OLIVER WYMAN

PREPARING FOR A CYBER ATTACK

"TABLETOP" EXERCISES HELP DEVELOP "MUSCLE MEMORY" TO DEFEND AGAINST INTERNAL AND EXTERNAL SYSTEM BREACHES

AUTHORS
Paul Mee
James Cummings

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

"TABLETOP" EXERCISES HELP DEVELOP "MUSCLE MEMORY" TO DEFEND AGAINST INTERNAL AND EXTERNAL SYSTEM BREACHES

Cybersecurity in many organizations has over the last few years been exposed as kind of a Swiss cheese solution, as cyber criminals have found vulnerable entry points to pull off major hacks costing companies hundreds of millions of dollars. In countless cases, companies have failed to erect strong defenses, or failed to recognize and quickly react to an attack. Clearly, cybersecurity needs to be elevated to the top levels of risk-mitigation strategy, alongside currency risk, natural disaster, and terrorist attacks.

In our view, cyber "tabletop" exercises can be enormously valuable for many companies, especially those with huge daily revenues and/or thousands of transactions. Tabletop exercises can start with straightforward scenarios and proceed to more sophisticated simulations with complicating factors. A given exercise is structured to simulate a real attack, with the various stakeholders – C-suite executives, heads of business units, or both – responding with potential actions and reactions, as well as their assumptions and expectations behind those actions.

A prepared moderator and team facilitate moves, putting defenders inside the mind of a hacker/criminal. The moderator applies complicating factors such as misinformation, distractions, extreme weather events, or timing. A team of analysts observes the simulation and upon its conclusion facilitates a "hot wash" – distilling the shortcomings, failures, and gaps, and translates them into a set of practical recommendations.

ROADMAP FOR A TABLETOP CYBER EXERCISE

A company should review its particular threat landscape and outlook, with the broad goals of identifying gaps in cyber resilience and optimizing response governance (who calls whom when?). Based on the threat landscape – recent attacks, especially to peer organizations – you can customize the exercise with cyber-related risks specific to your organization's ecosystem. From the outset, it's essential to define what a given organization or community wants to learn from a cyber tabletop exercise (see "Define Learning Objectives").

Exhibit 1: Define learning objectives

1. What is the full scope of parties that should be involved throughout a major cyber incident?
2. What relationships with government and other agencies, and law enforcement, need to be in place?
3. What leadership arrangements are needed and how does this vary by incident type/severity? For example, when would the mayor's office lead the response?
4. Where do governance arrangements and decision rights need to be better defined?
5. How will key decisions be made, communicated and acted on, regarding:
   - Determination of incident severity
   - Containment
   - Systems shutdown
   - Public, media, and supervisory messaging
   - Declaring an "all clear"
6. What coordinated recovery and remediation related decisions do we need to be prepared to make?
7. What remediation plans, operating arrangements and resources would be needed following a major cyber incident?
8. What is the full scope of parties needing to be involved in recovering from a major cyber incident?

SCENARIOS

Drawing on case studies of recent major cyber events, you can select scenarios based on the real-risk probability to your organization. The basic scenarios can be drawn up with varying degrees of severity, idiosyncrasies, and surprises, depending on your current level of preparedness or sophistication.

The standard process is to start with a basic, linear path, such as Coordinated Insider Action or Denial of Service (DoS), with which most stakeholders are familiar. The second, more dynamic path, adds more serious attack scenarios, such as Data Manipulation, Pervasive Destructive Malware, or Severe Internet/ Power Grid Outage. The third path builds on the previous but adds complicating factors – such as a Smokescreen Attack, Negative Media Response, Severe Weather, or Terrorist Attack (see "Cyber-Attack Scenarios").

