iManage
Making knowledge work

ABOVE THE LAW

ABOVE THE LAW SURVEY RESULTS

The high stakes balance between security, productivity, and collaboration

CRITICAL CONCERNS FOR MANAGING LAW FIRM SECURITY

According to Forbes, remote or hybrid working remains one of "The 4 Biggest Workplace Trends In 2023," intensifying the growing threat landscape and the need for even more sophisticated security measures. With cyberattacks at an all-time high and 95 percent of all cybersecurity issues traceable to human error, the risk to law firms of all sizes is real and growing.

Adding to the overall sense of urgency, another big data breach or ransomware attack appears in the headlines on what seems like a daily basis — and those high-profile incidents are just the tip of the iceberg. Ransomware demands can create significant financial hardship, compounded by downtime and lost productivity. But it is the potentially catastrophic effect on a firm's hard-won reputation that may be, and perhaps should be, the concern that keeps law firm leadership up at night.

Bottom line, law firms must maintain a high level of security across all sensitive content, preserving data integrity and protecting client information without affecting workplace flexibility — wherever or however employees access information.

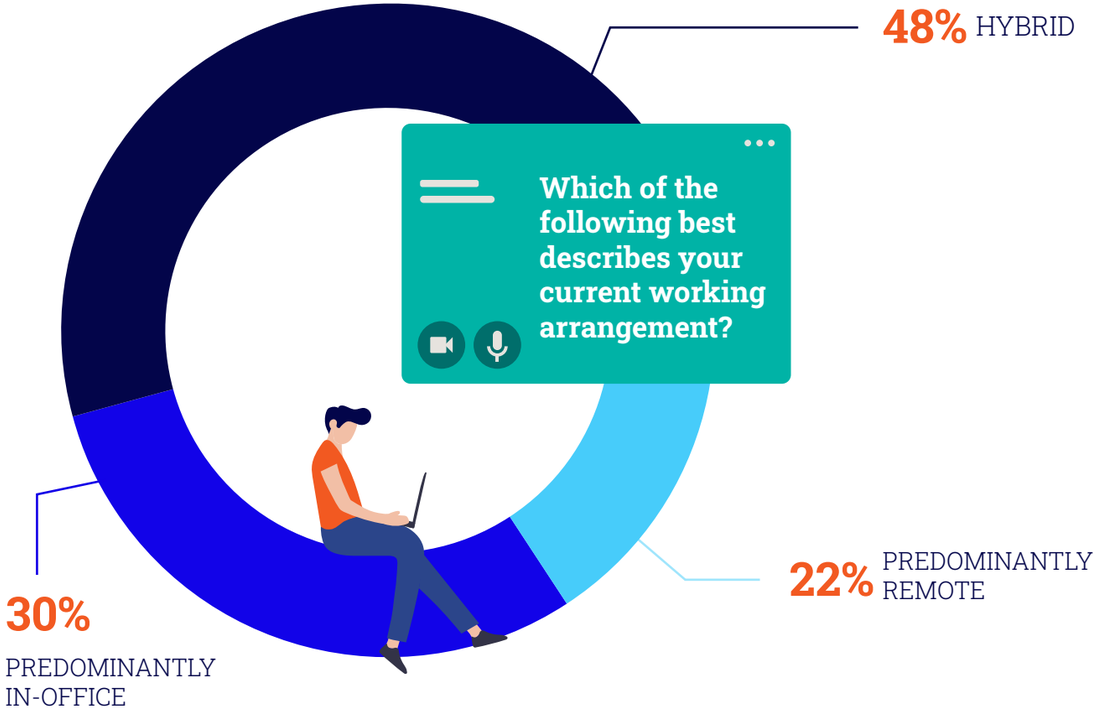
iManage partnered with Above the Law (ATL) to better understand these concerns, what steps law firms are taking to mitigate them, and what challenges firms are still working through to achieve operational efficiency. We were especially interested in understanding how law firms balance the need for productivity and collaboration in document and email management against security considerations, and with rising adoption of cloud-based platforms.

Our survey confirmed that security is very much on the minds of law firm leadership and their clients and that law firms take these threats very seriously. Significant pain points exist around many firms' ability to protect client data in a complex threat landscape, and most are either considering or already taking steps to mitigate the risks.

The survey also found that a secure document management system (DMS) is viewed as a critical component of a law firm's tech stack. IT leaders advocate using an advanced DMS to provide security against external threats like phishing and to ensure secure file transfer for clients. There is consensus that without the right tools, the right talent, and a strong security culture — one that both understands the need for change and embraces it — even the most dedicated efforts may fail.

