Turning the Tables on CYBER BREACHES

How Incident Response Tabletop Exercises Prepare Your Organization For Cyber Threats

AVALON

The exercise is designed to help your organization **practice for a real event** and facilitate conceptual understanding, **identify strengths and weaknesses,** and/or **achieve changes in policies and procedures.**

Just as you should run fire drills to keep your employees safe, your company should regularly practice managing security incidents and breaches. Incident response (IR) testing – in particular, tabletop exercises – helps you and your team increase awareness of cyber threats, determines the strengths and weaknesses of your incident response plan (IRP), and assesses how well you work together to respond to and recover from a cyber incident.

This white paper, created for small and medium-sized business leaders, explains what an incident response tabletop exercise is, who should be involved, types of scenarios, what some of the benefits and barriers are, and why it's time to assemble your team to ensure that you're ready to battle a breach together.

What is a tabletop exercise?

A tabletop exercise is a facilitated discussion of a scripted scenario in an informal, stress-free environment that is based on current applicable policies, plans, and procedures, including an IRP. The exercise is designed to help your organization practice for a real event and facilitate conceptual understanding, identify strengths and weaknesses, and/or achieve changes in policies and procedures. The success of the exercise depends largely on group participation and the identification of problem areas and the resolution of those problems.

Who should be included in the exercise?

Whether your team is remote, hybrid, or operates from multiple locations, all relevant personnel, commonly referred to as the incident response team (IRT), need to know how to react and must be included in the testing. This includes internal personnel, as well as third-party contacts such as vendors, law enforcement, and reporting agencies, which will vary depending on laws, regulations, and standards applicable. Examples of vendors who may be beneficial to include are your managed service providers (MSPs), breach coaches, and insurance carriers.

Depending on the **size and complexity** of your organization, you may want to hold **separate testing sessions** for IT personnel versus executive-level personnel.

Although it varies by organization, common roles and responsibilities that make up an IRT are:

- **Commander/Coordinator –** responsible for convening and overseeing operation of the IRT or crisis management team and is an expert on incident response, security threats, and vulnerabilities
- **Incident handler** – responds to suspicious activity reports, identifies potential vulnerabilities, and works with Commander to update IRT, track statistics and performance, preserve evidence, and provide overall support
- **Scribe** – documents incoming incident logging and reporting, helps schedule meetings of the IRT and gathers information from IRT members
- **Representatives from internal departments,** including the executive suite, finance, risk management, human resources, communications/public relations, and legal
- **Vendor support organizations,** such as incident response services, insurance contacts, and additional legal counsel

Depending on the size and complexity of your organization, you may want to hold separate testing sessions for IT personnel versus executive-level personnel. This is because the information you want to focus on for each group will differ based on the typical associated roles and responsibilities. IT tends to be more heavily involved and have a more technical-focused knowledge base, while executives are involved at a higher level and do not need to focus on the technical aspects of the procedures in most cases.

What scenarios should be considered?

Many events that occur at an organization will require investigation and may even require initiating incident response capabilities and the IRP. These can be cyber or physical incidents and can originate inside the business or via external attackers, or as a result of other events, such as weather that disrupts systems or the supply chain.

Examples include, but are not limited to:

- **Removable media or peripheral device execution** – can be tied to sensitive data loss and the intentional or unintentional spreading of malware between devices, which could infiltrate an entire network
- **Attrition or brute force compromises** – methods to systematically guess credentials and encryption keys to compromise, degrade, or destroy systems, networks, or services
- **Web attacks**
- **Email or phishing attacks**
- **Improper usage of assets** based on an organization's acceptable use policy (insider threat)
- **Loss or theft of equipment**
- **Ransomware**
- **Advanced persistent threat (APT)** – sophisticated attack where an intruder establishes a presence in the network undetected to access or steal data over an extended period of time
- **Cybercriminals or nation-states**
- **Weather events** interrupting technology, services, or systems

Each exercise can include testing based on one – or multiple scenarios – and your organization should aim to mature the exercise over time, once established.

"Cyber incidents can still occur regardless of your security awareness program and defense-in-depth strategy. There must be a plan for when that incident takes place.

