Microsoft

From Policy to Practice:

Strengthening Cybersecurity in State Governments

Authors

Ryan Harkins
Aaron Kleiner
Jim Pinter

Contributors

Erin English
Michael Mattmiller
Bobby O'Brien
Rob Spiger

Contents

Foreword

Securing Society by Securing the States

Cyberattacks threaten our societal fabric by undermining trust in institutions that people and organizations rely upon in everyday life. State governments often find themselves on the front-lines of cyber defense because states play a central role in the delivery of essential services, the administration of industry and commerce, and provide the backbone of governance in the United States. Indeed, state agencies may hold vast troves of personal data because they are responsible for human services that the private sector does not provide, they hold business confidential information because they are enforcers of consumer protections, and they often interface with counterparts across state lines, in the federal government, and even foreign governments in the conduct of official business. All this makes state agencies a desirable target for cyber attackers, including nation-state attackers who are eager to exploit state government networks.

With this paper, Microsoft aims to support state governments in securing their own Digital Transformation while protecting the people, processes, and institutions of those states. Across the country, states are making significant investments in information technology (IT) so that they can take advantage of the same efficiencies that are powering the private sector's charge towards the Fourth Industrial Revolution. For example, Alaska has leveraged cloud computing to significantly reduce road maintenance costs and save lives, using Microsoft Azure Internet of Things (IoT) services and the Fathym WeatherCloud solution. These use-cases are not just IT projects; they are revolutions in how state governments perform core functions with the aid of technology.

This paper puts forward several key policy recommendations for state governments, each of which is exemplified in existing state practices. Specifically, we recommend the following:

1. **Ground cybersecurity policy in established guidelines and standards.** State governments should adopt federal frameworks, such as the NIST Cybersecurity Framework, to help lay the groundwork for strong, effective state cybersecurity policy.
2. **Establish an ongoing cybersecurity advisory council with industry and academia.** In many states, most cybersecurity expertise lies across industry sectors and academic disciplines, and many of these experts would likely be eager to contribute to state cybersecurity policy. We recommend that states utilize these assets and create a cybersecurity advisory council, which would bring together industry experts, academics, and public sector leaders to develop cybersecurity strategies for the state and help respond to ongoing threats.
3. **Create a culture of cybersecurity.** It is well known today that the weakest point of security for an organization, and for states, is its personnel. Yet today, only 18 states require cybersecurity training for all their employees. We believe it is essential to develop a knowledgeable, cyberliterate workforce to reduce cyber risks to the state.

4. **Leverage new resources to enhance election integrity.** Over the past few years, threats to democratic processes from cyber-enabled interference have become a critical concern. In this section, we discuss the resources available to states to better protect their election systems and increase the overall election integrity in the US.
5. **Integrate cyber resilience into every step of strategic planning.** Cybersecurity is a journey that can be marked by major challenges and even failure. That is why we believe that states need to prioritize making their services and data more resilient and have processes in place to respond to and quickly recover from cyberattacks.
6. **Consider cyber insurance to help protect state assets.** Cyber insurance can help states complement their cyber risk management process by providing financial protection against risks that cannot be fully mitigated.
7. **Strong procurement policies and compliance are essential.** As data being created and stored by states has increased, so too have states' legal and regulatory obligations. It has become increasingly important that states examine their compliance and procurement policies, ensure that they comply with these obligations and almost more importantly, that their vendors can demonstrate that they will enable compliance through their tools and services.

Microsoft welcomes opportunities to help states develop their cybersecurity policies and translate those policies into practice. We hope that this paper and its recommendations enable collaboration across the public and private sectors to address shared concerns about cybersecurity and facilitate sharing among states about successful cybersecurity policy initiatives. Just as cyberattacks can transcend sectoral and jurisdictional boundaries, those of us committed to cyber defense must also reach across societal lines to advance the state of cybersecurity through both technology and policy.

Tom Burt, Corporate Vice President for Customer Security and Trust
Deputy General Counsel
Microsoft Corporation

What Is State Cybersecurity?

State cybersecurity is the protection of critical assets that are vital to the state's operations and infrastructure and to the stability and livelihood of its communities.

Introduction

Over the past decade, new technologies have continued to find their way into our everyday lives, businesses, and state infrastructure. This is creating fresh opportunities, but also new risks should the technology fail or its security be compromised. The world has watched while nations and corporations have been the target of large scale cyberattacks conducted by both nation states and organized crime. The United States is among the most heavily attacked nations in the world, and in recent years, US state governments have been targeted at an alarming rate.

Almost every US state has been the victim of a successful cyberattack, including access by cybercriminals to state data, threats to infrastructure, and even the theft of state pension funds.

State policymakers are looking for ways to protect state systems, but they face challenges as they adopt new technologies, grapple with limited budgets, and push to keep pace with rising threats, all while continuing to provide critical government services upon which their constituents rely. No longer can states sit idly by or ignore cybersecurity as a priority in their state plans.

