Implementing the NIST Cybersecurity Framework in Government

WHITE PAPER

Practical guidelines for CIOs and CISOs securing public sector data

ABSOLUTE®

EXECUTIVE SUMMARY

Security and risk management, consolidation, and optimization — these are the top priorities for Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) in government today.[1]

These priorities make sense against the current backdrop of escalating cyber threats, more mobile government employees, and decreasing budgets — government CIOs and CISOs must do more with less. Maintaining the status quo is no longer an option. They must reimagine the delivery of technology and information security in a time of increasing budget and resource constraints.

This paper outlines how government CIOs and CISOs can optimize their approach to security and risk management while gaining all the efficiencies of a distributed workforce. It describes how state and local and federal CISOs can — and should — implement the five functions of the NIST Cybersecurity Framework[2] to drive efficiencies while ensuring data security and protecting the communities they serve.[3]

[1] NASCIO and PTI Technology Forecast, 2018.

[2] National Institute of Standards and Technology (NIST), 2018. NIST Cybersecurity Framework.

[3] Absolute, 2018. NIST Cybersecurity Framework - Implementation Overview.

CONTENTS

INTRODUCTION: THE CHANGING FACE OF GOVERNMENT IT AND SECURITY

There is a shift happening across government organizations. Several forces are converging to drive significant transformation of the people, processes, and technology that enable these organizations to serve our communities while securing the data in their care.

These forces are both external and internal and are the culmination of a number of challenges that organizations have faced over the past number of years: the increasing cybersecurity threat, old infrastructure and legacy applications, budget shortages, people and skills gaps, and siloed operations.

Government agencies across the U.S. are responding to these challenges by moving away from the traditional model of individual owners and operators and toward a more centralized hub-and-spoke model.[4]

Some say we're witnessing the rise of the 'the Broker CIO' in government.[5] In this capacity, the CIO acts as a facilitator of information, assisting business units in making the right choices for their needs rather than controlling the full technology supply. They deliver solutions that integrate multiple offerings, platforms, suppliers, and so on.[6] This consolidated approach creates economies of scale and connects the fragmented efforts across different levels of government.

SECURING THE MOBILE WORKFORCE

Enabling a mobile government workforce has many benefits: better service to the public, happier employees, greater productivity, and higher retention.[7] It also helps attract younger employees into government — with some municipalities preparing for half their employees to retire in the next 5 years, bringing on new talent is a key priority.[8]

In the private sector, workforce mobility is now the norm; in government, it is still a relatively new phenomenon. Transforming a traditionally rigid environment into a more flexible one takes time. One of the main challenges of mobility is the risk to government data. Worryingly, IDC reports that 70 percent of all security breaches originate on the endpoint[9] (67 percent in state and local government).[10]

Many of the risks stem from the inability to maintain visibility of government devices (and the data they contain) once they leave the physical office environment and the VPN connection is broken. Encryption and other security software tools are helpful, but how can you be sure that security measures are in place and compliant at all times when devices are off the government network?

Being encrypted at all times — and having the ability to prove encryption status — is key. This is a particular requirement in law enforcement and justice departments where encryption is a requisite for compliance with the Criminal Justice Information Services (CJIS) Security Policy. Failure to comply means the law enforcement agency loses access to the CJIS databases, effectively preventing them from doing their job or putting the safety of field officers at risk.

---

[4] NASCIO and PTI Technology Forecast, 2018.

[5] NASCIO, 2018. State CIO as Broker: A New Model.

[6] Ismail, N., 2018. How CIOs can act as a service broker to the line of business. Information Age.

[7] Gaskell, A., 2016. Why a Flexible Worker is a Happy and Productive Worker. Forbes.

[8] Lipsey, S., 2016. In With the Old. In With the New: The Unique Recruiting Challenge the US Government is Facing. LinkedIn Talent Blog.

[9] Kirsch, C., 2016. IDC says 70% of successful breaches originate on the endpoint.

[10] Deloitte. 2018. Deloitte-NASCIO Cybersecurity Study – States at risk: Bold plays for change.

