International Legal Technology Association

FENIX24

JULY 2025

Security at Issue:

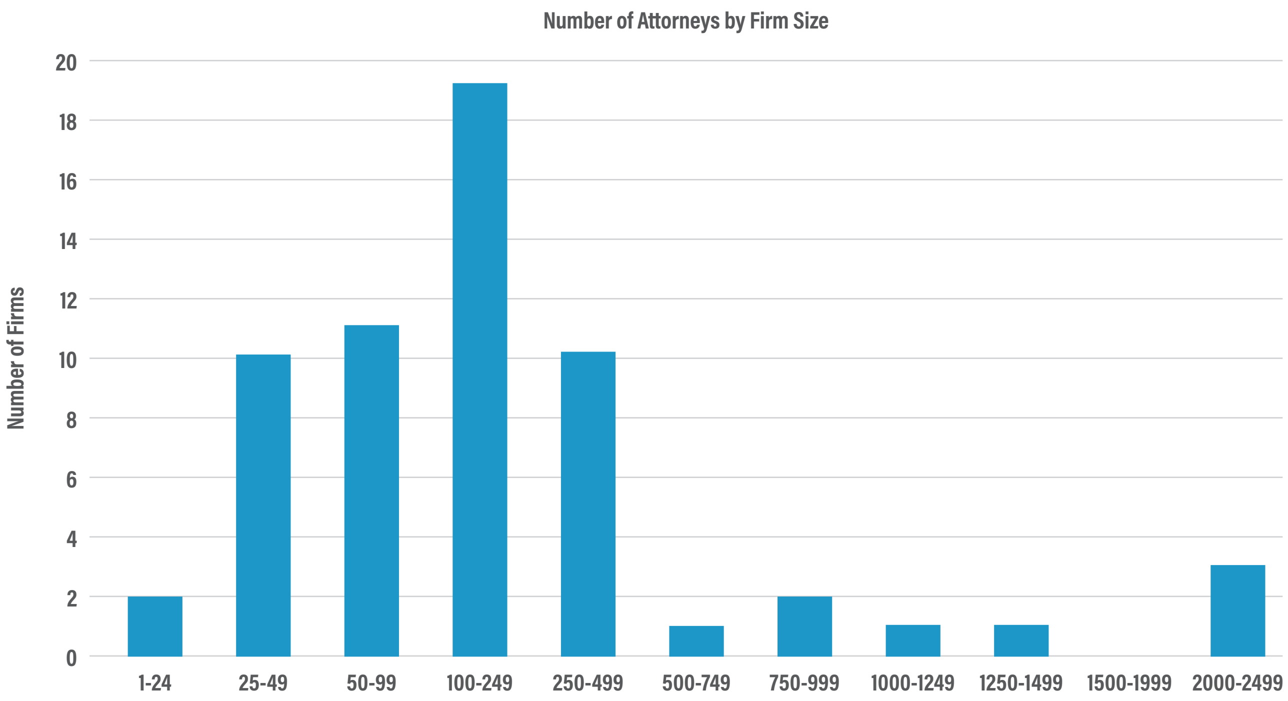
State of Cybersecurity in Law Firms

Results of the ILTA • Fenix24/Conversant Group Cybersecurity Survey

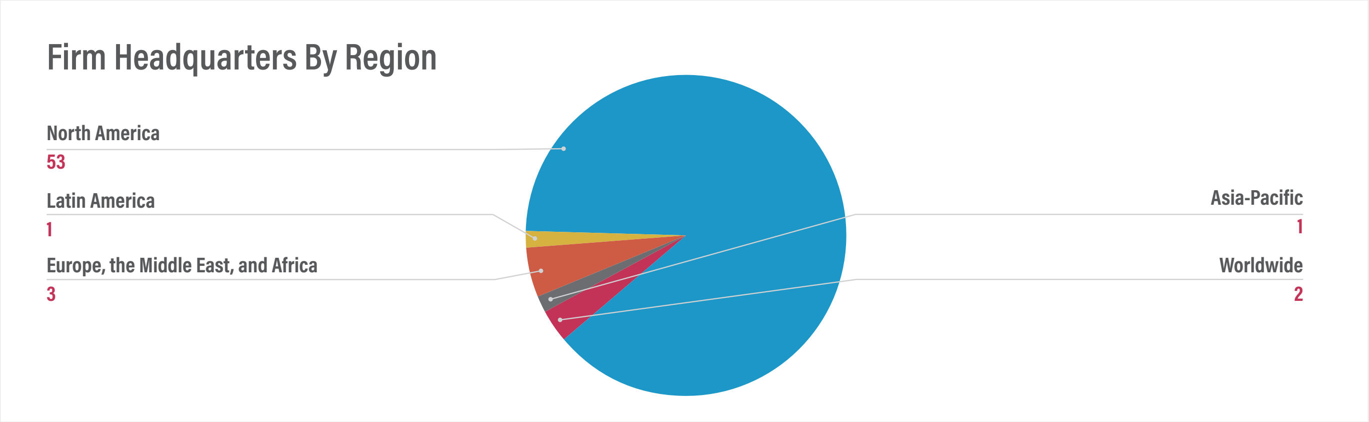
Executive Summary

This report is based on data gathered by the 2024 ILTA Breach Readiness Survey. Sixty law firms responded to 72 questions ranging from firm demographics to detailed technical configurations. The survey results are self-reported and not validated by a third party, although the questions were designed to be as granular as possible to produce accurate results.

Responding Firm Demographics



Executive Summary (cont.)



There are references throughout this report to results from the 2023 ILTA security survey. However, the survey questions changed substantially in 2024 to better reflect the changing landscape of IT security. This report makes comparisons where direct correlations can be drawn, but those interested in the 2023 results should consult the previous report.

Contents

Why Are Law Firms a Prime Target for Cybercrime?

Law firms are under attack.

Threat actors (TAs) recognize the high value of the sensitive data firms manage — business transactions, privileged client communications, and confidential case details — making the legal sector an attractive target for cyberattacks. Legal professionals also operate under strict deadlines and ethical obligations, increasing the likelihood that firms will pay ransoms or comply with extortion demands to regain access to critical files. Over the past year, these risks have only intensified.

TAs are shifting from broad, opportunistic attacks to more calculated, human-operated campaigns designed to exploit law firms' specific vulnerabilities. At the same time, new regulatory and insurance requirements are forcing firms to reassess their security posture, often revealing critical gaps in areas such as access controls, incident response, and data protection.

As cyber threats evolve, the legal sector faces a choice: adapt and invest in meaningful security improvements or risk exposure to increasingly aggressive and financially motivated attackers.

Key Takeaways: What Firms Must Know

For firms handling sensitive client data, the question is no longer if you'll be targeted, but when. Ransomware, phishing, social engineering, and data exfiltration aren't hypothetical threats — they are active risks that exploit weak points in technology, processes, and people.

The 2024 ILTA • Fenix24/Conversant Group Cybersecurity Survey reveals critical gaps in how the legal sector approaches security. Despite rising awareness and investment, fundamental vulnerabilities remain: inconsistent adoption of key safeguards like immutable backups and MFA, an overreliance on external drivers for change, and a disconnect between perceived and actual security readiness.

This year's findings provide an in-depth look at the challenges, gaps, and opportunities facing legal technology leaders today. The following key takeaways offer a preview of some of the report's most critical insights, helping firms focus their efforts on meaningful improvements that strengthen resilience and protect their most valuable assets.

Firms Face an Evolving Threat Landscape

Phishing, ransomware, data exfiltration, and social engineering are now the top security concerns, reflecting the growing sophistication of cyberattacks. Phishing, which was introduced as a new category this year, took the top spot, cited by 50% of respondents. Data exfiltration concerns have also risen significantly, from 5% in 2023 to 35% in 2024. Threat actors increasingly use targeted attacks to bypass defenses, extract sensitive client data, and leverage that data for extortion. These developments demonstrate a clear shift from traditional malware-based attacks to more complex, human-driven breaches, requiring law firms to reevaluate their threat detection and response strategies.

Backup Vulnerabilities Persist Despite Increased Awareness

Immutable backups, the single most reliable recovery measure in a ransomware event, remain underutilized. Only 50% of firms reported having at least one immutable backup system, and many fail to back up critical infrastructure like domain controllers or data stored in SaaS applications. This leaves half of responding firms exposed to catastrophic data loss. Even among firms that utilize immutable backups, the lack of clarity around configuration and scope raises questions about their actual recoverability in the event of an attack.

Inconsistent MFA Practices Leave Critical Systems Vulnerable

Multi-factor authentication (MFA) adoption remains inconsistent across high-value systems. Only 50% of firms apply MFA to backup solutions, 37% to backup storage, and just 18% to production storage systems — key targets for ransomware attacks. These gaps highlight an urgent need for firms to expand MFA coverage as part of a broader effort to secure critical infrastructure.

Security Confidence Continues to Decline

Confidence in security has dropped across firms of all sizes, with very large firms (750+ attorneys) experiencing a significant decline. Only 38% of these firms rate themselves as "very secure," down from 50% last year, and 23% of all firms acknowledge known gaps in their security. This decline likely stems from heightened awareness of threats, increased scrutiny through assessments, and the growing complexity of securing modern IT environments.

Persistent Access and Lateral Movement Remain Critical Weaknesses

Many firms fail to block the tools and techniques that allow TAs to maintain persistent access and move freely across their networks. Unapproved remote

Key Takeaways: What Firms Must Know (cont.)

access tools, unsecured VPNS, and proxy avoidance methods continue to be major blind spots, giving attackers prolonged control over compromised systems. Weak segmentation further compounds the issue, allowing lateral movement with little resistance. Even where MFA is in place, inconsistent implementation across administrative functions leaves openings for attackers to escalate privileges and spread ransomware.

External Pressures Drive Most Security Improvements

Firms continue to rely on external pressures to prioritize security initiatives, with client requirements and penetration testing tied as the top drivers of change. Insurance requirements are also a major factor, as cited by 31% of respondents. However, internal leadership often fails to prioritize cybersecurity, with many firms citing resistance from leadership and limited funding as barriers to improvement. This reactive approach to security poses risks as threat landscapes evolve faster than externally mandated changes can address.

Security Budgets Are Failing to Close the Gaps

Although 82% of firms report that their security budgets are “adequate,” 23% acknowledge existing security gaps, revealing a misalignment between spending and real-world risk. Rising costs for skilled professionals, advanced detection tools, and security services put increasing pressure on budgets, often forcing firms to prioritize compliance over proactive defenses. Many firms are investing in security, but without a clear alignment between budget allocation and threat mitigation critical gaps remain unaddressed.

The trends and vulnerabilities outlined in these takeaways reflect a growing urgency for law firms to rethink their approach to cybersecurity. To keep client data secure and operations running smoothly, firms need practical, effective strategies that close gaps and reduce exposure to attacks.

Findings Summary

As we have analyzed the results of this survey over the years, we have seen clear trends emerge and stay consistent. Larger law firms generally considered themselves more secure, and survey results sustained that belief. User behavior was viewed as the single largest security threat consistently across both the ILTA Tech Survey and the Cybersecurity Survey. The majority of firms viewed themselves as more secure than average (and they still do, but more on that later). But 2024 was a year of bucking trends.

User behavior took a tumble from the top threat to security all the way down to #5, with phishing, data exfiltration, ransomware, and social engineering — in that order — all now viewed as bigger risks. Interestingly, the percentage of firms rating user behavior as a top-three security risk is virtually identical to last year (27% in 2024 vs. 28% in 2023), which means that data exfiltration, ransomware, and social engineering all saw massive jumps in 2024. Concerns over data exfiltration increased from 5% to 35%, ransomware from 17% to 33%, and social engineering from 11% to 27%. Phishing is a net-new answer option in 2024, and it immediately took the top slot. We could argue that phishing is a subset of either user behavior or social engineering, but user behavior staying steady and social engineering concerns dramatically increasing imply that phishing in the #1 slot at 50% is not pulling any attention away from those two issues.

- 35% of firms rate data exfiltration as a top-three concern (↑ 30% from 2024)
- 33% of firms rate ransomware as a top-three concern (↑ 16% from 2024)
- 27% of firms rate social engineering as a top-three concern (↑ 16% from 2024)
- 27% of firms rate user behavior as a top-three concern (↓ 1% from 2024)

Taken as a whole, the top five security concerns all circle around breaches by a human TA. Firms no longer fear malware or drive-by encryption. They are increasingly worried about targeted attacks where a human agent maneuvers past weak points in the defenses, exfiltrates sensitive data for additional leverage and reputational damage, and then attempts to shut down operations and extract a ransom payment. This behavior is on the rise globally and makes headlines almost daily. It is a very real risk to law firms.

As an industry, law firms have been described as the easiest path to the most sensitive data. Law firms are data aggregators, and the data they collect and store is exactly the sort of data that threat actors want to access and exfiltrate. The law firm is not the only target in a ransomware event. If TAs can capture sensitive client data they have been known to extort those clients directly with the threat of making that data public. Firms are right to shift their concern towards these emerging threats.

Findings Summary (cont.)

Backup solutions are still not listed among the top-three security tools, but they are at #4 on the list, with 27% of respondents naming them as critical. This is a considerable increase from 11% in our 2023 survey. However, only 50% of responding firms have at least one backup system capable of immutability, defined here and through this report as: a security principle that states that data in storage cannot be changed, encrypted, or deleted by any means because there are no IT administrative technical overrides to the retention lock. Immutable backups are the single strongest indicator of post-ransomware recovery and therefore the best defense against the threats in the current zeitgeist. There is no way to conclusively determine if the 50% of firms' backups tools capable of immutability are actually properly configured for immutability, or what data they are backing up — a full set of all data in the firm, or merely a subset. Even if all these firms have flawless immutability practices and back up all firm data with these tools, that still leaves 50% of firms woefully underdefended against a ransomware event.

- 50% of firms are capable of immutable backups in some capacity
- 27% of firms rate backup systems as a top-three security control (↑ 18% from 2024)

Another major trend shift is the sudden rise of assessments/tabletop exercises/penetration test results as a top driver of change, jumping from 10% in 2023 to 53% in 2024 to a tie with Client Requirements (OCGs/audits/assessments) for the top position. Firms may be increasing the frequency of these tests and assessments, or they may have found new ways to leverage the results of these exercises to spark change in the environment. All of these top drivers leave artifacts of risk in their wake, and firms may be increasingly uncomfortable having known risks on the books.

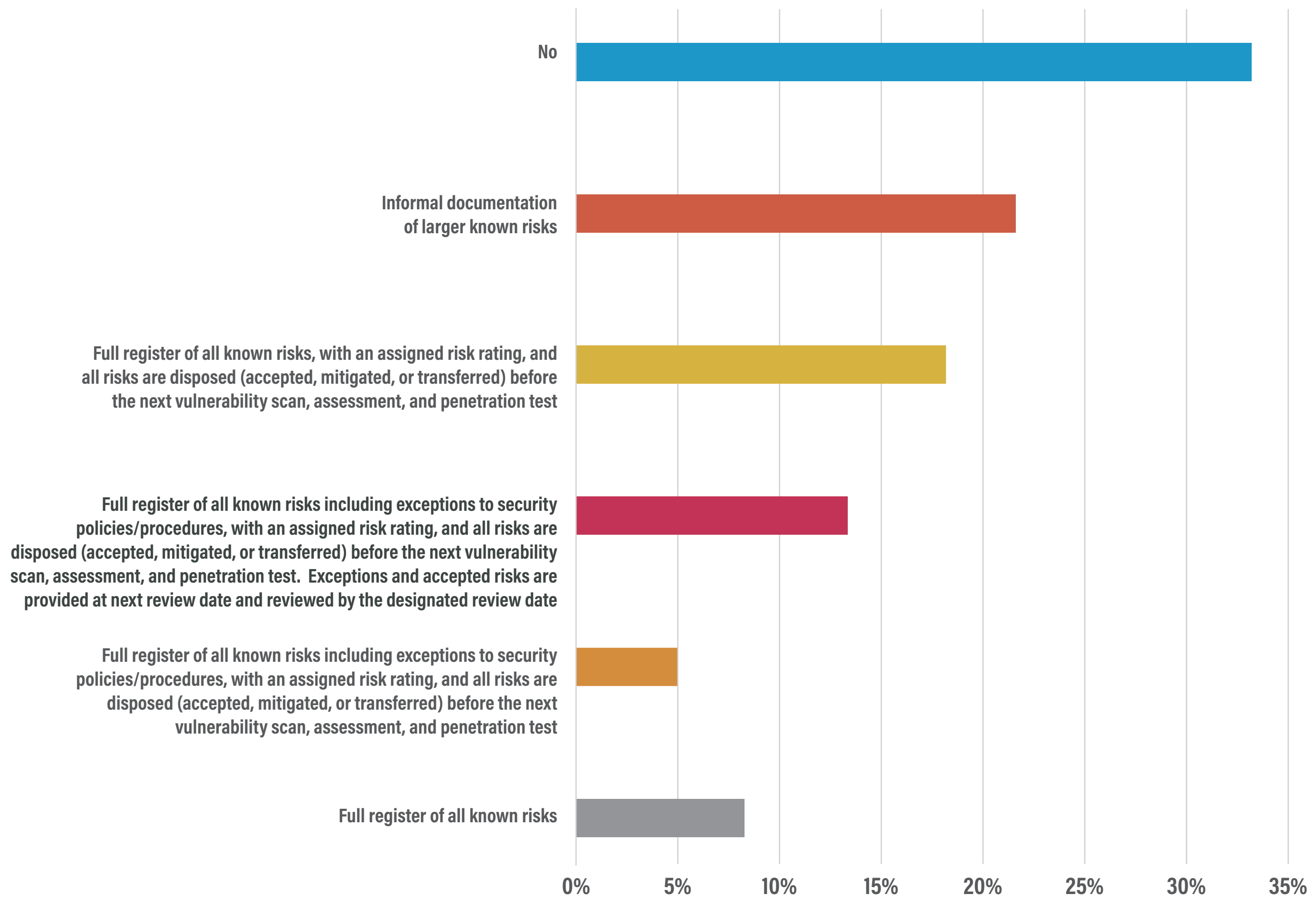
- 53% of firms rate assessments/tabletop exercises/penetration test results as a top-three driver of change (↑ 43% from 2024)

In 2024, for the first time we saw a decrease in the security confidence of larger firms. Only 38% of firms with more than 750 attorneys rated themselves as very secure (down from about 50% last year), and only 15% rated themselves as extremely secure (down from about 20% last year). In an equally surprising shift, the number of firms acknowledging security gaps increased across all firm sizes, from 14% last year to 23% this year.

