Center for Internet Security

CIS releases a list of critical security controls that organizations can implement to protect themselves from cyberattacks. Many organizations follow CIS to enhance their security posture. If your organization does so, it would be worth reviewing Control 17 and, more specifically, section 17.7, which recommends that organizations "plan and conduct routine incident response exercises . . . on an annual basis." While the controls do not specifically indicate that the incident response exercise is a tabletop, CIS has released numerous tabletop exercise templates; search for "tabletop exercises" at *https://www.cisecurity.org*.

Defense Federal Acquisition Regulation Supplement

In 2015, the United States Department of Defense (DoD) published DFARS to protect controlled but unclassified information. DFARS is more of a contract requirement than a standard and is required for any organization that performs business with the DoD, and the necessary controls can be found in NIST SP 800-171. Of note, section 3.6.3 lists tabletop exercises as one means of testing the effectiveness of an organization's incident response.

Fulfill Contractual Requirements

Increasingly, organizations that do business with each other must examine how these business interactions impact their overall cybersecurity risk. Often, one organization grants another limited access to a system so it can perform some service. For example, a manufacturing organization may give a vendor remote access to key manufacturing systems so that the vendor can perform software updates on them. Thus, if a threat actor were to compromise one party in the relationship, the other party that shares system access might also be impacted.

Because of this risk, organizations may insert language into their contracts defining minimum information security standards as well as requirements of either party in the event of a security incident. The contract might require an organization to perform regular tests of an incident response process, including a tabletop exercise. DFARS, mentioned in the previous section, is one example of a contractual requirement that organizations must adhere to if performing services for the DoD.

Another example is the Payment Card Industry Data Security Standard (PCI-DSS), an information security standard required by various credit card brands. PCI-DSS requires merchants who process credit cards to adhere to a set of information security controls designed to minimize the risk posed to the credit card brand. The standard requires that organizations test their incident response plan at least annually.

The tabletop exercise should not, however, become a "check the box" affair item to fulfill a contractual obligation or a regulatory requirement. Attendees should all understand that the tabletop exercise is an opportunity to learn, grow, and prepare for a cybersecurity emergency.

Examine a Recent Cybersecurity Incident

A tabletop exercise based on a recent cybersecurity incident may be an extension of the *lessons learned* stage of the incident response process. This stage can range from hosting an informal discussion to making a formal report and debriefing executive leadership. A tabletop exercise could supplement preexisting lessons learned activities and provide value even if performed several months after the incident.

A "recent cybersecurity incident" doesn't have to mean a catastrophic event that put the organization into a tailspin. Instead, these examinations could explore a simpler incident, such as a well-placed spam email that a user clicked, or an employee installing and using nonapproved cloud storage software to save sensitive information, thereby violating the organization's data practices. These basic incidents may be just as valuable to examine as an incident involving nation-state actors, silent reconnaissance, or a highly advanced piece of zero-day malware.

Because the organization has more context on how an incident occurred, the exercise facilitator could discuss what prompted the user to install the software in the first place (such as a lack of awareness) or whether current security controls are adequate to detect and prevent a similar incident. Cross-functional issues, such as the role of the HR or legal teams, are other notable avenues of exploration.

Finally, when a tabletop exercise scenario is based on what has *actually* happened versus what *could* happen, there's often a greater level of collaboration among participants. They sometimes hesitate to completely buy into a tabletop scenario, thinking, *Could this really happen to us?*, but a cybersecurity incident that really did occur requires no suspension of disbelief.

Identify and Prioritize Risks

Organizations might also want to perform tabletop exercises to rehearse various risk scenarios that may affect them. Of course, in order to do so, they must first understand what the top risks are. It's helpful to have a *risk register*, a tool that identifies and categorizes each risk to the organization and includes information like type of risk, description, probability, priority, and mitigation response.

Included on this risk register should be risks that could affect the confidentiality, availability, or integrity of the organization's data. These might include ransomware, malware, denial of service, lost or stolen laptops, business email compromise, and credential theft, among others. If you're unsure of the risks affecting your organization, consider networking with industry peers and reviewing current threats to your industry vertical. Risks affecting a health system will be very different from those affecting a manufacturing plant.

With risks defined, you can then select one (or more) to focus on during the tabletop exercise. Approaches to selecting a risk may vary; some teams prioritize the highest risk to the organization, while others spend time exploring unfamiliar threats or risks that represent the technical

team's largest weakness. Next, include the appropriate team members in the exercise; we'll offer guidance on this step in Chapter 2.

