Responding to Cybersecurity Incidents: A Guide on What to Do

LSU

The Reality: Incidents Happen Every Day

- Cyberattacks are constantly evolving, targeting businesses of all sizes
- Data breaches, malware infections, and unauthorized access are just a few examples.
- These incidents can have devastating consequences, including financial losses, reputational damage, and operational disruptions.

Training Staff

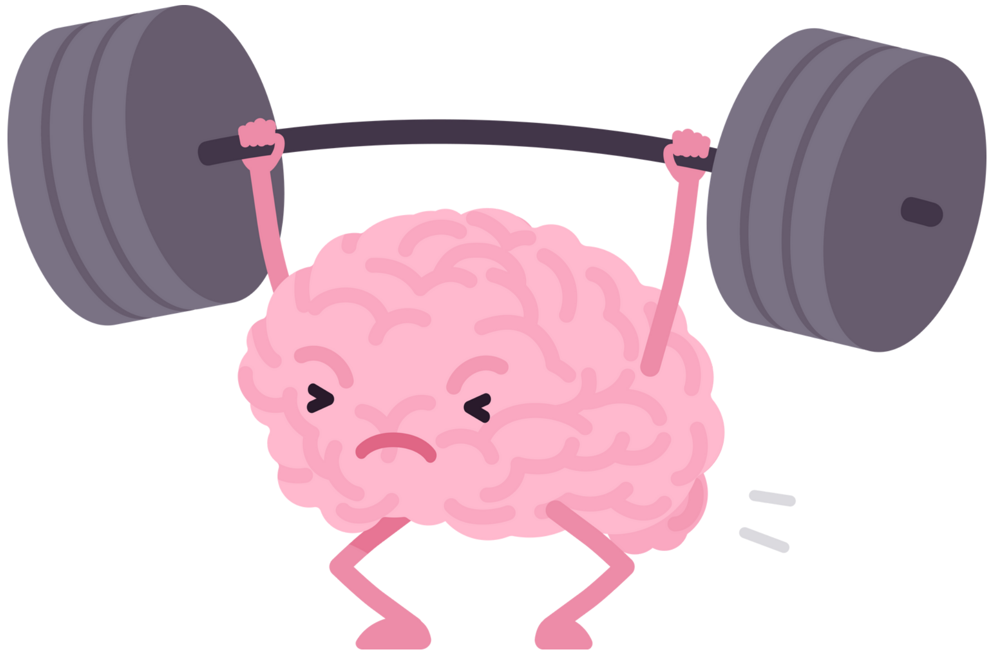
The Importance of Cybersecurity Training

- Cybersecurity is a rising issue that companies are facing
- In 2023, 70% of data breaches involved human element
- The average cost of a cyber incident is around 4 million dollars
- Every third breach involves phishing

LSU

Goals of cybersecurity training

- Awareness of threats and responsibilities
- Employees know how to react and who to contact
- Employees can spot when software does not automatically update
- Prevent and mitigate harm



Training Staff on Cybersecurity

- Implement policies and make employees aware of those policies
- CISA offers free IR training for government employees, contractors, educational institutions, and critical infrastructure partners
- CISA Awareness webinars: one-hour sessions (such as Defending Internet Accessible Systems, Preventing Web and Email Server Attack, and understanding Indicators ofCompromise)
- Make training role-specific, different job roles mean different levels of understanding and responsibilities

Who to Contact In Case of an Incident

- **Internally:**
  - Computer Security Incident Response Team (CSIRT)
  - Internal Legal Counsel
  - Data forensics team

- **Externally:**
  - National CSIRT
  - Security Operations Center
  - Critical Information Infrastructure Operators and Managers
  - External Counsel
  - Law enforcement
  - Affected businesses/individuals

How to Test if The Training Was Successful

- Simulated phishing campaigns
- Hire an external penetration testing firm
- Incident response drills with staff
- Awareness training follow-up

Detection & Analysis in the Real World

Why Detection & Analysis Matter

- **Early detection minimizes damage:**
  - The sooner you identify an incident, the quicker you can contain it and mitigate its impact.
- **Informed decision-making:**
  - Analysis helps you understand the nature and scope of the incident, guiding your response strategy.
- **Improved future defenses:**
  - Analyzing past incidents helps identify vulnerabilities and strengthen your security posture.

