Cybersecurity Law Report
An Acuris company
cslawreport.com

October 7, 2020

BENCHMARKING

Tips and New Benchmarks for Creating Effective Tabletop Exercises

By Matt Fleischer-Black, *Cybersecurity Law Report*

Are your company's tabletop exercises a good fit for today's cyber threat landscape? A survey conducted by Osterman Research (Survey) found that more than half of companies' exercises addressed ransomware and data breaches, although organizations reported scenarios involving many other threats, including insider and remote work incidents, said the Survey's author, Michael Osterman.

The pandemic has caused an uptick in tabletop exercises. The Survey shows that, by July 2020, 63% of companies already had conducted one exercise this year, despite a lull in exercises initially after the lockdown. Some companies likely "moved up the schedule on exercises to start considering the relatively new scenarios," Osterman told the Cybersecurity Law Report.

In another sign of the pandemic's impact on tabletop exercises, the Survey showed that three of four recent exercises evaluated business continuity.

The trans-Atlantic survey report included responses from company security leaders involved with tabletop exercises at 402 organizations. These companies had a mean headcount of 1,897 employees. The organizations' headquarters were evenly split between the U.S. and the U.K. This article discusses the results and takeaways from the Survey with Osterman, who conducted the survey, and lawyers from King & Spalding, Latham & Watkins and Shearman & Sterling.

See "Strategies and Tactics for Developing an Effective Tabletop Exercise (Part One of Two)" (Sep. 18, 2019); Part Two (Sep. 25, 2019).

Pandemic Scenarios

According to the Survey, companies focused primarily on exercises involving data breach and ransomware, at 59% and 57%, respectively. Spear phishing scenarios appeared in 45% of tabletop exercises, zero-day attacks in 41%, and insider threats in 33%. Companies reported using "other" scenarios in 51% of exercises. "We heard 50 different ones overall: malware infections, DDoS (denial of service), SQL injection attacks, cloud compromises, crisis management," Osterman said.

"The pandemic is affecting the scenarios directly and indirectly, he added. "With a lot of phishing attacks and ransomware exercises, you are still talking about COVID," Osterman observed.

Companies recently have wanted to test how to gather incident response teams virtually, said King & Spalding partner Phyllis Sumner. "We have been encouraging our clients to do

©2020 Cybersecurity Law Report. All rights reserved.

tabletops during the pandemic because they do not have the usual capability to establish a war room and collect decision makers all together," she reported. These exercises ensure company leaders "can communicate safely and securely and are able to interact in an organized way to make critical decisions," she noted.

Companies have been introducing realistic COVID-19 scenarios both "to test the ability to respond, and to raise awareness within the organization about how to deal with them," Sumner continued. Companies are mirroring the surge in ransomware and ransomed denial of service (RDOS) attacks in their exercises, she added.

See "Re-Evaluating Cybersecurity in the Remote Work Environment" (Jun. 3, 2020).

Business Concerns and Vendor Relations

Survey respondents indicated that 75% of the tabletop exercises addressed business continuity operations following incidents, while 47% considered impact on brand reputation. The organization's liquidity garnered attention in 27% of surveyed companies, while 24% of them considered the share price.

Vendor relations are more frequently arising in tabletop exercises, said Shearman and Sterling partner Emma Maconick. Incidents frequently happen through a company's vendors. Companies use an average of a 1,935 cloud apps, with 21% of their cloud data containing sensitive information, according to a 2019 McAfee cloud risk survey.

Companies should try to include managed service providers in their tabletop exercises, even if difficult during the pandemic, Maconick said, "especially when they are custodians of a lot of sensitive data. We see vendors in exercises in health care, in financial services and the sectors that touch on children, whether education or media."

Data governance and regulatory risks are other concerns regularly considered in tabletop exercises, Maconick added.

See "The Ongoing Complexity of Vendor Risk: Top 5 Considerations for C-Level Leaders" (Mar. 18, 2020).

Exercise Goals

Companies reported that they intend their exercises to identify vulnerabilities or risks that need further attention. Mentioned by 41% of respondents, this suggests a clear emphasis on testing process over training people. Far less frequently, respondents said exercises were meant to validate the incident response plan (16%), demonstrate security resources (16%), stress test human cyber readiness (15%) and meet regulatory requirements (12%).

In practice, Osterman said, "people probably view exercises more holistically. For a CISO or a security manager, the purpose may not be all that compartmentalized. When the exercise is looking for vulnerabilities, it is also in part to validate the incident response plan and evaluate how good are the security elements in the infrastructure."

