Stop Playing "Whack-a-Mole" with Security

Firms Are Doing Many of the Right Things–But in a "One-Off," Patchwork Fashion

Takeaway from the ILTA/Conversant Group Cybersecurity Survey of Law Firms

As we analyzed the results of our Conversant Group/ILTA cybersecurity survey, we observed that, overall, law firms are implementing many of the right solutions and practices but in an isolated, unorchestrated fashion. 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" security armor, rather than a continuous, layered defense that blankets the entire enterprise infrastructure in redundant, impenetrable controls leveraging people, process, and technology. Without these defensive layers, there are too many moles to whack.

Data Shows, Controls Are Not Stacked Against Differing Threats

To illustrate the issue, our data showed that 87% of firms have adopted some form of automated endpoint solution, such as Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), or Extended Detection and Response (XDR). These are solid investments in protecting the endpoint. However, only half report using traditional, signature-based AV on their endpoints; only a quarter are using application white/blacklisting; and only a quarter are using all three. In our experience, it's important to leverage these together, as every control has limitations.

Despite the results of the survey, Conversant has found, through our extensive experience assessing law firms, that less than 5% have controls stacked in this manner. 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.

As another example, 75% of firms have Multi-Factor Authentication (MFA) controls (leaving 25% using no MFA, one of the most critical controls!) to protect identity and access to application/data, but 35% have no lateral movement defenses. Firms should always assume that an attacker can penetrate their publicly accessible systems, even with MFA in place. Lateral movement defenses are a critical second line to ensure a threat actor cannot move through the network to escalate privileges, set up backdoors, and otherwise wreak havoc in the environment. This is another example where overlapping and stacking controls is essential to creating a more complete defensive armor.

The Solution: Focus on Orchestrated Security Controls and Configurations

We are intimately familiar with the many challenges law 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 is to avoid focusing on compliance, statutes, and the issue of the day, and instead layer security controls together across people, process, and technology, filling in blind spots with overlapping, diverse solutions, blocking access by default, and looking at defenses as a holistic, impenetrable whole. Firms can gain advantage from getting a controls and configurations-based assessment from a third party, which can help them determine their specific gaps and prioritize how to remediate them to provide a more complete defense, rather than checking boxes on compliance exercises.

About the Conversant Group/International Legal Technology Association (ILTA) Cybersecurity Survey and Report

In 2022, Conversant Group and ILTA collaborated to conduct the first-ever cybersecurity-focused benchmarking survey for the legal industry. The survey was targeted specifically at understanding cybersecurity controls, tools, practices, and assumptions in law firms. The results were presented in the report, "Security at Issue: State of Cybersecurity in Law Firms," available for download now. This snapshot presents one key takeaway from the report.