States must think holistically and adopt comprehensive, risk-based cybersecurity strategies that, rather than simply responding to the most recent cybersecurity incident or headline, take the long view, and instill best practices that are flexible and capable of adapting to the evolving threat landscape.

This paper presents seven best practices that every state should implement to protect its government and constituents from cybersecurity threats. They are based upon Microsoft's expertise and years of experience in protecting customers and dealing with threats in cyberspace around the world. Today, there are many examples across industry and government of strong cybersecurity practices and approaches and there are many technologies available to help protect state governments and their constituents.

These practices will not only help states protect the data and assets that their governments maintain, but also provide the flexibility necessary to adjust strategies and approaches to respond to an ever-changing security environment.

I. Ground Cybersecurity Policy in Established Guidelines and Standards

The increase in cyberattacks against states, the rapidly evolving threats, and the growing costs to state treasuries have heightened pressure on state lawmakers to quickly enact protective laws and develop and implement cybersecurity policies to guard against them.

Over the past decade, the federal government has worked to develop strong cybersecurity guidelines, recommendations, and standards. At Microsoft, we believe that these guidelines can easily apply at the state level and help lay the groundwork for strong, effective state cybersecurity policy.

In particular, Microsoft believes that every state should build a comprehensive, risk-based cybersecurity framework based upon the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[1] It provides a high-level, strategic view of

the lifecycle of cybersecurity risk to help states better understand their cybersecurity risk, and it enables them to apply the principles and best practices of managing risk to improve the security and resilience of critical infrastructure and services. That in turn will help them set priorities for cybersecurity investments to get the most out of every dollar spent on cybersecurity. The framework does not take a one-size-fits-all approach to risk management. It assumes that organizations have unique risks—different threats, vulnerabilities, and risk tolerances—and is meant to be customized to best suit the risks, situations and needs of an organization.

The NIST Cybersecurity Framework was developed over years of collaboration by leading security experts from government, technology companies, and academia. It is considered to be the gold standard by many computer security professionals as it has been thoroughly tested and widely adopted by governments, public organizations, and private entities of every size around the country. Indeed, it is embedded in our own cybersecurity practices at Microsoft, and the entire US government is required to use it. State governments have embraced it, too. According to a 2017 survey of state CIOs by the National Association of State Chief Information Officers (NASCIO), 95 percent of respondents reported that they have adopted a cybersecurity framework based on national standards and guidelines.

We believe that using a widely-recognized standard like the NIST Cybersecurity Framework can support state efforts to promote interoperability across government agencies, such as with the US Department of Homeland Security, Health and Human Services or with technology providers hired by the state, many of whom base their cybersecurity strategies on it.

According to a 2017 survey of state CIOs by the National Association of State Chief Information Officers (NASCIO), 95 percent of respondents reported that they have adopted a cybersecurity framework based on national standards and guidelines.

Helpful Resources

- NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity [2]
- NIST Frequently Asked Questions [3]

Best Practice: Iowa Builds Its Cybersecurity Strategy on the NIST Cybersecurity Framework

In 2015, the Governor of Iowa established an inter-agency partnership to develop a comprehensive cybersecurity strategy. In just one year, Iowa crafted an effective strategy for cybersecurity risk assessment and management, rooted in the NIST Cybersecurity Framework

By utilizing NIST Cybersecurity Framework as an asset in the development of their cybersecurity strategy, Iowa was able to take out much of the guesswork out of building the Iowa strategy and limited the number of cycles needed to pull it together.

Helpful Resources

- **State of Iowa Cybersecurity Strategy, July 2016** [4]
- **Local Government Cyber Security: Risk Management, A Non-Technical Guide** [5]
- **NIST Guide for Conducting Risk Assessments** [6]

[1] www.nist.gov/cyberframework

[2] www.nist.gov/cyberframework

[3] www.nist.gov/cyberframework/frequently-asked-questions

[4] https://ocio.iowa.gov/sites/default/files/documents/2016/08/2016_cybersec_document_web_version_2_final_0.pdf

[5] http://msisac.cisecurity.org/members/local-government/documents/Cyber-Security-Risk-Management-for-Local-Governments.pdf

[6] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

II. Establish An Ongoing Cybersecurity Advisory Council with Industry and Academia

Microsoft recommends that each state create a cybersecurity advisory council, convening local cybersecurity experts from the private sector, other public-sector entities, and academic institutions to advise on the development of cybersecurity strategies and help state government respond to online threats. This council can help ensure that the right laws and regulations are put forward and that the state is implementing the best standards, policies, and procedures to better protect state infrastructure.

Formalizing these relationships will also help cultivate a deep understanding of the state's cybersecurity strengths and weaknesses over time and better enable the state to stay abreast of new cyberthreats. A cybersecurity advisory council can, both routinely and in response to a crisis, help reduce the burden on state IT professionals. They can share threat intelligence, data on hacking trends and new threats to critical systems.

