Incident Management

- Privacy Incidents vs Information Security Incidents
- Know when to talk to legal, users, managers, directors
- Run a scenario from A to Z, how would you ...
- Good Practices for Running Incidents
    - How to delegate.
    - Who does what role.
    - How is communication managed + methods of communication.
    - When to stop an attack.
    - Understand risk of alerting attacker.
    - Ways an attacker may clean up / hide their attack.
    - When / how to inform upper management (manage expectations).
    - Metrics to assign Priorities (e.g. what needs to happen until you increase the prio for a case)
    - Use playbooks if available
- Important Things to Know and Understand
    - Type of alerts, how these are triggered.
    - Finding the root cause.
    - Understand stages of an attack (e.g. cyber-killchain)
    - Symptom vs Cause.
    - First principles vs in depth systems knowledge (why both are good).
    - Building timeline of events.
    - Understand why you should assume good intent, and how to work with people rather than against them.
    - Prevent future incidents with the same root cause
- Response models
    - SANS' PICERL (Preparation, Identification, Containement, Eradication, Recovery, Lessons learned)
    - Google's IMAG (Incident Management At Google)

Privacy Incidents vs Information Security Incidents

“Privacy incidents” and “Information Security Incidents” are **distinct but often related terms in cybersecurity**, each with its focus and implications:

Privacy Incidents

- Privacy incidents involve the **unauthorized or accidental access, disclosure, or misuse of personal information, like names, addresses, or health data**. These incidents primarily **concern the privacy rights of individuals and can result in legal and regulatory implications, especially under laws like GDPR or HIPAA**.
    - Example: An employee unintentionally shares sensitive customer information with unauthorized individuals.

Information Security Incidents

- Information security incidents **cover a broader range of threats to information systems, including breaches that impact data integrity, availability, and confidentiality**. These incidents **may affect any type of data, not limited to personal information, and often involve threats like malware, unauthorized access, or denial-of-service attacks**.
- Example: A system intrusion where a hacker compromises a database, potentially impacting data integrity and security.

Summary

Understanding the difference is crucial because privacy incidents generally trigger specific privacy-related response actions, whereas information security incidents focus more broadly on protecting systems and data.

Know when to talk to legal, users, managers, directors

Knowing **when to involve** legal teams, users, managers, and directors is essential for effective incident management in cybersecurity:

Legal Team:

- When: **As soon as an incident involves potential breaches of laws, regulations, or contractual obligations**. This includes privacy incidents involving personally identifiable information (PII), intellectual property exposure, or regulatory compliance issues.
- Why: Legal can help assess compliance obligations, guide responses to regulatory bodies, and mitigate potential liabilities.

Users (Affected or Potentially Affected):

- When: **Only when it's confirmed** that their data or services have been impacted or might be at risk.
- Why: Transparency is critical, especially for maintaining trust and meeting legal obligations (such as data breach notification laws). **Timing is crucial**; notifying users too early or too late can create confusion or reputational damage.

Managers (Direct Supervisors or Team Leaders):

- When: **Early in the incident** lifecycle, **as soon as the incident is confirmed** to require a response.
- Why: Managers need to know promptly so they can allocate resources, support the incident response, and keep their teams informed and on standby as needed.

Directors (Executive-Level, e.g., CISO or CTO):

- When: For significant incidents that **could impact the organization's reputation, operations, or finances**.
- Why: Directors need the full scope to make informed, high-level decisions about resource allocation, public statements, and overall incident response strategy.

Summary

This approach ensures that each stakeholder is engaged **at the right time**, helping to **keep the incident response streamlined, efficient, and legally compliant**.

Run a scenario from A to Z

Let's walk through a cybersecurity incident scenario, covering each stage and explaining when to engage each stakeholder and take critical actions.

Scenario

Phishing Attack with Data Exposure An employee unknowingly clicks on a phishing email link, which leads to unauthorized access to a database containing personal customer information.

Step-by-Step Incident Response

1. **Detection and Initial Assessment**

- Action: SOC (Security Operations Center) or security detection system flags unusual access patterns on the database.
- Assess: Determine the scope **— confirm if it's an actual incident**, and **identify what systems and data are impacted**.
- Notify: **Contact managers as soon as the incident is verified**.

2. **Containment**

- Action: **Isolate** affected systems to prevent further unauthorized access.
- Internal Coordination:
    - **Inform legal** if PII or sensitive data exposure is suspected. Legal will begin reviewing regulatory requirements and prepare for potential disclosure obligations.
    - **Brief managers** to ensure immediate containment resources and communicate with affected teams.
- User Involvement: If users' accounts are directly impacted, **consider notifying them to be vigilant of suspicious activity**.

