IRON MOUNTAIN®

GOVERNMENT SOLUTIONS

WHITE PAPER

ENHANCING CITIZEN TRUST

PRIVACY AND DATA SECURITY IS STEP ONE

CONTENTS

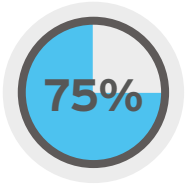
GROWTH IN DIGITAL CITIZEN INFORMATION

Citizens are demanding state and local governments and educational institutions to secure their most valuable personally identifiable information (PII). These organizations store data about constituents, including Social Security numbers (SSNs), driver's licenses, tax returns, health and school records, voter registration databases and more.

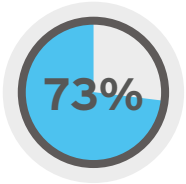
As agencies and educational institutions continue to offer new and valuable digital services to citizens, the vast amount of data collected and stored increases exponentially. Protecting this information has become a top priority for government and educational CIOs.

In the 2022 Public Sector Identity Index[1], conducted by AuthO and Market Connections, the vast majority of government entities surveyed indicated that they are considering expansion of their digital services in the next two years. With these expanded service offerings, organizations expect rapid growth in constituent data they will be held accountable for. As a result, these same government entities consider protecting citizen's privacy and data one of their most critically important priorities.

A 2021 Deloitte survey[2] of improving trust in state and local government revealed that individuals who are pleased with a state government's digital services tend to rate the state highly in measures of overall trust. Citizens had a very positive view of state agencies when they felt that digital services were easy to use, web-based services helped them accomplish their needs, and the government safeguarded their data securely. At the same time, when citizens found digital services difficult to use or inadequate, their trust of the state government agency was significantly lower. These results suggest a reasonable correlation between citizens' digital experiences and their general confidence in the government.



Government entities considering expansion of their digital services



Government entities rank protecting citizen's privacy and data as critically important

Source: AuthO and Market Connections

DATA PROTECTION PRIORITIZATION

As expectations and demand for digital services increases, so does the need to protect privacy to ensure citizen information is secure. Government agencies and educational institutions must follow the highest standard of privacy due to the amount of sensitive information that is collected. Besides the associated costs of a data breach, government entities run the risk of fines associated with non-compliance, potential lawsuits and most importantly the loss of citizen's trust.

State and local governments, as well as education institutions, are gatekeepers for critical records – voter, tax, school, financial and more. Because of the enormity of the information contained within these organizations, it is not a surprise they have become a focal point of attack and a security risk for constituents.

[1] 2022 Public Sector Identity Index
[2] 2021 Deloitte Survey

GOVERNMENT REGULATIONS

Privacy laws and directives enacted by state and local governments provide guidance on protecting citizens' data. Many of these laws have been enacted in just the past several years, as cybersecurity threats and attacks against the government have increased[1].

In the education sector, the Family Educational Rights and Privacy Act (FERPA), a federal law that protects the privacy of student education records, applies to all colleges and universities that receive funds under an applicable program of the U.S. Department of Education. It's essentially the education market's version of the Health Insurance Portability and Accountability Act (HIPAA) – another legislative measure aimed at protecting privacy.

Adhering to privacy laws and regulations adds a layer of complexity to the information management function, providing significant challenges for government and educational institutions.

As cybersecurity threats and attacks against the government have increased[3]:

AT LEAST 32

of these states require by law that their agencies have measures implemented to ensure the protection of their systems and stored data[3].

AT LEAST 35

have enacted laws that require private and governmental entities to destroy, dispose, or make personal information unreadable or indecipherable.

PROTECTING CITIZENS' PRIVACY

As the expansion of customer data continues to grow, this presents an attractive opportunity for cyber criminals seeking to steal and sell data for profit as well as use illegally acquired data to breach sensitive networks, disrupt critical infrastructure, or deploy denial-of-service attacks.

Protecting PII and maintaining citizens' trust has never been more critical for government and educational institutions. Since PII can be stored anywhere, on unused servers and mobile devices, in file cabinets, or even in the backseat of a car of a remote employee, it requires a significant focus by these organizations to attempt to mitigate lost or stolen data. State and local agencies and educational institutions are facing a barrage of attack vectors – from network intrusions to lost or stolen records or devices to simple errors made by employees – with the real possibility of exposing constituents' personal data.

[3] National Conference of State Legislatures

Ransomware in state, local and education markets has become a key tactic for cyber criminals looking to take control of vulnerable systems and information. A January 2022 report by Emsisoft found at least 77 state / municipal governments and 1,043 schools were impacted by ransomware incidents in 2021. One state alone faced a ransomware attack costing $18 million, as well as multiple cyber attacks preventing hundreds of thousands from accessing both medical care and education classes[4].

Loss of critical data and information are an enormous risk of state, local and education organizations because they know data loss erodes constituents' trust. In early 2022, personal information of more than a quarter-million licensed professionals may have been exposed in a breach of a Washington State Department of Licensing database. The compromised data may include SSNs, birth dates, driver's license numbers and other PII[5].

State and local agencies and educational institutions often lack the internal resources and technology required to effectively maintain their expanding digital information. As a result, government entities must look for dynamic ways to meet state-based privacy laws / regulations in a cost effective manner.

Cyberattacks are not the only way records are breached, and it's not always a hacker behind a computer infiltrating a network. The 2021 Verizon Data Breach Investigations Report shows that physical incidents are prevalent and involve theft of paperwork or devices such as laptops, phones and storage devices. "Devices continue to be lost or stolen, a pattern that is unlikely to change anytime soon. While the actor may be Internal (for loss) or External (for theft), the controls to protect the data on these devices remain constant," according to the report[6].

