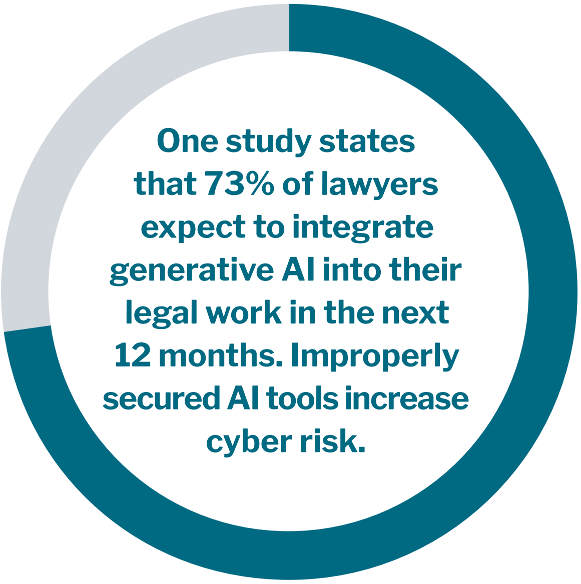
# Ensuring IT Continuity and Security in Law Firms

## A Strategic Guide to Mitigating Cyber Risks and Strengthening Operational Resilience

Small and midsize law firms handle highly sensitive data, but they don't typically have specialized IT and security people on staff. IT and security tasks may be done by lawyers, paralegals and business administrators. As a result, cyber defenses may be weak and employees likely aren't trained to be cyber-aware. Fundamental security mistakes leave law firms vulnerable to threat actors who use common, unsophisticated tactics to exploit security weaknesses.

This paper describes cyber risks specific to law firms, the key components of an IT continuity and security strategy and insights into proactive cybersecurity measures designed to combat modern cyber risks.



One study states that 73% of lawyers expect to integrate generative AI into their legal work in the next 12 months. Improperly secured AI tools increase cyber risk.

## Challenges to IT Continuity

Disruption of normal operations can lead to reputational damage, financial loss and compliance violations. Preserving IT continuity begins with awareness of the leading causes of disruption: cyber risks and operational complexity.

### Cyber Risks Facing Law Firms

Law firms are targeted because they manage sensitive client data such as competitive business information, intellectual property and financial information. Social engineering attacks, such as phishing, are the most common method used by threat actors to exploit security weaknesses in small and midsize law firms.

The top cyber risks include:

### Ransomware

Attackers encrypt case files, legal records and communications, potentially halting firm operations and causing significant disruption. Ransomware locks firms out of their data.

### Business Email Compromise (BEC)

Attackers create emails that impersonate attorneys or clients, leading to fraudulent transactions or unauthorized data access.

### Insider Threats

Disgruntled employees or compromised accounts leak confidential information.

### Data Breaches

Unauthorized access exposes confidential client records and trade secrets.

### Compliance Challenges

Legal ethics and client confidentiality standards require robust security measures, but many firms lack formal security policies and procedures.

### Cyber Insurance

Many law firms have cyber insurance, but policy language can be difficult to understand and audit results difficult to interpret. As a result, there may be gaps in coverage or basic security controls aren't implemented.

## Notable Law Firm Breaches

**Houser, LLP** – Houser was the victim of ransomware that compromised 1.5 terabytes of data, including tax IDs, financial information and medical information.

**Genova Burns LLC** – Uber drivers were notified by this law firm that sensitive data, including names and Social Security numbers, was stolen. Attackers used malicious search engine optimization techniques to lure potential victims to malicious sites, which then used malware to compromise users' machines.

## Signs of a Business Email Compromise BEC Attack

- Simultaneous logins by an individual from different geographic regions.
- Creation of unexpected email rules, such as auto-forwarding to external addresses.
- Requests for wire transfers or account changes that deviate from standard procedures.
- Unusual changes to authentication settings, such as new devices or updated MFA methods.