Detection: Spotting the Signs

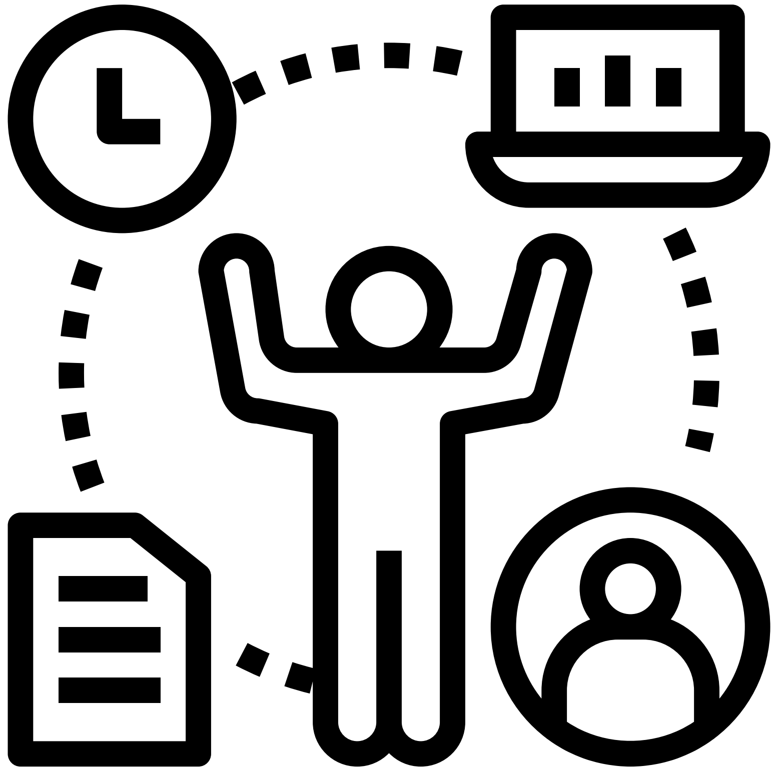
- **Security tools and SIEM:**
  - Utilize security software, firewalls, and SIEM (Security Information and Event Management) systems to monitor activities and flag suspicious events.
- **Log analysis:**
  - Regularly review system logs for anomalies, unauthorized access attempts, or unusual activity patterns.
- **User awareness:**
  - Train employees to recognize potential phishing attempts, suspicious emails, and social engineering tactics.

Common Indicators of Compromise (IoCs)

- **Unusual File Activity:**
  - Unexpected deletions, modifications, or downloads of files, especially after hours or from unauthorized locations.
- **Suspicious Network Traffic:**
  - Spikes in network traffic, unauthorized connections to external servers, or attempts to access restricted resources.
- **System Performance Changes:**
  - Slower processing speeds, unexplained reboots, or applications not functioning properly.
- **Unfamiliar Login Attempts:**
  - Failed login attempts from unknown locations or using uncommon credentials.
- **Phishing Attempts:**
  - Emails or messages designed to trick users into revealing sensitive information.

Building a Process with Limited Resources

- **Prioritize critical assets:**
  - Focus on protecting your most valuable data and systems first.
- **Leverage open-source tools:**
  - Utilize free and community supported security tools for basic detection and analysis.
- **Automate what you can:**
  - Script repetitive tasks to free up analyst time for complex investigations.
- **Foster collaboration:**
  - Encourage information sharing and cross-departmental cooperation on security matters.



Choosing the Right Solution

- **Consider your needs and budget:**
  - Assess your risk profile, critical assets, and available resources before selecting a solution.

