# A ROADMAP TO INTEGRATED CYBER DEFENSE IN GOVERNMENT

## A NEW APPROACH STRENGTHENS CYBERSECURITY AND MAKES BETTER USE OF BUDGET AND STAFFING.

Cybersecurity has been a top issue for public sector IT leaders for many years, but the rapidly evolving – and persistent – nature of threats is garnering the attention of government executives and elected officials. In many cases, the concern comes from firsthand knowledge of security risks. A Center for Digital Government (CDG) survey of 160 state and local officials found agencies had experienced several types of serious cybersecurity attacks, including phishing (76 percent), malware (58 percent), hacking attempts (43 percent) and ransomware (37 percent).

This new era of cyber threats is raising questions about whether current security measures are adequate. The CDG survey, underwritten by Symantec, uncovered four key concerns among government leaders about the state of cybersecurity in their organizations.

The biggest concern is whether their internal networks, applications and cloud infrastructure are adequately protected. They are also concerned about their ability to detect network intrusions, and whether their employees have enough security training and awareness. When threats arise, survey respondents aren't fully confident in their organization's capabilities for incident response.

This paper will discuss these concerns in more detail and present a new approach to help governments overcome vulnerabilities and tackle cybersecurity enterprise-wide.

## How Well Is Government Prepared for Growing Cyber Threats?

There are several challenging dimensions of IT that contribute to public sector cybersecurity concerns. Many government agencies must contend with outdated infrastructure. In some cases, they have implemented siloed security solutions that cannot be scaled or integrated to protect the enterprise as a whole. Adequate staffing is another common challenge. The government workforce is aging and agencies find it difficult to compete with the private sector for new talent.

But the top challenge? Budget constraints – cited by 60 percent of CDG survey respondents. Unfortunately, budget shortfalls mean agencies often invest in cybersecurity solutions only after they experience a data breach, system disruption or ransomware attack. The impact of such a disruption, especially when public disclosure is required, creates an awareness of business risk.

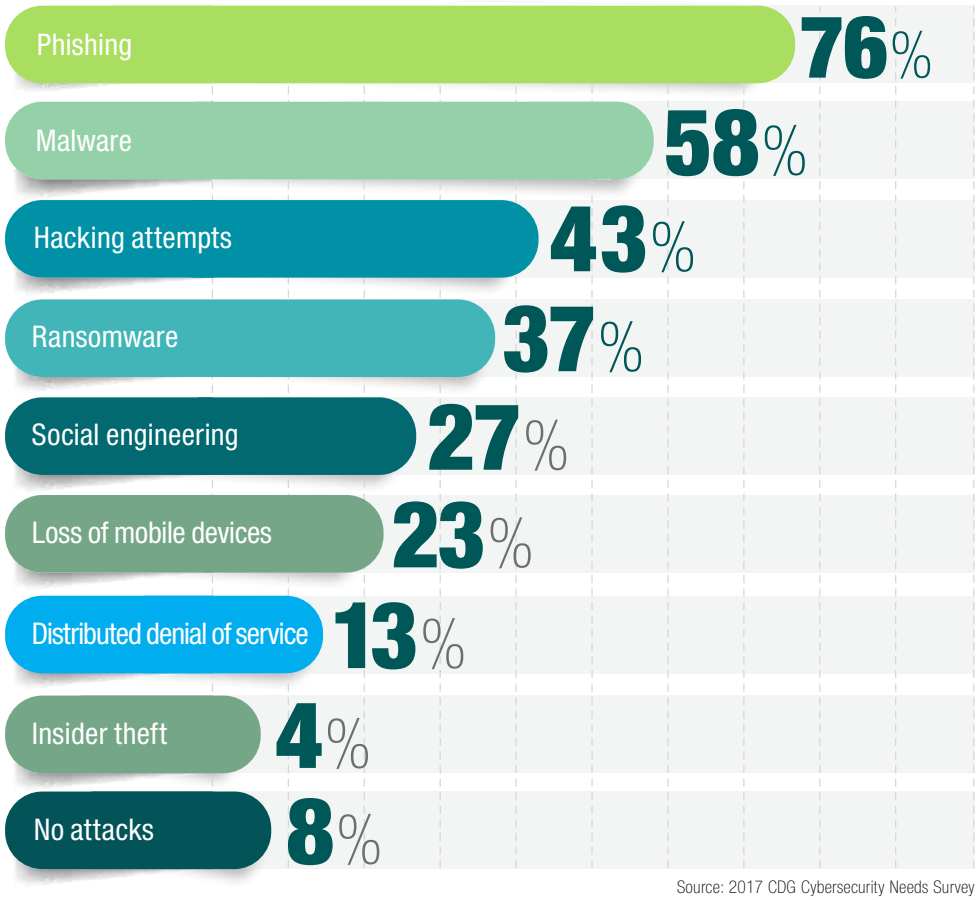
However, a strong business case can often help IT gain executive support for funding a comprehensive cybersecurity strategy. For instance, the Michigan Department of Technology, Management and Budget created a two-part business case to educate the state's governor and legislators about budget needs for cybersecurity.