Tabletop exercises–meetings in which participants discuss **simulated emergency situations**–help businesses assess whether they are sufficiently prepared to respond to a cyber-related incident."

EXAMPLE SCENARIO:

Ransomware

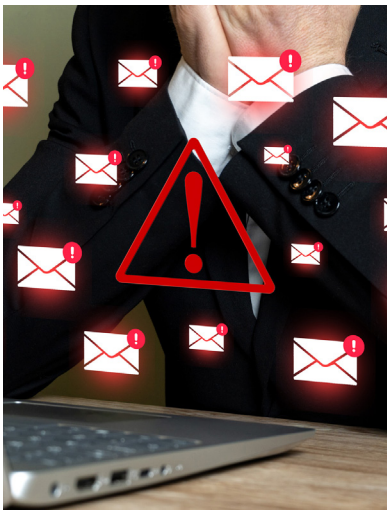
A high volume of IT tickets has come in regarding phishing emails sent to employees, which contained unusual links and attachments. Computers of those who fell victim to the phishing email appear to have been infected with ransomware. A message demanding payment for the decryption key is displayed, as well as a warning that the key will expire if payment is not received within 48 hours, at which time the data will be lost and/or publicly posted. What is your response?

Sample discussion questions:

- Who within the organization would you need to notify?
- Who has authority to activate your IRP?
- How would you check to see if data backups are viable?
- Do you pay the ransom? Who would make this decision?
- Are any outside parties needed to assist in this process?
- Does your organization have training and policies to prevent this from occurring again?

What happens before, during, and after a tabletop exercise?

- **Preparation and Planning** – Begin with a kick-off call with your key stakeholders. During this call, and any subsequent planning calls, all details of the project should be confirmed, including scope, needed resources, deliverables, and timelines. This should also include gathering relevant documents for review and answering a few questions that will help the cybersecurity vendor gather applicable context on your environment and perform the exercise using the most relevant scenarios.
- **Executing the Exercise** – The cybersecurity team will facilitate the exercise and come prepared to lead with scenario injection points applicable to your organization and associated questions. The IR tabletop exercise includes a walkthrough of the plan based on the scenarios presented, and participants will learn of the scenario, enact the plan, and work through different situations and viewpoints.



Research found that an employee at **a small business** with less than 100 employees **will experience 350% more social engineering attacks** than an employee at a larger enterprise.

- **Analyze and Report** – The exercise will help analyze your organization's ability to coordinate, collaborate, and use response capabilities in reaction to a significant cyber incident. In doing so, the cybersecurity vendor will identify any changes or lessons learned that will improve your IRP approach and ability to handle an incident more effectively in the future.

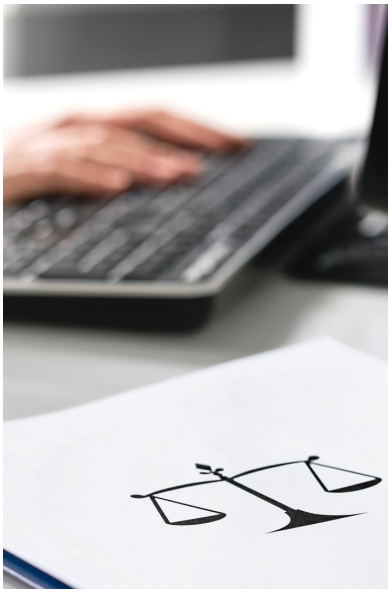
What are the benefits of tabletop exercises?

No matter what industry you're in or the size of your organization, you will eventually be targeted by cyberattacks. In fact, research found that an employee at a small business with less than 100 employees will experience 350% more social engineering attacks than an employee at a larger enterprise.

One of the best ways to be prepared for these events is to practice how your team will respond to a variety of scenarios and demonstrate the capabilities of your organization's processes, personnel, and technology. This will avoid confusion, last minute scrambling, and delayed response or containment during an actual incident or breach.