- 38% of firms with 750+ attorneys rate themselves as very secure (↓ 12% from 2024)
- 15% of firms with 750+ attorneys rate themselves as extremely secure (↓ 5% from 2024)
- 23% of all firms rate themselves as having security gaps (↑ 11% from 2024)

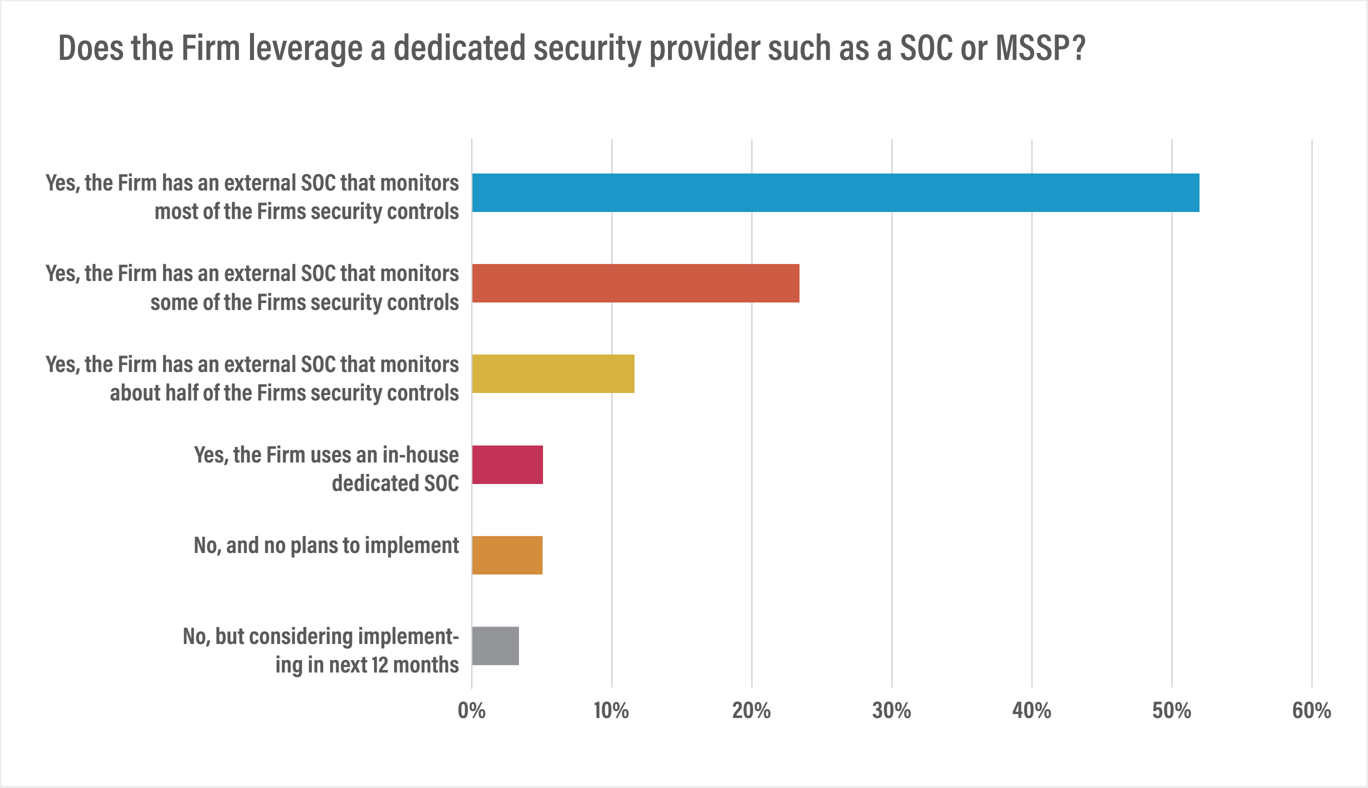
Results By The Numbers

Does the Firm maintain an up-to-date risk register?

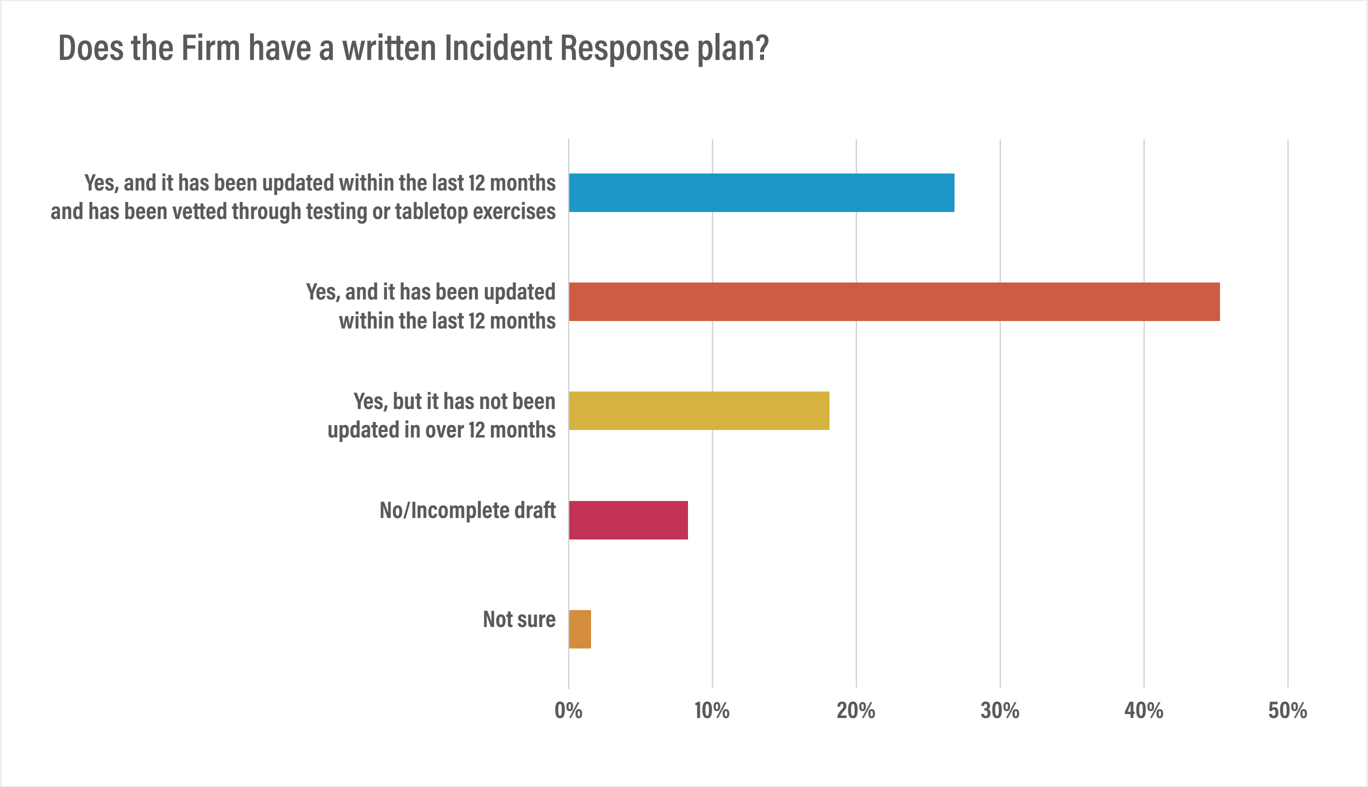


Our interest in how firms rate themselves drove new lines of questioning this year, revealing why firms believe they are (or are not) secure. We found that 45% of firms employ a full risk register, up from 30% last year. Increasing awareness of risks could certainly shake a firm's confidence. Even if these risks are being addressed and mitigated in a timely fashion (and 36% of firms state that they are), having an appreciation for the quantity and pace of newly discovered risks may be enough to make a firm question its security posture.

Results By The Numbers (cont.)

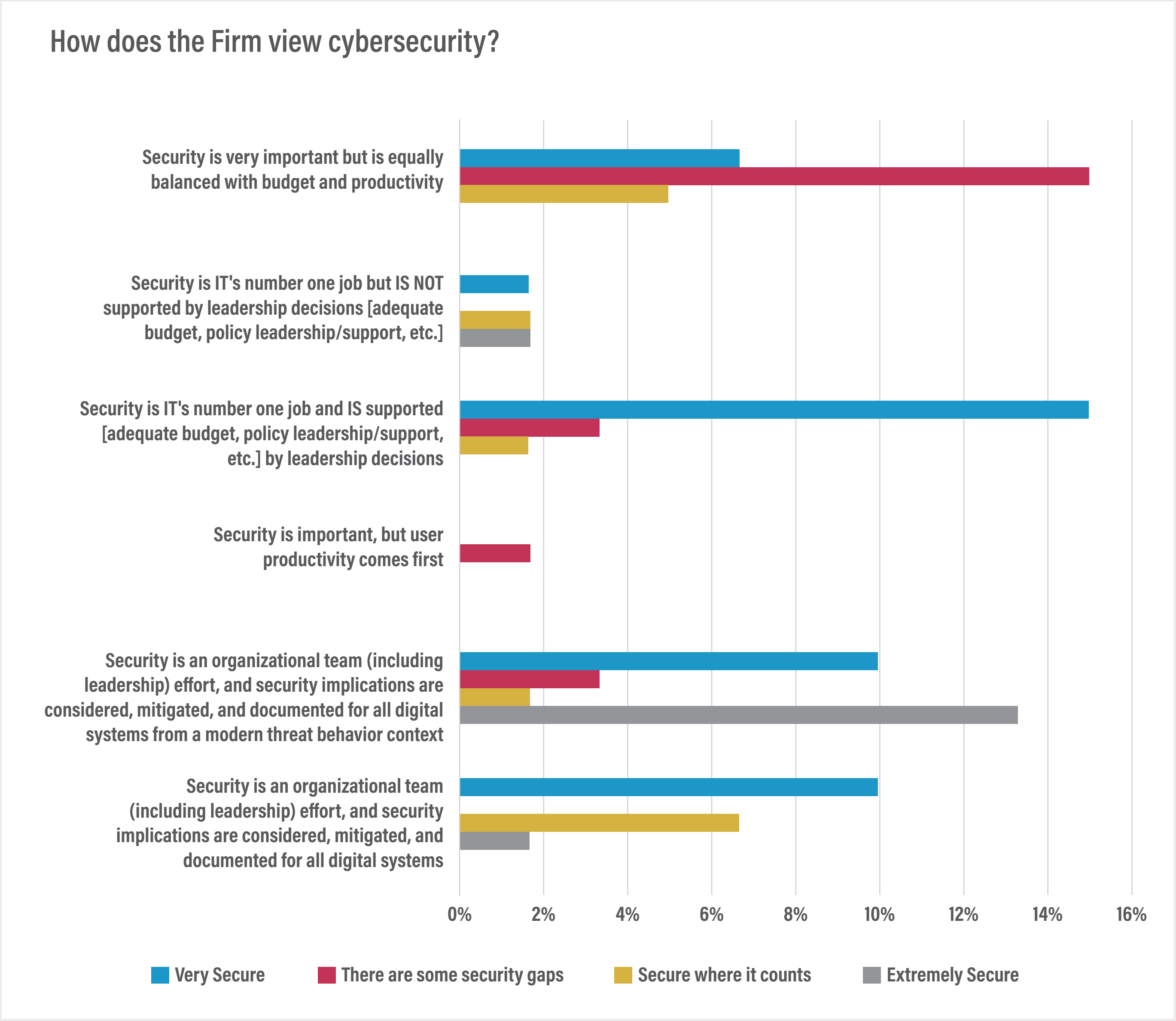


The percentage of firms reporting use of an external Security Operations Center (SOC) increased from last year as well, with 52% of firms reporting that an external SOC monitors most controls (up from 41% last year), and 87% of firms leverage an external SOC to monitor at least part of the environment. We can reasonably assume that firms using a SOC would feel more secure with additional eyes watching the network 24/7, but that is not borne out by the survey numbers. It is true that 80% of the firms who rated themselves as extremely secure have a SOC monitoring most of their security controls, and no firms without a SOC rated themselves as extremely secure. However, using a SOC to monitor half or more of a firm's security controls made no real impact on the percentage of firms who acknowledged having security gaps.



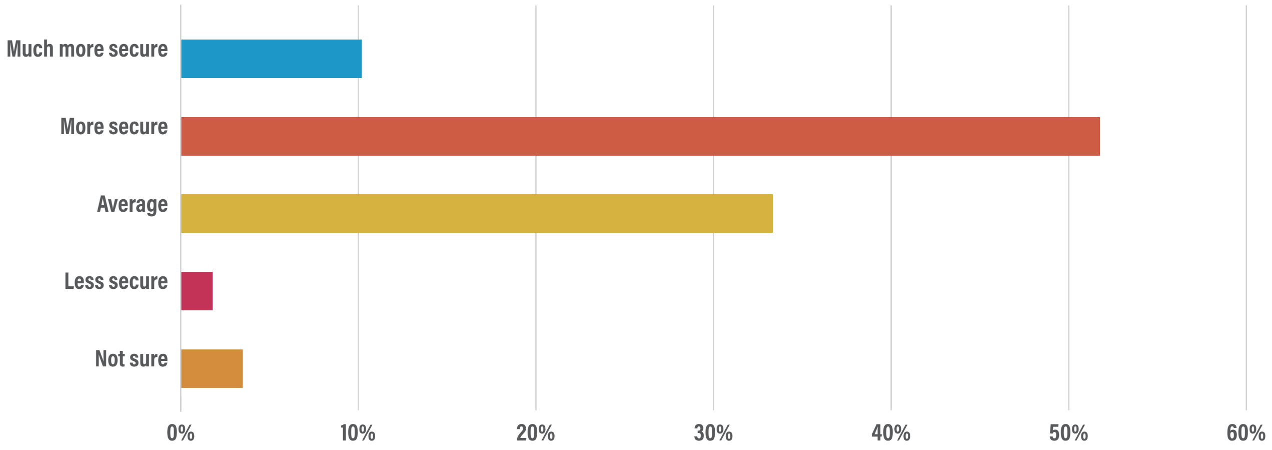
IR planning correlates closely with overall security confidence: 90% of firms rating themselves extremely secure and 84% of firms rating themselves as very secure have IR plans updated within the last 12 months. Notably, it is maintaining the IR plan itself — not testing — that correlates with improved confidence. There is no statistical difference in confidence between firms with up-to-date plans and firms who have taken the extra step to test and vet those plans.

Results By The Numbers (cont.)



Perhaps the #1 predictor of security confidence is the firm's attitude towards security. Firms that view security as a holistic effort not limited to the IT/InfoSec teams, with buy-in and support from firm leadership, comprise 90% of the extremely secure firms.

How secure is the Firm compared to the industry average?

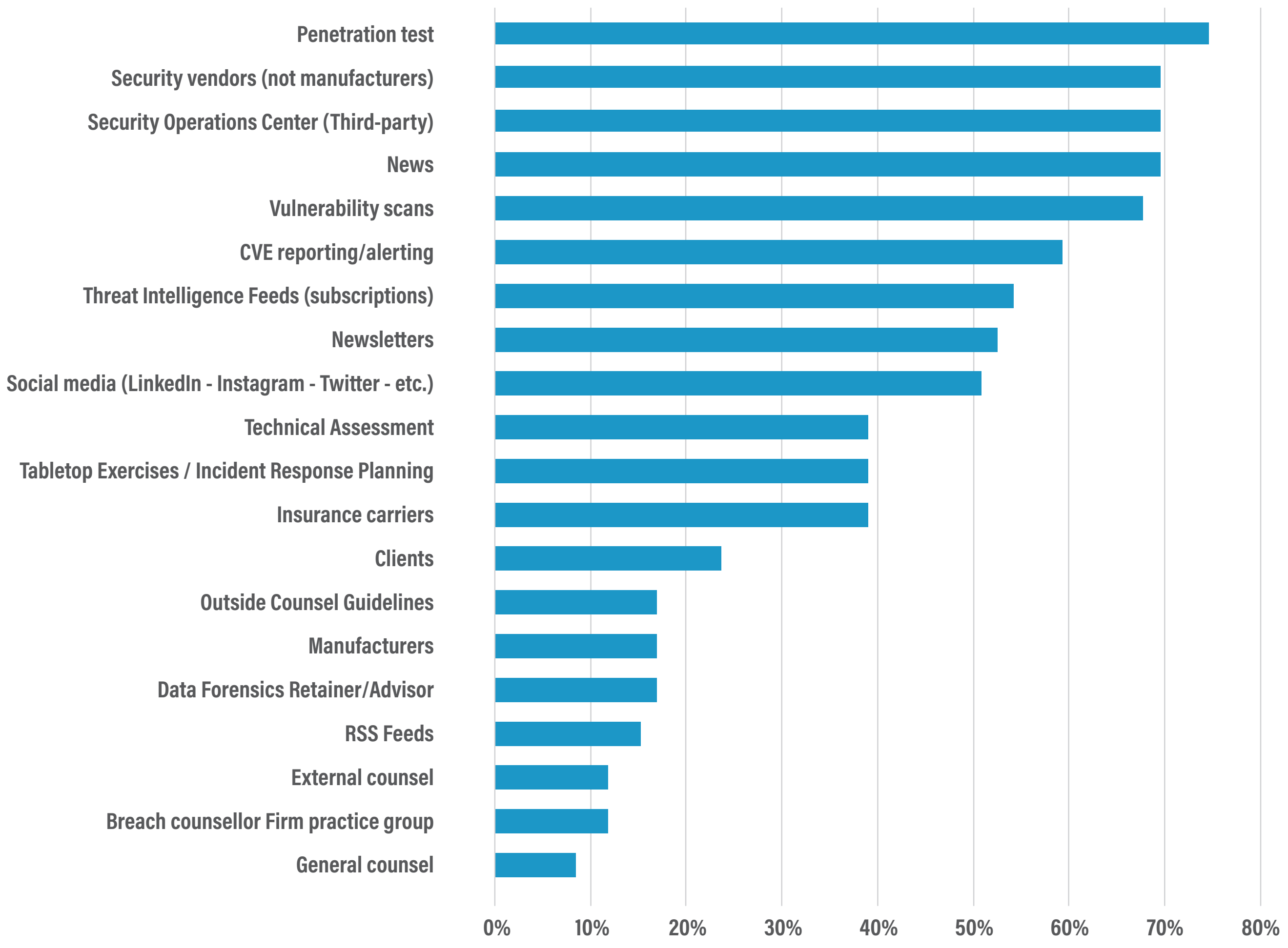


So, how do firms think they stack up against their peers? When asked, “How secure is the Firm compared to the industry average?” 52% of responding firms listed themselves as more secure than average, with an additional 10% believing they were much more secure. Is it possible that 62% of responding firms are more or much more secure than average? Maybe. The key word is “responding.” It is plausible that firms opting to respond to a security survey have a vested interest in security and are performing at an above-average level. Last year, almost 75% of firms listed themselves as above average, prompting questions about the definition of average. This percentage shrinking in the current survey may indicate that firms are becoming more aware of the landscape or believe that their peers are beginning to get serious about security orchestration. The truth is probably somewhere in the middle.