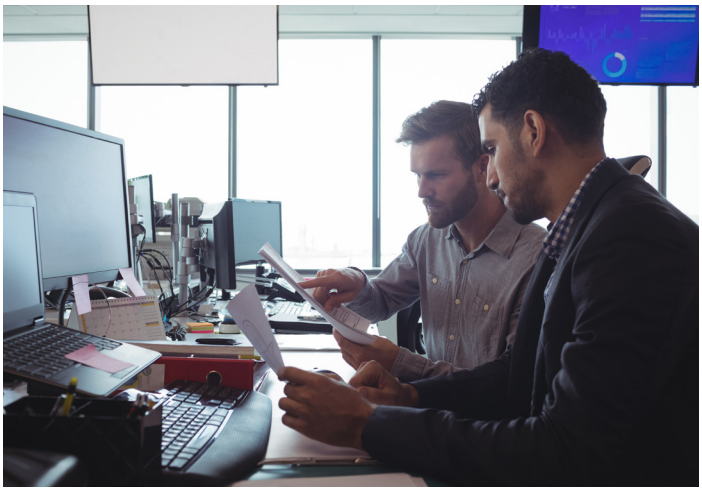
While mobility plays a key role in creating efficiencies, CIOs and CISOs must address the significant threat it can represent to government data.

THE VALUE OF GOVERNMENT DATA

Data is critical to the operation of government agencies. It helps them serve the public, make informed decisions, allocate resources, and perform the tasks needed to support communities.

Despite this, there is an assumption that government data does not have the same value to an attacker as corporate data. Based on the latest Verizon Data Breach Report, all sizes of organizations are vulnerable to breaches but mid-sized organizations are generally easier to penetrate since they often lack the same level of security resources as larger ones.[11]

Governments use data that includes social security numbers, driver's license details, criminal records, healthcare information, personal income, home addresses, and confidential government information — all of which are attractive (and valuable) to potential attackers.



Cost of a Breach

A government data breach can be costly. According to a recent Ponemon study, the total average cost of a data breach to a public sector organization is $2.3 million ($75 per breached record).[12] The financial penalty is not the only consequence — damaged reputation, loss of funding, and the inability to access other government resources can be just as detrimental.

TOP 10 MOST COMMON PIECES OF DATA SOLD BY CYBERCRIMINALS:

- Social Security number: $1
- Credit or debit card (credit cards are more popular): $5-$110
  - With CVV number: $5
  - With bank info: $15
  - Full info (including SSN, birth date, etc.): $30
- Online payment services login: $20-$200
- Loyalty accounts: $20
- Subscription services: $1-$10
- Diplomas: $100-$400
- Driver's license: $20
- Passports (US): $1000-$2000
- Medical records: $1-$1000

EXPERIAN, 2018[16]

Protecting data and devices appropriately has become a top priority for government IT and security leaders. Despite this, 96 percent of state governments still assess cybersecurity only once a year or on an ad hoc basis.[13] Implementing a cybersecurity framework will increase the frequency of cybersecurity risk assessments, ensure continuous compliance, and help protect all levels of government agencies.

NIST CYBERSECURITY FRAMEWORK FOR GOVERNMENT

The National Institute of Standards and Technology (NIST) sets the standard for cybersecurity framework models.[14] Over half of cybersecurity professionals say their organization has already adopted some or all of the NIST cybersecurity framework.[15]

---

[11] Experian, 2018. Here's How Much Your Personal Information is Selling for on the Dark Web.

[12] Verizon, 2018. Verizon Data Breach Investigations Report.

[13] NASCIO Cyber Webinar Series, 2018. Ponemon Institute's Cost of a Public Sector Data Breach.

[14] Deloitte, 2018. Deloitte-NASCIO Cybersecurity Study.

[15] National Institute of Standards and Technology (NIST), 2018. NIST Cybersecurity Framework.

[16] National Institute of Standards and Technology (NIST), 2018. Industry Impacts: Cybersecurity Framework.