Exercising your IRP:

- Provides an opportunity to discuss and answer critical questions such as:
  - *Who will maintain and update the IRP?*
  - *Who has authority to enact the IRP or the IRT?*
  - *Who is responsible for internal and external communication? Do we have statements prepared?*
  - *Do we have appropriate personnel (internal and external) and technology in place?*
  - *If dealing with ransomware, would we pay the ransom? In what circumstances?*
  - *What third-party support do we have available?*
  - *What does our cybersecurity insurance actually cover?*



Many laws, regulations, and standards that may apply to your organization **require an IRP to be in place** and tested regularly.

- Benchmarks preparedness and understanding of your IRT's roles and responsibilities
- Increases awareness and understanding of threats and solutions
- Promotes communication between departments and levels of stakeholders
- Increases preparedness and reduces liablity
- Decreases costs related to incidents that do occur
- Shows your organization's strengths and weaknesses through lessons learned
- Prepares your team for the future by providing insights that will help you revise your IRP and related documentation and procedures
- Proves diligence in this area and is important for audit and insurance purposes

In addition to being an overall best practice for organizations, many laws, regulations, and standards that may apply to your organization require an IRP to be in place and tested regularly. The cybersecurity pros at Avalon highly recommend performing incident response exercises once a year, at a minimum, and documenting the methodology, participants, topics, outcome, and lessons learned.

What are potential barriers to performing a tabletop exercise?

Unfortunately, many organizations do not exercise their IRP as often as they should. This is commonly due to one or more of the following challenges:

- Not knowing where to start (documentation or process)
- Limited budget
- Absence of documented policies, procedures, or plans (or outdated ones)

In 2022, weekly cyberattacks worldwide reached a peak of 1.2K attacks, a **32% increase year-over-year.**

- Not having assigned roles and responsibilities
- Lack of training (at hire or on a regular basis) for key participants, which makes exercises inefficient or unsuccessful
- Aligning schedules of all involved
- Lack of management buy-in

The last barrier – getting C-suite approval – may be the biggest issue, as without their support, financial or otherwise, tabletop exercises are unlikely to happen. Cyber incidents are one of the largest threats to organizations and the realization and importance of this should be conveyed to management to ensure they understand the criticality of these efforts to the business operation and the financial status of the organization. Setting aside time, money, and personnel resources for response preparedness, training, and exercises will be far less of a burden than those needed to recover from incidents and breaches.

Why it's time to perform a tabletop exercise

So far, 2022 has been quite a year for cybercriminals and nation-states, beginning with the Apache log4j vulnerability, soon followed by the invasion of Ukraine by Russia, which spurred cyber warfare like we've never experienced before. And the hits kept coming, from ransomware attacks on hospitals and schools to data breaches and distributed denial-of-service (DDoS) attacks against financial institutions and governments.

According to Check Point Software Technologies, in 2022, weekly cyberattacks worldwide reached a peak of 1.2K attacks, a 32% increase year-over-year, and one out of 40 organizations were impacted by ransomware attacks, a 59% increase year-over-year.

To some businesses, however, it can still seem as if cybersecurity is an "extra" expense and that they'll never be targeted. Unfortunately, it's just not true and there are dozens of statistics that prove otherwise. This means, of course, that cybersecurity should officially be considered a cost of doing business for organizations of all size and across every industry.

By year-end 2024, Gartner predicts that **75% of the world's population** will have its personal data covered under **modern privacy regulations**.

But, if you're still debating whether your business needs a cybersecurity program in place, consider this: Which situation is more fiscally sound? 1) Budgeting for cybersecurity and knowing how much you're spending each year or 2) suffering a breach and paying the price for years to come? Keep in mind that there are a multitude of expenses associated with a cyber breach and they can vary widely: from the direct costs – lost business, lost reputation, operational disruption, a ransom (if your company decided to pay) – to indirect costs like forensics, public relations and crisis response, legal counsel, customer notifications, and credit monitoring for affected customers.