This will help state IT departments respond more quickly to emerging issues and may also lead to new protections or mitigations—sometimes in advance of any negative impact—that can blunt a hacker's head start.

Best Practice: Indiana Sets Up an Executive Council on Cybersecurity

Many in the Indiana state government realized that securing the state's information technology infrastructure and managing the complex control systems that protect state assets were beyond the reach of government alone. Consequently, the governor signed an executive order creating the Indiana Executive Council on Cybersecurity. It formalized a partnership between the public and private sector by bringing together a group of leaders from the governor's office, law enforcement agencies, the state CIO office, local corporations and academia.

The advisory council is empowered to produce an overview of Indiana's cyber risks and opportunities, create a cybersecurity framework for the state and establish capabilities to respond to cyberincidents.

Helpful Resources

- **Organizational Charter of the Indiana Executive Council on Cybersecurity**[7]
- **Guide to Cooperative Models for Effective Public-Private Partnerships.** In this document, the European Network and Information Security (ENISA) puts forward 36 recommendations for successful public-private partnerships.[8]

[7] www.in.gov/cybersecurity/files/Exectuive%20Council%20on%20Cybersecurity%20Charter_Voted_September%2027%202017.pdf

[8] www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

III. Create A Culture of Cybersecurity

In many cases, the weakest point of security for an organization is its personnel. It takes just one person to click an infected link, open a phishing email, or insert an infected USB drive into a computer to put an entire network of systems and information at risk. According to a recent survey of 4,000 financial institution employees,[9] 66 percent of data breaches resulted from the unintentional actions of employees.

This means that cybersecurity is not only an IT concern, but a human resources one as well. It is essential to develop a knowledgeable, cyberliterate workforce to reduce cyber risks to the state.

Despite the fact that employees cause the vast majority of data breaches, organizations nationwide devote a surprisingly small percentage of their resources to cybersecurity training. For instance, while businesses spent an estimated $90 billion on information security in 2017, only $1 billion of that amount was spent on cybersecurity awareness training.[10]

Similarly, 32 states today do not require cybersecurity training for their employees; and of the 18 states that make cybersecurity training mandatory, several require it only for new hires or executive branch agencies.[11] This means, of course, that only a relatively small number of state employees nationwide will ever see or take courses on cybersecurity.

We can do better.

To create a culture of cybersecurity and reduce the risks from cyberattacks, state governments should implement a robust cybersecurity training program for all state employees. Research shows that anti-phishing training programs result in a manifold return on investment, even accounting for the loss of productivity during training time. A Ponemon Institute study commissioned by Wombat Security Technologies, which provides anti-phishing training, surveyed more than 375 IT specialists, a third of them from organizations with 1,000 or more employees. They measured how often employees clicked on the phishing links before and after training, and found that, as a result of effective training, there was an almost 50 percent long-term improvement in fighting phishing scams.[12]

To reduce the risk from cyberattacks and develop a culture of cybersecurity, states should implement a cybersecurity training program that includes at least the following key steps:

- An annual cybersecurity awareness training class that relies on a "learn by doing" approach. It should include highlighting risky behaviors and training in good security hygiene, such as not logging in to a work device on an unsecured public network or clicking hyperlinks irresponsibly.
- Augment the class with regular tests throughout the year of employees' ability to recognize phishing email messages. These can educate employees on emerging

Explaining Phishing:

At Microsoft, we have found that more than 90 percent of attacks use a hyperlink to initiate the attack to steal credentials, install malware, or exploit vulnerabilities, making it all the more important to understand phishing.

Phishing is an attempt to trick you by sending a phony email or text message that appears to come from a trusted source like your bank, a colleague, or a credit card company. The convincing message entices you to divulge credit card numbers, passwords, account data, or other sensitive personal information. Or it might ask you to call a phony toll-free number or to click a link that goes to a fake webpage and reveal the information there.

Criminals can then use this information for many different types of fraud, such as to steal money from your account, open new accounts in your name, or get official documents using your identity.

[9] Cyber risk: it's a people problem, too. Willis Towers Watson, September 25, 2017.

[10] Are your employees your biggest cybersecurity risk?. General Global Assistance, October 9, 2017

[11] http://www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx

[12] The Cost of Phishing & Value of Employee Training, Ponemon Institute Research Report, 2015.