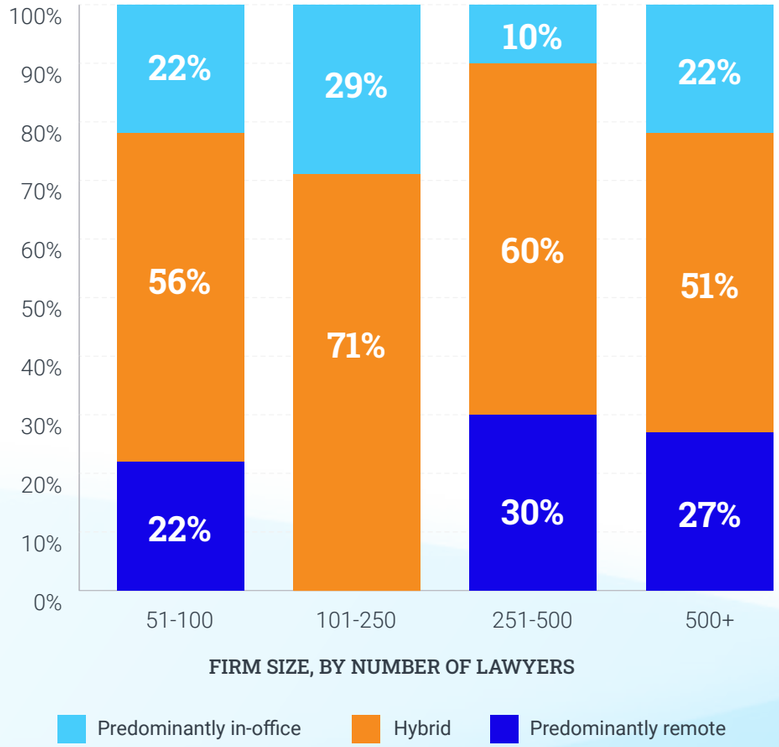
HYBRID AND REMOTE WORK
ELEVATE SECURITY CONCERNS

Across all law firms, but more so in larger law firms, the majority (70%) of survey respondents said they are following a work model that is either a hybrid (48%) or predominantly remote (22%).



For law firms that reported mixed working arrangements, the preferred working model varied by firm size. Those with 50 or fewer lawyers had at least 50 percent of their workforce predominantly in the office while firms with more than 50 lawyers reported a significant majority of their workforce either as hybrid or remote.

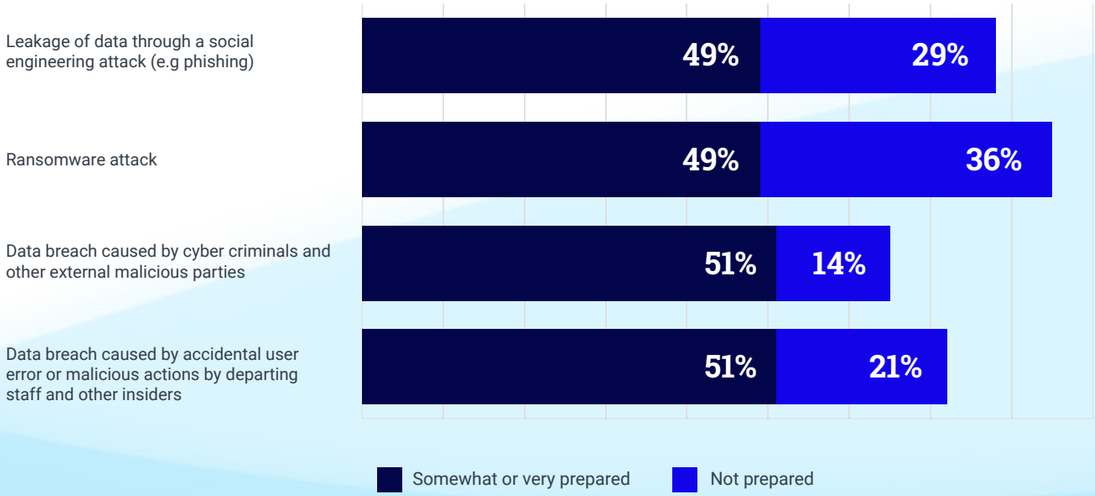
WORKING ARRANGEMENTS, BY SIZE OF FIRM



The shift from protecting the on-premises environment perimeter to a steep rise in remote-working staff using unsecured networks carries with it an elevated risk factor that is not lost on IT staff, information security, and compliance personnel. The legal sector finds itself increasingly more exposed to cyberattacks that exploit system vulnerabilities. According to MITSloan, "To take on the new cybersecurity challenges of this virtual working environment, organizations must understand the changes in their cybersecurity risk profile and revamp their strategies, training, and exercises to address these changes."

