Harvard Business Review

Technology

Cyberattacks Are Inevitable. Is Your Company Prepared?

by Keri Pearlson, Brett Thorson, Stuart Madnick, and Michael Coden

March 09, 2021

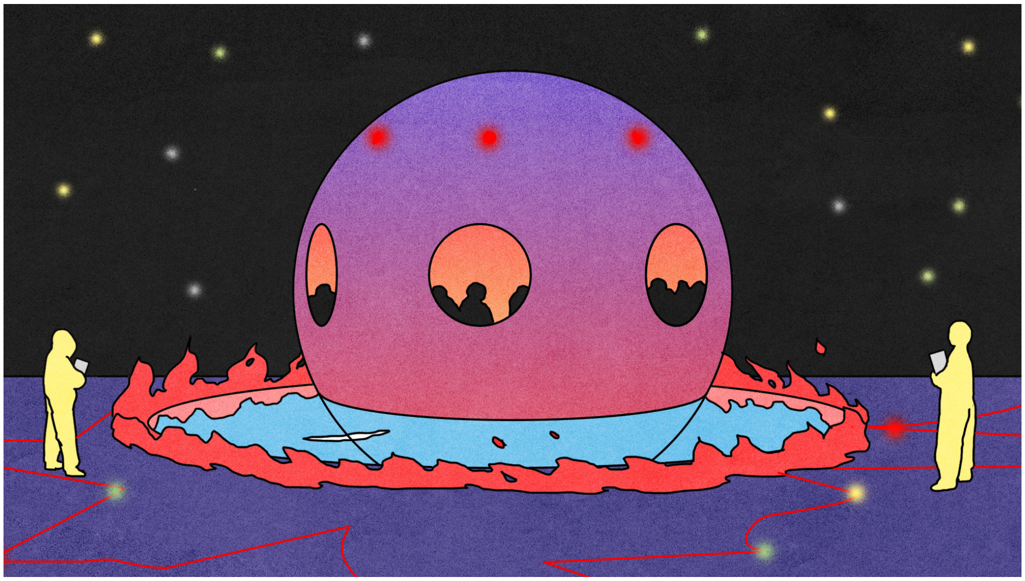

Illustration by María Medem

Summary. Preparing for the unexpected is much easier said than done. In the case of cyberattacks, many companies have vulnerabilities in their defenses and reactions they haven't prepared for that hackers will test. Many organizations can benefit from instituting fire drills and tabletop exercises, which test a company's response plan at every level. These exercises will almost certainly reveal gaps in security, response plans, and employees' familiarity with their own roles. While

investing in external facilitators for these exercises will often allow for a more rigorous test separate from internal dynamics, there is guidance for organizations who wish to execute internal exercises to better prepare for a cyberattack. **close**

Cyberattacks always happen when you least expect them. And when they happen, they happen quickly. Responding appropriately is not just the responsibility of your cybersecurity team; everyone in the organization has a role to play. Is your team prepared? Do they know what to do and what not to do? Most importantly, has your whole team practiced their response? Everyone — the board of directors, company executives, managers, and team members — has to know their roles and responsibilities and work out any potential problems with their response before a live cyberattack puts immense stress on the organization.

There's an easy way to determine whether your incident response plan (IRP) works and whether your team knows their roles: a test. Yet a Ponemon survey determined that 47% of organizations have not assessed the readiness of their incident response teams, meaning that the first time they test their plans will be at the worst possible time — in the middle of a cyberattack. Hackers constantly and consistently test your defenses and reactions. You must do the same.

In our work helping organizations — both public and private, large and small, domestic and international — plan for cyberattacks, we've found that fire drills and table top exercises (TTXs) are a great way to prepare for the worst.

Fire Drills and Table Top Exercises

Think of an emergency room scenario following a car accident. When seriously injured patients arrive, the ER staff has to know exactly what to do and how to do it. They cannot be learning at the same time the crisis is happening. The same goes for C-suite executives and top management. To make sure they are aligned and aware of company plans during a cyberattack, they need to practice ahead of time and build muscle memory in how to respond. Simulated scenarios help organizations to validate their plans and prepare company leaders.