## Operational Complexity: Managing Virtual Desktops, Applications and IT Workflows

Law firms rely on an IT ecosystem consisting of virtual desktops, cloud applications and legal practice management software. The ecosystem's complexity is compounded by the rate of technology change, the barrage of novel threats, the use of multiple clouds and hybrid work environments. The complexities of technology, combined with resource constraints and lack of expertise, can lead to oversights or mistakes in areas such as:

- Updating software, patching vulnerabilities and securing multiple endpoints.
- Understanding attacker tactics, prioritizing security decisions and taking action in a timely manner.
- Securing hybrid and remote workers that rely on home PCs, Wi-Fi and internet connections.
- Responding to unique compliance audits and requests from clients. Audits and requests lack a common language, and compliance standards vary.
- Understanding cyber insurance report language and recommendations and implementing appropriate security controls.

## State Privacy Laws

In 2024 and 2025, state privacy laws have taken effect in Washington, Nevada, California, Florida, Oregon, Texas, Montana, Maryland, Connecticut, Delaware, Iowa, Nebraska and New Hampshire. Later this year, new laws in Tennessee, Minnesota and Maryland will roll out.

## Cloud Versus On-Premises Considerations

Many law firms operate with hybrid IT work models that include cloud applications like Microsoft 365 and on-premises systems. Cloud adoption is increasing, but firms sometimes misunderstand cloud security benefits. AWS and Microsoft Azure, for example, offer superior security and compliance capabilities compared to in-office servers and other on-premises equipment.

Firms that use the cloud are familiar with the advantages of managed cloud solutions:

- Improved scalability and redundancy without capital expense.
- Built-in security features like encryption and access control.
- Easier compliance with industry standards. Cloud providers are compliant with data protection standards, for example, whereas servers in single offices may not be. In the cloud, firms know where their data is stored, and how it's protected by redundancy across multiple physical data centers.

# Building a Resilient IT Continuity and Security Strategy

The combination of risk reduction, an information security plan and a disaster recovery/business continuity (DR/BC) plan boosts a firm's ability to recover quickly from an operational interruption.

## A Risk-Reduction Starting Point: Security Fundamentals

Improving IT continuity and security doesn't have to be onerous, depending on a firm's approach to reducing risk. Some firms first schedule risk assessments to identify vulnerabilities in applications, endpoints and networks, and go from there. Other firms begin reducing risk and improving resilience immediately by implementing certain security fundamentals recommended for all law firms:

### Multi-Factor Authentication (MFA)

Two or more forms of verification are required to allow access to a system or account boosts security well beyond passwords. MFA is a non-negotiable requirement for cyber insurance.

## Tips for Assessing Cyber Insurance Reports

- Understand the scope of the report, including systems, processes and assets.
- Evaluate how the report describes and evaluates risk in categories of severity, likelihood and potential impacts such as financial loss, loss of productivity and reputational damage.
- Validate the analysis of vulnerabilities in systems, applications and operational processes.
- Determine to what extent the report aligns the firm's security practices with applicable regulations and industry standards.
- Review the recommendations, which ideally are prioritized, for clarity and specificity.

## Extended Detection and Response (XDR)

XDR is a comprehensive security solution that unifies disparate security technologies to provide greater visibility and a more complete understanding of threats. By correlating telemetry from across your environment, XDR applies AI and machine learning to detect anomalies, identify patterns and reduce noise—helping security teams focus on real threats rather than isolated alerts. It strengthens proactive threat defense by integrating threat intelligence, automating response actions and guiding recovery efforts. Additionally, XDR enhances threat hunting, forensic analysis and compliance by delivering deeper insights and a more cohesive security approach.

### End-User Training and Phishing Testing

Continual education raises user awareness and is a front line of defense in preventing user-related breaches. Many, if not most, attacks on law firms begin with an email. Educated users know when to be suspicious.

### Email Security

A robust email security solution includes anti-spam, anti-virus, anti-spoofing, and other anti-threat capabilities such as advanced filtering and BEC protection.