Elements of an effective cybersecurity training program

Employees are the weakest link in an organization's cybersecurity, but once trained, they can become its strongest defense. To cultivate a culture of cybersecurity, make sure:

- Infrastructure has the technology and administrative controls in place so IT staff can manage and monitor employee behavior and that your training program includes these components.
- Implement mandatory yearly cybersecurity training for all employees at every level of state government.
- Conduct regular phishing tests for all state employees to educate them about emerging threats. Require additional training for employees who fail the test.
- Make available a repository of training materials for employee reference—physical examples of phishing attacks, a checklist for good cyberhygiene and the like.
- Collect feedback and review statistics on your training program and, based on that data, make changes to improve its effectiveness.
- Make it easier for employees to report potential security breaches and enable a phishing and spam reporting button in the state government's email program.
- Consider offering a subscription to antivirus protection for employees' personal devices.

phishing tactics, increase the likelihood that they will look for suspicious links in email, and enhance their sense of personal responsibility for data security at work. The class should also require additional training for any employee who fails the test.

- Program administrators must collect feedback, review results, and analyze statistics from the classes and tests and, based on that data, make changes to improve the program's effectiveness.

Cybersecurity training not only helps defend state systems against cyberattacks. It also helps ensure that state IT departments have implemented the appropriate security controls, —such as event logging, forensic training, and dynamic network protection— so that IT staff can manage and monitor employee behavior and protect its networks and assets. Without these tools, training does nothing.

Best Practice: Pennsylvania Invests in Cybersecurity Training and Awareness Among State Employees

The Commonwealth of Pennsylvania has made a concerted effort to train its workforce on cybersecurity and enable stronger security practices for those working at home. It mandates an annual security awareness training course for all employees at every state agency. It teaches security best practices, discusses scenarios users may encounter such as phishing email messages, and provides clear guidance on what employees should do if they come across suspicious sites or email.

The state also encourages strong cybersecurity practices at home. Recognizing that employees often use personal devices to work out of the office, the commonwealth gives employees antivirus software for these devices free of charge. This helps reduce the possibility of contaminating commonwealth workstations with malware.

Helpful Resources

- **State cybersecurity training for state employees.** The National Conference of State Legislatures has published a chart that briefly describes the type of training each state offers, and links, where available, to state training resources.[13]
- **Cybersecurity for Commonwealth Agencies and Employees.** Pennsylvania publishes a variety of cybersecurity resources and services for state agencies and employees.[14]
- **The Microsoft phishing blog.** Includes examples of the latest phishing attacks, suggestions for protecting accounts and networks, and advice for defending systems against cyberattacks.[15]

[13] www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx

[14] www.oa.pa.gov/Programs/Information%20Technology/cybersecurity/agencies-employees/Pages/default.aspx

[15] cloudblogs.microsoft.com/microsoftsecure/tag/phishing

IV. Leverage New Resources to Enhance Election Integrity

Threats to democratic processes from cyber-enabled interference have become a critical concern. Nation-states have attempted to target and exploit key building blocks of the democratic system including voting systems and the technology infrastructure of political campaigns. While the manifestation of this threat at the national-level, especially as it relates to presidential campaigns, has received the vast majority of public attention, states, who often administer elections, have also been caught in the crosshairs. Indeed, in the leadup to the 2016 election, the voting systems in at least 21 states were targeted by malicious cyber actors.[16]

Since 2016, however, new resources designed to enhance the integrity of elections have been made available to states. Among them are federal funding for securing elections, free election security programs coordinated by the Department of Homeland Security (DHS), technologies supporting robust post-election audits (such as risk-limiting audits, or RLAs), and new election security best practice guidebooks.

On March 23, 2018, Congress allocated $380 million to states "to enhance election technology and make election security improvements."[17] These funds, which are being distributed as grants by the Election Assistance Commission (EAC), provide states with the opportunity to invest in election integrity enhancing technologies, including:

- New voting equipment that utilizes a voter verified paper record;
- Post-election audits, such as RLAs;
- Upgrades to election related computer systems to address cyber vulnerabilities;
- Cybersecurity training for election officials;
- and the implementation of cybersecurity best practices for election systems.[18]

The Department of Homeland Security (DHS) has also developed several notable new resources since 2016 to aid in enhancing election integrity.[19] DHS offers free services designed to secure elections infrastructure, such as vulnerability scanning of Internet-accessible systems on a continual basis and phishing campaign assessments. DHS has also created new communities to promote both information sharing on threats to elections and election security best practices. These new initiatives include:

- The Government Coordinating Council (GCC), which enables local, state, and federal governments to share information and collaborate on best practices to mitigate and counter threats to election infrastructure.[20]
- The Sector Coordinating Council, (SCC) which works with infrastructure owners and operators to advance the physical security, cyber security, and emergency preparedness of the nation's election infrastructure.

---

[16] https://apnews.com/cb8a753a9b0948589cc372a3c037a567

[17] https://www.congress.gov/bill/115th-congress/house-bill/1625/text?format=txt

[18] https://www.eac.gov/payments-and-grants/frequently-asked-questions-for-grants/

[19] https://www.dhs.gov/sites/default/files/publications/DHS%20Election%20Infrastructure%20Security%20Resource%20Guide%20April%202018.pdf

[20] https://www.dhs.gov/topic/election-security

What are Risk-Limiting Audits (RLAs)?

