Local Governments, Global Threats:

Top of Mind Cybersecurity Trends for State and Local Leaders in 2020

Guidehouse

Executive Summary

Government services are increasingly at risk by the new technologies that enable them. Sophisticated cybercriminals, hackers, and malicious actors now attack state and local government technology systems daily and seek to inflict financial, reputational, and physical damages to their targets. By nature of their large organizational structures, limited budgets, and complex political landscapes, government IT departments face a myriad of challenges in responding to these threats. Guidehouse identifies 10 key trends in cybersecurity that should be at the top of every state and local government CISO's mind for 2020 as they decide how best to lower their security risk profile.

Introduction

Gone are the days when random hackers or teenagers running code in their basements posed the greatest cybersecurity threats. Now, state and local governments are top targets of well-funded professional cyber criminals. Using various means to debilitate business processes, steal public records or data, and extort unprepared organizations for ransom, cases abound of governments being caught unprepared or ill-equipped to respond and recover from a cyberattack. For example, in March 2018, the City of Atlanta was paralyzed by a hack that held the city hostage.[1] The Atlanta Municipal Court could not validate warrants and police reports had to be done by hand for almost a week. One month later, the Colorado Department of Transportation was impacted by a similar attack, seriously limiting the agency's functionality and costing over $1M in damages to its system.[2,3] Authorities continue to speculate on the sources of these attacks, but it is clear that they are not the work of random hackers. Rather, they are the work of nefarious criminals. Responses and patches are only met by attackers adjusting their tactics to find new points of entry, new vulnerabilities, and new means to damage government services and reputations.

Politicians tout the cost savings made possible by technology and automation in their states and communities. Citizens appreciate increased access and greater convenience of renewing a license online or enrolling in health insurance. However, these improvements rely on state and local government IT departments to ensure that agencies function and deliver the services citizens need. E-government services with single sign-on access portals, user-friendly websites, and online payments are becoming political priorities. Internet of things capabilities unlock new revenue-saving and monitoring opportunities. IT functions spread across multiple agencies are undergoing consolidation to enjoy economies of scale. By nature of accessing these government services and operating in local jurisdictions, citizens increasingly provide valuable data to government servers. These forces all combine to exponentially increase the amount of data managed by government, expand interdependencies between systems, and heighten security risks and responsibilities.

Given the cybersecurity challenge to address new and evolving threats in an era of e-government, how can CISO's prioritize their efforts and make inroads on building a more resilient government IT infrastructure? We identify several leading trends in cybersecurity, emerging threats, and potential solutions that should be on the top of CISOs minds in 2020.

[1] Lily Hay Newman, "Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare," Wired, April 23, 2018. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[2] Benjamin Freed, "Colorado has spent more than $1 million bailing out from ransomware attack," StateScoop, April 10, 2018. https://statescoop.com/colorado-has-spent-more-than-1-million-bailing-out-from-ransomware-attack/

[3] Colorado Department of Transportation, "CDOT Cyber Incident: After-Action Report," July 17, 2018. https://www.colorado.gov/pacific/dhsem/atom/129636

Human Factor in Security:

Cybersecurity is often focused on technology, without recognizing the role of people and process in preventing attacks

Users are often the weakest link in an era of increasingly sophisticated attacks. While quickly procuring and deploying technology is alluring to address a daunting cybersecurity threat, the best cybersecurity defenses are thoughtful about the people and processes embedded in any technology system. Phishing attacks, a form of social engineering using deceptive tactics to trick you into disclosing personal information such as user names and passwords, against state and local systems occur daily, often in the hundreds, if not thousands for larger states and cities. It is estimated that more than 55% of all e-mail traffic was spam in 2017[4] and that 4% of all internet users fall for a phishing attempt.[5] Most systems are compromised within minutes of a cybersecurity incident and breaches in the public sector often go undetected for years making swift reporting of potential incidents critical. [6]

GUIDEHOUSE PERSPECTIVE

Many breaches start on the inside, and the first step to protecting the security of large IT systems starts with internal education and awareness. Most importantly, information security should be approached as an organizational mission, not simply an IT issue.