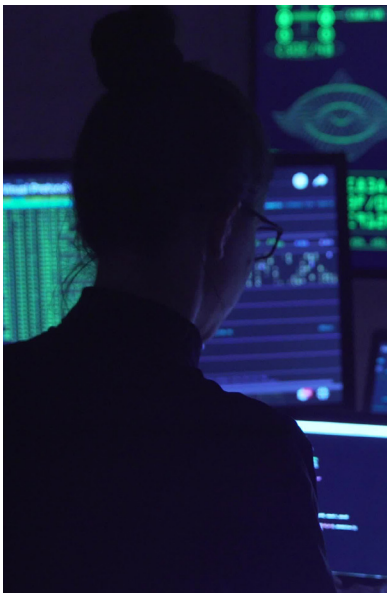
Additionally, since the number of cyber breaches continues to grow, so does the number of regulations – even for non-regulated industries – aimed at protecting online and data privacy. Many states in the U.S. already passed consumer data privacy legislation. And by year-end 2024, Gartner predicts that 75% of the world's population will have its personal data covered under modern privacy regulations. Most of these regulations require (or likely will require) an organization to have an established IRP and perform tabletop exercises.

What if I don't have an incident response plan?

An IRP specifies a predefined, repeatable methodology, which defines the roles and responsibilities when dealing with a security incident and the process to be followed. The IRP is where many key details are located, including who is responsible for updating it, who has authority to enact it, and who has critical roles making up the IRT.

While it is most beneficial to conduct testing only once an IRP has been established, trainings and high-level walkthroughs around incidents and how your organization might respond can help you build out an IRP.

Establishing and implementing even a basic plan can be beneficial to your organization, with a goal of maturing it over time. This can be done internally by organization personnel with the appropriate knowledge of the environment, risks, response processes, and who



For immediate assistance, call Avalon's Incident Response Team at: **877.216.2511**

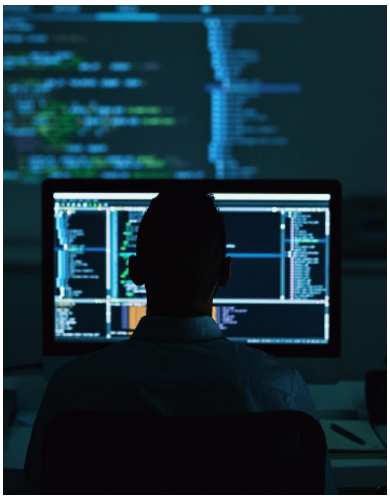
should be involved. Another option is using a third-party provider to help work out these details with your organization and develop the appropriate documentation and possible supporting documentation (e.g., policies, playbooks, etc.) needed to be more readily prepared when an event occurs.

Why use an outside vendor for tabletop exercises?

The benefits of using an experienced cybersecurity team, like Avalon, to lead your tabletop exercise include:

- Saving time and money by letting our team prepare and direct the exercise while you focus on your daily responsibilities
- Learning from our industry expertise and experiences with other organizations
- Receiving tailored scenarios that include the most relevant industry topics and incidents for your organization
- Having outside facilitation helps ensure group participation and communication, all at an efficient pace
- Achieving third-party validation of your plan efficacy and testing
- Obtaining documented methodology, results, and recommendations based on lessons learned

So, whether you carry out a tabletop exercise internally or hire a vendor to assist you, scheduling these exercises on a regular basis ensures your team keeps the policies and procedures top of mind and continues to learn about and improve upon your IRP.



About Avalon

With cyber threats rising in both volume and sophistication, you require a battle-tested cybersecurity team to help defend your organization against adversaries. As a full-service MSSP, Avalon offers security assessments, system and network monitoring, and proactive and reactive cyber services, including vulnerability assessments, penetration tests, digital forensics, and incident response, and we can assist you in constructing a highly resistant cyber program.

Our expertise stems from performing complex cyber investigations around the globe, identifying security program strengths and deficiencies within organizations. This experience has positioned us to assist you in bolstering your information security defense-in-depth strategy while giving you the insight to detect and respond to internal and external threats. Additionally, our offensive security assessments and next-generation system and network monitoring help prevent cyber incidents. Avalon is proud to serve as a trusted resource to businesses seeking a greater level of data security.

To learn more about how Avalon can assist you with tabletop exercises, including developing custom scenarios, facilitating the exercise, and providing a helpful document of lessons learned, contact our experts today.

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

AVALON

www.teamavalon.com

QUESTIONS?

For more information about any of our services or to set up a consultation, contact:

Rebecca Rudell
Marketing Manager
rebecca.rudell@teamavalon.com