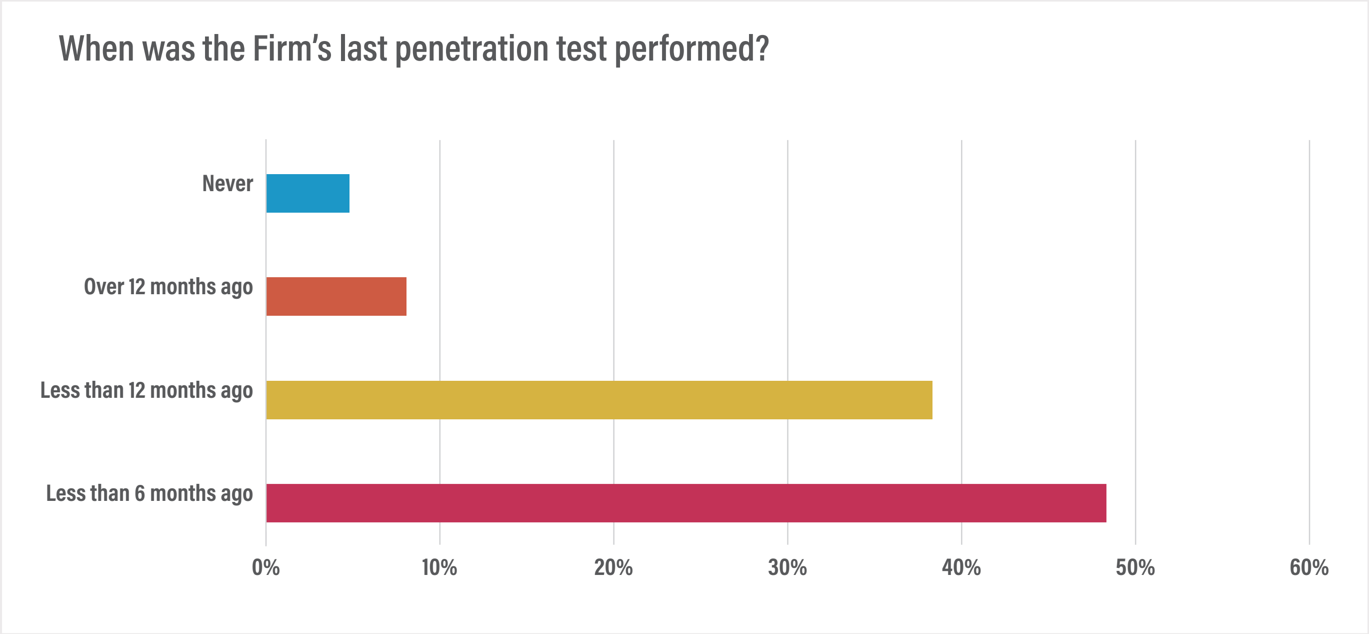
As usual, there is a correlation between size and comparison to the industry as a whole, with larger firms consistently believing that they are more secure than average, although mid-sized firms showed significant confidence as well. This makes logical sense. Large firms tend to have more access to resources in the form of money, staff, and outside expertise. In all likelihood they are more secure than average, at least on paper. Meticulous and ongoing orchestration of security controls is the best way to stay ahead of the curve, and larger firms with more resources can maintain this pace more easily.

Results By The Numbers (cont.)

Where do you get breach context (how companies are being breached from a technical perspective)?



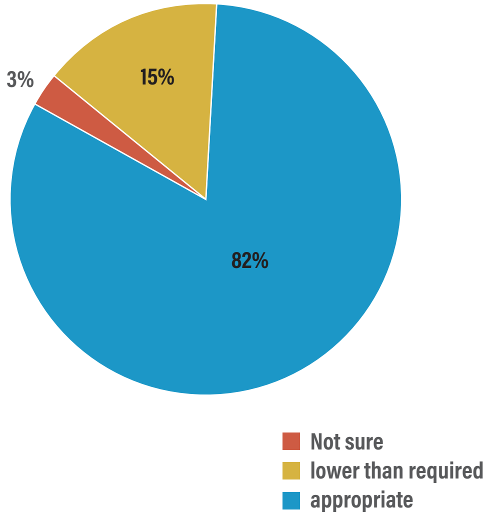
Control orchestration requires up-to-date threat intelligence. Without an understanding of current risks and threat actor tactics, firms cannot properly secure their networks. We found that 75% of firms rely on their penetration tests for guidance, with security vendors, SOCs, and the news all coming in at 69%.



The good news is that 87% of firms have had a penetration test within the last year, and 48% have conducted testing within the last 6 months. If firms are relying on penetration testing to provide them with breach context, then staying current with penetration testing is critical. Only 5% of firms have never conducted a penetration test, which is roughly consistent with last year's results, but the number of firms who have not had a penetration test in over a year tumbled from 28% last year to only 8% this year. Overall, penetration testing is trending in the right direction.

Security Budgets vs. Threats: Where Firms Are Spending

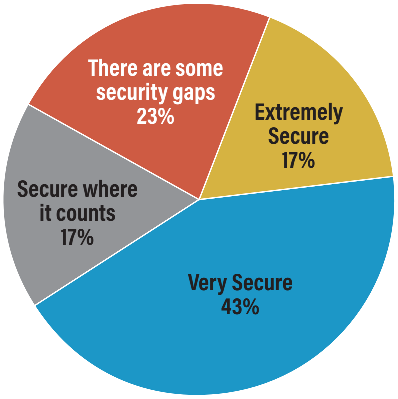
We asked law firms if they believed their security budgets were “adequate.” An overwhelming number — 82% — responded that they believed their budget was sufficient. Meanwhile, 15% believed their security budgets were less than what they needed, and just 3% responded “not sure.” Notably, no responding firms indicated a budget surplus related to security spending.



Is the Firm’s security budget adequate to protect the Firm from modern threats?

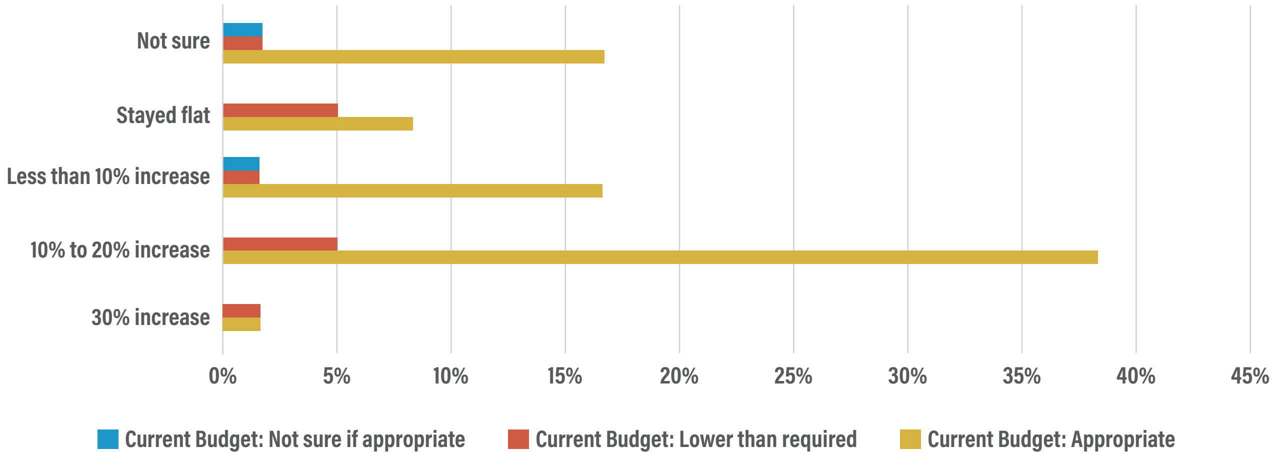
However, an adequate budget does not equate to strong security. When asked how secure firms were from cybersecurity threats, 23% noted gaps in security. With only 15% of firms reporting that their budget is lower than required to maintain proper security, we would have expected no more than 15% of firms to report security gaps.

Instead, 23% of firms acknowledge some gaps in security, and another 17% believe they are only secure where it counts. Is an adequate budget enough to maintain but not improve a security posture?



How secure is the Firm from cybersecurity threats like ransomware?

Projected Percent of Security Spending Increase In The Next Budget Cycle

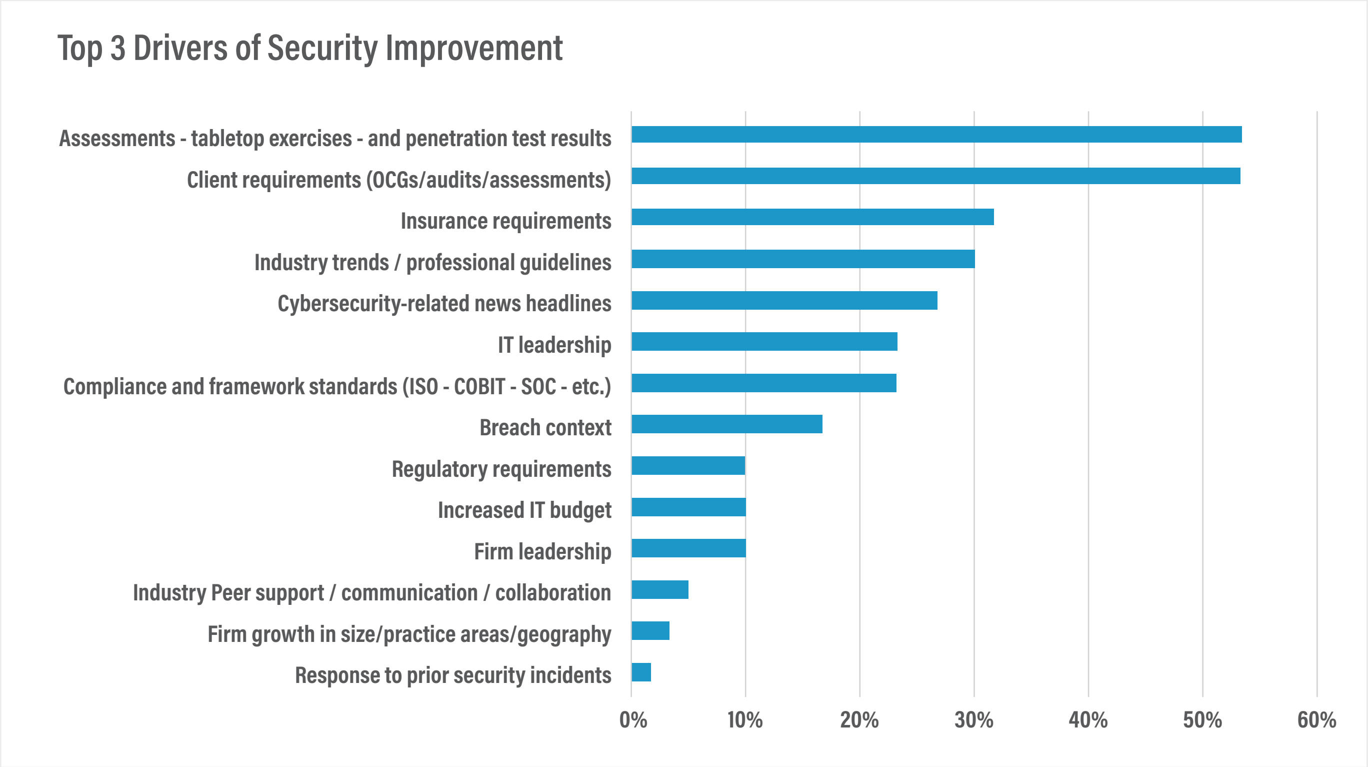


We saw a range of responses to our question about how much law firms expect to increase their security spending in the next budget cycle. Just under 40% expected an increase of 10-20%. Meanwhile, 17% said they were not sure or believed the increase would be less than 10%. About 7% expect the spending to stay flat, and only 2% expected at least a 30% increase. Comparatively, our 2023 survey revealed that the majority of respondents saw budget increases of less than 20% over the previous 24 months.

Even those firms who believe their budgets are adequate are increasing security budgets next year. Meanwhile, security costs continue to rise. Firms that have adequate budgets today, but are not increasing budgets year over year, may soon find themselves falling behind the security curve.

Security spending across the legal industry is rising for a variety of reasons, such as regulatory compliance, insurance requirements, and increasingly sophisticated client expectations. Clients are seeking assurances that their sensitive information is protected, and on the whole they have become more focused on the security of their outside counsel, thereby propelling adoption of emerging technologies and advancing the mounting emphasis on recovery over resilience. Additionally, there is a growing understanding that cybersecurity is a long-term investment, and firms may prioritize it in their budgets to avoid potentially catastrophic financial impacts from breaches.

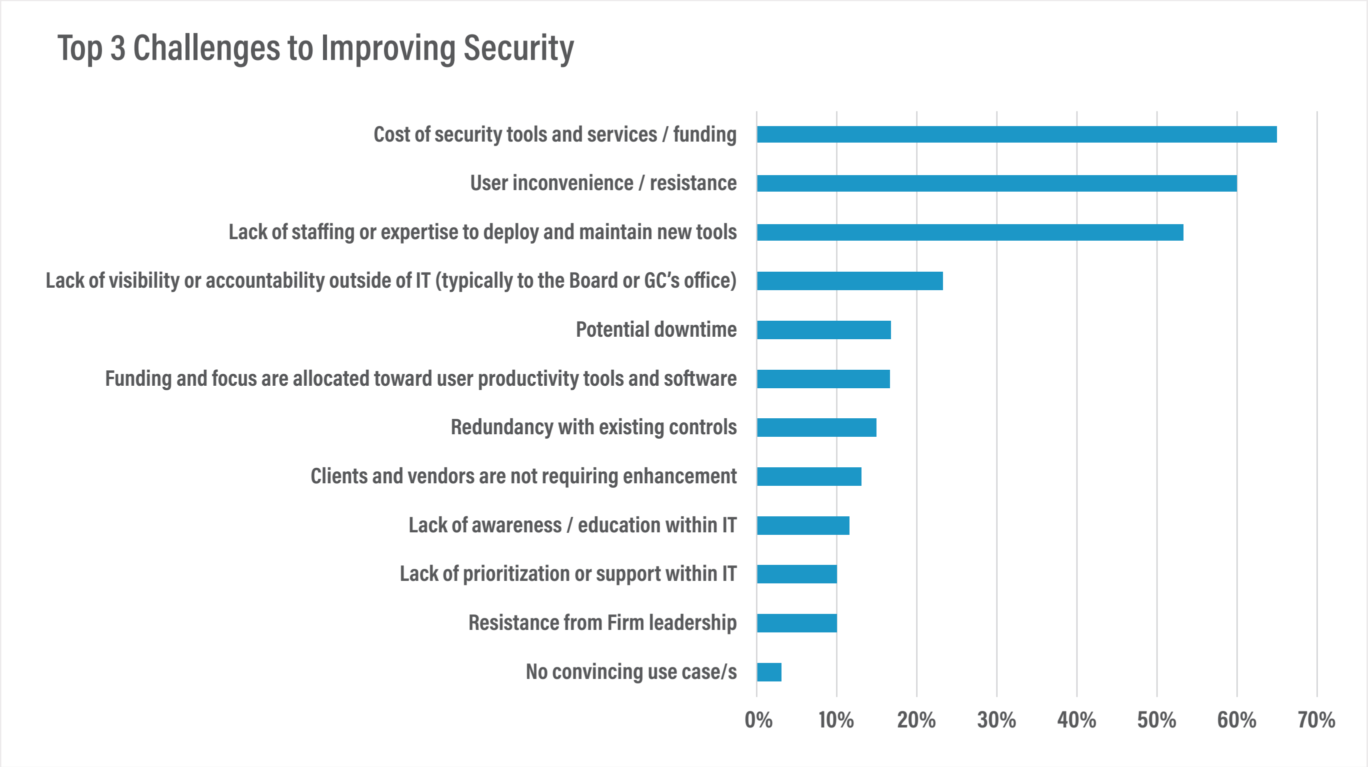
Why Firms Invest in Cybersecurity—and What's Holding Them Back



As evidence that both client and insurance requirements are major drivers of security change (and spending), 53% of responding firms listed client requirements in their top-three security drivers, followed by insurance requirements at 31%. These standings track with the 2023 survey, although the percentages for both client and insurance requirements increased considerably — up from 27% and 22%, respectively, in 2023.

However, there is a newly emerging top driver of change: assessments/tabletop exercises/penetration test results (53%). This driver drew only a 10% response in the 2023 survey, ranking third from last. The reason for this meteoric rise is unclear, but these items all produce clear documentation of risks that are hard to ignore.

IT leadership ranks sixth at 24% and is the first result that is internal to the firm. Year after year this survey finds that external forces continue to drive security improvement. Ideally, CISOs, CIOs, IT leaders, COOs, and executive committees should lead the charge for security improvements. Law firms may prioritize external pressures over internal IT advice due to a lack of understanding of technical risks or a belief that the feedback from external influencers is more relevant.



