International Legal Technology Association

CONVERSANT GROUP

ILTA / Conversant Group – Executive Summary

# Security at Issue:
## State of Cybersecurity in Law Firms

Law firms store some of the most sensitive information available regarding material business transactions (e.g., mergers, acquisitions, and tax returns), civil/criminal prosecution, and personal transactions (e.g., divorces and wills), and lawyers have an ethical responsibility to protect this data. Due to fears of losing this sensitive information and pressing court dates that often cannot be moved without system access, law firms are highly motivated to succumb to an attacker's demands when their files are encrypted by ransomware, or they are threatened with the public exposure of that data. Toward the end of 2021, nearly a third of law firms surveyed reported a breach within the year; and 36% reported past malware infections, according to an American Bar Association report.

While law firms are in the crosshairs of threat actors, our data shows only ~15% of law firms felt they had security gaps, while over double that number have endured some form of breach. For this reason, Conversant Group and the International Legal Technology Association (ILTA) were highly motivated to better understand how law firms were fortifying their defenses. This 2022 survey jointly conducted by International Legal Technology Association (ILTA) and Conversant Group was the first cybersecurity-focused survey ILTA has co-issued (and possibly first for the industry) designed to hone in on the cybersecurity practices, processes, and procedures implemented by law firms. We wanted to know how firms were layering their solutions with their people and process to achieve an orchestrated approach to defending the wide swath of sensitive data they have. And, importantly, what could they do differently to improve their security practices.

What we learned was illuminating. In this summary, we analyze these results, born of our 14 years' experience intricately assessing organizations' security controls and configurations and helping them restore their systems to health after disaster has struck.

## Key Takeaways

The data reveals that legal IT and cybersecurity professionals suffer from a definitional and paradigm problem. Clearly, IT leaders understand terms, definitions, and concepts differently, and no survey instrument can capture those nuances. As examples:

- Only 15.5% of responding firms of all sizes believed they had some security gaps, or that their security needed significant improvement; the rest believed they were relatively to extremely secure. This, unfortunately, does not track with either our experience from our assessments (which always yield some significant risk factors), the previously mentioned study that showed a third of firms suffered breaches in a single calendar year, or security gaps uncovered throughout the survey. We believe this is a definitional problem by what is meant by "secure" and what achieving true defensibility looks like.
- Nearly three-quarters of respondents believed they were more or much more secure than their industry peers. This obviously defies mathematical logic; while we can possibly hedge our results with the likelihood that those taking the survey were more confident in their security (and thus more willing to participate), we find this still unlikely. We think it more likely that we are seeing a definitional glitch in what "average" looks like.

- Sixty-five percent of reporting firms state they have lateral movement defenses in place. Conversant is aware of only two products on the market that provide these comprehensive defenses. Thus, we believe there is a definitional disparity by what is meant by "lateral movement defenses," and that few organizations truly have them. These defenses require, at the very least, the deployment of MFA on UNC administrative shares, PowerShell, command prompt, Windows Management Instrumentation, Microsoft Management Console, Remote Registry, Remote Desktop, Windows Remote Management, and all forms of administrative control of a server, switch, and firewall (among other controls).

Perhaps the reason firms believe they are secure comes down to our next thought: there is an overall paradigm problem among technical professionals. It largely falls into three buckets:

- **Security Does Not Equal Compliance**: We find IT organizations and CISOs are often far more focused on complying with established frameworks, regulations, statutes, and client/insurance requirements than on implementing actual defenses against threat actors. As we have seen from years of breaches of "compliant" enterprises, "compliant" does not equate to security; threat actors do not care if a firm aligns with NIST, FedRAMP, SOC2, or CIS. These frameworks are only a point-in-time, periodic snapshot of line items to be documented. Most often, they lack prescriptive instructions and rarely are translated into actual detailed-level changes to the security controls that keep organizations secure. Organizational controls and configurations are continually changing, as are threat actor tactics, and security defenses must change dynamically along with them and be layered to leverage people, process, and technology toward a Zero Trust method.
- **Users Are Not the Problem**: The data shows IT professionals fear their users' behaviors more than they fear the threat actors themselves, and believe these behaviors are the greatest challenge to their security. They also believe users are the biggest impediment to improvement through their resistance to change and education. We will explore this topic in more detail below, but in short: It's time to stop fearing our users and work to remove user risk from the equation by blocking access by default. We need to shift the solution paradigm away from users and toward IT empowerment.
- **Focus on the True Enemy—As They Are Certainly Focused on You:** Since we have posited that our user isn't the enemy or the direct danger, we need to understand that the cybercriminal is the enemy, though they are not always as sophisticated as we make them out to be. We will not deny that there are sophisticated nation state actors or threat actors more generally; but, in our experience, initial penetration of an environment (often through email phishing/harvesting of credentials and moving laterally within the organization) is not that sophisticated and could have easily been avoided with proper defense.

