitoring and incident response protocols, downtime decreased by 35%, surpassing expectations.

Credit : https://www.nist.gov/cyberframework

GOVERN (GV)

- Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders
  - Has 10 Sub-Categories
  - Ex1: Establish a strategy that expresses the objectives of the cybersecurity supply chain risk management program
  - Objective 1: Mitigate Vendor Risk – Ensure that all suppliers comply with cybersecurity standards by requiring security assessments and third-party audits before partnership agreements are finalized.
  - Objective 2: Ensure Business Continuity – Establish contingency plans for critical supply chain disruptions to minimize impact in the event of a cyberattack or breach within the supply chain.

Credit : https://www.nist.gov/cyberframework

IDENTIFY (ID):

- Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy
  - 8 Sub-Categories
  - Ex1: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices
  - What would get included in this ?

Credit : https://www.nist.gov/cyberframework

IDENTIFY (ID):

- Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization
  - 10 Sub-Categories
  - Ex1: Use vulnerability management technologies to identify unpatched and misconfigured software
  - What would get included in this ?

Credit : https://www.nist.gov/cyberframework

Case Study Discussion

- Apply the NIST 2.0 Framework to Equifax data breach issue
- Apply the NIST 2.0 Framework to Target data breach issue
- Propose Solutions to fix the issue
- For NIST CSF 2.0 Implementation Example reffer to https://www.nist.gov/system/files/documents/2024/02/21/CSF%202.0%20Implementation%20Examples.pdf

NIST CSF 2.0

SANS INCIDENT HANDLING PROCESS

SANS

Launched in 1989 as a cooperative for information security thought leadership, SANS Institute helps organizations mitigate cyber risk by empowering cyber security practitioners and teams with training, certifications, and degrees needed to safeguard organizations and advance careers.

https://www.sans.org/apac/

What Is Incident Response?

- **Purpose**: Detect, prioritize, contain, and eliminate cyberattacks.
- **Goals**:
  - Be aware of major security incidents.
  - Act quickly to halt attackers.
  - Minimize damage.
  - Prevent future attacks.

Phases of Incidence response

- **Preparation**
- **Identification**
- **Containment**
- **Eradication**
- **Recovery**
- **Lessons Learned**

Preparation

- **Preparation Stage Goal**: Ensure the organization can respond to incidents instantly.
- Critical elements that should be prepared in advance
- **Policy**
  - Define principles, rules, and practices for security processes.
  - Ensure the policy is visible to employees and users.
- **Response Plan/Strategy**
  - Create a plan for handling incidents.
  - Prioritize incidents based on their impact on the organization.

Preparation

- **Communication**
  - Establish a communications plan like who, when and why to contact.
- **Documentation**
  - Documentation is mandatory and can be very critical if you need to file charges.
- **Team**
  - Develop and train an incident response team
- **Access control**
  - Ensure the incident response team has appropriate permissions to do the job

Preparation

- **Training**
  - Provide initial and ongoing training for all members.
  - Cover incident response processes, technical skills, and cyberattack patterns and techniques.
  - Conduct Mock drills for the team
- **Tools**
  - Evaluate, select, and deploy effective software and hardware for incident response.
  - Ensure that are accessible to the response team at short notice.

Identification

- Identification procedure includes the following elements
- **Setting up monitoring**
  - Include all sensitive IT systems and infrastructure
- **Analysing events**
  - Use data from multiple sources like log file, error messages and alerts from SIEM or similar tools.

Identification

- **Identifying an incident**
  - Post analysis of the data report incidence
- **Notifying Incidence**
  - Follow the process to work with point of contact for incidence response.
  - Activate Incidence response team
  - Communicate about incidence on Need to Know basis.
- **Document**
  - All actions that the team is taking as part of response.

Containment

- Limit the damage by isolating affected systems and prevent any further damage
- Important Processes
- **Short-term containment:**
  - Limit damage before it worsens.
  - Immediate actions like disconnecting an affected system/host
  - Route to failover systems.