An effective engagement takes a few weeks of planning, and works best when realistic situations and scenarios are used. We usually create videos simulating the company being criticized on the evening news, have journalists show up and demand to interview the CEO, or interrupt a press conference to ask about the cyberattack. We have simulated dark websites where executives can see their most valuable intellectual property being auctioned to the highest bidder, and their stock price dropping like a rock.

The first step is to make sure there are clear learning objectives and to determine which cyberattack consequences will have a serious negative impact to the organization. Fire drills and TTXs help organizations identify vulnerabilities and risks that need to be addressed, demonstrate to the organization the magnitude of the risk and the importance of security resources and investment, and test plans in a way that helps everyone be ready. It's almost a certainty that something unanticipated will occur. Knowing what to do helps executives respond when the unexpected actually happens.

Each test serves a different purpose. TTXs are occasional and test managerial capability and team-level response; fire drills are regular exercises that test people, processes, and technologies to make sure they respond appropriately and that there are contingency plans in place in the event that first-line responses don't work. If the digital systems that support the organization are compromised, it is critical to have alternative communication plans, operational plans, back ups, and emergency resources identified that can back-fill until normal processes and systems can be restored. Without these tests, companies are left vulnerable to whatever might be thought of in the moment when their main systems are compromised, and that can result in major business disruption such as was experienced recently by Santander Bank, the City of Baltimore, and just recently, the U.S. Treasury.

The 4 Most Effective Fire Drills and TTXs

So where should you start? It depends on who and what you want to test. We have found four types of fire drills and table top exercises to be the most effective.

Target audience	**Type and objective of exercise**	**Motivation**	**Approximate length of exercise**
Board of directors	TTX: education and awareness	Boards need to know what the company will do in the event of a cyber emergency.	1–2 hours
C-suite	TTX: crisis management	C-level executives need to have plans for crisis management so that they know immediately what to do and whom to contact.	2–4 hours
Organization	Fire drill: test and practice incident response and business continuity plans	Detailed drills build organizational confidence and strength to respond quickly and effectively throughout the company. Especially useful for the cybercrisis management team.	A few hours to multiple days

Technical team	Fire drill: technical response planning	Testing on a regular basis ensures that detection systems, technology backups, and contingency plans are in place and working and that the tech team knows what to do and how to do it.	Continuous, with a full fire drill at least quarterly

Each approach listed above tests a different part of a company’s plans. A TTX for your C-level team will help them practice the current company response plan and test alternative contingencies should the unexpected happen. A TTX for your board provides a similar opportunity. Ultimately TTXs and fire drills drive awareness and build values, attitudes, and beliefs around the importance of everyone participating in keeping the organization secure. Importantly, each test helps companies find out what about their plan *isn’t* going to work — and gives them time to fix it before they need to put it into action.

What Your Organization Will Likely Discover

A good TTX immerses participants in a cyberattack so they can feel the effects of the decisions they make and the effectiveness of the company plans. Most organizations discover something about their plans that previously had not been obvious, such as:

Flawed and unmanageable plans: One manufacturing company realized their incident response plan was 400 pages long and no one had ever read it. When your shareholders and the press are clogging your switchboard asking for information, your employees are not sure what to do, and the cybercriminal is exfiltrating gigabytes of data or encrypting your computers so the employees cannot work, that is not the time for each executive to read a 400 page document — of which only 5-6 pages may apply to them — to determine what actions to take.

Knowing who to call: In another exercise, the first line solution to the crisis was that "someone will call Pat who will handle that by checking this software." However, only one person knew Pat, Pat didn't know it was their responsibility, and the software didn't really work as the person assumed. It's this level of detail that maximizes the value of the exercise.

New unanticipated risks: At other times, these tests can make companies aware of risks they had never considered — let alone planned for. In 2018, we conducted several TTXs where the scenario included several physical locations of an organization being uninhabitable, and the organization had to move to an all-work-from-home scenario. We unwittingly prepared these organizations for the reality of the current Covid-19 situation (though some at the time didn't believe there was a situation in which this could occur).

Impacts beyond business continuity: A TTX is a useful tool to highlight impacts beyond business continuity. In a very large financial institution, we created an exercise with a scenario that caused customers to lose confidence in doing business with the organization. One of the C-suite executives stopped the exercise in the middle and responded, "You realize that he [the TTX facilitator pretending to be a cyber criminal] just destroyed our company with one plausible scenario! We need to invest more in cybersecurity."