Here are of the top detailed conclusions we have drawn from the data:

## User Behaviors Are the Source of Our Security Woes and a Roadblock to Change–or Are They?

When asked what the top three threats to security are in the firm, the top response at 39.4% (and 40% in the ILTA Technology Survey) was user behavior and lack of training to prevent this harmful behavior. User behavior/training arose as a greater concern than ransomware or any threat actor tactic that would exploit these key drivers of organizational productivity.

There is one unassailable truth: Users are human, and they will always be fallible no matter how much training you throw at them. Thus, blaming them or exercising an extreme focus on securing their behaviors will not lead to defensive actions that secure the organization. Firm IT, with support from leadership, must take a stronger stance to defending systems—assuming users will make mistakes—while also training these users to reduce risk on multiple fronts.

So, what defensive actions can firms take? The data sheds more insight here as well. Users are only a risk when they click the wrong link, open the wrong attachment, access the wrong website, or conduct other risky behaviors. Firms can dramatically reduce these risks by using controls that eliminate these options from users entirely.

From our survey data:

- 90% do not block or restrict external file hosting sites.
- 72% do not automatically enforce encryption of email through content examination.
- 43% do not enforce encryption of removable media.
- 79% require fewer than 16-character passwords.
- 20% do not have deep packet inspection configured on their firewall.
- 38% do not block malicious sites at the firewall.
- 33% have not enabled anti-spoofing/ impersonation protection in the spam filter.
- 24% do not run AV scans on inbound email.
- 80% do not provide a password vault to users.
- 20% have no form of MFA on user accounts.

Simply put, threat actors exploit users because organizational controls allow them to. The recommended remedy is to stop allowing and start blocking. Otherwise, firms are making security optional, at the whim of human foibles with potentially disastrous consequences.

Which brings us to our next area of concern in our survey: **Users are viewed as the greatest impediment to change.** In our survey, 59% said user inconvenience was the greatest roadblock to implementing more stringent security controls (with cost being the second greatest concern).

Firms should move toward a policy of Zero Trust: trust no one and nothing by default. As examples, choose one IT-vetted password vault and block all others; choose one browser and block all others; choose one file sharing platform, and by default, block all others (and so on). All necessary exceptions should be tracked on a Risk Register. Once a threat actor takes control of a user's endpoint, the user endpoint and threat actor become synonymous in how freely they can move throughout and access your systems.

We argue that it's time for the firm to take control, led from the top down. We recognize these controls require an investment and that leadership is often resistant to sweeping changes; similarly, IT teams must bear the burden of convincing these leaders that the costs and user inconveniences are needed to secure their firms against user risk. Organizing firm defenses against these threats rather than around user convenience is an essential step to mitigating this considerable area of vulnerability.

## Legal Security Is Evolving—But Clients and Insurance Carriers Are in the Driver's Seat

Ideally, CISOs, CIOs, IT leaders, COOs, Executive Committees, Executive Directors, and CEOs would lead the charge for security improvements. However, in law firms, our data instead indicates that client and insurance carrier requirements are the top drivers for security change (at 27% and 22% of stacked rankings, with IT leadership coming in at 15%).

First, it's important to understand how clients have influence over firm security: firms sign documents with their clients called Outside Counsel Guidelines ("OCGs"). These requirements often include specific instructions on how firms should conduct their business, ranging from ethics and conduct to staffing and billing. OCGs typically also include specific security practices. Over 50% of IT leaders are aware of and report they are following OCGs most of the time. An additional 18% have a dedicated person or entity, such as General Counsel, tracking compliance with OCGs independently. However, nearly one third (27%) of IT teams are unaware of these guidelines but assume they are being followed most of the time.