- Start with your leadership. Promote cyber awareness from the top down to build a culture of cyber awareness. Leadership should model and encourage cybersecurity best practices and consider cybersecurity when setting organizational strategy objectives and tasks.
- Ensure security awareness. Design a training that's short, simple, engaging, and recurring. Make the training mandatory to drive compliance.
- Encourage reporting and cybersecurity data sharing. Provide resources and develop a culture of disclosure for employees to identify and elevate potential incidents quickly.

Incident Response:

It is not a matter of "if" you will be breached, but "when"

It takes an average of 197 days for an organization to become aware of a breach and 69 days to contain it.[7] Due to the nature and sensitivity of data stored in them, government information systems and applications are an attractive target for cybersecurity adversaries. State and local governments must face the reality that it is not a matter of "if" you will be breached, but "when" and how you will respond. Responding to a cybersecurity incident appropriately ensures the confidentiality, availability, and integrity of data stored in government systems. Having incident response policies, plans, and procedures in place is critical in guiding government organizations and agencies to respond to an incident and minimize the impact and resulting disruption of services.

GUIDEHOUSE PERSPECTIVE

Security related incidents occur all the time. Knowing your organization's critical assets and defining roles and responsibilities for responding to a crisis is important. Organizations must respond to incidents based on the procedures outlined in their incident response policy or plan and take steps to develop a plan if it is outdated or not available.

- Practice beforehand. Table-top exercises that engage leaders and technicians at all levels should be conducted to test defined incident response procedures. Incident response plans and policies should be reviewed periodically and updated based on lessons learned from previous incidents.
- Have a contract in place beforehand with vendors that specialize in computer security incident response services to help your organization respond to breaches immediately.
- Consider purchasing cybersecurity insurance policies to mitigate losses from cybersecurity incidents. A robust cybersecurity insurance program may help strengthen an organization's overall security posture by providing incentives such as additional coverage and reduced premiums based on the level of self-protection.

[4] Symantec Corporation, "Internet Security Threat Report (ISTR): Volume 23," March, 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
[5] Verizon, "2018 Data Breach Investigations Report: Executive Summary," 2018. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf
[6] Verizon, "2017 Data Breach Investigations Report," 2017. https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf
[7] Ponemon Institute sponsored by IBM Security, "2018 Cost of a Data Breach Study: Global Overview," July 2018.

Workforce Development:

Attracting and developing talent amidst a cyber-skills shortage impacts all organizations and is especially acute in the public sector

Cybersecurity and advanced IT skills are in high demand as organizations, both public and private, compete for talent to protect themselves from sophisticated attacks and meet new compliance obligations. Private sector companies and service providers offer monetary incentives that are difficult for public sector IT organizations to compete with. Schools and universities increasingly emphasize IT and cybersecurity training to expand the cyber workforce and match job training to in-demand skills. As cyber criminals constantly seek new means of entry to exploit vulnerabilities or inflict damage on key systems, cybersecurity teams must constantly evolve with these threats, developing new skills and maintaining awareness of new developments across the wide field of cybersecurity.

GUIDEHOUSE PERSPECTIVE

Responding to new technologies requires constant emphasis on training and development within your organization and focus on the cultivation of new talent. Working with universities, consortia, and public-private workforce development or tech ecosystem organizations can create pipelines of talent and information and skills sharing between the public and private sector.

- Embrace partnerships and use the convening power of government to bring together resources and generate discussion between the public and private IT community. Host cybersecurity events to encourage knowledge-sharing. Pursue partnerships with private sector organizations to exchange best practices and discuss cybersecurity approaches and challenges.
- Coordinate internships with local universities to bring in new talent and inspire an appreciation for government IT and the unique challenges government faces in deploying and managing IT resources.
- Develop skills internally by sharing best practices and resources. Encourage employees to convene internal working groups and networking events and develop online resources such as internal blogs and videos to spread new tech ideas and explain current work challenges to a broader audience.