The deficit of internal awareness and education is acknowledged by respondents as well, many of whom said their organizations were inadequately prepared for escalating ransomware attacks (36%) and data leakage through phishing and other social engineering techniques (29%).

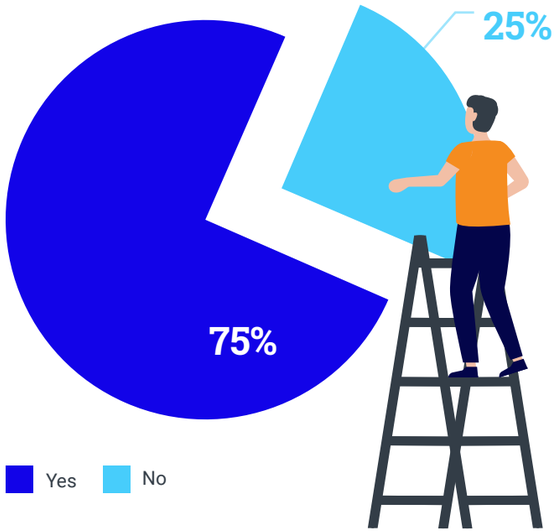
ORGANIZATIONS READINESS AGAINST THE FOLLOWING THREATS



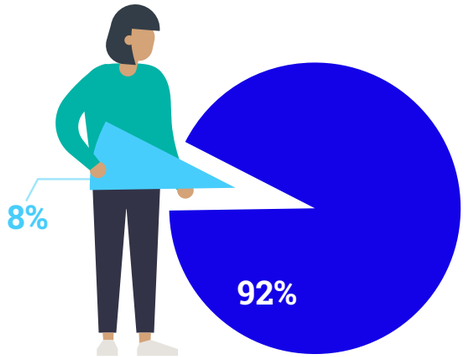
CLIENT DEMAND FOR **WORLD-CLASS SECURITY** DISADVANTAGES SOME FIRMS

Most respondents believe clients perceive larger firms to be better equipped to meet their data security requirements (75%), and respondents almost universally agree that this perception works to the larger firms' advantage (92%), leaving mid-sized and smaller firms to assess not only their security posture, but also how it is positioned or perceived by clients.

DO CLIENTS PERCEIVE A LARGER FIRM IS BETTER EQUIPPED?



DO YOU SEE THIS PERCEPTION AS A BUSINESS ADVANTAGE?

