Develop an Organization Incident Response and Incident Handling Plan

Ryan Coon

CYB-650

Dr. Howard Goodman

August 13, 2025

Procedures for Performing Incident Handling and Reporting

Incident response strategies are structured plans outlining steps to identify, analyze, and mitigate security breaches, minimizing impact and enabling swift recovery. This involves a proactive approach, encompassing planning, detection, investigation, and continuous improvement of incident handling procedures to address vulnerabilities and enhance overall security posture. A key element is the incident response cycle, a structured process for responding to and learning from security events (Johnson & Easttom, 2022).

Preparation

To effectively prepare for and respond to incidents, prioritize these preemptive steps:

A. **Establish Baselines and Optimize Assets:**

1. Identify Critical Assets - Determine your most valuable assets—both tangible (servers, applications, network segments) and intangible (sensitive data, intellectual property). Consider the potential financial and operational impact of their compromise. A compromised asset might cause temporary disruption or, in a worst-case scenario, lead to insolvency. For example, a critical database containing customer information is far more valuable than a less-used internal tool. Remember, your attackers may prioritize assets differently than you do.
2. Prioritize and Categorize - Create a comprehensive inventory, ranking assets by their criticality to business operations. This list should include users, applications, systems, databases, and other assets, noting the potential impact of their unavailability or compromise. The higher the potential impact, the higher the priority for protection.
3. Quantify Asset Value - Assigning monetary values to your assets strengthens your security budget justification. This allows you to demonstrate the return on investment (ROI) of security measures and allocate resources effectively.
4. Define "Normal" - Establish baselines for normal system behavior by monitoring network traffic, system performance, and user activity. This will help you quickly identify anomalies that may indicate a security incident. For example, a sudden surge in network traffic or unusual login attempts from unfamiliar locations could be early warning signs.

B. **Build Relationships, Communicate Effectively, and Collaborate:**

1. Engage Leadership - Schedule meetings with corporate leadership to discuss your assessment of the company's current security position. Present market trends, highlight key challenges, and propose recommendations for improvement. Clearly define the roles and responsibilities of the Incident Response (IR) team, other departments, and external parties, setting expectations for communication, metrics, and contributions (Lowe et al, n.d.).
2. Foster Cross-Functional Collaboration - Streamline incident management processes by establishing collaborative relationships with administrative, Human Resources, and procurement teams. This facilitates efficient handling of requests and ensures a coordinated response during critical incidents. Let's make sure we're all on the same page and working together smoothly. This is about building strong relationships, talking openly, and collaborating effectively

C. **Direct, Document, and Update:**

1. Clarify Roles and Responsibilities - For each team member, clearly define:
   * What specific actions they should take.
   * The precise timing of these actions.
   * The rationale behind their actions.
2. Provide Comprehensive Training and Instructions - Offer thorough training, guidance, and detailed instructions, especially for team members outside of IT. Document these procedures and regularly review them, both individually and as a team. The time invested in preparation before an incident will be invaluable.
3. Establish and Maintain a Communication Cadence - Set a regular schedule for providing updates that is acceptable to all stakeholders. Consistent and timely updates are crucial, especially for the executive team, to keep them informed and allow them to make informed decisions. This is about clear instructions, detailed records, and keeping everyone in the loop.

**Guidelines for Communication with Outside Authorities**

**Immediate Transparency:**

Upon encountering an issue, swiftly acknowledge its presence. Paint a concise picture of its immediate impact, foreshadowing further updates to come. If possible, immediately address any anxieties regarding data breaches or security vulnerabilities.

**Consistent Communication:**

Maintain a steady flow of information, keeping your audience informed. Updates should occur at intervals of approximately 30 minutes, or as frequently as the situation demands.

**Crystal-Clear Communication:**

Honesty, accuracy, and integrity are the cornerstones of effective crisis communication. Articulate the issue with the precision of a surgeon, ensuring clarity for all stakeholders. Explain its impact with sensitivity, showing an understanding of their concerns.

