INCIDENT RESPONSE TESTING AND PREPAREDNESS: READINESS THROUGH RESPONSE PLAN EXERCISES

In today's data-driven world, companies of all sizes face the sobering threat of a cybersecurity incident like a data breach or ransomware attack. Recent high-profile breaches impacting organizations such as Yum! Brands, T-Mobile, Uber, or Equifax underscore how vulnerable even sophisticated enterprises can be. With hackers continually honing their craft and developing new vectors of attack, no system or network is immune.

When (not if) your organization faces a cyber incident, your response in the first hours and days is critical. An immediate, well-coordinated response can significantly limit damage and cost. However, hesitation, confusion, or gaps in your response plan can allow the impact to spiral. That's why thoroughly testing your incident response capabilities before an actual breach is essential.

Structured incident response exercises assess readiness, surface issues, and empower your team to respond confidently in a real crisis. This article delves into creating an effective incident response testing program to equip your organization to act swiftly and effectively when hackers come knocking.

ASSEMBLING THE INCIDENT RESPONSE TEAM

The first step in preparing for incident response is identifying key stakeholders from across your organization to assemble an incident response team. This cross-functional team should include:

- IT and IT security leaders to investigate, contain, and remediate technical issues
- Legal counsel to provide guidance on compliance, disclosure obligations, and law enforcement interactions
- Communications/PR to control internal and external messaging
- Business leaders like the CISO, CIO, and CFO to assess business impact and make strategic decisions
- Human resources to address issues like contacting affected individuals, post-breach support for employees, etc.
- Other roles like risk management, internal audit, corporate investigators, etc. as applicable

This team composition allows you to tap into a diverse set of skills and expertise required for an effective breach response. Team members should have clearly defined roles and responsibilities. Consider developing an incident response plan document or playbook outlining the team structure, communication protocols, technical and legal response procedures, reporting requirements, and integration with business continuity plans.

CONDUCT TABLETOP EXERCISES

Once you've assembled your team, tabletop exercises offer an impactful yet efficient way to validate your incident response plan. A tabletop exercise gathers the response team in a conference room or virtual meeting to walk through a hypothetical breach scenario.

The facilitator (perhaps the CISO or legal counsel) sets the stage and discloses details of the fictional incident one step at a time. This could involve a ransomware attack encrypting critical servers, a phishing scheme resulting in stolen customer PII, or even an insider threat situation.

As new information is revealed, the team discusses their response. Who would they notify first internally? What technical actions would they take? How would they communicate externally if needed? The facilitator may also toss in plot twists or inject obstacles to raise new considerations.

ETHICO

TABLETOPS PROVIDE SEVERAL BENEFITS

- Tests policies and procedures outlined in the response plan in a low-stress setting
- Clarifies roles and responsibilities for each team member
- Surfaces potential gaps in the plan, outdated contact information, need for additional tools or capabilities
- Allows the team to ask questions and think through complex response decisions
- Offers post-exercise debriefs and plan updating based on findings

To maximize effectiveness, keep the exercise timeframe tight (e.g. a high-level overview in an hour, or a more detailed half-day version). This mimics the urgency of responding in the first hours of an actual incident. Also, encourage participants to be candid about weaknesses they observe - this is about strengthening capabilities, not showing off.

EXECUTE RED TEAM EXERCISES

- While tabletops offer high-level walkthroughs, red team exercises involve simulated hands-on attacks to probe an organization's detection and response capabilities in an operational environment. Security professionals launch actual penetration tests against systems and networks to emulate tactics of real-world attackers.

- The key distinction is that the red team does not actually access or delete non-test data. However, much like an ethical hacker, the team may attempt phishing, social engineering, malware, scanning tools, and other tactics to breach defenses. Defenders are not given advanced knowledge of the specifics or timing of red team activities.

