International Legal Technology Association

CONVERSANT GROUP

JUNE 2023

Security at Issue:
State of Cybersecurity in Law Firms

Results of the ILTA / Conversant Group Cybersecurity Survey

Foreword

Beth Anne Stuebe, Director of Publications and Press at ILTA

Looking out over the field of legal technology, we have seen a marked shift in the way firms and organizations have viewed security over the past few years, especially post-pandemic. Security has become the leading thread in any technical conversation, no longer a secondary or tertiary thought . . . and only then when a client brought it up.

And over these past few years, the discussions between security, attorney technology competency, and firm innovation have converged: thinking about one has led to thinking about all the rest. Security is the conversation: the rest, mere technical details.

This joint survey, a first for our industry, was conducted with the sole purpose of benchmarking security threats across law firms and providers to see where firms believed their gaps occurred. Questions on compliance, control, and configurations of tech were reviewed, and it became apparent that what we all thought were the biggest threats were not always the case. Threat actors were not the fear; our own users were often the issue.

Security concerns can come from within.

For decades, ILTA has conducted a Technology Survey aimed at the products and service side of legal that technologists use and consume on a daily basis. However, that survey and the team that orchestrates it have never tried to step into the shoes of a threat actor or looked at security as one who has suffered a breach.

To step into those shoes requires a deeper, often darker view, into a discussion landscape that most firms don't want to dive into, because they simply can't imagine that they are at risk. The key results we see from this survey show clearly that, without policy and procedure, firms are making security optional, left in the hands of users that are not technologically competent or trained enough to know how to be safe in a world that is both ever-changing and harder to innovate in without risk.

And security is risk. Data breaches can occur anywhere, including at the very peak of the legal industry. In the first quarter of 2023, the American Bar

Continued

Foreword (cont.)

Association suffered a breach. If the ABA, which has a national standard for attorney technical competency, can falter and lose data, threat actors can attack any firm, any organization.

It is not a question of "if" anymore, it is a question of "when."

Together, ILTA and Conversant looked back at a prior survey we had done together and then stepped further out with this all-new survey. ILTA is grateful to have a survey partner like Conversant: they are steeped in the daily world of recovery and know how to help clients, like our ILTA members, when the worst-case scenarios come to pass.

ILTA hopes this all-new security survey will help our members, those in all facets of legal technology, and those who may fall victim to a threat actor, to deal with and avoid future or any attacks.

The key to security is in your hands.

Contents

Executive Summary & Key Takeaways

John A. Smith, Chief Executive Officer, Conversant Group

Threat actors are typically known for being motivated by political malfeasance, social righteousness, espionage, or even revenge (as is often the case with insiders). But in our experience, most of the time, they are simply following the money. Most threat actors preferentially target victim organizations that can be easily penetrated and are incented to relent to their demands, maximizing their returns for the least time and effort expended.

Unfortunately, law firms make an ideal target.

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. ILTA conducts an annual Technology Survey to gather information about which IT-related technologies, products, and services law firms use. This 2022 follow-on survey jointly conducted by 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 a deeper view: What were the firms doing with these technologies—and beyond these technologies? How were they layering these solutions with their people and process to achieve an orchestrated approach to defending

Executive Summary & Key Takeaways (cont.)

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. We provide the full, unadulterated data results in the Data Findings section to follow for you to interpret as you will. 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. And we will give insights into how firms, generally, can improve their defenses.

Key Takeaways

While the data lends itself to obvious conclusions—which we will discuss below—we also see 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), nor the previously mentioned study that showed a third of firms suffered breaches in a single calendar year. We believe this is a definitional problem by what is meant by "secure" and what achieving true defensibility looks like. IT and cybersecurity professionals often lack context around what it means to be "secure." As one example, Conversant recently had a discussion with a leading law firm implementing MFA on administrative functions. The IT professionals involved in the discussion asked, "Will we have to accept an MFA push for every administrative function accessed on a server?" When we affirmed that would be the case, the law firm replied, "That's absurd and simply too much aggravation." It is our view that, not only is this requirement far from absurd, it displays a paradigm, position, and understanding of our definitional problem. If an administrative function is easily accessed by IT and cybersecurity professionals, then it, too, can be easily accessed by a threat actor. Also, many cyberliability carriers require MFA on administrative functions: this means all functions all the time. Threat actors will use the ease of administrative function access to cause damage—this much is abundantly clear. Further, how much aggravation is the acceptance of an MFA push for an administrative user anyway? We argue very little when weighed against the potential consequences.

- Nearly three-quarters of respondents believed they were more or much more secure than their industry peers. This obviously defies mathematical

Executive Summary & Key Takeaways (cont.)

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. ("Zero Trust" is a security method that trusts no one and nothing by default; Zero Trust assumes that everything is risky until proven otherwise.) Cybercriminals are probing constantly, waiting for any change to open a new line of vulnerability. If an organization relies heavily on the established frameworks to determine their level of trust in their security programs, they have a false sense of security and are following the wrong paradigm. The underlying tech orchestration, of which the frameworks are not specific, is critically important to prevent a breach.

- **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

Executive Summary & Key Takeaways (cont.)

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. Often, the threat actor is depicted as a highly intelligent, devious figure cloaked in sinister mystery. 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. Many threat actors use Ransomware as a Service (RaaS) or Malware as a Service (MaaS) that they did not create; so, after the initial penetration, these more sophisticated actors are engaged and execute much more sophisticated tactics to destroy the service layer, encrypt key data/systems, and exfiltrate data to increase the pressure to pay their ransom demands. They are criminals: they should not be credited with more sophistication than they have nor granted Hollywood-style villain status. The best protection is having a solid, layered defense and backup strategy that can thwart their attempts.

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. In cybersecurity, simple solutions rarely solve holistic problems. Firm IT, with support from leadership, must take a stronger stance to defending systems—assuming users will make

Executive Summary & Key Takeaways (cont.)

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. Many of today's firms expect users not to engage in risky behaviors but enable those behaviors. This would be like an airport TSA checkpoint listing forbidden, hazardous materials, but failing to scan for them, putting the onus of security on the traveler.

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). Thus, users are not only cited as the greatest security concern, but they are also viewed as the biggest blocker of security betterment.

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. Systems are simply not designed to detect and block a threat actor accessing systems from an approved device and user account: systems are open by default.

Executive Summary & Key Takeaways (cont.)

Thus, the tools a firm might purchase for remote control, like Screen Connect, SolarWinds, Manage Engine, Bomgar, etc., can also be used by a threat actor for the same. Risks must be managed from this paradigm: if a user or IT admin can do it, assume that a threat actor can as well.

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. But in 2022, over 100 law firms reported sensitive data breaches to state authorities (according to a report by Law360), up 14% over 2021 and 117% from 2020. The data lost can be material to corporate business and sensitive to clients' personal and financial wellbeing. The incidents themselves can cause significant financial losses, and even business insolvency. To complicate issues for law firms, releasing client confidential information is a violation of the ethical standards to which lawyers have agreed and can result in malpractice and class action lawsuits. In January and February of this year alone, malware groups began specifically targeting law firm employees, attacking some firms with targeted threat campaigns, according to eSentire. Organizing firm defenses against these threats rather than around user convenience is an essential step to mitigating this considerable area of vulnerability. Users must be educated on why these controls are necessary, shifting the paradigm of the law firm security approach away from users and toward stronger controls. We are not arguing that systems should not be usable; however, we are arguing that users must grow accustomed to many behaviors being blocked by default and following an exception process when a specific action is required for business.

So, are users really the problem? Can firms "secure the user" to prevent a breach?

Emphatically, no. The core issue is that systems are open by default, and this configuration must change. Additionally, law firms have not invested in adequate security operation center services and lateral movement/backup defenses to prevent a non-recoverable mass destruction event.

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

Organizations of all sizes and in all industries have many forces pressing them to improve their security defenses. While risk is clearly one factor, others like regulatory requirements, customer or client needs, industry pressures, and even pending acquisitions can each play a role in how and when they fortify their security. 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

Executive Summary & Key Takeaways (cont.)

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, and then we will discuss why their leadership over firm security is a concern. 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% has 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. Often, the same organizations to which the law firm is complying find themselves in embarrassing breaches: why? They, too, have compliance, regulatory, and governance-focused security programs and largely disregarding the real risk: tech orchestration. 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. Compliance does not equal security. A firm could perfectly track and follow OCGs and still find itself in an embarrassing breach.

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

In a digital world, organizations of all types live and die by their data. For law firms, this holds especially true: 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.

Let's be clear by what we mean by "immutable" (to avoid that pesky definitional problem). This means that data in storage is incapable of being changed, encrypted, or deleted. The only way it should be

Executive Summary & Key Takeaways (cont.)

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, 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.

Executive Summary & Key Takeaways (cont.)

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. As noted previously, maybe only those with more certainty in their security program replied to the survey; however, this does not seem to hold true considering other critically lacking security controls among the survey population mentioned within this study. It is also doubtful that this quarter of respondents translates to the larger law firm population, because stacking controls in this manner, as recommended by Conversant, is often contrary to traditional IT paradigms and many vendors' recommendations.

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. Always assume that an attacker can penetrate the firm's publicly accessible systems, including SaaS applications, even with MFA in place. 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: we are intimately familiar with the many challenges law firms face in staffing, resources, and time dedicated to security. Many firms are making an effort to employ many of the right tactics, techniques, and procedures that are components of a strong security program. But we still see more of a focus on compliance than the controls and configurations that threat actors target, a lack of true understanding of the enemy as well as their determination to find ways to penetrate the organization. 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.

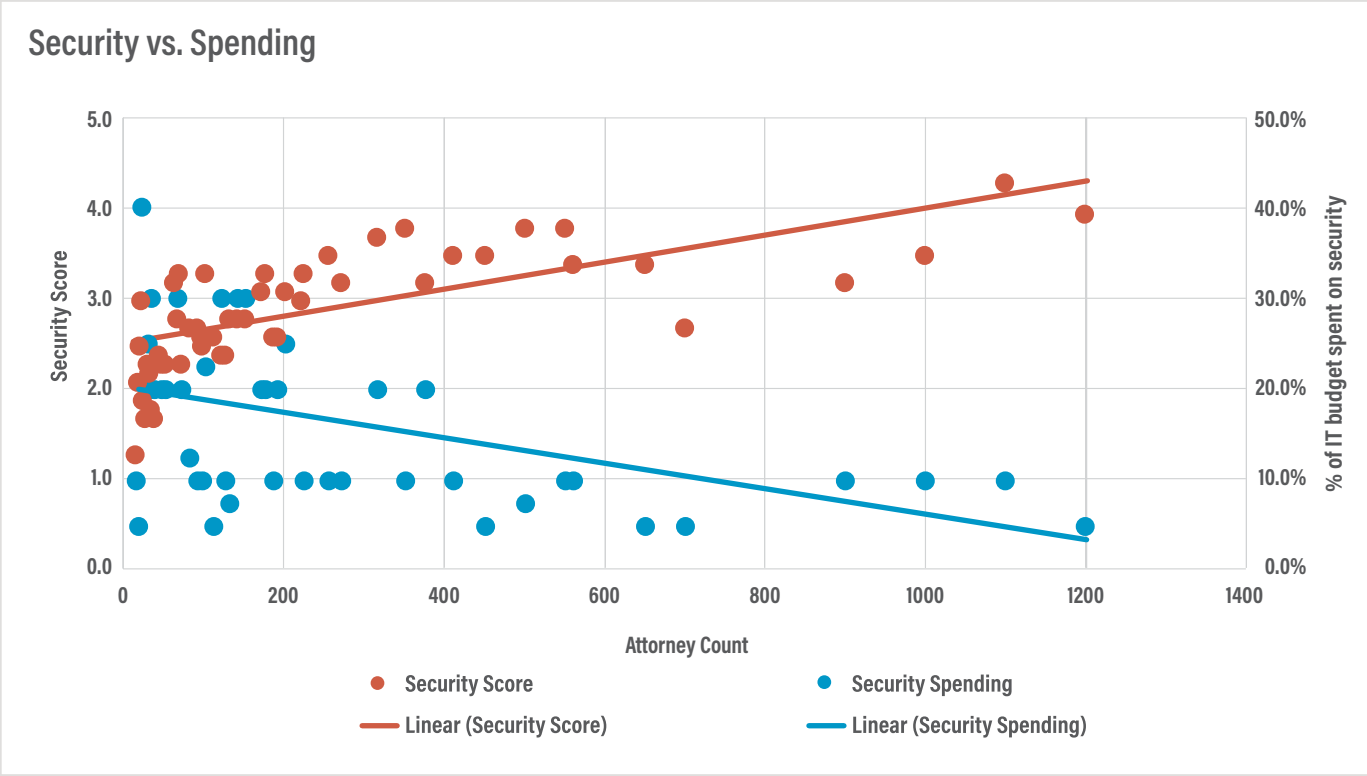
Is Bigger Better? How Small and Large Firms Compare*

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.

Executive Summary & Key Takeaways (cont.)

The chart below uses a scoring system applied to all quantitative answers of the survey to produce a security score of one through five for every respondent. One indicates less security; five indicates more. These scores are not indicative of a firm's overall security in the wild but are intended as a simple metric to provide comparisons within the data sample. The more security controls a firm has in place, the higher the security score.

The chart compares security spending (blue) as a percentage of IT budget to the calculated security score (orange) and clearly shows a divergence as firms scale up. Larger firms spend significantly less of their budget on security but have significantly more controls in place.

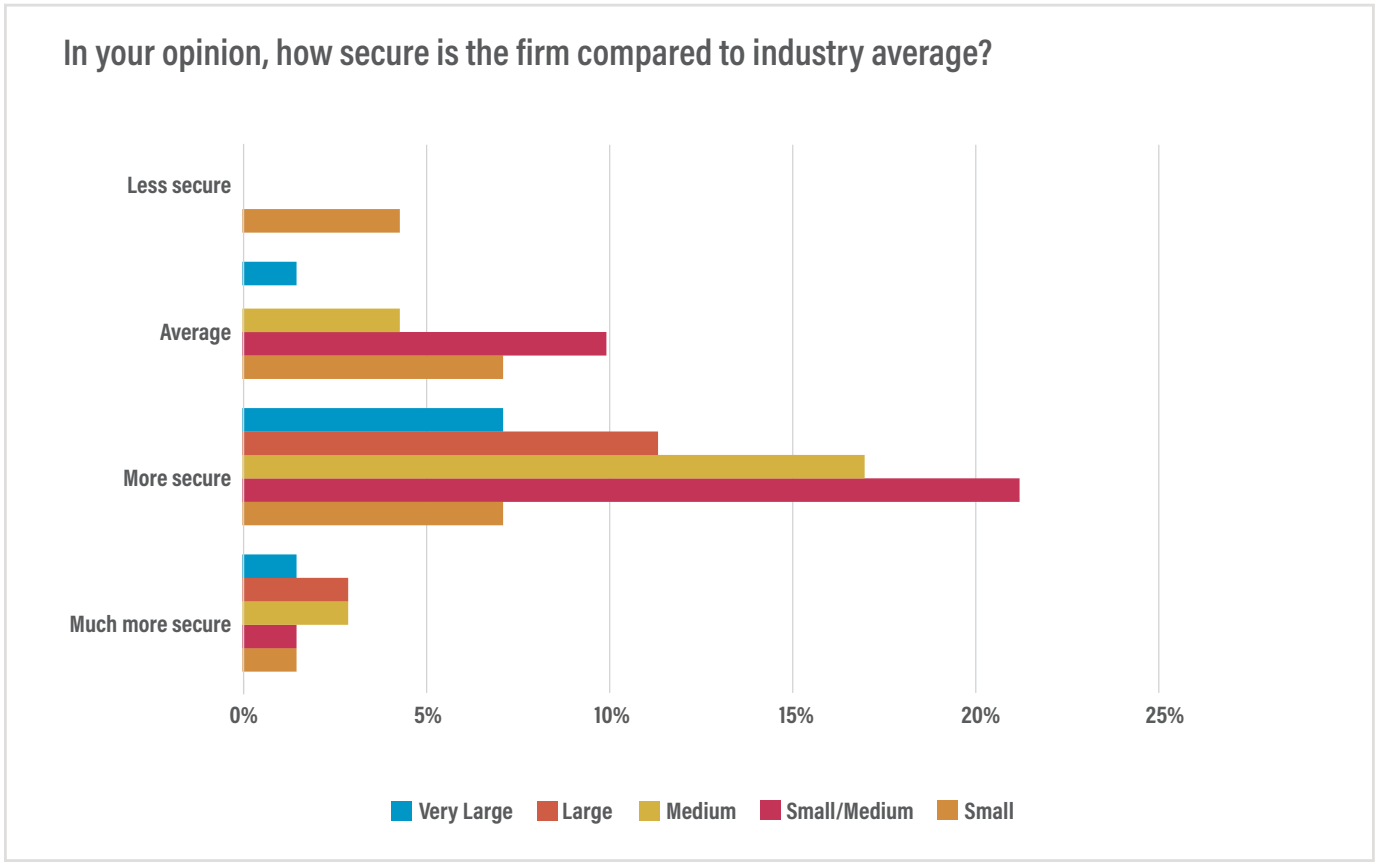


* For a breakdown of firm size categorization by attorney count, see the "Methodology" section to follow.

Executive Summary & Key Takeaways (cont.)

Larger firms may have made upfront investments in past years or may spend their budgets more wisely through a targeted, formalized approach involving assessments and prioritization. Larger firms may also simply have fleshier IT budgets overall. In our experience, one obvious conclusion is there is a basic set of controls that all firms must purchase to achieve base-level security. For the larger firm, those costs are spread across a larger set of users and overall larger revenue. Smaller firms are making new investments spread across fewer users, requiring them to spend a larger percentage of their IT budgets to secure the organization.

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:



Executive Summary & Key Takeaways (cont.)

By their own perspectives, smaller firms believe they are less secure, and confidence increases with organization size:

Very large firms may understand that their larger estate of controls and more expansive threat surfaces are harder to rein in, providing a bit more realism to their self-assessment.

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. However, generally, firms of all sizes were underperforming in conducting this essential task, and likely all have not operationalized the risk register in the context of Zero Trust.
  - Larger firms are more likely to have a **formalized change management process**, with a change review board involved in

Executive Summary & Key Takeaways (cont.)

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).

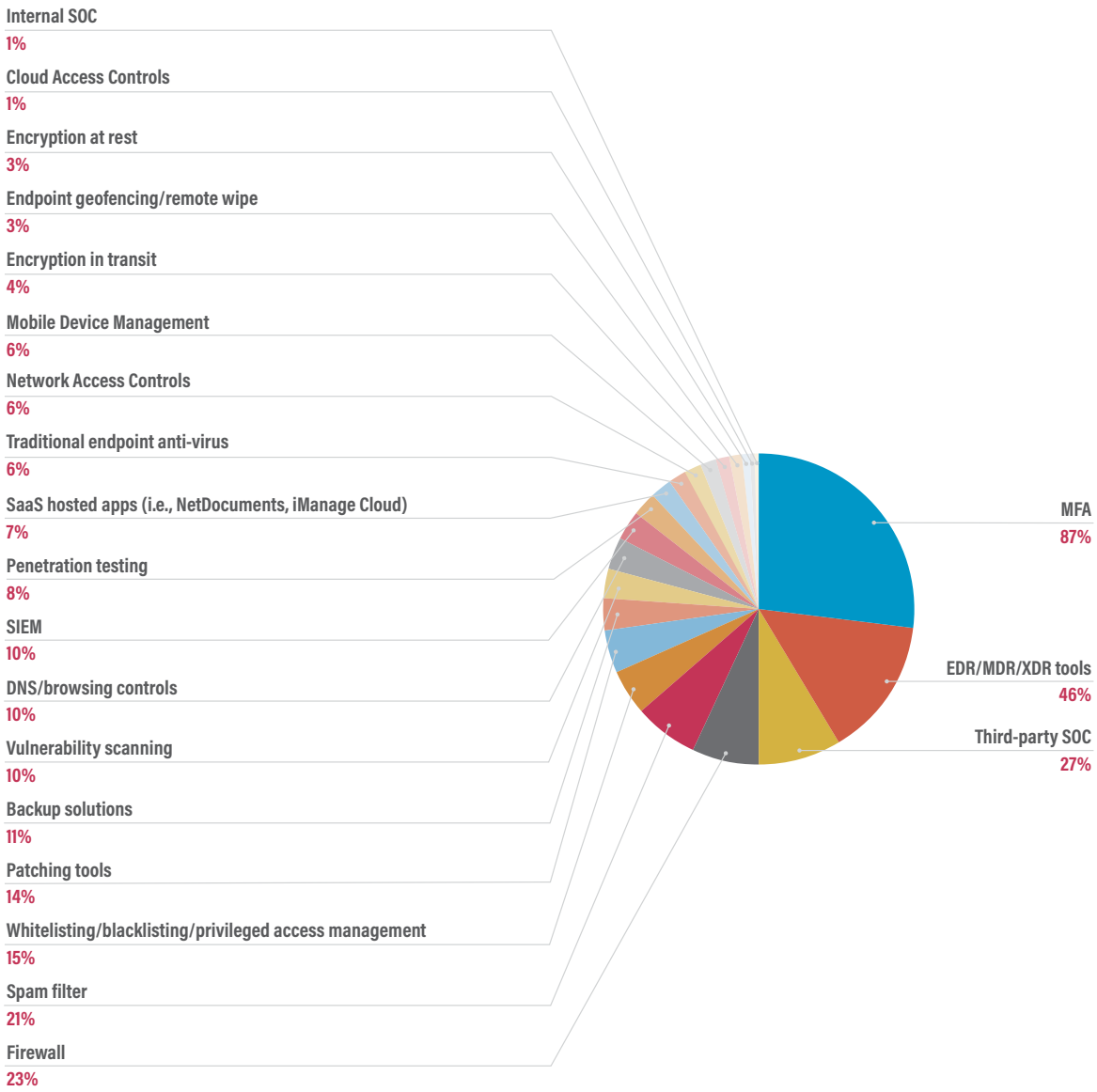
Thus, the data reflects that apparent security maturity increases with firm size. We see consistently across the data set that larger firms have more formalized programs and are employing more rigorous practices than their smaller peers.