RLAs provide a statistically robust mechanism for election officials to verify that a representative sub-set of votes cast has not been miscounted as the result of error or tampering. Though RLAs do not guarantee the accuracy of an election outcome, they vastly increase the ability of election administrators to detect an inaccurate outcome. RLAs were first developed in 2008 and first adopted in a statewide election by Colorado in 2017.

- The Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), which serves election community by providing near real time threat and risk sharing as well as cybersecurity best practices geared towards election officials.[21]

Over the last 12 months, new technologies supporting robust post-election audits have also become available to election administrators. These technologies, which are eligible for the aforementioned EAC grants to states, enhance the integrity of elections by increasing confidence in their results. One such method for accomplishing this goal is risk-limiting audits (RLAs). RLAs provide a statistically robust mechanism for election officials to verify that a representative sub-set of votes cast has not been miscounted as the result of error or tampering. They were adopted by Colorado in statewide elections in 2017 and are in the works or under consideration in several other states across the country.

Finally, cybersecurity and election experts across civil society have produced a number of election security best practice guidebooks over the last year.[22] Among the most prominent is the State and Local Elections Cybersecurity Playbook, released by the Defending Digital Democracy Project (D3P) at Harvard's Kennedy School of Government.[23] The Playbook, which is one of a series of election security playbooks released by D3P, provides policy and technical best practices to the full range of election stakeholders, from administrators to staffers.[24]

Best Practice: Colorado's Use of RLAs

Colorado became the first state to adopt risk-limiting audits, passing a law in 2009 that required counties to adopt the statistically robust method to enhancing election integrity and implementing them for the 2017 statewide general election. Upon completion of the audit, Colorado's Secretary of State, Wayne Williams, noted his perception of RLAs' positive impact on voter confidence in the integrity of elections: "It required a lot of work and effort from my office and the county clerks and they all came through fabulously. I was thrilled with the success.[25] The fact that every single county passed, I think gives everyone a very high level of assurance of elections in Colorado."

Since Colorado's completion of its first statewide RLA, two additional states, Rhode Island and Virginia, have passed laws requiring its use in their election jurisdictions, while two others, Ohio and Washington, have amended existing requirements to make it one of several acceptable forms of post-election audit. Ten states do not have a post-election audit requirement of any form in place.[26]

Helpful Resources

- **U.S. Department of Homeland Security: Election Infrastructure Resource Guide**
- **Belfer Center at the Harvard Kennedy School of Government: State and Local Election Cybersecurity Playbook**

[21] https://learn.cisecurity.org/ei-isac-registration

[22] https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

[23] https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf

[24] https://www.belfercenter.org/publication/cybersecurity-campaign-playbook

[25] https://thevotingnews.com/colorado-leads-the-way-with-risk-limiting-audits-electionlineweekly/

[26] www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx

V. Integrate Cyber Resilience Into Every Step of Strategic Planning

As state governments develop and implement strategies to protect their IT assets and data from cybersecurity threats and other disasters, they must focus not only on preventing bad things from happening, but on making their services and data resilient in the event that bad things happen. In other words, they must focus on ensuring that if a successful cyberattack occurs the state can respond quickly, minimize any damage done and recover as soon as possible, all while continuing to provide critical government services that their constituents rely upon. That is, resilience does not mean that operations and their supporting infrastructures will not fail, nor that a state is no longer vulnerable to cyberattacks—but rather that it can adapt and recover from them.

Cyber resilience can best be understood as a state's capacities and capabilities for readiness, response, and reinvention in the face of a cyberthreat with processes that enable stability, ensure recovery and help restore services rapidly. Cyber resilience ensures that services can continue to be available and operate without being compromised, whether by cyberthreats or the impact of natural or man-made disasters.

- **Readiness.** States should plan for long-term readiness for cyberincidents and other disasters by, at minimum, identifying their assets, assessing and managing infrastructure risk, developing capabilities to respond to and recover from disruptions, and investing in research, education, and practices that contribute to cyber resilience goals.
- **Response.** States should conduct fire drills and walk through the plans and strategies set in place during the readiness phase to help ensure that agencies will continue to function during a crisis and rebound quickly. In addition, state plans must enable an adaptive and flexible response to incidents, so that state government can quickly respond even to threats or other disruptive events that may be unforeseeable or unexpected.
- **Reinvention.** Learning from and improving on existing plans and strategies is a hallmark of cyber resilience. After a crisis has passed, every state should evaluate its response—identifying what was effective and what was not—and then update its cybersecurity plan based upon what was learned. It's important for states to think beyond short-term gains and actions, often the changes that can best lead to resilience are long-term actions that may be relatively expensive but have a stronger return on investment.

Embracing cyber resilience will not only ensure that states are more secure; it will create opportunities for states to build comprehensive, long-term strategies that set them on a path toward digital transformation. It will promote a culture of innovation, generate new avenues for investment, and contribute to a vibrant and economically competitive state.