The National Association of State Chief Information Officers (NASCIO) latest annual State CIO Top 10 Priorities ranks "Cybersecurity and Risk Management" as the top concern in 2022, with a specific focus on governance, data protection, insider threats and third-party risk[7]. EDUCAUSE, a nonprofit association whose mission is to advance higher education through the use of information technology, listed "developing processes and controls, institutional infrastructure and institutional workforce skills to protect and secure data and supply-chain integrity" as its number-one IT issue for 2022[8].

[4] Emsisoft
[5] Washington State Department of Licensing
[6] Verizon Data Breach Investigations Report
[7] NASCIO Top 10
[8] EDUCAUSE

DATA SECURITY AND PROPER DISPOSITION

INFORMATION ASSESSMENT AND TRACKING

State, local and education organizations have a significant task in front of them to remain compliant with statutes, and support hybrid working environments, while still mitigating security and privacy risks. They need to be proactive in creating comprehensive risk management strategies that adapt to the needs and capabilities of constituents. The organizations must also establish a comprehensive data management framework that includes research and insights into their various IT systems.

Having a complete inventory of information repositories, stored data, and applicable regulations is an essential first step in developing a comprehensive data management framework to protect PII for citizens. This includes implementing processes to manage how future information will be tracked through the entire lifecycle - beginning when data is created and continuing through its usage, storage, retrieval and maintenance.

1. Information Privacy Assessment

Conducting a comprehensive privacy assessment audit will help state, local and education organizations define the necessary requirements associated with risk management as well as retention and compliance to better control information; from creation to final disposition.

A complete audit includes inventory of stored data and developing an information roadmap of records (i.e., location and who is responsible for managing them). This improves an organization's analytical insights by better understanding their data-driven processes, information systems, and the most sensitive/confidential information.

At the conclusion of the initial privacy assessment audit, organizations should use their data inventory findings to perform an additional review of their data protection needs and regulatory obligations. The findings from both sets of analyses will form the foundation of an information management program.

2. Information Classification

Data classification provides a mechanism to manage the control and disposition of records. State, local and education organizations should perform a large-scale classification of their data inventory to comply with retention schedules and maintain records in accordance with legal, regulatory or privacy requirements.

This process of "content classification" leverages rules databases and software to determine how informations set need to be maintained and managed; ensuring that records are properly preserved and only become eligible for disposition in accordance with their respective retention policies.

The City of Albuquerque's Office of Internal Audit conducted a PII security audit on its city systems in 2019 and set the stage for proper information lifecycle management.

Identified Improvements:

- **Maintaining an active inventory of systems and devices containing PII**
- **Ensuring policies and procedures and underlying controls for classifying and safeguarding PII at the department level are established**
- **Ensuring that employees with access to PII are trained on and aware of their responsibility to safeguard PII**

REDUCING RISK WITH PROPER IT DISPOSITION

As technology devices become outdated or reach the end of their useful life, state, local and education organizations need to ensure that individual assets are disposed of in a secure manner that protects privacy on all citizen PII. IT Asset Disposition (ITAD) services enable organizations to securely dispose of obsolete technology assets in an environmentally-responsible manner.

A comprehensive ITAD program should be part of every state, local and education organizations' overall data management strategy. It's critical that the program is consistent throughout the organization and crucial that all employees are aware of, and understand, the policies and procedures. Organizations should also focus on tailored security that includes chronological and auditable history of possession and handling of assets.

Given the security and privacy concerns on citizen PII associated with the retirement of IT assets, organizations must ensure they are taken care of responsibly and in adherence to laws and regulations. A successful program should be viewed as a data security and environmental sustainability investment. By partnering with a leading ITAD company, agencies can avoid fines and other costs associated with mismanaged ITAD, plus share in the benefits of recycling components.

IMPACTS OF IMPROPER ITAD

Morgan Stanley[9] agreed to pay

$60 million

to settle a lawsuit after it exposed personal customer data when it failed to properly retire IT assets during a data center decommission.

The bank had to notify wealth management customers that their personal data might have been compromised, and offer two years of free credit monitoring services to affected customers.

[9] Morgan Stanley lawsuit article

CONCLUSION

In today's world of frequent cyberattacks and loss of PII, citizens want peace of mind and knowing they can trust state, local and education organizations with their most valuable information. To truly enhance citizens' trust on the journey of digital transformation, organizations need to complete a comprehensive, detailed plan to ensure PII and other data is not at risk, and meet the regulations required for compliance. When it comes to citizen trust, ensuring data privacy and security is the first step.

Iron Mountain, a global leader in information lifecycle management, provides services to state and local government and educational agencies to assist with enhancing the data privacy and security of your citizens. With solutions ranging from providing Information Governance Advisory services and content digitization to IT asset disposition, Iron Mountain is a trusted partner with 70 years of experience protecting your information assets

To talk to a representative of Iron Mountain Government Solutions, email **sled@ironmountain.com.**

IRON MOUNTAIN®

GOVERNMENT SOLUTIONS

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) is the global leader in innovative storage and information management services, storing and protecting billions of valued assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Founded in 1951 and trusted by more than 225,000 customers worldwide, Iron Mountain helps customers CLIMB HIGHER™ to transform their businesses. Through a range of services including digital transformation, data centers, secure records storage, information management, secure destruction, and art storage and logistics, Iron Mountain helps businesses bring light to their dark data, enabling customers to unlock value and intelligence from their stored digital and physical assets at speed and with security, while helping them meet their environmental goals. Visit www.ironmountain.com for more information.

USSLED-ITAD WHITEPAPER-0422