Responding to Real-Time Cyberattacks in Government

Research Brief

Symantec

DLT

govloop

Introduction

Ransomware. Election technology attacks. Breaches of citizen data. In a year that has seen multiple kinds of cyberattacks on government entities, it's now critically clear that cyberattacks in government are not a matter of if, but when.

Today, the public sector must accept that no government agency is immune to cyberattacks, and it's virtually impossible to stop every attack. It takes only one person to click a link and open a weaponized attachment in a malicious email, or one security vulnerability in the software supply chain to give hackers the advantage.

Agencies must be prepared and know how to respond to breaches.

But in today's environment, are agencies prepared to respond effectively to all types of cyberattacks, or do they face obstacles that make adequate response difficult, if not impossible?

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) can help agencies improve response preparedness. To learn how agencies are using the CSF to respond in real time to attacks, GovLoop partnered with DLT and Symantec for this report that analyzes survey responses of 150 federal employees working on cybersecurity challenges.

We've previously discussed the state of overall adoption of the CSF in government, as well as the perception and use of its Identify, Protect and Detect functions. But how is the federal government using the Respond function? Is it adequately responding to threats in a timely manner, or are challenges holding it back from rapid response?

In this report, we look at how agencies deal with critical cyberattacks, where they succeed and the challenges they face. We'll also gain insight from Ken Durbin, CISSP Senior Strategist of Global Government Affairs and Cybersecurity at Symantec, and Don Maclean, Chief Cybersecurity Technologist at DLT Solutions.

Why Federal Agencies Need a Response Plan

In May 2017, the president issued an executive order titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The fiscal 2019 budget also highlighted integrating cybersecurity into all aspects of IT modernization and prioritizing it at all agencies.

Additionally, in May 2017, OMB released a memorandum on reporting guidance for strengthening cybersecurity.

These documents stress that since breaches are inevitable, preparation and response are essential.

The cybersecurity response plan determines the outcome of a cybersecurity incident. Timely detection of the threat is paramount, but rapid response, analysis and containment can mean the difference between a large-scale breach and an ineffective intrusion. Everybody knows about the Office of Personnel Management (OPM) breach that took place in 2015 – which compromised the data of millions and caused both the director and the CIO of OPM to resign.

Additionally, the May 2018 report from the White House, the Federal Cybersecurity Risk Determination Report and Action Plan, determined that 71 of 96 agencies (74 percent) participating in its risk assessment process have cybersecurity programs that are either at-risk or high-risk – meaning they're very vulnerable to an attack.

Clearly, an effective response plan is necessary for the public sector. Let's look at our GovLoop survey results to gauge the effectiveness of response planning in government.

NIST Cybersecurity Framework: Respond

NIST describes its framework as consisting of "standards, guidelines and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security."

They state that, "The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident."

Examples of outcome categories within this function include:

- Ensuring response occurs during and after an incident
- Managing communications during and after an event with internal and external stakeholders, and law enforcement
- Analyzing the incident to ensure effective response and support recovery, including forensic analysis, and determining the impact of incidents
- Rapid mitigation to prevent expansion and to ensure resolution of the incident
- Incorporating lessons learned from current and previous detection/response activities, to promote continuous improvement

The State of Response: Survey Results

We asked 150 federal employees who deal with cybersecurity at their agencies if they have a response plan, if that plan is effective and what challenges they face in expanding and using these plans.

The biggest takeaways? Only half of the federal respondents knew if a response plan was in place at their agency. Those who were aware of response plans at their agencies, however, found them almost uniformly effective. Others yet said they still faced many obstacles to creating an effective plan: getting the right technology, finding personnel with the right skills, implementing the right procedures and communications, and more.

We also discovered the following takeaways: A large percentage of respondents do not have response plans at their agencies or are not aware of them. Some of the reasons? Lack of training, political issues or lack of prioritization. Awareness in general about response plans and the legislation and guidance around them is low, and some struggle with securing the right technology to put in place for response efforts.

Those who do have response plans in place, however, find them indispensable. Respondents uniformly cited them as useful, especially when tested regularly.

Ideas for progress include better testing, looking to data loss prevention technology and more education on metrics and legislation around the issue.

Let's take a closer look.

Although a response plan is as critical as detection, only 52 percent of the respondents said their agency had a response plan in place (See Figure 1).