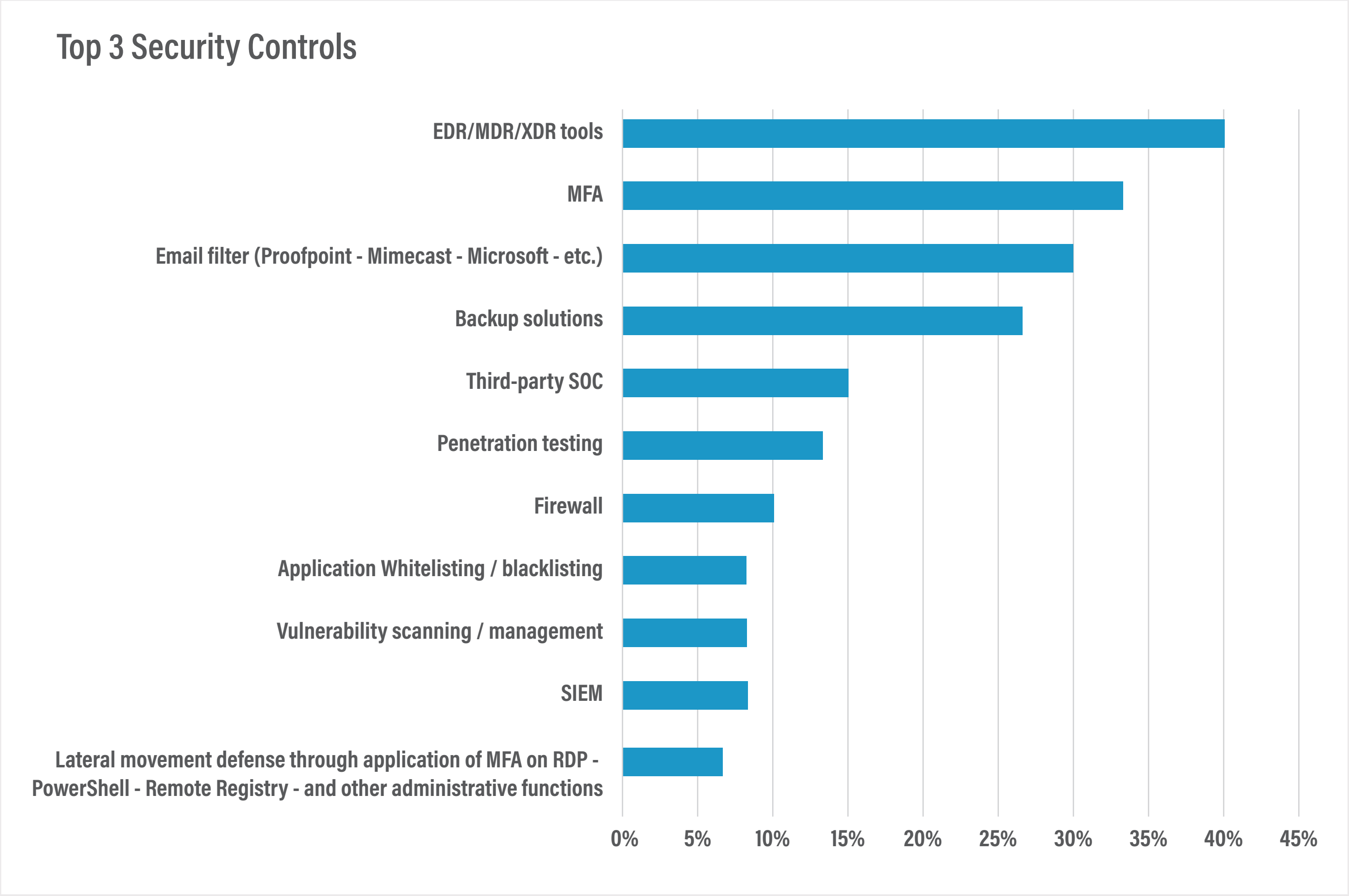
We asked respondents what they see as the top-three challenges to improving security, and we weren't surprised that the cost of security tools and services/funding topped the list at 65%. Cost was the #2 concern in the 2023 survey, surpassed by user inconvenience/resistance. These issues have swapped places in the 2024 survey but remain the primary impediments to improving security.

Costs involved in rapidly deploying technologies to stay ahead of threat actors and the expenses of hiring skilled cybersecurity professionals, as well as training and awareness and balancing budgets with other operational costs, factor greatly into the challenges of improving security.

The good news for firms is that while cost challenges remain at roughly the same percentage year over year, user inconvenience dropped from 80% in 2023 to 60% in 2024. Either users are recognizing that security is worth the inconvenience, IT security teams are treating security enhancements as non-negotiable, or a bit of both. It is still a long road to a fully compliant user population, but there is significant progress.

Why Firms Invest in Cybersecurity—and What's Holding Them Back (cont.)

In third place, in both 2023 and 2024, is the concern of lack of staffing or expertise to deploy and maintain new tools. Tools themselves are expensive, and contracting vendors to deploy them adds to the cost if an IT team does not have expertise on staff. Once deployed, these tools need to be monitored and maintained, which takes additional focus and time from IT teams or require involvement from a vendor partner.

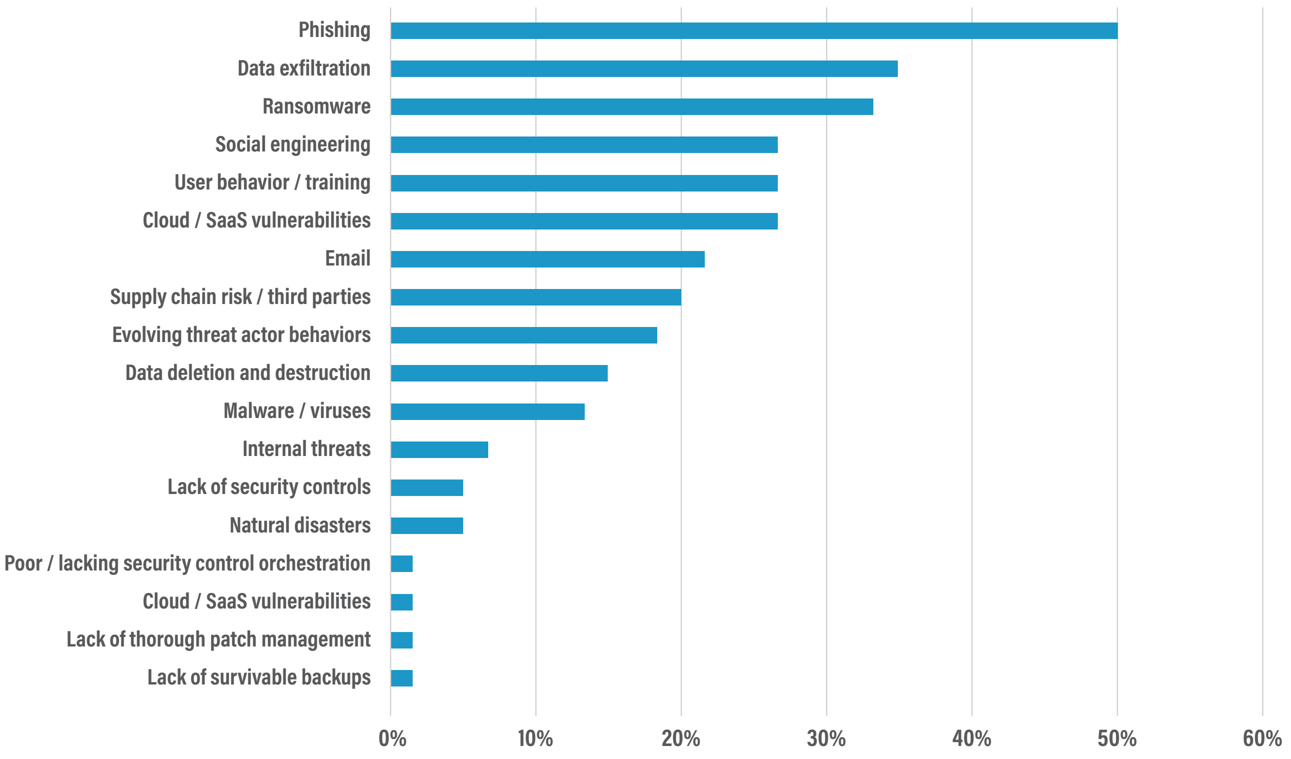


Survey respondents listed (collectively) endpoint detection and response (EDR), managed detection and response (MDR), and extended detection and response (XDR) as their top security controls. Multi-factor authentication (MFA), at 34%, and email filtering, at 30%, were the next most popular tools. Unquestionably, email remains an easily exploitable attack vector in 2024.

Backup solutions was a top-three security tool among 27% of respondents. Only 11% had selected backups in our 2023 survey, so the change is heartening, but the top three controls still indicate a security resistance mindset rather than a recovery mindset. As we said in last year's survey and will say again even more loudly, law firms have not sufficiently invested in backup defenses to prevent a non-recoverable mass destruction event. Immutable backups should be the #1 security control.

It is possible that well more than 27% of firms have received the message but lack confidence in their existing backup tools. Well, we are encouraged that more than twice as many respondents reported backups as a critical security control in 2024 as compared to 2023. We are optimistic that backups are continuing to gain in prominence as a security control.

Top 3 Threats to Security



Why Firms Invest in Cybersecurity— and What's Holding Them Back (cont.)

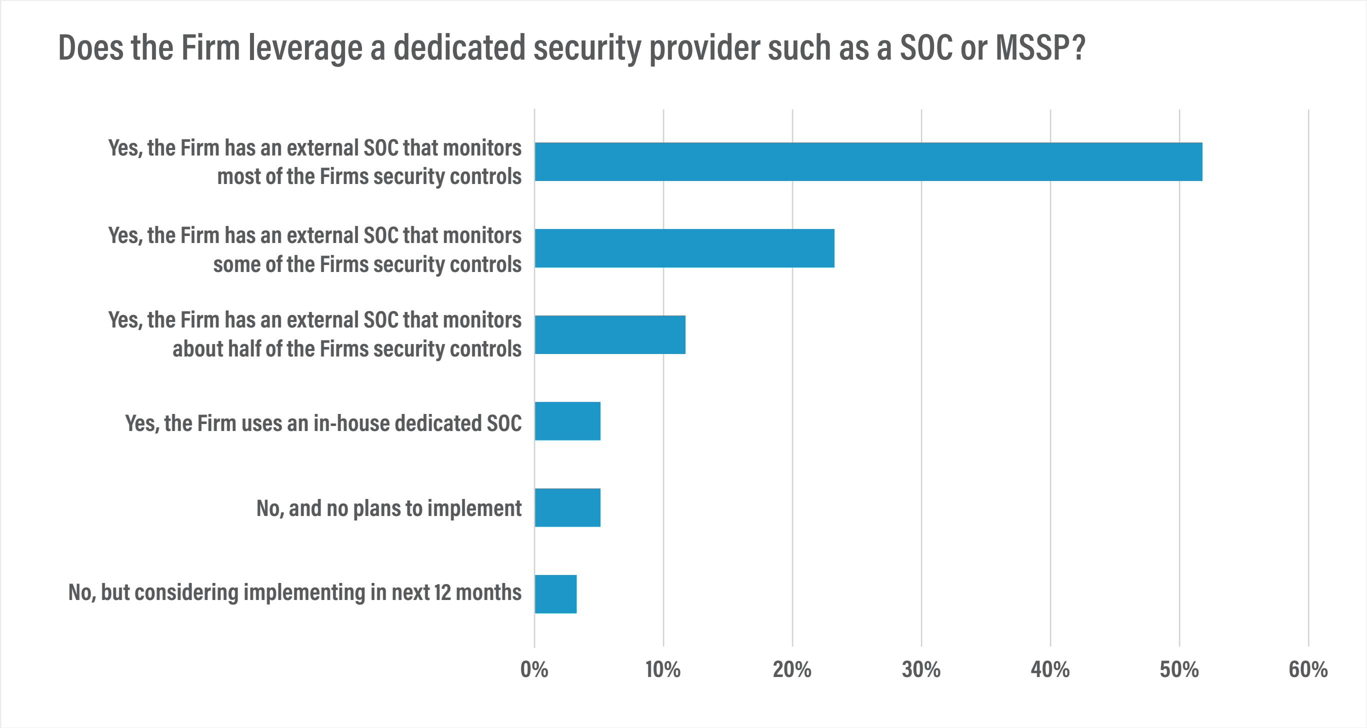
In the 2023 survey user behavior took the top slot as a threat to security. Because this has consistently been the #1 perceived risk across many ILTA surveys, we added several new categories to attempt to identify what specific behaviors are keeping security teams up at night.

Overwhelmingly, respondents listed phishing (50%) as the top threat to security, with social engineering in fourth place and more general user behavior/ training in fifth. These results imply that user naivety is the overall concern — that threat actors could take advantage of unaware or incautious users.

The Fenix24/Conversant Group's position is that it is hard to control user behavior but is comparatively easy to limit users' options for risky behavior. Essentially, users can behave badly because IT teams allow them to. Rather than trying to change the behavior through better training, which has limited success, firms should be restricting the opportunities for risky behavior. Blocking access to personal email, blocking password caching in web browsers, not allowing users to release quarantined messages, and restricting access from personal devices all help to mitigate bad user behavior.

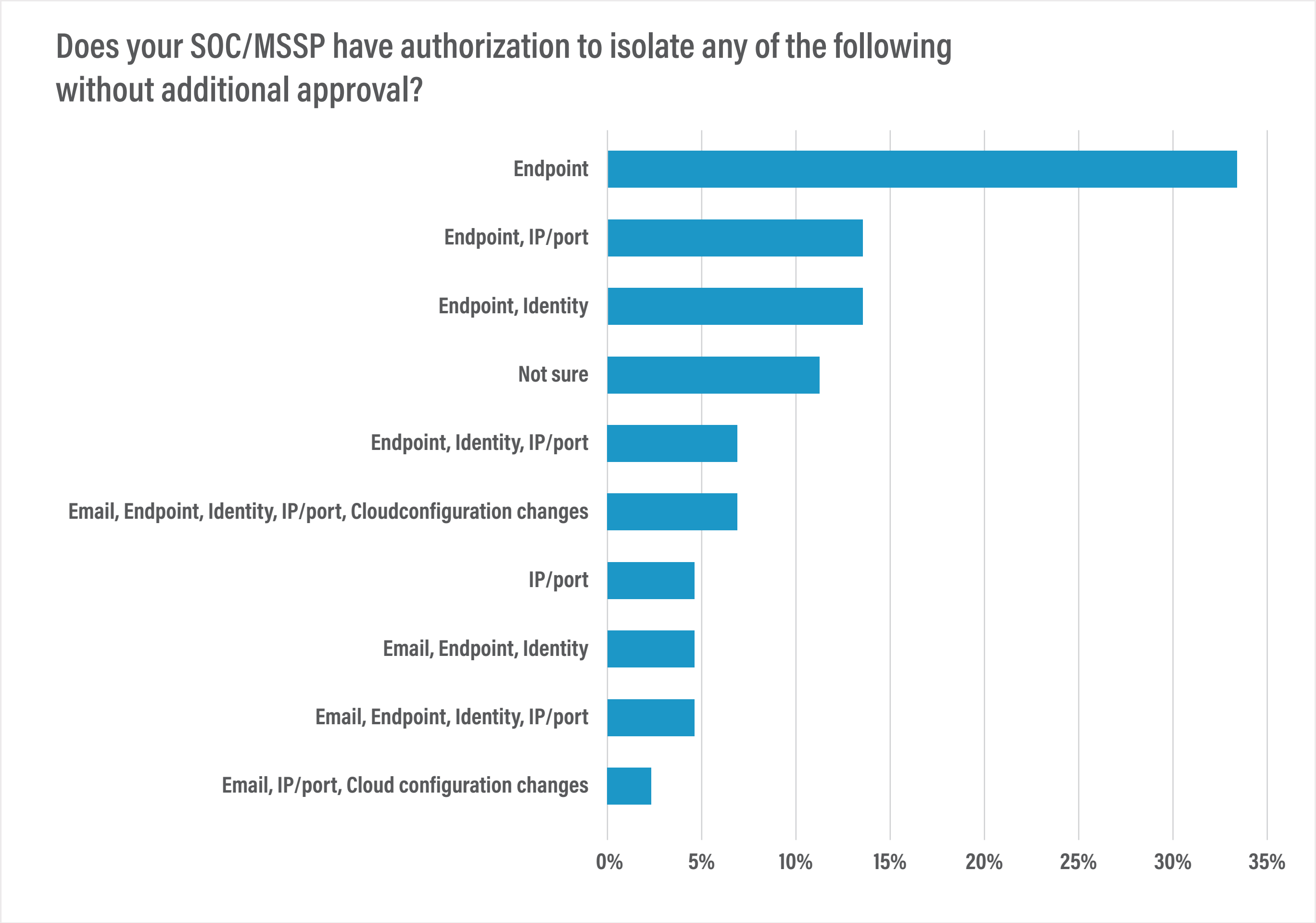
Data exfiltration (35%) and ransomware (33%) are often linked as a common tactic during a ransomware event is to exfiltrate data for additional leverage. However, data exfiltration edges out ransomware, meaning that firms are suddenly very concerned about where their data resides and who controls it — beyond ransomware-related exfiltration concerns. Last year, data exfiltration rated at 5%, so there has been a seven-fold increase in awareness of data exfiltration.