Tabletop exercises can also uncover new risks to the organization. Any new risks should be properly documented, reviewed, and prioritized during the evaluation stage of the exercise (discussed in Chapter 5).

Advantages of Tabletops over Other Security Exercises

Tabletop exercises are just one way to train staff, assess residual risk after an incident, and refine processes. An organization could also hire red teams to actively probe systems for vulnerabilities or perform classroom-oriented security awareness training, for example. But tabletop exercises do provide a few advantages over other training and testing formats.

Low Cost and High Return on Investment

Tabletop exercises are an extremely cost-effective way to explore an organization's plans, policies, and procedures. Additionally, they ensure that employees understand the processes they must follow in the event of a cybersecurity incident. Unlike some security exercises (for example, red teaming), a tabletop exercise requires no additional equipment beyond the standard office suite of tools, a conference room, and a projector. You won't need technical resources the way you would in a hands-on exercise, only employees' time.

Even with its low overhead, the return on investment from a tabletop exercise can be significant. Consider the value of these lessons learned from tabletop exercises:

- In discussing a scenario involving the compromise of social media accounts, you discover that the social media accounts followed by thousands of customers use a password shared by multiple employees and lack multifactor authentication: two compounding security failures.
- During a ransomware-themed tabletop exercise in which the organization decides to pay a ransom, you determine that the organization lacks a method to quickly attain and transfer cryptocurrency. This step alone could add several hours or days to the process, prolonging the incident.
- When discussing how the information security team would analyze a suspicious employee's laptop during an employee misconduct scenario, staff determines that they lack common computer forensic tools needed to preserve the employee's hard drive.

If discovered by a low-cost tabletop exercise and rectified, each of these process deficiencies could mitigate a costly cybersecurity incident or lead to a swifter resolution.

Finally, high-quality tabletop exercise templates are increasingly available for no cost from a variety of reputable sources. CISA (the Cybersecurity & Infrastructure Agency) is just one of many sources that provide free

tabletop exercise templates for organizations wishing to conduct their own internal tabletop exercises (*https://www.cisa.gov/cisa-tabletop-exercise-packages*). We discuss other sources in Chapter 3.

Efficiency

Tabletop exercises offer an additional perk: they let you discuss an incident, from identification to remediation, in a matter of hours. By contrast, operations-based exercises require staff to respond to activities in real time, such as by performing containment measures (like severing network connectivity) and conducting analysis (like investigating logs and artifacts).

According to the European Union Agency for Cybersecurity (better known as ENISA), it takes approximately 206 days to detect a data breach. (You can find its report, titled "ENISA Threat Landscape 2020 - Data Breach," at *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach*.) This is in line with Ponemon and IBM Security's finding that, in 2022, it took 207 days to identify a data breach and another 80 days to contain it. A tabletop exercise takes an event that would normally require significant time to identify—and even more time to resolve—and compresses the discussion down to a few hours. When a discussion point is brought up that may require hours or days of work, the facilitator of the exercise can artificially "move the clock ahead" and provide the next block of information to consider, filling in any information gaps. We discuss these strategies further in Chapter 3.

Tabletop exercises are a compromise to balance the time an employee spends preparing for events and performing their primary job. Requiring key personnel to plan an operations-based exercise and then devote one or more working days to play out the response may not be tenable for many organizations.

No Operational Disruption

Every business has information systems that are key to its operations—for example, medical equipment that monitors patient health, manufacturing equipment whose downtime would result in significant financial loss, and operational technology that controls banks of elevators in a high-rise building.

An obvious benefit of tabletop exercises is that they don't require interacting with critical systems in a way that could impact human safety or cause serious financial harm to the organization. On the other hand, even very basic operations-based exercises would involve interacting with critical information systems. In some cases, this might be too risky or downright irresponsible.

Tabletop exercises enable experts on critical systems to discuss hypothetical cybersecurity incidents without actually interacting with those systems. This discussion allows them to better identify weaknesses that may cause a cybersecurity incident, potential containment and analysis strategies, and the implications of an incident.

CASE STUDY: SAFELY TESTING MANUFACTURING SYSTEMS

The new director of information security at Pacific Baby Formula, a nutrition company that makes infant formulas, wanted to test the organization's ability to respond to a security event involving its manufacturing systems. However, the chief risk officer informed him that they couldn't perform penetration tests on the manufacturing lines due to strict quality controls and safety concerns.