The Survey likely captured tabletop exercises that IT departments conduct to satisfy a line item in a written information security management program, said Latham & Watkins

©2020 Cybersecurity Law Report. All rights reserved.

partner Jennifer Archie. "The CISOs will assign that to an engineer, who gets the functional leads in key technical areas together for a tabletop" that may run an hour, Archie explained. "The enterprise crisis management tabletops are more rare," and usually run for three or four hours, she noted.

The tabletop-exercise practice is shifting, Sumner said, and companies now run more full-company crisis exercises "that test the human component and the full incident response plan and use it as a learning exercise for all the different stakeholders."

The costs of tabletop exercises are varied, the Survey found, with two in five costing between $30,000 and $50,000, while another two in five cost under $30,000. Another 18% cost between $50,000 and $80,000. A few cost more.

Frequency

The top preference among surveyed companies, at 29%, is to schedule one tabletop exercise each year. Another 23% do not schedule them at all. "For some very mature companies, not scheduling tabletops is common, more common than you might expect," said Archie.

Many cyber insurance policies now mandate at least an annual tabletop exercise, noted Archie. Law firms and forensic contractors typically offer client companies a free tabletop exercise when they sign retainers, she noted. Thus, a simpler explanation for this summer's apparent uptick in exercises is that companies that postponed tabletops during the initial pandemic lockout were moving to claim this contractual benefit.

Despite the current percolation of threats, only 36% of companies schedule an exercise to occur every six months, quarter, or month, according to Osterman's Survey. "We will see more interest in tabletop exercises to explore the ramifications of how we are dealing with" what promises to be an erratic distribution between remote and office work, said Osterman. As of mid-September, remote work in the U.S. had dropped to 51% from an April high of 80%, according to Osterman's research for another report. With so much shifting, "security is being reconsidered in many ways," including exercise frequency, he added.

Companies that have already suffered a breach may need to do tabletop exercises under consent decrees and settlements, Sumner noted. Archie observed that "a very large retailer that has suffered a significant breach might do it quarterly."

Maconick recommended running a smaller crisis tabletop exercise every three months, using different scenarios. Participants "need to go through several, at least two a year, to get to a stage where they have muscle memory" during the response, she said. Mature organizations may want only a semi-annual or annual general crisis exercise, but it is beneficial each quarter for teams do their own run-through as a team-building experience, Maconick added.

See "Tips From Ponemon/Experian Survey on Building an Incident Response Plan That Fosters Confidence" (Feb. 26, 2020).

Who Participates?

Many companies, 59%, include more than 11 participants in exercises, while 37% involved 5 to 10 people, the Survey found.

©2020 Cybersecurity Law Report. All rights reserved.

Small Enough for Involvement and Learning

Maconick most often sees 12 to 15 participants, with exercises topping out at 20. "These are really effective between 8 and 12 people," she noted, adding that any larger can stir up notable "group dynamics, where you see the psychology of tribes and alpha personalities emerge." The 5 to 12 range is preferable even for larger companies, she added.

Some organizations, Sumner said, opt "to keep the exercise roundtable focused, with a smaller, higher-level executive group." Those groups may "want others in the organization to observe and understand the process," and will hold "sessions in large training rooms with the incident response team up front, but up to 50 people being involved."

To share lessons from the tabletop, Maconick recommended that leaders "video the exercise in an unobtrusive way" with the small group, then have the participants conduct a post-mortem with a broader team.

Some business sectors run larger tabletop exercises, Archie noted. "For hospital and financial institutions that are highly regulated, with everything on the line, it's common to have dozens and dozens of people participating in separate rooms," she said. "One exercise with 100 people turned out especially well because each room had only 5 to 10 people in it. They only knew what we told them in that room, which gave them a true experience. In a large incident, that separation between teams is very real."

See "How Asset Managers and Others Can Mitigate Pandemic-Related Operational Risks and Maintain Business Continuity" (May 6, 2020).

Cross-Functional Teams for Managing a Crisis

Respondents said that cybersecurity leadership usually attended (76%), followed by the business continuity team (56%), and operational staff (43%). Cyber leaders said less than half the time C-suite executives (41%) legal team (34%) and communications (20%) team attended.

"There is probably a lack of motivation in many organizations for the legal team, communication team, and operational staff to be involved," Osterman said. "A lot of organizations are adding security education for the board but don't look as carefully at security as they should," which "may be reflected in the roles involved in their tabletop exercises. They don't include stakeholders from across the organization when they probably should."

Cybersecurity leaders may resist involving other business functions, Archie noted, because "these CISOs and CIOs face a whole lot of operational tasks to address disruptions" while following the company cybersecurity protocols.