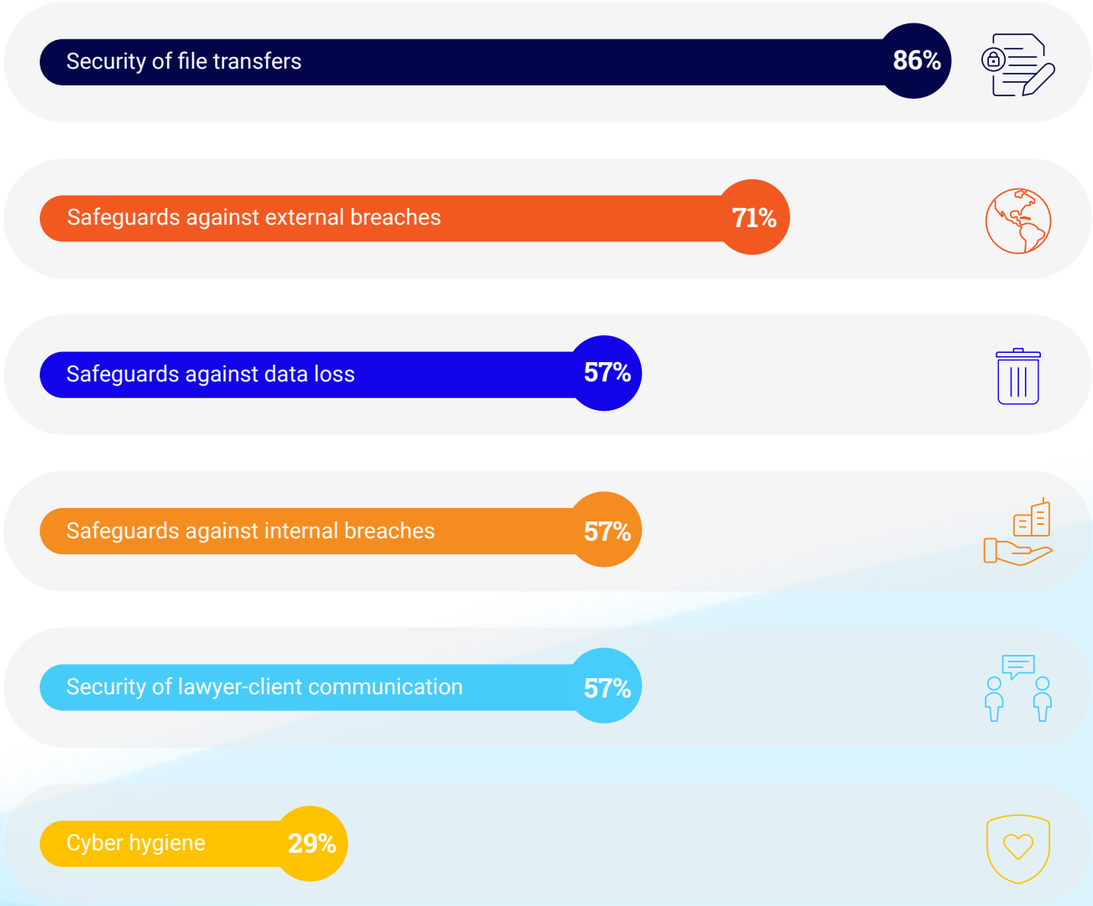


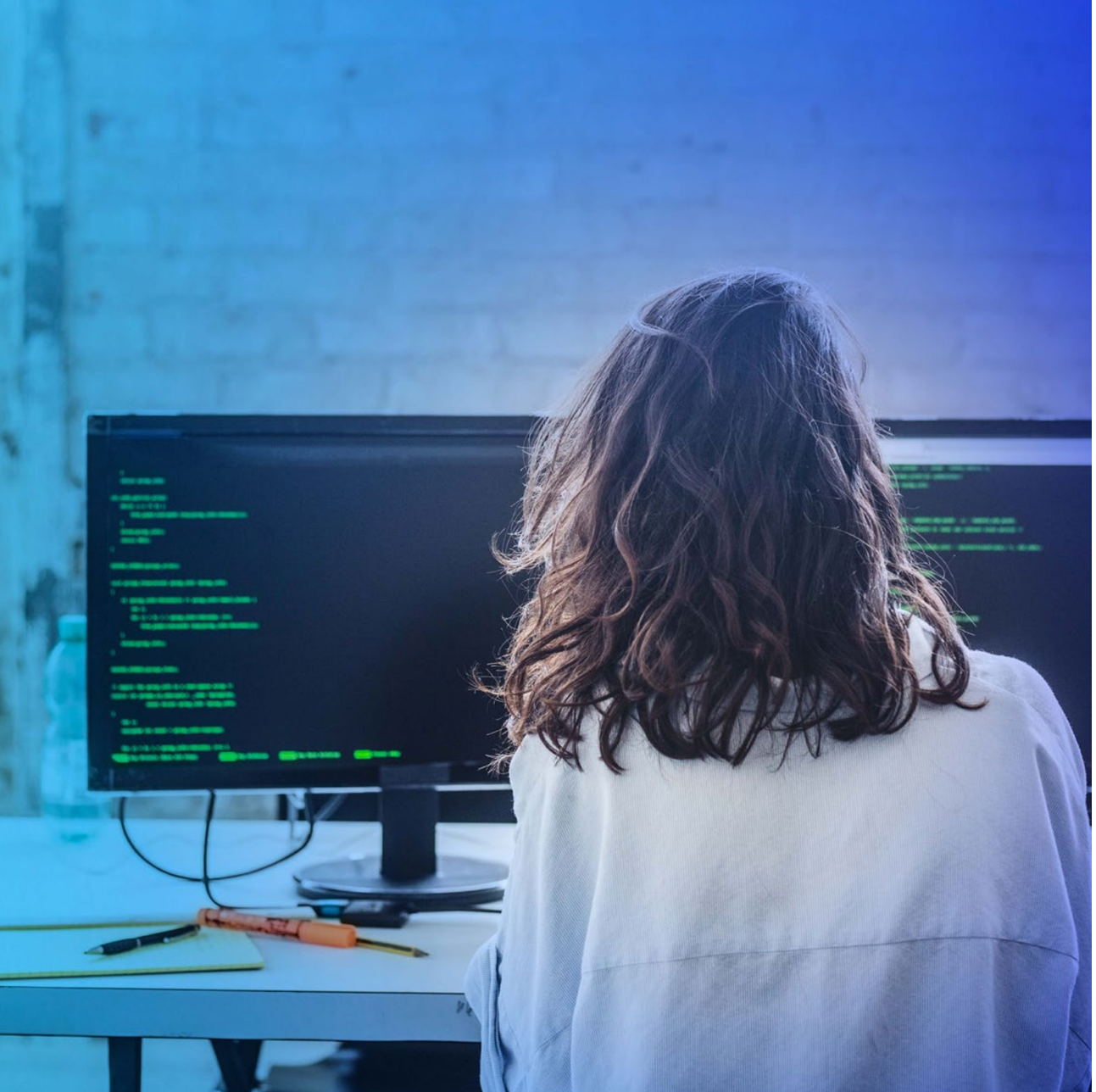
What specific client concerns do respondents seek to allay?

Nearly one third of those surveyed state their clients have become more focused on the law firm's ability to demonstrate strong security policy and a good track record of keeping client data safe, since the pandemic. Concerns about the security of file transfers (86%) and safeguards against external breaches (71%) were among the most frequently raised by clients. Notably, nearly two-thirds (57%) of respondents said that clients need assurances of protection against internal breaches and data loss, as well as the security of lawyer-client communications

This data makes it clear that security is of critical importance to law firm clients across all firm sizes and segments — and that their concerns encompass a broad range of cyber risks. We can surmise that clients expect to see evidence of the measures law firms have in place to maintain information security. Law firms are understandably keen to allay client concerns. What actions are they taking?

LAW FIRM RESPONDENTS: WHAT SPECIFIC CONCERNS HAVE BEEN RAISED?





STEPS TO MITIGATE **DATA BREACHES**

Our survey results substantiate a shift in how firms think about security — that it cannot be addressed purely through technology, and that human behavior is a key part of security readiness. Accordingly, the top three strategies considered essential in preventing data breaches are: advanced phishing protection; secure file transfer for clients and other external parties; and security awareness training for remote and hybrid workers.

WHICH OF THE FOLLOWING DO YOU SEE AS ESSENTIAL TO PREVENTING DATA BREACHES?

Rating scale: 1 (of minimal importance) to 5 (of greater importance)

The most important initiatives law firm respondents say they are taking to help prevent data breaches align closely to the most prevalent client concerns. These include advanced phishing attack prevention, security awareness training for remote and hybrid workers, secure file transfer and sharing, and regular cyber hygiene training for all workers.

A more holistic approach to security that includes people, process, and technology is ideal. Staff should have regular training on cybersecurity awareness, which includes "do's and don'ts" for when working in the office versus from home or from a public place. Auditable processes governed by policies are key, and the auditing process must be transparent and ongoing. Finally, to facilitate any evidence sharing with clients, technology should support both process and people areas, helping to automate and track performance.

And although the responses indicate law firms are working to mitigate risk, the challenges can seem nearly as daunting as the threats themselves.

WHICH OF THE FOLLOWING DO YOU SEE AS ESSENTIAL TO PREVENTING DATA BREACHES BY ROLE?

	Partner or counsel	Associate	Solo practitioner	Legal ops	Paralegal/ litigation support	IT staff	Information security, compliance, or records management
Retention rule-based content disposal	3.89	3.41	4.71	3.83	5.00	4.25	4.50
Monitor user activity to flag odd behavior	4.00	3.23	4.00	3.67	3.00	4.42	4.25
Enforce unique, complex passwords	4.05	3.14	4.14	2.83	5.00	4.42	3.75
Document encryption	4.16	4.14	4.57	4.40	5.00	4.17	3.25
Regular cyber hygiene training for workers	4.37	3.50	4.57	4.67	4.50	4.92	5.00
Secure external file transfer/sharing	4.53	4.00	4.71	4.83	5.00	4.33	4.75
Security awareness training for remote workers	4.58	3.64	4.57	4.83	5.00	4.92	5.00
Antivirus and malware protection for devices	4.58	3.82	4.71	4.17	5.00	4.58	4.25
Advanced phishing attack prevention	4.58	3.82	4.71	4.50	4.50	4.83	4.75

THE TOUGHEST DATA SECURITY CHALLENGES

Internal culture topped the list of difficulties the respondents face around data security, closely followed by infrastructure. This reinforces the idea of an apparent shift in how firms think about security.