"First, we created an enterprise risk assessment for all IT assets to identify areas that needed priority for funding," says Rajiv Das, chief security officer for the department. "The second part is a cybersecurity strategy based on our opportunities for improvement, as well as best practices identified by other states."[1]

Chris Hill, deputy chief information security officer in the Illinois Department of Innovation and Technology, notes, "With our 2017-2019 cybersecurity plan and support from our executives, we know what projects we're going to do and we've been very successful in getting budgets to execute that strategy."[2]

Even with a good strategy and business case, the choices for new technologies and approaches to maintain strong security can quickly become overwhelming. To help navigate the complexity, many governments are adopting a standards-based framework for security operations and a technology platform that delivers an integrated cyber defense.

Which of the following types of attacks has your organization experienced in the past year?




Source: 2017 CDG Cybersecurity Needs Survey

## Adopting the NIST-CSF Framework

The National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF) is published by the U.S. Department of Commerce and provides detailed guidelines that IT organizations can use to evaluate and improve their cybersecurity practices and operations. Government agencies and private sector organizations alike apply this framework to strengthen their capabilities for risk detection, management and mitigation.

The framework specifies five core functions to help an organization improve its security posture:

1. **Identify:** Address the organizational understanding of cybersecurity risk
2. **Protect:** Safeguard delivery of critical services
3. **Detect:** Enhance awareness of security events
4. **Respond:** Improve ability to take appropriate action on a detected event
5. **Recover:** Identify timely actions to restore services and normal operations

Agencies that align their cybersecurity strategy with NIST-CSF typically gain:

- A stronger organizational focus on protecting critical information and technology assets
- Improved cyber threat detection and response capabilities
- Expanded understanding of gaps in security protections
- A common foundation for working with agency leaders and users to develop new security policies and practices

Given the framework's significance, nearly eight out of 10 CDG survey respondents believe it is important for a cybersecurity vendor to help their agency apply NIST-CSF to security operations. To meet this need, some vendors offer in-depth assessment programs that review an organization's current alignment with standards and identify prioritized areas for improvement.

Michigan is leveraging the NIST-CSF and is in the early stages of implementation of its risk management program.

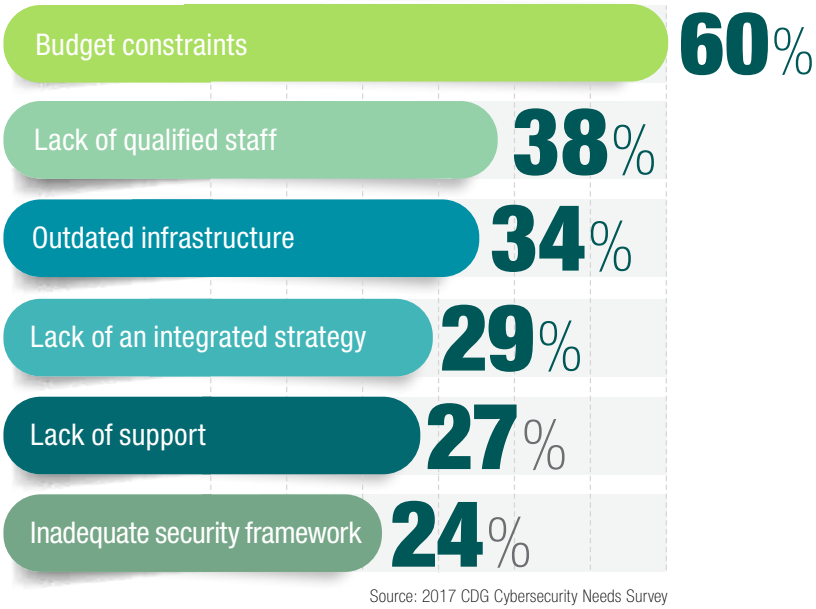
"Aligning with the framework is valuable because it gives you best practices and a way to baseline your operations against those of other organizations. It also helps to make sure your thinking is complete and that you don't have any blind spots about cybersecurity," says Rod Davenport, Michigan's chief technology officer.[3]

For governments that may not be ready to adopt a framework, he recommends looking at less formal checklists and best practices already developed by other state and local technology departments.