3. **Eradication**

- Action: Analyze and **remove** phishing emails from the system, **close** exploited vulnerabilities, and enhance controls.
- Legal Review: Reconfirm if there's a need for regulatory reporting.
- Directors Briefing: Notify directors if the attack is part of a larger threat pattern or could escalate to impact operations or reputation.

4. **Recovery**

- Action: **Restore** systems and **monitor** closely to **prevent recurrence**.
- Users Notified: If personal information was accessed, **inform impacted users per regulatory guidelines**.
- Management Update: Ensure managers and directors are **updated with timelines and recovery status**.

5. **Post-Incident Review**

- Action: **Conduct a root cause analysis, review the response process, and improve controls**.

- **Management Debrief**: Report findings and lessons learned to managers and directors.
- Legal Follow-Up: Legal may support final reporting or **address compliance concerns** that arose.
- Users Communication: For significant incidents, **inform users** of corrective actions taken to improve security.

Summary

This A-to-Z scenario demonstrates a structured approach:

- **Early containment** and **collaboration with legal for compliance**.
- **Timely updates to managers and directors** to ensure alignment on resources and response strategy.
- **Transparent user communication** where relevant to maintain trust.

Good Practices for Running Incidents

Running an incident smoothly **requires clear roles, effective delegation, communication, and timing**. Here's a breakdown of best practices, with insights into handling roles, communication, and management expectations throughout an incident.

1. Delegation Best Practices

- Assign Roles and Responsibilities Early: Use a **predefined incident response team (IRT)** structure. Common roles include:
  - **Incident Commander**: Leads the incident response, makes final decisions, coordinates efforts.
  - **Triage Lead**: Assesses and prioritizes alerts, determines severity.
  - **Forensics/Analysis Team**: Investigates the root cause, examines logs, and assesses attacker actions.
  - **Communications Lead**: Manages external/internal communication, including updates to legal, compliance, and users.
  - **Legal and Compliance**: Advises on regulatory requirements, reporting, and risk.
- **Use Playbooks**: Ensure team members **have access to playbooks for specific incidents** (e.g., phishing, malware). **Playbooks provide step-by-step guidance, improving response efficiency**.

2. Communication Management

- Channels:
  - Secure Chat Platforms (e.g., Slack or Teams): For real-time coordination. Create private channels for each incident.
  - Incident Management Platform (e.g., PagerDuty, ServiceNow): To track progress, document actions, and keep all information centralized.
- Frequency:
  - Initial Notification: Alert relevant teams immediately upon incident detection.
  - Regular Updates: Provide updates at predetermined intervals (e.g., every hour) for significant incidents.
- Stakeholder Updates:
  - Internal Team: Regular updates on status, containment efforts, and ongoing investigations.
  - Upper Management: Notify upper management **when impact becomes clear, and set realistic timelines**.

3. When to Stop an Attack

- Contain vs. Stop: Sometimes, monitoring attacker actions without immediate intervention can yield critical intelligence.
- Balance the Risk:
  - Stop if the attack's harm exceeds the value of continued observation, especially if sensitive data is actively being exfiltrated.
  - Delay if monitoring can uncover attacker techniques, tools, or broader compromise without significant damage.

4. Risks of Alerting the Attacker

- Considerations:
    - Premature Blocking: May prompt attackers to intensify, diversify, or attempt lateral movements in a system.
    - Data Exfiltration: Attackers may execute final data exfiltration if they detect containment efforts.
- Best Practices:
    - Plan carefully for containment and eviction, ensuring all affected entry points are addressed to prevent re-entry.
    - Coordinate timing so all containment actions occur simultaneously, reducing the chance of alerting the attacker prematurely.

5. Attacker Cleanup/Hiding Techniques

- Methods:
    - Log Deletion/Modification: Attackers may delete or alter logs to remove traces.
    - Backdoor Installation: Attackers install hidden access points for future entry.
    - File Timestamp Manipulation: Alter timestamps on compromised files to avoid detection.
- Detection: Regular, thorough log monitoring and use of forensic tools can help spot these activities.

6. Management Communication and Expectation Setting

- When to Inform:
    - For significant incidents, **inform upper management as soon as the potential impact is understood**.
- Setting Expectations:
    - **Share a high-level incident summary, anticipated timelines, and potential business impacts**.
    - Regularly update management on milestones (containment, eradication, recovery) to keep them informed without overwhelming them.