**Unified Communication:**

Maintain a consistent message across all platforms. Regular updates, delivered with the same urgency and clarity, should resonate across all communication channels (e.g., Twitter, email). This unified front ensures a strong, harmonious response, like a well-rehearsed orchestra.

**Taking Ownership:**

Even if the problem originates from a third-party provider, it is your responsibility to address it. In the eyes of your clients, the issue reflects directly on your services. Embrace this responsibility, showing empathy and consideration. When appropriate, offer a sincere apology, demonstrating your commitment to their well-being. This is more than just damage control; it is a testament to your character.

**Incident Report Process Standards for Subcontractors or Customers**

The International Organization for Standardization (ISO) is a private, non-profit body that develops global standards to ensure the quality, safety, and efficiency of products, services, and systems. For example, the ISO/IEC 27035 standard on Information Security Incident Response provides crucial guidance for clients and subcontractors on preventing and managing information security incidents. This standard details procedures for handling security incidents, events, and potential threats (Coccolini, 2020).

**Incident Handling Team Structure**

Incident response teams are the first line of defense against cybersecurity threats, requiring a diverse skillset to effectively manage crises. These teams, often known as CSIRT (Computer Security Incident Response Team), CERT (Computer Emergency Response Team), or Cybersecurity Centers, are comprised of specialists who must act swiftly and decisively(Wang & Johnson, 2018). The success of these teams hinges on the careful selection of personnel and the implementation of robust response strategies.

**Key Roles and Responsibilities:**

The optimal incident response team is a carefully orchestrated symphony of expertise. Consider these essential roles:

* Team Leader - This individual orchestrates team operations, ensuring seamless collaboration and providing crucial updates to senior management. They are the conductor of this critical response orchestra.
* Communications Specialist - This vital role manages both internal and external communications, ensuring transparency and coordinated messaging to clients, partners, and regulatory bodies. They are the voice of calm amidst the storm.
* Lead Investigator - This individual spearheads the initial investigation, meticulously analyzing the incident's scope and impact. They supervise other analysts, providing a comprehensive understanding of the cybersecurity breach. They are the detectives, meticulously piecing together the puzzle.
* Analysts and Researchers - These experts assist the lead investigator, providing invaluable insights into the threat landscape and the circumstances surrounding the incident. They are the forensic scientists, providing critical data analysis.
* Legal Counsel - Providing expert guidance on compliance, interacting with law enforcement, and ensuring the preservation of evidence. They are the guardians of legal and ethical integrity.

**Communication between Staff and Incident Response Teams**

Effective incident communication is crucial for maintaining user trust and confidence. It involves four key phases:

1. Immediate Notification - Upon discovering an incident, promptly inform users. This initial communication is vital; delayed discovery by users can severely damage trust and create more significant problems.

2. Frequent Updates - While the incident persists, provide regular updates to keep users informed about the situation and the expected restoration timeline. Frequent updates demonstrate your team's dedication and proactive problem-solving approach. Avoid prolonged delays between updates.

3. Resolution Announcement - Once the incident is resolved, formally announce its resolution to users. Clearly explain the issue, its root cause, and the implemented solution. If necessary, guide users through any required actions, such as password changes or monitoring their accounts.

4. Post-Incident Review - Conduct thorough post-incident assessments and, where appropriate, publish public postmortems to enhance transparency and facilitate continuous improvement. This fosters accountability and demonstrates a commitment to learning from past experiences.

**Types of Service Incident Response Teams Provide**

Elevate your incident response capabilities with our expert team. We enhance your risk intelligence, enabling more strategic planning and faster emergency response. Our collaborative approach helps you develop a comprehensive, proactive security strategy to prevent incidents before they occur(Baskerville, 2002). Should an incident arise, we swiftly minimize impact, identify root causes, and lead the response. This service is adaptable, complementing your existing security measures or functioning as a standalone solution. Tailored to your specific needs, our services encompass communication, proactive incident management, risk intelligence, security assurance, vulnerability assessments, and threat hunting. We deliver support in three phased deployments, focusing on your critical areas.

