CECILIE_ARCURS/E+/GETTY IMAGES

TECHNOLOGY

Cybersecurity Training Through Tabletop Exercises

Strengthen your disaster recovery plan by shooting holes in it

by Michael J. van Zwieten
Florida League of Cities

Imagine turning your computer on, and it takes longer than normal. Eventually, the login prompt comes up, and you type in your password. The computer seems to be taking forever to get started this morning, so you grab a cup of coffee while you wait.

After you return to your desk, a large error message is displayed on your screen. It reads, "Your files are encrypted. If you are reading this message, your files are no longer accessible. You can recover your files if you send us 3 Bitcoins," which is worth $88,111 as of May 25, 2022.

Your co-workers are experiencing the same message on their screens. Citizens are starting to call and want to pay their utility bills. Computers are down. City services are, at this point, completely nonfunctional. The media just called and is asking questions. What do you do?

Of course, this situation is hypothetical, but it's realistic and could very well happen in today's world. Amid hurricane season and hackers continuing to test your defenses relentlessly, you hope a well-developed disaster recovery (DR) or business continuity (BC) plan will be able to help mitigate some of these risks. While best practices call for making sure you review and test these BC plans regularly, how will you be sure these plans will execute flawlessly? There isn't a way to exactly know whether your BC plan will truly work unless you have experienced a disaster requiring it. However, there are ways to test your plan in smaller, more manageable bites, namely, through tabletop exercises.

According to the **Department of Homeland Security**, tabletop exercises are "discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation." Facilitators are an important ingredient to the mix, as they help guide and set up the various scenarios that the participants need to work through. The duration of tabletop exercises is dependent

From a technology perspective, tabletop exercises ... can uncover unknown holes or potential vulnerabilities related to a city's infrastructure, cybersecurity defenses, policies or procedures.

on the scenario and audience. Some last only 30 minutes, while other sessions can take a few hours or more. The benefit of these exercises is that personnel involved in responding to these incidents become more familiar with and understand their roles and the procedures necessary to handle different, potentially catastrophic events.

Outside of testing the DR or BC plan, tabletop exercises can be highly beneficial for other types of scenarios. For example, members of the Information Technology team may already hold tabletop exercises regularly to come up with various cybersecurity scenarios and explore how they might handle a potential attack. After setting up the initial scenario, the team considers more detailed questions to help uncover any potential deficiencies in defenses, such as the scenario below.

An employee inserts a flash drive into their personal home computer to download files they need for work. The employee is unaware that these files were infected with malware. At the office, the employee tries to copy the files on their workstation that is connected to the internal network. After files are opened by others across the organization, the malware infects the organization's entire network.

Some questions to consider:

- Given the initial path of attack, how would you be able to identify this malware infection?
- What technologies are used to identify malware intrusions of this type?
- Are anti-malware defenses deployed on all network devices? What's not being defended?
- What can be done further to prevent future malware infections or incidents of this type?
- What further training, policies and procedures would benefit this scenario?

From a technology perspective, tabletop exercises such as this example can uncover unknown holes or potential vulnerabilities related to a city's infrastructure, cybersecurity defenses, policies or procedures. Simple "gotchas," like generators running out of fuel, data centers located in a flood-prone area or redundant internet connectivity not available to provide service during major events or outages, will come to light quickly. More difficult issues to overcome are highlighted by designing multiple types of cyberattack scenarios and identifying the technologies or policy changes that could help mitigate the risk.

The **Florida Center for Cybersecurity**, also known as **Cyber Florida**, leads a spectrum of initiatives to inspire and educate future and current professionals, support industry-advancing research and help people and organizations better understand cyberthreats and what they can do to stay safer in cyberspace. In partnership with the **Florida League of Cities** (FLC), the **Florida City and County Management Association** (FCCMA) and the **Florida Local Government Information Systems Association** (FLGISA), Cyber Florida held four regional workshops throughout Florida, training many of our cities' executive staff through the means of a cyber wargame scenario. Wargames are very similar to tabletop exercises, but the outcome of each successive scenario is shaped by the decisions being made by the participants.

In January 2022, **Ronald Sanders**, DPA, **Staff Director** at Cyber Florida, facilitated their local government wargame scenario at the FLGISA Winter Symposium, which was attended by nearly 100 technology professionals from across the state, to experience a scenario from the perspective of the fictitious "City of Beachside." This unfortunate city was the subject of one disaster after another, ranging from insider data theft, ransomware attacks on their utility and even data breaches within their billing department.

In this multi-hour scenario, teams of six to eight individuals would take on various roles within the City, deliberate with each other on how they would handle the current scenario, give recommendations and answer questions that the facilitator asked. The audience would learn from the ideas and suggestions that other teams had, while the facilitator helped share a new perspective on how these situations could have been handled. Tough questions, such as "Who's in charge of the City's response right now?" and "What do you tell the Mayor or City Council, citizens and employees, local businesses, the media and the public?" required some deep thought and careful consideration.

Wargaming not only requires the audience to deal with attack and incident response but quickly turns into crisis management. While wargaming is the ultimate tabletop exercise, it can be intimidating to set up and organize, as it takes time and thought to devise the scenario and the end-goal lessons that you want the audience to walk away with.

Wargames and tabletop exercises can be valuable tools. Devising or attending a wargame, even holding some regularly scheduled tabletop exercises throughout the year, can greatly help your team stay sharp regarding your DR or BC plans. They will also continue to strengthen internal defenses with that never-ending goal of making them bulletproof.

Michael J. van Zwieten, CGCIO, MCSE, is the Director of Technology Services at the Florida League of Cities and Executive Director of the Florida Local Government Information Systems Association. QC