How Firms Detect and Respond to Threats



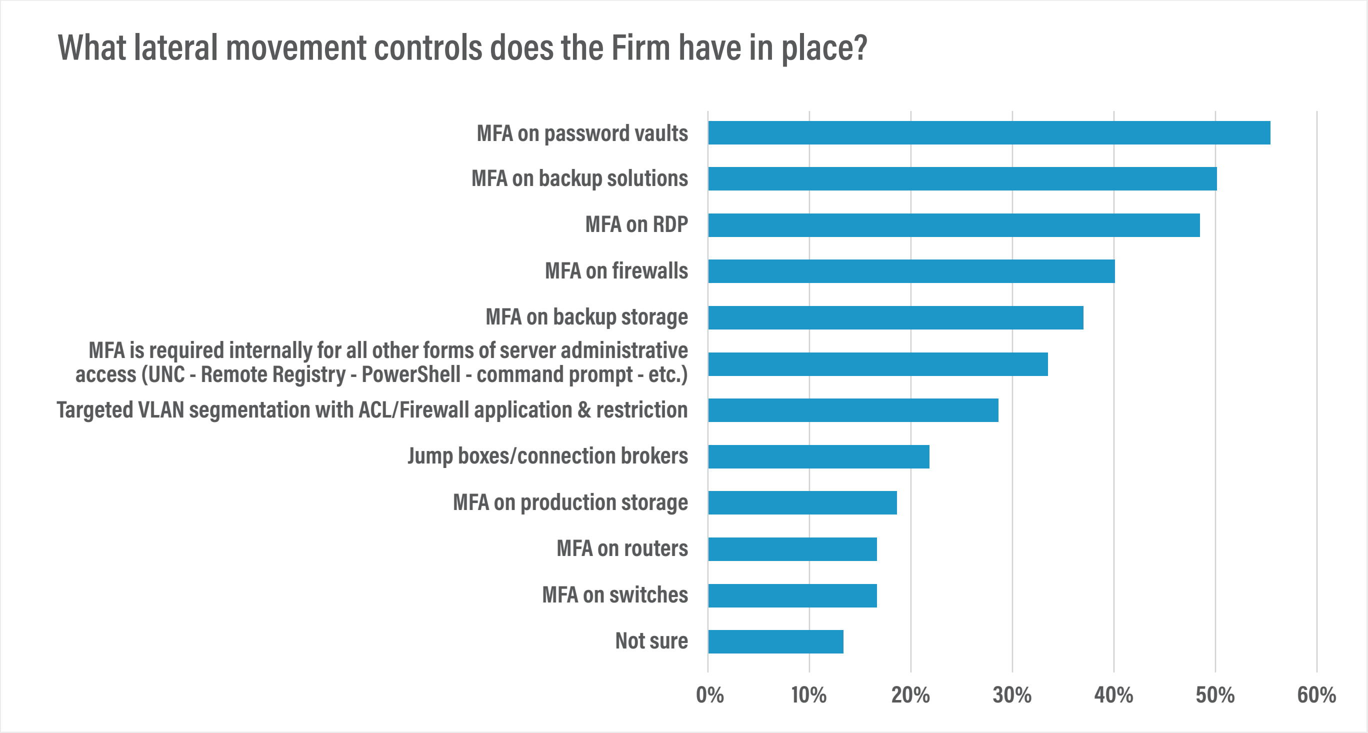
Our survey found that 92% of responding firms use a SOC to monitor at least some of the environment, and 52% of these firms leverage an external third-party SOC to monitor the majority of the firm's security controls. SOC adoption is up 16% since 2023, and SOCs have become a key component of many firms' security meshes.

How Firms Detect and Respond to Threats (cont.)



Probing law firms' SOC isolation capabilities reveals that 33% of firms with SOC can isolate an endpoint only. Endpoints are just one part of the kill chain required to limit a ransomware event. Only 7% of firms with a SOC can isolate endpoints, email, identity, IP/orts, and cloud configuration changes — and having these items in the SOC kill chain is critical to ransomware defense.

We know all too well that in the event of a security incident isolating compromised endpoints and other attack vectors allow SOC teams time to investigate and remediate threats without risking further impact to the IT network. Unquestionably, rapid response is critical for minimizing damage, retrieving lost data, and restoring normal operations, thereby limiting the effect of a ransomware attack.

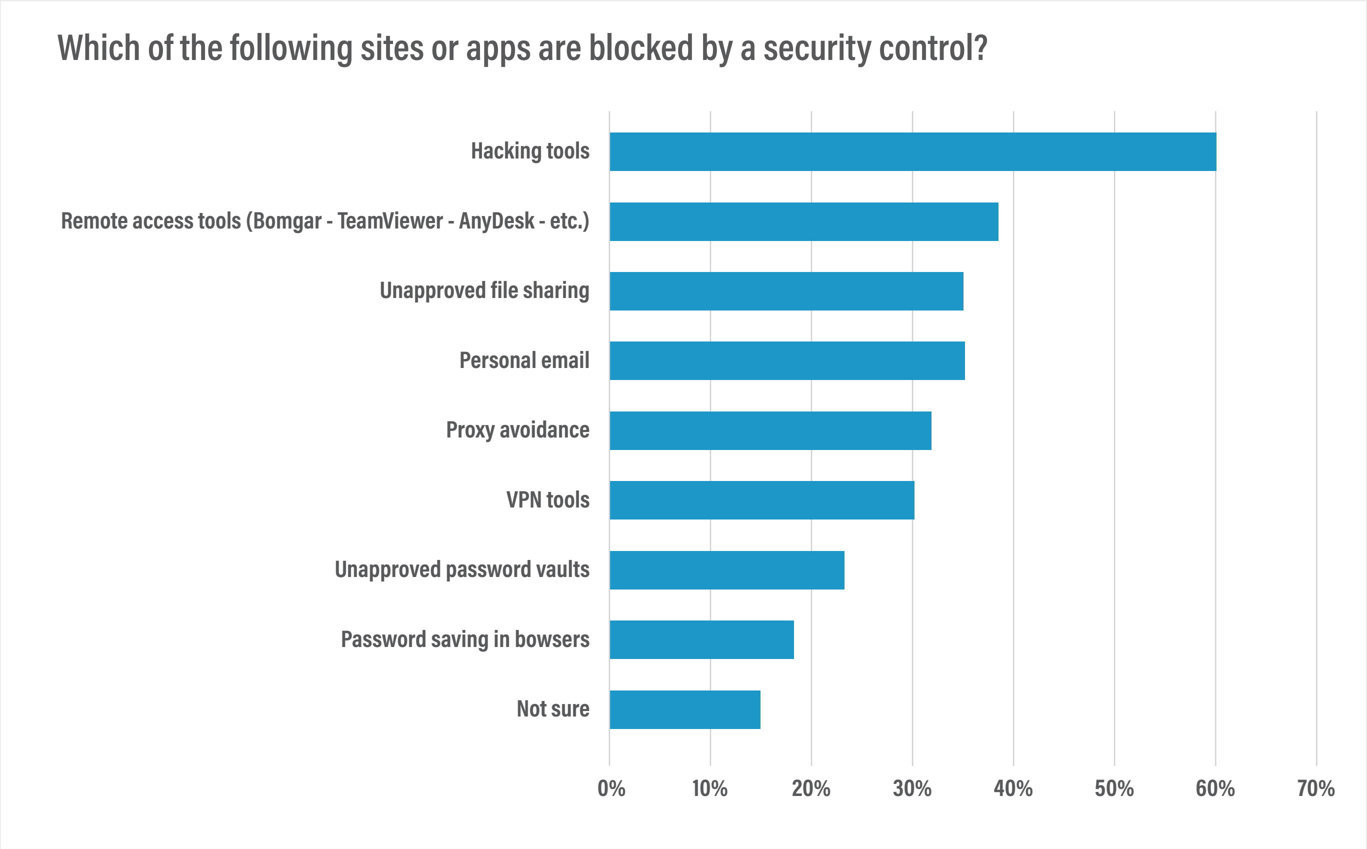


MFA is inconsistently applied to internal consoles, tools and controls. Consider that during a breach event threat actors will have access to the firm's network. If MFA is not applied to internal systems, it cannot slow an attacker who has breached the network perimeter. Network segmentation and micro-segmentation (to separate critical systems) also limit access to specific resources. This reduces the attack surface, making lateral movement more difficult once a threat actor gains access to the network.

"MFA on password vaults" was the top response (55%) regarding use of internal lateral movement controls. Meanwhile, 97% of responding firms employ one of more password vaults, and the remaining 3% responded "not sure," which dispels the myth that this number is artificially lower because not all firms are using vaults. The password vault contains the proverbial keys to the kingdom and is a prime target during a breach event, but 45% of firms are not protecting these credentials with strong MFA controls.

Only 50% of firms employ MFA on backup solutions, 37% have MFA on backup storage, and a mere 18% secure production storage with MFA. These three items are the end goals of a threat actor during a ransomware event, and they are underdefended.

How Firms Detect and Respond to Threats (cont.)

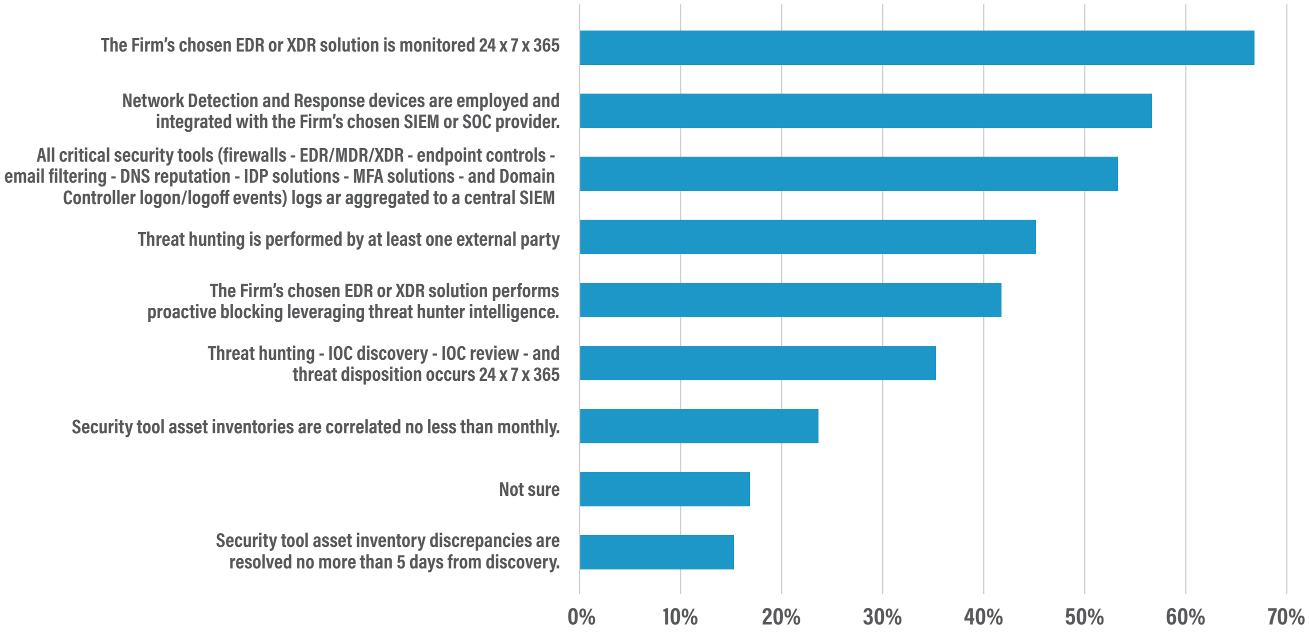


Most law firms are not adequately blocking potential attack vectors. While blocking "hacking tools" was the top answer, only 60% said they were doing so. Less than 40% said they were blocking remote access tools, personal email, unapproved file sharing, VPN tools, password vaults, and password caching in browsers.

Allowing access to these tools creates a permeable network perimeter and, consequently, an environment where a threat actor can establish persistent access, harvest elevated credentials, and easily exfiltrate data. Personal email, for example, bypasses the firm's email filter and may allow malicious mail to reach its intended targets. Allowing unapproved, commercially available remote access tools provide threat actors with an open door to ingress and egress the network. Unapproved password vaults place firm secrets outside of firm-controlled locations where they are not subject to the firm's security measures. Unapproved file sharing tools provide threat actors with an easy path for data exfiltration.

The evolution of hybrid or fully remote work environments has necessitated more remote access tools to allow staff to securely access files, applications, and resources from outside the office. Legal work often requires collaboration with third parties (clients, experts, consultants) who may need remote access to certain systems. If remote access by third parties is required, this access should be tightly scoped and controlled.

How is the Firm monitoring its security solutions?



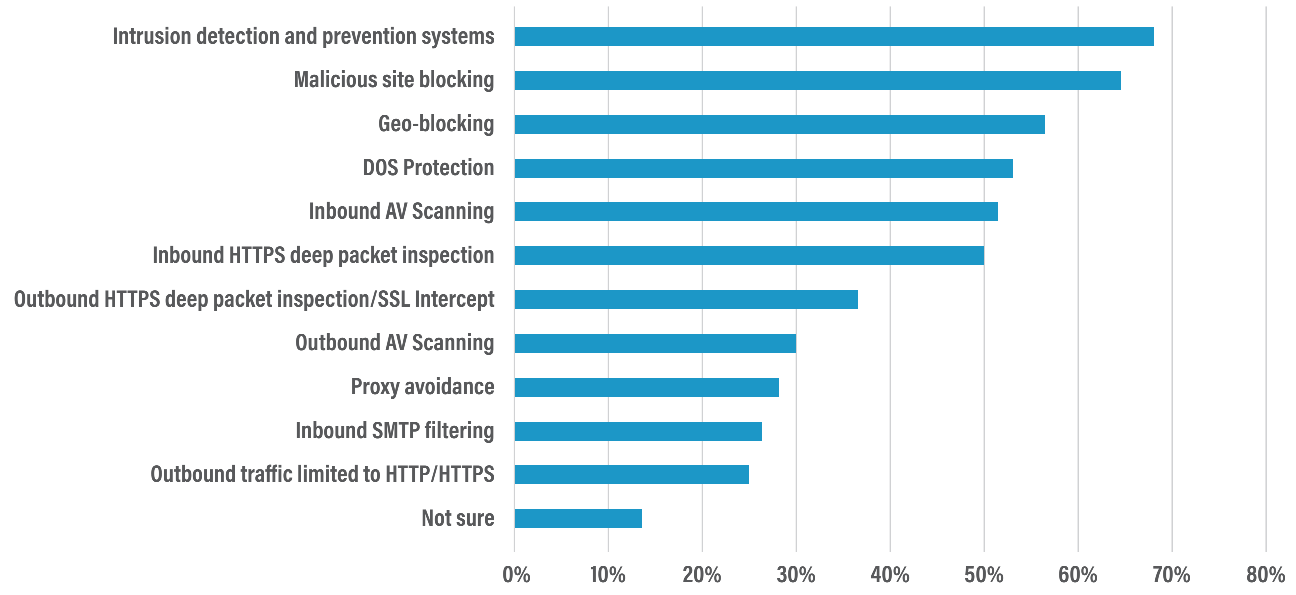
Almost half of responding firms said they do not have a centralized log source for monitoring or forensic purposes. While 67% of firms have adopted 24/7 monitoring of EDR and XDR tools, only 53% are aggregating logs from all critical consoles to a SIEM tool. Only 23% correlate security tools and asset inventories at least monthly, meaning 77% of firms cannot confirm that all systems are actually protected by their security controls.

There may be a variety of organizational, financial, and technical challenges, as well as concerns to data sensitivity and compliance, causing law firms to lack centralizing logging and monitoring

How Firms Detect and Respond to Threats (cont.)

systems. Contributing factors include high costs and underfunded budgets, limited in-house IT and cybersecurity expertise, privacy and confidentiality concerns, complexity of legacy systems, and data storage and retention challenges. Engaging a managed security services provider (MSSP) can often provide centralized logging, monitoring, and forensic analysis, thereby delivering a more holistic view of the security environment.

Enabled Firewall Security Features

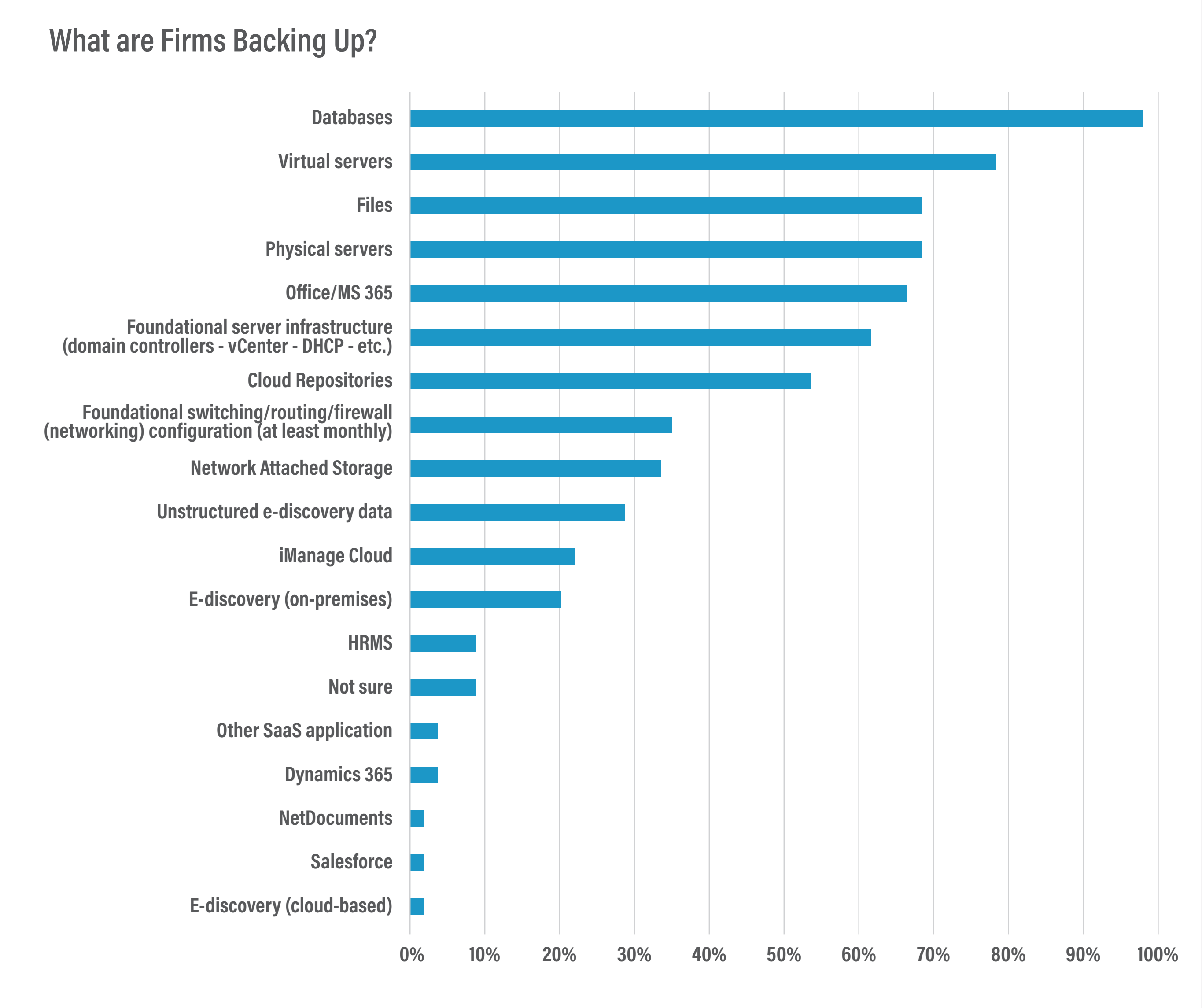


The survey indicates that many firewalls are missing key features like intrusion/detection prevention (68% enabled), malicious site blocking (65% enabled), and geo-blocking (57% enabled). Only 50% of firewalls are conducting deep packet inspection (DPI) on encrypted traffic.

