Data Privacy and the Evolving Regulatory Landscape

Strategies for Addressing Compliance

As state and local governments collect ever-growing volumes of constituents' data, protecting consumer privacy has become a significant concern. It has also increasingly become the focus of government regulation.

While the federal government oversees many data privacy laws (including the Health Insurance Portability and Accountability Act, or HIPAA, and the Electronic Communications Privacy Act), a wave of state-level consumer privacy legislation is also impacting private- and public-sector organizations. According to Center for Digital Government (CDG) research, 32 states now have privacy laws.[1] In addition, any state and local governments that gather data from citizens of the European Union are subject to the EU's General Data Protection Regulation (GDPR), which is one of the most stringent and consequential privacy laws to date.

Interpreting regulations, implementing controls and maintaining compliance over time is an extremely complicated task.

"There's a very complex morass of state and local data privacy laws and regulations. As laws and regulations and risk concerns have shifted, most organizations are not prepared to fully meet requirements," says Deborah Snyder, a CDG senior fellow and the former chief information security officer for New York state.

As part of an overall risk-based approach to data privacy and compliance, many organizations include encryption in their arsenal of compliance controls. While hardware encryption has existed for years, recently introduced file-level encryption tools on legacy systems add an important layer of protection against the cyber attacks that target software and account for the majority of breaches.

"A risk-based approach will help organizations meet reasonable

expectations of privacy," says Snyder. "Good cybersecurity is critical, but it can't address all privacy risks. Effective privacy risk management helps the organization build trust in their operations, products and services, as well as communicate privacy practices and meet compliance obligations."

Time is of the essence. If the spate of new data privacy regulations is any indicator, data privacy and regulatory compliance will become even more urgent concerns in the months ahead — especially as deadlines for compliance approach and the consequences of non-compliance pose intolerable risks.

Protecting Billions of Records

Several concurrent trends are driving the need for state and local governments to take action on data privacy:

Increasing digitization of private data and the shift to remote work. Government mainframes hold billions of records and vast amounts of personally identifiable information (PII). As organizations modernize and transition to remote work, they need to share and integrate that data with processes in the cloud, systems outside the enterprise network and mobile devices — all of which vastly expand the attack surface.

Escalating number and severity of data breaches. Telework-related phishing attacks are on the rise, and ransomware is rampant. The threat affects all levels and aspects of government. In Nevada last year, for example, a ransomware attack not only locked a school district out of systems but also published Social Security numbers, student grades and other private data.[2]

High-impact consequences of PII breaches. Breaches of private data can have a devastating impact on individuals, ranging from stolen identities and financial losses to public sharing of highly personal information. Organizations suffer too. Besides reputation damage and fines for breaches, recovery costs for PII breaches average $150 per record.[3]

Steep Climb to Compliance

Data privacy is the right of a person to have control over how their personal information is collected and used. Data protection is the first step in keeping sensitive data private and meeting compliance requirements. However, as different legislatures enact data privacy laws, compliance is becoming increasingly fragmented. In addition, the path to achieving compliance is not well defined.

"The climb is made steeper by the fact that it involves understanding decades of processes and use cases that are already in place as well as evolving new use cases that need to be considered as new technologies are adopted," says Snyder.

A number of developments have complicated agencies' compliance efforts, including:

Recent and emerging legislation. Many of the state data protection laws in the U.S. were enacted within the past few years and have rapidly approaching (or already passed) deadlines for compliance. Penalties for noncompliance are stiff. The California Consumer Privacy Act, enacted in 2018 and effective as of January 1, 2020, was an early data privacy model for other states. It stipulates substantial fines and penalties for data breaches, including statutory damages of up to $750 per person whose data is breached.[4] A 2020 Florida law requires government entities to notify individuals who have been affected by a breach within 30 days of detection, or face a civil penalty of up to $500,000.[5] The massive move to remote work has created a new wave of privacy concerns, and states continue to propose legislation to strengthen or implement compliance, breach notification and data protection. As of April 2020, lawmakers in at least 18 states were considering proposed data legislation.[6]

Vague language around controls. While legislation clearly mandates protection of data in transit and data at rest, most — if not all — laws steer away from specifying exactly which controls should be used to protect that data. Twenty states have requirements for "reasonable" security, but definitions of reasonability vary from state to state. In addition, the word "reasonable" is associated with the legal principle of "reasonable expectation," leaving each organization to determine for itself whether its controls would constitute what's legally reasonable and satisfy regulators' expectations for protecting data privacy.

NIST cybersecurity framework as a guidepost. While the language around specific data privacy controls is vague, some state laws refer to or specify use of the NIST framework. For example, a California information security statute introduced in February 2021 would require certain state agencies "to adopt and implement information security and privacy policies, standards, and procedures based upon standards issued by the National Institute of Standards and Technology and the Federal Information Processing Standards."[7] The NIST framework includes industry

standards and best practices that specifically mention protection of data in transit and data at rest.

NIST Security and Privacy Controls as clarification. Although the NIST cybersecurity framework does not specify exactly how to protect data, a Security and Privacy provision published in September 2020[8] sheds some light on which controls are deemed best practices by NIST — and potentially by legislators. The document identifies 86 security and privacy controls and establishes encryption as one of multiple valid methods for protecting data. This is welcome validation for many organizations and security professionals who — as part of a multilayered approach to privacy risk management — have made encryption their tool of choice for rendering data unreadable.

Strategies to Help Protect Data

Protecting data and complying with data privacy regulations require multiple layers of control and a solid, risk-based approach. The following controls and strategies are important components of this approach:

Disk-level encryption. Disk-level encryption protects data privacy and integrity by limiting access to the physical database disk in the event someone steals the disk. When executed on a high-performance platform, hardware encryption provides the strongest levels of disk encryption while eliminating the CPU overhead that is often associated with encryption processes.