Identity and Access Management:

Ensuring the right people have the right access to the right resources at the right time throughout the employee lifecycle

Security professionals refer to identity as the new security perimeter. Physical and network security perimeters have been rendered less efficient as modern business and technology processes are increasingly distributed by interconnected networks and technologies such as web services, software as a service (SaaS), and dispersed workforces that work remotely or access services from various endpoints. When done correctly, identity and access management (IAM) ensures the right people have the right access to the right resources at the right time. Implementing an effective IAM strategy encompasses many technologies including user provisioning, single-sign on, privilege access management, password management, role based access control, multi-factor authentication, compliance and user recertification, and identity proofing. These technologies coupled with an overall IAM strategy introduce identity governance and automation reducing the risk of unauthorized access and limiting the expansiveness of a breach.

GUIDEHOUSE PERSPECTIVE

IAM solutions are not just technically challenging. Their implementation also forces you to look at your existing identity management processes that are often flawed or nonexistent. Tackling IAM is a business transformation effort that will challenge your organization's existing culture and processes and will require coordination with many stakeholders beyond the IT department.

- Start with a long term strategy that takes into account businesses needs surrounding identity. Consider all benefits and impacts of an IAM program and how you will rationalize the decision to implement IAM. You may need to emphasize security posture, cost savings, or process efficiencies to different groups to gain buy-in, drive your technology purchase choices, and design implementation priorities.
- Prioritize protecting access to your most critical systems and resources first.
- Remember that a successful IAM program involves people, process, and technology. Implementation requires investment and commitment from many different stakeholders both within and beyond the IT department. Many organizations make the mistake of focusing on technology only, and fail.

Application Security:

Critical business functions depend on applications that are only as safe as their code and the attention devoted to them

State and local governments deploy various off-the-shelf and in-house applications to carry out day-to-day functions and deliver services to their constituents. Both internal and constituent facing applications are under constant threat of attack starting with the application code. Faulty code or vulnerabilities result in data breaches, leaks, and disruptions to staff work and service outputs. The cost of fixing vulnerabilities after an application is released in production is 30 times more than in the design and architecture phases of the software development lifecycle (SDLC).[8] Therefore it is more important than ever to proactively identify and remediate code related vulnerabilities and defects in the earlier phases of the SDLC.

GUIDEHOUSE PERSPECTIVE

In an age of digital transformation, security is no longer an afterthought. State and local governments must employ a risk-based approach to application security that can help in prioritizing applications for more stringent security reviews and code development.

- Prioritize applications based on their risk profiles. Application risk profiles should be determined using criteria including application user base, sensitivity of data handled by application, and the operational and business impact if the application goes down. Use this risk profile and assessment when determining the security rigor that an application is subjected to in the SDLC with your organization's most critical applications demanding the greatest security oversight and scrutiny.
- Think like an adversary. Consider implementing an enterprise-wide threat modeling process that can help your organization identify threats and threat vectors that applications are susceptible to. Putting yourself in an attacker's shoes gives you a wider picture of the threat landscape and aids in the prioritization of mitigation efforts to match allocated budget and resources.

Cloud Security:

Don't let "economy of scale" also apply to your cybersecurity weaknesses

Enabled by virtualization technologies and the ubiquitous presence of the internet, cloud technology applies economy of scale principles to software infrastructure with the mission of making them cheaper and more reliable. Many technology solutions are now shifting to "as-a-service" models and away from on premise technology. Following the path of private sector organizations, state and local governments are lowering on premise server and software costs and relinquishing data and processes to cloud technology. With this shift comes the challenge of protecting the data that organizations have distributed to cloud providers.

GUIDEHOUSE PERSPECTIVE

Moving to the cloud has the potential to enhance your security posture. Cloud providers are able to implement security controls that would be difficult for agencies to implement on their own. The savings from deploying cloud solutions may free up resources to dedicate to security elsewhere in your organization.

- Consider certifications such as FedRAMP or SOC 2 when choosing your cloud solution. FedRAMP certification follows NIST 800-53 and is a compliance requirement supporting the implementation of the Federal government's "cloud first" initiative. SOC2, established by the American Institute of CPAs, is a common IT security requirement adopted by most SaaS companies to minimize risk and ensure security of cloud data.
- While the responsibility of safekeeping data and ensuring availability of data in the cloud remains entirely yours, it is possible to transfer risk to your provider using your contract agreement and service-level agreement (SLA).
- Implement access management controls such as multi-factor authentication to prevent unauthorized access to critical systems and resources that reside in the cloud. Consider leveraging encryption capabilities provided by your Cloud Service Provider (CSP) to protect data at rest.