7. Prioritizing Incidents

- **Priority Metrics**:
    - **Data Sensitivity**: High-priority if sensitive information (PII, financial data) is affected.
    - **Business Impact**: Higher priority if core business functions are disrupted.
    - **Scope**: Broad scope incidents affecting multiple systems or users take precedence.
    - **Compliance Risk**: Higher priority if compliance or legal reporting requirements are triggered.
- **Escalate Priority** if an incident's severity or impact increases, such as new data exposures or expanding attacker access.

8. Using Playbooks for Efficient Responses

- Purpose: **Playbooks** offer structured **steps for specific incidents**, helping teams work **quickly and consistently**.
- Updating Playbooks: **Regularly update** playbooks based on recent incident reviews and lessons learned.
- **Customization**: Adapt playbooks to address organizational nuances, such as unique system architecture or compliance requirements.

Summary

These practices establish a disciplined, structured incident response process, ensuring that every team member knows their role, communication is clear, and management stays informed, all while minimizing risks and ensuring a swift resolution.

Important Things to Know and Understand

Here's an overview of each of these critical areas in incident management, with explanations of why each aspect is essential for effective responses and prevention.

1. Type of Alerts and Triggers

- Why It's Important: **Different alerts indicate various stages or types of threats** (e.g., unauthorized access attempts, data exfiltration). Understanding how these alerts are triggered helps identify the nature of the threat and its severity.
- Key Knowledge: Familiarize yourself with alert types, thresholds, and how to set them based on the organization's risk tolerance. This helps prioritize response efforts.

2. Finding the Root Cause

- Why It's Important: **Identifying the root cause prevents recurrence** by addressing the actual problem rather than just symptoms. Without root cause analysis, incidents may reoccur, wasting time and resources.
- Key Knowledge: Train in investigative techniques and logging tools to trace the issue back to its origin (e.g., compromised credentials, configuration errors).

3. Stages of an Attack (Cyber-Kill Chain)

- Why It's Important: Knowing the attack stages (reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives) **aids in understanding where the attacker is within the system, enabling timely responses**.
- Key Knowledge: Tailor detection and response strategies to each stage to **disrupt attacks earlier** in the kill chain.

4. Symptom vs. Cause

- Why It's Important: **Symptoms are visible** signs (e.g., slow system performance), but **causes are underlying** issues (e.g., malware). Responding to symptoms alone may leave the root problem unaddressed.
- Key Knowledge: Document common symptoms and their potential causes to help distinguish them quickly.

5. First Principles vs. In-Depth System Knowledge

- Why Both Are Valuable: First principles thinking encourages understanding fundamental security principles, helping to solve novel problems. In-depth systems knowledge enables efficient troubleshooting within specific systems.
- Application: Use first principles to reason through unprecedented attacks while leveraging system knowledge to quickly understand and address known issues.

6. Building a Timeline of Events

- Why It's Important: **Timelines provide a chronological view of an incident**, helping to reconstruct attacker activities and identify delays or missed detections.
- Key Knowledge: Maintain logs, capture timestamps, and document actions taken. Use incident management tools to automate timeline tracking.

7. Assume Good Intent and Collaborative Communication

- Why It's Important: When working with colleagues or other departments, **assuming good intent fosters cooperation and avoids blame**. Misunderstandings can delay response efforts.
- Application: Use collaborative language, and listen actively to others' perspectives. Frame inquiries as part of learning and response improvement rather than critique.

8. Prevent Future Incidents with Root Cause Analysis

- Why It's Important: Preventative measures save time, resources, and reduce organizational risk. **Learning from each incident** strengthens overall defenses.
- Implementation: Use the **Lessons Learned stage** to create actionable follow-ups, such as patching vulnerabilities, updating configurations, or training staff.

Summary

Understanding these concepts equips incident responders to handle incidents methodically, reducing risks and creating a proactive security posture for the organization.

Response Models

Both models **provide structure and ensure a systematic approach, reducing oversights and enabling continuous improvement**.

SANS PICERL Model

- **Preparation**: Develop response playbooks, train teams, and establish clear protocols.
- **Identification**: Detect, validate, and assess incidents.
- **Containment**: Limit the attacker's access without causing further harm.
- **Eradication**: Remove the attacker from the environment.
- **Recovery**: Restore normal operations securely.
- **Lessons Learned**: Review the response, document findings, and adjust protocols.

Google's IMAG (Incident Management at Google)

- Focuses on: **Speed, scalability, and post-incident documentation**. IMAG emphasizes rapid response, clear communication, and **robust post-mortem analysis** to learn from every incident.