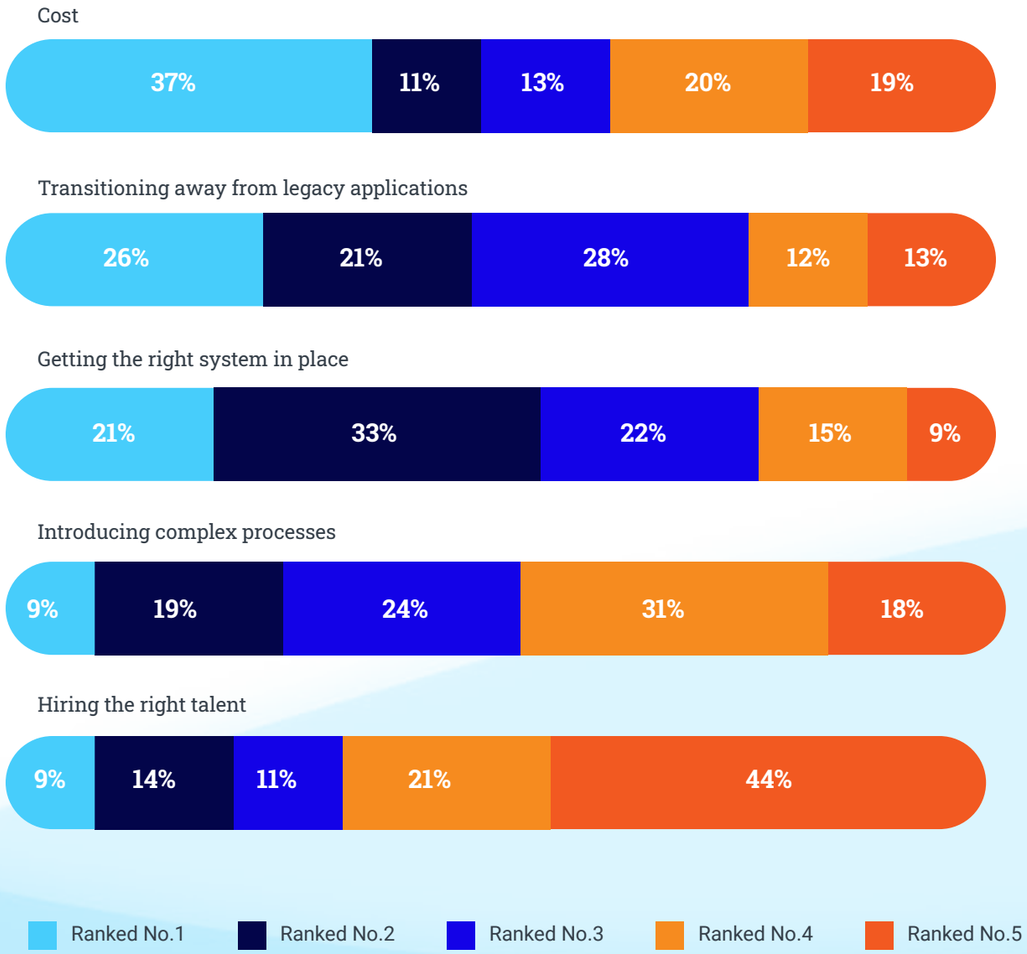
TODAY, WHAT DO YOU SEE AS THE BIGGEST SECURITY CHALLENGES?

In the not very distant past, data security was viewed primarily through the lens of IT — as a problem that required a technology solution — and that has changed. Today we know that our data protection is only as strong as the weakest link, and the weakest link is usually human. It is now widely understood that a strong security culture is as necessary to preventing data loss or a data breach as the right technology. The two strategies must work together to be effective.

We learned that cost is the number one perceived barrier to overcoming the aforesaid security challenges in pursuit of better outcomes, but it is closely followed by transitioning away from legacy applications.

A demonstrated ability to keep client data secure is clearly the most desirable position for law firms, given the risks and client concerns. But building a world-class security infrastructure, internally from scratch, is cost-prohibitive, and most firms lack the time and resources to do so, making finding and implementing the right systems all the more critical. With the threat of a cyberattack looming, firms of all sizes are taking a closer look at enterprise-level cloud architecture — where security is built in, along with the resources, skills, and the cutting-edge technology to deliver a secure working environment 24/7.