- Designed thoughtfully, red team exercises provide organizations several advantages:

    - Tests effectiveness of intrusion detection systems, firewalls, and other controls
    - Gauges the ability of security staff to rapidly detect and respond to threats
    - Measures adherence to incident response plans and procedures during high-pressure situations
    - Builds collaboration, communication, and coordination between cybersecurity and IT teams
    - Drives proactive improvements to policies, tools, and processes

- Start with limited-scope tests (e.g. targeting a single application or just social engineering attempts), then broaden into enterprise-wide exercises over time. Thoroughly document lessons learned after each exercise. Implement remediation plans for identified vulnerabilities before the next exercise. Maintain close coordination between red teams and business leaders throughout testing.

SET A REALISTIC TIMEFRAME

- Whether conducting a tabletop, red team exercise, or other simulated incident, setting the timeframe is vital. Limit the duration to 12-72 hours. This compresses decision-making and forces responsive action, as occurs during an actual breach.
- Resist the temptation to provide the response team extensive time to deliberate on "perfect" solutions. Also avoid scenarios that drag on for weeks of simulated time. The intensity will quickly wane as participants lose focus.
- A compressed timeline also curtails "Monday morning quarterbacking" where teams over-analyze decisions after the fact. Make the duration short enough to keep participants engaged but long enough to incorporate the crucial initial response steps. This strikes a balance between realism and practicality.

DOCUMENT FINDINGS IN AN AFTER-ACTION REPORT

Shortly after completing an incident response exercise, gather participant feedback and document findings in an after-action report. Capturing strengths and areas for improvement while the experience is still fresh can provide valuable input for enhancing your cybersecurity posture.

Include the following elements in your after-action report:

- **Exercise overview:** Date, duration, scenario, participating teams/roles, and objectives
- **Summary of events:** Brief timeline of what happened and decisions made during the exercise
- **What went well:** Strengths like clear communication, decisive leadership, or effective containment measures
- **Improvement opportunities:** Shortcomings like unclear responsibilities, lack of visibility into systems, inadequate tools, or slow mobilization
- **Remediation plan:** Specific steps to address gaps, owners, and timeframes
- **Lessons learned:** Key takeaways to guide training, policies, and future exercises

Have participants review the report to validate that it accurately captures their perspectives. Most importantly, follow through on the remediation plan. This transforms observations into concrete preparedness improvements driven by your team's actual response capabilities rather than theoretical best practices.

FOCUS ON LEARNING, NOT PERFECTION

Approach incident response exercises as learning opportunities rather than assessments. The goal is not to flawlessly execute your plan - unknown variables and unanticipated challenges will invariably arise during real crises.

By rehearsing and identifying weak spots in a low-risk setting, your team can fine-tune responses, relationships, and procedures. Prioritize exploring different scenarios and decision points over scoring achievements. Foster an environment where participants can be candid about areas for bolstering preparedness without fear of blame.

Reflect on mistakes as wisdom gained rather than failures. Document them as lessons learned and implement changes to do better next time. Celebrate progress made with each iteration. Measure readiness by your ability to quickly adapt and respond cohesively as a team. Perfection is unrealistic - continuous informed improvement is the mindset to maintain.

DEVELOP A CYCLICAL EXERCISE PROGRAM

One-off exercises are valuable, but ingrain incident response proficiency organization-wide, build exercises into a normal business rhythm. Establish a cyclical schedule of tabletops, red team drills, and other exercises with different scopes and formats.

Integrate these into ongoing training, education, and policy review initiatives. Regular exercises keep plans fresh, extend reach to more teams, and incorporate learnings continuously. Tie tests into updates of your incident response playbook.

Variety also boosts engagement from participants. Vary scenarios, teams involved, and exercise formats. Occasionally involve external facilitators to bring new perspectives. Maintain a backlog of exercise ideas linked to recent incidents, high-risk areas, and preparedness gaps.

Up your game by coordinating exercises across partner organizations to rehearse coordinated response processes. This forges trust and sets expectations for real cooperation during mutual crises.

ETHICO

Contact Us for More Information | 800-859-8840 sales@ethico.com | www.ethico.com