Cybersecurity: A Better Way to Test Readiness than Experiencing Reality

Let's face it, when it comes to some realities it is best to not experience them at all. No one wants to experience a fire in their home or a devastating earthquake, tornado, tsunami, or pandemic. Similarly, no one wants their privacy stolen or the critical assets of their organization threatened. While we would like to avoid risks altogether, we know that they are part of reality; and while nothing tests our readiness quite like reality, we will perform better if we properly prepare.

So, we prepare accordingly. We use risk management protocols to protect and defend against a variety of risks. An example of this is the auto-shutoff switches to our electrical breakers in our homes that prevent a surge in electricity which could cause a fire. We use seat belts to prevent injury from an auto accident. We also use incident response and recovery plans when risks do become reality. Conducting fire drills in schools, offices, and our homes help to prepare us if there is a fire and where we need to respond quickly to protect ourselves and others. We use documented playbooks and manuals sometimes when responding and recovering from a risk-turned-reality because emotions and anxieties can cloud judgement and impair decision making during the chaos of a crisis. It is for similar reasons that we have cyber simulations; we prepare for a reality that we hope never occurs. We prepare because we know the occurrence is very possible, and perhaps, very probable in today's world.

Our understanding of the probability of a cyber risk occurring is similarly high. We know that it is common practice to talk about an inevitable hack, phishing attack, data ransom, or even network sabotage. We also know from security officers, risk managers, and administrators in our community that counties, government agencies, and organizations are not as prepared as they would like to be for the cyberattacks threatening their operations, stakeholders, critical assets, and overall brand. For a variety of reasons (budget, staffing), counties lack fully tested incident response procedures and fully detailed operationalized playbooks ready for use to mitigate cyber threats and to adequately respond to attacks before they become a crisis. Consider the following list of threats. Are you prepared?

A WORLD OF THREATS		
Website defacements	Obtain data left undeleted in cloud	Delete or modify data on public site
Malware-directed internal spying	Blocks access to information system	Computing critical data
Phishing attack	Counterfeit website	Obtain unauthorized access
Compromise mission-critical information	Cause disclosure of sensitive information	Compromise key suppliers' design, manufacturing, or distribution
Network sniffers intercept communications	Exploits weak or no encryption of information	Obtain sensitive data from publicly-available sources
Counterfeit certificates	Malware via email	Wireless jamming
Multi-staged attacks (e.g. hopping)	Malware via removable media	Denial of Service (Dos) attack
Internal and external attack (mixing physical and cyber methods)	Dumpster diving (written passwords left exposed)	Distributed Denial of Services (DDoS) attack
Tampered hardware in supply chain	Software collect network traffic data	Physical attack (e.g. bombing)
Fire	Flood	Hurricane
Earthquake	Pandemic	Tornadoes
Zero-day attack	Data scavenging attacks in the cloud	Exploit vulnerabilities in mobile
Wireless sniffers collect data inside facilities (e.g. key cards)	Physical attack on supporting infrastructure (e.g. cut power)	Subverted individuals placed into organization
Exploit split tunneling (e.g. entering network through laptop on public and secure system simultaneously	Man-in-the-Middle attack (e.g. third party secretly joins a two-way online engagement)	Exploit multi-tendency in cloud (e.g. observes organizational processes, acquire info, or interfere)
Login/password guessing attack	Hijack IT sessions	Ransomware
Attack timed with critical organizational operation	Malware directs transmission of sensitive information	Third-party violations to policy or procedure accessing information
IoT/SCADA compromises	Insider threat	Software releases with malicious code

There are likely many risks on this list that you feel highly confident about addressing if faced in reality. There are likely many as well that you are not very sure about your abilities to face effectively and that you may not even recognize. Finally, there are likely many others that you know for sure that you are not prepared to face with any level of confidence.

In a recent cyber simulation we engaged in, 48% of participants said they have nothing in place to protect, defend, respond, and recover from a ransomware attack. Another 20% in the study said they had a defense defined, but it has not been tested. No one in the study felt highly prepared in their readiness to experience such a cyberattack.

Collaboration is key to success when facing any of these risks. It is for this reason that the NACo County Tech Xchange and the Professional Development Academy have partnered to offer quarterly cyberattack simulations for leaders (https://www.naco.org/naco-cyberattack-simulation) – collaborating with one another in a highly facilitated, online program to increase readiness to address the riskiest of risks.

The overriding objective of any cyber simulation is to assess current risk management capabilities among individuals, teams, and key stakeholders. Most simulations assess how well that team of people can detect, defend, respond, and recover from a cyberattack. In addition to people, a well-planned simulation can also highlight readiness of planned processes and use of risk management technologies. In short, the purpose of a simulation is to assess current preparedness to develop action steps that will help close gaps from current state of readiness to a future ready state. That is exactly what these simulations accomplish.

The objectives of each simulation are to:

(1) provide a certified test of incident management plans and associated cybersecurity and risk management playbook details aimed to detect, defend, respond, and recover from a cyber risk,
(2) baseline current cybersecurity and risk management work capabilities relative to a cyber risk,
(3) strengthen the leadership skills of incident managers leading the company through risk planning and incident resolution,
(4) improve the quality of the incident management plans and playbook details based on participant engagement in assessments, peer reviews, and best practice benchmarking, and
(5) develop immediate action improvement plans to strengthen people, process, and technical security controls.

We encourage county leaders to participate in our quarterly sessions – which are held online and facilitated by expert practitioners; and engagement is 100% FREE! Learn more and enroll today at https://www.naco.org/naco-cyberattack-simulation.

Tim Rahschulte is the CEO of the Professional Development Academy and chief architect of the NACo High Performance Leadership Program (www.naco.org/cyberskills).

Rita Reynolds is the CIO of the National Association of Counties.