He struck a compromise: instead of actively testing the manufacturing infrastructure, he used a tabletop exercise to explore how a cybersecurity incident involving those systems might play out. The premise of the exercise was that a contractor had accidently introduced malware into the environment while servicing those systems. The malware, which was nothing more than a cryptocurrency miner, impacted multiple manufacturing systems by consuming processing power. To contain the incident, parts of the manufacturing pipeline were shut down.

The tabletop exercise revealed several deficiencies in the company's ability to identify and respond to a cybersecurity incident:

- Several operational technology devices weren't monitored for potentially malicious software.
- IT contractors regularly updated the software for certain specialty manufacturing equipment, and the process to verify IT contractors' software patches had gaps that would have allowed malicious software to enter the environment.
- The team maintaining the manufacturing plant operations would not have notified the information security team in a timely manner because the teams had different standards for what constituted a security incident.
- If impacted by malware, certain manufacturing systems would have taken days to service, creating an unacceptable period of downtime.

Each of these issues had the potential to cause a cybersecurity incident or stifle its response; if combined, they could be catastrophic. Even without hands-on testing, the tabletop yielded significant findings.

What Tabletop Exercises Can Test

Because tabletop exercises require minimal infrastructure, there are few limitations to what they can test. In discussion-based exercises, you might begin by focusing on technical controls, only for other issues (such as problems with a vendor contract) to emerge as a focal point. Even so, organizations often find it beneficial to narrow their focus by digging deep into one topic or focusing on organizational goals (such as reducing risk to a critical system). This section will review a number of common focus areas.

The Potential Impact of Current Threats

You can use tabletop exercises to continually explore the cybersecurity threat landscape and how it applies to your organization. It's no secret that the threat landscape evolves frequently—consider just a few events over the past several decades:

The Morris Worm (1988)

This self-replicating piece of code created by Robert Morris caused the early internet to come crashing to a halt, highlighting the vulnerabilities of information systems.

Distributed denial-of-service (DDoS) attacks (2000)

Fifteen-year-old Michael Calce managed to take several websites offline, including Yahoo!, Amazon.com, and eBay, causing cyberattacks to enter the mainstream conversation.

Stuxnet (2010)

This worm, which targeted Iranian centrifuges responsible for enriching uranium, was believed to be a cyberweapon for possible use in a nuclear attack.

The Shamoon virus (2012)

Designed to cause destruction in victim networks by erasing operating systems, this virus greatly impacted Saudi Arabia's state-owned oil company, Saudi Aramco.

Sony Pictures' film *The Interview* (2014)

Angered by this film's portrayal of North Korean leader Kim Jong Un, the North Korea–connected hacker group Guardians of the Peace attacked Sony, stealing and then releasing significant personal information and intellectual property in an attempt to harm the company.

Colonial Pipeline ransomware attack (2021)

This event shut down Colonial Pipeline, which transports almost half the fuel on the East Coast of the United States, causing widespread fuel shortages. Ransomware is the number one threat identified by the ENISA for that reporting period and has been a significant concern for the better part of a decade.

Casino hacks (2023)

This series of cyberattacks leveraged social engineering and other techniques to cause havoc for the Caesars and MGM casinos. According to an MGM Resorts International regulatory filing, it caused an approximate loss of $100 million due to interruptions in revenue, remediation efforts, and other factors.

As highlighted in these examples, the threat landscape has evolved from relatively simple attacks impacting availability to more purposeful attacks aimed at stealing intellectual property or for financial gain. Threat

landscapes change because threat actors—whether individuals, groups, or nation-states—have unique motivations that also evolve. Factors completely independent of traditional cybersecurity, such as the emergence of new attack vectors or geopolitical issues, can also change the threat landscape, as was the case during the COVID-19 pandemic when many workforces adjusted to working from home.

By performing exercises that take into account the current threat landscape or plausible hypothetical scenarios, organizations can assess whether they have properly prioritized their security investments. For example, an organization involved in critical infrastructure (such as water and electric distribution) would take particular interest in the Colonial Pipeline attack, knowing that attackers are now targeting critical infrastructure. Also, because organizations can perform simplified tabletop exercises on an ad hoc basis with minimal planning, they can relatively easily tailor an exercise topic to a recent news event to assess its impact to the organization.

CASE STUDY: AN AD HOC RESPONSE TO CURRENT EVENTS

Canadian Shield Bank, a regional financial institution in Ontario, Canada, became aware of a spike in smishing attacks targeting the banking industry. *Smishing* is a type of phishing attack that attempts to trick mobile phone users into clicking links sent via SMS. A regional competitor had reported a large number of these texts, which claimed that the victims' checking accounts were overdrawn and prompted them to click a link to avoid overdraft fees.