Exhibit 2: Cyber-attack scenarios (and complications factors)

THE MOVES IN A GIVEN EXERCISE INVOLVE STEPPING THROUGH WHAT WOULD HAPPEN ACROSS SELECTION OF CORE SCENARIOS THEN ADDING DISRUPTIVE "SURPRISES"

Not exhaustive

EXAMPLE CYBER ATTACK SCENARIOS

A. Coordinated insider action
B. Extensive (replicating) ransomware
C. Credit bureaux forced closedown
D. Markets/Transaction data manipulation
E. Massive denial of service
F. Data manipulation/corruption
G. Pervasive destructive malware
H. Payments systems attack/outage
I. Large-scale internet outage
J. Power grid outage

INCIDENT RESPONSE COMPLICATING FACTORS

1. Management inaccessible
2. Negative media attention
3. Diversion attack (e.g. DoS a smokescreen)
4. False alarms (e.g. bomb threat called in)
5. Communication services disruption
6. Severe weather
7. Natural disaster

CYBER EXERCISE

The length, timing, and setting of the actual tabletop exercise is to a large extent determined by the objectives – and the availability of executive or key stakeholders. Full attendance is not totally necessary, but helpful. Ideally, the exercise is a one or two-day offsite to enhance the active engagement of responsible senior managers and executives. Cyber experts and technicians are also in attendance as a reality check and to challenge assumptions or proposed actions.

Conduct cyber exercises across agreed scenarios:

- Linear path #1 – fairly basic (~60 minutes)
- Linear path #2 – more complex (~90 minutes)
- Dynamic path – complicating factors (90 to 120 minutes)

Responses include determining incident severity, containment, systems shut down, and media communications. Once an attack is detected, the immediate question is whether or not to shut down all systems, just a segment, or none at all. Do you try to contain the visible attack, or do you heighten defenses all around to protect against a wider attack? Part of the calculation is a function of determining whether you are dealing with a 14-year old hacker or a nation state.

The nitty-gritty of this cyber exercise is mapping out who does what, and when. Who makes the call? How is it then executed? If key actors are offsite, can remote action be easily taken? When do you alert the media or local law enforcement? What's the "call tree" – and are there redundancies built in in case a key player cannot be reached? Part of designing a call tree, in addition to basic contract information, is drawing a map of decision rights – who has the authority in a given organization/unit or geography? And are there redundancies if a given person is unavailable?

As to the end game, who gives the "all clear" signal that the attack is over and business systems can be restored? In all cases, timing is important – how do weekends, holidays, or vacations affect response? Is there a backup team, and is it up to speed?

"HOT WASH" DEBRIEF

The "hot wash" post-mortem is a key element of the overall exercise. The proposed responses and identification of call trees needs to be fully analyzed and refined. Were the right people making decisions? Where are the key gaps, what issues rise to the fore, is the governance set for attacks, what's the internal and external communication plan?

Rehash the analyst's notes to determine if there really was a prepared plan in place, or whether people were making things up on the fly. In the latter case, it's clear that a book of procedures needs to be drafted. Determine if law enforcement should have been called – or called earlier. When Sony Pictures was hacked in 2014 – possibly by North Korea – it waited a week before calling in law enforcement. In retrospect, it appears that immediate notification would have made the event much less painful for Sony. Even if you decide not to call law enforcement, it's clearly good to make that a conscious decision and not an oversight.

This "hot-wash" exercise naturally leads to a set of recommendations for individuals, the collective group of key stakeholders, and outside pillars such as law enforcement and the media. Develop a long list of observations, gaps and primary concerns, then distill into recommendations. Produce a briefing pack and socialize the findings.

RINSE AND REPEAT

Setting up the first tabletop exercise is typically a multi-week exercise. Subsequent exercises can be organized much more quickly. The set-up includes interviewing key participants to set objectives and assess availability. Once a time and place is agreed on, the core team (moderator and analysts) should run a dress rehearsal.

Running such an exercise is not a one-time event. Given the increasing sophistication of cybercriminals, and the ever-expanding, cloud-based infrastructure, there are always new vulnerabilities to protect against. Ideally, such tabletop exercises are a quarterly or biannual event. Many organizations now run quarterly exercises in different areas of the organization – finance, risk, lines of business. A regular cadence of exercises will develop an organization's "muscle memory" to react and justify the spend to improve defenses. Just as when painting the Golden Gate bridge, when you have run through all parts of the organization, you start over again. You're running a race without a finish line.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

www.oliverwyman.com

OLIVER WYMAN