Best Practice: UK National Health Services Mitigates Impact of Cyberattack Through Operational Resilience

Cyber resilience can make a huge difference in the wake of a cyberattack. In February 2017, a global ransomware attack known as WannaCrypt held government and corporate systems hostage—locking up files and encrypting them so that the owners could not access them unless and until attackers were paid a ransom. While not the first

such attack, its scale was unprecedented, leading to massive shutdowns of healthcare systems, transportation grids, and major corporations. This resulted in hundreds of millions of dollars in lost revenue and productivity, as well as substantial payments to the attackers.

But not all organizations felt the same impact to their operations. The UK National Health Service (NHS) was targeted and its systems held hostage. But the NHS had prepared for this kind of incident by building in enough redundancy so that its systems continued to function with only a slight delay while the NHS recovered its data from backups. The NHS was not completely unscathed—for example, it was forced to cancel many appointments, but it survived the WannaCrypt attack without losing any data or making any ransom payments to the attackers, and continued to serve patients, albeit with some changes in procedure, whose lives depended on functioning medical services.

Helpful Resources

- **Microsoft: Advancing Cyber Resilience with Cloud Computing.** Based on extensive Microsoft experience and conversations with customers, this white paper makes recommendations for how your state can use cloud computing to support its cyber resilience, covering both technical and policy obstacles that must be overcome. [27]

[27] www.microsoft.com/en-us/cybersecurity/content-hub/advancing-cyber-resilience-with-cloud-computing

VI. Consider Cyber Insurance to Help Protect State Assets

Over the past few years, we've seen organizations around the globe hacked, resulting in the loss of billions of dollars. Based on the principle that it's not a matter of if there will be a cyberattack but when, many organizations, including state governments, have begun to consider cyber insurance as a way of helping states complement their cyber risk management processes by providing financial protection against risks that cannot be fully prevented.[28] In fact, in a 2017 survey of state CIOs, 38 percent of those who responded said they have some type of cyber insurance, up from 20 percent in 2015.[29]

The benefits of cyber insurance are not just financial—cyber insurance is, of course, no substitute for a robust cybersecurity strategy and practice. To qualify, insurance companies require that states meet a certain set of cybersecurity standards such as regularly training staff, encrypting sensitive data, and keeping servers up to date. It therefore forces state governments to implement strong cybersecurity practices, increasing the overall health of their technology systems and protection of their data.

As states look to incorporate cyber insurance into their risk transfer strategy, they play a broader role as there is no federal regulator of insurance; insurance is regulated by states, so state governments can work closely with regulators to help define and determine cybersecurity policies while gaining a better understanding of the extent of the cyber risk exposure for the insurer. It is also important for state regulators to look to harmonize their policies due to the interstate dimensions of cyber risk and cybersecurity.

Best Practice: Montana Turns to Cyber Insurance For Greater Protection

In 2011, Montana was the first state to secure cyber insurance, paying an annual premium of $88,000 for a $2 million policy covering all state agencies with a $100,000 deductible per incident.[31] In 2014, hackers broke into a server at the Montana Department of Public Health and Human Services, compromising the names, Social Security numbers, and health data of potentially more than a million people. Lynne Pizzini, chief CISO, reported that the insurance company helped mail letters to everyone affected, set up a center to respond to citizen calls and offered credit monitoring, and provided investigative and legal help. She said that their services would have cost far more than the state's annual premium and deductible. Pizzini cautioned, however, that although the coverage was a huge help, offsetting some of the risk, cyber insurance is not a substitute for a comprehensive security program

Helpful Resources

- **Pew Charitable Trust: States Turn to Cyber Insurance.** This analysis provides insight into how state governments are using cyber insurance.[32]
- **Report: The Impacts of a Growing Cyber Insurance Market.** In this joint publication, experts from Marsh McLennan, Microsoft, and the East-West Institute describe how cyber insurance is changing technology risk management.[33]

What is Cyberinsurance?

The Federal Insurance Office refers to cyber insurance as a broad range of insurance products that cover risks arising from the use of electronic data and its transmission, physical damage that can be caused by cyberattacks, fraud committed by misuse of data, liability arising from data storage, and the availability, integrity and confidentiality of electronic information.[30]

[28] Unleashing the Potential of the Cyber Insurance Market, Organisation for Economic Co-operation and Development (OECD), February 2018.

[29] Worried about hackers, states turn to cyber insurance. Pew Charitable Trusts, November 10, 2017.