**Training and Staffing Requirements for the Incident Response Team**

Incident response team structures vary widely, influenced by several key factors:

* Team Mission and Objectives - The team's goals directly shape its composition and skillset.
* Service Scope - The types of services offered determine the necessary expertise.
* Staff Expertise - A skilled team is paramount for effective incident response.
* Organizational Context - The size, technological infrastructure, and overall environment influence team structure.
* Incident Volume - High-volume environments require larger, more specialized teams.
* Incident Severity - Complex or critical incidents demand highly skilled personnel.
* Budgetary Constraints - Resource allocation impacts team size and capabilities.

Regardless of team structure, every member requires a core set of essential skills for effective incident handling. Many teams maintain a core group providing foundational incident management services, ensuring a baseline level of competence across all operations.

**Personal Qualities:**

Incident handlers regularly interact with diverse stakeholders, including colleagues, response partners, subject matter experts, and individuals with varying levels of technical knowledge.(Leme, 2024) Therefore, strong interpersonal skills are essential for effective communication and collaboration. The professional conduct of team members directly impacts the organization's reputation. Incident handlers spend a significant portion of their time communicating with a wide array of individuals, including colleagues, response partners, subject matter experts, and stakeholders with varying technical expertise. Consequently, robust interpersonal skills are critical for effective communication and collaboration. The professional conduct of incident response team members directly influences the organization's reputation and public perception. Since incident handlers spend a large chunk of their day talking to people – their teammates, partners, experts, and folks with different levels of tech knowledge – strong people skills are a MUST. It's all about clear communication and working together. The way team members act and interact can seriously impact the organization's reputation.

**Teamwork:**

Incident response team members must collaborate effectively and professionally. Adaptability and a willingness to adjust are essential. Strong teamwork skills are also necessary for communication with other teams, such as IT. Interpersonal conflicts can negatively impact team performance, efficiency, and reputation, potentially leading to employee turnover within the incident response team. Incident response team members must possess strong interpersonal skills, fostering effective and professional collaboration. Adaptability and a willingness to adjust to evolving situations are also critical. Teamwork skills are essential for effective communication and coordination with other departments, such as IT. Interpersonal conflicts can severely undermine team performance, efficiency, and reputation, potentially leading to employee attrition within the incident response team. Incident responders have to work well together. Adaptability is key, and they need to be flexible. They also need solid teamwork skills to communicate with other teams, like IT. Bad vibes and conflicts can kill team performance, hurt the company's image, and even make people quit.

References:

Baskerville, Richard, and Mikko Siponen. “An Information Security Meta‐Policy for Emergent Organizations.” *Logistics Information Management*, vol. 15, no. 5/6, Dec. 2002, pp. 337–346, https://doi.org/10.1108/09576050210447019.

Coccolini, Federico, et al. “COVID-19 the Showdown for Mass Casualty Preparedness and Management: The Cassandra Syndrome.” *World Journal of Emergency Surgery*, vol. 15, no. 1, 9 Apr. 2020, https://doi.org/10.1186/s13017-020-00304-5.

Johnson, Rob, and Chuck Easttom. *Security Policies and Implementation Issues*. Burlington, Ma, Jones & Bartlett Learning, 2022.

Leme, Rodrigo. “Incident Response Teams: Roles and Responsibilities.” *Right-Hand Cybersecurity*, 19 Nov. 2024, right-hand.ai/blog/incident-response-teams/.

Lowe, Nick, et al. “How Can IT Operations Teams Collaborate with Other Departments during a Security Incident?” *Www.linkedin.com*, www.linkedin.com/advice/1/how-can-operations-teams-collaborate-other-departments-mif8e.

Wang, Ping, and Christopher Johnson. “CYBERSECURITY INCIDENT HANDLING: A CASE STUDY of the EQUIFAX DATA BREACH.” *Issues in Information Systems*, vol. 19, no. 3, 2018, pp. 150–159, iacis.org/iis/2018/3\_iis\_2018\_150-159.pdf.