5 Steps Toward Cybersecurity Resilience for Government Agencies

MARKET TRENDS REPORT

govloop DELL Technologies Secureworks®

Executive Summary

Cybersecurity attacks continue to grow in number, in complexity and in impact. State and local government entities are not immune, and the ransomware attacks on the Colonial Pipeline and meatpacker JBS USA demonstrate how cyberattacks can affect daily life.

Another famous attack – the 2018 ransomware incident involving Atlanta's government – was more limited in geographic scope, but affected as many as 6 million people. Recently, there have been cyberattacks against hospitals, even while they are coping with the COVID-19 pandemic. As school systems juggle remote learning and social distancing, they are also facing these same problems. Cybercriminals are even targeting water utilities and endangering a precious, finite resource.

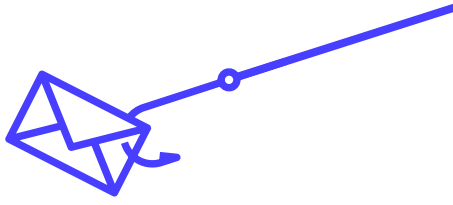
While not all cybersecurity attacks receive national attention, they are just as disruptive and destructive for the people relying on those services.

At the state and local levels, the best answer to these dangers is deploying a robust threat detection and response solution. In particular, managed detection and response (MDR) solutions uncover threats that evade traditional security defenses, rapidly respond to these threats and include access to security experts that a government entity likely does not possess.

This report, created by GovLoop in collaboration with Dell Technologies and Secureworks, discusses how a managed service with advanced analytics can help state and local agencies monitor cyberthreats and strengthen their response to security incidents, and how to build greater cybersecurity resilience into organizations.

"In 2020, while the American public was focused on protecting our families from a global pandemic and helping others in need, cybercriminals took advantage of an opportunity to profit from our dependence on technology to go on an internet crime spree. These criminals used phishing, spoofing, extortion and various types of internet-enabled fraud to target the most vulnerable in our society."

- Paul Abbate, Deputy Director, FBI



By The Numbers:
Today's Complicated Cybersecurity Landscape

A shortage of about

36,000 public sector cyber jobs

exists across federal, state and local governments.

66

The average number of zero-day exploits (previously unknown vulnerabilities that can be used by hackers) found each day in 2021, which almost doubles 2020's total and is more than any other year on record.

75%

of organizations worldwide experienced a phishing attack in 2020.

1,097 organizations

were hit by ransomware attacks in the first half of 2021.

$3.92 million

is the average cost of a data breach.

241,342

phishing/vishing/smishing/pharming attacks were reported in 2020 – a **110%** increase over 2019.

State, Local Agencies Look to Turn Tide on Cyber Battle

The Challenge: Rising Digital Danger

As the threat landscape expands, security management tools cannot keep up with agencies' needs. Agencies' networks face twin perils – cybercriminals and threat actors sponsored by nation-states.

Ransomware attacks, meanwhile, have become national news stories. States, cities, medical and school systems and more have been targeted. The newest trend is a two-pronged attack: first, cybercriminals extract sensitive data from hijacked files like emails. Next, the attackers demand a ransom to prevent releasing this data online, usually using a tight deadline to increase the pressure on agencies.

With the COVID-19 pandemic forcing many people to work from home, phishing attacks have also skyrocketed. Now, employees do not have the same technical support that they did at their offices, and they often lack in-depth education about threats like phishing. For security professionals, these factors have significantly expanded attack surfaces.

Additionally, there have been more zero-day exploits in 2021. While cyberdefenders have become more adept at finding exploits and issuing patches, agencies just do not have enough staff to identify, prioritize, patch and address every flaw in the changing digital landscape. Even worse, cybersecurity jobs are often vacant at every level of government, partially because the private sector also needs cybersecurity professionals but typically offers higher salaries. For potential public sector employees, the federal government has more pay flexibility than states or local agencies.

Finally, the public sector – especially state and local agencies – generally suffers from aging IT infrastructures. Most government IT budgets go toward maintaining systems that have functionally exceeded their lifecycles, subsequently giving agencies another cybersecurity burden. This makes prioritizing security projects critical, since all agencies must assess data, systems and assets for their daily operations. Furthermore, vulnerability management cannot be an occasional activity, as new gaps are discovered all the time.

The Solution: Managed Threat Detection and Response

Effective threat management must be ongoing rather than a point-in-time activity. Managed detection and response solutions can automatically scan assets, probe vulnerabilities and assess risk factors simultaneously. These solutions can also prioritize vulnerabilities based on their potential for risk using artificial intelligence (AI) and machine learning. Here are five steps toward cybersecurity resilience for state and local governments:

1. Preventing as many endpoint threats as possible by using next-generation antivirus (NGAV) solutions on every endpoint. This also helps reduce the attack surface and provides context for investigations.

2. Detecting potential threats across all IT elements – endpoints, networks and cloud computing environments. This includes data and alerts from existing tools like endpoint detection and response (EDR), network detection and response (NDR) and cloud telemetry combined in one system, so that analysts have full visibility across their environments without having to piece together and manually correlate evidence from multiple consoles.

3. Investigating any suspicious activity to identify malicious behavior. The best MDR solutions provide automated machine learning and built-in detectors to correlate data across all security tools and quickly elevate the most critical issues to investigate.

