Tabletop Exercises for Cybersecurity

Maintaining a healthy incident response

White Paper

By Michael Everett, Security Analyst

essextec
GETTING IT DONE TOGETHER

Effectiveness of Incident Response

Formulating and implementing an incident response plan is a critical step in providing security for your organization or business. But how do you know if you are prepared to defend your business systems and data from the growing threat of ransomware disruptions, Distributed Denial of Service attacks (DDoS), malware intrusions, and similar attacks?

Cybersecurity incident response must be challenged and regularly verified through the execution of tabletop exercises (TTX) the same way in which traditional disaster recovery tests are.

What is a Tabletop Exercise?

One important distinction to make is what a TTX is NOT. A TTX is not a simulation of an actual cyber attack or ransomware outbreak. Rather, it is a low-stress, meeting environment where pre-defined incidents are discussed openly and where participants discuss and identify who will make decisions, the impact of those decisions, and how each team will react to each scenario. No technical environment or equipment is required.

TTXs can have enormous value, without consuming inordinate amounts of time from participants' other duties. Typical TTX commitments encompass only a few hours of time (generally five (5) hours), although they can be left to an organization's discretion. Constructive questions, challenges, and discussions are the focus of the exercise and all parties are encouraged to contribute suggestions for changes in procedure that will help resolve problems more efficiently.

Tabletop Exercise Benefits

One key output from a TTX is detailed notes generated by the facilitator of the exercise.

These notes offer the basis for analysis which provides stakeholders with the information that generates action items for the business:

> Did we have the right personnel/skills involved in the TTX to ask and answer questions?

> Were appropriate decisions and actions taken for the scripted exercise?

> Do the participants have the tools and authority to take action within the desired time?

> Did we react appropriately to the incident? If not, why, and how should we do things differently?

As a result of the TTX, there are likely to be more questions than answers generated and opportunities for improvement, which will translate into other scenarios for a future TTX.

An important component of the exercise is the facilitator. This resource must continuously focus on each activity of the exercise:

> Who made each decision and what precipitated the decision (facts, assumptions)?

> What was the outcome of the decision (positive, negative, solution, additional problems)?

> What, if any, solutions were identified for this specific scenario and who has the associated action items?

> If there is a solution identified, how quickly can it be implemented?

> Did company policies and incident response plans facilitate the solution? If not, what changes could facilitate faster time to resolution?

> Were all parties made aware of documented plans and policies, to incorporate them in their decisions and responses?

A TTX is an opportunity to walk through and evaluate the effectiveness of one's cybersecurity defenses at every level (infrastructure, applications, and data) and is invaluable in determining strengths and weaknesses of an organization's cybersecurity defenses. Review of TTX results will also provide insight into where strategies, tools, and training may be appropriate.

TTXs engage resources and stakeholders from multiple departments of the organization to walk through scripted scenarios in a verbal exchange of discovery, containment, resolution, and recovery. This provides additional insight into the critical nature of cybersecurity for business units previously not aware of potential or real issues.
Goals of a TTX are straightforward and closely tied to the management of a real incident:

> Decision making – are the right leaders in place and do they have the proper information to make decisions and delegate actions to the appropriate resources?

> Have we identified all stakeholders, departments, and even external resources that need to be engaged in real cyber attack scenarios?

> Do our teams have the tools and information necessary to detect, contain, and resolve each situation discussed in the TTX? Are these resources available in the timeframe that is acceptable to the organization?

Planning and Execution of a Tabletop Exercise

Proper planning for the TTX is critical to provide value to the organization. Specific scripts should be developed for threats that are identified by the business, as not every scenario will apply to every company.

TTX scenarios are simple in that they require no physical preparation. No equipment or infrastructure is needed since the entire exercise is composed of individuals discussing scripted incidents and evaluating the success or issues discovered through verbally walking through the incident response process.

TTX scenarios may include any type of cyber incident that could conceivably pertain to a given organization: malware, ransomware, or Distributed Denial of Service attacks (DDoS), or even attacks or theft from an internal source. Each type of intrusion requires a particular TTX script that can be addressed by the team.

Why and When?