WHAT DO YOU SEE AS THE BIGGEST CHALLENGES IN IMPROVING YOUR SECURITY PROGRAM?



MODELING A **STRONG SECURITY** POSTURE

A strong security posture conveys an untarnished reputation and says to clients "We take data security seriously, and these are the measures we've taken and the environment we've cultivated to back that up." What does our survey say is the most effective way to model this to clients?

The best approach, according to our respondents, is establishing clear processes for preventing, identifying, and responding to security incidents, as well as using proven applications with advanced security features. This strategy implies working with vendors who stay on top of the latest threats, which was the third highest-rated response.

WHAT ARE THE BEST WAYS A LAW FIRM CAN DEMONSTRATE TO CLIENTS THAT IT TAKES DATA SECURITY SERIOUSLY AND HAS THE RIGHT MEASURES AND CULTURE TO PROTECT THEIR INFORMATION?

Rating scale: 1 (of minimal importance) to 5 (of great importance)

Although certifications were not specifically addressed in the survey questions, people brought them up in the free response areas, citing independent standards certification, ISO certification, and "knowledge and mention of security levels." This highlights the weight that independent or third-party assessments can carry in demonstrating a strong security posture to existing and prospective clients, and the value of choosing vendors and platforms that have them.

Certifications prove that a vendor adheres to a set of standards and best practices that ensure measures are up-to-date and effective. World-class vendors hold specific security certifications so your law firm can comply with various regulations and industry standards. These potentially include but are not limited to:

- **ISO 27001**
- **SOC 2**
- **CSA STAR**
- **PCI-DSS**

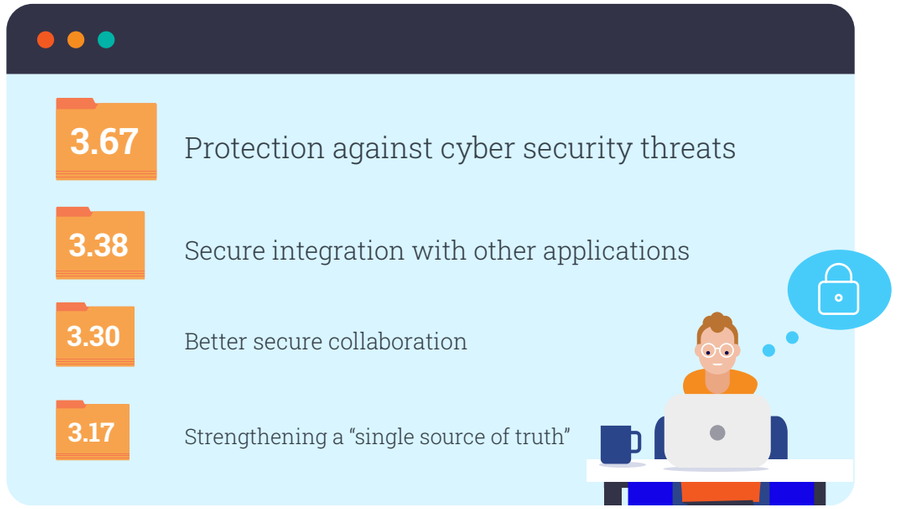
What do survey participants say about applications that can (or should) provide needed security for the firm?

THE CRITICAL ROLE OF **THE DMS**

Knowing how important client and matter information is, law firms have high expectations of their DMS to provide security against external threats, and the survey bore that out. Integrations with other apps are also welcome, with "better secure collaboration" and "strengthening a single source of truth" running a close third and fourth.

THINKING ABOUT YOUR DOCUMENT MANAGEMENT SYSTEM OR CENTRAL REPOSITORY FOR DOCUMENTS AND EMAILS, WHAT SECURITY BENEFITS DO YOU VALUE MOST TODAY?

Rating scale: 1 (of minimal importance) to 5 (of great importance)



"**REINFORCEMENT IS THE SECRET SAUCE OF CHANGE MANAGEMENT.** It's all about mindset and educating the organization about what it is, why it's important, and cultivating a culture of change.

MELISSA SPEIDEL
DIRECTOR, BUSINESS TRANSFORMATION OFFICE & ENTERPRISE APPLICATION AND DEVELOPMENT, K&L GATES

DMS features appreciated by the respondents included an easy to use, centralized repository of knowledge — or single source of truth — as well as advanced security features to keep up with the latest threats, such as protection from phishing. Cited as a number one concern by 86 percent, secure internal and external file transfer is a must-have.