While some of these features can be managed via other controls, layered defense is a key component of modern security. Even with compensating controls in place, a firm's perimeter firewalls should have these features enabled. DPI in particular is critical, as 95% of internet traffic (and approximately 85% of malicious traffic) is encrypted. Without DPI, the vast majority of traffic passes the perimeter without inspection.

[1] https://www.zscaler.com/blogs/security-research/2022-encrypted-attacks-report

Backup Strategies: What's Protected and What's at Risk?



While firms are generally diligent about backing up databases, servers and files on premises, they are not as attentive to foundational infrastructure (62%), Office 365 (67%), or cloud repositories (53%).

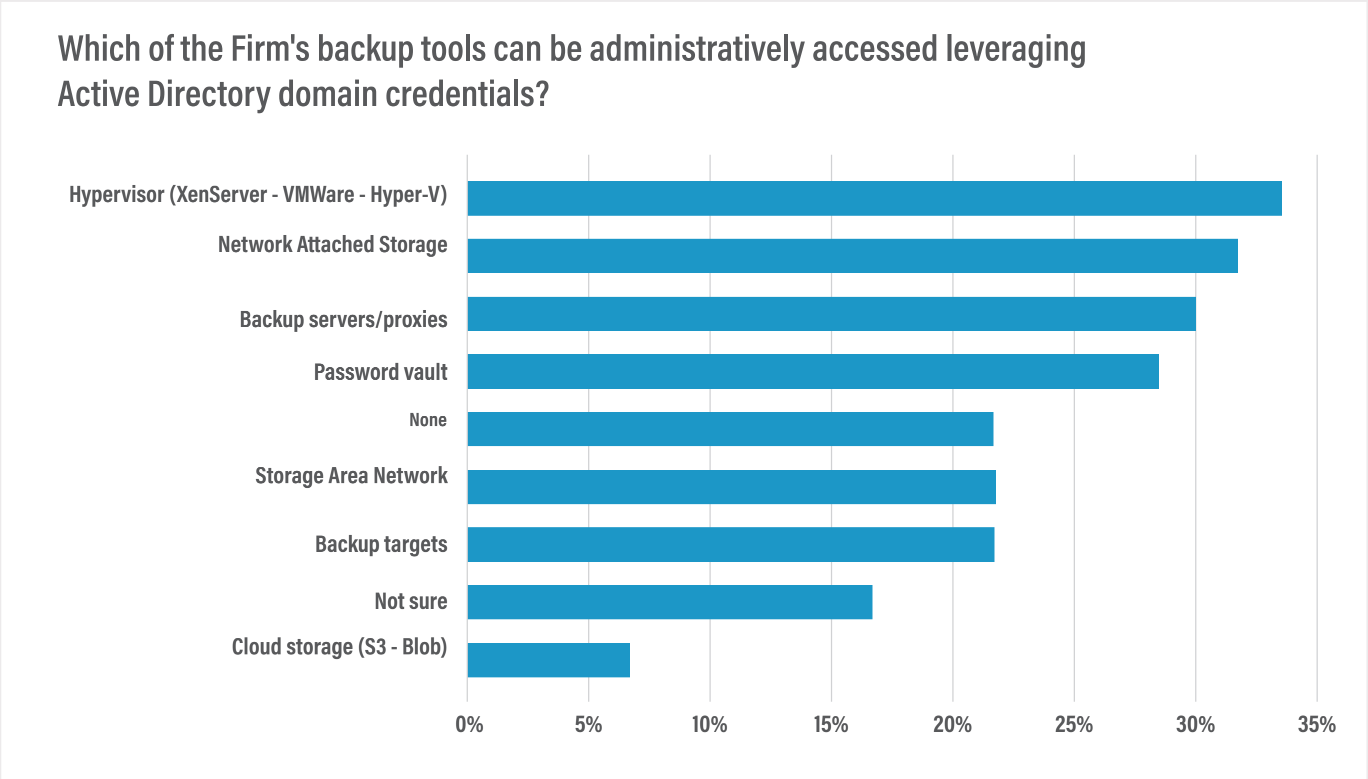
Other SaaS tools, including document management, eDiscovery, and HRMS systems, had significantly lower rates of backup, all under 25%.

Backup Strategies: What's Protected and What's at Risk? (cont.)

Because vendors often do not adequately protect their cloud-based systems, law firms are strongly advised to include cloud and SaaS data as part of their holistic backup plan. Because many vendors do back up client data they often have inadequate protection enabled to properly defend these backups. A firm may not be the target of a breach but can still suffer consequences from one if a vendor loses firm data. The safest practice is to maintain a firm-controlled backup copy of all SaaS and cloud data.

The cost and perceived complexity of backup management, in addition to a lack of understanding of backup best practices regarding SaaS data, may be keeping some firms from delivering on this strategy. Many vendors do not provide an easy option for backing up data stored in SaaS tools, and bespoke solutions are often required. However, if this data is vital to the firm's operations, it is incumbent on the firm to maintain a copy.

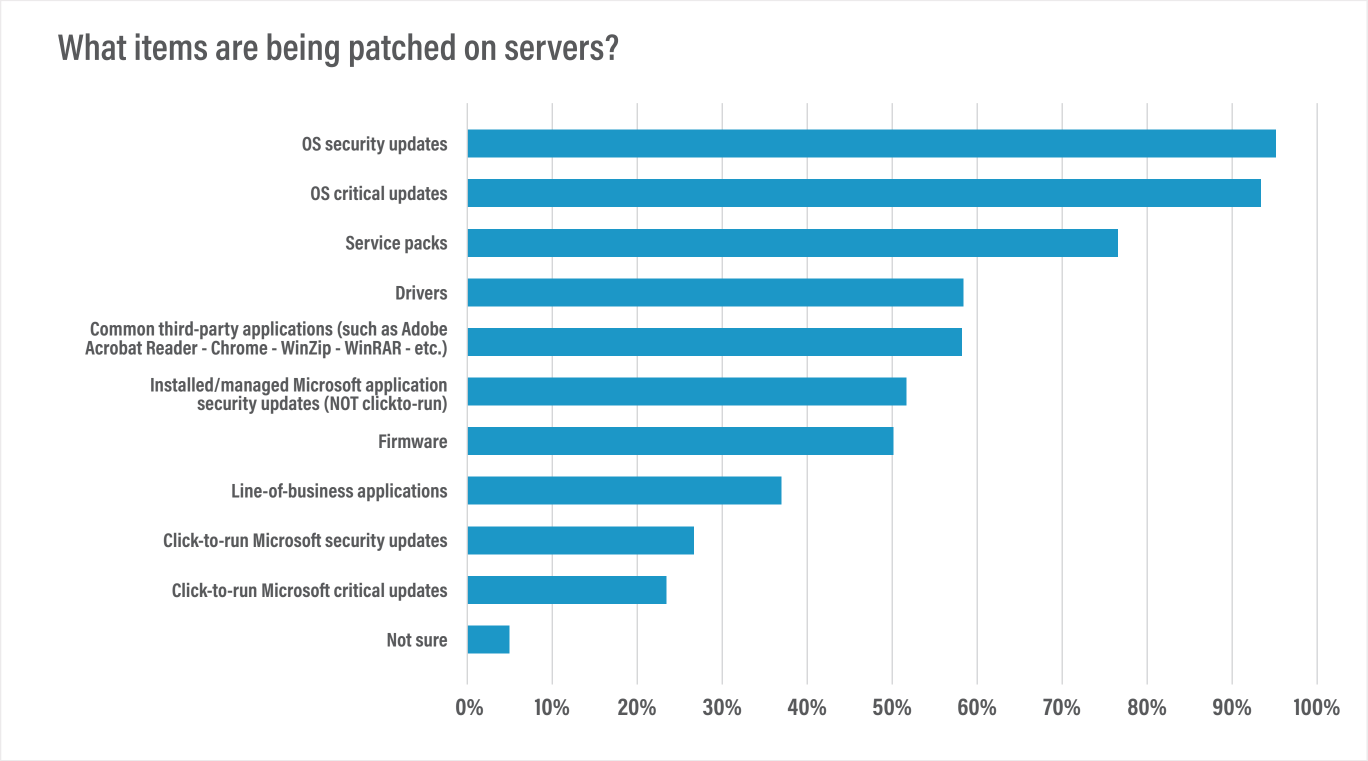
Domain Joined Backup Consoles



We see that 22% of firms have removed all consoles involved in the backup chain (production devices, backup consoles, and backup targets) from the domain — the most secure approach barring the use of a segmented and separate SSO admin tenant. While the percentages of each domain-joined tool are low overall, there is massive risk in any one of these consoles being discoverable and accessible via active directory (AD) credentials.

A compromise to any part of the backup chain can lead to a mass destruction event. These consoles should be removed from the domain, have access segmented from user networks, and require strong MFA before they can be accessed. Domain-joined backup consoles decrease data security because they increase the risk of lateral movement by a threat actor. Joining consoles to the domain increases the ease of daily management but introduces major security risks.

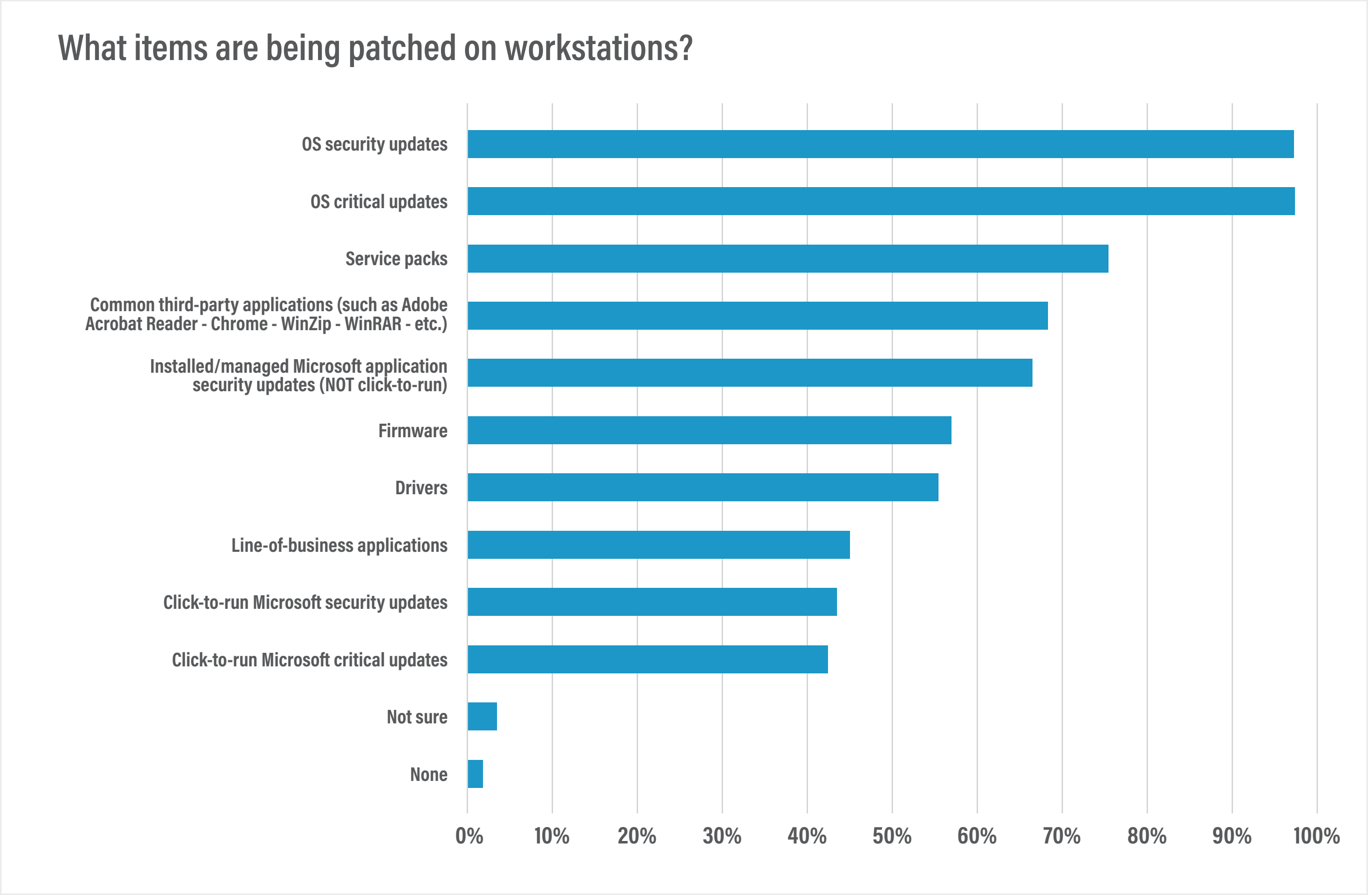
Patch Management: Where Are Firms Falling Behind?



More than 90% of respondents conduct routine security updates of their server operating systems. However, 50% of firms are not patching firmware, and 42% are not patching drivers on their servers. EDR and XDR tools often require up-to-date firmware and drivers to perform effectively and may be forced into low functionality by lack of updates.

Driver and firmware updates are more difficult to orchestrate than OS patching, as they are system-specific and are often not released with the same regular cadence and OS updates. Firms with a mix of hardware face additional challenges in running down all the required updates for each system. These updates rarely have a significant performance benefit and, unfortunately, they are often ignored.

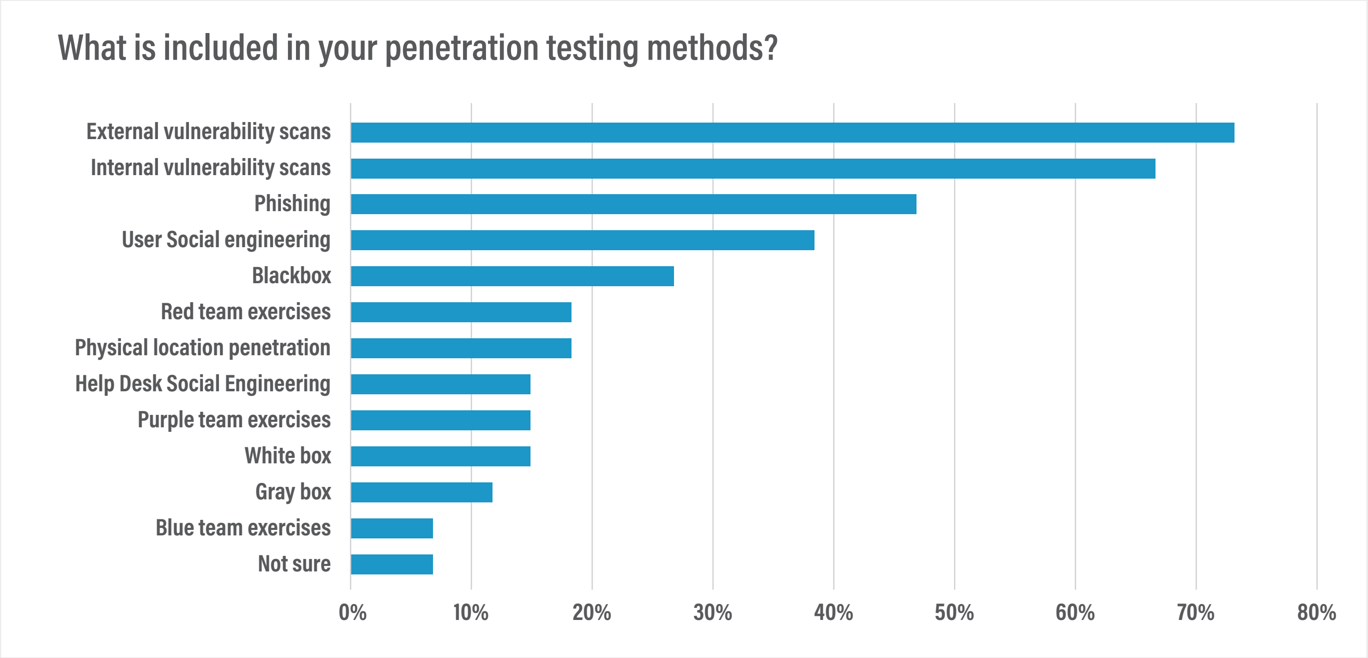
These patching challenges can be addressed through retention of a managed service provider (MSP) to reduce the burden on internal IT teams, but only 3% of firms report using a vendor for patching. Implementing centralized patch management software can also address these driver and firmware update challenges but will still require an investment of time and resources from the IT team.



The survey results regarding server patching are also reflected by a query around workstation patching. Here, 43% are not patching firmware and 45% not patching drivers, although 90% are patching operating systems security updates.

Law firms looking to get a jump on workstation patching can partner with a managed IT services provider that offers patching services. Of course, it's critical that firms institute patching policies that regularly update firmware and drivers on critical systems. Such initial planning and investment can seriously reduce security risk, prevent hardware issues, and enhance operational resilience.

Security Hardening and Penetration Testing: Are Firms Locking Down Systems?