While we consider it worrisome that nearly a third of firm IT teams are unaware of security requirements in their OCGs, we find it more concerning so many IT professionals believe these guidelines (to which a portion has little to no visibility) and insurance requirements are a primary driver of security. Clients, insurance companies, and regulatory bodies do not have esoteric knowledge of each law firm's infrastructure; and they aren't aware of the threat tactics as they change daily and how those threats pertain to the firm's controls. IT needs to take the helm and see themselves as the primary driver of security evolution if change is to be appropriate, effective, and efficient for their individual firm.

## Backups Are Not Viewed as a Top Security Control—at Firms' Peril

Firms are wholly dependent on the information they store and maintain regarding their clients and matters. Should a threat actor access and destroy that data permanently, it would have dire consequences for not only ongoing business, but also reputational trust, a crucial component of law firms' client relationships. Yet only 11% of our responding firms reported backups as a critical security control, and as we will explore, many of the methodologies used to establish immutable, resilient, and redundant backups are lacking across firms of all sizes.

"Immutability" means that data in storage is incapable of being changed, encrypted, or deleted. The only way it should be modifiable is by a two-key simultaneous lock turn (similar to a nuclear bomb launch like we see in movies) and the expiration of a designated retention period (such as a timed lock on a safe). This is essential for law firms, which are often victimized by ransomware actors who target backups in 98% of attacks (68% of times successfully). Immutable backups are a requirement of many cyber insurance carriers and are the single most important security control of the enterprise—and they themselves require controls around and within them.

Yet, all immutability is not equal. Should a threat actor break controls around one data repository, it is essential that there be several others (we recommend four), all immutable and preferably of different types and differing manufacturers to hedge bets, adding additional layers of insurance against total loss.

From our study, we see that 38% of respondents reveal that their backup copies are either not immutable or they are unsure whether they are, and only 24% report having multiple immutable copies of all data. While these are concerning statistics, we must dig even deeper to understand whether those reporting one or more copies are immutable are correct. Storage snapshots emerge as the most common form of backup (at nearly double most other backup methods). While this may not be the only method of backup for some firms, it is the most often used, and it cannot be relied upon to be immutable. Only Pure snapshots offer immutability to our standards, and we can see from the ILTA Technology Survey that only 9% of law firms surveyed are using Pure for their shared storage (and all of those are likely not taking immutable snaps of all data). Coupling this with the fact that a significant population is using non-immutable local and remote storage, it is likely that few have the recommended redundancy in immutability to safeguard the firm in the event of determined, targeted backup attacks. Finally, we must shed light on an additional Achilles' Heel in our firms' backup resilience strategies: far too many of our firms have components of backup infrastructure as part of the Active Directory domain. No backup servers, proxies, or targets should be domain-joined, as any attacker that can penetrate the network can then access company data in storage.

## Firms Are Doing Many of the Right Things–But in a Patchwork Fashion

Across the survey, we see firms implementing many of the right solutions and practices, but in many cases, in an isolated fashion. For example, 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 are 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, every control has limitations.

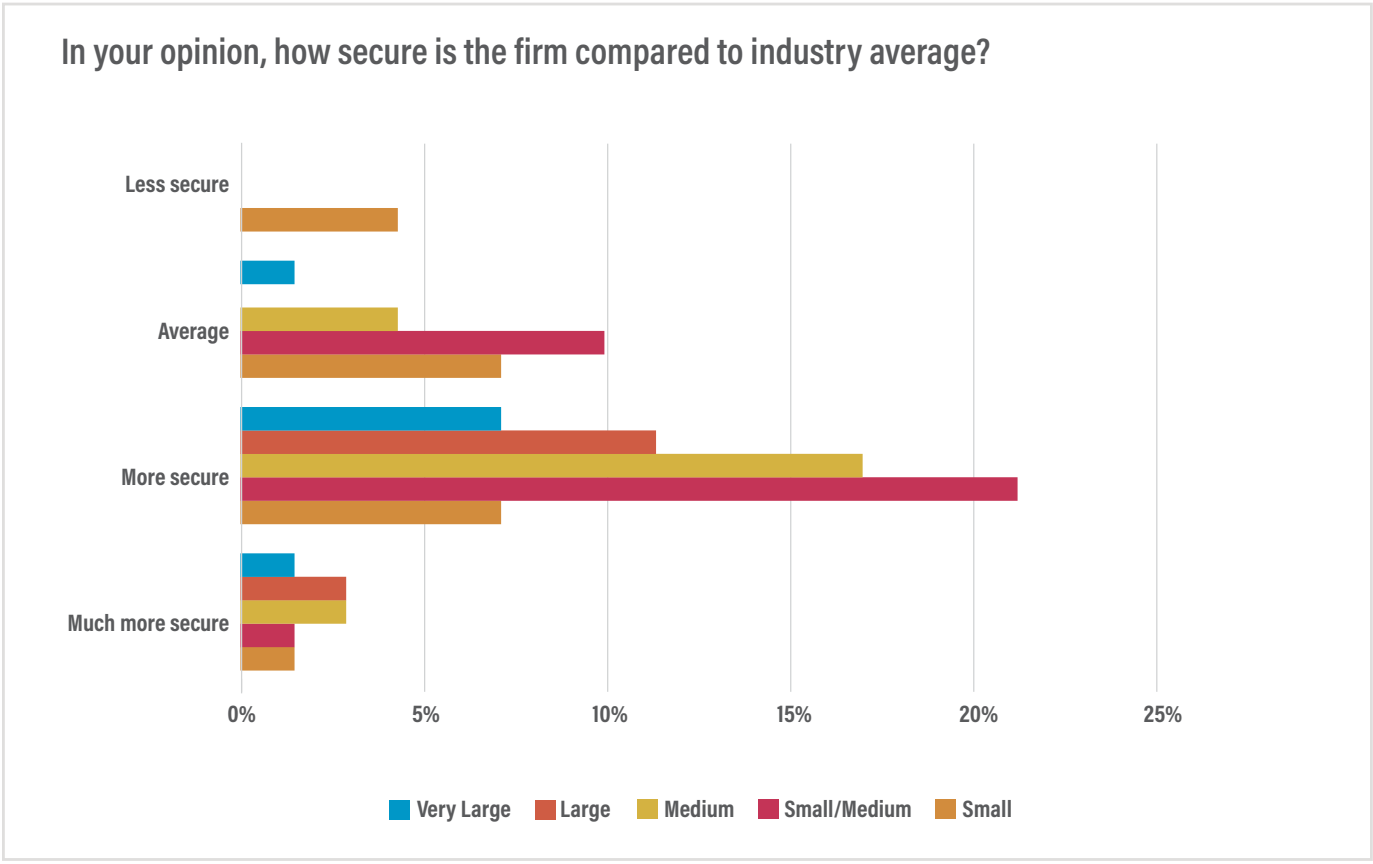
Only by stacking controls, preferably by different manufacturers with different gaps or weaknesses, can you eliminate blind spots found in any one solution to work toward comprehensive defense. Further, upon assessment Conversant finds less than 5% with controls stacked in this manner. Stacking controls in this manner, as recommended by Conversant, is often contrary to traditional IT paradigms and many vendors' recommendations, but in our experience with breaches, it is essential for complete 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. Lateral movement defenses are a critical second line to ensure a threat actor cannot move through a firm's networks 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.

In summary: What is still missing is an understanding of how to layer security controls together across people, process, and technology, filling in blind spots with overlapping, diverse solutions, blocking access, 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.

## Is Bigger Better? How Small and Large Firms Compare*

While larger firms spend less of their IT budget on security (firms >500 users spend an average 11.4% of IT budget on security, vs. an average of 18.5% for firms <500 users), it's difficult to infer how this translates to overall security quality. Let's first assess survey respondents' views on their security defenses and then assess how the data supports those views. As discussed previously, 73% of firms believe they are more or much more secure than their industry peers:



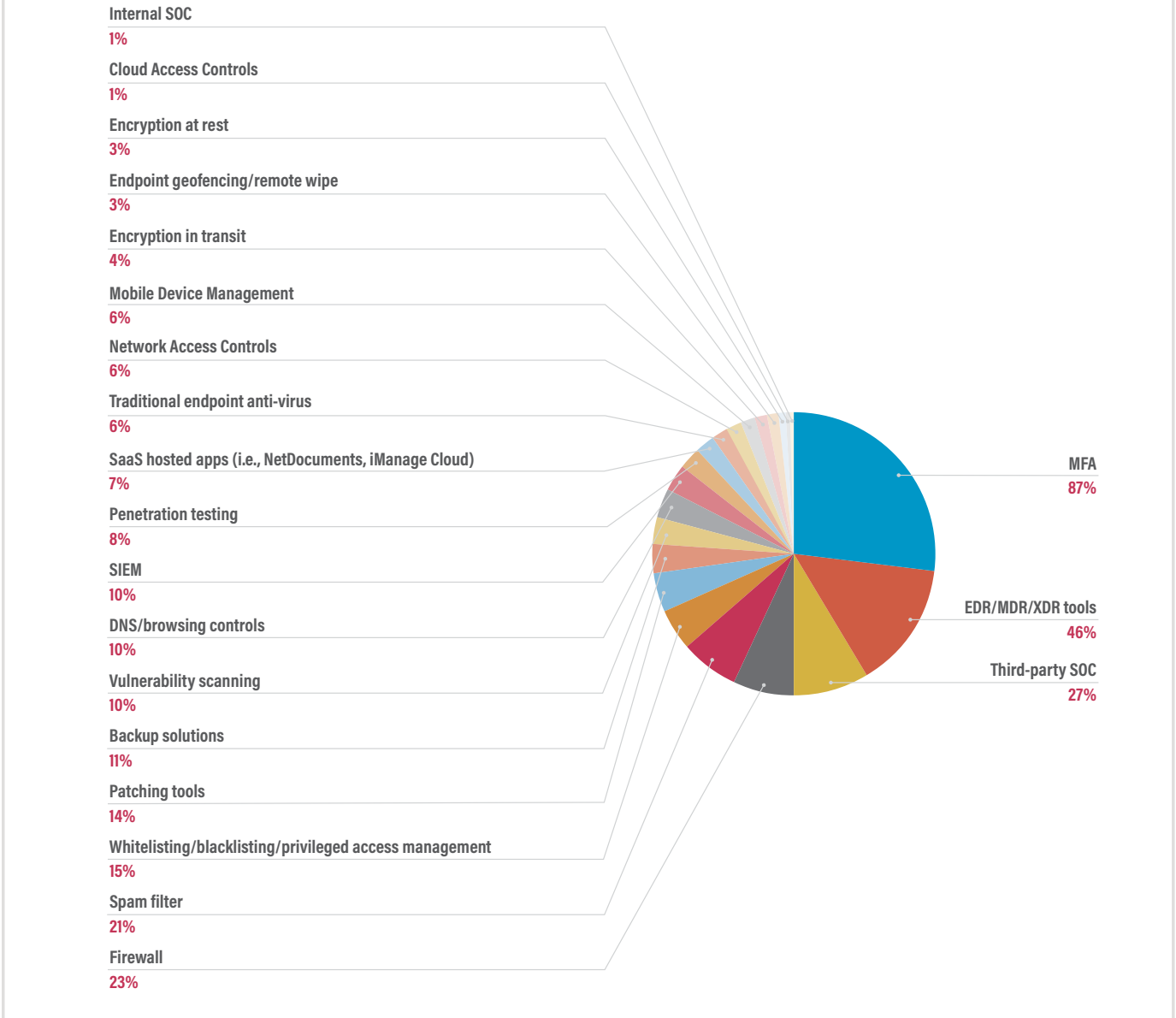
Perhaps larger firms believe they are more secure because, as the data reflects, on average they have several markers of a more formalized security program, including:

- They are more likely to have staff fully dedicated to security, either in-house or outsourced. All large and very large firms had dedicated security leadership, but 86% of small firms did not.
- They conduct processes that indicate more mature security programs:
- They report being more likely to maintain risk registers, which are essential to tracking, managing, and mitigating all risks in the organization. While no small firm and only 52% of small to mid-sized firms had a risk register of any kind, most medium to very large firms had at least informal documentation of risks, and many maintain a formal register with a process to rate, manage, and dispose of those risks.
- Larger firms are more likely to have a formalized change management process, with a change review board involved in approvals for major changes (though we suspect that security is often not a significant consideration in approving those changes). All medium to very large firms have at least an ad-hoc approval or documentation process, and most large to very large firms have formal change review boards. Forty-three percent of small firms have no process at all.
- Larger firms regularly probe for weaknesses so they can understand where to focus their efforts and spend:
  - Vulnerability scanning: Most medium to very large firms scan for vulnerabilities monthly or more frequently, but 14% of small firms don't scan at all.
  - Penetration testing: While nearly 14% of small firms never conduct penetration tests, most others conduct them periodically. But the majority of large to very large firms conduct them annually or more often (100% and 86%, respectively).

Thus, the data reflects that apparent security maturity increases with firm size. We see consistently across the data set that larger firms have more formalized programs and are employing more rigorous practices than their smaller peers.

However, with that said, in our experience, "more mature" does not equate to "secure," as "compliant" does not equal "secure." From Conversant Group's experience assessing firms, over 90% of firms we assess do not comply with their own stated policies and procedures, once examined down to the technical controls and configurations level. Let's review how firms view their top controls:

## Top Security Controls



- MFA is viewed as the top control; however, 44% of firms still permit access to remote solutions from personally owned devices, and 83% of firms permit access to SaaS applications on non-firm networks and untrusted devices. Thus, law firms have done little to mitigate the risk of a session token capture (an effective means of bypassing MFA). As an example, LastPass' most recent breach was caused by personal device usage.
- DNS/browsing controls were only viewed as a top security control by 3.1% of respondents; however, many breaches are caused by credential leakage from user browsers, such as Chrome, Edge, and Firefox.
- EDR is viewed as the second top control; however, only 24% have EDR + whitelisting/blacklisting + traditional AV, which is necessary to achieve a more comprehensive defense.
- The SOC is the third most-popular control, but only 57% have a SOC + SIEM, again, essential for a layered (and total) defense. In our experience, many cyberliability carriers now require this control.
- Firewalls are the fourth most-popular control; however, 54% admittedly do not have deep packet inspection enabled, rendering the firewall largely useless, as it is missing a large portion of potentially malicious traffic. According to one study, 63% of all threats were discovered in encrypted traffic; some studies have stated as high as 90%.

## Summary and Conclusions

These are just a few examples of what we see, though we recognize security is a difficult, ongoing challenge that requires difficult choices. Further, no organization ever reaches that nirvana, "fully secure." But we believe firms still need to look at their security from the thousand-foot view: understanding how all elements work together, blocking by default, enabling solution features (not assuming they are turned on by default), and probing for weaknesses so they can target their security actions. Firms would be best served to continually remember the determination of their enemy—the threat actor—and how continuously, relentlessly they probe for any defensive weakness. It's essential to not just build a fence; but to build a system of walls without gaps and monitor them regularly. Some are doing many of the right things; a few are doing most of the right things; none are doing all the right things. Understanding where your gaps lie and prioritizing your actions against those gaps remains the best path to a layered defensive strategy.

# About the International Legal Technology Association (ILTA)

ILTA is a volunteer-led, staff-managed association with a focus on premiership. The organization aims to educate legal professionals and connect them with their peers to support their work in the legal sector. While ILTA has a strong focus on technology, their offerings support all types of professionals within law firms and corporate/government legal operations.

Learn more at iltanet.org.

# About Conversant Group

Conversant Group is changing the IT services paradigm with our relentless focus on "Secure First" managed services, IT infrastructure and consulting. Conversant has been a thought leader for over 14 years helping over 500 customers and entire industries get answers to the security questions they may not even know to ask. We are the world's first civilian cybersecurity force, with three time-tested battalions:

Learn more at ConversantGroup.com.


**Ransomware rapid response, remediation and recovery**


**IT security assessments, strategy and planning**


**Ongoing, security-based management**