CNA

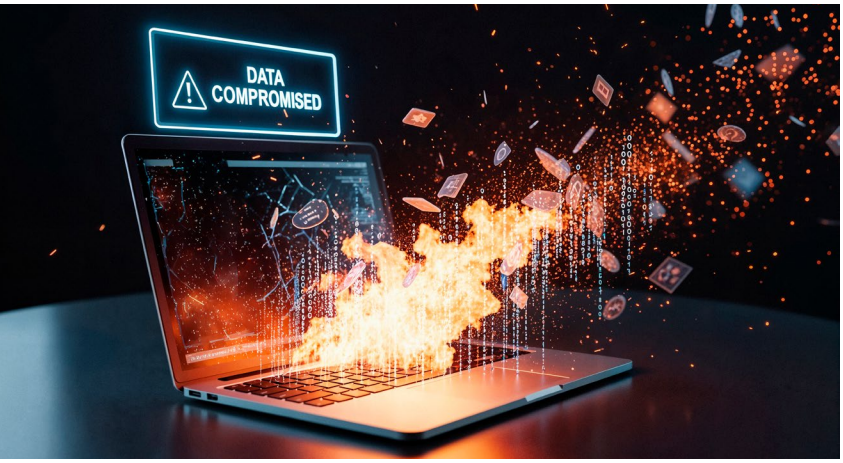
From Exercises to Real-World Readiness: Enhancing Cyber Response

Are You Prepared for a Cyberattack?

It's Friday morning, with just one week to go until payday. The skies are blue, but your team is closely monitoring a major rain event forecasted in your area for early next week. Meetings are already on the calendar in preparation for possible activation.

Meanwhile, you're looking forward to a relaxing weekend with a mix of community events and downtime with your family. At 0900, while settling into the office for the day, you notice your agency's emergency notification platform isn't loading. You check your phone to troubleshoot, but it won't connect either. Every site and app you try either won't load or returns an error.

At 0915, your screen goes blank. A message appears stating that your system has been compromised. It's a ransomware attack—your files are encrypted, and criminals are demanding money to restore access and functionality. Your office, responsible for coordinating emergency response in your area, is effectively offline, just days before a potential weather emergency.



Considerations for Cyber-Incident Response

- Determining roles and responsibilities
- Communicating (including in a degraded environment)
- Acquiring required resources
- Communicating with the public
- Working with external organizations for forensics and attribution
- Working with private sector partners

Using Exercises to Develop and Test Cyber Response Plans

As the emergency services sector—and society as a whole—has become increasingly reliant on cyber technology, including computer-aided dispatch, platforms such as WebEOC, and smartphone applications, cyber threat concerns have become increasingly important. In this threat environment, developing a cyber annex in emergency operations plans is essential for comprehensive preparedness and operational resilience. However, a written plan is just the starting point—the crucial next step is bringing together relevant stakeholders to test and exercise the plan.

Over the past ten years, CNA has led and supported cybersecurity workshops and exercises at all jurisdictional levels for civilian and military sponsors. Participation varies but generally includes members of leadership, emergency management, law enforcement, IT, the private sector, and other jurisdictional departments. These exercises are scenario-based and time-phased, with varying time frames, primary cyber threats (e.g., malware, ransomware), secondary threats (e.g., flooding), and targets (e.g., 9-1-1). Typically, CNA uses workshops to develop content for a cyber-incident response plan and uses tabletop exercises to test draft plans. Relying on CNA's long history of support to military and public sector organizations, we draw on wargaming and design thinking elements to ensure that these games are effective, immersive, and engaging. Examples of past CNA work in this space include the following:

Developing and executing a **scenario-driven tabletop exercise** and producing an **after-action report** and improvement plan to help a large US city test and revise the cyber annex of its continuity of operations plan

Planning and executing a **cyber-incident response tabletop exercise** for the US Space Force

Developing and executing **workshops in nine countries** centered on long-term cybersecurity planning

About CNA

CNA is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the Department of the Navy's federally funded research and development center (FFRDC)—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform the decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and innovative methods to support federal, state, and local government officials as they work to advance national and homeland security.

For more information on developing and testing a cyber response plan, please contact Dawn Thomas (thomasdh@cna.org).