Respondents also preferred easy (painless and frictionless) integration with email and other software used daily. They advocated auditing and user behavior tracking, as well as governance for compliance with legal and regulatory standards. Plus, innovation to ensure ongoing improvement of capabilities and integrations.

With broad consensus that robust cybersecurity for documents is the objective, the partners/counsel, legal ops, and IT roles agreed that organizational resistance is the biggest barrier to moving the needle forward.

How can firms counter this push-back?

It depends. Resistance to change comes in many forms and at many stages in an initiative. And while every firm is different, keeping people top-of-mind, rather than technology, throughout the process of change is a good place to start. That advice comes from one of your peers whose firm learned about the importance of change management the hard way. They lived to tell the tale — and to take a vastly different approach the next time around.

MAJOR HURDLES TO MORE ROBUST CYBERSECURITY FOR DOCUMENTS (RESPONSE BY FIRM ROLE)

	Partner or counsel	Solo practitioner	IT staff	Associate	Paralegal/ litigation support	Information security, compliance, or records management
Difficulty in choosing the right system	21%	42%	57%	50%	10%	0%
Personnel bandwidth/ resources	29%	26%	71%	50%	44%	33%
Costs to improve or replace existing systems	50%	37%	100%	50%	44%	67%
Inconvenience of remaining compliant	50%	58%	57%	50%	44%	67%
Difficulties with onboarding new systems	57%	47%	29%	50%	33%	67%
Organizational resistance to change	79%	53%	0%	50%	67%	33%

SET A HIGHER BAR ON SECURITY **WITH CLOUD**

Some respondents supported the view that cloud is more secure than on-premises technology with far less on-site management of resources. We also heard that cloud levels the playing field for small and mid-sized firms — particularly for those with 50 to 100 lawyers — and the conviction that cloud provides a competitive advantage leading to tangible business benefits. This is despite a widespread perception that larger organizations are better prepared to address security concerns.

Cloud-based applications built on an enterprise-grade cloud bring Zero Trust architecture for controlled access. Zero Trust architecture assumes that all users, devices, and networks are untrusted and must be verified before they can access data.

Controlled access is necessary to protect client and firm data. Look for:

- Military-grade authentication that requires users to prove their identity before they can access the data
- Two-factor authentication that adds an extra layer of security by requiring users to provide two pieces of evidence that they are who they say they are
- Authorizations that determine levels of access for each user
- Advanced encryption that ensures only authorized users can view the data
- Restricted access to the vendor's facility with surveillance and alarms
- Disaster prevention

Disaster prevention involves additional practices such as:

- Penetration testing
- Methods to prevent data co-mingling in a multi-tenant environment
- Virtualization or containerization for additional security layers
- Regular data backup and recovery procedures to protect against data loss and accidental deletion.

"**CLOUD-BASED iMANAGE** is ahead of the game as most on-prem versions of software are no longer innovated at the same pace as cloud versions.

IT STAFF
51-100 LAW FIRM

THE TANGIBLE BENEFITS OF AN ENHANCED SECURITY POSTURE

Law firms frequently cite security as a primary incentive for moving to the cloud with iManage. Adopting the latest cloud technology reduces the need to hire additional security SMEs, allowing firms to improve their security posture without the challenge of hiring the right talent, while simultaneously making security costs easier to manage.

Law firms of all sizes see tangible business benefits in strengthening their security, but smaller firms in particular view cost and hiring the right talent as limiting factors.

An advanced, highly secure document management system is a critical component of any law firm's tech stack. High-level security alleviates clients' concerns about their information being protected, turning an advanced security posture into a competitive advantage.

iMANAGE

iManage is the knowledge work platform that helps organizations to uncover and activate the knowledge that exists in their business content and communications. By leveraging the context of information and data, iManage goes beyond basic productivity, empowering data-driven insight that drives successful business decisions and outcomes.

Visit www.imanage.com to learn more.

ABOUT ABOVE THE LAW

Above the Law takes a behind-the-scenes look at the world of law. We provide news and insights about the profession's most colorful personalities and powerful institutions, as well as original commentary on breaking legal developments.

iManage

Making knowledge work

Law firms of all sizes can implement an advanced, highly secure DMS and experience the benefits of moving to the cloud with iManage Work 10 in the Cloud.

To learn more about iManage Work 10 or the iManage Cloud, visit our website.

twitter.com/imanageinc

youtube.com/imanage

linkedin.com/company/imanage

www.imanage.com