[30] https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2017_FIO_Annual_Report.pdf

[31] https://www.nascio.org/dnn/portals/17/2015MY/Cybersecurity%20Insurance.pdf

[32] Worried about hackers, states turn to cyber insurance. Pew Trusts, November 10, 2017

[33] www.eastwest.ngo/sites/default/files/16_Impacts%20of%20Growing%20Cyber%20Insurance%20Market_as%20of%2015Feb2017.pdf

VII. Strong Procurement Policies and Compliance are Essential

As the scope and scale of data created and stored by organizations of all types has increased, so too have the legal and regulatory obligations that organizations, including state governments, must take to adequately handle and protect it. The many different regulatory requirements can be exceedingly complex, particularly for state governments, which store and maintain a wide variety of information types.

For example, entities that store criminal justice information may need to protect it following the requirements of the FBI Criminal Justice Information Services Security Policy. Agencies that handle protected health information may have certain obligations under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. IRS Regulation 1075 may apply if an entity handles certain tax or financial information.

Obviously, every government should consult its own lawyers and other experts to determine what its legal obligations are and how to comply with them. But failure to comply with regulatory obligations to protect data not only creates a serious risk of liability, but puts the privacy and security of the data, and ultimately of the state's constituents, at risk.

In general, legal obligations to protect certain types of information will continue to apply to the organization regardless of whether it chooses to store the information on its own premises—on computers or servers that it owns and operates—or in the cloud, in datacenters owned and operated by a third party.

Consequently, state governments should examine their procurement policies and ensure that whenever they hire a vendor to provide software or cloud services, the vendor can demonstrate that it will enable the state to comply with the its legal and regulatory obligations to handle and protect information appropriately.

Helpful Resources

- **Microsoft: Achieving Trust and Compliance in the Cloud.** This paper illustrates the transformative power of cloud computing on industries and organizations, and provides guidance to in-house counsel on addressing compliance obligations in the cloud. [34]
- **Microsoft: An Introduction to Cloud Compliance for Legal and Compliance Professionals.** This paper puts forward foundational concepts, definitions, and examples to enable technical and non-technical audiences to understand the impact of cloud computing on legal and compliance matters [35]

Conclusion

Policymakers today must continuously make thoughtful, multidisciplinary decisions to respond to the challenges of their growing populations, increased interconnectivity, changing expectations of government services and the uncertainties of security in cyberspace. Implementing cybersecurity and policy frameworks that enable and better protect state's departments, local business and organizations can help meet those challenges while enabling employees to do their jobs.

Microsoft supports states efforts to develop strong cybersecurity strategies, policies and practices. By following the strategies and approach described in this paper, states can establish a clear path toward innovating and advancing their security goals and better protect their information technology systems and their constituents.

[34] https://aka.ms/cloud-trust-compliance (link opens PDF)

[35] http://download.microsoft.com/download/0/D/6/0D68AE95-6414-4074-B4B8-34039831E2BF/Introduction-to Cloud-Computing-for-Legal-and-Compliance-Professionals.pdf

Appendix: Technologies to Strengthen the Cybersecurity of State Government

Based on decades of securing billions of computers and computer systems, we at Microsoft have learned there are key technologies that are indispensable to the protection of a state's most critical data and assets, the advancement of its cyber resilience, and its digital transformation.

Here, we identify seven essential technologies and security features that can serve as a solid and strong cybersecurity foundation for your state. Widely recognized as security best practices, these are also the backbone of federal cybersecurity guidelines and regulations, so implementing them brings state implementation into alignment with federal policy.

1. Enforce Identify and Access Management Controls

Protecting systems, applications, and data begins with identity-based *access controls*, security features that are used to regulate who can access resources in a computing environment. Weaknesses in these controls can lead to security infractions or granting inappropriate access.

Controlling access requires the ability to confidently authenticate a user and to effectively manage the rules and permissions that dictate access rights. This technology includes robust multifactor authentication for all users at every level of government. This means requiring a user to present at least two pieces of evidence—credentials—to log onto the network. It goes beyond the traditional username and password to include use of smart cards and biometric verification technology such as fingerprint and retina scans, and voice identification.

A significant factor that can also increase the risk from unwanted intrusions is the tendency to give users more administrative privileges than are necessary to complete their jobs. (Administrators have broad powers including the ability to make changes to the system.) In many organizations, these are accorded to most employees when only a small fraction of employees need them.

To minimize unauthorized access to systems handling sensitive data, organizations can use controls that give access to data and other system resources when needed but restrict it when an individual or group no longer needs it. These administrative privileges include advanced rights and system configuration management controls that include restricting privileged access such as just-in-time administration, just-enough-access controls, and role-based access controls. These help reduce opportunities for malicious users to gain access, increase control and awareness of the environment, and provide the ability to remotely wipe data on lost or stolen devices, including all their access permissions.

2. Safeguard Sensitive Data

Data is a state government's most valuable and irreplaceable asset, so it is essential to safeguard its digital assets from unauthorized use, whether by accidental loss of mobile devices and laptops, inadvertent public disclosure of sensitive data by an employee, or illegitimate access by a malicious outsider.