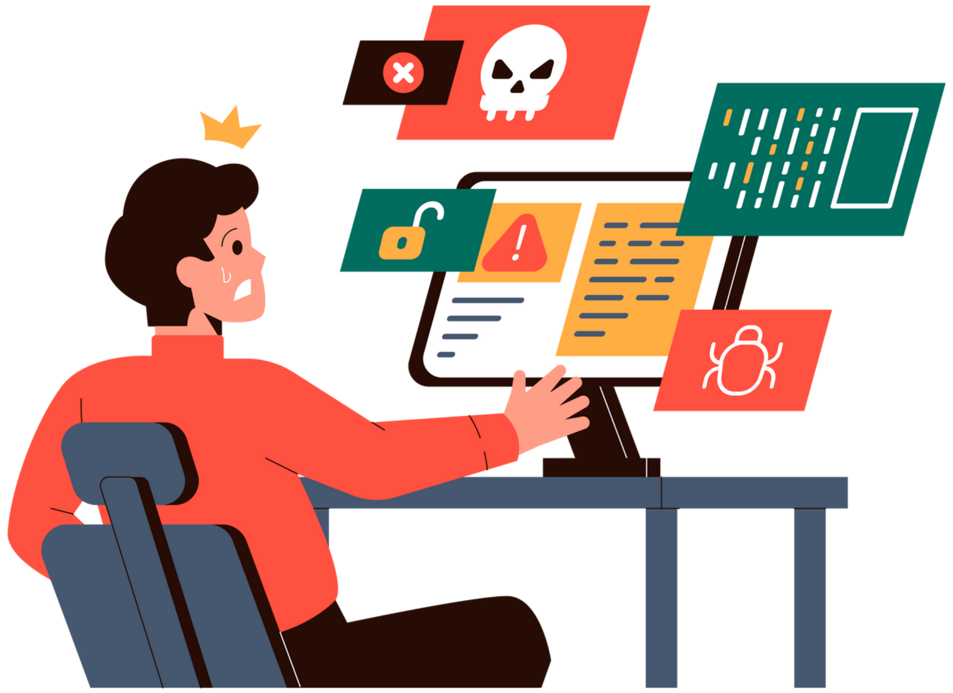
- **Evaluate vendor capabilities:**
  - Compare different vendors based on their detection and analysis techniques, response options, and threat intelligence integration.

- **Look for scalability and flexibility:**
  - Choose a solution that can adapt to your evolving security needs and integrate with existing infrastructure.

Containment, Eradication & Recovery in Cybersecurity

Containment Measures

- **Objective**
  - To prevent the spread of the cyber threat and isolate the affected system
- **Identify**
  - We need to identify the affected system or network segment
- **Isolate**
  - Think of this as building a digital quarantine
  - Affected devices are immediately disconnected from the network, preventing the malware from spreading like wildfire
  - This swift action minimizes potential damage and buys us valuable time
- **Restrict**
  - User accounts associated with the breach are suspended, and access controls are tightened



Eradicating the Threat

- **Objective**
  - To remove the cyber threat from the affected system and prevent future occurrences
- **Root Cause Analysis**
  - Conduct a thorough investigation to determine the root cause of the compromise, such as vulnerabilities or misconfigurations
- **Patching and Updates**
  - Install patches and updates to the operating system and applications to mitigate known vulnerabilities
- **System Rebuild**
  - Rebuild the affected system using a clean version of the operating system and ensure all security measures are in place
- **Security Controls**
  - Implement additional security controls, such as intrusion detection systems (IDS) and antivirus software, to prevent future incidents

LSU

Recovery and Beyond

- **Objective**
  - To restore affected assets to normal operation and resume business activities
- **Data Restoration**
  - Restore data from backups to ensure data integrity and availability
- **System Reintegration**
  - Reintegrate the recovered system into the network and conduct thorough testing to ensure its security.
- **Business Continuity**
  - Implement measures to ensure business continuity, such as alternative systems or processes to minimize the impact of the incident
- **Lessons Learned**
  - Conduct a post-incident review to identify areas for improvement and update the incident response plan accordingly