There are two main benefits to implementing a cybersecurity framework:

1. Security disciplines are formalized. Teams can focus on repeatable methods so knowledge is shared and people pay attention to the right things (only a quarter of states have appropriately documented cybersecurity competencies today).[17]

2. Security operations can be scaled. By focusing on doing the right things right, teams can accomplish more, even if faced with resource constraints (62 percent of state CISOs and 53 percent of federal CISOs say they face a cybersecurity skills and resource gap).[18]

The five functions of the NIST CSF outlined below offer government agencies the ability to formalize their disciplines and push toward the shared goal of cyber resilience — despite resource constraints.

1. IDENTIFY DEVICES THAT STORE, TRANSMIT, AND PROCESS DATA

The Identify function of the NIST CSF outlines a series of sub-categories. These help government organizations set benchmarks for their risk tolerance according to their asset management, business environment, governance policies, risk assessment, and risk management strategies.

This function can significantly reduce the number of data security incidents through adopting more appropriate policies and behaviors but, ultimately, it's the endpoint devices that will access and contain the sensitive data. Unless you can actually see your devices at all times, it will be impossible to properly assess risk, investigate incidents, and take action.

According to NASCIO, risk assessments and metrics to measure and report cybersecurity effectiveness are the top initiatives in state and local government in 2018.[19] The Identify function of the NIST CSF, coupled with the right technology to give you a persistent connection to each endpoint, are the keys to achieving this NASCIO initiative.

2. PROTECT DATA AND MANAGE AT-RISK ASSETS

The NIST CSF provides four sub-categories to help you establish the Protect function, covering areas such as access control, awareness and training, data security, and protective technology.

COOK COUNTY SHERIFF LIGHTS UP DARK ENDPOINTS

Headquartered in Chicago, the Cook County Sheriff's Office (CCSO) is the principal law enforcement agency that serves Cook County, Illinois. It's the second largest sheriff's department in the U.S. with over 6,900 members when at full operational strength.

According to Keith Morrison, Director of Information Security at Cook County, before Absolute, it was a guessing game as to where the devices were and how they were being used, "We have a lot of mobile devices, and devices being loaned to other people, when someone goes on vacation, for example."

Keeping track, let alone ensuring the devices were running as they should, was a challenge. With Absolute, CCSO can minimize security risks, spot and remediate issues in near real time. They can tap into Absolute's ability to detect, understand and remediate vulnerabilities across all of their endpoints on-demand, whether the device is on their network or not. **Watch the video**.

"If I didn't have Absolute, I would be in the dark. It has provided us with incredible transparency related to our single device per user policy. It is the single source of truth so I can, without a doubt, provide my peers and supervisors with visibility of the device user, what they are using it for, and how long they are using it per day."

KEITH MORRISON
DIRECTOR OF INFORMATION SECURITY
COOK COUNTY SHERIFF'S OFFICE

[17] Deloitte, 2018. Deloitte-NASCIO Cybersecurity Study.

[18] *Ibid.*

[19] *Ibid.*

One key area that the Protect function focuses on is the risk of the insider threat. A recent study found almost 40 percent of state CISOs are not confident that they can protect against security threats from insiders.[20] Training and awareness initiatives can mitigate some of the negligence and ensure each user understands security best practices and the unique security needs of their organization.

Protective technology is also essential. Assets should be protected throughout their entire lifecycle. Insist on the installation of tracking technology in a laptop before it is shipped from the factory. Activate its security on arrival and establish a base-level hygiene score. When a device reaches the end of its life, the onus is the organization to prove that the media has been sanitized so as to make all previously-stored data irretrievable.

Secondly, NIST challenges our assumptions about data security; specifically, the assumption that encryption alone is enough. There should be a persistent health check on all of the security applications as well as an automated way to remediate them whenever they fail. This, along with audits, serve as a forcing mechanism to push toward greater compliance.

"When your devices are stolen, and you have secure company information walking around out there, you come to realize how vulnerable you really are."

