Preparing for Cyber Breaches with Fire Drills and Table Top Exercises

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

(Submitted to Harvard Business Review)
February 7, 2021

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? You don't want the first time they take action to be in response to a real crisis. You want everyone — the board of directors, company executives, managers, and team members — to know their roles and responsibilities and to have worked 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: 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 cyber attack. 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 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 those seriously injured arrive at the emergency room, everyone has to know exactly what to do, how to do it, and remove any bystanders getting in the way. They cannot be learning at the same time the crisis is happening. For the entire C-Suite and top management, that learning should be practiced in fire drills and table top exercises (TTXs) to make sure executives are aligned and aware of company plans.

These are simulated cyberattack scenarios that help organizations validate their plans and help the C-Suite and top management build "response muscle memory." An effective engagement takes a few weeks of planning and is much more effective when realistic situations and scenarios ~~a~~re 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 fire drills and TTXs, 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 US Treasury.

We have found four types of fire drills and TTXs to be the most effective.

Target Audience	**Objective of Exercise**	**Motivation**	**Approx. 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 they know immediately what to do and who to contact	2-4 hours
Organization Fire Drills	Test response plans and practice processes and roles	Detailed drills that build confidence and strength to respond quickly and effectively at operations levels within the organization	Few hours to multiple days
Technical Team Fire Drills	Technical response planning	Testing on a regular basis that detection systems, technology back ups, and contingency plans are in place and working and that tech team knows what to do and how to do it.	Continuous with full fire drill at least quarterly

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; it will help your board be aligned with company plans. Ultimately TTX and fire drills drive awareness and build values, attitudes and beliefs around the importance of everyone participating in keeping the organization secure.

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. One manufacturing company realized their incident response plan was 400 pages long and therefore no one had ever read it. 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.

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.)

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 faciliatator] just destroyed our company with one plausible scenario! We need to invest more 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 TTX and fire drills had better prepared their organizations to respond to future cyber threats.

TTX and fire drills create stronger teams. In one financial firm, the fire drill included a failure of their email and phone systems. The chief counsel was the only person capable of communicating with the rest of the team because she had printed out the response plan and brought it with her, making her the de-facto expert on her organization's next steps. The result was a stronger connection between the participating executives who learned they could rely on each other in new ways.

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 group think 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 'tribal knowledge'. 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.

What Should Your Organzation Do Next?

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. The costs to run multiple TTXs is typically less than $200,000 per year, 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.

ABOUT THE AUTHORS:

Dr. Keri Pearlson is the Executive Director of CAMS, a cybersecurity research group at MIT Sloan School.
Brett Thorson is a CyberSecurity Senior Manager at the Boston Consulting Group - Platinion.
Michael Coden is the Managing Director, Global Leader Cybersecurity Practice at BCG Platinion at the Boston Consulting Group.
Dr. Stuart Madnick is the founding Director of CAMS and the John Norris Maguire Professor of Information Technologies, Sloan School of Management & Professor of Engineering Systems, School of Engineering.