SEPTEMBER 28, 2022

Legaltech® news

ONLINE

ALM.

Technology and Data Security: Is Your Firm Ready?

In an evolving cybersecurity landscape, these are the steps law firms should be taking to protect client data and comply with global privacy regulations.

BY TONY DONOFRIO, VERITEXT LEGAL SOLUTIONS

Part 3 of a 3-part series on how the pandemic changed the litigation process. Find part 1 here and part 2 here.

In today's outsourced systems world, technology has created many possibilities for sharing and integrating different tools and content. Because of the options that exist, law firms both small and large can avoid investing in infrastructure and direct support for their systems.

However, this can generate increased exposure to cyberthreats as the liability risk is not fully passed on to the cloud provider when sharing client details and content in the cloud. With this evolving landscape, there are some practical things you can do today to improve and maintain an effective cybersecurity posture to ensure your clients' data remains secure.

Confronting the Evolving Cyberthreat Landscape

Software-as-a-service (SaaS) and cloud infrastructure have matured to the point that IT has become democratized. The smallest firms can utilize applications and systems that were out of reach ten years ago due to the infrastructure investment required to deploy and manage them. Even the largest firms are now leveraging SaaS and cloud technology to focus more investment on innovation.

This new norm has elevated cybersecurity risks for small or medium-size firms and has shifted those risks for larger firms that transitioned from self-managed systems to SaaS and the cloud. According to a 2020 American Bar Association survey, 29% of firms experienced a security breach—such as a lost/stolen computer or smartphone, hacker incursion, break-in or website exploit—in 2020, compared to 26% in 2019.

Consider the relevant shifts in the cyberthreat landscape and how to address them:

- ***Your firm no longer has direct oversight of physical, logical and governance controls over your data and applications. However, you are still liable to your clients for any exploits that expose their data.*** It is important to shift resources from controlling and supporting your tech to vetting and monitoring your tech providers. Many reputable cybersecurity firms can perform third-party risk assessments as well as monitor and process oversight for your providers.

Credit: gopixa/Adobe Stock

- ***Your firm may leverage SaaS integrations to internal systems and between SaaS-provided systems, multiplying the "doors" through which clients' data can be accessed by bad actors.*** These integrations can provide spectacular efficiency and innovation for your firm. However, to mitigate risk in such an integration, work with your IT provider to perform initial and periodic reviews of any system interface as well as audit reporting and review of data transacted via those channels.
- ***Your firm is faced with rapidly evolving privacy regulations, from HIPAA and HITECH to PIPEDA, GDPR and CCPA, with several countries and U.S.***

states adding or modifying their regulations at this time. Your firm can become overwhelmed in assuring compliance and addressing client questions and concerns about your compliance. Work with a qualified security expert to implement a clear, simple information security policy that includes data classification describing what types of data your firm manages and how it is to be controlled. Then continually execute education and awareness campaigns whereby all staff learns how to be vigilant about each class of data and how it is to be managed. Simplification of policy and best practices is critical to ensure compliance and to continuously evolve through changes in regulation and threats.

The Proliferation of Privacy Laws

With the growing awareness of personal information proliferation across social networks, data privacy regulations are propagating. The most impactful privacy laws today are the General Data Protection Regulation (GDPR) in the EU, the Personal Information Protection and Electronic Documents Act in Canada, and the California Consumer Privacy Act (CCPA). The GDPR, in effect since 2018, has become the most comprehensive law in the world. CCPA can be seen as the California version of the GDPR; however, its effect is considered global because California is the world's fifth-largest economy. Both laws protect consumers and businesses from security breaches of personal or otherwise protected information.

Currently, Colorado, Connecticut, Utah and Virginia are legislating data privacy laws similar to the CCPA. While the laws are similar, there are differences in violation thresholds, penalties, reporting requirements and enforcement protocols.

Due to this proliferation, it is crucial that firms:

- Implement a well-defined and simple information privacy and security policy with annual reviews to address emergent regulation and threat changes.
- Drive practice compliance with continual education and awareness campaigns.
- Validate and monitor SaaS service providers to ensure they are compliant with policy.
- Work only with service providers who demonstrate compliance with the firm's policy and practice guidance.

With the outsourcing of systems to third-party providers, it is important to not lose sight of your locally managed devices and data, which remain under your direct control as an organization. Key practices in this regard continue to be applicable, which are:

- Limit data stored on the firm's devices and encrypt those devices in general.
- Ensure firewalls and antivirus and end-point-detection software are installed on all firm devices.
- Prepare an incident management plan to identify, mitigate and resolve any potential or actual exploit.
- Your firm or service provider should have a security operations center that is capable of inspecting traffic, classifying it as safe or malicious, stopping malicious traffic and taking any necessary steps to remediate the damage as threats emerge.

Conclusion

With the shift to integrated SaaS and cloud-based technology, the threat landscape has changed, while at the same time cybercrime is booming. Firms are held hostage for millions of dollars in ransom to recover their clients' sensitive data every single day. At the same time, a confusing plethora of information privacy regulations is emerging.

The advantages of using SaaS-based tools can be enjoyed while effectively addressing the challenges by defining and continually communicating simple policy. By partnering with service providers that demonstrate best security practices and engaging with professional tech security partners to assist with your policy and management of your providers, you can rest assured you are taking the necessary steps to keep your data and your clients' data secure.

Tony Donofrio is the chief technology officer at Veritext Legal Solutions. In this role, he develops and supports the mission-critical systems the company's clients, reporters and employees use every day. His focus is to ensure that clients and Veritext staff have the very best experience with easy-to-use, highly reliable and highly secure tools.