exabeam

Checklist

Business Continuity as Part of Your Incident Response Plan

You've experienced a cyberattack.

How are you supporting business continuity as part of your incident response?

Here is a checklist to help.

An incident response (IR) plan without a business continuity component is like a house without a roof — seven months out of the year you could be just fine, but when winter comes, you're in trouble. The incident response plan reviews and responds to any cybersecurity incident or attack which may, or may not, disrupt business operations. Either way, including a business continuity component is the proactive way to support business operations and critical infrastructure.

Having some critical steps related to business continuity can mean the difference between costly downtime or a barely noticed disruption. Business continuity as a part of your incident response plan prepares you to minimize the impact of an attack while finding and fixing the cause to prevent further damage.

While business continuity often lives within the IT department, when an incident results in an intrusion, the cybersecurity team is a key partner in minimizing the impact on the business. With this in mind, this checklist outlines how to incorporate business continuity steps within your incident response plan.

Define Processes for Decision Making

- External threats — Determine whether intentional or unintentional actions by a person or group outside the organization have affected systems or the business.
- Internal threats — Determine whether intentional or unintentional human intervention has affected systems or the business.
- Once determined, apply the use case content relevant to the external (phishing or ransomware) or internal (malicious insider or lateral movement) threats.

Define Processes for Response

Consult your incident response plan to determine the steps that need to be taken next.

- What are the symptoms of an incident? What systems are impacted? Who reported it?
- Who in IT, Facilities, Product Operations, and Engineering will be involved in incident response (related disaster recovery teams)?
- Who can declare that a triaged event is an incident? What defines that declaration? Who is notified of the incident? When do you launch the incident response plan?
- What are the defined criteria that define the difference between a critical, high, medium, or low severity incident? What is the target reaction time for each as output from the process?
- Who is the incident commander?
- Who has the "stop work" authority? Who determines whether customers or employees must be notified?
- Understand how you will work the incident: What systems will preserve information and what information must they collect? Who in IT or Security owns these?
- Containment: This should occur only if the indications observed conclusively show that an incident has or is occurring.
- Preservation: Gather all the artifacts and details of the breach for further analysis of origin, impact, and intentions. Make sure support teams know what to preserve.
- Eradication: Ensure with Security Operations that any infected files are fully deleted before the system(s) is restored to its normal operational state or requires a replacement of hardware.
- Recovery: Return the systems back to normal — can involve backups, both "warm" or "hot," and be local, remote, or cloud (with different test cases for each).
- Follow-up: Perform a post-incident analysis to document exactly what happened and when, and how to improve incident handling by your organization in the future.

Define Processes for Communication

- Have an incident declaration mechanism (email, phone call, Teams/Slack/IM, etc.) communicated to relevant stakeholders, and identify necessary information gathering steps for the first-level responders.
- Identify all levels of escalation for cyber incidents — a clear "chain of command"
- Identify who owns communication of the incident to the rest of the chain
- Ensure contact information for each involved primary and secondary stakeholder is recorded in the incident response plan.
- Map out your incident response workflow between different stakeholders: When are IT and Security involved? What kind of incidents require corporate communications or legal?
- Determine a cadence for both top-level and top-down communications: hourly, daily, etc.
- Create clear instructions for all members of the organization to understand if and how they should talk about the incident.

Define Processes for Recovery

- Evaluate which recovery and continuity actions should be invoked
  - Set restoration priority based on the damage assessment reports
  - Determine recovery needs
  - Determine if IT vendors or other teams are needed to assist with detailed damage assessment
  - Facilitate business and technology recovery and restoration activities
  - Provide guidance on replacement equipment and systems, as required
  - Prepare post-disaster debriefing report
  - Coordinate the development of site-specific recovery plans and ensure they are updated regularly
- Facilities
  - Assess the status of facilities
  - Manage facilities damage assessment and restoration
  - Manage relocation of facilities and personnel
  - Manage safety and security issues
  - Communicate with building owners and insurance as needed
- Product Operations and Engineering (DevOps)
  - Assess the status of product infrastructure, applications, and services
  - Coordinate with relevant vendors on mitigations or workarounds if a fix is not available
  - Establish recovery priorities and timelines
  - Engineer patches and/or workarounds
- Corporate IT
  - Assess the status of corporate infrastructure, applications, and services
  - Coordinate with relevant vendors
  - Establish recovery priorities and timelines
  - Track and manage high level IT support
  - Apply mitigation, patches, or workarounds
  - Ensure employee connectivity to infrastructure regardless of location
  - Address any new employee equipment needs
- Ensure that post-mortems are conducted on all events regardless of size, and documented so that all lessons learned are incorporated into the future program

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR), from common security threats to the most critical ones that are difficult to identify. The Exabeam Security Operations Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm.

For more information, visit exabeam.com**.**