4. Responding with confidence to remediate damage by evicting threat actors and keeping them out.

5. Improving user behavior and increasing vigilance. This is crucial, as users are the front line of the cybersecurity battle. Deploying awareness and educational programs designed to boost end user knowledge and teaching best practices like avoiding suspect links are effective in making workforces more resistant to phishing attacks and other threats. Employees should be encouraged to trust their instincts if emails don't feel right; for instance, they can send senders a fresh message asking if they wrote the original email. Agencies can track and measure the effectiveness of such education by testing employees with fake phishing campaigns.

Best Practices in Threat Detection and Response

The three-legged stool of cybersecurity includes people, processes and technology. Agencies should direct their energy toward these best practices addressing all three legs:

1. Focus on what is most important, not what is most visible.

Agencies must have a solid understanding of what data and systems are most vital to their organizations and target remediation efforts there first. The "correct" answer is going to vary widely – schools may consider personnel and students' privacy most important, so they prioritize HR systems and payrolls, while a state highway department might be most concerned with contracts, disbursements and safety databases. It is crucial to remember that this isn't a one-time assignment for agencies; prioritizing systems and remediating emerging threats and vulnerabilities must be a continuous activity.

2. Consolidate vulnerability management so you can see and address threats across the entire organization.

Even small agencies are likely to have multiple systems used by different departments. In this interconnected age, however, there are going to be many places where these disparate systems connect with one another. Historically, many systems have their own security in place; this makes it difficult to combine information and see threats that could spread across all the systems, and almost impossible to react in a timely way agencywide. Implementing a consolidated solution changes this equation, providing the early warning system needed for fast responses while freeing up security staff to tackle other important tasks.

3. Use automated MDR to speed remediation and maximize available human resources.

The first objective for security professionals is to find ways to improve threat detection and expedite responses. The second is finding ways to cut costs and free up time for more valuable work. Implementing MDR meets both these needs by providing threat hunting, detection and rapid response capabilities that can be matched to all the systems' needs, whether endpoint, network or cloud. Combining enterprisewide threat visibility via MDR and a robust vulnerability management solution provides a level of continuous monitoring and protection that security professionals can leverage for more strategic responses to threats and tailoring measures to permanently shut them out.

Case Study: How One Agency Upgraded Its Cybersecurity

A state agency with a citizen-facing website that collects fees discovered unauthorized activity in a data center. This led to the discovery that a third-party account on a different server had been compromised. The security team investigated, isolated and patched the server, and then analyzed the rest of the agency's IT environment to be sure that no other assets had been compromised.

While the agency had dodged the immediate bullet, the security staff started looking for an around-the-clock monitoring and response solution. Building out its own staff for such activities wasn't feasible. The security staff recommended a managed detection and response service that included threat hunting and incident response capabilities that could help the agency scale its security operations without increasing headcount.

In evaluating prospective vendors, the agency also looked for a company with a long track record of success. The agency also wanted a partner that conducted threat research to identify emerging threats and consistently built long-term partnerships with its customers.

After the agency selected a company for its MDR services, it was notified by an employee working at home that a family member had clicked on a bad link on their personal device. The security staff was able to look at the employee's agency-issued device to see if the breach had affected it, found a couple of phishing emails blocked by the agency email server and changed the employee's passwords. The log data revealing the attempted attack was kept by the MDR firm, and the agency was able to see it in its unified security picture. What could have taken hours was instead resolved in seconds.

HOW SECUREWORKS HELPS

Secureworks is a leader in cybersecurity. We protect organizations by providing battle-tested, best-in-class cybersecurity solutions that reduce risks, improve security operations, and accelerate ROI for Security and IT teams. Secureworks products are built on the cloud-native security platform Taegis that continuously gathers and interprets telemetry from proprietary and 3rd party sources, including endpoints, networks, cloud, and identity. We use this telemetry to detect and prevent threats, automatically prioritizing the most serious ones, and enabling faster, more confident responses with time- and cost-saving automation.

Taegis XDR is an open extended detection and response solution that leverages advanced security analytics to meet and respond to threats.

***Learn more:* Taegis XDR, Cloud-Based Security for Extended Detection and Response | Secureworks**

Taegis ManagedXDR is a 24/7 service that combines software, proactive threat hunting, threat intelligence and incident response in one solution.

***Learn more:* Taegis ManagedXDR | Managed Extended Detection & Response | Secureworks**

Taegis VDR automates vulnerability management with a cloud-based, machine learning-powered solution that enables security professionals to intelligently prioritize remediation efforts based on actionable recommendations that reflect the context of the customer's environment.

***Learn more:* Taegis VDR | Vulnerability Management | Secureworks**

Conclusion

State and local agencies working to strengthen their cybersecurity defenses face many challenges, from the complexity of the threat environment to manpower shortages in the field and remote workforces. But today's threat landscape is large and growing, as demonstrated by highly visible attacks against state and local agencies.

Automated threat detection and response solutions, and vulnerability management offerings can provide advanced analytics and response capabilities across endpoints, networks and cloud environments. Managed solutions enable a level of security that would be difficult to achieve even if an agency were able to hire sufficient IT security personnel. Once in place, a managed detection and response solution empowers the existing security staff to respond effectively when threats are identified, minimizing the risk of a cybersecurity event that can damage the organization.

Secureworks®

ABOUT SECUREWORKS

Secureworks is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

DELL Technologies

ABOUT DELL

Dell Technologies is a unique family of businesses that provides the essential infrastructure for organizations to build their digital future, transform IT, and protect their most important asset, information.

govloop

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop