Nine Questions

EVERY STATE & LOCAL CISO SHOULD BE ASKING

SECURING PUBLIC TRUST

Citizens trust government agencies to provide essential services while safeguarding a range of sensitive data, whether that data is related to taxes, elections, utilities or other broad-based PII.

The ability to protect systems and data from breaches varies among agencies, depending on security maturity, funding, policies, and technical resources. This is because, despite working tirelessly on core services, many state and local agencies are resource-constrained. And with ongoing efforts to modernize government IT and services, security may not always receive the prioritization or resources it needs.

Low maturity puts organizations at greater risk of a disruptive cyberattack, and studies show that cybercriminals are increasingly aware of this vulnerability. In 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware. And the average ransomware payment increased 171% from 2019 to 2020[1].

nearly

2,400

U.S.-based governments, healthcare facilities, and schools were victims of ransomware

increase of

171%

from 2019 to 2020 for the average ransomware payment

[1] IST Ransomware Task Force Report, 2020

Where do you begin to fix the gaps? While every agency is unique, many share common concerns.

Based on our experience helping state and local governments address their security challenges, Rapid7 has compiled a list of the 9 essential questions SLED security leaders should be asking.

Acting on these 9 primary challenges across people, process, and technology will help you shape **a security strategy that is lean, strategic, and compliant**.

01

PEOPLE

How do we demonstrate our threat exposure to leadership?

Some state and local executives underestimate the hard cybersecurity realities. Investing in staff or technology to correct deficient practices may seem low priority in the face of other pressing projects. It's essential to communicate—beyond infosec—the mission-critical role of security professionals, technology, processes, and compliance.

You'll need to demonstrate:

01

The organizational impact of a security incident, with facts on:

- The amount and nature of personal data you hold
- The length of service interruption a breach would likely cause
- The financial impact of shutting down services or schools
- Other relevant evidence-based projections

02

The frequency and financial impact of government breaches in your sector or state

03

Some stories about organizations that failed to address security and paid the price

Effective messaging helps everyone see why it's important to fund security, follow directives, and take secure procedures to heart in everyday work. The ultimate win is when your CEO and Board of Directors decide to take on oversight of infosec program strategy and goals.

RAPID7 CAN HELP

Keeping your organization aware of security goals, threats, and consequences can be a lot of work. All Rapid7 products make this easier by offering reports to document and communicate vulnerabilities, remediation progress, incidents, responses, and other critical updates. Because Rapid7 products are based on threat intelligence gained in real-world penetration tests, we can help you communicate realistic projections based on actual global incidents.

Read more about Rapid7's reporting features.

02

PEOPLE

How can we cover for shortages of skilled staff?

A global shortage of cybersecurity professionals means high competition for trained staff. The private sector’s ability to attract top talent through better compensation leaves many government agencies short, especially those with tight budgets.

Many team members have to wear multiple hats to cover both security and IT without specialized training. So how can you overcome the skills gaps and constant employee churn that is the norm in state and local agencies?

RAPID7 CAN HELP

Rapid7 managed offerings allow for seamless transitions without increased exposure when staffers leave and as new staff is onboarded. Rapid7 Managed Detection and Response supports security teams of all sizes and experience levels. It combines security expertise with technology solutions to quickly detect threats across your entire ecosystem, providing hands-on 24/7/365 monitoring, proactive threat hunting, effective response support, and tailored security guidance.

↓

Read more about Rapid7's **managed services**.

03

PEOPLE

How can we make security awareness training more effective?

More than 67% of breaches result from credential theft, phishing, email compromise, and errors[2]. So how do you strengthen the user weaknesses so well exploited by threat actors?

[2] Verizon Data Breach Investigations Report, 2020

Security awareness training can reduce the risk of socially engineered cyber threats by up to 70%[3]. But there's a difference between effective awareness training and the training carried out to check a compliance box. How can you ensure trainees are engaged, on board with your goals, and, most importantly, competent in their ability to recognize social attacks?

RAPID7 CAN HELP

Rapid7 offers classroom and online training to ground users in the basics. But like any skill, the real results come through practice. We can help you carry out internal phishing campaigns to train users in real-life situations. Getting duped by a phish provides powerful learning. We can help you track improvements in user behavior after successive campaigns to calculate your return on investment. You may never get a perfect result, but if you can get employees to spot phishing most of the time, you're doing well.

Read more about Rapid7's **security awareness training**.

[3] Aberdeen Group and Wombat Security Technologies, *"The Last Mile in IT Security: Changing User Behavior."*

04

PROCESS

How can we secure our cloud footprint?

The headlines we are seeing in today's security realm highlight issues that are not complex. Most cloud breaches today are simply a result of misconfigurations. These are more common in multi-cloud environments, especially with today's IT staff who tend to be less aware of security issues than in the past. Such missteps can easily allow attackers to access S3 buckets and other unauthorized resources.

RAPID7 CAN HELP

Using Rapid7's DivvyCloud technology, you can quickly scan through multiple cloud environments to spot misconfigurations.

Read more about Rapid7's DivvyCloud.

MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTRE (MS-ISAC)

Every U.S. state has different security regulations to comply with. Luckily, the MS-ISAC is there to set best practices, compare notes, and highlight who's doing it best among the nation's state, local, tribal, and territorial governments. Nothing like a little friendly competition in the effort to improve overall cybersecurity posture.