## Implementing an Integrated Cyber Defense

While a cybersecurity framework provides guidance as to key areas of focus, an organization's security tools still need to work together to protect information, optimize detection and minimize the impact of security incidents. An integrated cyber defense platform, such as the one provided by Symantec, unifies security point solutions – whether deployed on premises or in the cloud – with the goal of building a comprehensive security posture. Integration improves how an organization governs access to information and applications, as well as protects against data breaches and application disruption, especially when moving more IT services to the cloud.

What are your agency's biggest challenges around meeting cybersecurity needs?




Source: 2017 CDG Cybersecurity Needs Survey

Symantec's platform, specifically, secures the endpoint, network, email and the cloud – offering multiple layers of advanced threat protection and solutions to ensure information is protected and in compliance at all times.

The following example of an integrated cyber defense approach highlights the advantages to government: An employee at a health and human services department uploads an individual's information to a file share application for a doctor to access. The content monitoring controls detect the sensitive data as it's uploaded to the site and assess it against the data loss prevention policies to determine if the data is allowed to be posted. If the data is deemed to be benign, it can be uploaded without restrictions. If it's determined to be sensitive, it's encrypted, or the upload is aborted if data should not be posted. Finally, to ensure only the intended recipient is accessing the information, the receiving doctor must verify his or her identity before being granted access to the file. Once the consult is completed, that access can be revoked to prevent future breaches.

In this scenario, the data was uploaded to a cloud app, but the integrated Symantec security controls would operate similarly if the data was located on premises. The policies and controls set follow the data everywhere it goes for complete protection. This is just one example of how point solutions can be integrated to better protect sensitive information.

## Starting the Journey to Integrated Cyber Defense

Adopting a new technology platform for cybersecurity is an evolutionary effort. The following steps will help IT teams pursue that evolution in a logical, well-timed manner.

1 A vital first step is to determine how a new security program will align to business operations and initiatives. It's important to identify the key information assets to protect and the controls that must be in place for compliance, e.g., for HIPAA and payment card industry (PCI) requirements. Educating agency executives about the business rationale for strong cyber defense is essential to gain their sponsorship of the necessary budget investments.

2 The next step is to create a multi-year technology roadmap based on a framework and a well-defined security architecture. Evaluate current and new security solutions for the digital roadmap and develop plans for integration or replacement as appropriate.

3 Once the program has launched, establish baselines for governance, compliance and metrics to assess the effectiveness and results. Use those metrics to identify opportunities for continuous improvement and to justify ongoing technology funding.

## 4 Key Benefits of an Integrated Cyber Defense Platform

1. **Stronger protection when the security solution is integrated across endpoints, web and business applications, and the network**
2. **Improved efficiencies in both security spending and operations with better ability to orchestrate all security solutions in use**
3. **Correlated threat events through aggregated intelligence across the endpoint, network, email and cloud applications**
4. **A more comprehensive overview of an organization's risk management program**

There's no question that cybersecurity will continue to be a race to stay ahead of new and changing threats. But by aligning security strategies with a standards-based framework and adopting an integrated cyber defense platform, agencies will find it easier to keep pace.

*This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Symantec.*

ENDNOTES


1. Government Technology Webinar, "Building an Effective Cybersecurity Roadmap to Combat Threats Now and in the Future," http://www.govtech.com/webinars/Building-an-Effective-Cybersecurity-Roadmap-to-Combat-Threats-Now-and-in-the-Future-83432.html
2. Ibid.
3. Ibid.



**PRODUCED BY:** CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government is a national research and advisory institute focused on technology policy and best practices in state and local government. The Center provides public- and private-sector leaders with decision support and actionable insight to help drive 21st-century government. The Center is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.centerdigitalgov.com**

**FOR:** Symantec™

Symantec Corporation, the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.