Containment

- **System backup**
  - Create a forensic image of affected systems using tools like Forensic Tool Kit (FTK) or EnCase
  - After imaging, wipe and reimage the systems.
- **Long-term containment:**
  - Applying patches, workarounds, updates and configuration changes
  - Remove attacker accounts and backdoors; address the root cause.

Eradication

- Identify the root cause of the incident .
- Remove malware and artifacts; fully restore affected systems.
- **Reimaging**
  - Wipe and reimage affected drives to remove malicious content.
- **Preventing the root cause**
  - Understand the cause and prevent future compromise by patching vulnerabilities.

Eradication

- **Applying basic security best practices**
  - Apply latest patches
  - Disable unused features or functions
- **Scan for malware**
  - Scan the systems to ensure it is free for any virus or malware

Recovery

- Fully restore systems after confirming they are clean and threat-free.
- **Define the criteria to get system up.**
  - Restore affected systems and services to normal operations.
- **Test and verifying**
  - Test that the threat is fully mitigated before bringing systems online.
  - Test, verify and monitor affected systems to ensure they are back to normal activity.
- **Monitoring**
  - Monitor for signs of reinfection or further compromise.

Lessons Learned

- Conduct a post-incident review/retrospective of the incident
- **Completing documentation**
  - Investigate further if required to provide complete documentation
- **Publishing report**
  - The report should review the incident and answer Who, What, Where, Why, and How questions.

Lessons Learned

- **Improvements for team**
  - Identify gaps in security controls and incident response procedures
  - Update policies, procedures, and training based on findings
  - Share insights with relevant teams to improve future response
- **Lessons Learned Meeting**
  - Conduct meeting to communicate Lessons learned for IR Team and stake holders

SANS Incident Handling Process

ROLE OF LAW ENFORCEMENT AND REGULATORY BODIES

Law Enforcement

- Agencies maintain law and order.
- Investigate crimes and enforce laws.
- Prosecute offenders.
- Handle various aspects, including cybercrime.

Major Law Enforcement Bodies in India

- State Police Cyber Crime Cells
  - **Jurisdiction:** Handles cybercrimes at the state level.
  - **Cybercrime Role:** Investigates cyber fraud, hacking, identity theft, and online harassment.
  - **Legal Authority:** Operates under the **IT Act 2000**, **IPC**, and **CrPC**.
- Central Bureau of Investigation (CBI)
  - **Jurisdiction:** National-level criminal investigations, economic offenses, cybercrime, corruption cases.
  - **Cybercrime Role:** Handles high-profile cyber frauds, hacking cases, and digital forensics.
  - **Legal Authority:** Operates under the **Delhi Special Police Establishment Act, 1946**.

Major Law Enforcement Bodies in India

- Enforcement Directorate (ED)
  - **Jurisdiction:** Economic crimes, financial frauds, and money laundering.
  - **Cybercrime Role:** Investigates online financial fraud, cryptocurrency scams, and digital money laundering.
  - **Legal Authority:** Operates under the **Prevention of Money Laundering Act (PMLA), 2002**.
- Indian Cyber Crime Coordination Centre (I4C)
  - **Jurisdiction:** Nationwide coordination of cybercrime investigations.
  - **Cybercrime Role:** Assists law enforcement in handling cyber fraud, online harassment, and hacking cases.
  - **Legal Authority:** Works under the **Ministry of Home Affairs (MHA)**.

Major Law Enforcement Bodies in India

- National Cyber Crime Reporting Portal (MHA Initiative)
  - **Jurisdiction :** National cybercrime complaint reporting.
  - **Cybercrime Role:** Allows individuals to report cybercrimes, including financial fraud, online abuse, and hacking.

Regulatory Bodies

- Set rules and guidelines for industries.
- Ensure organizations follow legal and security standards.
- Do not investigate crimes.
- Can impose fines, revoke licenses, and mandate audits for non-compliance.

Key Regulatory Bodies in India (CyberCrime)

- Indian Computer Emergency Response Team (CERT-In)
  - **Jurisdiction:** Cybersecurity incident management and compliance.
  - Responsibilities:
    - Issues security guidelines and advisories.
    - Mandates reporting of cybersecurity incidents within **6 hours**.
    - Conducts audits and assessments.
  - **Regulatory Power:** Can **impose fines (₹1 lakh per violation)** and mandate security improvements.
  - **Legal Authority:** Section **70B of the IT Act, 2000**.