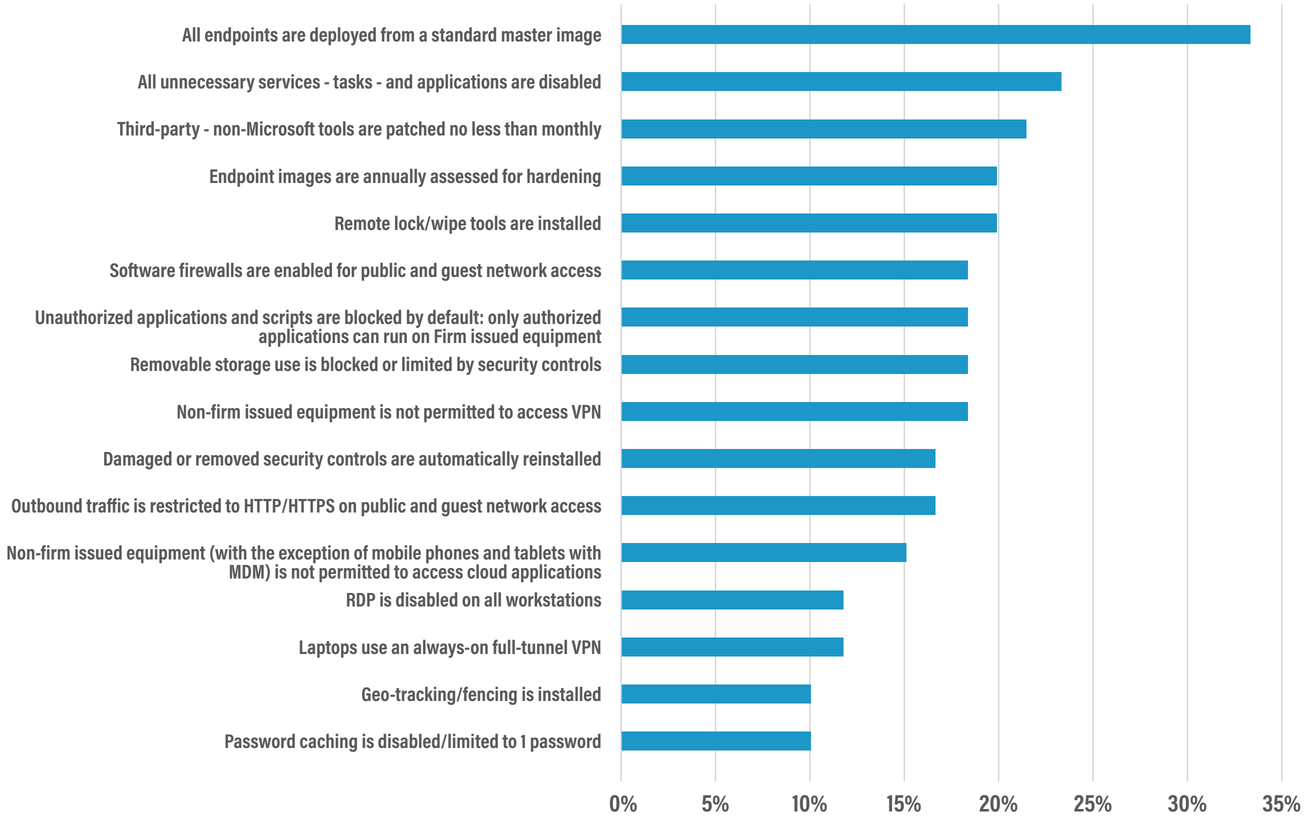


Most law firms we queried conduct external vulnerability scans (72%) or internal scans (67%). However, only 53% of them are engaging in some form of penetration testing (either black, white, or grey box). Unfortunately, 53% is considerably below the 87% reporting at least annual penetration testing in an earlier question. It is possible that some of these firms are conflating vulnerability scanning along with penetration testing. The primary definitional difference is that a penetration test involves a human actor attempting to compromise the network, as opposed to an automated scan.

We know that penetration tests are an excellent measure of how a human actor can exploit weaknesses in an IT environment. Fenix24/Conversant Group recommends grey box testing because it blends the best elements of black box, which mirrors a real attack, with white box whereby the tester has full access and knowledge of the environment and can move and test freely. Grey box testing shows what a true TA will likely exploit and also provides information about risky configurations that might not lie along the path of least resistance.

Again, cost, complexity, and business disruption are likely drivers around the lack of penetration testing among survey respondents. Penetration tests have the potential to create many alerts (not necessarily a bad thing) that the firm would have to address in some fashion.

How does the Firm harden endpoint systems?



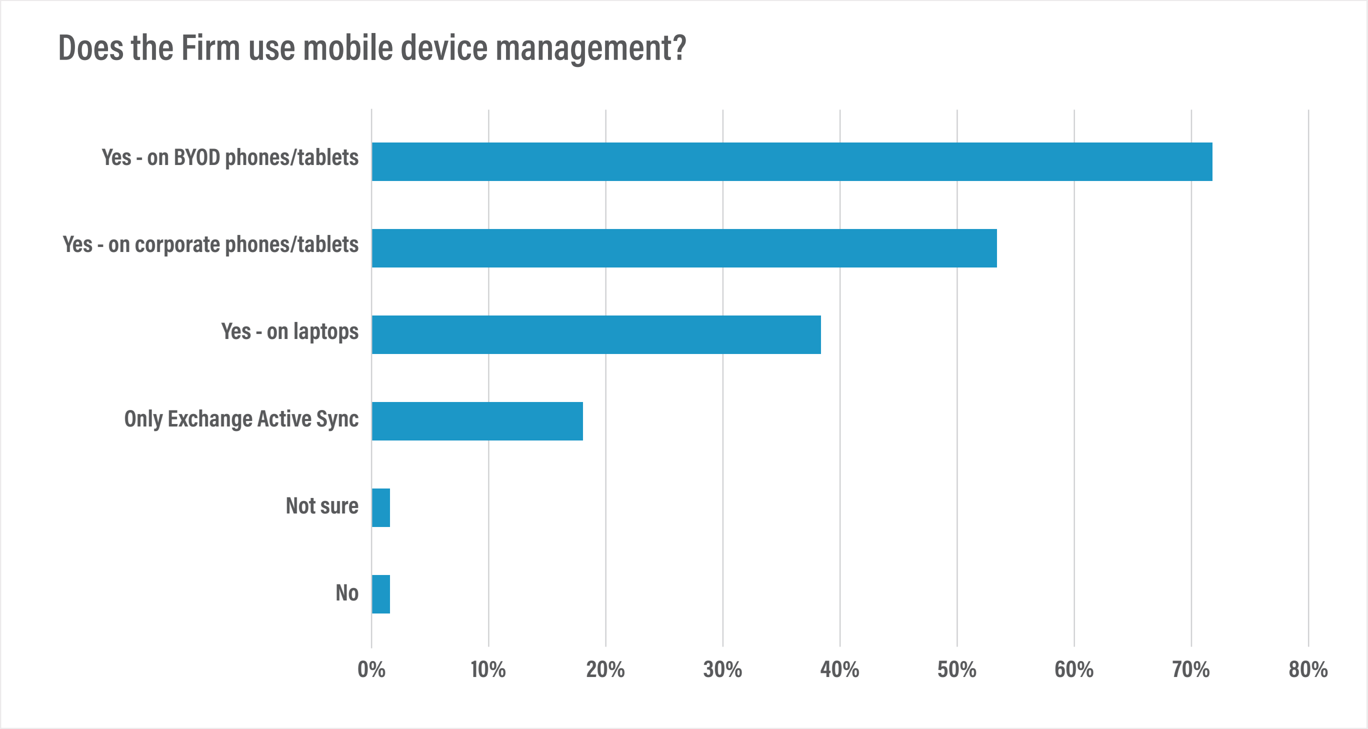
Endpoint hardening is crucial for law firms due to the highly sensitive information they manage and their requirements to protect client confidentiality, uphold regulatory obligations, and maintain a high standard of trust. As it was in last year's survey, "all endpoints are deployed from a standard master image" was the top answer regarding endpoint hardening, although only 33% of firms are using centralized deployment to help ensure that all devices are configured to a consistent baseline.

Only 20% of firms can remotely wipe a lost or stolen endpoint. While many firms may limit by policy the amount of sensitive data stored on a user's endpoint, there are still risks associated with a stolen device in the hands of a TA, as only 10% of firms are restricting the number of cached passwords on these devices.

Security Hardening and Penetration Testing (cont.)

Also telling, only 18% said they block unauthorized applications and scripts, which is a key component of layered security to supplement endpoint tools. Another 18% allow VPN from a non-firm-owned device — a massive risk in that essentially any person with proper credentials can access the firm network from any device. In addition, 15% of firms allow access to SaaS apps from personal devices, potentially allowing firm credentials to be stored on those less protected devices where they could be harvested and used by TAs.

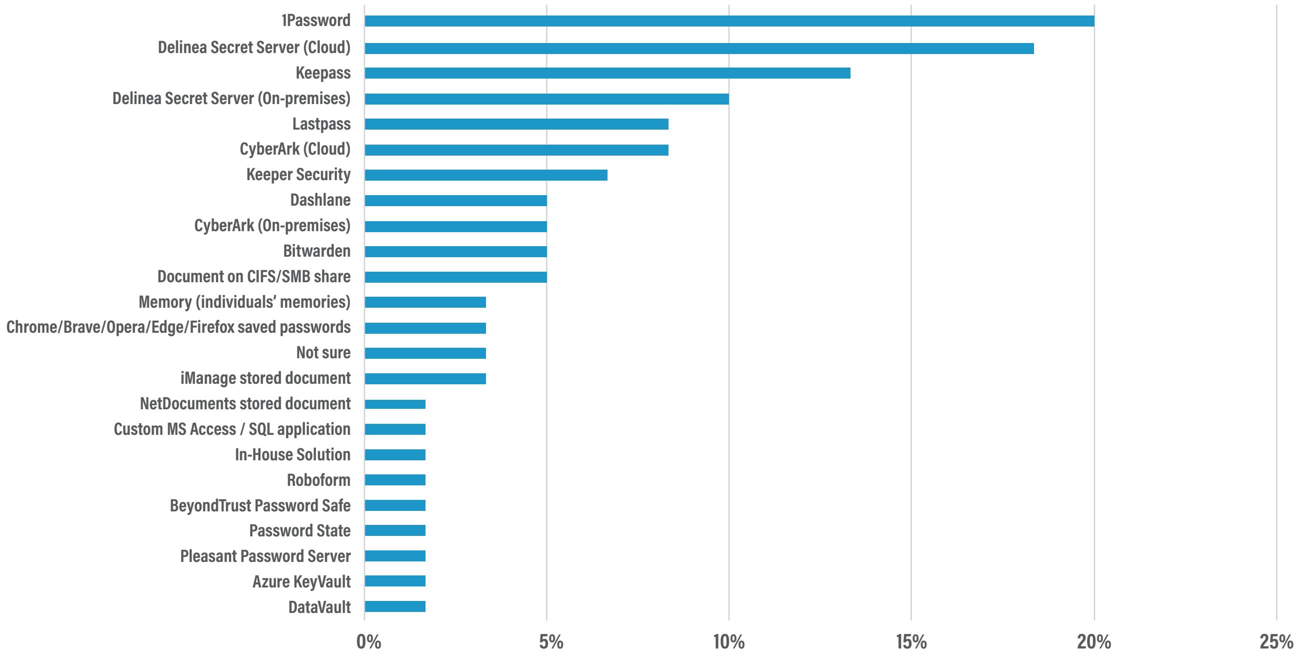
Mobile Device Management



Most law firms are using some form of MDM on either bring your own device (72%) or firm-owned devices (53%), and 38% have adopted MDM on their laptop fleets. However, 20% of firms are not protecting their mobile devices with strong MDM (18% relying on Exchange Active Sync and 2% not using MDM at all), which can lead to data and program access from unauthorized devices, data exfiltration, and other risks.

Credential Security and Access Management: What's Working and What's Not?

Where does IT store sensitive, privileged credentials, such as Service Accounts, Domain Admins, vCenter, Storage, etc.?

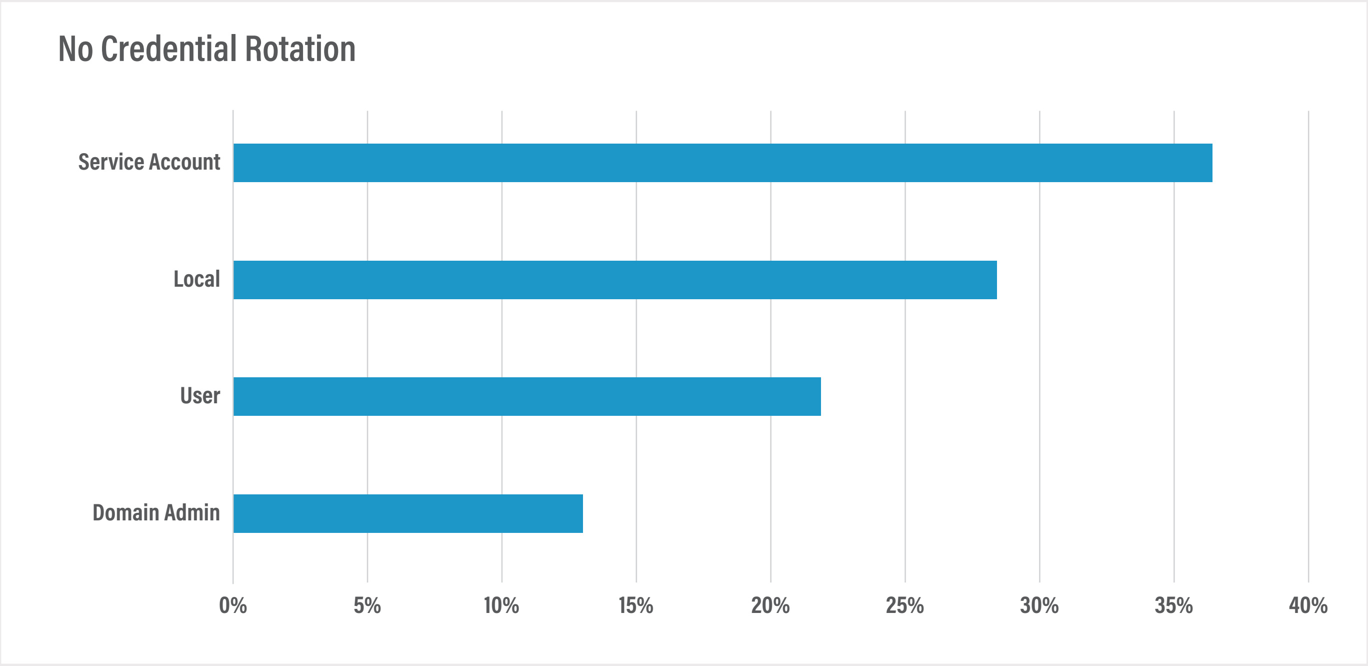


Fenix24/Conversant Group regards cloud-based password vaults as inherently riskier than on-premises solutions. They place the *keys to the kingdom* in a location not controlled by the firm and in a location that aggregates passwords from many businesses. These vault vendors are a prime target for threat actors, which can lead to a breach via a third party.

However, law firms may opt for a cloud-based solution for reasons such as lower initial costs and pricing predictability, streamlined deployment and maintenance, scalability for growing businesses, ease of compliance and certification, and automation of updates and security patches.

Fenix24/Conversant Group strongly advocates for an on-premises solution — one that is segmented from the user network and accessed through a jump-box, using a separate identity plane and MFA tool. An on-premises password vault allows firms to maintain direct control over their systems and reduce exposure to third-party cloud providers. On-premises vaults also offer improved incident response and forensic capabilities in the event of a security incident.

Credential Security and Access Management (cont.)



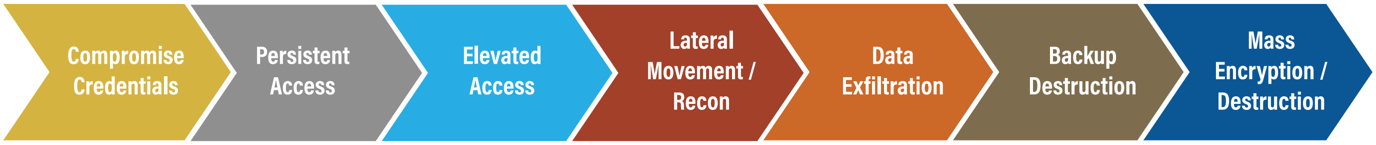
No Credential Rotation

According to the survey, 38% of firms do not rotate service account passwords, 28% do not rotate local admin passwords, 17% do not rotate user passwords, and 13% do not rotate domain admin passwords.

Current NIST guidelines advise against password rotation unless there is evidence of a compromise, suggesting that frequent changes often lead to poorer password habits. However, NIST also deems an eight-character password to be sufficiently long, provided it is a unique password or a passphrase that users can easily remember. NIST also encourages, but does not require, use of MFA.

NIST guidelines are exceedingly weak in the face of modern threats, and Fenix24/Conversant Group strongly believes that a password change will never make an account less secure. However, 35% of firms said they are still using eight-character passwords — again, meeting the NIST standard but missing the mark in the face of emerging security threat.

Breach Context: Understanding Law Firm Breaches



Breaches and ransomware events generally follow predicable patterns. First, a TA gains initial access to the network via a compromised credential, often through a phishing attack or by violating a system outside the network like a personal computer with cached browsers credentials synced into a personal account. Optionally, the TA establishes persistent access to the network, allowing them to come and go as they please. The dwell time of attackers on a network has dropped from weeks to hours in recent years, making this step less critical to attackers who often treat these events as a smash and grab. Once in the network, the TA attempts to elevate their access through compromising administrative credentials, which are then used to move laterally through the network, compromising additional systems and widening the breach. Data exfiltration is a common step, as it provides additional leverage to the attacker and may allow them to also blackmail the firm's clients. Sometimes exfiltration is the end goal of a breach, but more commonly attackers continue on to destroy backup systems, which deny recovery avenues before encrypting data to force a ransom payment.

This survey has identified many common risks along this breach path and quantified their prevalence among responding firms. Any firm that can place itself in each tranche of the breach pattern is at significant risk of a breach.

Breach Context: Understanding Law Firm Breaches (cont.)

