THE NEED FOR TABLETOP EXERCISES

Maybe you have heard of cyber security tabletop exercises, or they may be new to you. Several types of tabletop exercises exist, and many topics can be covered in the sessions. These facilitator-led, guided discussions walk through an organization's processes and incident response plans for specific cyber events. The exercises are meant to test those processes, highlight any areas for improvement, build cross-team communication, and increase security awareness in the organization.

Much like a fire drill, a tabletop exercise allows everyone to perform a live walk-through of an emergency plan, rather than just having the written plan available. Drills provide critical awareness of issues that may occur in an event that are not covered on paper but are brought to light in the exercise.

Preparing personnel to function well in a cyber event requires similar practice. Everyone needs to know what their responsibilities are and have an idea of what others are doing so that they can coordinate their response. A plan that exists on paper but has not been looked at in years or has only been reviewed by some of the personnel and might not always match up to a real-world event, could end up not actually being useful when needed.

Ransomware tabletops are a popular form of the exercise and a good choice because of the ever-growing threat of ransomware attacks. A strong, in-depth cyber defense that reduces the risk and likelihood of attacks succeeding, or causing damage in the first place, is hopefully already in place; however, preparing against ransomware events also includes having incident response plans, communication plans, and backup and restore plans in case the attack is successful.

SO, HOW DO YOU GO ABOUT JUSTIFYING A TABLETOP EXERCISE?

Like all high-level organizational projects, a good place to start is getting executive buy-in. Your request needs to address a specific need or goal, have a specific solution, and have an imminent time frame. Just saying that you want to have a tabletop exercise to improve security is not enough. You must translate the request so that management understands the importance of the exercise.

Executives balance requests from all the company's departments, and securing funding is just the first part of executive support. You need to convince leadership to fund the initiative while also convincing them to be a part of the exercise. Including executive staff in the tabletop is a key step.

Many of the decision points in an incident response plan can trigger discussions and opposing views. Tabletop exercises can focus on those discussions and allow for decisions and policies to be created before the crisis of an event takes place. During a real cyber event, executives will want to understand what is going on and who is responsible for handling the different parts of the response effort. A tabletop allows all of the parties to be familiar with the different pieces and processes taking place and to be more comfortable with the process during an actual event.

Cyber insurance is an item that is usually discussed in a ransomware tabletop exercise. The details of what the insurance will and will not do for your organization, as well as what the insurance covers and what it does not, in a cyber event are critical points to understand. Some insurance policies have specific clauses for ransomware events compared to other malware events.

SOME POINTS TO UNDERSTAND:

- Will the insurance cover the initial ransom if your company chooses to pay it?
- Will the insurance company negotiate the amount for you?
- What is the dollar figure cap for the payment?
- If, after the initial ransom, a second ransom request is made to return exfiltrated data, is that event considered a separate event by the insurance company or a continuation of the first?
- Will the insurance company cover notification costs if any personal identifiable information (PII) was exposed?

While insurance may pay reimbursement for some or all the financial costs, other, non-financial costs can be incurred by the organization. Ransomware attacks can also include some non-immediate recovery costs from an attack:

- The disruption of normal business activities. In addition to systems affected by Ransomware, other critical systems and services may need to be taken offline until the threat can be identified can contained.
- Sensitive information can be lost or exposed. Not only can data be lost and irrecoverable, but data exfiltration is also common as a second prong of the attack.

- The organization's reputation, professional relationships, and image can be damaged, which can lead to a loss of user/consumer trust.
- Long-term potential revenue and productivity can be lost.

Communication is another key feature that is often included in tabletop scenarios. Cyber events can compromise standard communication and messaging systems. During these cyber incidents, alternative communication solutions must be accounted for to allow a coordinated technical response to the event, make any public announcements needed, and keep stakeholders apprised of the status of the event.

Organizations often only have the required manpower and expertise available on staff to handle day-to-day operations. When a cyber event occurs, these organizations turn to a third-party expert for help in their response. Having contracts in place with these organizations before the event occurs is a good idea, rather than trying to find assistance in the middle of the incident.

With a response organization on retainer, the response process can be sped up. A quicker reaction to containing malware in a cyber event can reduce the harm and exposure done to the organization. Trying to get contracts legal-reviewed and approved is a slow process on good days in an organization, so think about how this approval process would be during a crisis when servers and messaging applications are compromised or shut down. Having assistance within hours instead of days could change the outlook of an event. In some cases, if the retainer is not used for the year, the retainer cost can be reassigned for other security services, such as user security training.

Another topic that can be covered in a tabletop exercise, and the best actual defensive measure in a ransomware event and other cyber incidents, is having good data and server backups. Backing up data goes beyond just saying that you turned on the backups years ago. To ensure that you have good backups, here are some tips:

- Ensure that all the critical and confidential data in your organization is identified to verify that this critical data is being backed up.
- Conduct testing on a regular basis to ensure that the data can be fully restored from those backups.
- Like any other critical system, the backups need to be monitored for failure or tampering.
- A method will be needed to validate system restores so you are not reintroducing malware back into the environment.
- Archive older backups in case you discover that newer backups have been compromised by attackers and you need an older copy for comparison.
- Have a list of critical systems to restore in order of priority to get up and running efficiently.

- Know how long full system restores take. Large data restorations can take more time than expected.

Remember that the idea for any organization with a security plan is continuous improvement. You are unlikely to have an unlimited budget or resources to do everything that is needed immediately. Find the areas where you can improve, plan for the next step, and make progress. You will only fail of you stop trying. Maybe a tabletop exercise is the next way you can improve the security posture of your organization.

For more information please contact Rick Bush, Cybersecurity Architect, RESPEC, rick.bush@respec.com.

Rick Bush

CyberSecurity Architect

RESPEC