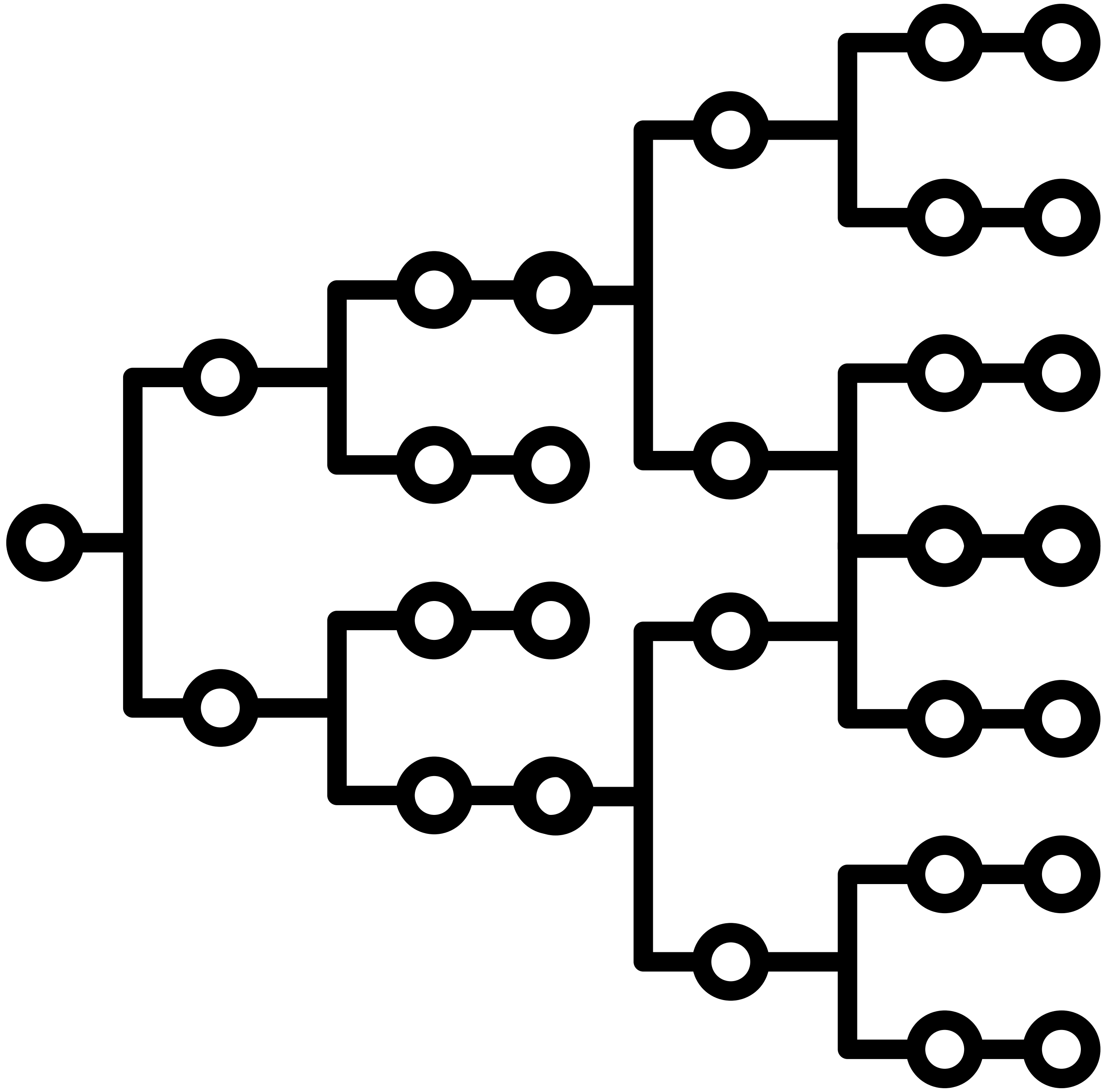
Incident Response Workflow Plan

What is a Workflow Plan?

- **Definition**
  - A workflow plan is a systematic series of steps or tasks designed to achieve a specific goal or complete a process. It outlines the sequence of actions, dependencies, and responsibilities to ensure that a task or project is executed efficiently and in a well-organized manner.
- **Purpose:**
  - They help streamline work, allocate resources effectively, and provide a structured approach to achieving objectives.