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% we assess do not comply with their own stated policies and procedures, once examined down to the technical controls and configurations level. For example, many firms maintain a policy that states their backups must be immutable; yet publicly available data shows backups are affected 68% of the time in ransomware attacks.

Executive Summary & Key Takeaways (cont.)

Below are results of what respondents believe their "Top Security Controls" are; yet we believe firms still have gaps:

Top Security Controls



Executive Summary & Key Takeaways (cont.)

- 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%.

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.

Methodology

In 2022, ILTA and Conversant Group collaborated to conduct the first ever cybersecurity-focused benchmarking survey for the legal industry. The survey was targeted specifically at understanding cybersecurity controls, tools, practices, and assumptions in law firms. The questions were crafted to uncover the true cybersecurity risks present in law firms and to reveal their ability to prevent a breach.

A total of 71 firms responded to this very in-depth survey, lending their very intimate understanding of the challenges inherent in securing the nuanced legal environment. Over 550 responded to ILTA's Technology Survey (which included a security sub-section), and where appropriate, we aggregated or supported data points across surveys to provide a more holistic view. While the sample sizes of the cybersecurity survey were limited and responses were self-reported, the audience included highly targeted professionals representing 19,144 attorneys and about 38,290 users; these technical professionals are keenly familiar with legal IT environments and the esoteric challenges in defending the threats specific to the legal sector. Typically reticent to share information on their IT environments and security controls, this report represents a unique opportunity to glean insight into the security stance of today's law firms.

For this survey report, respondents were aggregated based on firm size: small firms are defined as employing fewer than 50 lawyers; small to medium: 50-149 lawyers; medium: 150-349 lawyers; large: 350-699 lawyers; and very large firms are defined as employing 700 or more lawyers.

We also draw data (where applicable) from ILTA's 2022 Technology survey, a separate study that explored the full range of technologies used in law firms. As the technology study had a subsection dedicated to security practices, the data therein is used where applicable to elucidate on, support, or elaborate on findings of our cybersecurity focused survey.

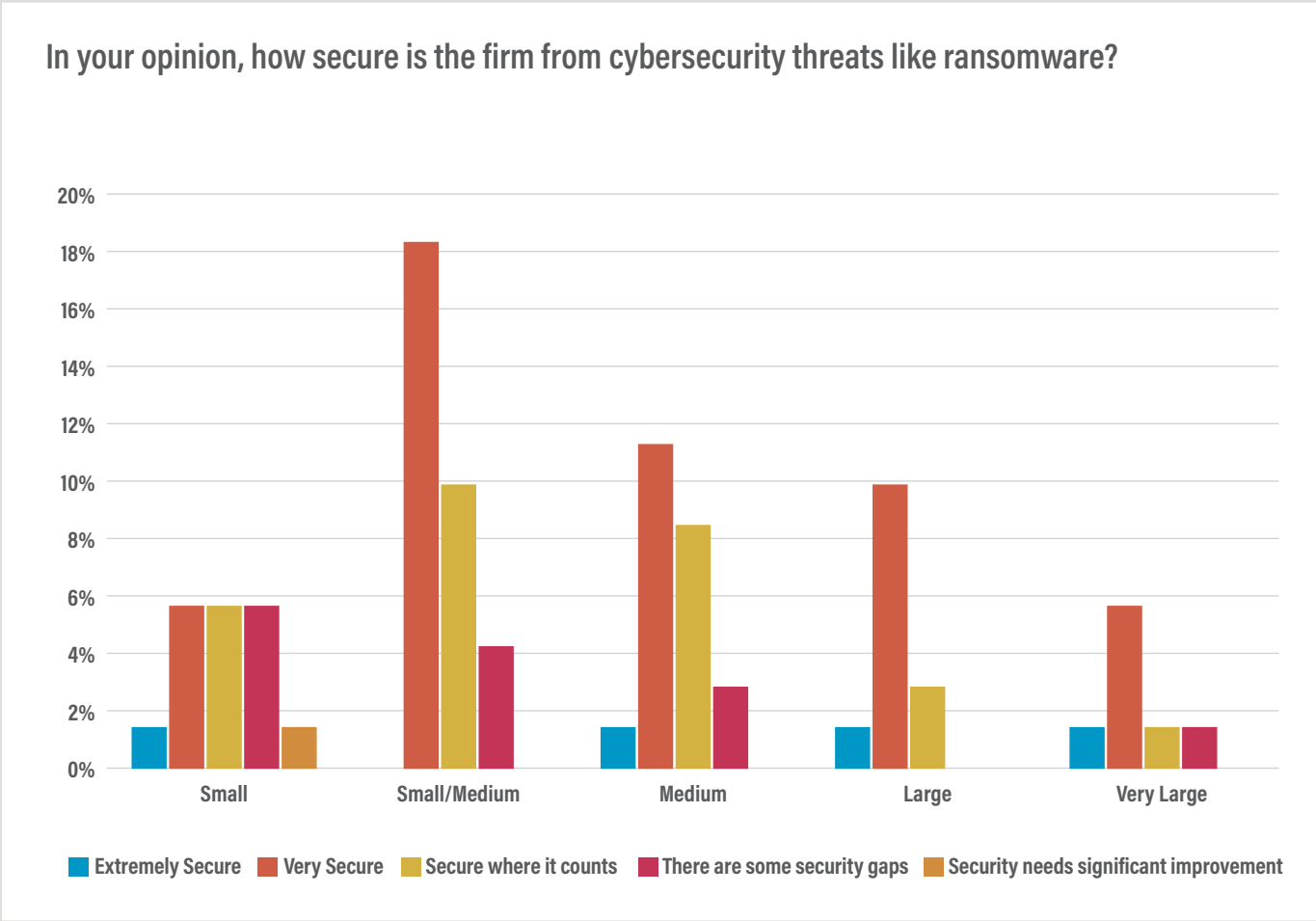
The purpose of this report is to both present those data findings and offer Conversant Group's expert interpretation of those results: where these firm's true vulnerabilities lie (despite assumptions made) and how they can "shift the paradigm" of their security perspectives and approaches to better understand and defend their environments in a prioritized manner, even when staffing and budgets are limited.

Many myths still abound around cybersecurity; we will endeavor to unwind these myths herein. We hope you find this report illuminating.

Data Findings

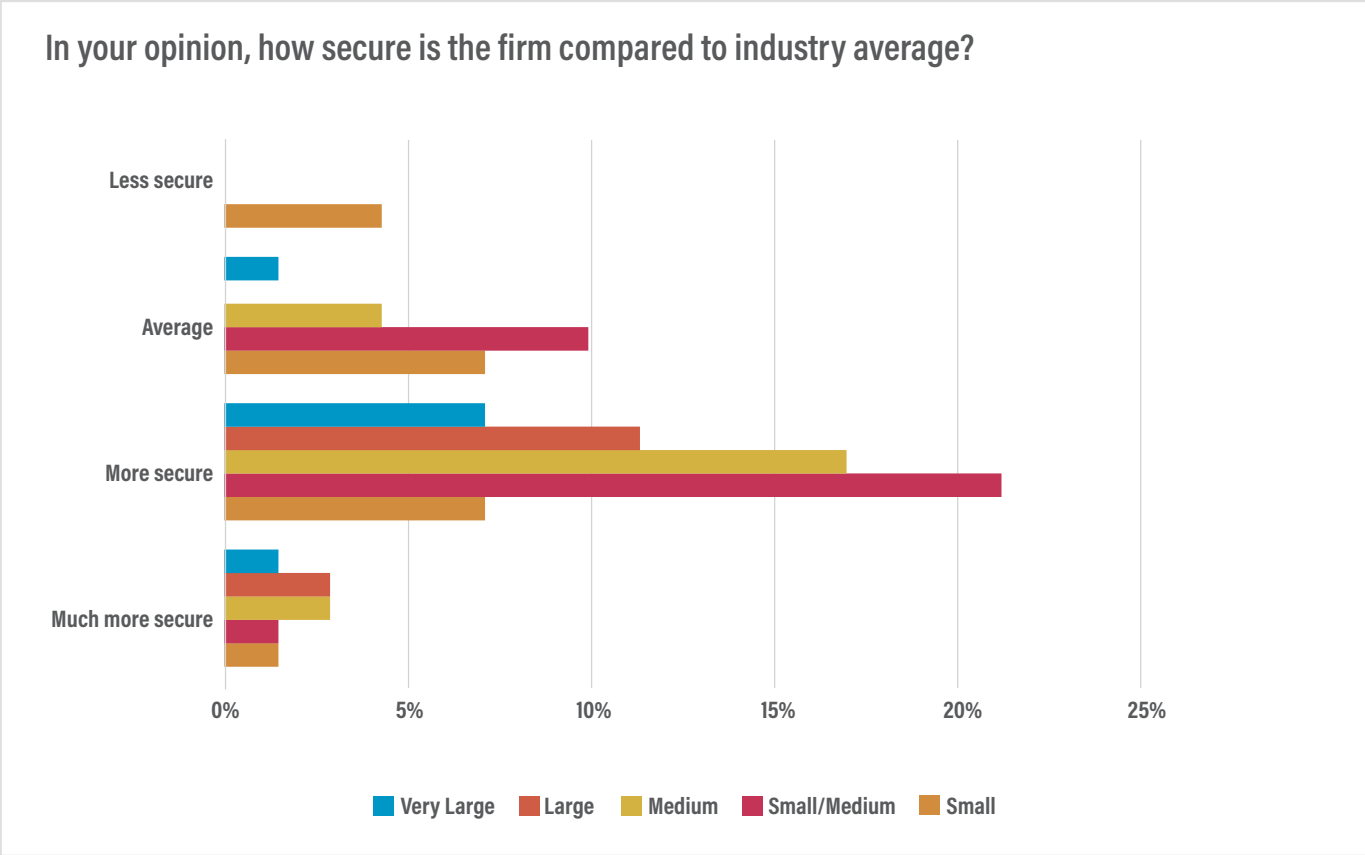
Below are results of the 2022 Conversant Group Cybersecurity Survey of Law Firms, with a top takeaway of the data finding.

Security Perspectives



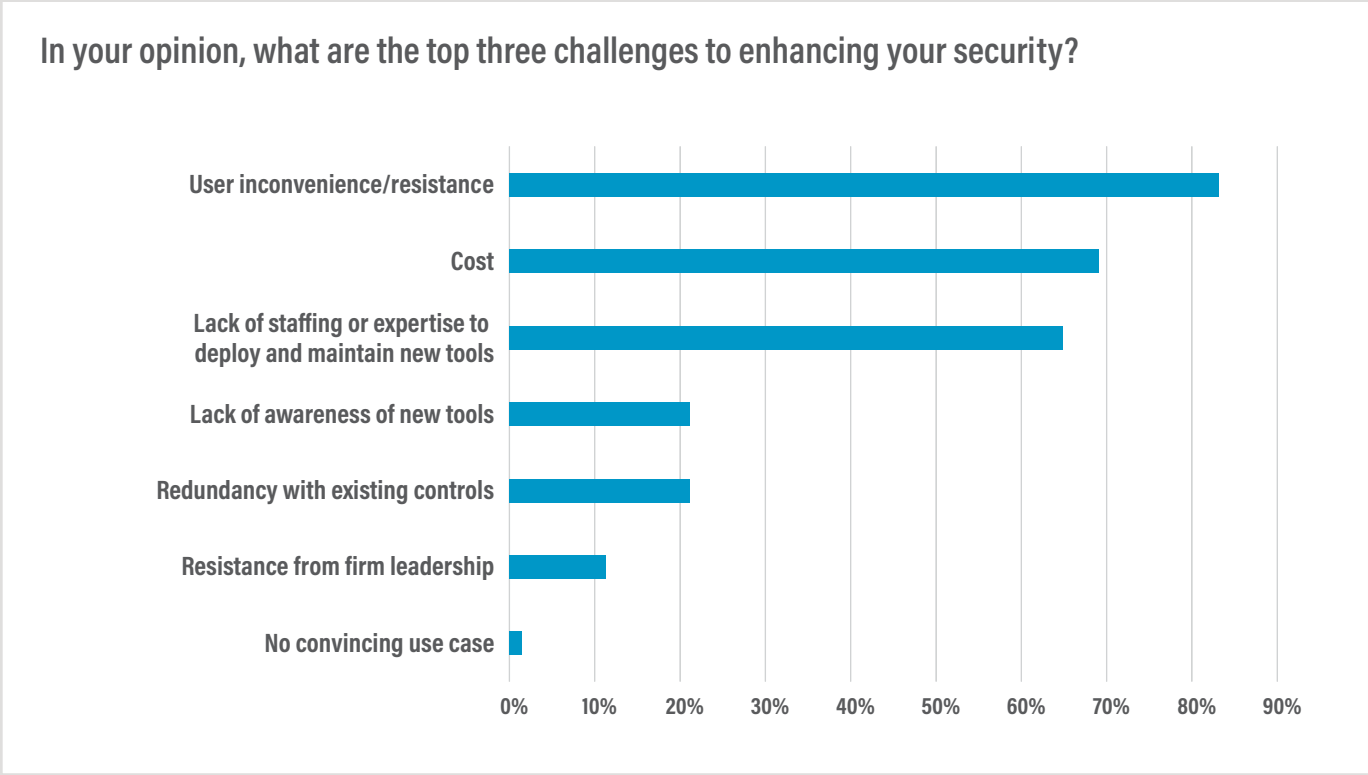
Over half of respondents (50.7%) believed they were very secure.

Data Findings (cont.)



Nearly three-quarters (73%) believed they were either more or much more secure than their industry peers.

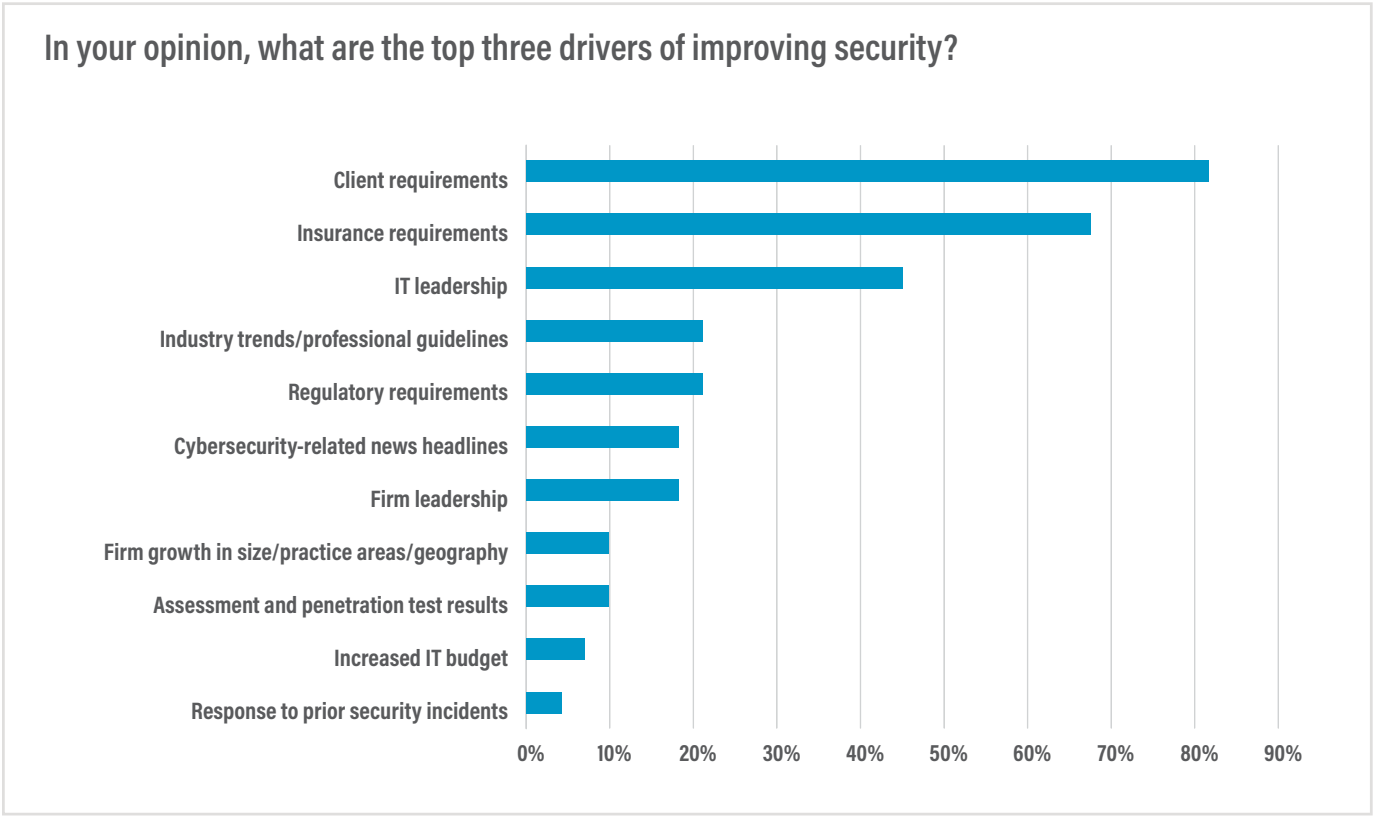
Data Findings (cont.)



Concerns over inconveniencing users and their resistance to change are perceived as the greatest challenge to implementing more rigorous security controls (followed by costs).

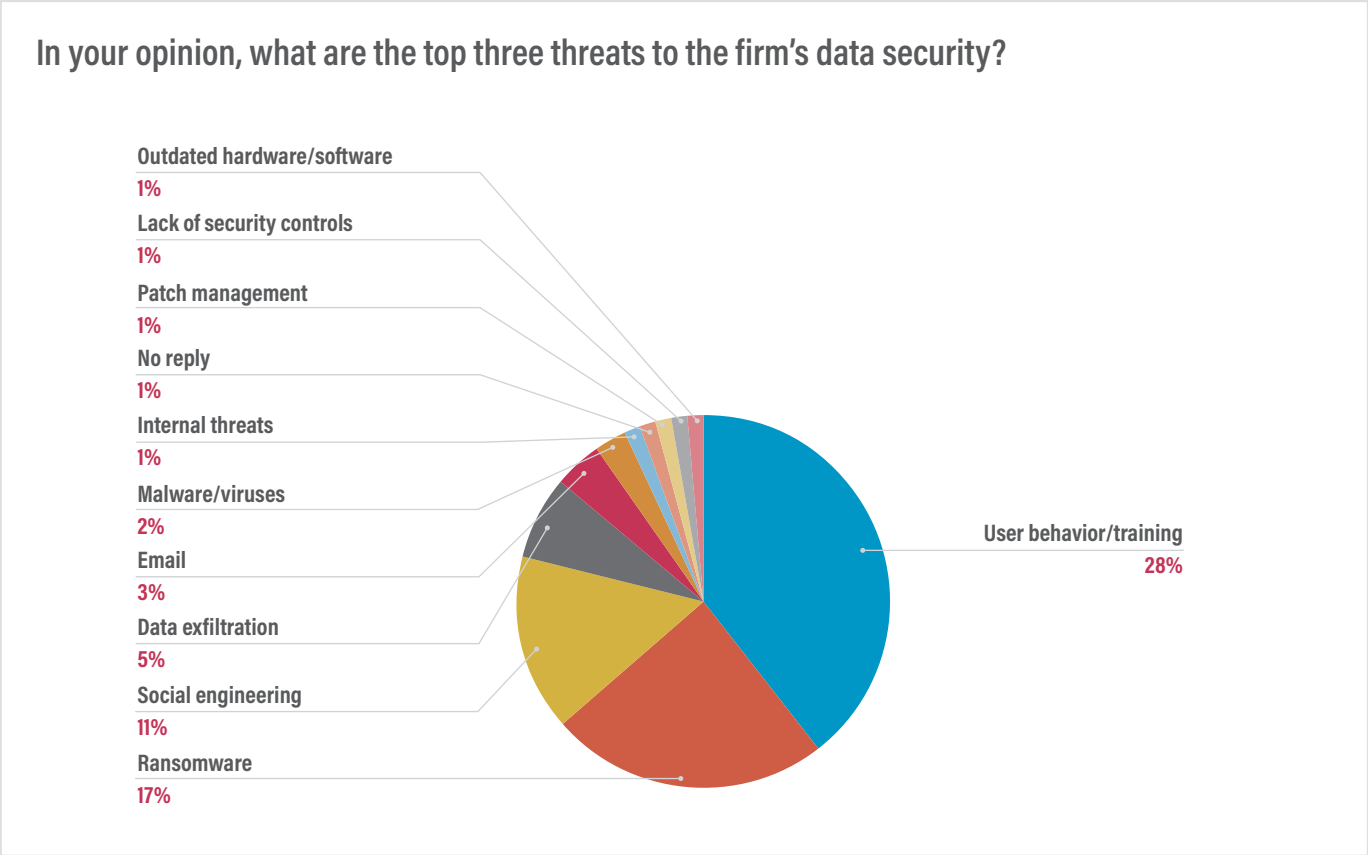
This finding was echoed by results in the 2022 ILTA technology survey, which found that 40% of respondents said user behavior is their greatest challenge.

Data Findings (cont.)



Firm security evolution is primarily driven by their clients' requirements and insurance carriers; IT and firm leadership are not the primary drivers of change.

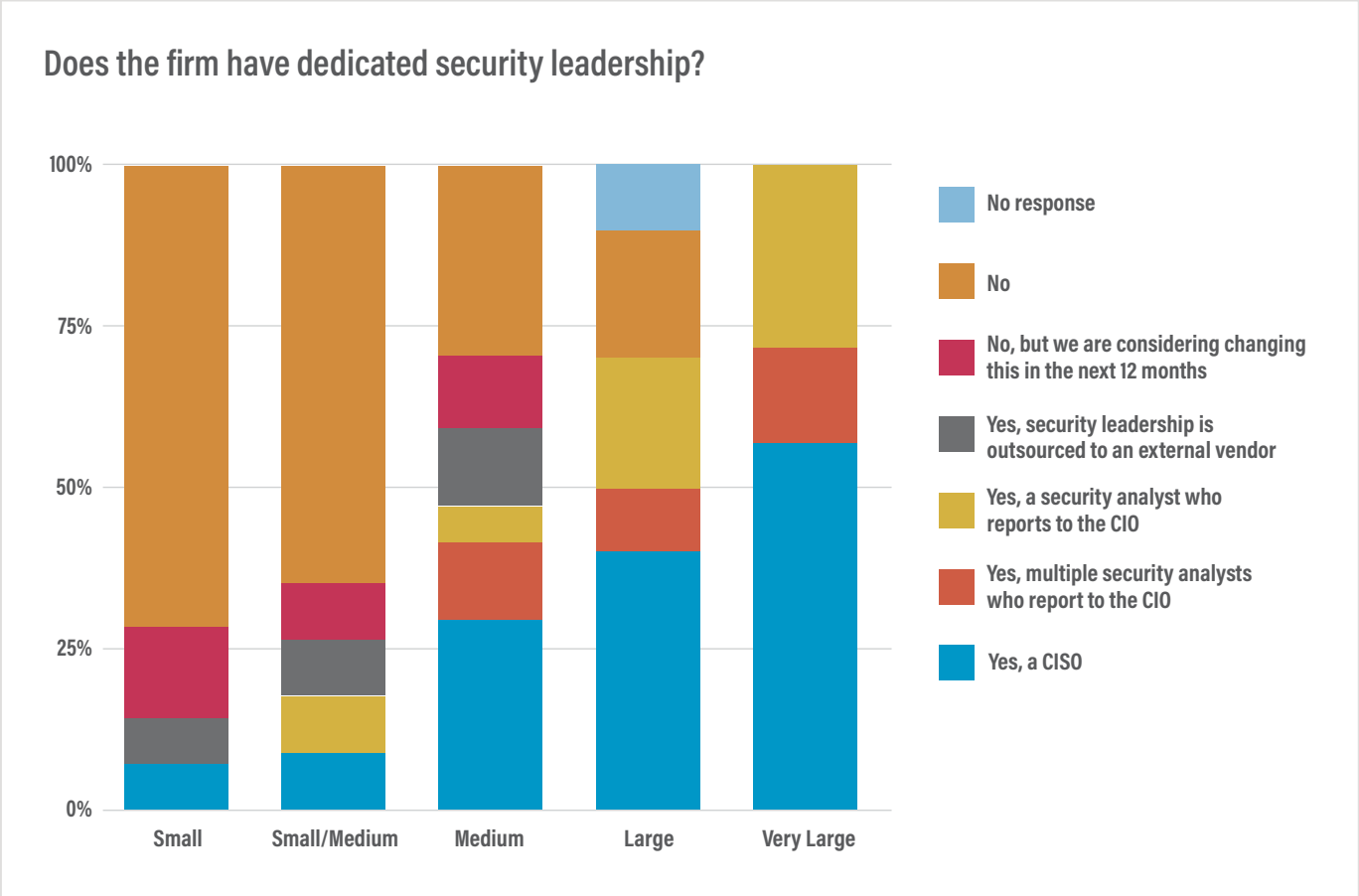
Data Findings (cont.)



User behavior arises as the greatest security concern among those surveyed, above any one threat actor tactic or vulnerability. Respondents are primarily concerned about user behavior and training (or lack thereof), and when coupled with social engineering fears, we see a primary focus on the security risk users introduce into the firm.

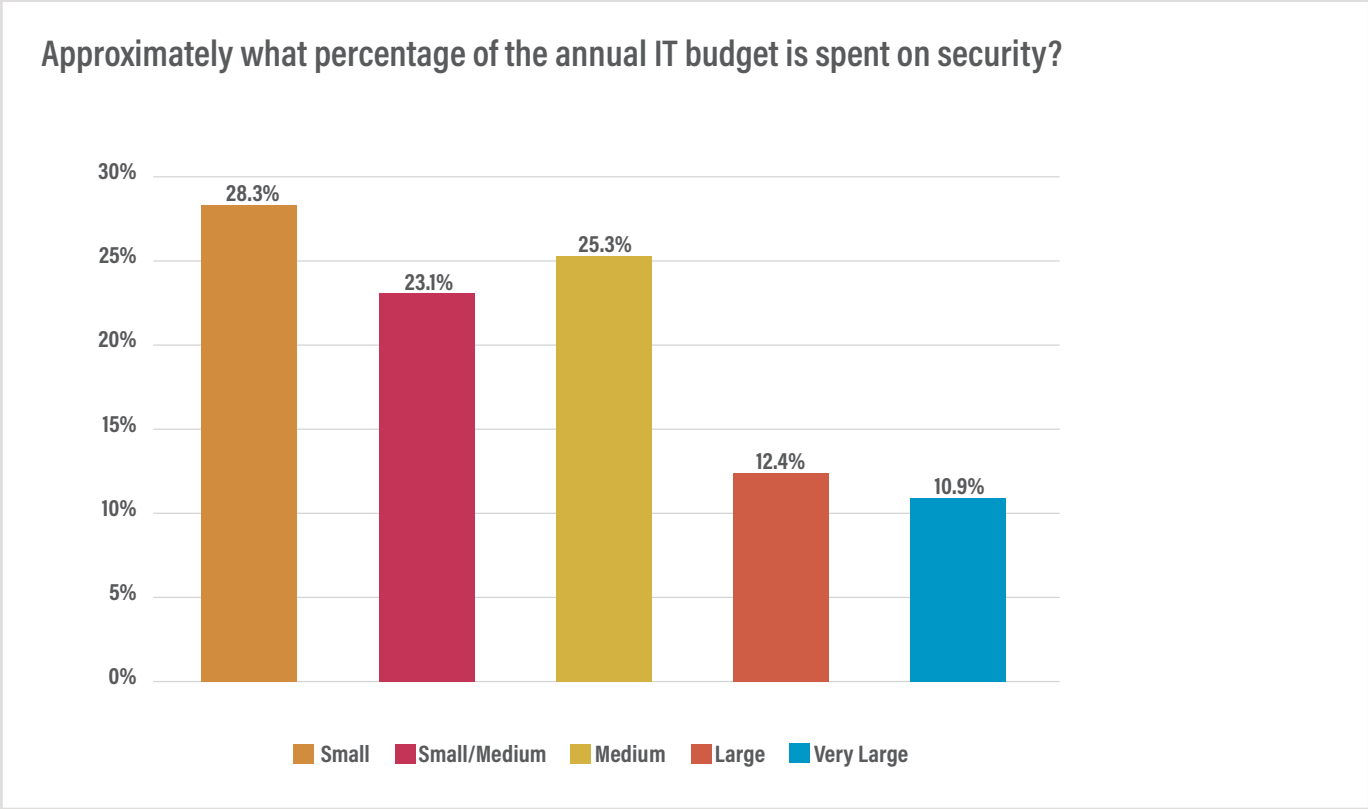
Data Findings (cont.)

Leadership & Resources



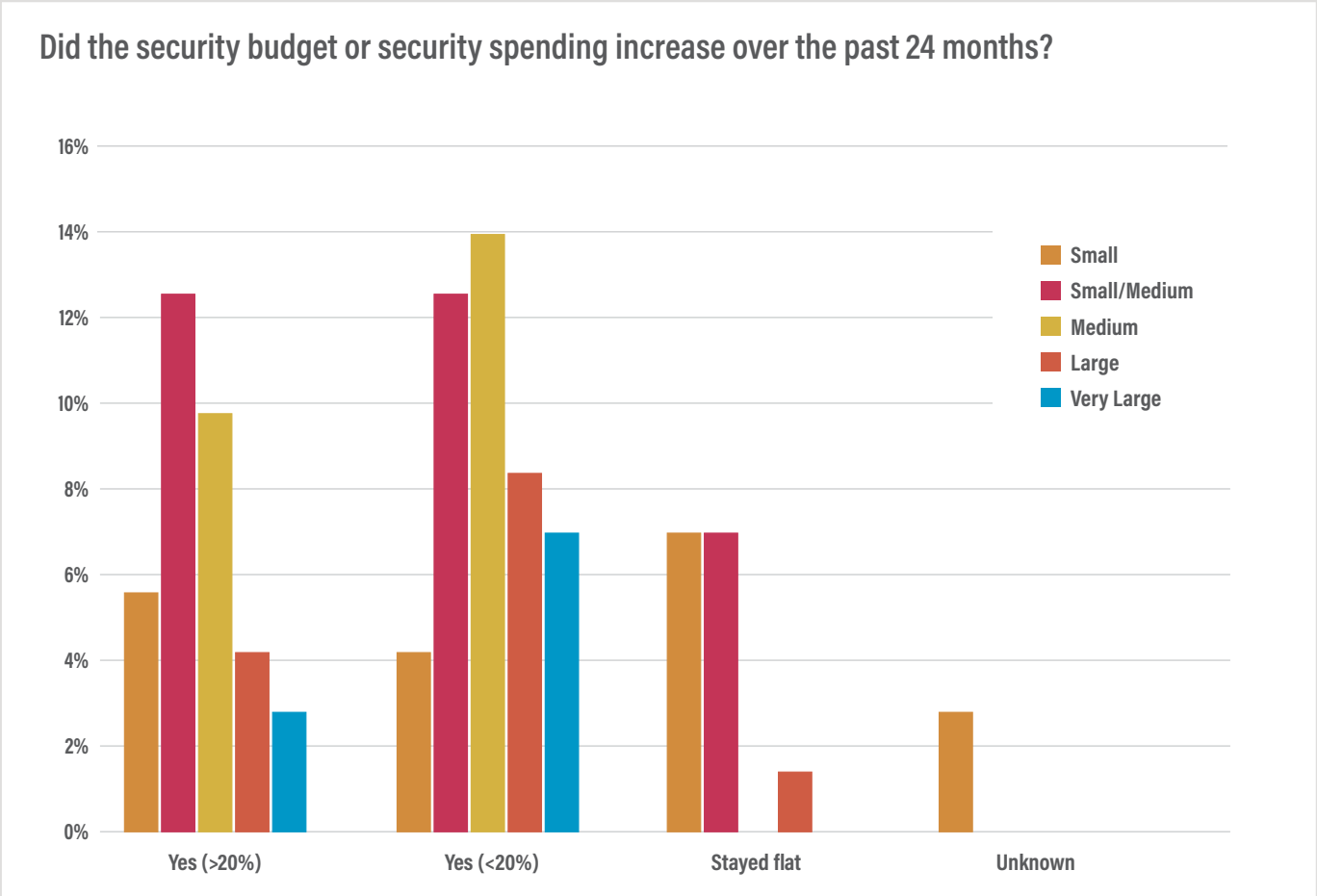
Nearly half of respondents (45.1%) indicated that their firm has no one individual responsible for leading security efforts, while 22.5% have an appointed CISO. Our findings show that dedicated leadership is far more likely in larger organizations (below).

Data Findings (cont.)



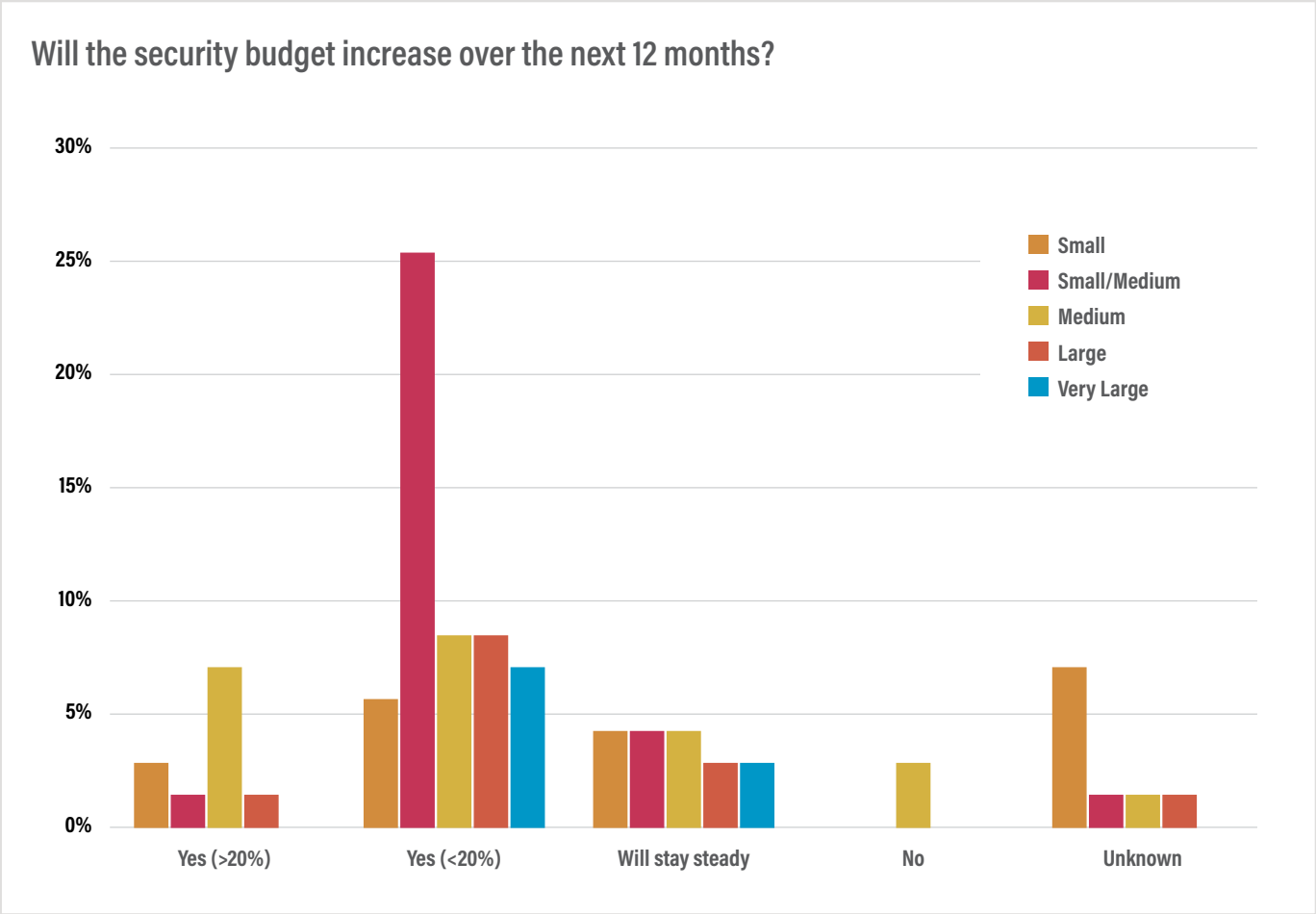
Security spend as a percentage of IT budget is roughly inversely proportional to firm size.

Data Findings (cont.)



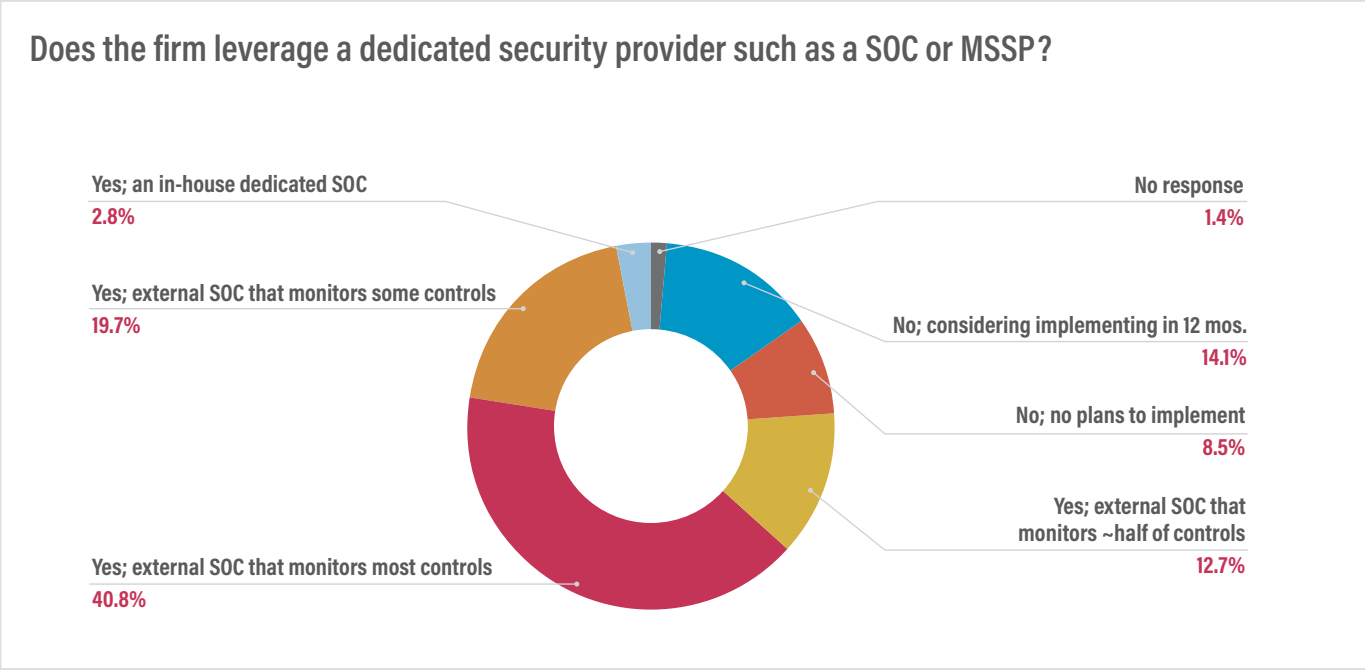
The majority of respondents saw budget increases of less than 20% over the past 24 months.

Data Findings (cont.)



Most firms in our study will see security budget increases of less than 20%.

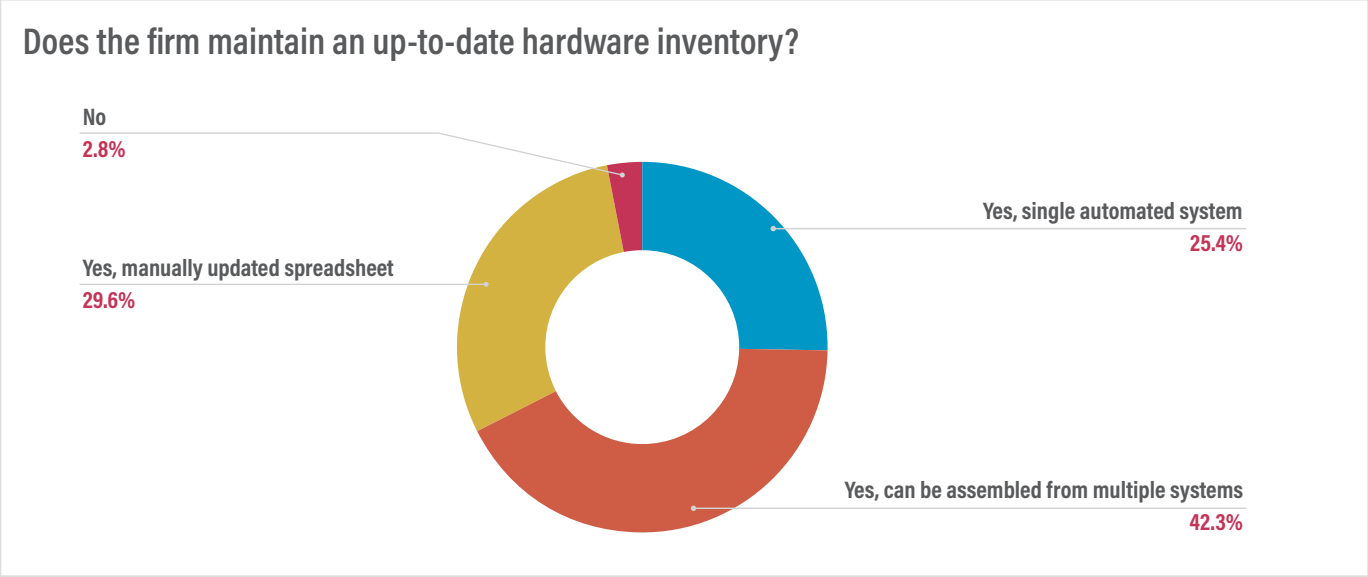
Data Findings (cont.)



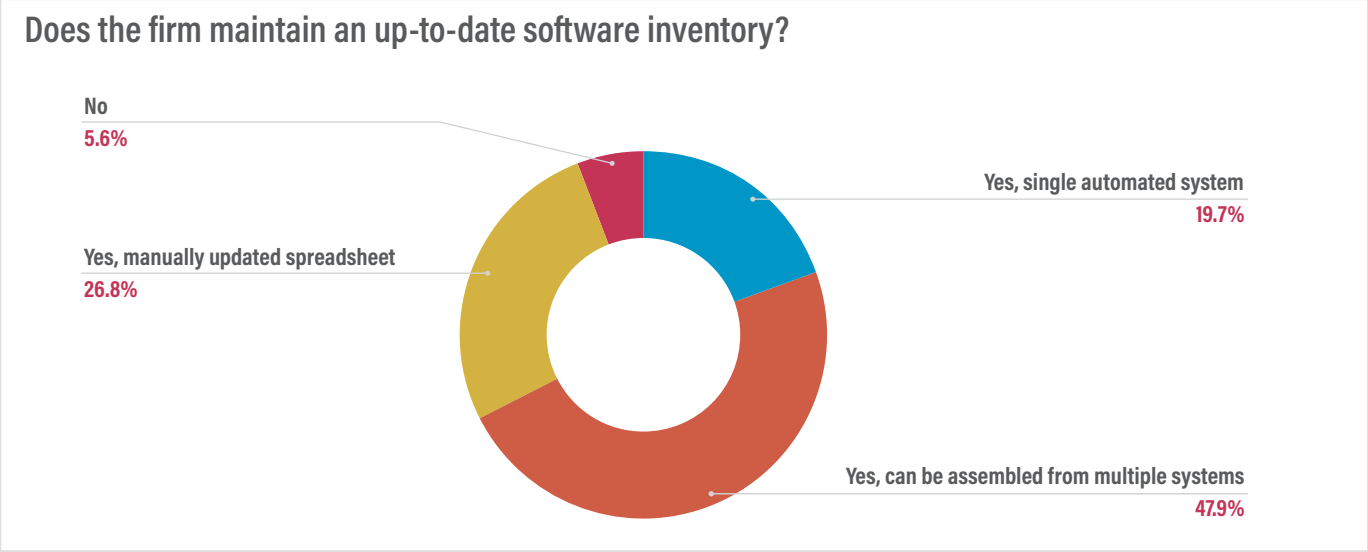
While almost three-quarters of firms in the study (73.2%) leverage an external SOC to manage some to all their security controls, the rest are going it alone, either with an internal SOC or with no assistance. However, 14% are considering implementing a dedicated security provider in the next 12 months.

Data Findings (cont.)

Documentation, Policies & Process

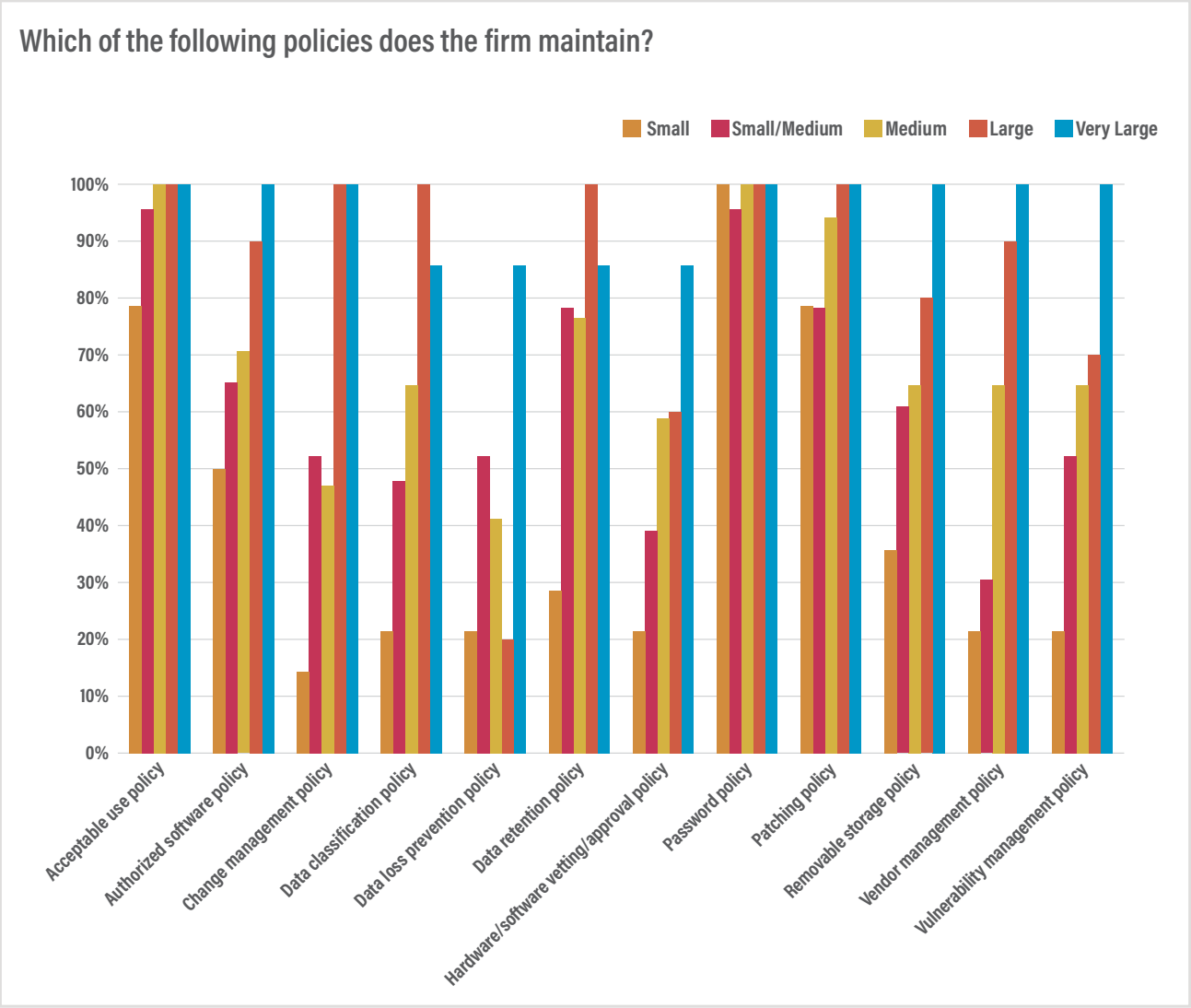


Over a third of firms (29.6%) track their hardware inventories manually on a spreadsheet, or not at all.



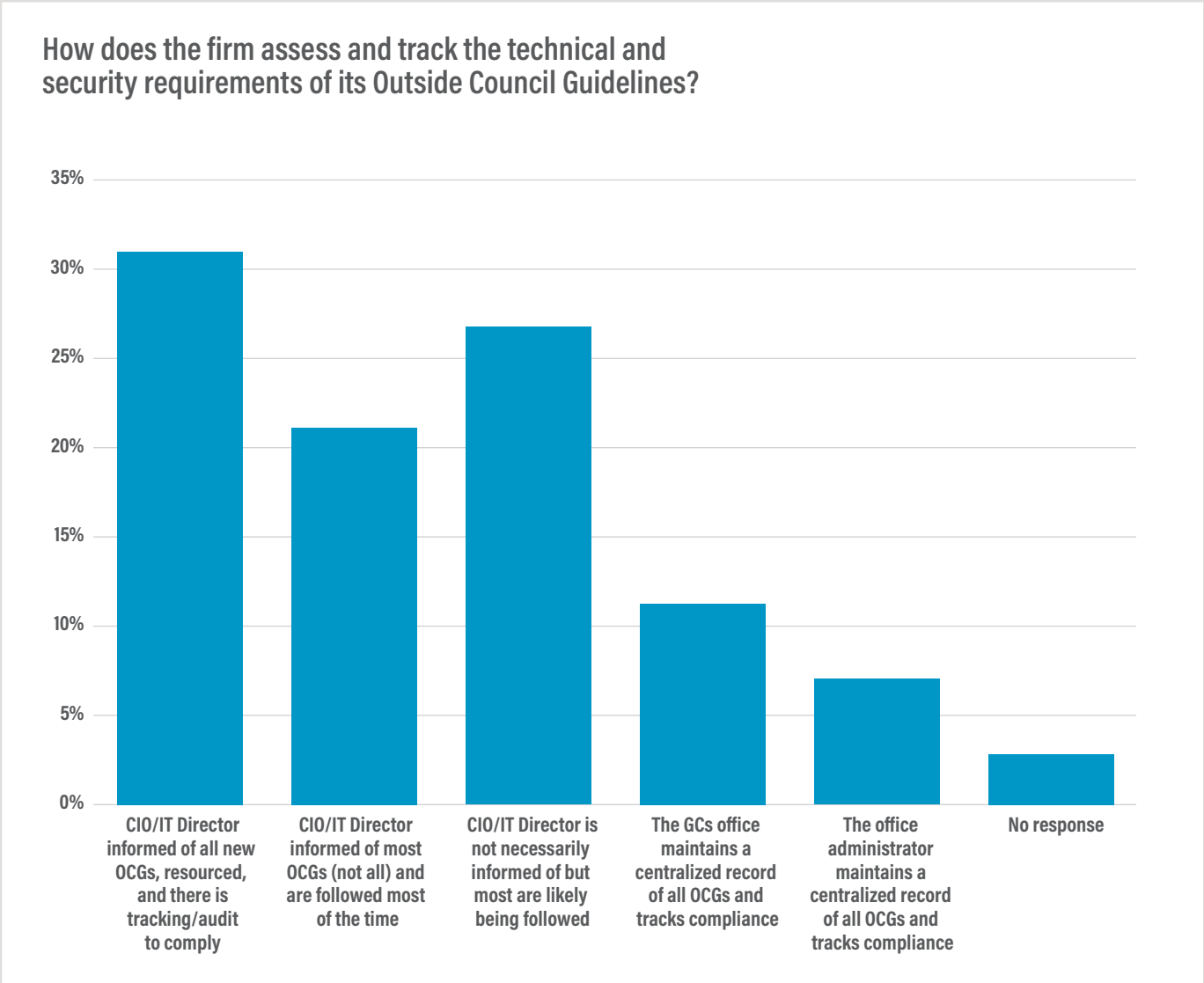
Only 20% of firms use a single, automated software inventory; the rest either assemble inventory from multiple systems or perform inventory manually on a spreadsheet.

Data Findings (cont.)



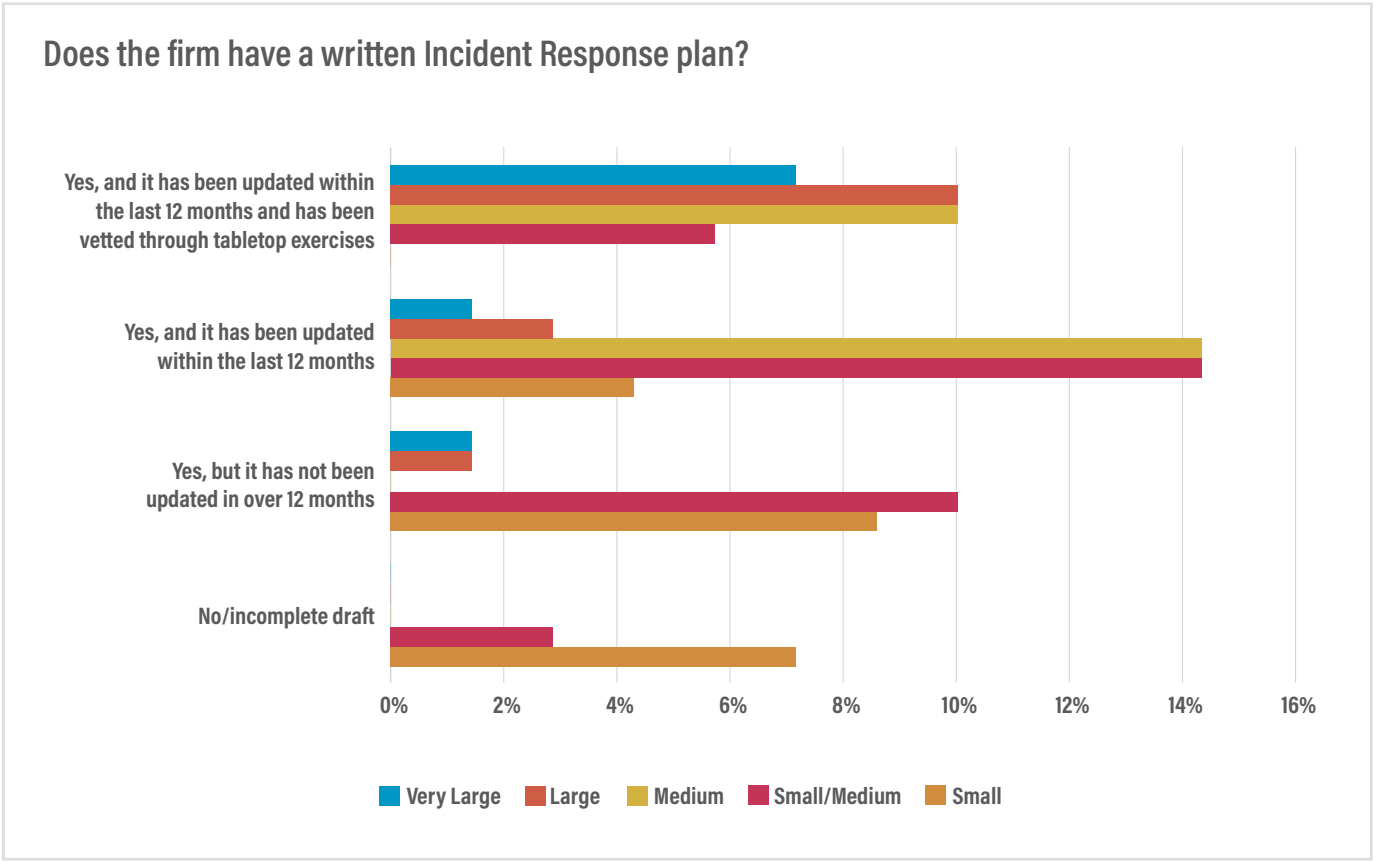
Large and very large firms report much more complete policy suites than their smaller peers.

Data Findings (cont.)



Over 50% of IT leaders are aware of OCGs and follow them most of the time, while nearly one-third (27%) are uninformed about them.

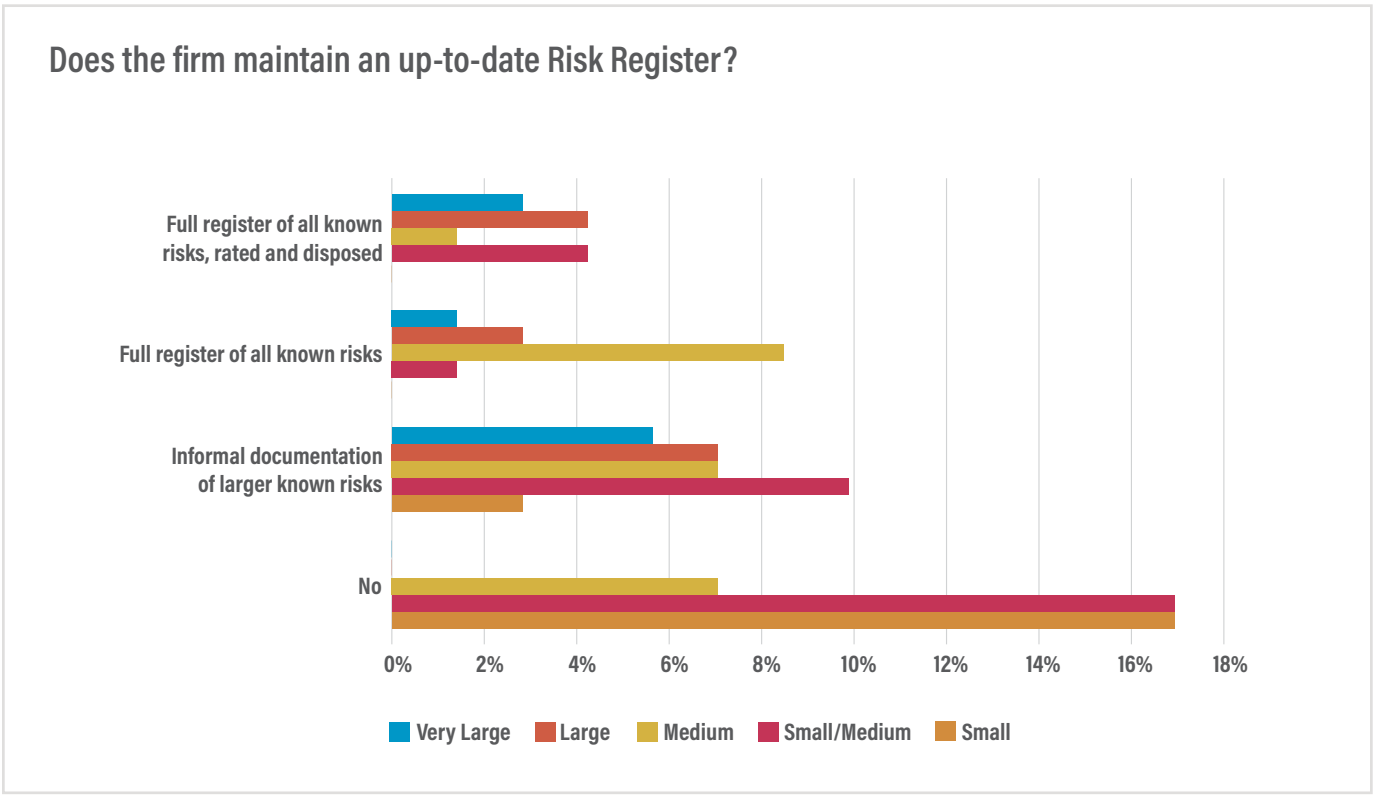
Data Findings (cont.)



All very large firms reported having an IRP, the majority of which had been updated within the past year and vetted through tabletop exercises. On the other end of the spectrum, small firms reported either having no completed IRP or an outdated one. In the middle, medium-sized firms reported having up-to-date IRPs, many of which were tested via exercises.

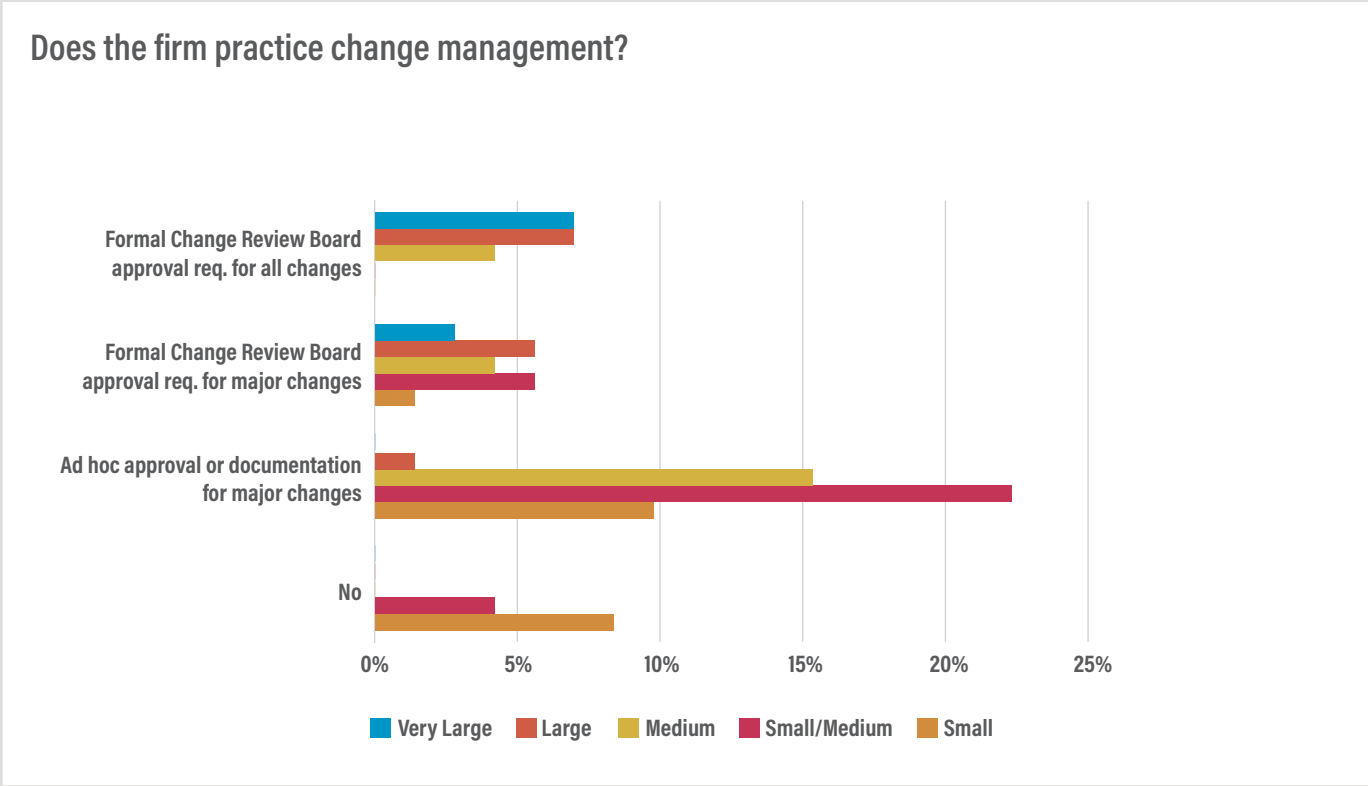
We see that medium-sized firms are less prepared to recover and restore. While most medium-sized firms had current IRPs, nearly half (47%) had no or an out-of-date DR/BC plan.

Data Findings (cont.)



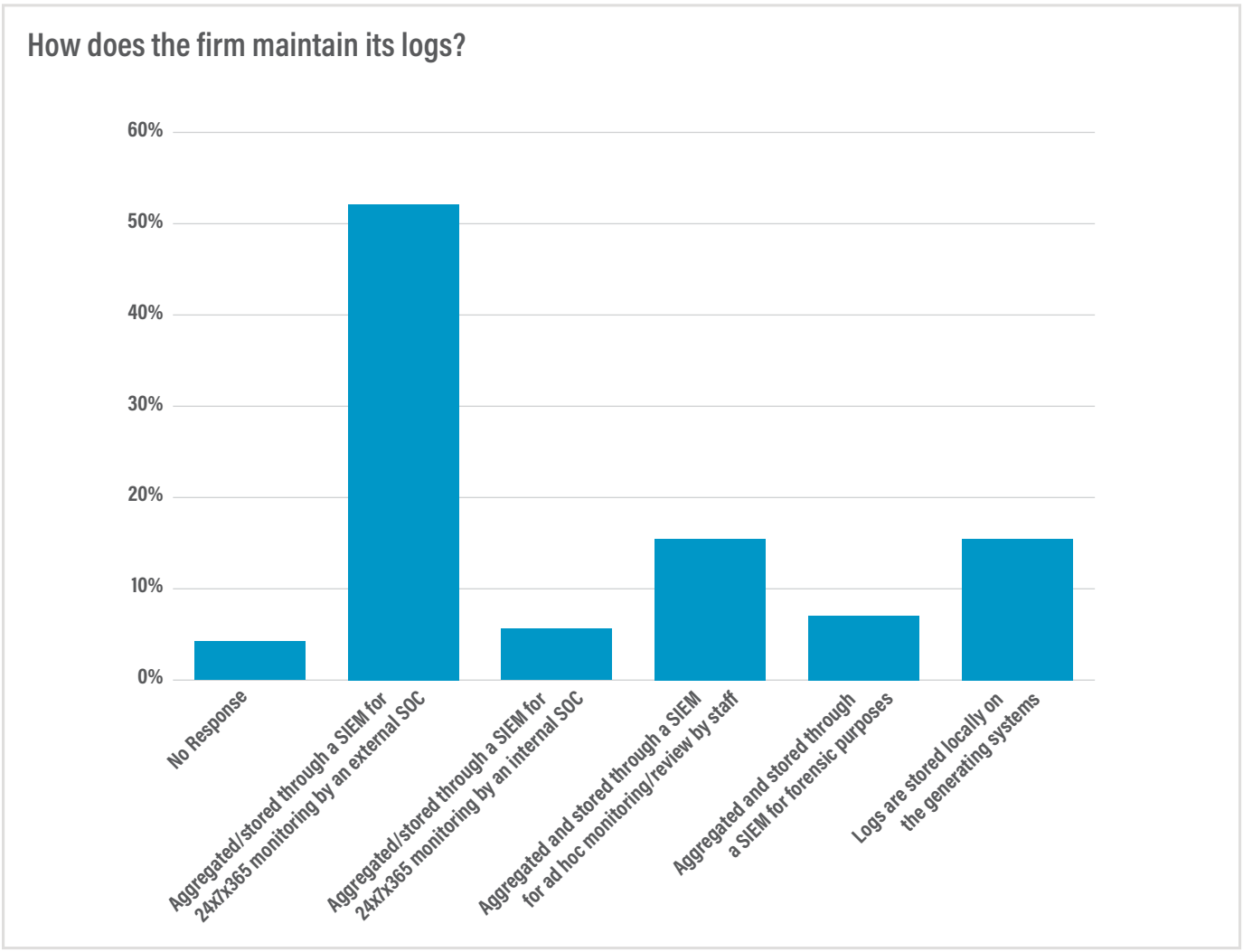
On average, organizations of all sizes are failing to practice formalized risk register processes.

Data Findings (cont.)



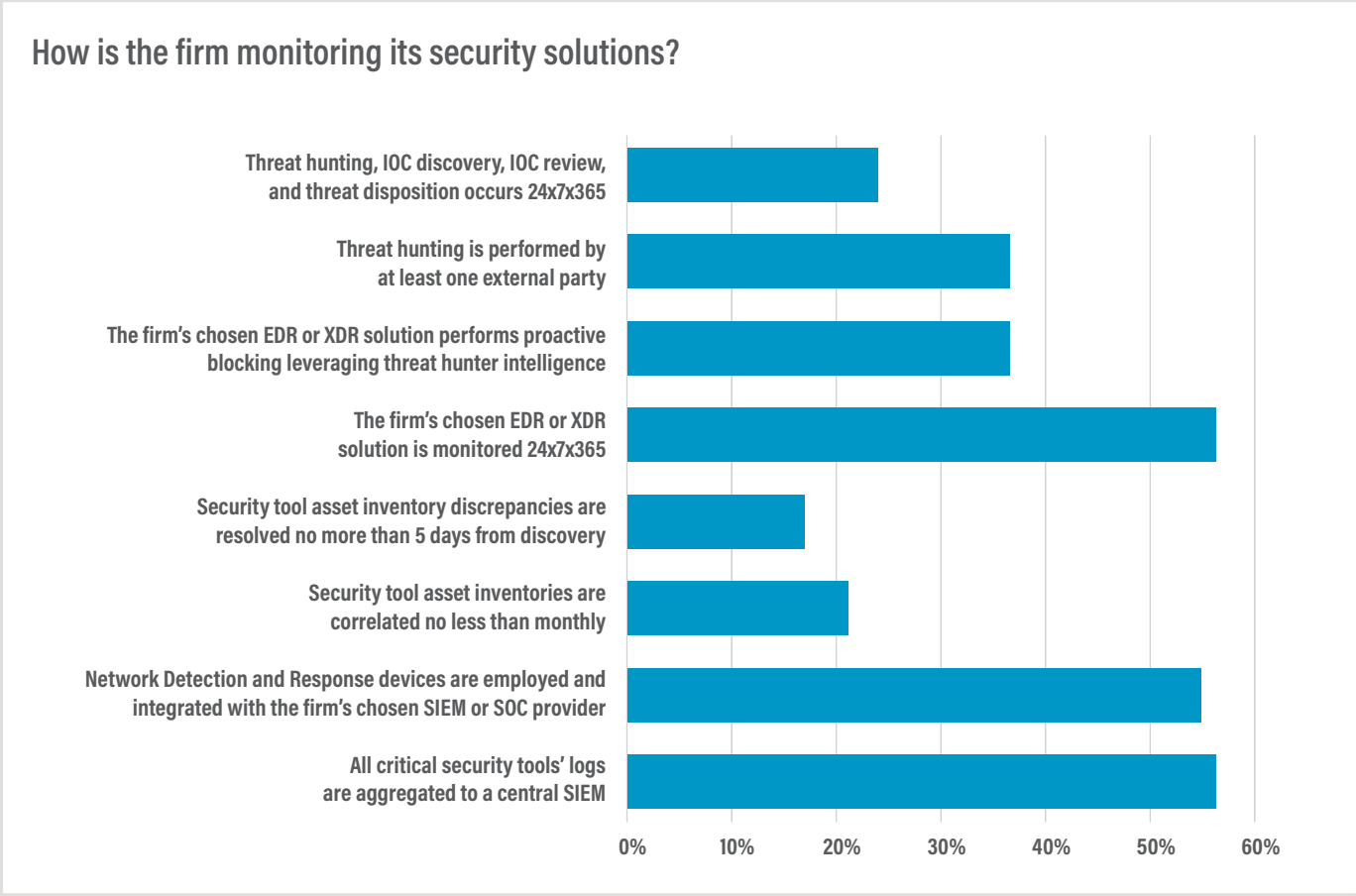
Formality of change management seems to be directly correlated with organization size: the vast majority of small, SMB, and mid-sized businesses (93%, 82%, and 64%, respectively) have no or ad hoc change management processes, whereas the vast majority of large to very large organizations have some form of a formal change management program.

Data Findings (cont.)



Most firms leverage an external SOC for log management.

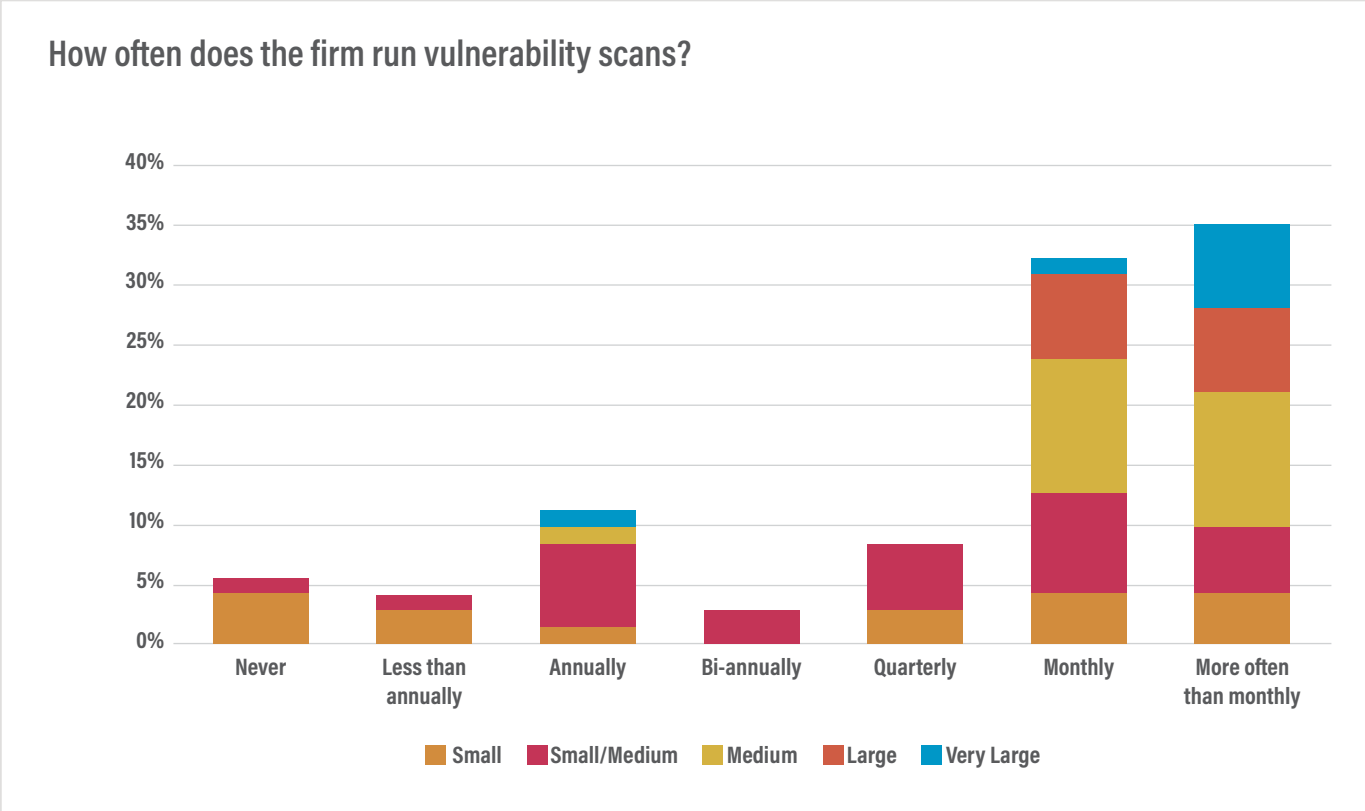
Data Findings (cont.)



Only 21% of firms correlate their asset inventories with expected security controls, and only 17% of firms resolve issues with missing controls within five days of discovery. About 50% of firms are relying on a SOC/SIEM to monitor key controls. Advanced proactive features like threat hunting are more atypical.

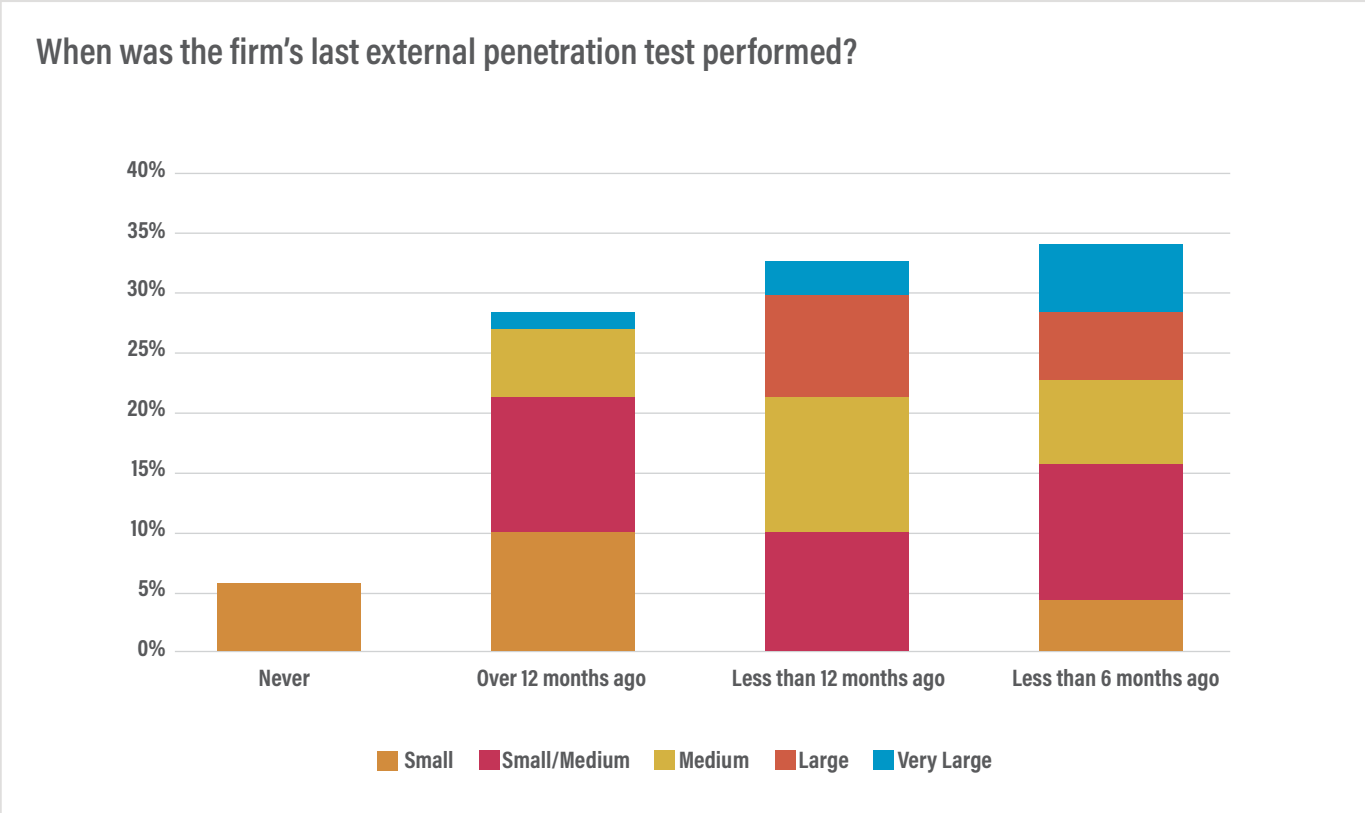
Data Findings (cont.)

Proactive Testing



While some small to SMB businesses never scan, most businesses of all sizes scan for vulnerabilities at least annually. As we scale in size to larger firms (medium to very large organizations), scanning is conducted monthly or more frequently, as a best practice. This finding is confirmed by the ILTA Technology Survey, which found that 57% of firms scanned at least monthly.

Data Findings (cont.)



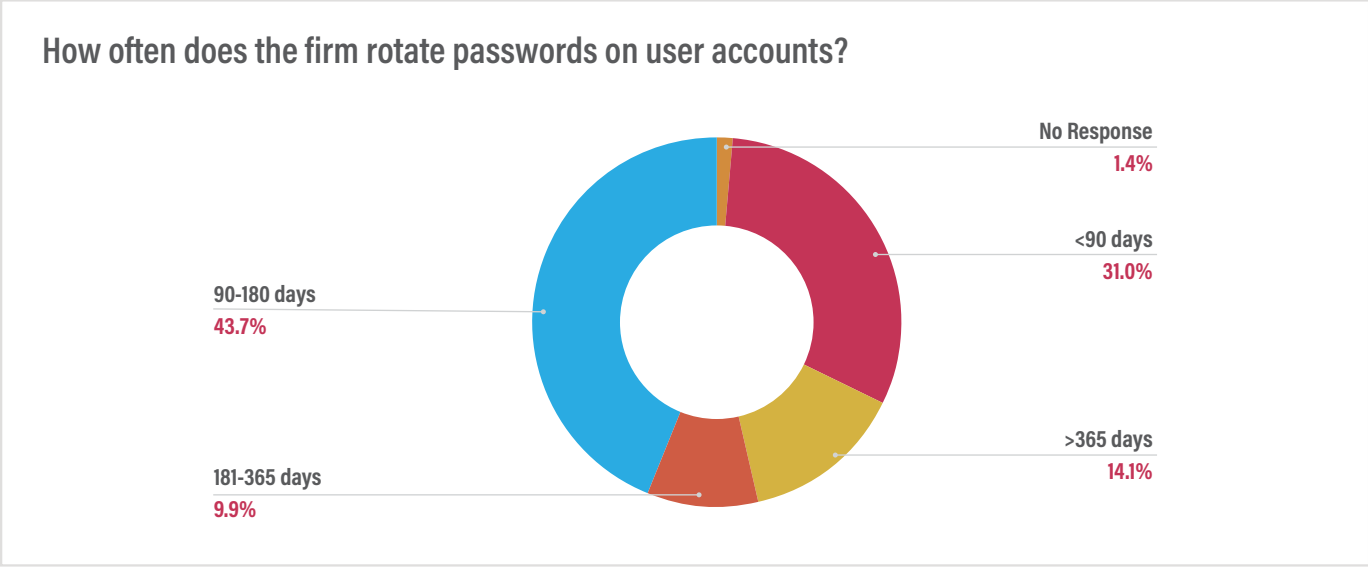
Nearly a third of small firms never conduct penetration tests, while the vast majority of SMB to very large organizations probe their defenses bi-annually to annually.

Also, while our survey included no questions about overall security assessments, the ILTA Technology Survey found 67% of firms in their survey performed a third-party assessment annually or more often.

Data Findings (cont.)

Security Controls

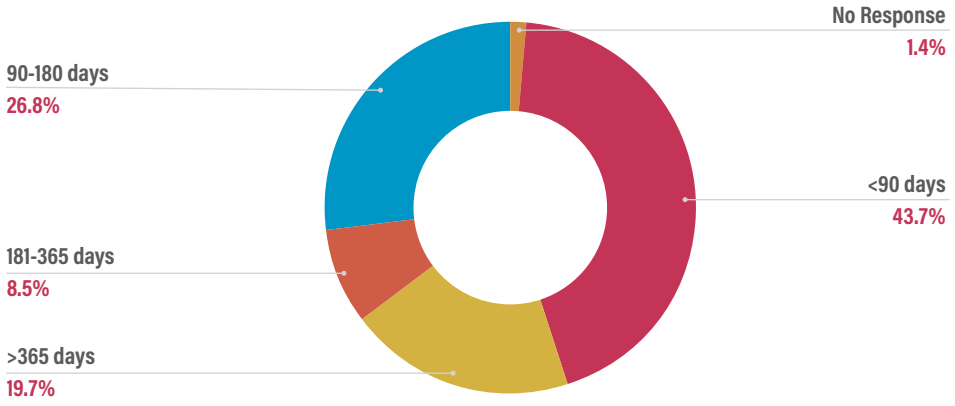
CREDENTIALS MANAGEMENT



While nearly 44% rotate user passwords between 90-180 days, over 14% rotate on a frequency of a year or more. The ILTA Tech survey found that 58% have no password management system.

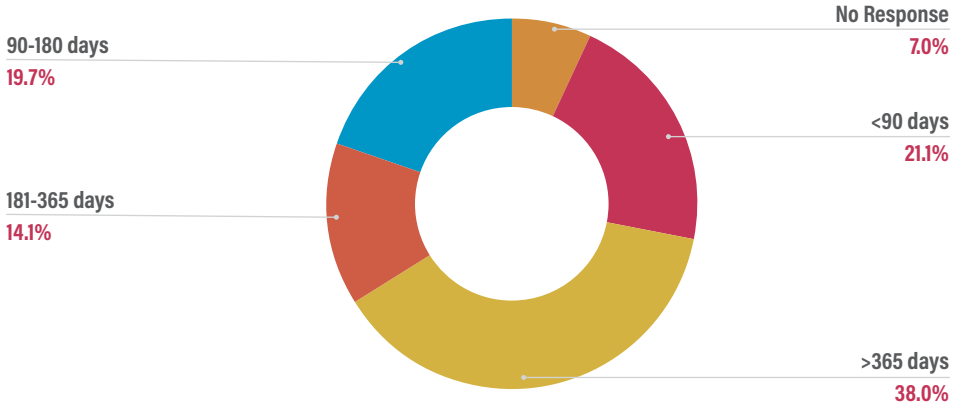
Data Findings (cont.)

How often does the firm rotate passwords on domain admin accounts?



Nearly 20% only rotate critical domain administrative credentials annually or more, while 44% rotate at a more robust <90-day interval.

How often does the firm rotate passwords on service accounts?

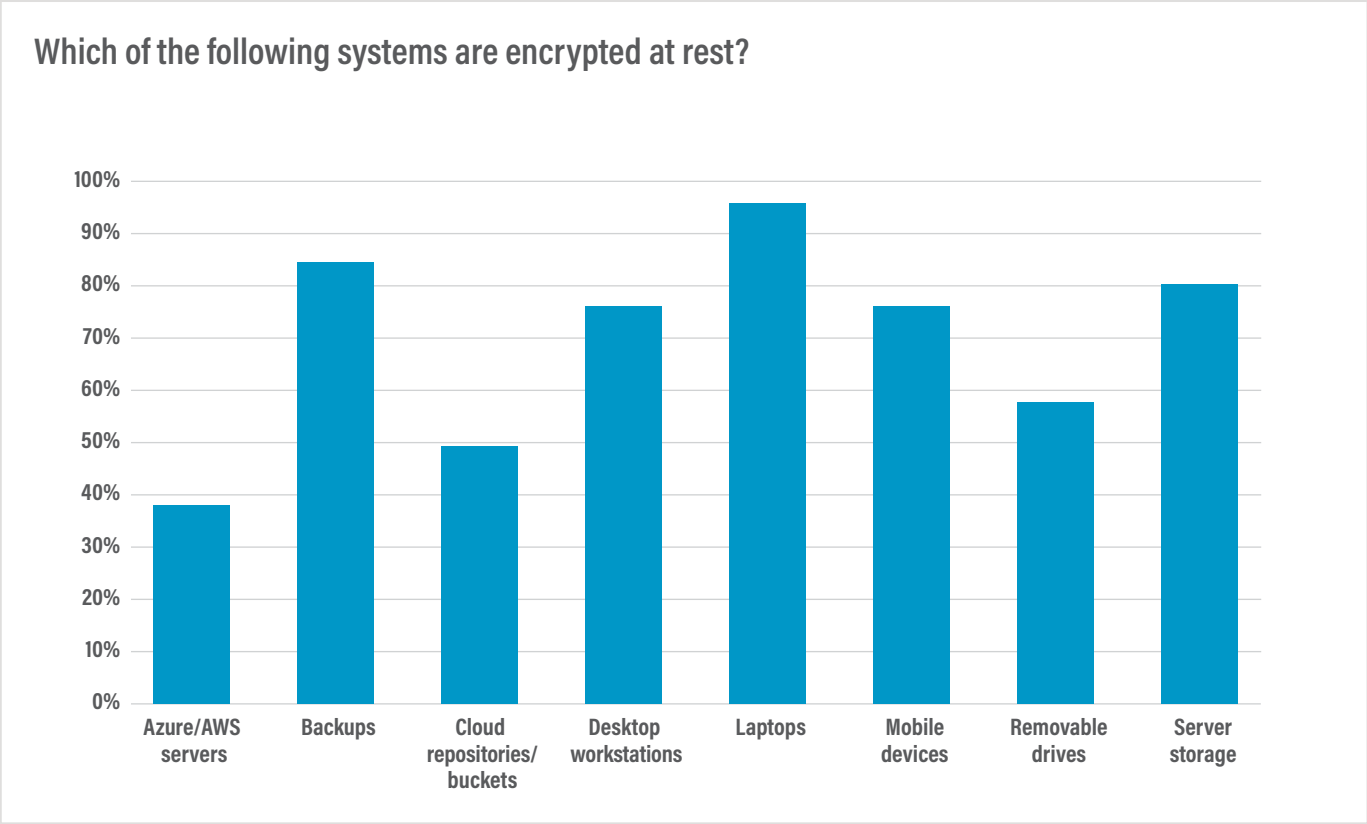


Only 21% of respondents are rotating service account passwords at a 90-day interval or less.

Data Findings (cont.)

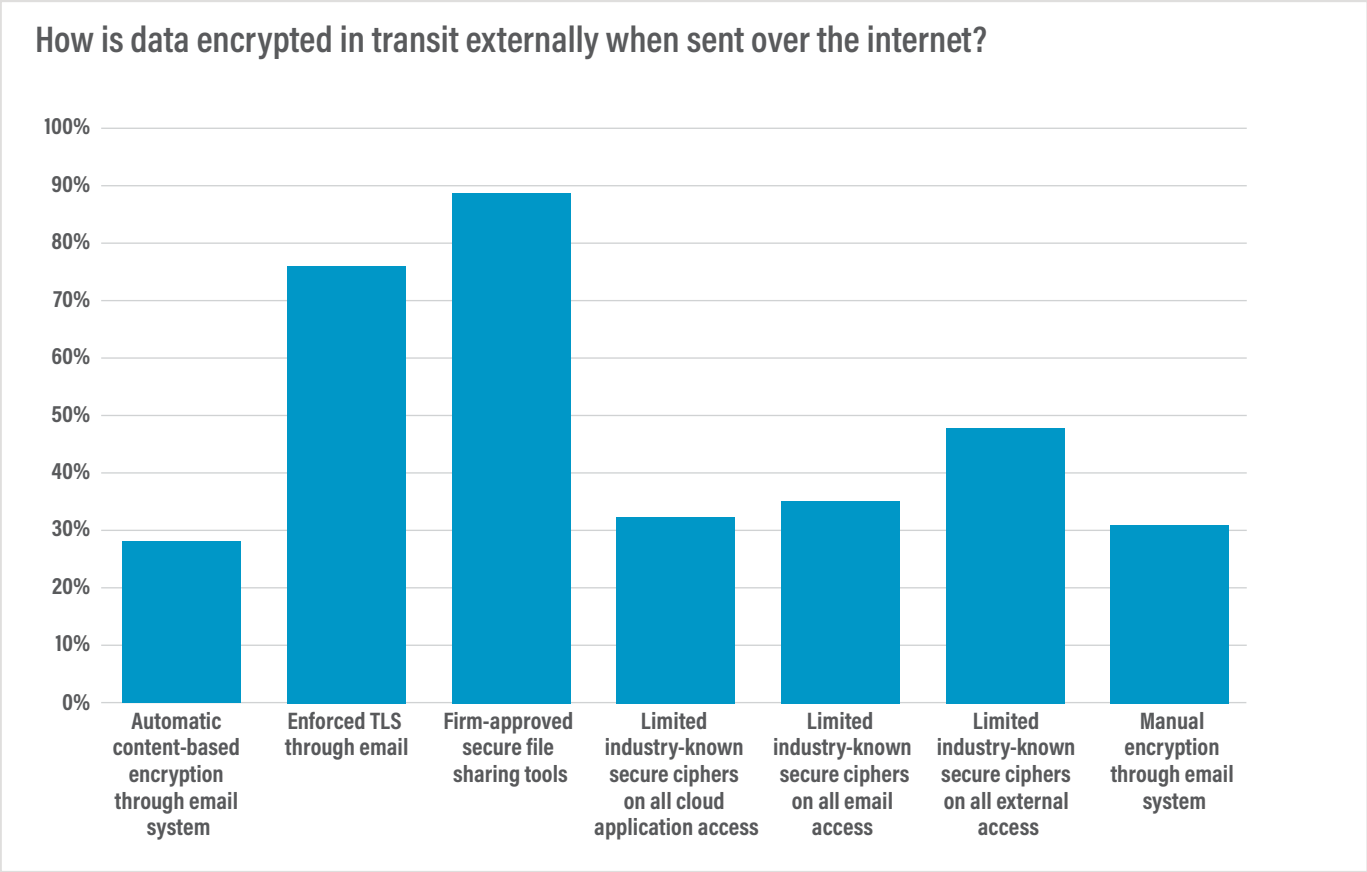
Security Controls

ENCRYPTION



Firms are more focused on encrypting physical devices than they are on encrypting cloud repositories.

Data Findings (cont.)

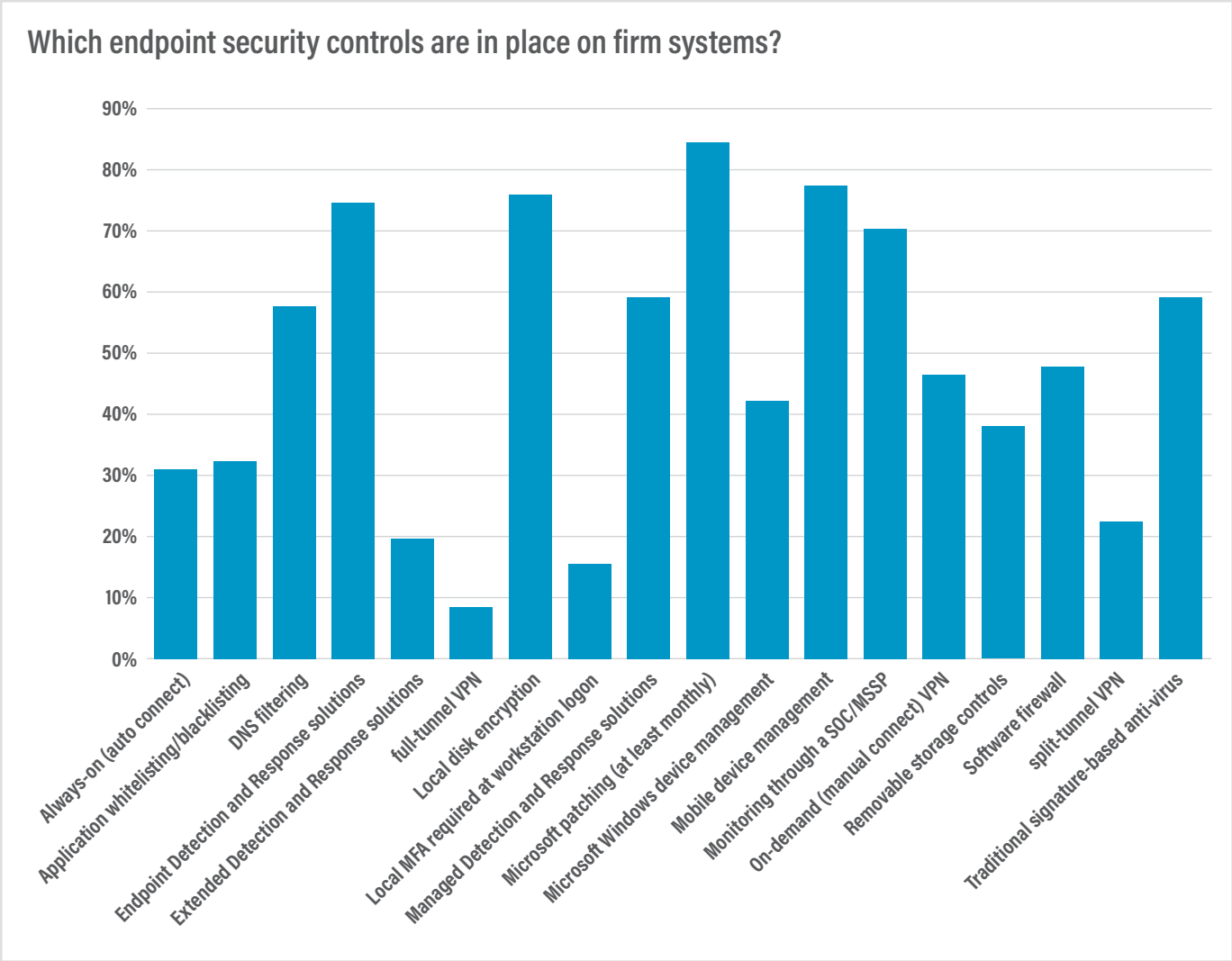


Only 28% of firms are using automatic, content-based encryption to prevent users from inadvertently sending sensitive information through unencrypted channels.

Data Findings (cont.)

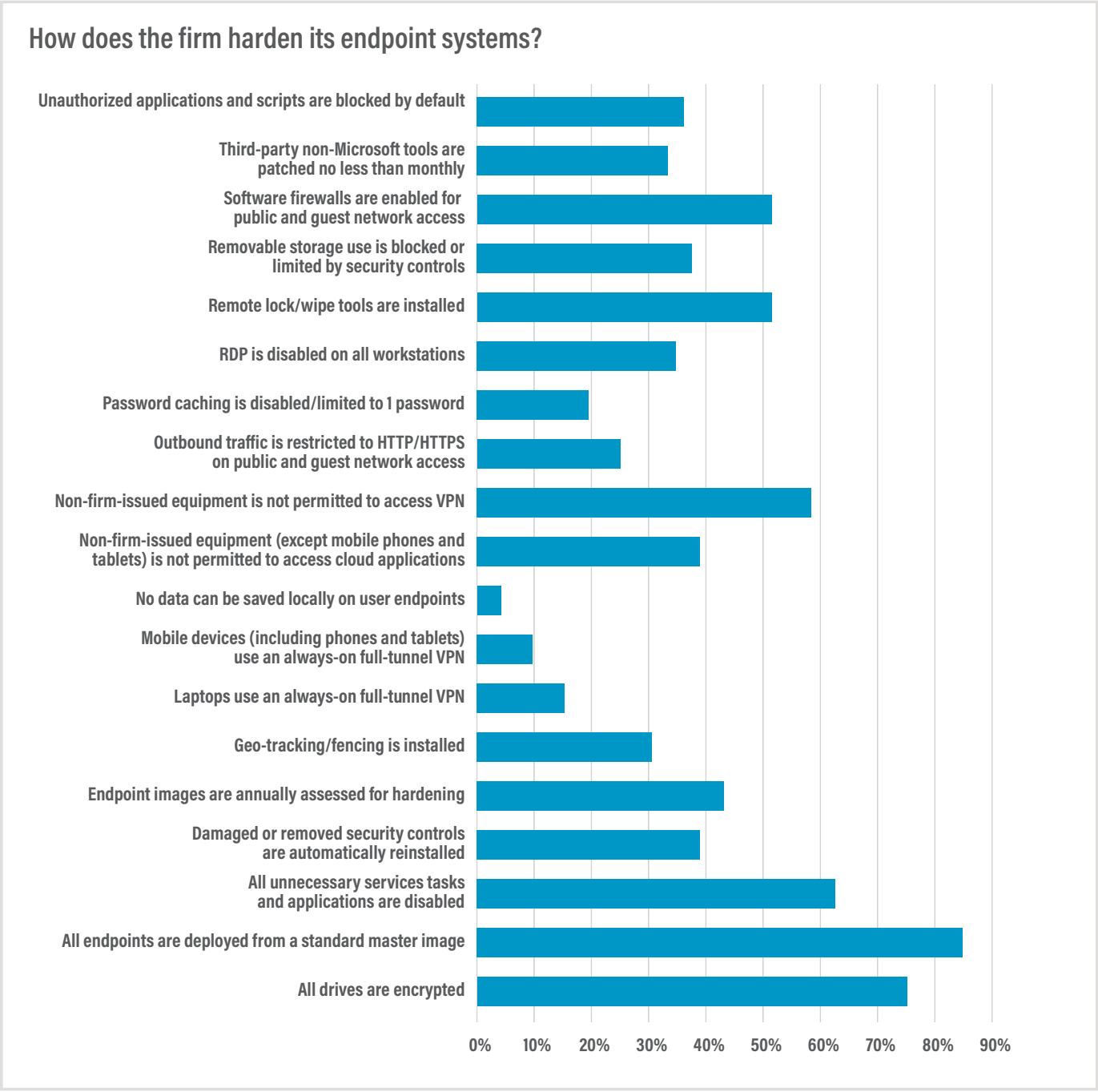
Security Controls

ENDPOINT MANAGEMENT



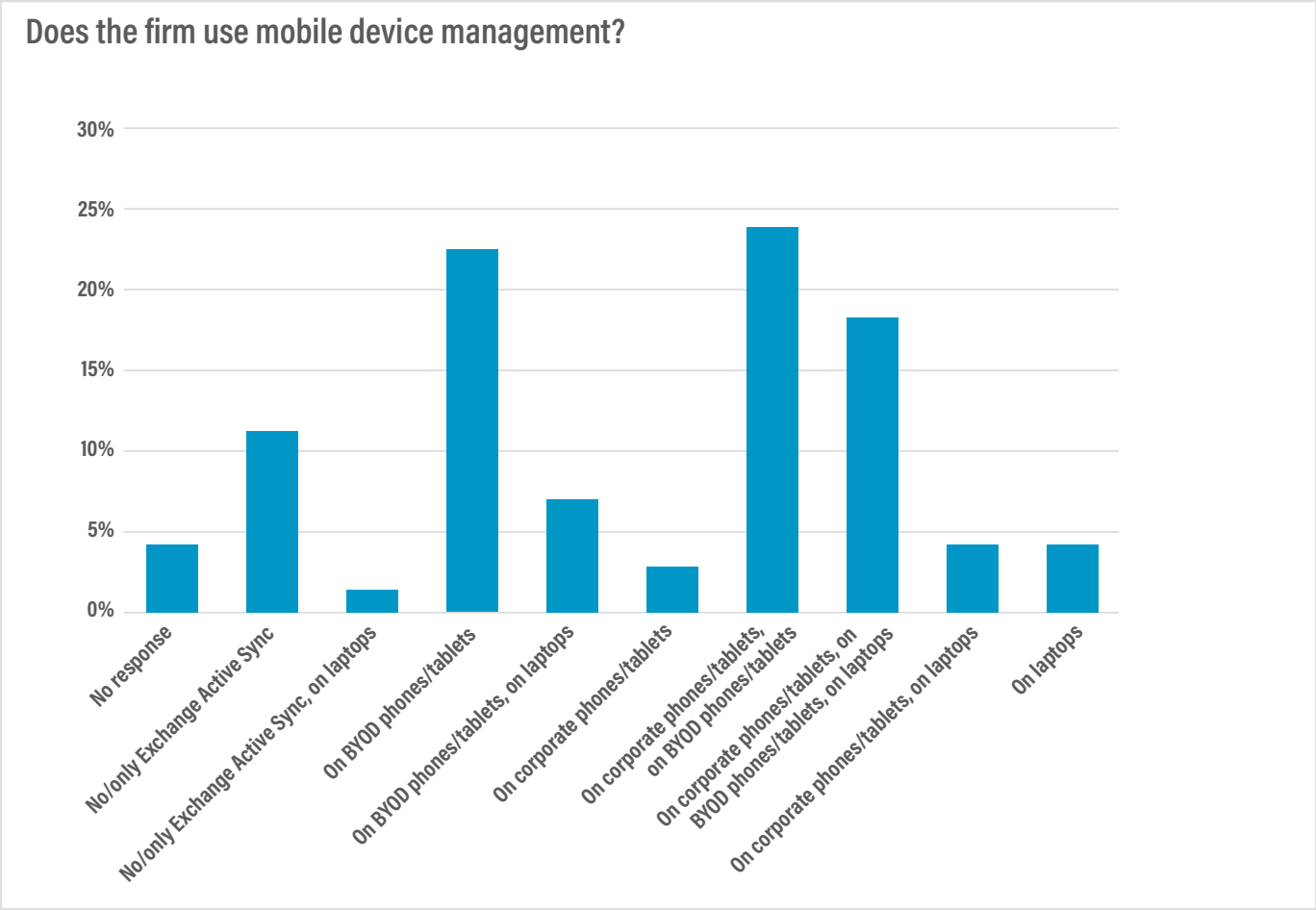
While most firms have MDR/EDR/XDR deployed, only 32% complement it with application whitelisting/blacklisting tools, which are a vital component of the security stack.

Data Findings (cont.)



Firms are using an array of tactics to harden endpoint systems and could possibly benefit from using more built-in security settings.

Data Findings (cont.)

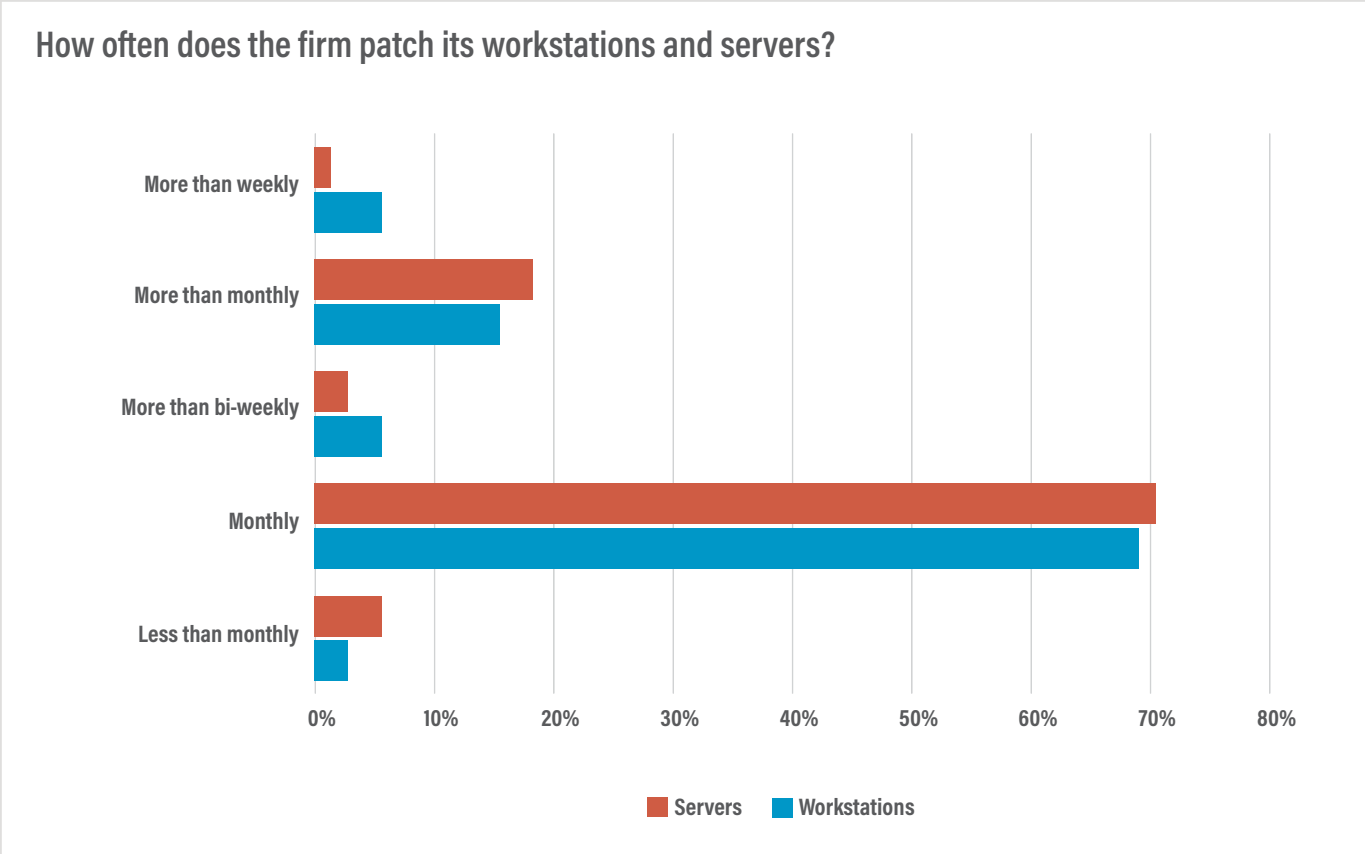


MDM is prevalent on phones and tablets (both corporate and BYOD), but it is comparatively rare on laptops.

Data Findings (cont.)

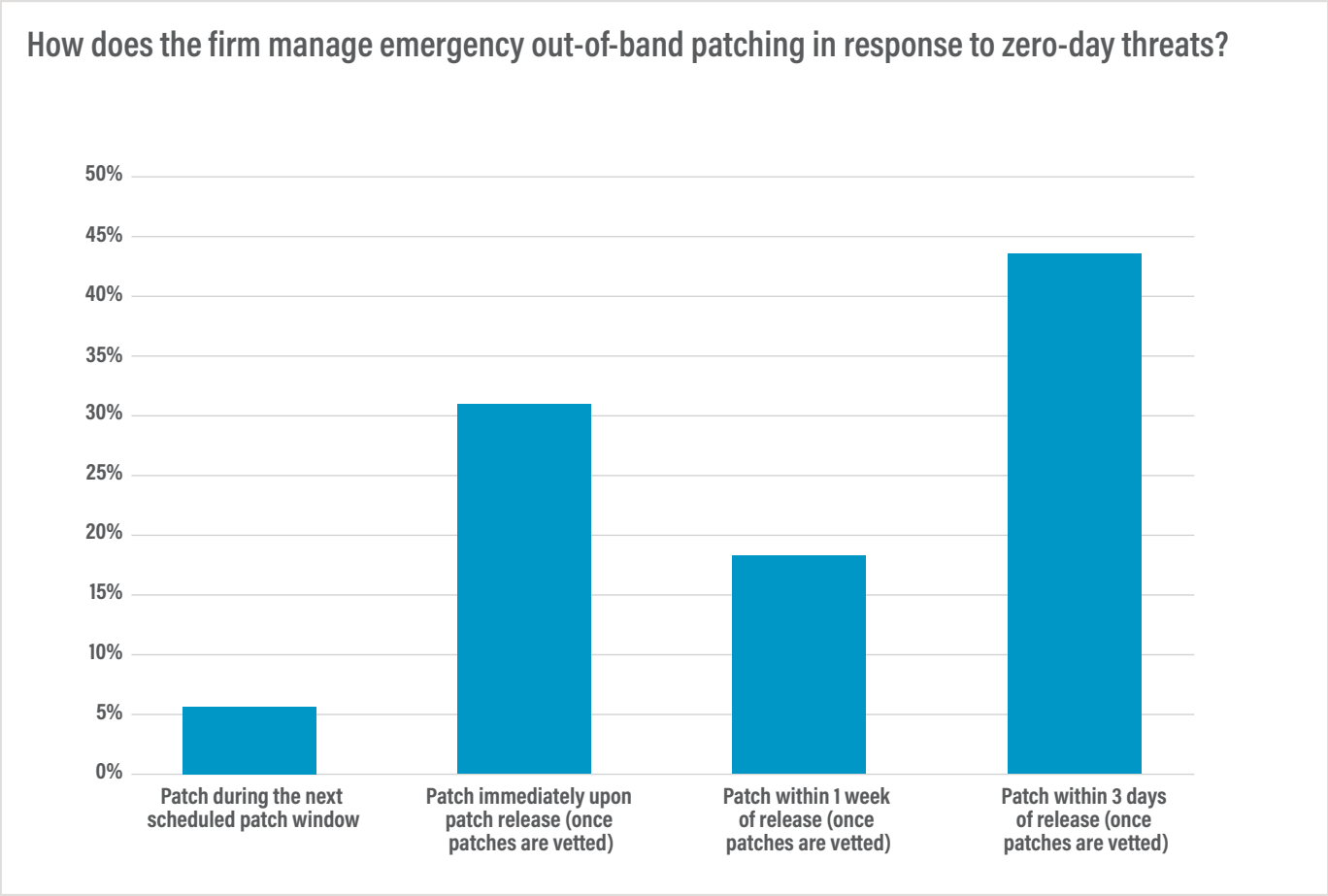
Security Controls

PATCHING/UPGRADES



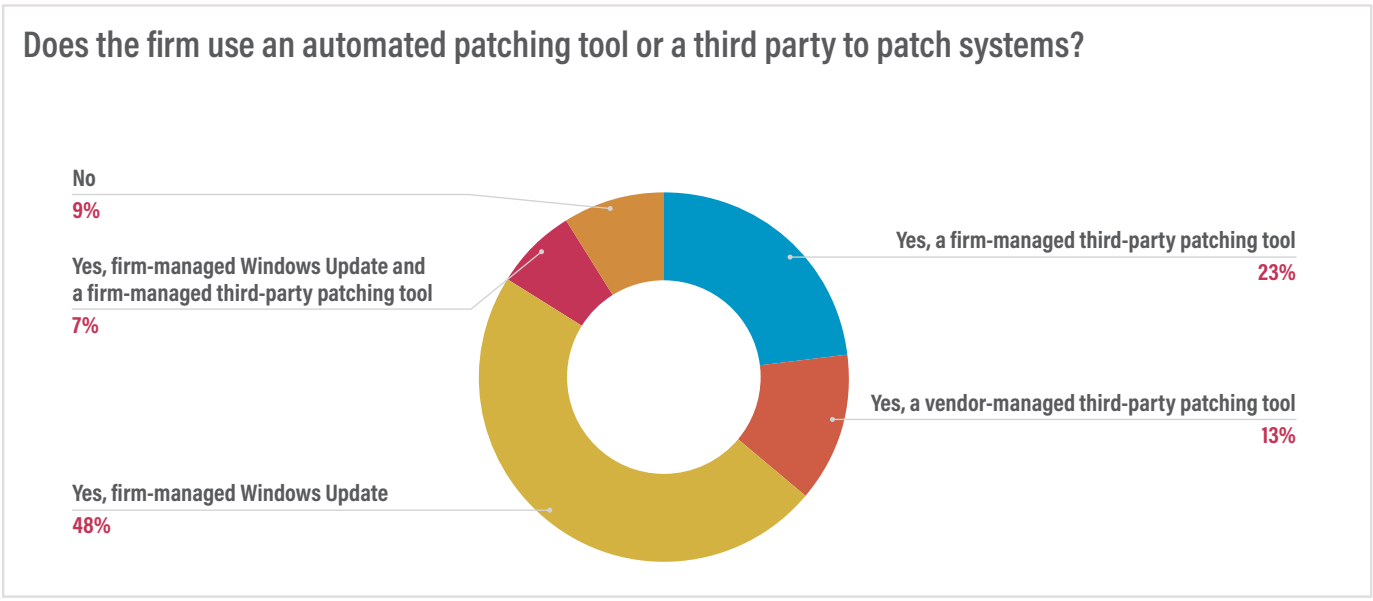
Most firms are patching monthly, but best practice and increasingly stringent OCGs and insurance requirements dictate the need for more frequent patching.

Data Findings (cont.)



Most firms patch within three days of release, once vetted.

Data Findings (cont.)

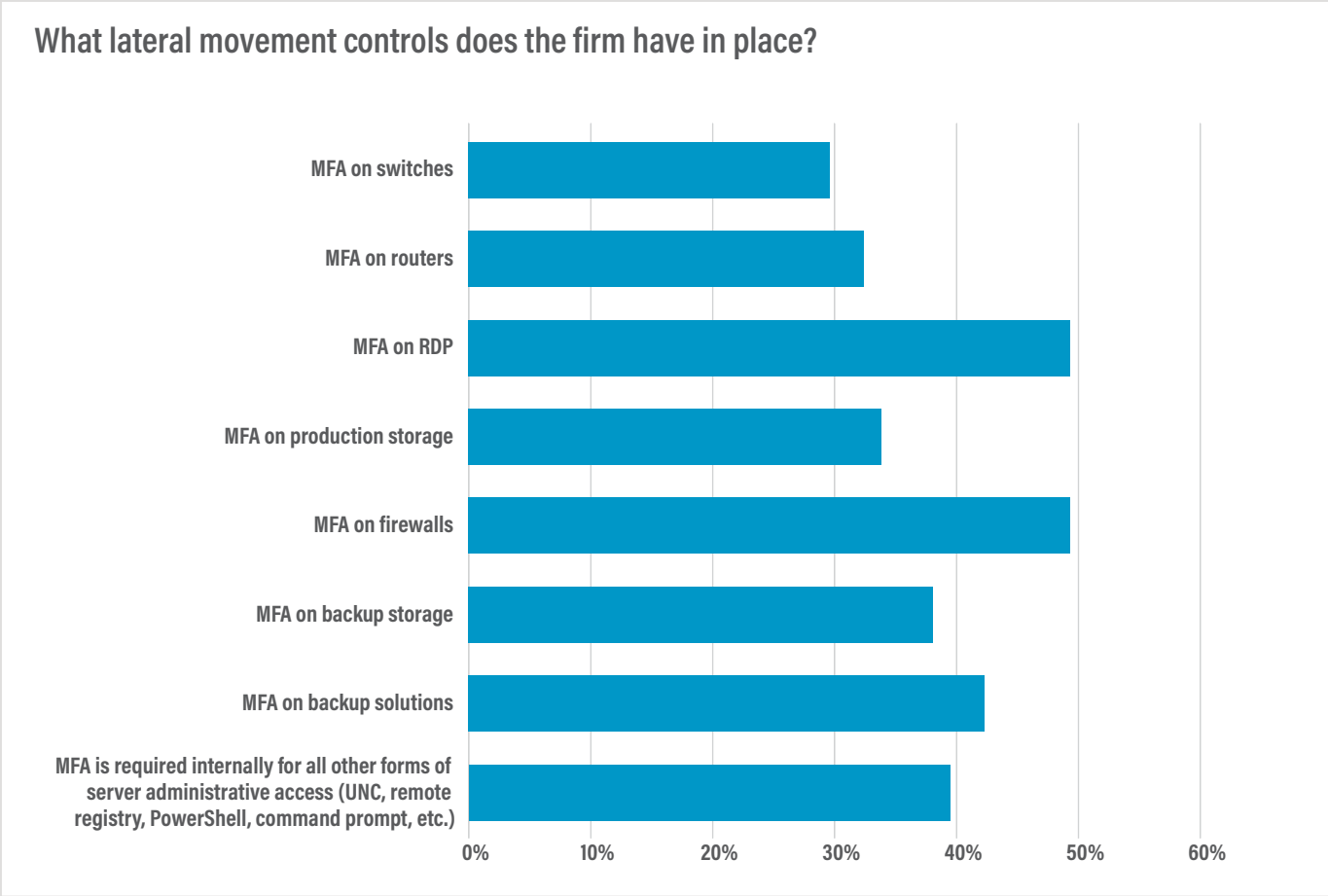


Only 13% of firms are outsourcing patching to a third party.

Data Findings (cont.)

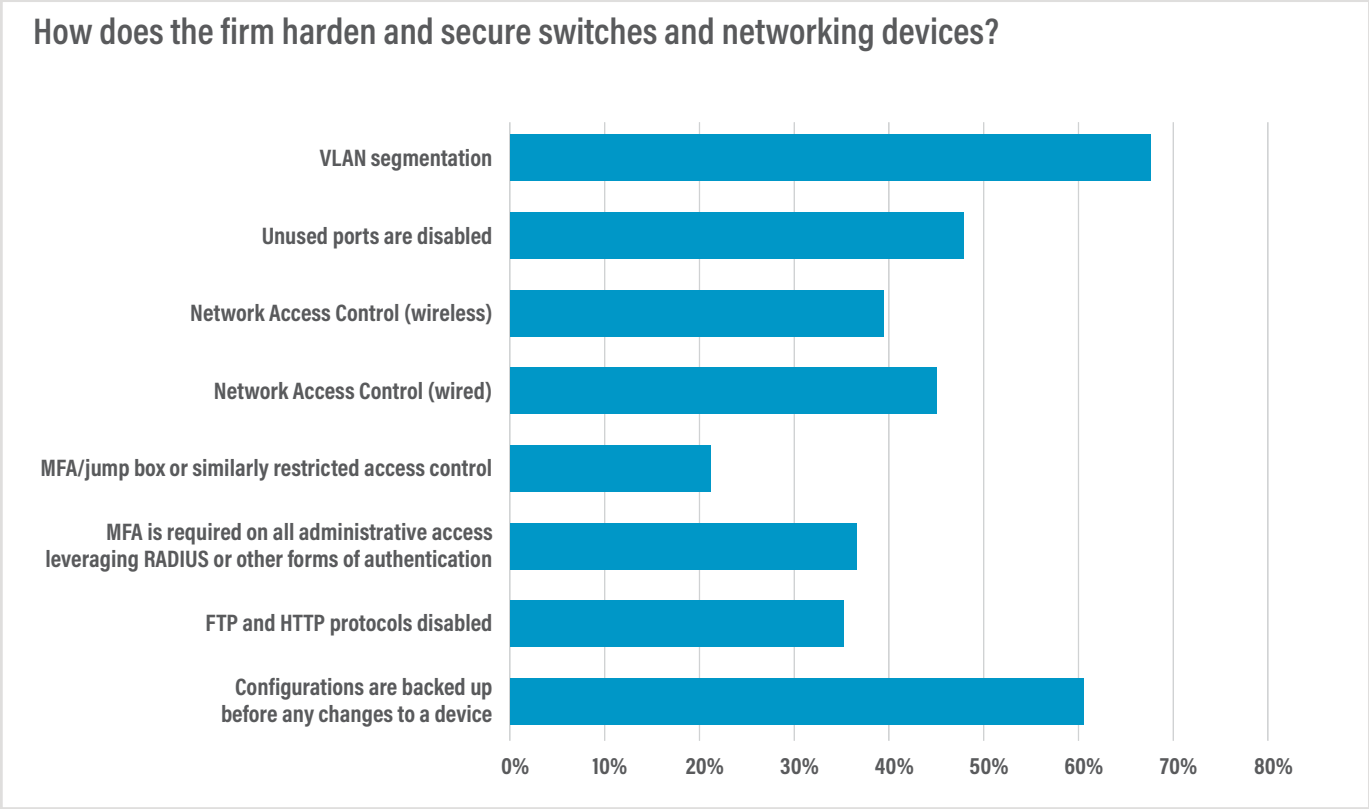
Security Controls

CONFIGURATION



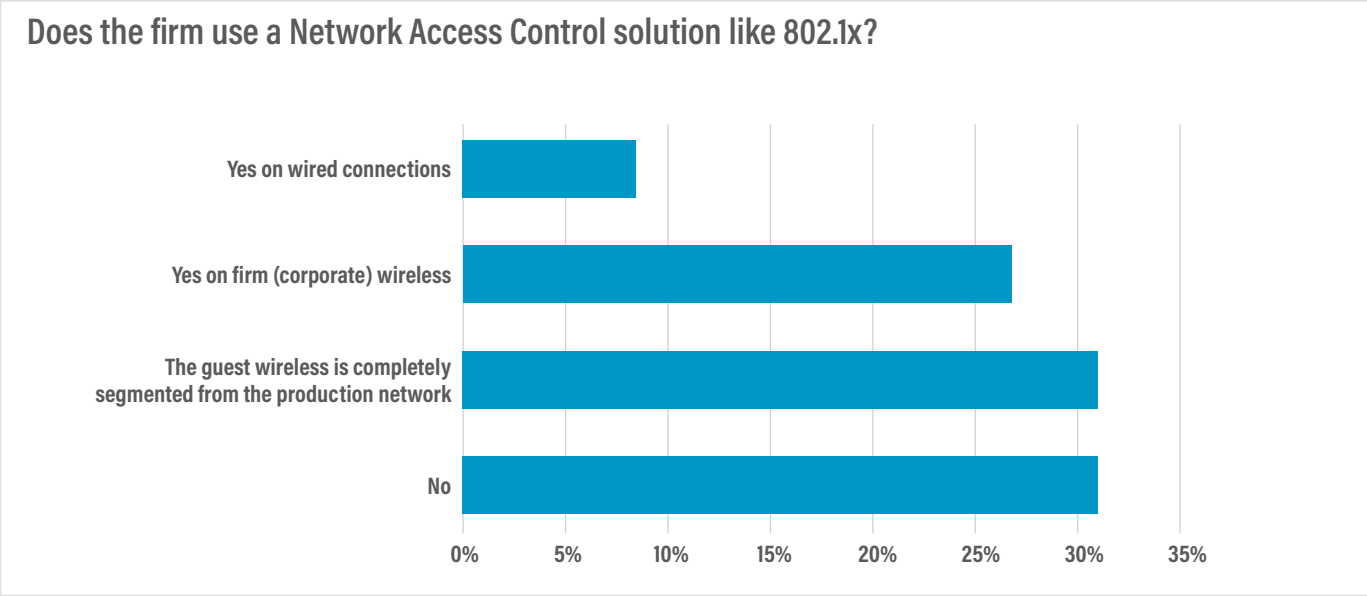
As one of the most critical security controls across the organization, our survey shows that MFA adoption still has a way to go in today's law firms. The ILTA Technology Survey also indicated that only 33% have MFA on server access/lateral movement defenses, essential to thwarting threat actor progress inside the perimeter.

Data Findings (cont.)



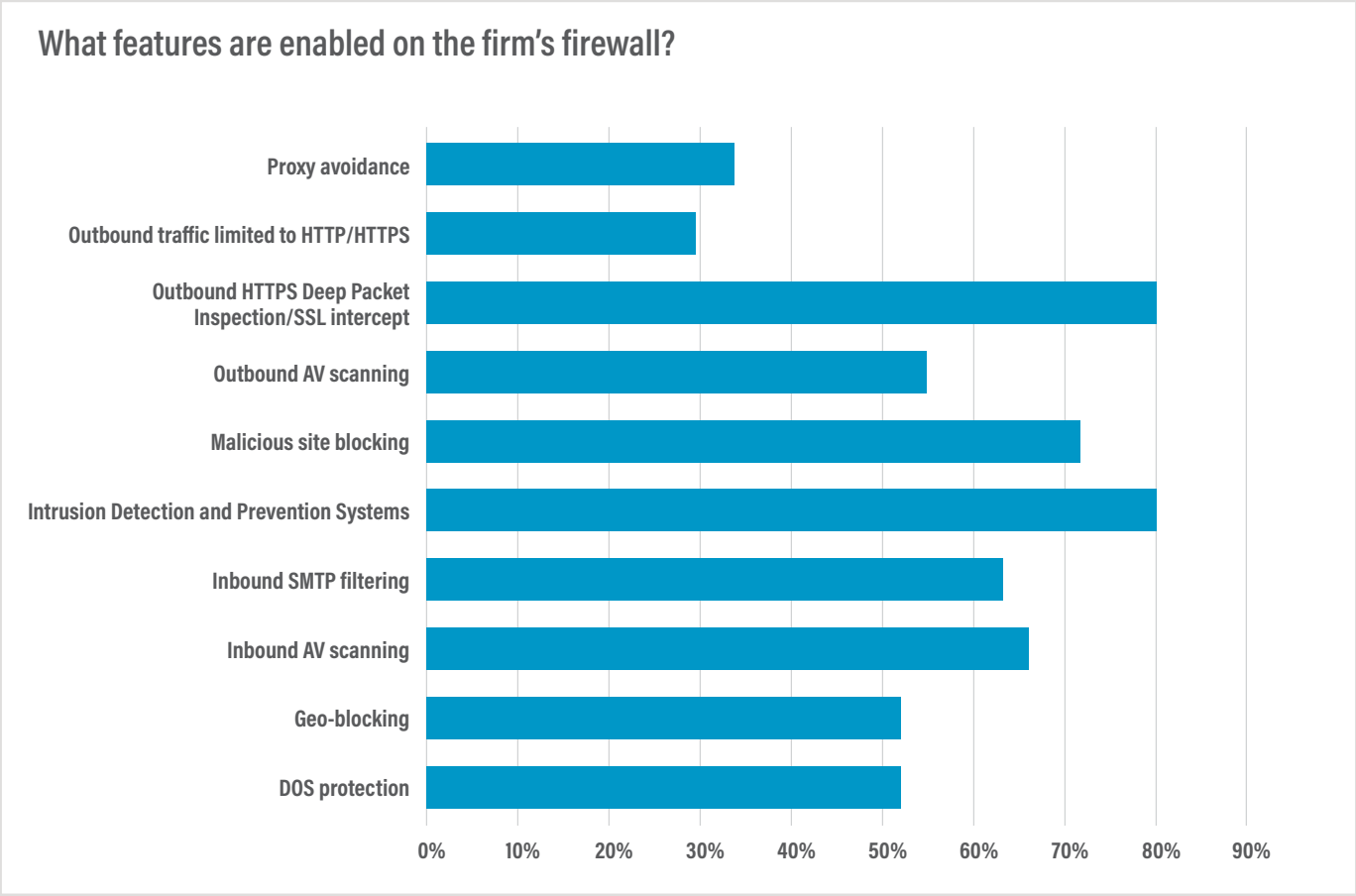
Firms use an array of tactics to harden switches and devices, with VLAN segmentation at the top of the list.

Data Findings (cont.)



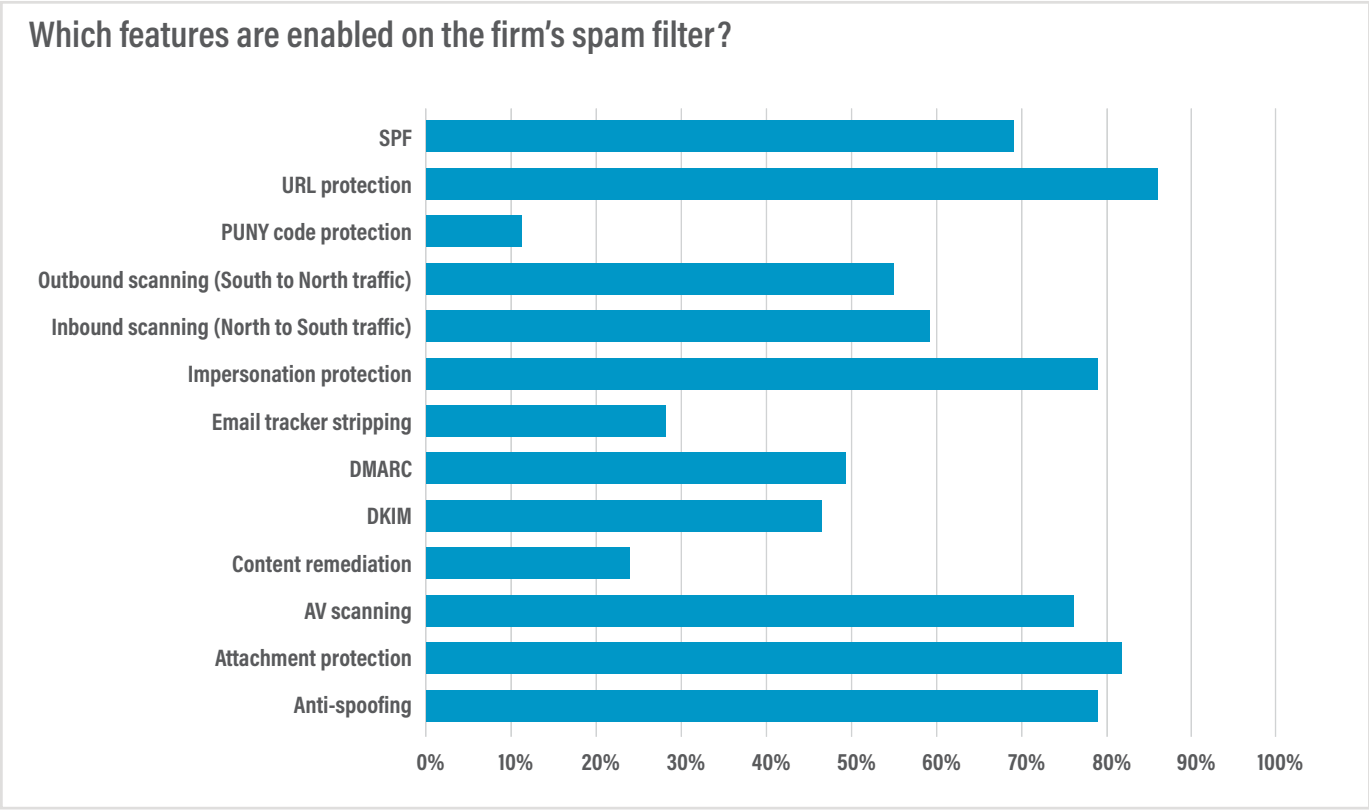
Forty-five percent of firms listed wired Network Access Control (NAC) as a switch-hardening feature that they employ, but only 8% listed it here. Thirty percent of firms use no form of NAC.