### Least Privilege Access

This security best practice restricts each user's permissions to those necessary to do their job. Limiting access reduces the risk of unauthorized access and related fallout.

### Endpoint Detection and Response (EDR) Managed Detection and Response (MDR)

The latest EDR/MDR solutions leverage AI and machine learning (ML) as they continually monitor cell phones, desktops, laptops and other endpoints and remediate threats before they spread.

## Extended Detection and Response (XDR)

- Simultaneous logins by an individual from different geographic regions.
- Creation of unexpected email rules, such as auto-forwarding to external addresses.
- Requests for wire transfers or account changes that deviate from standard procedures.
- Unusual changes to authentication settings, such as new devices or updated MFA methods.

## Information Security Planning

A written information security plan (WISP) covers the who, what, where, when and how of IT continuity and security. The plan describes roles and responsibilities, incident response protocols and compliance activities. An up-to-date plan satisfies compliance audit requests, eliminating time-consuming, one-off responses. Core plan elements include:

- **Critical Systems –** Determine which systems are critical for legal operations and prioritize them based on criticality. Accounting, document management and email systems usually top the list. In the event of unexpected downtime or breach, everyone knows where to focus their efforts to get the business up and running swiftly with the least amount of disruption.

- **Policies and Procedures** – Write policies and procedures for the processes that are essential to running the firm. For example:
    - Employee onboarding policies and procedures cover background checks, the process for granting access to systems, requirements for security awareness training and more. Define acceptable use to spell out the do's and don'ts of smart cyber use of technology.
    - Security incident response policies and procedures cover tools, training, alerts, threat containment and other aspects of response.
- **Cybersecurity Controls** – Identify and evaluate controls for endpoint protection, network protection, user access and so on. An inventory of security controls provides insights into security posture, which is a focus of cyber insurance providers and IT/cloud-managed services providers. Standards such as the Center for Internet Security (CIS) and NIST are useful yardsticks. Additionally, cyber insurance providers have lists of required and/or recommended controls.

### Disaster Recovery and Business Continuity (DR/BC) Planning

Many law firms do not have a formal DR/BC plan, yet client audits may request one. DR/BC plans describe what your firm will do when something bad happens. Critical systems are the priority focus, because getting them up and running as soon as possible speeds recovery.

**DR planning** relates to protecting and/or recovering critical applications and data. Cloud-based data backups are considered more secure than on-premises alternatives.

**BC planning** relates to the processes that will be sustained during and after a disaster—such as a cyberattack, power outage, IT downtime or other event—and describes the associated risk management activities and incident response actions. Other components of a DR/BC plan are:

- A communications strategy that describes how to keep employees, clients and suppliers informed.
- An emergency management team that coordinates all aspects of the DR/BC plan.
- Regular plan testing and updates to ensure that employees are prepared.

## Proactive Cybersecurity: Moving from Defense to Detection and Response

The use of reactive-only security measures is no longer effective in combating cyber risks. Continuous threat monitoring is recommended for law firms of all sizes as a proactive cybersecurity measure. EDR, MDR and XDR detect and remediate threats before they escalate.

Most security tools operate independently, and the alerts they provide are hindsight. Some threats are undetected for weeks or months and move throughout

a firm, exploiting security gaps. Zero-day vulnerabilities—previously unknown flaws that attackers exploit before a fix is available—pose an even greater challenge, as traditional security tools struggle to detect them in real time. Meanwhile, threat actors continuously refine their tactics, uncovering new vulnerabilities and often outpacing the capabilities of on-premises security tools.

## How Extended Detection and Response (XDR) Enhances Security

XDR enhances threat detection and response by continuously monitoring endpoints, network devices, servers, email and cloud environments. It centralizes, integrates and analyzes threat data from all monitored sources using AI and ML. By providing a unified view of security events on a dashboard, XDR makes it easy to understand the firm's entire security picture. Key XDR capabilities include:

- Threat intelligence and behavior-based detection that stops ransomware and phishing attacks.
- Automated response capabilities that isolate compromised systems and prevent further spread.
- Actionable security insights that help firms continuously improve their defenses.