Creating a Workflow Plan

- Identify the Goal
- Map Out Tasks
- Assign Responsibilities
- Consider Dependencies
- Establish Timelines
- Review and Refine



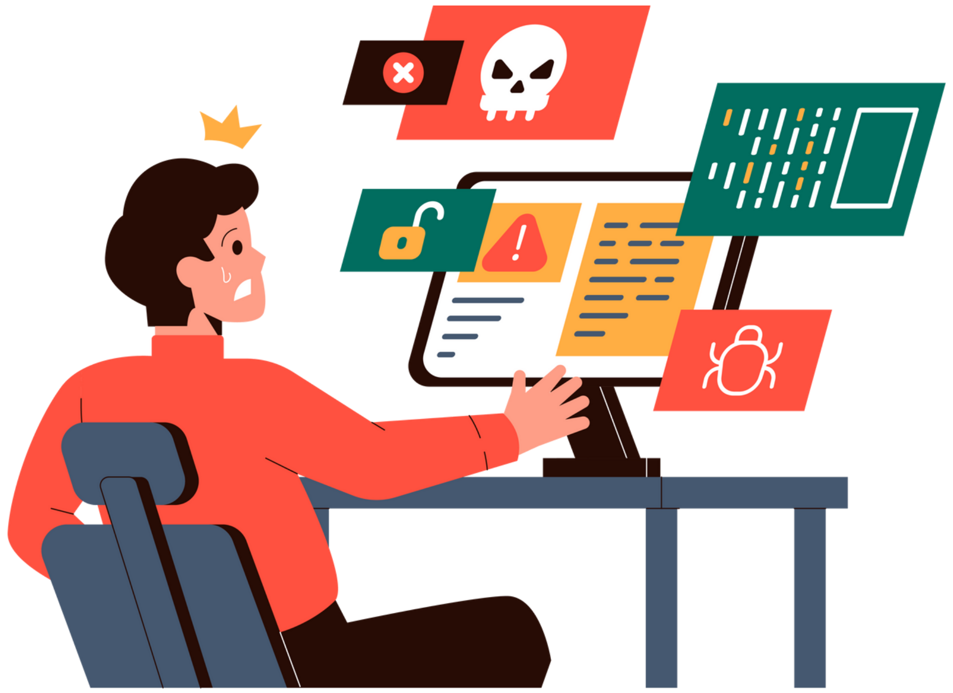
Using a Workflow Plan

- **Efficiency**
  - Streamline processes, reducing unnecessary steps and optimizing resource use.
- **Consistency**
  - They ensure a consistent approach to tasks, reducing the likelihood of errors or oversights.
- **Communication**
  - Enhance communication by defining roles, responsibilities, and dependencies.
- **Productivity**
  - Everyone understands the sequence of tasks and their role in the process.

LSU

Challenges

- **Challenges**
  - Creating and analyzing a detailed workflow plan can be time-consuming.
  - Requires a certain level of expertise in incident response.
  - Can be vulnerable to biases.



Post Incident Response

Document Incident

- **Provide a summary of the cyber attack incident**
  - Date and time of the attack
  - Method of attack (eg., phishing, ransomware, DDoS)
  - Systems or data affected

Learning From the Incident

- **Identify the key lessons learned from the incident**
    - weaknesses in cybersecurity defenses
    - lack of employee awareness and training
    - importance of regular data backups

- **Discuss how these lessons can inform future cybersecurity strategies and mitigate similar risks**

Legal Obligations

- **Report to these federal agencies immediately after an attack if any of the following data has been compromised**

- **Federal Trade Commission (FTC):**
    - Consumer Data
- **Department of Health and Human Services (HHS):**
    - Medical Records
- **Federal Bureau of Investigation (FBI):**
    - Notification based on severity and nature
- **Internal Revenue Service (IRS):**
    - Taxpayer info or sensitive financial data
- **Payment Card Industry Data Security Standard (PCI DSS):**
    - Payment card data

Legal Obligations Cont.

- **The Health Insurance Portability and Accountability Act (HIPPA)**
    - It's a federal law in the United States that sets standards for the protection of sensitive patient health information
    - In the event of a data breach of sensitive health information HIPPA requires that businesses report to both affected parties and authorities
    - Penalties are put into place for noncompliance

Disclosing to the Public

- **It is important to disclose to the public the occurrence of a cyber attack**
  - It builds trust through honesty and transparency
  - Addresses concerns and mitigates speculations
  - Demonstrates accountability and commitment to resolve the issue