How Firms Can Stop Playing Whack-A-Mole With Data Security

By **John Smith** (September 26, 2023)

John Smith

As law firms work to protect their stores of confidential client data, many are implementing scattershot right solutions, processes and practices.

Yet, these controls are being implemented in silos: They are not orchestrated together or layered across people, process and technology to create a solid security barrier across organizational systems.

This often speaks to a "whack-a-mole" approach — as one security gap is discovered, a new solution is implemented to knock it down. As a new threat type emerges, the new, specific vulnerability area is fortified.

This results in a patchwork or reactive security approach, rather than an overarching security strategy that yields a defensive layer blanketing the entire enterprise infrastructure in redundant, impenetrable controls.

Without these defensive layers, there are too many moles to whack, and the enterprise is often left with vulnerabilities for a determined threat actor to find and exploit.

The very nature of the proprietary data in law firms makes them a significant target of threat actors — with nearly a third reporting breaches[1] in a single calendar year, according to the American Bar Association's 2022 tech report — so it is essential that firms hold true to their fiduciary duty to protect their data in trust by all practical means necessary.

To wit, data from a 2022 study conducted by my firm and the International Legal Technology Association, titled "Security at Issue: State of Cybersecurity in Law Firms,"[2] showed that there are still gaps in how law firms are protecting their systems and data assets.

The study, which intricately queried 71 information technology professionals from very small law firms with less than 50 attorneys to very large firms with more than 700 lawyers on their security practices, indicated that 87% of firms have adopted some form of automated solution to continuously monitor the devices lawyers or other employees use — like laptop and desktop computers, and mobile phones — for security threats.

While these are solid investments in protecting these users' endpoints, only half reported using traditional antivirus software — such as McAfee Corp., Symantec or others — on these endpoints to recognize and block known malware.

Only a quarter are using preset rules to allow only IT-approved applications to run while blocking all others — called "whitelisting" and "blacklisting" — and only a quarter are using all three techniques.

It's important to leverage these together — or layer technologies with similar intent but differing mechanisms on top of one another — as every control has limitations.

Layering or stacking technologies on top of one another provides an overlapping layer of defense. And, it means that threat actors must have the skills and ability to peel back every layer while remaining undetected, greatly enhancing defensibility.

As another example, 75% of firms have multifactor authentication, or MFA, controls — leaving 25% using no MFA, one of the most critical controls — to protect identity and access to application or data.

Yet, 61% have not deployed MFA in a way that will stop a threat actor from moving from system to system once they have entered the network, also called lateral movement defenses. Proper lateral movement defenses require IT staff to use MFA on all forms of system administration, including consoles, remote access platforms and scripting mechanisms.

Firms should always assume that an attacker can penetrate their publicly accessible systems, such as Office 365, NetDocuments, the virtual private network and others, even with MFA in place.

Lateral movement defenses are a critical second line to ensure a threat actor cannot gain higher levels of access to privileged systems — like databases or backup systems — set up backdoor routes to send firm data out of the business undetected in order to use as extortion, or do any other kind of malicious damage.

This is another example of when overlapping and stacked controls are essential to creating a more complete defensive armor.

We believe it is essential to leverage the power of three: three separate solutions by different manufacturers to layer defenses around things like access. This includes one system for verifying username and password, another for MFA, and yet another for monitoring and blocking risky logon behavior.

Only by stacking controls, preferably by different manufacturers with different gaps or weaknesses, can you eliminate blind spots found in any one solution to work toward comprehensive defenses.

Any legal professional is intimately familiar with the many challenges firms face in staffing, resources and time dedicated to security.

Many firms are working to employ many of the right tactics, techniques and procedures that are components of a strong security program but are still playing whack-a-mole — being reactive in their defenses.

The Best Path Forward

The way to achieve a robust and comprehensive security posture involves adopting a holistic and proactive approach that goes beyond just compliance — which is limited in technical specificity and timeliness — and reactively addressing current issues.

Firms should focus on adopting a risk-based approach to security. It is essential to first identify and prioritize potential risks based on their likelihood and potential impact on the organization.

When addressing gaps, deploying diverse security solutions from multiple manufacturers is another valuable strategy. Relying solely on one tool or one manufacturer for all security needs can create a single point of failure.

Having overlapping solutions ensures that potential weaknesses or vulnerabilities are addressed from various angles, and challenges threat actors' capabilities.

By consistently reviewing and analyzing security intelligence, organizations can detect and respond to threats more rapidly, reducing the effects of potential breaches.

Staying informed about emerging threats via multiple threat intelligence sources is vital. This knowledge helps anticipate potential attacks and enables firms to adjust their security controls accordingly, staying ahead of threat actor activities.

Gain Buy-In to Be Strategic and Stop Whacking Rodents

Security is an ongoing process, and the landscape is constantly changing. That does not mean firms can't have a unifying strategy that adjusts and reacts to evolving threats.

By assessing gaps, using that data to gain leadership buy-in for the needed changes, and adopting a dynamic and layered approach, firms can strengthen their security posture and transcend the inadequacies of traditional compliance-driven measures to arrive at a much more defensible organization — rather than whacking down problems as they arise.

John A. Smith is the CEO at Conversant Group.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] American Bar Association Tech Report 2022, "2022 Cybersecurity," John W. Simek, November 29, 2022.

[2] Conversant Group and the International Legal Technology Association, "Security at Issue: State of Cybersecurity in Law Firms," June 2022.