Key Regulatory Bodies in India (CyberCrime)

- Ministry of Electronics and Information Technology (MeitY)
  - **Jurisdiction:** IT, digital governance, and national cybersecurity policy.
  - Responsibilities:
    - Oversees **National Cyber Security Policy (2013)**.
    - Develops data protection laws (e.g., **Digital Personal Data Protection Act, 2023**).
  - **Regulatory Power:** Can **mandate cybersecurity standards** and enforce compliance.

Key Regulatory Bodies in India (CyberCrime)

- National Critical Information Infrastructure Protection Centre (NCIIPC)
  - **Jurisdiction:** Protection of **Critical Information Infrastructure (CII)** sectors (e.g., energy, defense, banking, telecom).
  - Responsibilities:
    - Identifies and secures **CII assets**.
    - Conducts **risk assessments and cybersecurity audits**.
  - **Regulatory Power:** Can **revoke permissions** for companies failing to secure CII.
  - **Legal Authority: Section 70 of the IT Act, 2000**.

Key Regulatory Bodies in India (CyberCrime)

- National Cyber Security Coordinator (NCSC)
  - **Jurisdiction:** National cybersecurity policy and coordination.
  - Responsibilities:
    - Implements **National Cyber Security Strategy**.
    - Advises the government on cyber threats and foreign technology risks.
  - **Regulatory Power:** Can **restrict the use of foreign technology in critical sectors** (e.g., **Huawei, ZTE restrictions**).

Key Regulatory Bodies in India (CyberCrime)

- Data Protection Board of India (DPBI)
  - **Jurisdiction:** Personal data protection and privacy.
  - Responsibilities:
    - Enforces **Digital Personal Data Protection Act (DPDPA), 2023**.
    - Regulates companies handling **personal and sensitive data**.
  - **Regulatory Power:** Can **impose fines up to ₹250 crore per violation** and **restrict data processing**.

Key Regulatory Bodies in India (CyberCrime)

- Reserve Bank of India (RBI)
  - **Jurisdiction:** Banking, financial institutions, and fintech companies.
  - Responsibilities:
    - Issues **Cyber Security Framework for Banks** (2016).
    - Requires banks to **conduct regular security audits** and **report cyber incidents**.
    - Mandates data localization for payment companies.
  - **Regulatory Power:** Can impose fines up to **₹10 crore or more** and **restrict digital operations** of non-compliant banks.
  - **Legal Authority: Banking Regulation Act, 1949**.

Key Regulatory Bodies in India (CyberCrime)

- Securities and Exchange Board of India (SEBI)
  - **Jurisdiction:** Stock markets, brokers, and financial institutions.
  - Responsibilities:
    - Enforces **Cyber Security & Resilience Framework (2015)** for stock exchanges, brokers, and mutual funds.
    - Mandates **periodic cybersecurity audits**.
  - **Regulatory Power:** Can impose penalties up to **₹1 crore per violation** and suspend trading licenses.
  - **Legal Authority: SEBI Act, 1992**.

Role of law enforcement and regulatory bodies

BCP

CMP

DRP

Business Continuity Plan (BCP)

Business Continuity Planning (BCP) is a proactive strategy that ensures an organization’s essential functions continue during and after a disruption (e.g., cyberattacks, natural disasters, power outages, pandemics).

Key Components of BCP

- Risk Assessment & Business Impact Analysis (BIA)
  - Identifies critical business functions and assesses the impact of disruptions.
  - Helps prioritize resources and response efforts.
- Preventive & Mitigation Strategies
  - Implementing redundancy for critical systems (e.g., backup power, alternative suppliers).
  - Establishing security controls to prevent cyber incidents.