ROBERT MIKA
MANAGER OF IT SUPPORT SERVICES
LAS VEGAS VALLEY WATER DISTRICT

3. DETECT ISSUES

Once the Identify and Protect functions of the NIST CSF are satisfied, agencies can move on to the Detect function, paying particular attention to changing circumstances. This function is critical, considering that the average time to detect a breach in the public sector is currently a staggering 231 days.[21]

According to the latest Verizon Data Breach Investigations Report (DBIR), 30% of all cyberattacks involved insiders.[22] The insider threat can be particularly difficult to guard against — without the right technology and processes, it's hard to detect if someone is using their legitimate access to your data for nefarious purposes.

The NIST CSF Detect function can help. It is split into three sub-categories: anomalies and events, information security continuous monitoring, and detection processes. With the right processes and technologies in place, you can recognize incident precursors and take action immediately, based on alerts triggered automatically that allow you to focus on what needs attention.

4. RESPOND TO VULNERABILITIES AND THREATS

Once you've detected a threat, it's vital to respond in a consistent, rational way to ensure fast remediation. The Respond function outlines five sub-categories to help you mobilize quickly in the event of an IT crisis: response planning, communications, analysis, mitigation, and improvements.

Time is of the essence with incident response, yet it currently takes public sector organizations an average of 93 days to contain an incident.[23] Even more concerning, over a third of states don't have a formal incident response process for breach of privacy.[24]

Having standard emergency procedures defined in advance will reduce the response time when a real event

[20] Deloitte, 2018. Deloitte-NASCIO Cybersecurity Study.

[21] NASCIO Cyber Webinar Series, 2018. Ponemon Institute's Cost of a Public Sector Data Breach.

[22] Verizon, 2018. Verizon Data Breach Investigations Report.

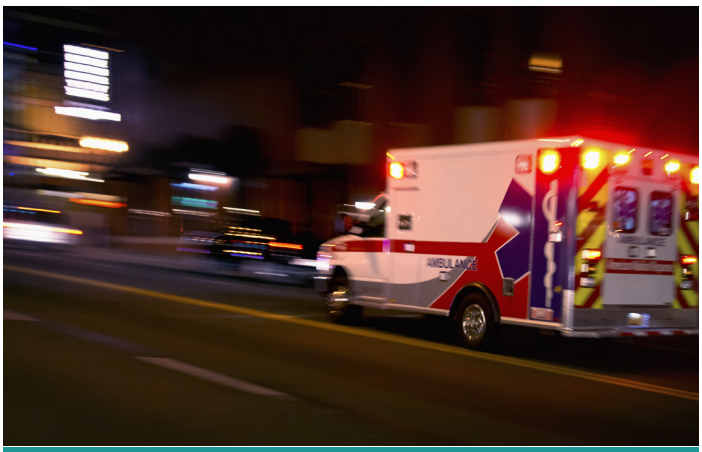
[23] NASCIO Cyber Webinar Series, 2018. Ponemon Institute's Cost of a Public Sector Data Breach.

[24] Deloitte, 2018. Deloitte-NASCIO Cybersecurity Study.

occurs. A reliable connection to a device, even when it is off the network, is critical.

Imagine that you are alerted about credit card information present on a laptop that is currently being used at home by a contractor. Furthermore, it turns out that this user installed Dropbox on the device a couple of days ago and is syncing the sensitive data to an unauthorized cloud folder. You may want to remotely delete the file right away — perhaps even before you communicate with the user — and definitely before the device is back on the government network.

When an incident occurs, confidence in your ability to know what happened and which data was breached is vital. If you have the right technology and processes implemented, you can prove encryption was in place at the time the incident occurred and that you've taken action to mitigate the risk. You can definitively prove that no data was compromised, avoiding the requirement for a breach notification and all the negative consequences that it may bring.



"I was really impressed with Absolute's ability to see any device and remotely freeze or wipe it, as well as to monitor and prove encryption status. Field officers also need uninterrupted access to crucial data to make the right decision on the appropriate protocol in seconds, so keeping their computers up and running with Absolute could save their lives."