To do this, governments can use:

- Data loss prevention policies and tools, which are designed to protect information that has been flagged as sensitive. Organizations can customize policies to address their own unique concerns—for example, policies that can auto-detect confidential data and block external sharing or monitor employee data sharing to ensure they are following rules.
- Technologies that enable administrators to remotely lock devices that have been lost or stolen or wipe their data so no one can gain illegal access to sensitive government data.
- Industry-standard encryption, which serves as the last and strongest line of defense in a multilayered data protection strategy. Encryption transforms data so that only someone with the decryption key can access it, rendering it unreadable to unauthorized persons even if they break through firewalls, infiltrate the network, or bypass the permissions on internal machines.

3. Use Hardware That Supports Security Technology

Protecting devices, systems, and data cannot be achieved by software alone; for software to be fully effective it must work with hardware that has security built in. State governments must look for hardware that follows secure boot standards, uses technologies such as the Trusted Platform Module, and supports biometric identification technologies.

- UEFI with Secure Boot ensures that when a device starts up, it uses only software that the device manufacturer trusts.
- The Trusted Platform Module is a secure cryptographic module that implements cryptographic functions such as encryption and decryption. It contains a protected enclave on a device and includes physical security mechanisms to make it tamper-resistant by malware. It also generates, stores, and limits the use of cryptographic keys—technology that transposes plain text into cipher text and vice versa—to ensure that communication is secure and private.
- Biometric identification technologies are authentication methods that include fingerprint scanning, iris and facial recognition, and voice identification.

4. Enable Modern Browser Security

The web browser acts as a first point of entry to the vast resources available online, but it can also serve as a doorway for bad actors to break into a network and threaten critical systems and the security of sensitive data.

To guard against this, states can employ such modern security features as:

- A certificate reputation system, which can detect fraudulent digital certificates and flag them if they are untrustworthy.
- HTTP Strict Transport Security, which helps secure connections to important sites, like those of banks or state government.
- Windows Defender Application Guard that defends against targeted attacks. When an employee visits a site that the network administrator does not recognize or trust, Application Guard steps in to isolate the potential threat.

5. Protect Against Cyberattacks Based on Vulnerabilities

There are times when an attacker can target an organization using an unknown or unpatched vulnerability in its software—a particularly difficult intrusion to prevent. Exploit mitigation technology built into operating systems and other software, such as Windows Defender Exploit Guard, provides visibility into areas that may have gone unnoticed, and enables organizations to manage and reduce the totality of these vulnerabilities (the attack surface) in applications that employees use, thereby making an organization less vulnerable to such intrusions.

6. Guard Against Advanced Threats

An advanced threat involves sophisticated malware or stealthy hacking attacks that target the sensitive data of a specific entity, like a state government, for either financial or political reasons. States can defend their systems against such threats using solutions available either as software or a service. Most include some combination of securing the endpoints (employee devices and organizational servers), defending email gateways to the system, and automated malware protection. Solutions also require a central point from which to correlate and analyze alerts and manage defenses, such as Windows Defender Advanced Threat Protection, which helps detect, report on, and respond to advanced threats to a network.

7. Manage Computer Assets Over Time and Keep Them Up to Date

A 2011 census determined that there were over 16.4 million full-time state employees across the United States.[36] Based on a rough (and probably low) estimate that each employee uses three devices for work—a government computer, a personal computer, and a mobile phone—that translates into almost 50 million devices that state governments must protect, in addition to servers and other computers that states use to process and store data.

Managing the lifecycle—purchase, deployment, maintenance, use and disposal—of all the hardware and the software that runs on it is difficult, expensive, and complex. State governments must adopt measures to ensure strong governance over their assets to help configure, maintain, update, and decommission software (and hardware) over time. Technology, such as Microsoft Software Asset Management, can help states protect the security of, track, and get the most out of hardware and software.

In addition, as employees increasingly use their own devices at work, organizations must find the right balance between allowing employees to choose the devices they use, while making sure those devices have access to the right set of applications and meet corporate data protection and compliance requirements. To achieve this, states can use management systems such as System Center Configuration to configure, update, and monitor PCs, mobile devices, and servers from a single infrastructure and administrative console. Not only does this decrease risk, but it is also enormously cost effective, lowering the costs associated with managing many devices.

What is a digital certificate?

When you visit a web site—your bank, for example—your browser relies on a *digital certificate* to ensure that you are connected to the intended website. For the certificate to be considered valid, it must be issued by a trusted authority. This is similar to a driver's license, which is valid and accepted only if it is issued by a state department of licensing. On the web, a Trusted Certification Authority issues certificates for websites; its certificate is considered legitimate by a browser just like a driver's license issued by a department of licensing is considered a valid form of identification.

[36] State and Local Governments Employ 16.4 Million Full-Time Equivalent Employees in 2011, Census Bureau Reports. United States Census Bureau, August 23, 2012.


Microsoft