Building a Cohesive Plan for Cyber Resilience

The pandemic gave many government organizations the impetus to launch or accelerate digital initiatives. As the digital footprint expands into nearly all areas of operation — from remote work and digital constituent services to intelligent transportation systems and smart city programs — cybercriminals are more focused than ever on compromising the valuable data within systems. Ransomware and other threats are targeted, persistent and advanced, making it a matter of when — not if — an organization will be attacked.

Cyber resilience — an organization's ability to recover from and adapt to threats and other disruptions in the digital environment — is essential for maintaining business and service continuity in state and local governments. Cyber resilience helps organizations prevent, detect, respond to and recover quickly from adverse cyber events. It also reduces recovery costs and helps maintain public confidence in government and its services.

The key to achieving cyber resilience is developing and implementing a cohesive plan that incorporates best practices and densely layered cybersecurity technologies.

Maintaining cyber resilience in a rapidly changing world

State and local governments face a variety of challenges in maintaining cyber resilience.

- ✓ **Device/endpoint proliferation.** Today's employees frequently use multiple devices — including personally owned desktops, laptops and smart phones — to perform their jobs. The higher the number of sanctioned and unsanctioned devices, the greater the organization's vulnerability.
- ✓ **New services and operations.** Remote work, digital services, smart city projects and the Internet of Things (IoT) have erased the traditional network border. Protections such as firewalls and intrusion detection are no longer sufficient.
- ✓ **Abundance of high-value data.** Personally identifiable information, critical infrastructure data and other sensitive content make today's digital coffers increasingly appetizing to cybercriminals.
- ✓ **Constantly changing threat landscape.** Cybercriminals continually evolve their tactics to take advantage of new opportunities. To remain resilient, organizations can no longer "set and forget" their cyber resilience plans and controls. They need to systematically update their strategy and tools to stay ahead of their adversaries.
- ✓ **Regulatory compliance.** As new government and industry regulations emerge, organizations must review and adjust cyber resilience plans, processes and technologies to meet requirements. They should also review compliance standards whenever they deploy new functionalities, such as online payments or digital benefits enrollment. Tracking and complying with existing government regulations as well as newer legislation such as the EU's General Data Protection Regulation and the California Consumer Privacy Act is a complex task full of easily overlooked details.
- ✓ **Cybersecurity staff shortages.** Ongoing staff and skillset shortages threaten cyber resilience and damage employee morale.

Building cyber resilience on multiple fronts

Modern organizations must ensure business continuity during and after any cyber incident, whether it's a malicious, targeted attack or something as simple as a power outage. A cohesive cyber resilience plan helps organizations adapt to any cyber disruptions that come their way. It incorporates proven processes and dense layers of cyber resilience technology that are woven together on a unifying platform. Using this platform, organizations have a single pane of glass into threat intelligence, real-time activity and analytics. They can leverage machine learning to automatically find anomalies, make data-based decisions and rapidly mitigate threats.

A well-crafted cyber resilience plan starts with thorough assessment and documentation and addresses every detail of protection, detection, response and recovery. Leaders in charge of cyber resilience can take the following actions to create a cohesive plan.

- ✓ **Assess and document processes.** Identify critical assets and determine the business impact if those assets were compromised. Consider the risk

tolerance for various compromises, prioritize what needs protection, and then identify controls and processes for protecting assets. Document decisions and controls so incident response teams, risk managers and business leaders have the information they need to respond quickly and appropriately in the face of day-to-day issues as well as emergent crises. Make certain they have the appropriate access and authority to respond to an incident.

- ☑ **Predict/identify potential attacks.** This layer of cyber resilience requires tools to maintain visibility into the health and integrity of endpoints and other systems, as well as analytics and machine learning to better predict and thwart attacks. Training and education are also essential. Teach C-level leaders, cybersecurity staff and IT teams how to better understand threat intelligence, and show them how threats affect the organization's ability to execute its mission. Educate business users on cyber hygiene and how to avoid threats such as phishing attacks.
- ☑ **Protect assets.** Incorporate a Zero-Trust approach that focuses on continually verifying user identities and access permissions, encrypting data at rest and in transit, and applying other user-centric, data-centric controls. In addition to on-premises applications, be sure to protect cloud-based applications, email, devices/endpoints and real-time processes that occur at the network edge. Include provisions for backing up data and maintaining immutable copies of data for disaster recovery and business continuity.
- ☑ **Detect attacks that do get through.** Ransomware and other attacks often start with a stealthy incursion that goes undetected. Use intelligent, automated tools to scan for and identify anomalies in traffic and user behavior. Incorporate historic and real-time security and threat intelligence to further inform threat detection. Have plans in place to change processes and capabilities as needed to reduce the impact of actual or predicted attacks.
- ☑ **Respond.** Monitor attack activity that cannot be blocked and adapt accordingly. This is where a well-documented escalation and crisis communications plan comes into play. Organizations should regularly conduct exercises to test their preparedness to respond to events. Doing so at frequent intervals is especially important in fast-changing environments or when significant threats emerge.
- ☑ **Recover and learn.** Institute processes to recover/restore data and business functions quickly after an attack. It's also important to have a plan for communicating promptly with constituents or other stakeholders regarding potential privacy breaches or service disruptions. After the incident, conduct forensics to assess what happened; identify lessons learned; and prepare for reporting to regulators, the public and internal teams.

Getting started

The following best practices will help organizations get started on a dynamic cyber resilience plan that meets today's needs and helps prepare for the future.

- ☑ **Build a roadmap that aligns with the organization's overall vision** for cyber resilience, outlines its specific goals and benchmarks, and identifies metrics or key performance indicators to help track progress along the way.
- ☑ **Obtain buy-in from the top down.** Include IT and cybersecurity teams as well as executives, managers, business leaders, users and other stakeholders.
- ☑ **Seek outside expertise to bolster in-house knowledge and skill sets.** Consider working with a managed security services provider that can lend expertise to help internal teams understand the output from various tools and respond effectively when serious incidents occur. These specialists can also alleviate the capex, staffing and operational burdens associated with maintaining cyber resilience day to day.

Most government agencies today collect or handle valuable digital data that is at risk of compromise. It's no longer a question of whether a cyberattack will occur, but when. While cost is an important factor when considering a cohesive plan for cyber resilience, the cost of not having a cohesive plan is often far greater. With densely layered security tools and a plan based on best practices, organizations can mitigate and manage the impact of an attack, ensuring their ability to recover and adapt when issues arise.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from ESET.

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Sponsored by: ESET®

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit **www.eset.com** or follow us on LinkedIn, Facebook, and Twitter.

SHUTTERSTOCK.COM