COREY NELSON
MANAGER, IT
EMERGENCY COMMUNICATIONS OF SOUTHERN OREGON

5. RECOVER AND ITERATE

Once a breach has been contained, it's important to investigate it, question assumptions, change security controls, and apply any knowledge gained to influence future cybersecurity decisions. The final function of the NIST CSF — Recover — calls for reflection on what happened and the opportunity to incorporate new knowledge to improve your people, processes, and technology for greater resilience against future attacks.

Approach the Recover function with three sub-goals: planning, improving the four other functions, and communication.

Planning ensures that you are prepared when an incident occurs. This will save you from reacting in panic and help you move toward adequate recovery, quickly. Improving the first four functions of NIST means weaving your new knowledge into your cyber defenses, along with recovery plans for future incidents.

For the communication step, the goal is to have a clear information transfer to all stakeholders. Be honest and outline the steps you're taking to lower the probability of a repeat occurrence. Government agencies must show that the issue has been addressed and remediation is in the works, or future funding will likely be withheld.

CONCLUSIONS

Government agencies have made progress with cybersecurity but there is still a long road ahead. The good news is that all the signs of positive change are present. Change is never easy, but the end result will be modern, secure, efficient IT processes across all levels of government.

The first step on this journey is an important one — the implementation of the NIST Cybersecurity Framework. This looks daunting but it's not. It's likely you are already performing many of the functions already. The framework simply documents your processes so your security disciplines are formalized and your security operations are sustainable — even when you're short on staff and budget. It will ensure your team's focus remains firmly on the principle of doing the right things right.

The next step will be to invest in the technologies and risk assessments that are right for your organization.

Governments must use public funding wisely — spending it on breach notifications, fines, and lawsuits is wasteful, creates negative public sentiment, and is highly disruptive to progress.

By investing in technology and risk assessments that highlight gaps in your cybersecurity, you can evaluate risk, calculate remediation costs, and prioritize the technologies that have the most significant impact. Government organizations that have a formal cybersecurity plan in place receive more funding than the ones that don't.[25] Quick security wins will open up more funding as you prove your success.

Are you ready to start implementing the NIST Cybersecurity Framework in your organization? Learn more about how Absolute can help your organization. Visit: **absolute.com/government**


SOLUTION SHEET

ABSOLUTE FOR GOVERNMENT

FORTIFY DATA, SECURE DEVICES, AND STAY AUDIT-READY

PROTECT THE GOVERNMENT DIGITAL TRANSFORMATION

SENSITIVE, DISTRIBUTED DATA

Government's IT and Security Challenges:

THE SOLUTION: CONTINUOUS VISIBILITY AND CONTROL OF EVERY ENDPOINT

KEITH MORRISON
DIRECTOR OF INFORMATION SECURITY
COOK COUNTY SHERIFF'S OFFICE

absolute.com

/ABSOLUTE

ABSOLUTE FOR GOVERNMENT

Learn how to identify potential security threats and respond rapidly, helping you to prove compliance with stringent regulations.

GET IT NOW

[25] Deloitte, 2018. Deloitte-NASCIO Cybersecurity Study.

The information in this white paper is provided for informational purposes only. The materials are general in nature; they are not offered as advice on a particular matter and should not be relied on as such. Use of this white paper does not constitute a legal contract or consulting relationship between Absolute and any person or entity. Although every reasonable effort is made to present current and accurate information, Absolute makes no guarantees of any kind. Absolute reserves the right to change the content of this white paper at any time without prior notice. Absolute is not responsible for any third party material that can be accessed through this white paper. The materials contained in this white paper are the copyrighted property of Absolute unless a separate copyright notice is placed on the material.

/ABSOLUTE®

ABOUT ABSOLUTE

Absolute enables a world where security and IT professionals always retain control over their devices and data. We're the first and only company to offer uncompromised visibility and near real-time remediation of security breaches at the source.

Absolute Persistence® returns devices to their desired state of safety and efficacy after malicious attacks or user error, thanks to our unique location in the firmware of more than 500 million devices built by most of the world's top device manufacturers.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com