TTXs provide an open discussion of how security policies will address each type of incident, who will be involved in identifying and responding, and how resolution and recovery will be determined and established.
Many factors determine how often a TTX should be conducted:

> Has the business climate or infrastructure changed?

> Are new personnel on board that are not familiar with security policies, who could benefit from specific TTX scenarios?

> Has there been a recent cyber attack or threat that initiated management concerns regarding your cybersecurity readiness?

A TTX can be relatively inexpensive to execute and the benefits can be considerable for employees and the business. At the very least, planning and executing TTXs should be conducted annually to ensure all impacted resources and stakeholders are well-acquainted with the policies and procedures.

How to Conduct a Tabletop Exercise

Identify stakeholders based on the nature of the organization or business. For example, public companies will need to include such departments as public relations and legal to manage press announcements and work done with law enforcement. IT teams and software vendors may also be included where appropriate.

Develop specific scenarios that have been agreed to by stakeholders and management. Support by management is also critical to the participation of essential departments and individuals. The goal is to identify threats that are relevant to one's business and make them the highest priority.

Don't attempt to be all-encompassing. Determine the scenarios that are appropriate to a specific TTX, develop the unique scripts, and focus on them. Additional scripts can be covered in future TTXs. Limit the TTX to a small investment of participants' time. An accepted guideline is five (5) hours for an effective TTX.

Consider all internal and external parties, to cover the whole picture. Hardware and software vendors, authorities, regulatory agencies, and more may be involved in a real-world incident. Where possible, be certain that those contacts are identified and even interacted with during the exercise. Collaboration with disaster recovery teams will be appropriate in some scenarios, so include those resources where needed. Outside resources may further enhance the success of the TTX through their experience in participating with other businesses.

Manage the exercise with at least one facilitator/observer who is dedicated to documenting the TTX as it unfolds. This includes all decisions made, who made the decisions, and why. It's also essential to monitor how policies and procedures are adhered to, or if deviations are in order, and why. Be certain all participants understand the role of the facilitator, so that questions asked for documentation purposes are not taken personally and that all team members feel free to express any suggestions or challenge decisions.

Follow-up with all TTX members and elicit their input related to how they perceived the value for time spent, whether new ideas or suggestions were identified, and if they feel there are open issues, (i.e., Did the scenarios prove realistic and were policies effective in identifying, containing, and resolving the problems?). Combining the information gathered by the facilitator with that of the TTX team members for analysis of policies and procedures will prove invaluable in updating those processes and providing a more comprehensive cybersecurity policy for actual incidents.

Summary

Cybersecurity is not a project or policy. It must be an integrated, well defined, yet dynamic strategy for business continuity, system availability, data privacy, and the safety of employees and customers. It's important to plan and conduct regular TTXs as part of a comprehensive corporate and organizational security strategy.

A TTX is a meaningful, cost-effective method of testing one's cybersecurity policies and procedures to ensure readiness for actual cyber attacks. TTXs enable an organization to maintain visibility into the different types of attacks being launched in the real world. Similar to traditional disaster recovery tests, TTXs demonstrate how to effectively tackle those attacks and create the appropriate defenses against them. Simply having a policy in place will not prepare an organization in a time of crisis. Executing a TTX prior to an incident is the only way to properly evaluate the effectiveness of the incident response plan in place. Planning, execution, and analysis of TTX results provide a foundation for confidence knowing that your business and employees are aware of security policies and procedures and how to apply them.

For more information on our full suite of solution offerings,
visit essextec.com or call 1-888-519-1518
to schedule a consultation.

Essextec offers Cloud, Cognitive, and Cybersecurity solutions delivered by a team of experienced technology and security experts, business consultants, and industry thought leaders. Our innovative and cognitive era solutions are uniquely tailored and enable us to provide differentiated value and outstanding business outcomes for each of our clients.

We are headquartered in Rochelle Park, NJ, with offices in New York City and Delaware. We serve clients throughout the Northeast U.S. Visit essextec.com

essextec
GETTING IT DONE TOGETHER

IBM Platinum Business Partner
IBM Watson Award
Winner 2016

Cloud | Cognitive | Cybersecurity