To supplement its mandated yearly tabletop exercises, Canadian Shield Bank ran an ad hoc tabletop: a quick one-hour discussion over lunch to play out how such an attack would impact the company and what response steps might be required. By all accounts, the tabletop exercise succeeded: Canadian Shield Bank identified a number of process improvements and gaps it had not previously considered, as this was the first time its region had seen such attacks. For example, participants realized they didn't have a method to quickly warn bank customers via the bank app or text messaging.

Going forward, the bank began performing short quarterly tabletop exercises based on changes to the threat landscape and within one week of a unique threat popping up on its radar. Because the tabletop exercise scenarios weren't based on a hypothetical "what if?" and took few creative liberties, participants were far more likely to think critically about how the incident would play out at the company.

The Sufficiency of the Information Security Budget

When information security teams want to implement a certain technology, develop a product, or add head count to the team, they usually must make

a business case for the added cost. One way to use tabletop exercises is to explore an already known risk in an effort to raise awareness of it and form a coalition that supports dedicating resources to mitigating it.

For example, if an information security manager recognizes that the current budget to maintain and store logs is inadequate, the tabletop can weave in a component that highlights the logging deficiency and its potential impact on a cybersecurity incident. This strategy may work best if the exercise uses an external facilitator to point out the deficiency, as the information security manager may be perceived as biased.

Tabletop exercises are an excellent way to highlight current gaps in the environment because they are flexible and can be built around a known deficiency. The exercise provides a forum for the information security team to demonstrate why an investment is needed and what the costs of inaction would be.

Information Sharing Protocols for IoCs

When responding to an event, the team might want or feel obligated to share *indicators of compromise (IoC)* with other entities. IoCs are artifacts unique to the cybersecurity incident that are identified on devices in the organization's network and, if observed elsewhere, may indicate another cybersecurity incident. IoCs could include firewall logs showing that a system beaconed out to a suspicious network address, unique registry changes on an operating system, or characteristics of possible malicious files.

IoCs are extremely valuable, as they may be the first digital breadcrumbs available to identify how far an incident has spread. Some organizations are contractually obligated to share these details, or they may do so for altruistic reasons to allow potentially affected entities to bolster their own defenses against a mutual cyber adversary.

Tabletop exercises are an excellent way to discuss how to share information with outside parties. During your exercise, consider exploring the following questions from the Microsoft publication "A Framework for Cybersecurity Information Sharing and Risk Reduction " (*https://www.microsoft.com/en-us/download/details.aspx?id=45516*) when confronting the topic of information sharing:

- Who should share information?
- What should be shared?
- When should it be shared?
- What is the quality and utility of what is shared?
- How should it be shared?
- Why is it being shared?
- What can be done with the information?

Organizations should consider well in advance the nuances of sharing information, such as maintaining confidentiality, while also balancing the interests of other internal stakeholders, particularly the legal team.

Gaps in the Incident Response Plan

One of the most crucial parts of effective incident response is the incident response plan. *Computer Security Incident Handling Guide* (NIST SP 800-61r2) provides excellent guidance on what should be included in this plan. One critical component is a *charter*, which defines what an incident is and includes the mission statement, goals and objectives, and authority of the team. The plan should also define the members of the incident response team, their roles and responsibilities, and the incident severity levels set by the organization. It should spell out an organized incident response approach and communication protocols.

In addition, the plan should designate a specific person to oversee testing (to avoid the diffusion of responsibility) and define a testing frequency; at a minimum, the plan should be tested once a year, and ideally twice a year. Testing the plan using an exercise allows the team to collaborate in an organized manner to resolve the incident, learn from one another, and potentially find gaps in the plan itself.

Even in the best-written incident response plan, tabletop exercises often uncover areas for improvement. Take time during the tabletop to document these gaps so the plan can be updated accordingly. You want to find the weaknesses during these exercises—not in the heat of a real incident.