Yet this older impulse does not fit with the latest expectations from regulators, who will "scrutinize management and board oversight and understanding of the company's level of readiness," after any incident, said Sumner. Boards are increasingly focused on participating in tabletop exercises or, at minimum, she said, "getting readouts about the tabletops that are happening. Board members should be discussing with management the expectations around policies for escalation to the board and management."

©2020 Cybersecurity Law Report. All rights reserved.

Rather than participate in a full tabletop, boards often have shorter simulations of one to three hours, said Archie. "The board needs to have a fluency and a literacy around cyber risk management and compliance with laws," to fulfill its role of protecting the company's interests, so at least some modelling of the liabilities and harms is crucial, she added.

See "Getting Board Buy-In for Edge Cybersecurity Initiatives Post COVID-19" (Jul. 8, 2020).

Format and Role Playing

Survey respondents reported that in 61% of tabletop exercises the scenario was altered by participant responses. On average, Osterman said, companies indicated their exercises used at least three different formats per exercise, with PowerPoint leading the way, at 65%. Online systems and videos were common, Osterman said.

Role playing occurred in 44% of the exercises. Archie highlighted its importance for testing the strength of enterprise-wide incident responses. "People learn from needing to speak up and make a decision," she said, noting that determining who the decisionmakers are is an important element of the exercise.

Maconick agreed. "Part of the tabletop exercise is figuring out who really does have the keys to the kingdom. That might not be the head of marketing or the head of investor relations. It might be a specific person within a specific team who really knows where we manage access control" or can quickly achieve other key details for the response tasks.

Maconick noted that "systems, procedures and processes are only ever as good as the employees' skills and how they react in a difficult situation," adding "the human component is the piece that the exercise really tests."

For incident responses, a core learning point arises around the communication, Archie said. It is important to have "the experience of seeing what happens when different people have different information and will try to do their best, but really mess up," said Archie. "It is critical that during an incident that you maintain a single source of truth mentality. You can't have five truths in five different rooms. It does not work because you won't be in lockstep." Instead, route all facts to a central hub, or war room.

See "How to Establish an Efficient Incident Response Plan" (Jul. 17, 2019).

Follow-Up Materials and Actions

More Than Completion Certificates

Exercise organizers reliably produce and deliver materials after tabletop exercises. Only one in nine respondents reported that a run-through created no materials.

The most common supplied material is a list of recommended measures, mentioned by 60% of respondents. Organizers supplied "simulation results" in 44% of the companies, and an equal proportion received a summary of the exercise. Organizers generated personalized guidance in 30% of the companies, while an equivalent number of companies produced certificates.

Business Actions

The most common business response to the tabletop exercises was to increase the security budget (45%). Organizations also procure

©2020 Cybersecurity Law Report. All rights reserved.

additional security solutions (42%), conduct additional training for non-security employees (39%), and update the incident response plan (37%). In the U.K., 41% of companies provided additional security staff training, but only 22% did in the U.S.

The moderators of enterprise-wide crisis tabletop exercises sometimes follow up specifically with each team about issues, Sumner said. The exercise may have shown, for instance, that the company does not have a project manager to organize and track privileged communications about the incident, a legal team concern.

The legal team is a critical decision maker and advisor during the incident, Sumner said, noting that commonly she has highlighted "the importance of the legal and communications teams to coordinate efforts, and not work from separate playbooks."

Enterprise-wide exercises do typically prompt updates to the incident response plan, Sumner added.

Value of Tabletop Exercises

Fifth Most Effective Preparation Method

Most respondents viewed tabletop exercises as a moderate help to prepare for a security incident, although one third of respondents (32%) ranked exercises as highly effective preparation. Views varied notably by continent, as 36% of U.S.-based organizations cited exercises as highly effective, compared to 28% of U.K. companies.

The most effective preparation to handle a security event is having a complete, in-place incident response plan, according to 61% of respondents. That was followed by procurement of security solutions, chosen by 58%. Improving the skills set of individuals and teams was cited by 54% as highly effective.

Having a legal policy in place was deemed slightly more crucial than tabletop exercises, ranked as highly effective by 38%, although U.S. respondents emphasized it more. Only one quarter of respondents deemed having incident response consultants on retainer as highly effective.

Good, Not Great, Preparation for Imminent Attack

Four of five professionals responding (78%) view tabletop exercises as helping prepare their organization for a cyber incident, with 11% disagreeing and another 11% opting not to decide.

Fewer respondents, 62%, believed that the tabletop exercises had left the company's designated responders genuinely ready for an imminent attack. Many professionals, 24%, declined to say.

©2020 Cybersecurity Law Report. All rights reserved.