Many organizations may mistakenly believe that simply protecting database disks and other hardware is sufficient. But the truth is that physical hardware breaches account for very few data breaches. "The data that lives on mainframes is no longer siloed to that application," says Chris Oskuie, vice president of state and local government and education at Software AG Government Solutions. "Organizations want to use it for modernization and data sharing initiatives. Encrypting that data not only reduces the risk and exposure, but also enables business by making data sharing initiatives more palatable."

> **"Encrypting data not only reduces the risk and exposure, but also enables business by making data sharing initiatives more palatable."**
>
> *— Chris Oskuie, Vice President of State and Local Government and Education at Software AG Government Solutions*

Dataset encryption. This adds another layer of protection by encrypting the actual database information itself, rendering the data useless in the event a cybercriminal bypasses other controls. File-level encryption addresses software-based breaches, which account for the majority of data breaches and are mainly caused by cloud misconfiguration, compromised credentials, third-party software vulnerabilities, phishing and malicious insiders.[9] File-level encryption can be quickly deployed on top of hardware encryption solutions such as IBM z/OS. Depending on their needs, organizations can easily enable encryption of entire databases or specific files.

User authentication and access. Data protection, cybersecurity and compliance with privacy laws require multiple layers of defense. To ensure the right people have the right level of access to the right datasets and other resources, organizations often include multifactor authentication and role-based access control. Multifactor authentication requires a user to separately confirm they are who they purport to be. Role-based access control, meanwhile, limits data access based on a user's role or "need to know."

Auditing tools. Auditing tools use artificial intelligence and machine learning to detect unauthorized access. Organizations can track and detect unusual behavior — either by authorized or unauthorized users — that may indicate abuse or a breach. Customized rules can flag suspicious behavior, such as a user attempting to read an entire child support database, access the database at unusual hours or change data. Auditing tools also maintain records of database access and activity and allow organizations to rapidly prepare reports to help demonstrate compliance.

Moving Toward Compliance

As government organizations work to comply with current and future privacy laws, there are some key measures to keep in mind.

Start by instituting data management and governance processes. Understand your organization's legal obligations related to privacy regulations. Then determine what data needs protection and what privacy values should apply, including autonomy, anonymity, dignity, transparency and data control. Connect those values and policies with a privacy risk assessment to build trust into operations, products and services. Ensure employees know their roles and responsibilities related to privacy and provide training so they can make better decisions about effectively managing privacy risks.

Use the NIST privacy framework to create, assess or improve your privacy risk management program. The voluntary framework is designed to work with the NIST cybersecurity framework and follows its structure in terms of profiles, implementation tiers and other components. "NIST can be a bit overwhelming to digest sometimes, but it provides well-vetted standards and strategies for implementing privacy controls," says Snyder.

Many organizations don't have an accurate idea of all the data they collect, use, store and share. Establishing a mapping process helps create a foundation for understanding privacy-related risks. Map the flow of relevant data throughout the enterprise and throughout its full life cycle, from collection to disposal. Be sure to include sensitive data that exists in testing and development environments, something that's overlooked by many organizations.

Privacy and compliance risks often change due to system improvements, deployment of new technologies and services, or the introduction of new mandates. Have a plan for regularly assessing changes and their impact on current controls and policies. In addition, continue to monitor, assess and document compliance and security controls over time to ensure they're working properly and to measure progress against the NIST privacy framework or other standards.

Although the path to compliance with data privacy laws is not always clear, organizations can improve their compliance posture by taking a risk-based approach to compliance, drawing on guidance from NIST and other industry standards, and implementing multilayered data protection. A number of administrative and physical controls are required to assure compliance with data protection and privacy mandates. Hardware encryption, file-level encryption, access control and auditing help create a strong foundation for compliance and are the tools of choice for many organizations. To meet compliance deadlines and improve their overall risk posture, organizations should act now to implement these foundational controls.

This paper was written and produced by the Center for Digital Government, with information and input from Software AG.

Endnotes:

1. Center for Digital Government. Data Security Policies. April 2020.
2. T. Hobbs, Wall Street Journal. Hacker Releases Information on Las Vegas-Area Students After Officials Don't Pay Ransom. September 2020. https://www.wsj.com/articles/hacker-releases-information-on-las-vegas-area-students-after-officials-dont-pay-ransom-11601297930
3. IBM Security / Ponemon. Cost of a Data Breach Report 2020. https://www.ibm.com/security/data-breach
4. California Department of Justice. California Consumer Privacy Act. Accessed May 2021. https://oag.ca.gov/privacy/ccpa
5. 2020 Florida Statute § 501.171 — Security of Confidential Personal Information. Accessed May 2021. http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0501/Sections/0501.171.html
6. Center for Digital Government. Data Security Policies. April 2020.
7. California Legislative Information. AB-809. Information Security. Accessed May 2021. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB809
8. NIST. Security and Privacy Controls for Information Systems and Organizations. Accessed May 2021. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
9. IBM Security / Ponemon. Cost of a Data Breach Report 2020. https://www.ibm.com/security/data-breach

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: software AG GOVERNMENT SOLUTIONS

Software AG Government Solutions delivers leading edge software that helps the Government connect existing, new and future technologies together. Leveraging our API and Integration platform, webMethods, and our FedRAMP authorized IT portfolio platform, Alfabet, along with our effective "Prove IT First and Prove IT Fast" approach to solving mission critical IT challenges, we specialize in helping customers optimize large scale solutions across complex enterprises. Complex IT, Simplified. Learn more at **www.softwareaggov.com**.