The Efficacy of Processes and Procedures

Some organizations have predefined plans to respond to specific types of cybersecurity incidents. In addition to the incident response plan, you might want to validate the following:

- Playbooks that address a certain type of cybersecurity event or incident, such as ransomware; these playbooks provide in-depth guidance and thus require investments to keep up to date
- Incident escalation paths, which ensure that relevant members of technical and strategic teams are notified at the appropriate time via a predefined communications channel
- Incident identification and notification procedures, which help the organization identify an incident at all levels and notify relevant parties
- Containment procedures, which dictate how to execute containment efforts in tandem with business continuity plans
- External party notifications, such as required communications to government entities

A tabletop exercise doesn't necessarily need to validate all processes and procedures. Instead, it could home in on a single item of concern, such as a recently updated process or a change to the organization that has the potential to impact incident response efforts.

Compliance with Notification Requirements

Of particular salience, a tabletop provides a low-stress environment to evaluate the requirements related to notifying external parties. You've likely had the unpleasant experience of receiving a data breach notification letter from a financial institution, healthcare provider, or other business. That organization probably sent the letter to comply with a breach notification obligation.

Since the early 2000s, laws have imposed specific requirements for notifying consumers of the loss of protected data. In the United States, California pioneered data breach notification laws in 2002, and all 50 states now have their own variations. In the European Union, the GDPR legislation codifies, among other things, data breach notification rules. Other countries have followed suit, including Australia, China, and Barbados (as noted earlier in the chapter).

However, each data breach law defines sensitive data sets differently and outlines its own notification process. Perhaps most importantly, some define slightly different temporal requirements and thresholds at which a notification is required. For example, one data breach law may require notification to an authority within 72 hours of a *suspected* compromise of a data set, while another may allow seven business days for a *confirmed* compromise.

These data breach laws can quickly become cumbersome in even a simple cybersecurity incident. Consider the fictitious Executive Travel Experience (ETE), a publicly traded travel agency whose client list represents citizens from almost every US state, most Canadian provinces, several European countries, and a few Middle Eastern and Southeast Asian countries. Say ETE's information security team believes the threat actors may have had access to client data as well as employee data, including health plan information. ETE's employee base is mostly located in Chicago but has strategic account managers throughout the world.

Addressing the legal component of this relatively common scenario can become a beast in itself. ETE's legal team needs to consider, at a minimum:

- The nuances of data breach laws relating to almost every US state, Canadian province, and other impacted countries
- Notification requirements for each customer whose data was stolen
- In cases when the data involved was owned by a vendor and ETE had contractual requirements to safeguard it, whether ETE must notify the vendor
- Because ETE's health plan information was likely accessed, whether ETE must notify the United States Department of Health and Human Services, which administers the Health Insurance Portability and Accountability Act (HIPPA)
- Does the incident meet materiality, thus requiring ETE—as a publicly traded US company—to file SEC Form 8-K to notify investors ?

In addition, for each of these questions, ETE must consider temporal requirements for performing the notification. As you can see, a cybersecurity

incident could easily balloon into a myriad of downstream tasks. A tabletop exercise allows you to identify and explore these tasks in a low-stress setting.

Business contracts with other organizations might also outline notification requirements. For example, they may stipulate that you must issue a notification if a specific data set is lost. Finally, consider whether you have an ethical or moral responsibility to notify impacted individuals or organizations, even if the incident doesn't meet a legislative or contractual bar. While these ethical guidelines are less black-and-white than legal requirements, organizations should still assess them when determining whom to notify during a tabletop exercise.

Residual Risk after Corrective Actions

After most cybersecurity incidents, an organization will examine the factors that caused or contributed to the incident, such as a failure of technical controls, policies, or end user education. Once it identifies these factors, the organization may make changes or technology investments to reduce the risk of recurrence. At this stage, performing a tabletop exercise can enable stakeholders to run through a similar cybersecurity incident and discuss those corrective measures. This step functions as an additional check to identify residual risk as well as another opportunity to fully assess the downstream impact of any changes.

Summary

In this chapter, we've discussed many of the common reasons organizations choose to perform tabletop exercises. Tabletops have quantifiable benefits, such as monetary savings during a data breach, as well as more qualitative ones, such as improved relationships among response team members. Your organization may want to perform a tabletop exercise for reasons that aren't listed in this chapter, but what matters most is that you understand and align with its goals when starting your tabletop exercise journey.

Questions

As you begin planning an upcoming tabletop exercise, take the time to contemplate the following questions (some may have readily apparent answers, while others may require investigation):

1. In performing a tabletop exercise, are there specific conditions (such as contractual or regulatory requirements) you must meet?
2. What are the intended primary and ancillary benefits of performing a tabletop exercise in your organization?
3. What lessons would you like to learn by performing a tabletop exercise?
4. What people, process, or technology factors would you like the tabletop exercise to test?