Compromise Credentials

17% not rotating user credentials

35% using 8-character passwords

67% not using a password hygiene tool

57% not blocking impossible travel

53% not blocking malicious logons

38% allow SaaS app access from personal devices using SSO

89% allow password caching in browsers

67% permit unapproved password vaults

65% allow unchecked access to personal email

18% allow personal devices to access the VPN

43% allow SMS or phone call MFA verification

Persistent Access

62% allow unsupervised remote access by third parties

62% are not blocking commercially available remote access tools

70% not blocking third party VPN tools

68% do not block proxy sites

25% have no security operations center (SOC)

93% with a SOC cannot isolate the full kill chain

33% with a SOC are only capable of endpoint isolation

Elevated Access

13% not rotating domain administrator credentials

38% not rotating service account credentials

12% do not secure password vault with MFA

77% not restricting password caching on endpoints

Lateral Movement / Recon

73% no administrative segmentation

52% do not require MFA on remote desktop protocol (RDP)

63% no MFA on backup storage

82% no MFA on production storage

87% do not place MFA on switches

67% do not require MFA on Universal Naming Convention (UNC), remote registry, PowerShell task automation software, or command prompts

68% no network access controls (NAC)

43% have some portion of key ransomware targets joined to their domain (backup consoles, backup targets, hypervisors, and production SANs)

50% have no MFA on their backup tool console

Data Exfiltration

65% do not block unapproved file sharing sites

65% allow access to personal email

45% allow removable storage devices

30% not using Mobile Device Management on all mobile devices

72% do not enforce MDM on personally owned devices

47% do not require MDM on corporate devices

25% no outbound port restrictions on the firewall

72% not encrypting all hard drives at rest

Backup Destruction

52% do not have a single immutable backup copy

47% do not take snapshots of production storage systems

22% not backing up their virtual servers

38% not backing up foundational infrastructure (AD, DCs, DHCP, etc.)

30% have backup servers/proxies joined to the domain

22% have backup targets joined to the domain

Mass Encryption / Destruction

22% storage area network (SAN) is joined to the domain

33% have their hypervisor joined to the domain

32% have network attached storage (NAS) joined to the domain

Compromised Credentials

When a threat actor gains initial access to an IT network, the risks and repercussions can be devasting to a law firm's operations and reputation. Public-facing systems and devices on the edge of the network, or outside of it, can heighten the potential for compromised login credentials. The possibility that a threat actor can infiltrate the network is increased by use of personal computers and BYOD mobile devices, as well as the use of cached user passwords, weak credentialing methods, a lack of multi-factor authentication, and other lax security practices.

17% of firms said they are not rotating user credentials, meaning that compromised passwords can remain in use indefinitely.

35% of firms use eight-character passwords. Fenix24/Conversant Group recommends a minimum length of 16-character passwords — preferably a specific phrase using special characters — in addition to MFA and a password manager.

67% of respondents said they are not using a password hygiene tool. Password hygiene tools examine passwords for strength, comparing them against known weak or compromised passwords and forcing changes if they are at risk. However, many popular tools only warn of compromised passwords and do not enforce password changes.

57% of firms are not blocking impossible travel. Impossible travel restricts logons from different geographic regions, the logic being that it would not be possible to travel between those two locations in a set timeframe. For example, a user in New York City signs on and then attempts to sign in *from Hong Kong* only three hours later.

53% report that they are not blocking suspected malicious logons. Malicious logons are determined by a combination of factors, including geo-location, impossible travel, new/unknown devices, behavioral anomalies, and other factors to determine whether the logon is suspicious.

38% said they allow access to SSO-integrated SaaS apps from personal devices. Allowing access to single sign-on (SSO) SaaS apps from personal devices jeopardizes credentials and authentication tokens stored on poorly secured devices.

89% of responding firms said they allow users to cache passwords in browsers. These cached passwords can be harvested directly from a compromised endpoint, but some browsers also back up their caches to a user's personal cloud profile, potentially allowing them to be compromised outside of the firm's perimeter.

67% permit unapproved password vaults. Unapproved vaults place critical passwords within insecure locations not controlled by the firm, often in the public cloud, making them quite vulnerable.

65% of firms surveyed allow unchecked access to personal email. Unfiltered personal email opens a doorway to phishing, malware, and other risks that can bypass a firm's perimeter controls. It is estimated that 91% of breaches begin with an email, so permitting unfiltered mail on user endpoints is a major risk.

18% of firms report that they allow personal devices to access the VPN. If personal devices can access the VPN, then a threat actor with compromised VPN credentials and a client app or software can remotely log on to the firm's network. Firms can limit VPN access to personal devices that meet specific security criteria, such as encryption and antivirus software. The best practice is to only allow access from firm-managed devices.

43% allow SMS or phone call MFA verification. Both these verification methods are at risk of being compromised by a SIM swap, which redirects the MFA verification request to a threat actor's device. App passcode and verified push notifications are much more secure MFA verification methods.

Persistent Access

Persistent access allows a threat actor to come and go at will from an IT network, providing the time needed to orchestrate a cyberattack. Without persistent access, the entire attack must occur as a single, uninterrupted act. For law firms, persistent

Breach Context: Understanding Law Firm Breaches (cont.)

access has serious implications given the sensitive nature of their data around trade secrets, intellectual property, financial records, and personal data. Persistent access usually indicates the presence of an advanced persistent threat (APT) where attackers maintain a foothold to target high-value data.

62% of firms allow unsupervised remote access by third parties. This creates a supply chain risk. A vendor partner with free access to firm systems could be compromised and thus threaten the firm.

62% are not blocking commercially available remote access tools (RATs). Commonly used for remote access or remote support, RATs are popular among threat actors to establish persistent access within a network.

70% of respondents report that they are not blocking third-party VPN tools. Unsanctioned VPNs are another common threat actor tactic to establish persistent access.

68% of firms do not block proxy sites. Proxy sites increase anonymity and can be used to bypass other network restrictions by masking the end goal. For example, if access to hacking tools is blocked but proxies are allowed, a user or threat actor could access sites hosting those tools via a proxy.

25% of firms have no SOC. The SOC watches all network activity and can alert or intercede as it detects suspicious activity. No SOC means that nobody is continually watching the network, making early intervention during a breach very unlikely.

93% of those firms with a SOC cannot isolate the full kill chain (endpoint, email, identity, IP/port, cloud configuration changes), and 33% are capable of endpoint isolation only. Isolating the entire kill chain is critical for a SOC, as the endpoint may not be the source of a compromise. Endpoint isolation might not stop a threat actor from moving laterally inside the network. And if an identity, port, or email account is compromised, these need to be isolated too.

Credential Elevation

Credential elevation involves increasing a user's access level or permissions, typically from a standard user to an administrator or privileged user. A threat actor seeking access deep inside an IT network must harvest administrative credentials, which are often poorly secured and easily obtained once the network perimeter is breached. The breach widens with each new captured credential.

13% of firms are not rotating domain administrator credentials. Regularly rotating credentials limits the time an attacker, insider threats included, can use stolen credentials. Rotation minimizes potential damage while protecting against APTs, which often rely on long-term access to infiltrate systems.

38% of firms are not rotating service account credentials. Service accounts should be secured in much the same way as administrative credentials. Service accounts are prime attack targets because many service accounts have elevated privileges or access to critical systems and functions.

12% of surveyed firms with password vaults do not secure them with MFA. Once a TA breaches the perimeter, they will have nearly unrestricted access to

[2] Cybercriminals Exploit Content Platforms For Phishing Attacks And Data Breaches - Tech Business News

all the passwords they need to broaden the breach.

77% of firms are not restricting password caching on their users' endpoints, meaning that a compromised endpoint can be scraped for additional passwords, including elevated accounts which were used to initial setup or remote support.

Lateral Movement

Once a threat actor has control of your administrative credentials, the perpetrator will access and compromise critical consoles — a process known as lateral movement. MFA, network segmentation, and access controls are among the key tactics to limit lateral movement. Alarmingly, many law firms are using weak or no forms of lateral movement control at all. If perimeter controls fail, there's nothing in between the attackers and their targets.

73% of law firms surveyed said they have no administrative segmentation. Segmenting admin consoles restricts access from the broader user network and forces access through specific VLANs or devices. This limits a TA from moving directly from a workstation to a critical infrastructure or security tool. Network segmentation as a security control, rather than an organizational tool, can be challenging. It can be introduced gradually, starting with the most critical systems to minimize disruption and cost.

52% of firms said they do not require MFA on remote desktop protocol (RDP), which allows threat actors with captured credentials to move between workstations and servers unchallenged, compromising these systems and harvesting new credentials as they go.

63% of firms have no MFA on backup storage, which places backup systems in a vulnerable position. Even strong or immutable backup targets are potentially at risk if a TA has access to them. Any flaw in architecture or deployment could mean potential disaster if discovered and exploited.

82% of survey respondents have no MFA on production storage. A TA with direct console access to production storage has effectively completed their objective during a ransomware event. Strong MFA adds another hurdle for attackers, buying time to detect and respond or potentially stopping them in their tracks.

87% do not place MFA on switches, once again allowing TAs easier access to critical infrastructure, as well as to a key reconnaissance tool to understand the network and how to navigate it.

43% of firms who said they allow SMS or phone call MFA verification are at even more risk when an admin account is involved. A reliance on SMS or phone call MFA may open the door to SIM swapping attacks. A TA can impersonate a target and convince a mobile carrier to transfer the target's phone number to a new SIM card. The attacker can then intercept SMS messages or phone calls, gaining access to MFA-protected accounts.

67% of firms said they do not require MFA on Universal Naming Convention (UNC), remote registry, PowerShell task automation software, or command prompts. These are all potential attack vectors. The growing prevalence of cyber threats makes

Breach Context: Understanding Law Firm Breaches (cont.)

this a serious oversight. While there are barriers to adopt MFA for these tools — lack of awareness, perceived inconvenience, technical challenges, internal IT expertise, overreliance on default security configurations, and budgetary limitations — the risks far outweigh the challenges. Firms should view MFA as a crucial investment in protecting their clients' sensitive information and ensuring long-term operational security.

68% of firms report they have not deployed network access controls (NAC). Segmentation tools limit which devices are allowed to access the network and what devices can communicate with each other. NAC can be a component of admin segmentation. Once more, cost, lack of in-house technical expertise, perceived inconvenience, and underestimating the likelihood of cyberattacks may cause a firm to come up short on NAC. And as cyber threats continually evolve, NAC solutions are designed to adapt by integrating with other security tools, such as Security Information and Event Management (SIEM) systems and endpoint protection platforms. Adding NAC to the mix ensures a layered and adaptable defense strategy, helping detect unusual activity or unauthorized devices.

43% responded that they have at least some portion of key ransomware targets, including backup consoles, backup targets, hypervisors, and production SANs, joined to their domain. Domain-joined tools and devices make those systems more discoverable and accessible through compromised network credentials. Using local accounts or a secure segmented administrative identity plane can better protect these critical resources from lateral movement and compromise during a breach.

50% of firms report they have no MFA on their backup tool console. Without MFA there is nothing to stop attackers once they breach the network perimeter and secure valid credentials. By not securing these internal consoles or by allowing MFA bypass while on the LAN, firms are missing the strong protection provided by a simple security control that is likely already protecting other aspects of the environment. Some firms may omit MFA on the backup console because MFA is required elsewhere in the authentication chain (for example, MFA may be required to retrieve credentials form the password vault) but requiring MFA on the console itself provides a hedge against cached credentials or a breached vault.

Data Exfiltration

TAs are increasingly conducting data exfiltration activities during ransomware attacks — a tactic that provides greater leverage during payment negotiations. If the attacker gains access to cloud storage and file sharing sites, it provides an easy means to move large amounts of data. Personal email, removable mass storage devices, and poorly configured MDM are avenues to data exfiltration, whether malicious or accidental. Attackers may use a double extortion tactic whereby they not only encrypt data but also threaten to release client information if a ransom is not paid. Given the highly sensitive nature of legal information, the firm comes under intense pressure to comply with ransom demands.

65% of surveyed firms do not block unapproved file sharing sites. TAs can use file sharing sites to exfiltrate data during a breach while users can also exfiltrate data for either legitimate business purposes or malicious ones. Either way, the firm loses control of this data once it leaves the network perimeter. Balancing security with operational needs necessitates thoughtful policies that incorporate both client service and data protection. Many firms communicate with clients on the client's preferred sharing platform, which requires additional administrative overhead to secure and limit the opportunities for exfiltration and data leakage.

65% also allow access to personal email from company machines. Personal email is both a malware ingress and a data egress risk, as data can be sent via personal email to avoid network scanning. While this is a slower means of exfiltration, it still creates a risk, particularly from insider threats. In failing to block unapproved file sharing sites and personal email access, law firms often place business and client needs and productivity concerns above security concerns.

45% of law firms allow removable storage devices and thus are susceptible to data exfiltration — a common insider risk when someone is planning to leave an organization. Sensitive client data or other valuable information can be copied and removed from devices, such as USB drives, external hard drives, and SD cards. This can lead to a violation of attorney-client privilege, legal requirements, and confidentiality agreements. Removable devices can also introduce malware into the firm's network if they have been used on less secure devices. Even when used carefully and for approved purposes, there's always the potential for loss or theft of these devices — a risk that is magnified exponentially if the drive is not encrypted.

30% of firms surveyed say they are not using MDM on some portion of their mobile devices. While 72% do enforce MDM on personally owned devices and 53% require MDM on corporate devices, many firms use a mix of devices and only enforce MDM on a subset. Devices without MDM or with improperly configured MDM allow interaction with native and unapproved third-party apps on these devices that can save, store, or send firm data through unapproved and uncontrolled channels.

25% of firms have no outbound port restrictions on the firewall. Firms should restrict outbound connections to necessary approved ports and destinations and use DPI to monitor outbound traffic for suspicious activity. Allowing traffic only to trusted destinations and blocking malicious IPs and domains is highly recommended. Proper port restrictions can limit internal systems' ability to communicate freely with external networks, and regular reviews of outbound traffic logs can detect unusual behavior and anomalies.

72% of firms report that they are not encrypting all hard drives at rest. A stolen laptop with an unencrypted hard drive may contain sensitive data that is easily accessible. Laptop loss is a common tale in data breaches — and acutely detrimental within the legal profession. Encryption is increasingly seen as a baseline requirement for protecting

Breach Context: Understanding Law Firm Breaches (cont.)

sensitive client data and maintaining confidentiality. Modern tools make it easier than ever to implement encryption. Meanwhile, regulatory pressure and client expectations are driving encryption in the face of greater scrutiny for how firms manage sensitive data.

Backup Destruction

Destruction of backup data is a strategic and quite probable consequence of a ransomware attack. Without survivable backups, recovery of a law firm's network becomes virtually impossible. Ransomware victims are then left with little choice but to negotiate payment for a decryption key. Survivable backups — those that are truly immutable — are the top predictor of recovery after a breach. Even if a TA was able to gain access to the data, they would not be able to modify or destroy it because there are no administrative technical overrides to the retention lock.

52% of firms do not have a single backup copy that meets the standard of immutability defined above. These firms are acutely vulnerable to ransomware attacks and will likely be forced to pay a ransom to regain control of their data.

47% of firms do not take snapshots of production storage systems. These snapshots are the fastest path to restore production storage after a ransomware event and are incalculably valuable after a breach. However, for snapshots to be useful in restoration they must also survive the breach. If the snapshot is not stored immutably, it will likely be destroyed or encrypted alongside the production data.

22% of respondents are not backing up their virtual servers. Even if their data survives a breach, recovery will be delayed as the recovery teams rebuild servers to house that data. Backing up whole servers and system states alleviates this burden on the IR team and reduces downtime.

38% are not backing up foundational infrastructure like AD, DCs, DHCP, etc. This foundational infrastructure is required for a network to function. Rebuilding this infrastructure takes time, and rebuilding to a state that reflects the previous configuration can be difficult or impossible. These backups are critical to a recovery effort to prevent everything from network configurations to user and computer objects being recreated and rejoined to the network from scratch. No recovery of productivity tools can begin until the underpinning architecture is ready to receive them.

30% of firms have backup servers/proxies joined to the domain. As seen in the lateral movement section of this report, domain-joined backup tools and devices make those tools more discoverable and accessible using compromised network credentials. If accessed, these consoles can be used to disable and destroy backup jobs to increase a TA's leverage over the firm.

22% have backup targets joined to the domain. As above, joining the backup targets to the domain provides a relatively direct path for a TA to discover the asset, compromise the console, and destroy the backup data. This risk can be mitigated by obscuring access to the backup targets through network segmentation, ACLs, segmented administrative identity planes, or use of local accounts.

Mass Destruction

Mass destruction is a TA's end goal during a ransomware event. Destruction in this case likely does not mean deletion, but rather encryption to deny access to firm data. While destruction is possible during this step, unless the attack is state sanctioned with the express goal of doing as much damage as possible, most destruction is incidental due to the rough handling of data during the encryption process. Operations may be crippled until a ransom is paid for a decryption key or systems can be recovered from backups. Moreover, if backups are destroyed and data exfiltrated during a mass destruction event, the attacker has a powerful and likely intractable negotiating position.

Even if the ransom is paid, full recovery is far from certain, as not all decryptors are reliable and data loss during decryption is common. The longer the negotiation plays out the more it costs in terms of operational downtime, loss of business, and reputational damage, a potentially exorbitant ransom notwithstanding.

22% of firms report that their storage area network (SAN) is joined to the domain. These firms expose themselves to risk from attackers who compromise the domain controllers or gain administrative credentials for the domain through other methods. Administrative credential compromise can lead directly to unauthorized access, encryption, or destruction of all data in the network.

33% of firms have their hypervisor joined to the domain. Therefore, if ransomware spreads across a domain, it can encrypt endpoints, shared storage, and SAN resources if mapped or accessible via domain credentials. TAs can exploit lateral movement techniques, leading to faster infection. While domain integration simplifies access for legitimate users, it also increases the risk of abuse by threat actors during a breach.

32% of firms have network attached storage (NAS) joined to the domain. Firms should consider using local authentication or a separate authentication platform, coupled with strong MFA, for console access. To further secure these systems, firms can isolate them from the rest of the network by placing them on a separate management VLAN and limiting access via an Access Control List (ACL) while granting minimal necessary privileges for management and auditing.

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 Fenix24/Conversant Group

As the world's leading breach recovery company, Fenix24/Conversant Group has an unparalleled understanding of the tactics used by modern threat actors. Backed by the most comprehensive, end-to-end cyber resilience program in the industry, our team stands ready to defend — and rebuild — your business at a moment's notice. Fenix24 and its battalions were founded as part of the Conversant Group and continue to operate under its legal entity.

Learn more at Fenix24.com.

FENIX24 Recovery & Restoration

Ransomware rapid response, remediation and recovery

ATHENA7 Strategy & Execution

IT security assessments, strategy and planning

GRYPHO5 Managed Protection

Ongoing, security-based management

ARGOS99 Asset & Resiliency Software

Expert insights into data, assets and infrastructure