[8] IBM, "Minimizing code defects to improve software quality and lower development costs," October 2008. ftp://ftp.software.ibm.com/software/rational/info/do-more/RAW14109USEN.pdf

Mobile Device Security:

Staff and constituents now carry a risk to your IT infrastructure in their pockets

An increasing amount of online transactions are shifting from desktop computers to mobile devices. In October 2016, worldwide mobile internet traffic surpassed desktop traffic for the first time, a trend that has only continued. The ubiquity and convenience of mobile devices and mobile-enabled applications has lead public sector staff and the public at large to increasingly rely on these devices to access state services and business applications. While these devices improve convenience for constituents and efficiency for state workers, they introduce new security vulnerabilities. These security risks include vulnerabilities in the mobile device technology stack (e.g. security update delays, jailbreaking), mobile networks (e.g. data/voice eavesdropping, tracking), physical systems (e.g. tampering, theft), and mobile applications (e.g. vulnerable/compromised applications). Coupled with common bring-your-own-device (BYOD) policies, these risks pose significant threats to public sector IT infrastructure.

GUIDEHOUSE PERSPECTIVE

Given that mobile devices are widely used outside the organization's network range and firewalls, it is strongly recommended that organizations implement proactive security controls that minimize the risk of unauthorized access to data stored on these devices. In addition to protecting data at rest, proper measures should be taken to ensure security of data in transit. For example, mobile devices connecting to insecure Wi-Fi networks can open doors for man-in-the-middle attacks.

- Start with clearly defined mobile device policies and educate users on compliance. Staff and constituents should follow security policies (e.g., password requirements, bring-your-own device regulations, patching and operating system updates etc.) to prevent inadvertent disclosure of sensitive data.
- Introduce authentication mechanisms to control access to devices and mobile-enabled applications.
- Consider implementing a mobile security solution that detects threats at a device, network, and application level. Mobile Device Management (MDM) solutions may be explored to enforce governance on mobile device usage.

IoT Security:

The proliferation of IoT devices creates an exponential security threat

Network enabled sensors and controls are being installed in everything from industrial valves to refrigerators and washing machines introducing the ability to monitor, control, and update these devices remotely. This internet of things (IoT) opens up new opportunities for asset tracking and management, but also increases risks of hacking and security vulnerabilities. Symantec reports there was a 600% increase in hacking attacks on IoT devices between 2016 and 2017. The introduction of remote access and monitoring creates many security challenges, especially as security updates and firmware patches need to be sent to the individual asset level. Weak security in a Wi-Fi enabled toaster could be exploited to access other parts of the network and hackers are also exploiting supply chain vulnerabilities seeking out the weakest link in a software or manufacturing supply chain. As connected devices become more common and depended on to deliver key services, the security threat in an IoT world is exponential.

GUIDEHOUSE PERSPECTIVE

Many IoT devices are consumer products without the security features and controls that large organizations such as state and local governments require. Security flaws in these devices often result from manufacturers who are focused on getting new consumer products quick to market and who do not consider interoperability of connected products with other devices on the same network.

- Update default settings. Many past security breaches, including a large IoT device enabled botnet that attacked the service provider Dyn responsible for websites such as Amazon, Twitter were caused by hackers exploiting default security protocols such as passwords that were not changed by users after purchase.
- Consider linking critical devices to an intranet, rather than to external facing Wi-Fi network. IoT security risks extend to the physical world as IoT sensor vulnerabilities could be exploited to turn on gas in a building or overpower machinery resulting in physical damage to property and assets.
- Monitoring is crucial. Maintain a comprehensive inventory of all IoT assets and monitor for misuse and for security patches that may not be immediately pushed to devices.