Since cyberattacks are rampant and there are mandates and frameworks around creating response plans, what stops agencies without response plans (18 percent, according to our survey respondents) from creating one?

Respondents cited a variety of challenges that inhibit plan creation. The top challenge was lack of skills (33 percent), and "Not a priority" and "My organization is too small" were factors for 15 percent of our respondents (See Figure 2).

Figure 1

Do you have a response plan for cyberattacks in place at your agency?

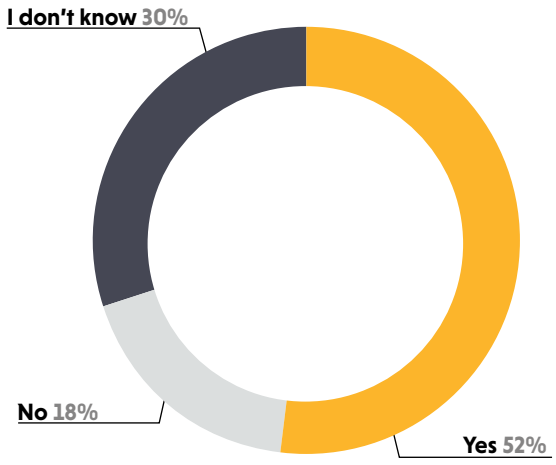
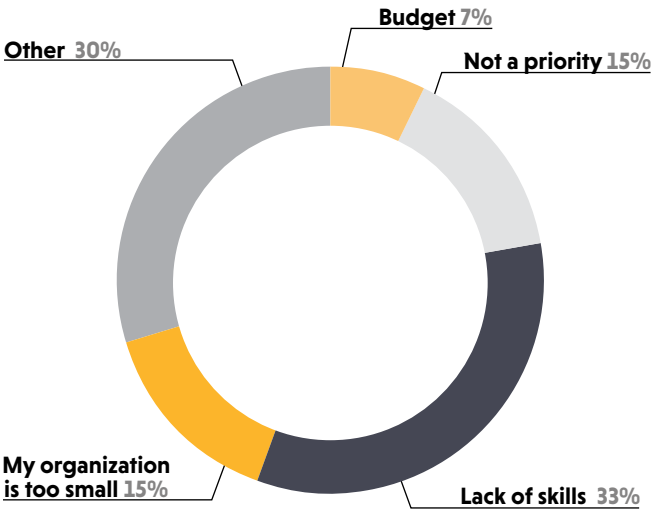


Figure 2

If no, what's preventing your organization from implementing a response plan?



Many others described more complex reasons for their agency's lack of a response plan:

- Inexperience in drafting a reasonable response plan.
- Lack of training, education, professional research and other knowledge.
- Lack of funding and direction.
- Former chief was in the process of updating our system, including security. Upon his leave, the program was scrapped.
- My agency's cyberspace is protected by another.
- government agency charged with that responsibility Politics.
- Budget, staff, lack of knowledge and understanding re: necessity from superiors.

According to our survey, inexperience and lack of training combined with a general lack of awareness of response plans and the mandates and legislation informing cybersecurity responses create this situation. Nearly 60 percent of respondents who did have a plan in place at their agencies did not know if it was informed by the NIST Cybersecurity Framework (See Figure 3). Of those whose response plans do not follow OMB guidance, (43 percent, see Figure 4) 56 percent said they did not know the OMB memorandum even existed (See Figure 5).

Looking at the lack of awareness from survey respondents about response plans in general and whether the response plans were informed by the Cybersecurity Framework or the OMB memo, Maclean focused on the importance of awareness and education around cybersecurity response for all employees of an agency, not just the IT team.

"Response plans and the way they are tested and communicated should include a representative of the end user community, to make sure that that they're aware of the plan, and know results," he said. "Think about a fire drill. You don't conduct that drill with just half of the people in the building, right?"

Maclean also noted stakeholders cannot test or execute a plan if they are not aware of it. As the following responses show, testing response plans is a critical part of an effective overall strategy.

Figure 3

If yes, is that response plan informed by the NIST Cybersecurity Framework 1.1 "Respond" function?

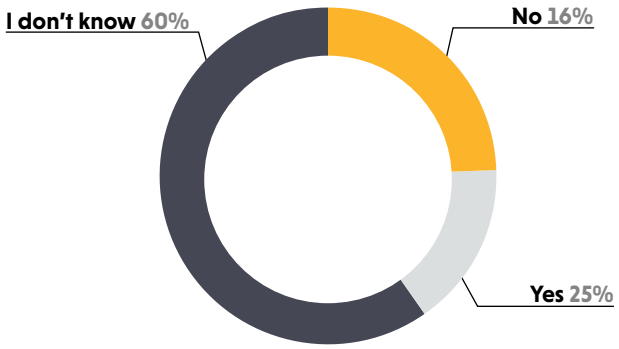
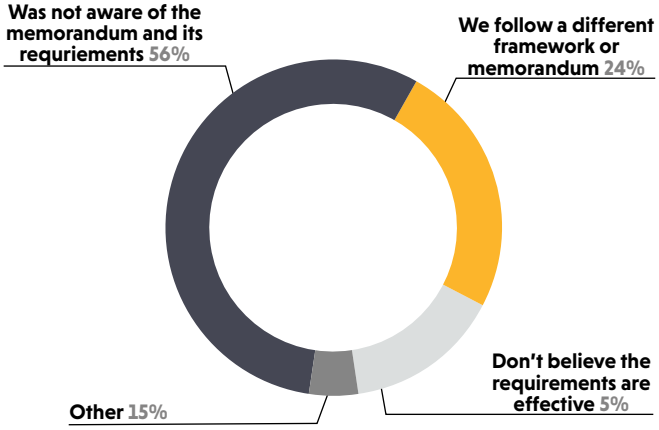


Figure 4

In May 2017, OMB released a memorandum on reporting guidance for strengthening cybersecurity, including instructions on how to report back on response plans in the case of a cyberattack. Are you following the requirements of this memo?

Figure 5

If no, why not?



Our survey validates this point: Of those who have used a response plan during an attack (71 percent, see Figure 6), a whopping 96 percent found the response plan effective (See Figure 7).

This result did not surprise Durbin and Maclean. Without a well-defined incident response plan to supplement prevention, security will be insufficient at data centers and critical facilities, they noted. "Merely having a response plan and executing on it is a huge step that will almost certainly help mitigate the attack when you follow it," Durbin said.

Repeated testing makes a response plan even more effective, they said; survey respondents agreed. Seventy-three percent said they had tested their response plan prior to their latest incident (See Figure 8), and an astounding 100 percent said testing improved their organization's response capability real time (See Figure 9). Finally, 100 percent of survey respondents firmly believed that continued testing of response plans would facilitate their agency's ability to continue to respond effectively to future incidents (See Figure 10).

Figure 6

If you have a response plan in place, was it used in responding to an attack you've had at your agency?

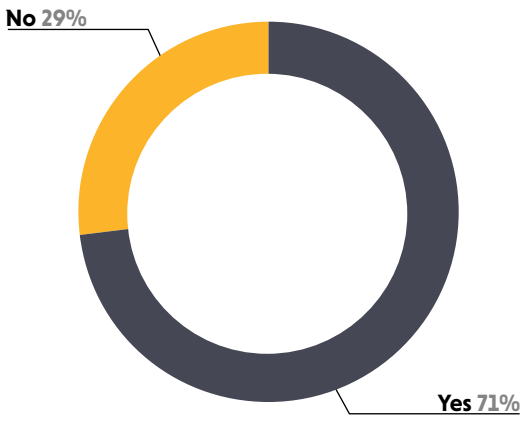


Figure 7

Was your response plan effective when used in responding to an attack?

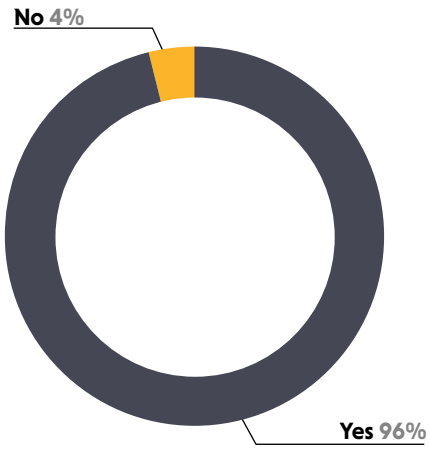


Figure 8

Did your organization test its response plan prior to your most recent incident?

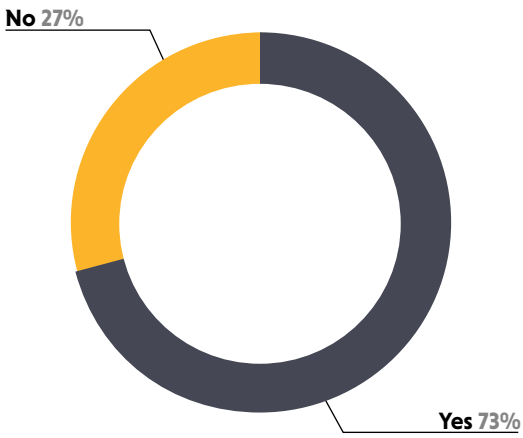


Figure 9

If yes, did the testing improve your organization's ability to respond?

Yes 100%

Figure 10

Do you believe testing will facilitate your organization's ability to respond to future incidents?

Yes 100%

"Phishing emails, tabletop exercises, gamifying testing – all of these are great ways to test a response plan," said Durbin. "Of course, a true test of a response plan is how useful it is during a live attack. But you can't wait for a live attack. That's why testing is crucial to your readiness."

Testing isn't the final item in a successful response plan. Analyzing how a response went, debriefing it with stakeholders afterward and creating a "lessons learned" document are crucial to continuous improvement. Nearly 57 percent of respondents, however, had not identified and disseminated lessons learned – a huge missed opportunity (See Figure 11).

This means that far too many agencies are missing chances to improve their response postures when they do not debrief after an attack. "When you document what you've learned from an attack, then you can go back and improve your defenses to keep that kind of attack from happening again," said Durbin. "If people failed a phishing exercise, and you don't go back and let them know that they failed, and understand why they failed, it's going to severely limit your ability to protect yourself when that event happens again."

Figure 12 shows responses from those whose agencies did implement lessons learned debriefs – and what they learned from it.

Lessons learned debriefs and testing are important, but success metrics are critical, too.

"The standard measurements for response plans are items like recovering point objective and recovery time objective," said Maclean. "These are basic measurements about how much data did you lose and at what time did you detect and respond? In other words, can you recover as of yesterday at 6, can you recover as of today an hour ago? Similarly, what's your maximum downtime and were you actually able to stay within those limits?"

"You can't be successful if you don't have metrics with which to measure your success," Durbin said.

Figure 11

Did your organization test its response plan prior to your most recent incident?

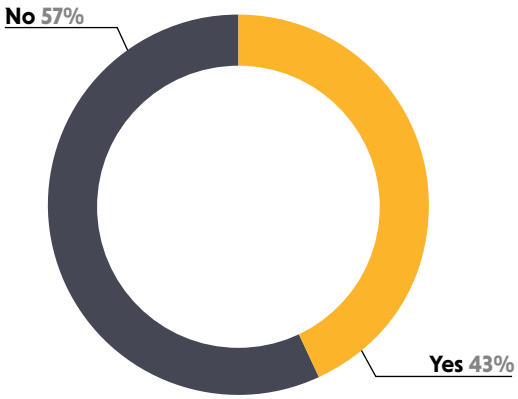


Figure 12

We asked our survey respondents to share their agency's lessons learned after incident debriefs. This is what they said:

- **Identify the training of staff to better thwart attacks, vishing/phishing episodes have been thwarted in the past.**
- **Continued education regarding thoughtful attention when clicking hyperlinks.**
- **Not to open emails where the sender asks you to click on a .exe link or where you are asked for personal information.**
- **I know there was a meeting held and the IT staff were to receive incident command training as a result of the meeting. I suspect there was a report compiled but it was not shared with our agency.**
- **To pay particular attention to email addresses to avoid phishing.**
- **Behavior on the part of system users is the weakest point in the agency's security.**
- **It is important that everyone knows and understands their role during the response.**

Only 50 percent of survey respondents, however, measure their attack response, missing another opportunity for response plan improvement (See Figure 13).

Maclean and Durbin suggest one final component of a successful response plan: a plan that includes correct technology, and also has good procedures and excellent communication.

"You need the right technology to support your procedures," said Durbin. "They're incredibly intertwined."

Our survey respondents agreed, with 45 percent citing procedure as important and 39 percent saying technology was. Sixteen percent wrote in saying that both were critical to their success (See Figure 14).

Fortunately, the majority of survey respondents (61 percent) felt they had the right technology in place at their agencies (See Figure 15).

What about the 39 percent who lack the right technology? They had a clear vision for what would help them succeed: primarily, data loss prevention technology to better track high-value assets (See Figures 16 and 17).

The right technology for data loss prevention can mitigate damage:

- Control who can use data, even from unmanaged locations or devices
- Define what level of access a user has using persistent encryption and digital rights
- Monitor user access to sensitive data to identify risky be havior or security compromises
- Revoke access to users, effectively digitally shredding a document

These abilities are critical when you suffer an attack or breach where bad actors compromise and share your data.

Figure 13

Are you working to measure and rate your response to attacks in order to improve?

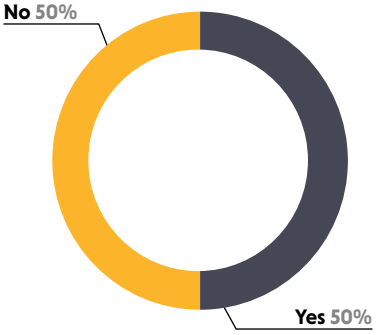


Figure 14

In your opinion, is a strong attack response plan more about the technology that's in place or the procedural steps listed out?

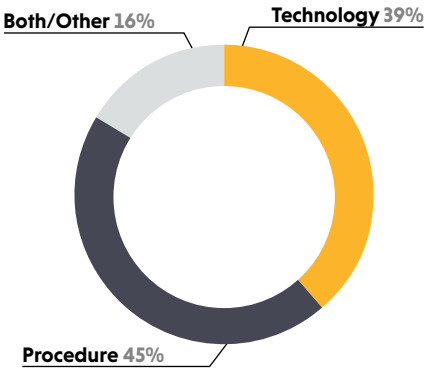


Figure 15

Do you feel you have the proper technologies in place at your agency to respond to attacks?

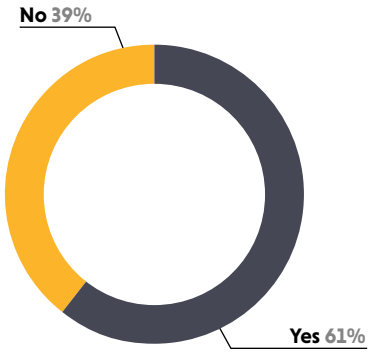


Figure 16

If no, what technologies do you feel would help you better address your response to threats and attacks?

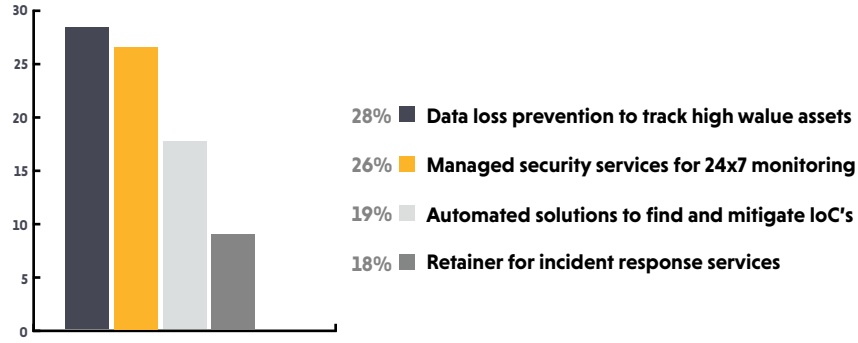
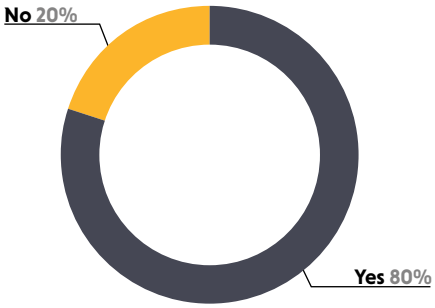


Figure 17

Do you believe that a Data Loss Prevention (DLP) system would enhance your organization's ability to respond more effectively to incidents by clearly identifying exfiltrated data?



Best Practices for Your Response Plan

To help those creating and executing response plans, a few best practices that can start them on the path:

1. Assess the Situation: Do you already have a response plan in place at your agency? If so, does it need an update? If not, creating a plan is critical.

2. Create Your Plan: As our survey showed, response plans are not necessarily in place throughout government. If your organization lacks a solid, formal plan, the first step is to put a good one together.

3. Define an "Incident": It may seem obvious, but the first step in building an effective incident response plan is recognizing what actually constitutes an "incident," then categorizing incidents by type and severity. NIST and OMB provide guidance on what constitutes an incident and a major incident; make sure your agency has read and applied these.

4. Keep the Plan (and Supporting Documentation) Up to Date: Response plans quickly become outdated as people move organizations, phone numbers change and definitions and compliance procedures progress. Regular updates to your network documentation and incident response plan will minimize confusion in a crisis.

5. Test Your Plan Often: Of the respondents who did have an incident response plan in our survey, nearly a third were not testing the plan after its creation. An untested plan may create a false sense of security. Tabletop exercises – meetings to discuss simulated emergencies – can solidify your plan.

"In theory, the best way to test a response plan is to actually implement an incident," Maclean laughed. "But nobody really wants to do that. So testing remains critical."

6. Involve the Right People – Including Non-IT Personnel: When conducting drills, core members of the team must participate, but the team must include others. Senior leadership, end users, program managers and public affairs representatives also play a big role. Develop these relationships now, and responding to an incident will be much easier.

"As they say in real estate, there are only three things that matter: location, location, location," said Maclean. "In the business of response plans, the only three things that matter are communication, communication, communication. Is your communications team and leadership team involved in external and internal communication for your response plan? They must be."

7. Have a Post-Incident Action Plan: A lessons learned debrief should be part of your post-incident process every time. What went well? What went poorly? What needs improvement? Document these discussions with stakeholders and update your response plan accordingly.

"A response plan should take into account analyzing what happened," Durbin said. "Then you can incorporate those lessons learned into your defense to be even stronger for next time."

8. Look to Data Loss Prevention (DLP) Technology: Sensitive information is leaving the safety of your network as more employees share files through cloud storage services and access those files on personal mobile devices. A strategy for data loss prevention is a comprehensive approach to information protection that embraces the realities. With a solid data loss prevention strategy, you can discover where data is stored across all of your cloud, mobile, network, endpoint and storage systems; monitor data usage; determine if employees are on or off the network and protect data from leakage or theft.

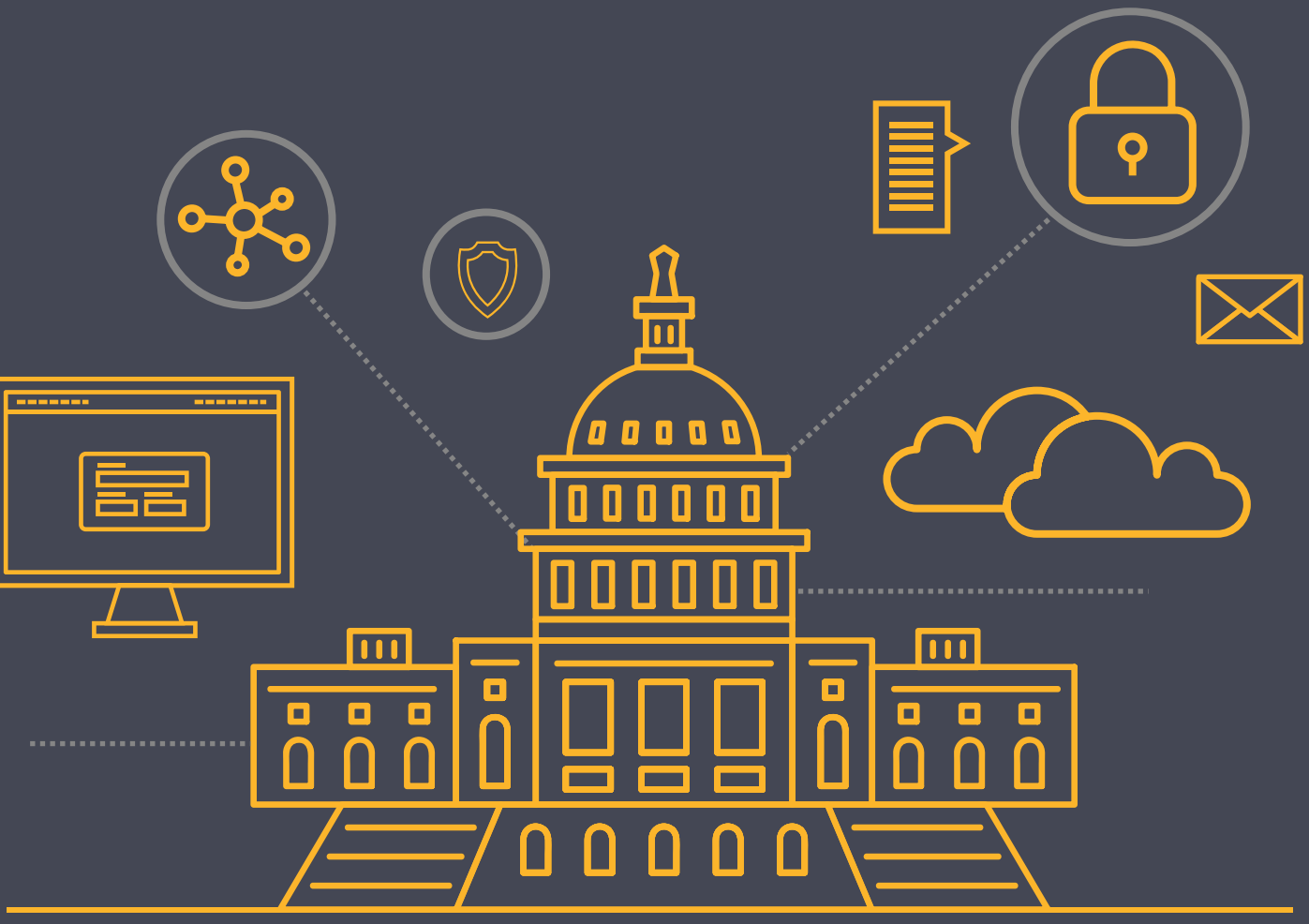
9. Partner With the Right Vendor: A partner that can critically assess your response capability journey and help move you to the next step, as well as assess your data loss prevention strategies and technology, is important.

How DLT + Symantec Help

Symantec and DLT can help you respond effectively to attacks of any shape or size and continuously assess and manage your cyber posture, while making the most out of the NIST Cybersecurity Framework.

Symantec and DLT help federal customers understand and manage the latest threats to better identify, protect, detect, respond to and recover from advanced attacks. Symantec's tools and comprehensive solutions make it easy for government agencies to discover what is in their network and continuously access and manage their security posture.

In particular, Symantec Data Loss Prevention can identify sensitive data and uses a variety of advanced data detection techniques to identify data in many forms. Its technologies identify regulated data and track its use and location while its protection policies regulate the flow of sensitive data. It can encrypt email, removable media, individual files and data in the cloud.



Conclusion

Today, the federal government faces untold numbers of attempted data breaches each year, and the reality is this: Sometimes the hackers get in. Even as agencies strengthen their cybersecurity vulnerabilities and work at faster, better detection, they must be ready to respond when inevitable breaches occur. A proper incident response plan can be the difference between calamitous damage from compromised data and harmless trespassing.

By investing in a response plan that has the right technology and the right procedures, agencies can minimize damage from inevitable breaches. Symantec and DLT work with agencies to create a comprehensive and resilient cybersecurity strategy – with full visibility from the cloud to the network edge to the endpoints – to secure information and the infrastructure in which it lives. Their technologies prepare your teams to respond to the latest attacker tools, techniques and procedures.

Agencies cannot prevent every incident, but with a solid response plan, you can minimize the negative impact of incidents and save your agency's time, money and reputation.

About Symantec

Symantec helps federal agencies develop and implement comprehensive and resilient security strategies to reduce risk and meet Cross-Agency Priority Goals, the NIST Cybersecurity Framwork, the Joint Information Environment and other federal mandates.

Learn more at: www.symantec.com.

About DLT

For 25 years, DLT Solutions has been dedicated to solving public sector IT chal- lenges.Guided by our relentless focus, we have grown to be one of the nation's top providers of world-class IT solutions. Leveraging our strategic partnerships with top IT companies, we develop best- fit solutions for our customers. Our sales, integration, and support experts have the certifications and experience in helping customers at any level of any agency. We have both deep subject matter expertise and in-depth knowledge of government mandated requirements and initiatives in areas such as a cloud computing, cyber- security, and consolidation.

Learn more at: www.dlt.com.

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 270,000 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