PROCESS

How do we map to multiple standards?

Access to federal and state funding often hinges on adhering to certain standards. Although state and local regulations vary widely across the country, the CIS Top 20 offers an effective master key. The CIS 20 is a prioritized set of best practices created to stop the most pervasive and dangerous of today's threats, developed by global experts and refined every year.

RAPID7 CAN HELP

In the 2016 ranking from SANS, Rapid7 was listed as the top solution provider addressing the CIS Top 20 Critical Security Controls. While your particular compliance frameworks may not have you moving in a straight line from CIS 1 to 20, implementing these critical security controls in any order is a solid way protect your organization from some of the most common attacks.

→ Read more about Rapid7's CIS compliance-related features.

GARTNER MAGIC QUADRANT SIEM REVIEW

In 2021, Rapid7 continues as a leader in Gartner's Magic Quadrant for Security Information and Event Management (SIEM), based on our vision and ability to execute.

06

PROCESS

How can we leverage automation to cover staff and technology gaps?

Lengthy budget, hiring, and procurement cycles can sometimes stall out your ability to detect and respond to incidents, leaving you exposed to a breach. Some agencies have found ways to maximize the staff and tools you already have through automated detection and response software.

RAPID7 CAN HELP

Rapid 7's Managed Detection and Response service offers round-the-clock monitoring and threat response, including integration with the open source community project Velociraptor. Velociraptor is an endpoint-monitoring, digital forensics, and incident response organization, and a professional community as well. It helps with response to potential intrusions in real time by quickly characterizing malicious technology and software, resulting in faster and more effective automated blocking.

FUNDING SECURITY

Because many government agencies struggle to fund anything beyond minimum operations, improving security can seem out of reach. But grant funding is often available for security objectives. In the U.S., you may be able to receive funds for services and technology through federal bodies like the Department of Homeland Security or Health & Human Services.

07

TECHNOLOGY

How do we keep our technology updated?

Government agencies tend to be cloud-averse, making it difficult for their security teams to adapt to new licensing styles. What's more, government's long procurement and budget cycles can mean technology is already outdated by the time the contract is approved. As a result, many public entities are far behind the curve of modern cybersecurity standards.

Engaging a cloud security service can help you overcome the problem of outdated technology because cloud technology is always the latest version. Your subscription ensures you only pay for what you use, letting you quickly scale up or down to meet demand while avoiding time-consuming internal procurement, development, and implementation processes. And all of those server rooms filled with outdated technology? Freed up for another use, minus the electricity and cooling costs.

RAPID7 CAN HELP

Rapid7 Insight Cloud gives you one-click access to vulnerability management, application security, incident detection and response, automation, and much more. Unite security, IT, and development teams and work faster (and smarter) together through visibility, analytics, and automation.

↓

Read more about Rapid7's **Insight Cloud security platform**.

TECHNOLOGY

How do we protect ourselves from ransomware?

The threat of a ransomware attack keeps many state and local IT, security, and executive team members up at night. Attackers target government agencies because they provide essential services like law enforcement, tax collection, and court proceedings and are more likely to pay a ransom to keep these necessary operations going at all costs.

Needless to say, ransomware has become one of the top attack vectors against governments. Not only can the impact be significant, but every ransomware story seems to make headline news.

RAPID7 CAN HELP

Rapid7 helps our customers create a solid cybersecurity plan to detect and respond to incidents, and train users to protect against phishing attacks. Educating users is the first line of defense in avoiding ransomware: basics like not clicking suspicious links or visiting websites with malvertising. In the event of an attack, a disaster recovery plan is essential. Being able to restore your data from backups will mitigate the damage done and allow you to maintain business as usual.

↓

Read our blog on **preparing for ransomware attacks**.

09

TECHNOLOGY

How do we secure BYOD?

In most organizations, employees use their own smartphones and tablets for work. While there are clear employee productivity gains, the negative by-product is a significant growth in data security risk. Many a breach has resulted from an employee logging onto the corporate LAN over hotel wifi or other casual use violations.

RAPID7 CAN HELP

Rapid7 InsightIDR combines the capabilities of SIEM, UBA, and EDR with your existing network and security stack to provide real-time detection of stealthy, malicious activity, even when users and endpoints are off the network. InsightIDR provides real-time endpoint data with user activity and log search for comprehensive incident detection across the entire attack chain.

→ See our BYOD infographic.

WHY RAPID7?

Rapid7's InsightCloud (InsightOne) is a complete range of security software and services that works together to cover all cybersecurity needs. We stay innovative and constantly aware through research and analysis of the attacker mindset. Experience with 7,400 organizations across 120 countries, including over half of the Fortune 1000, helps us look across industries and regions to get a complete global picture of risk. Our goal? To give you that inherently secure foundation on which to build constituent trust.

ON THE ROAD TO SECURITY MATURITY

Improving security is a multi-year process. A step-by-step, strategic approach is key: one where each phase in your maturity journey gets you closer to your end goal, with all elements working together and growing with you.

Fortunately, investments in security people, process, and technology can fall into different budget categories, with many governments offering grants to cover basic staffing, contracting, and technology needs.

Ultimately, your ability to protect constituent data and resources is the foundation of your organization's success. Effective security is your steady partner as you strive to offer more efficient, agile, digital, and strategic services to the people who rely on you.

→ **Read more at www.rapid7.com**