Secureworks®

WHITE PAPER

Planning an Effective Incident Response Tabletop Exercise

Background

This document is intended to shed some light on the process that the Secureworks™ Incident Response team utilizes when working with our clients to plan and facilitate a tabletop exercise, and imperatives that can be gleaned from that to ensure a successful exercise, regardless of whether you are managing it internally or having a third party facilitate.

Tabletop exercises are an excellent way to enhance familiarity with policy and processes, and to quickly provide insight into the areas where your Incident Response (IR) capabilities are strong or could use some tightening up. They are a great way to convey to your stakeholders – anyone from an internal stakeholder, to customers, to regulators and insurers – that you have established a capability and that you are continuing to hone and mature your capability to respond to incidents involving the data that is critical to your collective success. For only a handful of hours of everyone's time, you can evaluate the current state of people, process, and technologies that are required to support an effective IR. All of these reasons contribute to facilitation of an IR Tabletop exercise being the most frequently requested Proactive IR service.

That said, the burden falls on you as the planner and potential facilitator of the exercise, to ensure that the time invested is well spent. Everything from identifying goals, to selecting participants and creating an effective scenario that ensures active engagement of the participants, falls on you. This burden can be especially pressing when you are involving business units that are outside of yours, or when reaching to the C-level of the organization asking for their commitment and time.

Your boss's boss's boss will have all eyes on you, and you'll be posing the kind of questions like "what would you do in this situation" to them. No pressure, right? Here are some tips to make sure your exercise is a success.

1. Set Goals

It is important to go into the planning of an exercise with a specific description of what you are seeking to accomplish with the exercise. Without taking this step, you're effectively inviting participants to a meeting without setting an agenda, and may come across as executing this exercise "to check a box" rather than to drive ongoing improvement. Especially when asking for time from other parts of the organization or external stakeholders, conveying these goals will help to:

- clarify the importance of others' participation,
- show consideration and appreciation of their time, and
- set the direction for other aspects of planning.

Everything from "gauge cybersecurity IR preparedness" and "review and validate existing incident response plan and process documentation", to "investigate the implications of gaps in endpoint and network visibility" or "exercise external service provider's ability to support incidents impacting applications that they support", are great goals that will help

folks understand why they are participating and how they fit into the overall response. In general, considering specific processes, systems, data sets, or response to a specific kind of threat can help you identify the stakeholders that will be necessary to effectively understand how prepared you are to respond to a threat similar to what you are going to emulate during the exercise.

Identifying and focusing the group of stakeholders that you engage will lead to more detailed evaluation of the areas of focus, leading to more specific and actionable outcomes.

2. Select Stakeholders

The breadth of support required to effectively respond to all aspects of a business impacting incident makes it critically important to be prepared to address those processes in an exercise. Exercises that have too many participants or participants with widely varying roles and responsibilities are ripe with opportunity for folks to be disengaged and generally lose interest, so we tend to encourage our clients to keep the number of participants under 20 and to ensure that everyone will have a reason and an opportunity to "chime in" during the exercise. It's unlikely that in a reasonable amount of time (more on our feelings on what "reasonable" is later) you will be able to go through the entire lifecycle – from detection to post-incident activities – of an incident with any real level of detail, and keep participants engaged throughout. It's much more likely that you'll be able to effectively engage and observe by specifically focusing on a segment of the overall plan and organization. A few examples:

- Get a good look at where your technical capability and capacity breaks down by focusing on your cybersecurity and information technology personnel.
- Take a deep dive into engaging your communications plan by involving Public Relations and Communications personnel.
- Discuss how the team would engage legal counsel to protect information regarding an incident.
- Highlight a specific gap that you have identified and have been seeking support for, and convey the potential impact of not addressing it.
- Ensure that the IR team understands how and when to engage Human Resources if the need to approach an employee arises.
- Understand how the "front doors" of your IR processes – anyone from the helpdesk, to call center personnel, to the front desk receptionist – are prepared to identify and appropriately escalate an incident.
- Provide visibility into external support that is available to assist when your internal capability or capacity to do so would be exceeded.

3. Encourage Failure and Open Dialogue

Depending upon how frequently the participants typically interact, the subject of those interactions, and the organizational hierarchy of those in the room, the potential exists for participants to feel as though they are being "put on the spot" or "tested". It is

Secureworks®

important to make understood that the exercise is in the interest of improvement, that there is no pass / fail grading, and that participants are each there to improve the overall capability. The expectation is that there are gaps; no one is perfect, and tabletops provide a “blameless” forum where the team can collectively discuss holistic strengths and weaknesses. State this up front, loud and clear (possibly having the most senior person in the room stand up and tell everyone that this is the case), and encourage broad and open participation throughout the exercise. Most of the time, once you initially break the ice the conversation will flow freely. It may be, in cases where there are political or personality conflicts, that a tabletop is not the best initial approach in looking at a particular process or relationship. In these cases, it could be worth considering more of an open dialogue workshop than a situation-focused exercise.

In our experience, an effective tabletop session lasts for no more than 4 hours, with about one quarter of the allotted time going to kick-off information (“rules of engagement”, reviewing exercise goals with participants, introductions, etc.) and to out-briefing the participants at the conclusion of the exercise to get their perspective on how things went.

4. Set a Schedule

Exercises that go on for too long or are too narrowly focused can quickly lead to folks disengaging and moving on to other activities on their phones, tablets, or laptops.

For exercises where you want to exercise multiple process areas, set “break points” where a pause may be natural, or run multiple separate exercises where the story line from a session is predicated by the outcomes of a prior exercise. Some natural breakpoints for exercises can include the point where the team makes a decision to escalate to or engage another stakeholder group (i.e., prior to briefing the executive leadership team, to engaging a new IT group, to engaging an external vendor for support). Ensuring that participants are engaged and interested by the scenario is paramount to opening the communication channels and getting some honest exchange of ideas flowing.

It’s also critically important that you get tabletops on planned participants’ calendars as early as possible. You are likely asking some of the busiest people in the organization – technologists and leaders – to take a substantial chunk out of their day to participate.

We often tell clients that we are working with that scheduling can be the most difficult part of facilitating an exercise, so do yourself and everyone else a favor and get it on the calendar as early as possible. Plan ahead and get next quarter’s exercise on the calendar as soon as you wrap up this quarter’s (assuming you’ve identified goals so that you can select participants appropriately).

5. Develop a Realistic and Customized Scenario

No one likes receiving impersonal form mail, and effectively that’s what you are doing if you present your participants with a “canned” IR tabletop scenario – you’re presenting them with information that doesn’t pertain to them, and the experience is likely to end up in their "mental trash can" the same way that form letter would. Consider some specifics of the organization and the infrastructure when planning, and think of the things that if they were to actually occur would likely result in a really bad day. Having a scenario that represents a realistic and theoretically viable risk that the participants can associate with will both encourage their participation and will allow the team to investigate the controls and processes that are most critical to the organization. Variables to consider when developing a scenario include:

- selecting a threat scenario that represents real business risk to the organization (what keeps you up more at night - a substantial denial of service attack that knocks your production e-commerce platform off the web, or a motivated insider walking off with gigabytes of highly valuable intellectual property?);
- having the scenario "impact" the "crown jewel" assets of the organization (the highly sensitive or regulated data sets, or critically important applications make great "targets");
- using realistic metadata to add a feeling of realism or to infer importance (specific hostnames or IP addresses, names of reporters, "sample" log entries from specific business systems, crafted notifications from a security system, or Managed Security Services Provider);
- considering and exercising the likely channels by which the team would receive an initial report of an incident (as mentioned before, how prepared is your helpdesk to escalate a security issue, or does the receptionist know how to handle the arrival of someone claiming to be law enforcement?);
- engaging business units to get their operational perspective on what keeps them up at night as well; in the end the infrastructure is all here to enable their processes which in turn drives the processes that the organization exists to provide.

It's not necessary for the scenario to represent a crisis-level incident, as evaluating how effective and efficient response to incidents that are more likely to occur is just as, if not more, important.

6. Reporting and Follow-through

One item to consider and coordinate specifically on this reporting is the sensitivity of what you are documenting. This reporting is intended to capture potential deficiencies that your organization likely would not want to have broadly disseminated. This is a great first opportunity to get your legal counsel engaged in the exercise; reach out and request guidance for how they would like this information to be handled.

As mentioned before, it is crucial that you take the opportunity to gather feedback from the participants, and it's recommended that you do so fairly quickly after the conclusion of the exercise while it is fresh in their mind. You chose these participants because they are stakeholders in the IR process, meaning that they will get a feeling

Secureworks®

from this exercise as to whether the team performed in a way that would allow them to successfully complete their piece of the puzzle. Take sufficient time at the end of the exercise before dispersing and go around the room asking for feedback. Make sure that participants understand your perspective that their input is critical to fueling ongoing improvement, that you are committed to ensuring that vetted areas for improvement are tracked for action, and that someone is capturing the feedback. Once the team has dispersed, request any written feedback that folks may not have wanted to verbalize via email, or a web form that does not require them to provide any identifying information. From there, group the feedback and summarize it into a report that prioritizes areas for improvement and provides as much detail as possible on the observation of where a process or capability needed to be improved, the potential impact of that weakness, a recommendation for how to remedy it, and an appropriate assignee for follow-on actions. Remember, this is intended to be a "blameless" exercise – no finger pointing – and the intent is to find areas to improve upon. Participants should consider this effort an opportunity to display capability and gain support to fill gaps.

Socialize the report to gather feedback and gain consensus, but be sure that this is not used as an opportunity to "water down" the results.

Finally, be sure to follow up on the action items captured and assigned in the report. You really don't want to have to address the same gaps during the next quarter's exercise. Prioritization of these actions and ongoing discussions as to their implementation will ensure that the improvement you sought from the beginning is realized. If additional resources are required to fill a gap, those needs can be raised during follow-on sessions as well.

7. Leverage Objective Perspective

Finally, having security personnel facilitating an exercise can be perceived as "letting the fox watch the henhouse"; they are a part of the process, so they should be playing on a level playing field with everyone else. Unfortunately, these are also the folks that are likely to know enough about the infrastructure, threats, and processes to put together a good story line that will hit all of the aforementioned requirements.

Their participation in planning effectively "spoils" the exercise for them – like reading a review of a new movie on social media before you're able to get to the theater and see it yourself. It's important that all participants are stressed by the exercise, which is unlikely if they know what surprises await on the next slide.

Additionally, having an external or otherwise not directly interested party facilitate the exercise can help to avoid any internal political landmines and can lend to an open reception of findings. External parties such as Secureworks, who do this for many clients, can help you understand where you are relative to other organizations of a similar size and business.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp