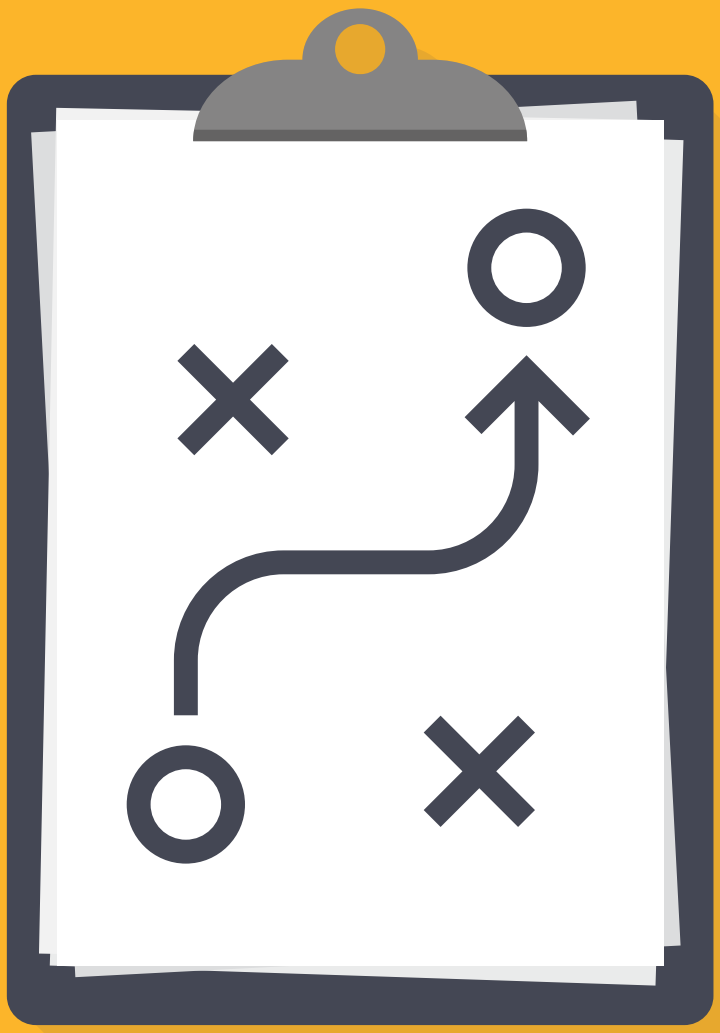
The Plan for Recovering from Cyberattacks in Government Today

Research Brief



DLT Symantec govloop

Introduction

If there is one lesson to learn about cybersecurity from the past decade in government, it's that a cyberattack is not a matter of if but when one will happen.

Cyberattacks are a serious threat to our economy and national security. Government agencies need to be able to detect, defend and respond to threats immediately, and quickly bounce back from cyber incidents, whether they are the result of an accident, natural disaster or malicious attack.

Often, after defending, detecting and responding to an attack, recovery is an afterthought – if it's considered at all.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) can help agencies improve recovery abilities. To learn how agencies are using the CSF to recover from attacks in real time, GovLoop partnered with Symantec and DLT for this report that analyzes survey responses of 169 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, Detect and Respond functions.

How is the federal government using the Recovery function? Is it adequately recovering from threats in a timely manner, or are challenges holding it back from strong recovery and lessons learned?

In this report, we look at how agencies recover from 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, CISSP, Chief Cybersecurity Technologist at DLT Solutions.

The Importance of a Recovery Plan Today

On May 11, 2017, the president signed the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which outlines actions to enhance cybersecurity across federal agencies and critical infrastructure partners, including guidance on how best to respond to a cyberattack. The fiscal 2019 budget also highlighted integrating cybersecurity in all aspects of government technology.

But even though it's in the president's Executive Order and is a requirement, federal agencies often overlook the recovery step of a cyberattack. Given all the energy that agencies must put into detecting, defending and responding to an attack, this omission is understandable, but today more than ever, recovery is critical.

"Think about a fire in your house," said Durbin. "You do many things to protect your house from a fire, such as installing smoke alarms. If a fire does take place, you know how to respond by planning an exit strategy, and putting the fire out. But have you considered the steps for recovery? Is the house livable? Can you still use it? How will you better stop the fire next time? That's where recovery comes in."

Developing a recovery plan and adhering to it is critical for agencies, because this function seeks to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that a cybersecurity event has impaired. It also supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

"It's not enough in a cybersecurity incident just to respond and do immediate triage," said Maclean. "You need to get back to normal, and you need a plan for future recovery so you're not just making it up as you go along – which could eventually make you susceptible to another cyberattack down the road."

NIST Cybersecurity Framework: Recover

NIST describes its framework as "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."

NIST states that, "The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident."

Examples of outcome categories within this function include:

- Ensuring the organization implements recovery planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents
- Implementing improvements based on lessons learned and reviews of existing strategies
- Internal and external communications are coordinated during and following the recovery from a cybersecurity incident

The State of Recovery: Survey Results

We asked 169 federal employees who self-selected as working in and around cybersecurity efforts at their agency if they have a recovery plan, if that plan is effective and what challenges they face in expanding and using these plans.

The biggest takeaways? Communication about recovery plans is sorely lacking at agencies, as many respondents were unsure if their agency even had a recovery plan. Obstacles to communication or creating a recovery plan stemmed from lack of leadership buy-in. Additionally, only 39 percent confirmed that if they had a recovery plan, NIST's Cybersecurity Framework informed it.

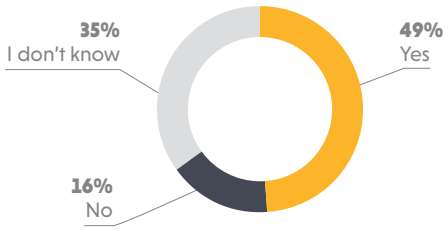
We also discovered the following takeaways: Those who do have a recovery plan and are aware of its existence almost uniformly said it was useful and that they are testing it regularly. In addition, and more critically, a majority of respondents cannot offer credit monitoring or equivalent protection for those affected by a breach – a key element of a recovery plan, and a potential area of concern.

Let's take a closer look at the results of the survey.

Though many in government realize that a recovery plan is critical to a holistic cybersecurity approach, only 49 percent of respondents said their department had one. Thirty-five percent were not even aware *if* such a plan existed. (See Figure 1)

FIGURE 1

Does your department have a recovery plan for cyberattacks in place?

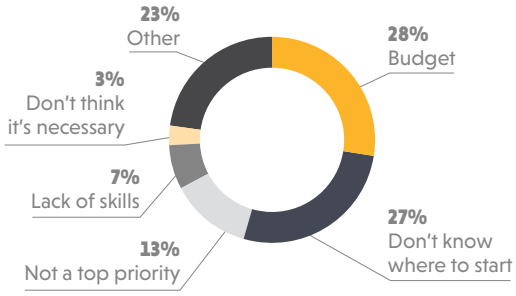


"To me, this speaks to a need to have a better communication plan around a recovery plan and its importance," said Maclean. "This statistic could indicate that the agency has a recovery plan, but only certain people know about it, and this means they've missed the best practice of constant communication." (For more best practices around a recovery plan, see Page 7.)

Those who did not have a recovery plan said there were many reasons preventing one from forming, with budget (28 percent) and simply not knowing where to start (27 percent) coming in at the top. (See Figure 2)

FIGURE 2

If no, what's the biggest reason preventing your organization from having one?



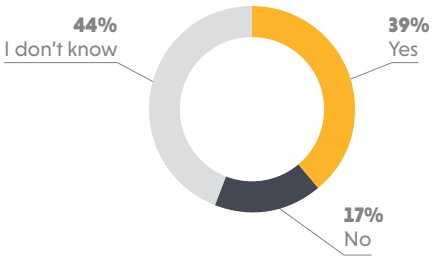
"Budget comes from leadership," said Durbin. "Leadership must first realize that creating a framework for recovery is crucial. If you don't have buy-in at that level, it can be hard to move forward."

In terms of getting started, Maclean noted the many resources available to departments. "NIST has a lot of great documentation that shows you how to start, and walks you through the complete lifecycle of a recovery plan," he said.

Of those who did have a recovery plan at their agency, 39 percent said it was informed by NIST's Cybersecurity Framework, whereas 17 percent said it was not, and 44 percent simply didn't know. (See Figure 3)

FIGURE 3

If yes, is the recovery plan informed by the NIST Cybersecurity Framework Recover Function?

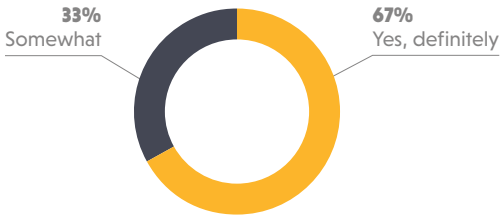


Maclean said that he actually sees the 39 percent as a hopeful sign that more and more agencies are using the NIST Cybersecurity Framework. "In my opinion, the framework is a relatively straightforward piece of documentation and an approach to security that is gaining traction more quickly than expected. Agencies saw it as an extra piece of work at first, but now it's doing quite well."

We then asked survey respondents who had used their recovery plans in the last year if they were actually useful. The answer was overwhelmingly "yes": 67 percent said the recovery plan was "definitely useful," while 33 percent said it was "somewhat useful" and zero respondents said it was of no use. (See Figure 4)

FIGURE 4

If yes, was the recovery plan effective?



That said, a recovery plan is only useful if you are testing it frequently. Fortunately, 69 percent of survey respondents said they are regularly testing the recovery function on a consistent basis. (See Figure 5)

FIGURE 5

If your agency has a recovery plan, does your department test the recovery function on a regular basis?

"It's absolutely important to test a recovery plan," said Durbin. "When you go to use it in real time, you do not want to find out at that moment you've missed something or it is defective."

A recovery plan is also only truly effective and comprehensive when it provides guidance on how to recover from the three major types of breaches: breaches of confidentiality; breaches of integrity; and breaches of availability. Confidentiality, integrity and availability, also known as the CIA triad, is a model critical to guide policies for information security within an agency to make sure all bases of security and recovery are being covered.

When asked if their recovery plan covered all three of these types of breaches, 55 percent said yes; 25 percent said some but not all; and 20 percent said none. (See Figure 6)

FIGURE 6

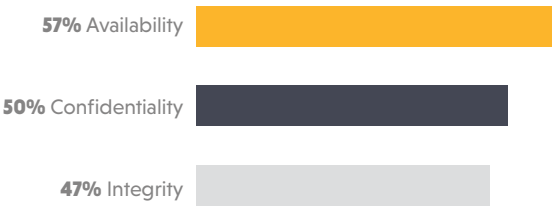
Does your recovery plan include recovery from all majority type breaches: Confidentiality, Integrity, Availability?

THE CIA TRIAD

When asked if their recovery plan only covered some types of breaches, 57 percent said their plan covered availability; 50 percent covered confidentiality; and 47 percent covered integrity. (See Figure 7)

FIGURE 7

If some breaches, which ones?

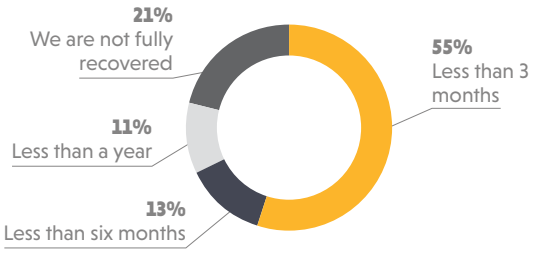


"It's critical to know what kind of breach is taking place and that your recovery plan accounts for it," said Maclean, "otherwise it will be very difficult even to start the recovery process. You can't recover without knowing the nature of the breach."

Ideally, with comprehensive recovery plans in place, agencies will see quicker recovery times from the attacks they do suffer. When asked: "If your agency has experienced a cybersecurity incident in the past year, how long did it take to recover from it?" the trend shows improvement in recovery time: 55 percent said it took less than three months to recover; 13 percent said less than six months; 11 percent said less than a year. But 21 percent did note they are not yet fully recovered, perhaps indicating that they suffered a particularly heinous cyberattack. (See Figure 8)

FIGURE 8

If your agency has experienced a cyber incident in the past year, how long did it take to recover from it?



Maclean views this information as a positive trend for federal cybersecurity. "It is true that these recovery times may be longer than we'd like to see, but this is improving overall," he said. "It used to be that dwell time and recovery time could take years in the federal government. Overall, I believe we are slowly but surely seeing some progress and improvement in federal security resilience."

Recovery isn't just about how the agency is affected, however. Oftentimes in breaches or attacks, citizen data is compromised, and agencies must be able to offer protection to them, particularly if the data is personal or financial. When asked, "In the case of stolen or breached personally identifiable information (PII), do you have the ability to offer credit monitoring or equivalent protection for those affected?" only 37 percent said they could offer this resource to citizens; 63 percent said they could not. (See Figure 9)

FIGURE 9

In the case of stolen or breached personally identifiable information (PII), do you have the ability to offer credit monitoring or equivalent protection for those affected?

Agencies must offer this sort of support to citizens and civil servants affected by data breaches. First of all, it's a federal requirement, and second, citizens and civil servants continue to believe the agency has their best interests and protections in mind. "If you have an attack but neglect to notify and help the affected people take steps to protect themselves, then anything that happens to them is a continuation of the attack that happened on the agency," Durbin noted.

Finally, agencies cannot have effective recovery plans if the following measures aren't in place:

- The proper technology
- Metrics to measure and improve recovery after an attack
- Enterprise-level plans for business and incident response or continuity of operations

When asked about these items, 72 percent of respondents said they think they had the proper technology in place (see Figure 10); 65 percent said they were measuring and rating recovery from attacks (see Figure 11); and 65-76 percent had disaster recovery, incident recovery and/or continuity of operations plans in place (see Figure 12).

FIGURE 10

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

FIGURE 11

Do you measure and/or rate your recovery from attacks in order to improve?

FIGURE 12

Which, if any, plans does your agency have available at the enterprise level? (check all that apply)

76%
Business continuity/ continuity of operations plan

72%
Incident response plan

65%
Disaster recovery plan

Best Practices for Your Recovery Plan

To help those creating and executing recovery plans, or to even make your recovery plan more effective, here are some best practices to follow.

Generally prepare for resiliency:

Focusing on the overall resilience of your enterprise cybersecurity posture is a smart first step in aiding your recovery plan. The DHS Risk Lexicon defines resilience as the "ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions." According to NIST's Guide for Cybersecurity Event Recovery, "Taking resiliency into consideration throughout the enterprise security lifecycle, everything from planning technology acquisitions based on standards-based systems engineering processes as described in the NIST SP 800-160 and developing procedures to executing recovery and restoration efforts, is critical to minimizing the impact of a cyber event upon an organization."

Identify key people:

You can't recover from an attack without having an understanding of the key personnel who are critical to the protocol. Make sure to identify and document the key roles and people who will be responsible for defining recovery criteria and associated plans, and ensure these individuals understand their roles and responsibilities.

Measure, measure, measure:

"Determining ahead of time the metrics that define a successful response is key so that you can measure and improve and go forward knowing you can do a better job next time," Maclean said. Some potential metrics include the time it took to recover; the number of business disruptions due to the incident; damages such as loss of brand reputation or trust from the release of citizen data; or financial metrics. Your metrics may vary according to your priorities, which is why it is important to determine them ahead of time.

Communication is key:

Communication during and after a recovery effort is more critical than you might suspect, both with internal employees and external users. Your agency must develop a comprehensive recovery communications plan. The plan should go over recovery communication goals, as well as discussing information-sharing rules and methods.

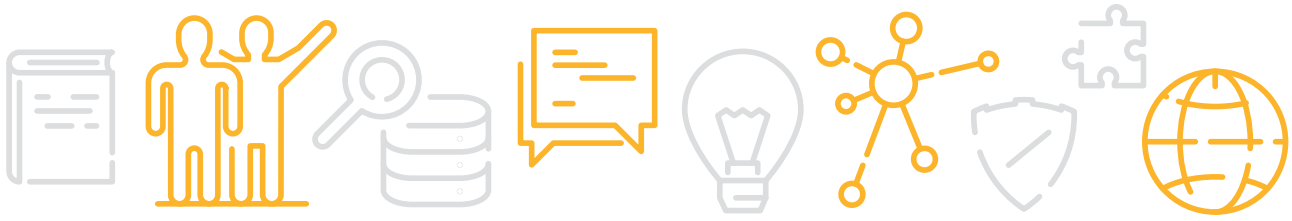
"Communication to users, to assure them that things are under control and will be back to normal is key," said Maclean. "That may include both logistical communication and also technical issues. The users need to know what kind of workarounds they might have to be struggling with until you're back to normal."

Share insights:

Post-recovery, you must decide: Will you share information that you learned about the attack or breach with others? "Are you going to help out others in the community avoid or respond to this kind a breach?" asked Maclean. "Will you share intelligence? Whatever you might have learned, you want to share that appropriately, but there may be times when you don't want to share what happened because that could compromise your operations. That all needs to be identified ahead of time."

Review lessons learned and identify improvements:

Agencies should also identify improvements from lessons learned during cyber event recovery actions. These lessons help drive improvements not only to recovery itself, but also to the organization's security operations, policies and more.



Additionally, OMB Memorandum M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, and the FY 2019 FISMA CIO Metrics report, name the following best practices for the Recovery function:

Plan and test:

As in the case of incident response, a strong incident recovery program requires advanced planning of activities as well as testing of those plans to ensure they execute properly. This enhances agencies' ability to restore capabilities and/or services following an incident or disaster. This means, in part, that the organization has a business continuity plan at the enterprise level that is tested annually; an incident recovery plan at the enterprise level that is tested annually; and a disaster recovery plan at the enterprise level that is tested annually. As Durbin noted, "Your recovery plan can't be something that you write and then put on a shelf; you have to rehearse it and update it when necessary."

Follow personal impact processes:

For those cases in which personally identifiable information has been, or potentially could have been compromised, it is imperative that organizations have in place capabilities to notify affected persons and provide them with necessary identification protection tools and/or services. This ensures that agencies are providing potentially affected persons with timely information and identity protection tools, which helps to preserve public confidence in the government.

Ensure your agency's backup capacity:

If an organization loses the capacity to execute its mission, whether due to an incident or a disaster, it is important that back-up facilities and capabilities have been designated and are prepared to come online. Such capabilities enhance organizational resilience and aid in the restoration of agency capabilities and services. This means that the organization has identified, through risk assessments, alternate processing and storage sites that are not subject to the same physical and/or cybersecurity risks as the primary sites.

As the FISMA metrics report points out, "The goal of the Recover metrics is to ensure that agencies develop and implement appropriate activities for resilience that allow for the restoration of any capabilities and/or services that were impaired due to a cybersecurity event. The recover function reduces the impact of a cybersecurity event through the timely resumption of normal operations."

Partner with the right vendor:

A partner that can critically assess your recovery capability journey and help move you to the next step is imperative. Given the complexity of government operations and environments, you need vendors who are subject-matter experts across a broad portfolio of the IT issues that government deals with on a daily basis, with technical expertise, product knowledge, systems integration and the right recovery technology.

How Symantec & DLT Can Help

Symantec and DLT can help you effectively recover from 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, manage and recover from advanced attacks. Symantec's tools and comprehensive solutions make it easy for government agencies to not only discover what is in their network but to continuously access and manage their security posture.

In particular, Symantec cyber services include a wide range of tools and skills to aid in the recovery step of the aftermath of a cyber event. They offer performance SLAs to ensure critical resources are available when you need them; documentation of response actions and recommended post-incident improvements; and post-incident technical and management briefings and lessons-learned sessions.

Conclusion

The best way to stop a cyberattack is to prevent it from taking place in the first place, but the reality is that the level of sophistication and persistence among today's hackers often negates this strategy. Attacks will happen, and agencies must focus on more than the detect and defend aspects of the NIST Cybersecurity Framework in order to make sure they are taking a comprehensive approach to cybersecurity.

In particular, the ability to recover quickly from a cyberattack is imperative. When agencies focus on holistic cybersecurity, including recovery, then their ability to carry out the necessary recovery actions quickly can help reduce the overall impact and prevent damage to the government's mission, data and reputation.

About DLT Solutions

For 25 years, DLT Solutions has been dedicated to solving public sector IT challenges. 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, cybersecurity, and consolidation.

Learn more at: www.dlt.com

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 Framework, the Joint Information Environment and other federal mandates.

Learn more at: www.symantec.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 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