## Cyberattack Scenarios: What Legal Firms Should Prepare For

Understanding the potential impact of cyberattacks can help firms prioritize security investments and mitigation strategies.

### SCENARIO 1 Ransomware Locks Access to Case Files

**What happens:** A ransomware attack halts operations and puts client confidentiality at risk.

**How to prevent ransomware:** Proactive threat monitoring detects unusual file encryption activity early, isolating the infected endpoint before the attack spreads. Regular data backups and a tested disaster recovery plan ensure quick restoration without paying a ransom.

### SCENARIO 2 Business Email Compromise (BEC) Results in Financial Loss

**What happens:** A managing partner unknowingly authorizes a fraudulent wire transfer after falling for a phishing email. The email spoofs the managing partner's address or gets into a managing partner's email box and sends an email to an assistant who doesn't question it or think twice about following instructions.

**How to prevent BEC:** Regular employee training helps staff recognize phishing attempts before engaging with an email. Multi-factor authentication and financial verification protocols validate bank accounts, active status and account owners. A good rule of thumb is never to transfer money without verbal confirmation from the sender. Taking extra precautions with sensitive assets reduces the risk of unauthorized transactions.

### SCENARIO 3 On-Premises Server Failure Causes Downtime

**What happens:** A firm's on-premises server experiences a hardware failure, causing significant downtime.

**How to avoid this risk:** Cloud-based virtual desktops provide built-in redundancy, minimizing disruptions and allowing attorneys to securely access files from anywhere. An IT continuity and security plan describes transition steps in case of hardware failures.

## Focus Efforts Where They Matter Most

Cybersecurity is a full-time responsibility that many law firms do not support with specialized internal resources. Consider working with a managed services provider (MSP) that specializes in the cloud to reduce complexity for law firm staff, save time and avoid missteps – all while strengthening operational resilience.

Whether firms operate in hybrid mode or full cloud mode, they should first implement security fundamentals before adding advanced solutions. A solid security foundation consists of practical, proven tools that reduce risk across endpoints, applications and networks.

Law firms build resilience in different ways, but recommended activities include:

- Risk assessments to identify security vulnerabilities.
- Information security planning.
- Disaster recovery and business continuity planning.
- XDR implementation to bolster continuous threat monitoring and automated response.
- Ongoing cybersecurity awareness training and phishing testing for users.

### An Evaluation Checklist for MSPs and Cloud Platforms

- ✓ Support for all users and specified applications with all server infrastructure within a cloud environment.
- ✓ Centrally controlled hosted desktops and applications.
- ✓ Management of setup of and updates for specified applications.
- ✓ Workstation management, including patching.
- ✓ Multi-factor authentication.
- ✓ Email security with robust anti-threat features, advanced filtering and BEC protection.
- ✓ Security certifications such as SOC 2 and SSAE 18.
- ✓ Scalable data storage.
- ✓ End-user support, including phone, email and web issues, local printing, file copying, web browsing and other user activities.
- ✓ Managed cybersecurity for the hosted environment, including virus protection, firewalls and monitoring.
- ✓ Layered, encrypted backups that are kept in a location separate from active client data.
- ✓ Management and monitoring of all MSP-provided IT resources.
- ✓ Virtual private network (VPN) services.
- ✓ Security awareness training.

For over 35 years, **Afinety has exclusively served law firms**, providing specialized cybersecurity and IT solutions designed for the unique challenges of the legal industry. With deep expertise in securing legal IT environments, Afinety helps firms implement solutions like XDR for proactive threat detection, reduce risk and ensure compliance with evolving regulations.

## Not sure where to start with your firm's IT and security needs?

We're happy to talk through what makes sense.

TALK TO AN EXPERT

afinety

afinety.com

☎ 877.423.4638

linkedin.com/company/afinety