Protecting the Data That Matters Most

Tony Encinias, chief strategy and innovation officer, state and local government for Dell Technologies, and former CIO of the commonwealth of Pennsylvania, shares best practices to simplify data protection and compliance.

What are the challenges of protecting personal information and complying with new data privacy laws?

For one, organizations must find funding for technologies that can meet the requirements of new legislation. In addition, the skillsets to fulfill those compliance requirements are very hard to come by in today's competitive market. Another challenge is that a lot of organizations adopt public cloud offerings to increase flexibility, but they lose visibility into the location of their data and they have less control over infrastructure compliance. Data can reside anywhere, even in several different states, each with its own set of data privacy laws. Appropriate data protection controls must be in place for each jurisdiction, which further taxes skillsets, especially if a breach or other issue occurs.

What's the best strategy to protect data and address compliance?

Knowing the data's disposition is essential; that means knowing exactly where that data is housed and the type of architecture surrounding it. If the data is on premises, you can implement new technologies as appropriate. Many new tools provide data protection from a backup and access perspective. Organizations should also implement robust data classification policies. Not all data is subject to HIPAA, CJIS, IRS 1075 or other regulations. A lot of data is public domain, so it doesn't need to meet those stringent requirements. Last but not least is applying risk and compliance best practices in accordance with National Institute of Standards and Technology guidance.

Please discuss the growing importance of identity and access management (IAM) technologies in meeting privacy requirements.

Identifying people with the correct level of need-to-know access is critical. HIPAA, CJIS and other regulations clearly document who can access certain data and what they can do with it. Once organizations identify what data needs to be protected, they need a mechanism to ensure people can't access data they're not approved to see. Simple authentication technologies such as username/password are no longer capable of preventing unauthorized access. Today's best practices for protecting sensitive data include mechanisms like multifactor authentication and secure ID tokens, which strengthen identity accuracy.

How can organizations improve the user authentication experience for citizens and employees?

One approach is to utilize standardized directory structures. Having one standardized directory structure eliminates the use of multiple security personas. For example, you don't need a username/password for transportation services, another for Medicaid and another for unemployment compensation. Besides standardization of directory structures, you can also leverage social media, Department of Motor Vehicles or other large directory structures to validate credentials. The key is using a significant enough directory structure that you don't have to replicate an identity multiple times. Once you implement multifactor authentication through these mechanisms, you enhance the user experience, as well as the security required for access not only to sensitive data, but users' own personal data.

What should organizations consider as they contend with the pandemic and "the next normal"?

Organizations should avoid the temptation to skip requirements and get things out there quickly. This crisis forced organizations to establish work-from-home policies overnight. Work-from-home technologies — whether employee-owned or government-issued — must incorporate the organization's security processes and policies around sensitive data. Government-issued laptops should have remote access capability to keep OS and security product patches up to date, ensure VPN connections are working and generally maintain security standards. It's also important to conduct and continually reinforce security awareness training focused specifically on working at home or remotely. Then, make the new normal as simple as possible; have everything in place for users to just basically turn on their laptop and log into the system.

With new regulations and new technologies always at the door, how can organizations future-proof their data protection and compliance programs?

It's important to identify data that doesn't require a high level of security so you're not wasting time, effort and money on protecting it. Then, you need to keep abreast of new technology. Vendors like Dell Technologies are at the cutting edge of what's available to secure and protect data. Leverage those partners and ask a lot of questions, but also do your own homework to understand government requirements from a policy and technology perspective. Identify which data elements are impacted by regulations and need to be protected, and clearly classify that data in your policy. Finally, be realistic. No single solution can magically solve all your problems.

Learn more at **Carah.io/Data-Dell**