Incident Response Plan

Bank of America Merrill Lynch

A proactive approach is your best defense.

In today's fast-evolving threat landscape, cybersecurity incident response plans are essential because security attacks can compromise systems in a matter of minutes. To avoid being unprepared, businesses need to amend their strategy and plan for intrusions. Companies should not ignore these threats; rather, they should actually plan for cybersecurity events via well-developed and tested incident response plans.

Incident response plan

Organizations must create an effective response plan that addresses the entire crisis management lifecycle. Each phase of the lifecycle presents opportunities to protect the organization from risks, costs and damage emanating from an incident. The overall goal of an effective response plan is to strengthen the organization's defenses going forward.[1] Once the organization has a plan, reviewing and testing the plan at periodic intervals is also essential.

Plan and prepare[2,3]

- **Security incident.** Incidents must meet defined and established thresholds in order to be designated a "security incident". This helps reduce false alarms and ensures that when a breach does occur, maximum resources are available.
- **Evaluate the organization's risk potential.** Look closely at all areas, systems and processes within the organization. Research and think through as many security breach scenarios as possible. Classify risks based on severity, scale, scope and potential confidentiality, integrity and information availability impacts. Determine the organization's greatest risks and stack rank them. Ensure that the organization establishes controls and contingency processes, prioritizing the riskiest situations ahead of those that present less risk.
- **Form an incident response team:**
  - Identify key-stakeholders and assign specific roles that clarify individual responsibilities and authority.
  - Ensure that all areas of the business are represented (e.g., information technology services, security management, legal, human resources and public relations).
  - Establish external communications guidelines and ensure that regulatory and compliance reporting requirements are met.
  - Establish handoff and escalation points within the incident management process.
- **Create a fraud event playbook**. Create detailed and comprehensive courses of action. Include metrics that measure the response team's capabilities and effectiveness. Create checklists, detailed processes and forms that will help walk incident response teams through each step in the recovery process. The incident response policy should give the response team the framework to quickly classify incidents into categories. Each category should have tailored security response plans and checklists. This approach provides response teams with quick, actionable guidance that will help achieve the goal of reducing breach impact.

[1] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf

[2] https://searchsecurity.techtarget.com/ehandbook/Crafting-a-cybersecurity-incident-response-plan-step-by-step

[3] https://www.incidentresponse.com/a-guide-to-creating-an-incident-response-plan/

- **Practice incident response.** Tabletop exercises are effective at simulating an incident response.
    - These exercises should engage all levels of employees within the organization, with the goal of fostering trust and responsibility among the team.
    - Ensure that all areas of the business are represented (e.g., information technology services, security management, legal, human resources and public relations).
    - Focus exercise preparation on detailed scenarios so that the incident response team can collaboratively develop a realistic and appropriate response plan.
    - Create robust exercises that allow organizations to identify weak points in recovery preparedness as well as develop strategic plans that address items that may be otherwise overlooked.
- **Ensure that audit logs are generated and archived.** Treat security breaches as a disaster; it's important to remember that – very likely – it is also a crime. If the latter, the data is the evidence and must be protected. Audit logs should contain the following information:
    - Identifying information, e.g., location, serial/model number, hostname, message authentication code and IP addresses.
    - Name, title and contact information of each individual that collected or handled evidence during the investigation.
    - Date and time (including time zone) of each occurrence of evidence handling.
    - Location(s) where evidence is stored.
- **Conduct post-incident review and discussion.** A lessons learned de-brief with all involved parties is critical to improving both security measures and the incident response process. This post-incident review should generate two items:
    - A comprehensive **incident report**. This report will serve as institutional knowledge for future reference.
    - A **list of changes** needed to the incident response policy or security infrastructure.
- **Engage external resources**, e.g., financial institutions, cyber security firms, vendors and law enforcement. It's essential to alert external resources in the event of a security breach. A timely response can lessen the impact of a breach.

For more information

For more information about risk assessments and incident response plans, visit our Fraud Education site through CashPro Assistant: https://cashproonline.bankofamerica.com/cpocms/sites/CashProUniversity/Landing/Fraud/page.htm