[9] StatCounter, "Mobile and tablet internet usage exceeds desktop for first time worldwide," November 1, 2016. http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide

[10] Department of Homeland Security, "Study on Mobile Device Security," April 2017. https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

[11] Symantec Corporation, "Internet Security Threat Report (ISTR): Volume 23," March, 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[12] Nicky Woolf, "DDoS attach that disrupted internet was largest of its kind in history, experts say," The Guardian, October 26, 2016. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Monitoring and Logging:

Effective monitoring provides a real-time view of an organization's security status and identifies vulnerabilities that may be exploited by adversaries

Government organizations and agencies require continuous monitoring of their critical infrastructure to identify and quickly respond to cybersecurity incidents at an early stage. In the public sector, breaches often take years to discover, leaving IT infrastructure and data at risk until it's too late to protect against leaks or unauthorized access. Proactive monitoring and logging solutions provide organizations the ability to monitor activities and reporting options to analyze threats allowing faster remediation of vulnerabilities. Many compliance programs and regulations such as PCI, HIPAA, FISMA, and FedRAMP require organizations to have monitoring and logging capabilities in place to meet prescribed levels of security.

GUIDEHOUSE PERSPECTIVE

Monitoring and logging is an integral part of an organization's comprehensive security strategy. Though effective in firefighting vulnerabilities, it is important to understand that it is just one step in a larger journey towards cyber resilience.

- Proactive monitoring and logging can alert organizations and help prevent the frequency and impact of cybersecurity incidents. Monitoring an organization's infrastructure and applications is critical in safeguarding privileged access to IT systems and resources. Logs may be integrated with Security Incident and Event Management (SIEM) solutions to provide near real-time analysis of security alerts generated by applications and infrastructure components.
- Consider establishing a Security Operations Center (SOC). Mature organizations can benefit from continuously monitoring their IT environment improving their overall cyber preparedness and defense posture.

Disaster Recovery and Cyber Resilience:

Prepare for the worst by understanding your existing capabilities and the investments needed to recover quickly from a disaster event

Data loss and technology disruption costs can be catastrophic for an organization. Ransomware, malware, natural disasters, and human error each threaten critical data and technology that drive business processes. Financial and reputational damages can be extensive and it may take days, weeks, or months to bring systems back online or for services to return to normal. High-profile ransomware cases in recent years such as that in Atlanta highlight the importance of introducing resiliency into core systems and developing a disaster recovery plan to respond to inevitable disruptions.

GUIDEHOUSE PERSPECTIVE

Investments made today can avert significant costs in the future from disrupted processes or lost data. Many public sector organizations are deeply siloed in their recovery capabilities with application knowledge and recovery capabilities resting in a single application owner. Disaster recovery requires a comprehensive and centralized approach to identify systems and capabilities, define desired recovery capabilities, and implement strategies to prepare systems for disaster.

- Consider a business impact analysis to understand the full extent of potential disaster scenarios on your core technology and business processes. Start by developing an inventory of all applications and technology systems, determining dependencies and criticalities between these systems, and then using industry best practices to prioritize recovery needs and solutions.
- Understand that a balance must be struck between the costs of maintaining robust recovery and storage systems with the costs of disruption to your organization. Developing disaster recovery infrastructure recovery time objectives (RTO) and recovery point objectives (RPO) must be grounded in business decisions and how the costs of meeting those objectives through new technology investments compare to the costs of disruption or data loss.

[13] Verizon, "2017 Data Breach Investigations Report," 2017. https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Conclusion

From eliminating a trip to the DMV to selecting health insurance, technology has transformed government. It has increased access to critical services, improved government customer service, expanded citizen engagement, and streamlined the bureaucratic processes government is most known for. The challenge now is how to protect these benefits from the destruction or disruption of malicious actors. Deploying technology in government increases security risks and requires a thoughtful and coordinated response to prepare for inevitable attacks, leaks, and data loss. The key ideas and themes introduced above provide a short list of priorities for the coming year that should be on the top of mind for state and local government CISOs. All of these ideas rest on a belief that any security strategy must be guided by business requirements, taking into account the people and process at the heart of any IT organization. State and local government CISOs have an obligation to protect the data of their constituents and protect the technologies that make government work well. The ideas above are first steps in a more robust and constantly evolving strategy of resilience for state and local government data and systems.

Email: statelocal@guidehouse.com / **Web:** guidehouse.com / @guidehouse linkedin.com/company/guidehouse