Motivation to invest in cybersecurity: In a recent study by Osterman Research, 45% of respondents said that following a TTX, they were able to increase their security budgets. Most of this budget was spent on procuring additional solutions and training their workforce. This same study highlighted that 78% of cybersecurity professionals believed that their TTXs and fire drills had better prepared their organizations to respond to future cyber threats.

What Should Your Organization Do Next?

Using an external source to create and conduct a fire drill or TTX can increase the benefits. Internally designed exercises often lack the level of surprise and unexpected scenarios and interventions. After creating the response plans, internal team members have a difficult time envisioning something unexpected. Further, team members may have difficulty challenging their peers and senior executives, resulting in groupthink or letting the team off the hook rather than challenging their responses and ideas. External leaders don't have the same assumptions and don't come to the table with the organization's institutional memory and habits. Pressing for details and discovering flaws in plans can be career limiting for an insider, but it's expected and necessary for an effective exercise.

That said, while there are benefits to bringing in outsiders (and we'd argue that it's worth the cost), companies can organize these tests on their own. Here are a few best practices for creating and conducting your own exercises:

1. **Get the right people in the room.** Schedule sessions far in advance and let the executives know they are mandatory. Getting everyone in the same room or Zoom call for the same 2-4 hours can be challenging.
2. **Build a likely scenario timeline for your organization and share information carefully.** Pick a cyberattack that seems plausible for your type of organization, since an exercise close to a real situation your team might encounter will be more engaging. Decide if the cyberattack will take place over hours, days, or weeks, and make sure you communicate how you may be speeding time up during the exercise. Real attacks happen over time, so the unfolding of events is important to the exercise. At each point on the timeline, the participants must make the best decision they can with the information they have. Do not give the participants all the information they would like to have at any given time. This helps them to realize what they need to know in a real incident.

3. **Create the scenario so every member of the team has a role to play.** It's very easy to tell someone else what they should do, but sometimes it's hard to hear or think up what you should do. Response plans often have activities for specific roles (what the CEO should do, what the CIO should do, what the CHRO role should do, etc.). If possible, share the full organizational response plan with the team ahead of time so they know it exists (and hopefully they read it). Create an abbreviated version, customized for each participant, that contains only that participant's roles and responsibilities to help them be as prepared as possible.
4. **Discuss action plans at each pause of the timeline**. After telling the participants a piece of the scenario, give them a chance to discuss what they would suggest doing. Ask them if what they are doing conforms to the company incident response plan or if they are improvising. If they are improvising — is it because the plan is not satisfactory and should be improved? Be sure to have someone taking notes so ideas from these discussions are not lost.
5. **Practice before the full team exercise**. The best exercises have been well thought out and test the organization's current response plans and improvisions. Prepare for this by running a short practice TTX one-on-one with each executive in the privacy of their office or a private call. Walk them through their role as described in the current response plan. This will avoid a situation where an executive does not participate in the group exercise because they are afraid to embarrass themselves. While this can be a powerful force for change, it often backfires and results in finger-pointing, leaving the room, or other emotionally-charged behavior.

Companies who conduct fire drills and table top exercises report that they are both better prepared for a cyber crisis and more cohesive as a team in the face of an emergency. The cost benefit of TTX can be realized quickly — and the result is an increase in the agility and quality of a response which could reduce the financial impact to an organization by millions. It's time to schedule your team's practice sessions.

Acknowledgement: This research was supported, in part, by funds from the Cybersecurity at MIT Sloan (CAMS) consortium at MIT's Sloan School and Boston Consulting Group. All authors contributed equally.

Keri Pearlson is the Executive Director of CAMS, a cybersecurity research group at MIT Sloan School.

Brett Thorson is a CyberSecurity Senior Manager at BCG Platinion at the Boston Consulting Group.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. He has been active in the cybersecurity field since co-authoring the book *Computer Security* in 1979.

Michael Coden is the Managing Director, Global Leader Cybersecurity Practice at BCG Platinion at the Boston Consulting Group.