Key Components of BCP

- Continuity Strategies & Recovery Plans
  - Identifying alternate work locations (e.g., remote work setups, backup office sites).
  - Ensuring access to necessary resources, such as cloud storage and remote IT systems.
- Communication & Leadership Roles
  - Establishing a clear chain of command and communication plan.
  - Keeping employees, customers, and stakeholders informed.
- Testing & Regular Updates
  - Conducting tabletop exercises and real-world simulations.
  - Regularly updating the plan based on new risks and lessons learned.

Crisis Management Plans (CMP)

Crisis Management Plans focus on how an organization responds to and manages crises in real time. This includes decision-making, communication, and coordination efforts to minimize chaos and reputational damage.

Key Components of CMP

- Crisis Identification & Escalation Procedures
  - Defining what constitutes a crisis (cyberattack, data breach, public relations disaster, etc.).
  - Setting up an escalation process to activate response teams.
- Incident Response Team (IRT) & Leadership Roles
  - Assigning crisis response team members with predefined roles.
  - Establishing an executive-level crisis management committee.

Key Components of CMP

- Communication Strategy
  - Internal: Keeping employees and executives informed.
  - External: Managing public relations, press releases, and social media.
- Stakeholder Management
  - Keeping customers, regulators, and business partners informed.
  - Ensuring legal teams are involved to handle compliance and legal risks.
- Training & Tabletop Exercises
  - Running mock crisis scenarios to ensure team preparedness.
  - Updating response plans based on lessons learned.

Disaster Recovery Plans (DRP)

Disaster Recovery Plans (DRP) focus on the restoration of IT infrastructure and data after a major disruption. This includes recovering critical applications, servers, databases, and networks.

Key Components of DRP

- Data Backup & Recovery Strategy
  - Regular backups (daily, weekly, real-time).
  - Offsite storage solutions (cloud-based, physical backups).
- Recovery Time Objective (RTO) & Recovery Point Objective (RPO)
  - **RTO**: How quickly systems need to be restored (e.g., 4 hours, 24 hours).
  - **RPO**: Maximum acceptable data loss in case of failure (e.g., last 15 minutes, 1 hour, 1 day).

Key Components of DRP

- Failover & Redundancy Measures
  - Hot, warm, and cold sites for alternate data centers.
  - Cloud-based disaster recovery solutions.
- Disaster Recovery Testing & Drills
  - Simulating system failures and testing recovery procedures.
  - Updating DRP based on test results.
- Roles & Responsibilities in IT Recovery
  - Assigning responsibilities to IT teams, vendors, and external consultants.
  - Ensuring cybersecurity and compliance measures are met.

Recovery Time Objective (RTO)

- RTO is the maximum acceptable downtime for a system, application, or process before it causes significant business disruption.
- Identify Critical Business Processes – Determine which systems and applications are essential for operations.
- Assess Business Impact – Determine how long each system can be down before severe consequences occur.
- Define Maximum Acceptable Downtime (MAD) – Decide the longest duration your business can tolerate an outage before operations are critically affected.
- Set RTO Based on Business Needs – Align your RTO with MAD and business priorities.
- Example Calculation:
  - If a company determines that a database outage must not exceed 2 hours before significant financial loss occurs, then the RTO is 2 hours.

Recovery Point Objective (RPO)

- RPO is the maximum data loss (in time) that a business can tolerate without serious damage. It determines how often backups should be taken.
- Steps to Calculate RPO:
  - Determine Data Criticality – Identify how crucial the data is for business continuity.
  - Assess Data Loss Tolerance – Evaluate how much data loss is acceptable (e.g., 10 minutes, 1 hour, 24 hours).
  - Define Backup Frequency – Ensure backup schedules meet the required RPO.
  - Example Calculation:
    - If a business can only afford to lose 30 minutes of data, then the RPO should be 30 minutes, meaning backups should happen at least every 30 minutes.

Key Differences Between RTO & RPO

Aspect	RTO	RPO
Definition	Max downtime before severe impact	Max data loss before severe impact
Focus	Time to restore systems	Time between last backup and disaster
Determines	How fast systems must be restored	How frequently data should be backed up
Example	If RTO is 1 hour, systems must be restored within 1 hour	If RPO is 15 min, backups must occur every 15 min