Data Findings (cont.)



Deep Packet Inspection is a key control for every firewall. With approximately 80% of the internet now using encrypted traffic, firewalls that are not performing DPI are not keeping firms safe.

Data Findings (cont.)



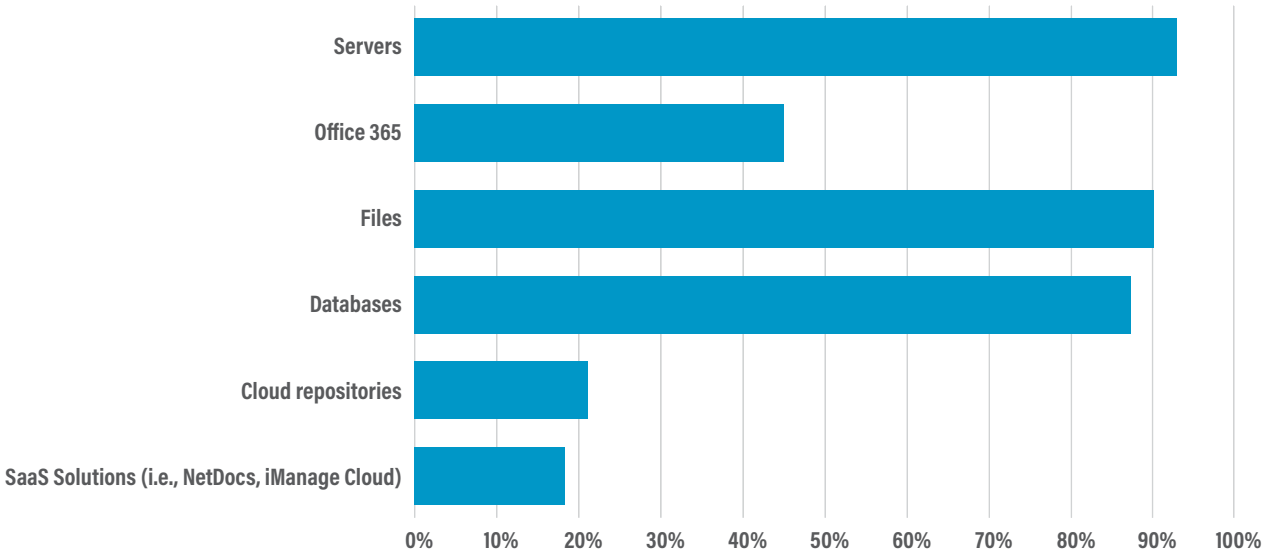
While firms are increasingly aware of incoming threats, they are less focused on internal and reputational threats like outbound scanning, DKIM, and DMARC.

Data Findings (cont.)

Security Controls

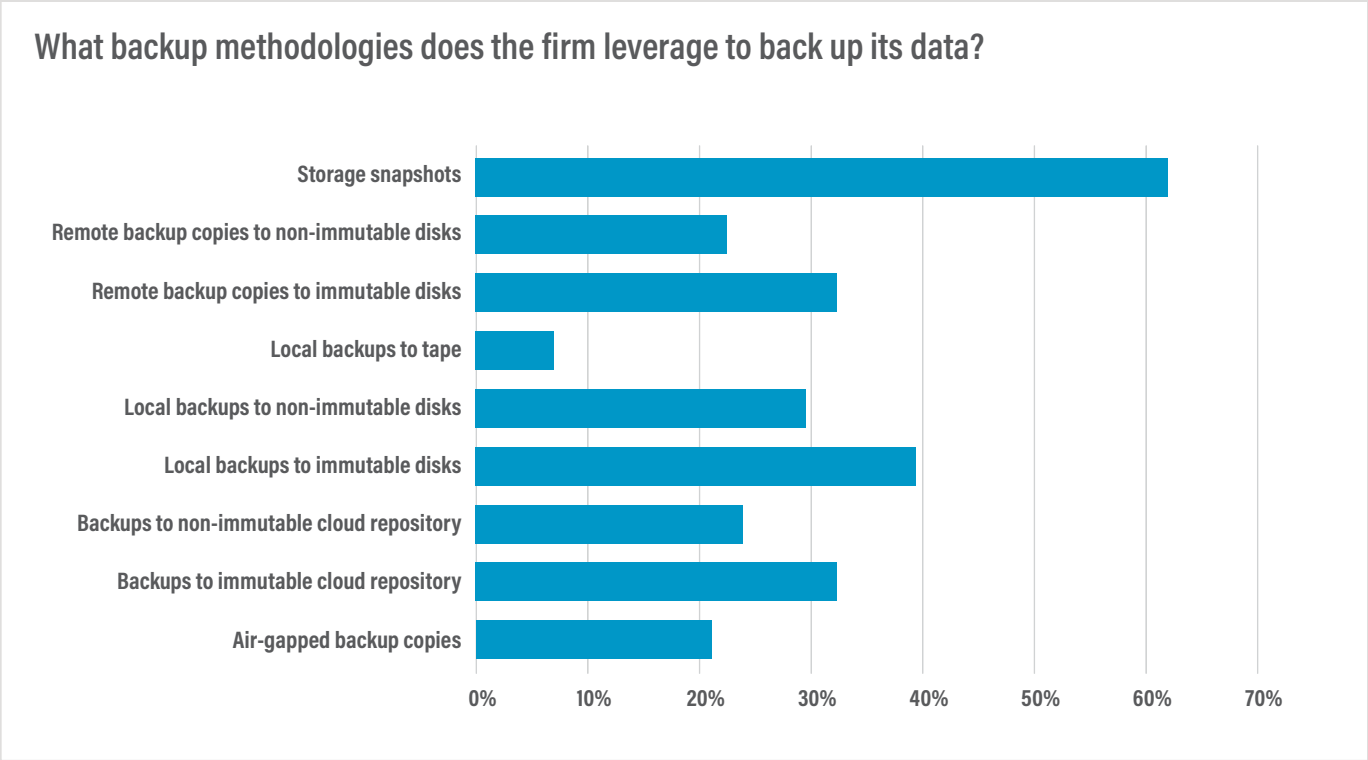
BACKUP & REDUNDANCY

Which of the following systems does the firm back up with a firm-controlled tool?



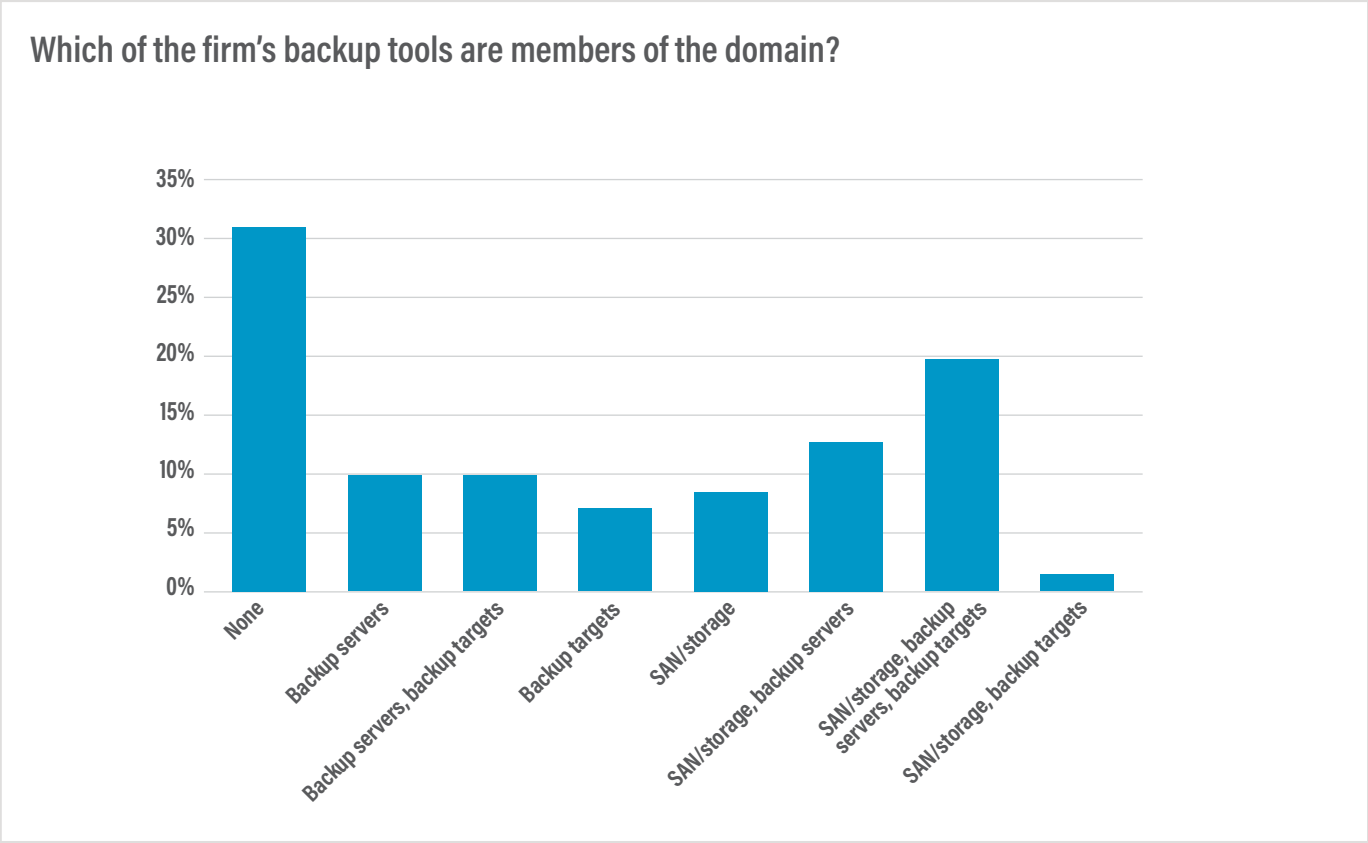
Firms tend to focus on backing up data on systems they own but are less vigilant about cloud and SaaS systems.

Data Findings (cont.)



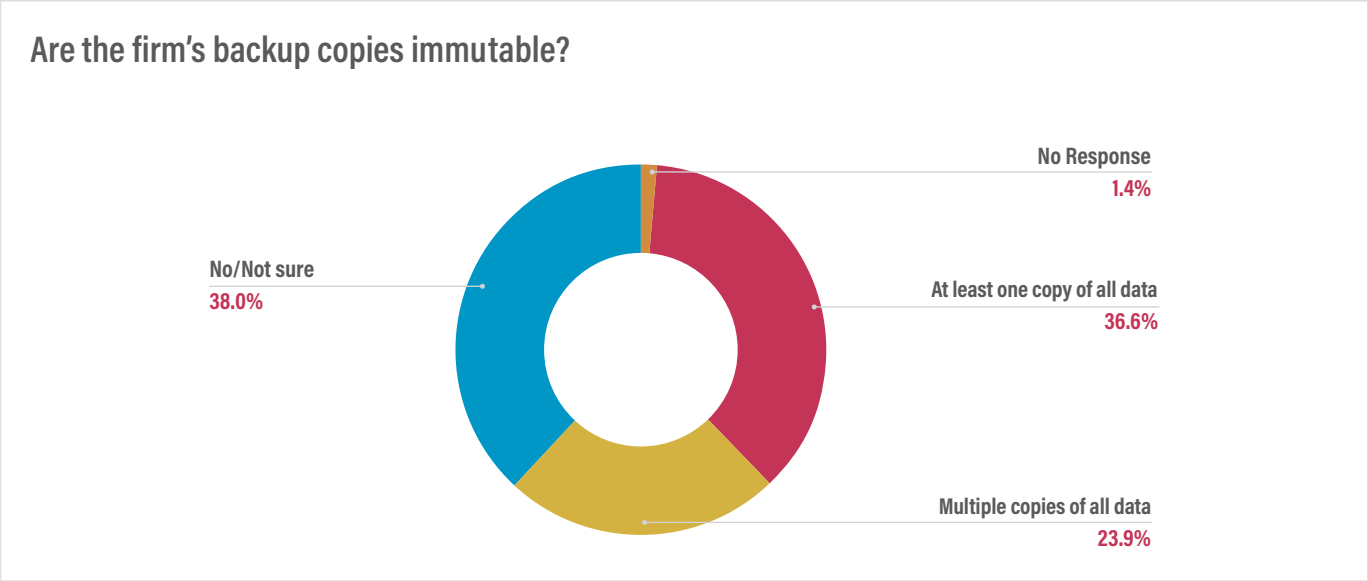
Firms are using a variety of backup methods, many of which are not immutable.

Data Findings (cont.)



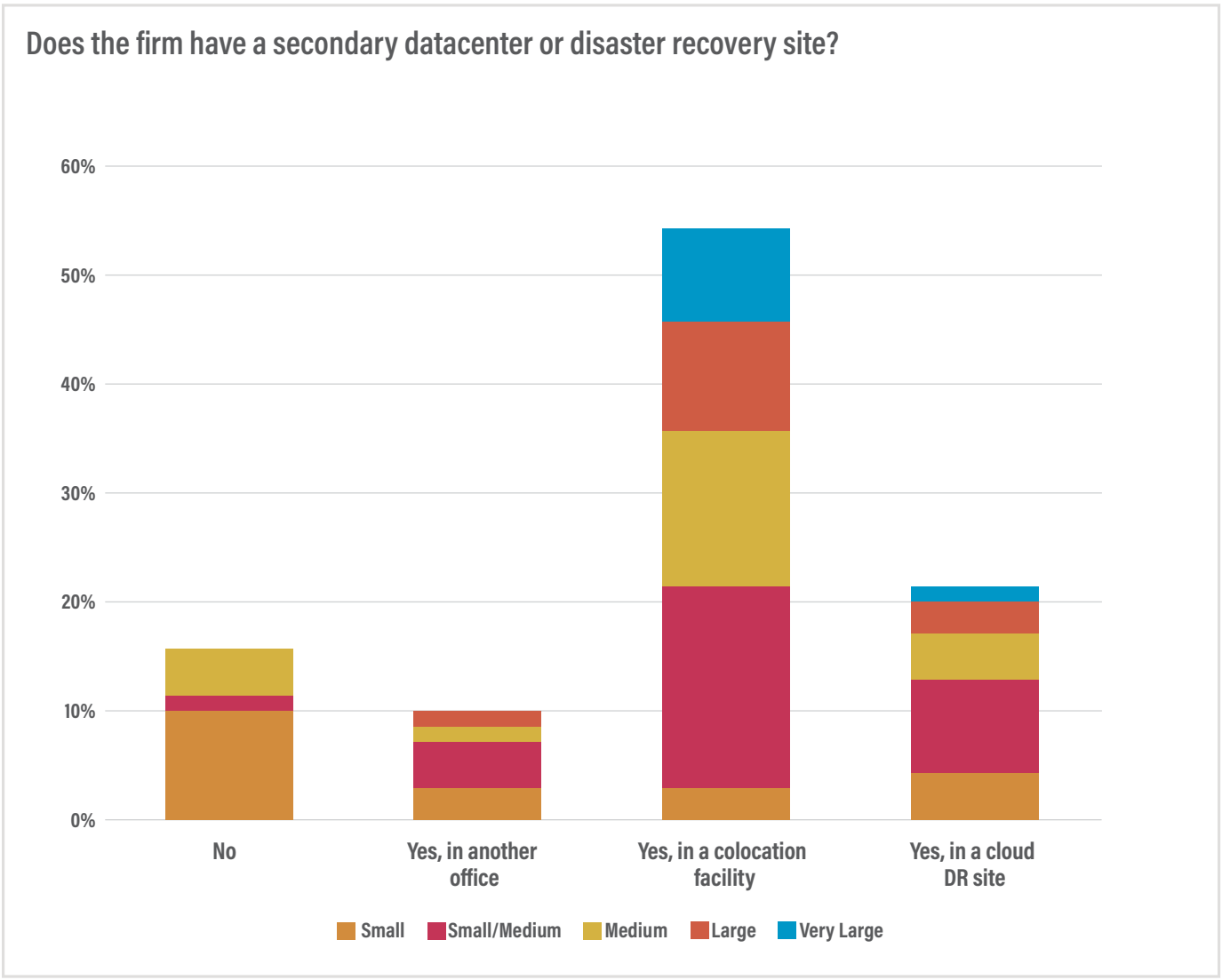
While the majority of respondents replied that no backup tools are members of the domain, there are still too many that are. Any part of the backup infrastructure joined to the domain is exposed and can easily be discovered by a threat actor. No backup servers, proxies, or targets should be domain-joined.

Data Findings (cont.)



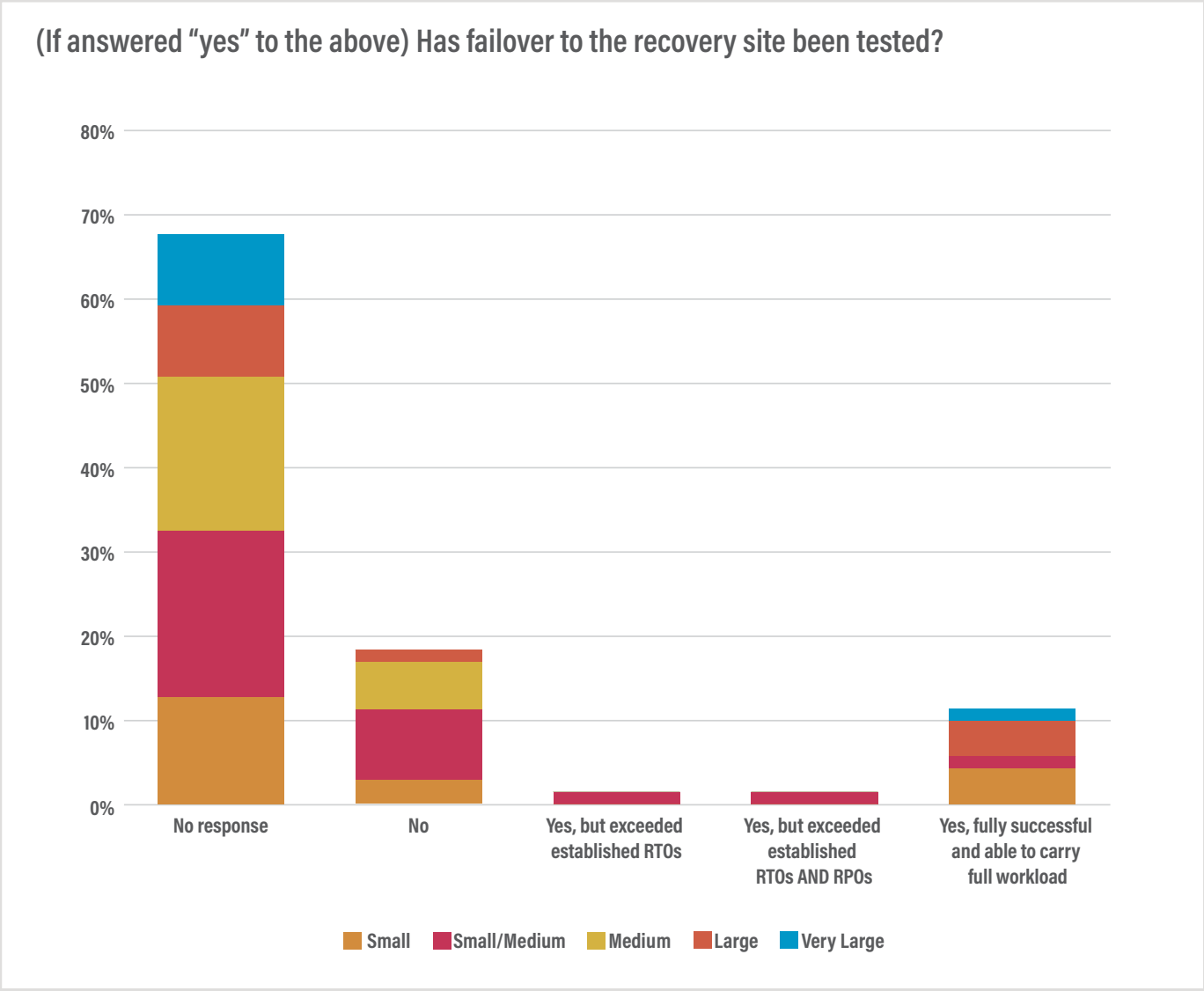
While the majority of firms report at least one immutable copy of all data, 38% of firms have not taken steps to ensure that backups cannot be destroyed during a ransomware event.

Data Findings (cont.)



Physical DR sites are still the most popular option. All large or very large firms have a DR site, while 29% of medium or smaller firms have no DR site.

Data Findings (cont.)



The vast majority of respondents chose not to respond to this question (take that as you will). Of those that answered, the majority have not tested failover.

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