integreon

# The Complete Guide to Reducing Cyber Incident Response Costs in the Legal Industry

Helping Law Firms Strengthen their Cybersecurity Efforts

# Guide Overview

When it comes to cyber attacks specifically within the legal industry, it is not a matter of if, but when. This guide is meant to help law firms better safeguard their data, fortify their systems, and mitigate the impact of cyber threats.

In our global, digital-first economy, cyber attacks are no longer isolated incidents targeting large organizations. They are a very real threat to businesses of all types and sizes, and law firms are a common target of cyber criminals. What often gets underestimated is the cost of recovering from a cyber attack. The financial, operational, and long-term costs can be staggering and, in many cases, business-ending. This guide aims to help law firms minimize cyber incident response costs and the impact on their companies.

The **American Bar Association (ABA)** reports that 42% of law firms with 100 or more employees have experienced a data breach. It is not difficult to see why law firms are often a target for cyber crime.
The information collected by firms – from trade secrets, intellectual property, merger and acquisition details to personally identifiable information and attorney-client-privileged data – is particularly attractive to cyber criminals.

The cost of these attacks? For all organizations, it is the highest it has ever been. An **IBM report** found the global average cost of a data breach in 2024 was $4.8 million – a 10% increase over last year and the highest total ever. For professional services organizations (including legal, accounting, and consulting firms), the cost of a data breach is even higher, totaling $5.08 million.

The guide is organized into two sections:

**Best Practices: Cyber Incident Prevention**

**Best Practices: Controlling Cyber Incident Response Costs**

integreon

# Best Practices: Cyber Incident Prevention

## Firmwide Best Practices

**The best way to reduce the cost of cyberattacks is to prevent them from occurring in the first place.** There are several ways to strengthen your firm's defense against threats, companywide.

- Control network access by establishing clear permissions and limiting entry points to critical systems. The security boundary should be as small and as controlled as practical to minimize the attack surface available to hackers.
- Setting up firewalls to act as a first line of defense can block unauthorized access and help monitor incoming and outgoing traffic.
- Using multifactor authentication (MFA) adds an extra layer of protection. This requires users to validate their identity through a second source, such as a code or biometric scan.
- Network segmentation enhances security by dividing the network into smaller sections, helping to contain potential breaches and minimize damage.
- Active threat intelligence and regular vulnerability scanning ensures that your firm stays ahead of emerging risks.

*"Defending against cyber threats requires a highly collaborative approach, involving not just a select few cybersecurity professionals, but everyone across the organization. Ultimately, companies must rely on humans acting responsibly and maintaining vigilance."*

***- John Wei, CTO, Integreon***

*While a free service, the ABA reports only 54% of firms have MFA in use*

## Employee Best Practices

According to **Verizon's 2025 Data Breach Investigations Report**, 68% of all breaches involve human error, from phishing clicks to misconfigured security settings. Employees must be educated in how to maintain good digital hygiene. Here are just a few important habits that should be included in your new hire onboarding and ongoing employee education efforts.

- Avoid reusing passwords across multiple accounts to minimize the risk of unauthorized access.
- Limit device access to only trusted individuals. Sharing devices with others can expose sensitive information.
- Use only secure Wi-Fi networks to help prevent potential security breaches and unauthorized access to personal and other data.
- Report any suspicious email activity as phishing emails can be extremely sophisticated. According to an **FBI report**, cybercriminals stole approximately $2.9 billion through business email compromise (BEC) scams, with law firms among the most common targets.

### LAW FIRMS WITH POLICIES IN PLACE TO GOVERN EMPLOYEE BEHAVIOR

- 55% – email use
- 51% – internet use
- 50% – computer acceptable use
- 50% – remote access
- 44% – social media

(source: ABA)

Further recommended reading: **Cybersecurity, Wire Fraud, and Attorney Liability: The Growing Risk Landscape**

## Detection and Response Automation Best Practices

Detection and response automation is revolutionizing how firms address cybersecurity threats.

Security Information and Event Management (SIEM) platforms can monitor and analyze log data from various systems. These systems detect suspicious activity in real time and allow teams to quickly mitigate risks.

- Automated incident response tools take this a step further by eliminating the delays that come with manual intervention. If a threat is detected, these tools can immediately isolate compromised systems, block malicious traffic, or trigger other predefined actions to contain and neutralize the risk.
- Machine learning-based security solutions further enhance detection capabilities, leveraging AI to identify advanced threats and anomalies. These systems learn over time, adapting to the normal behavior of a network and flagging deviations that could indicate a breach.

***$2.2 million***

*That's how much AI-driven security automation saves companies per breach by cutting response times and improving containment.*

(source: IBM report)

integreon

# Best Practices: Controlling Cyber Incident Response Costs

Back to the **IBM study** reporting that the cost of a data breach is the highest it has ever been – 75% of the increase is due to the cost of lost business and post-breach response activities.

The lesson? Investing in post-breach response preparedness can help dramatically lower breach costs. Below we break down five things law firms should do now to best recover from a cyber incident.

### 1. Have a cyber incident response plan

A cyber incident response plan (CIRP) can help prepare, guide, and protect a firm during and after a cyber incident. According to a report by **Ponemon Institute**, companies without a formal CIRP pay 58% more per breach compared to those with structured, tested response protocols.

All CIRP plans should include the following efforts:

- Define the purpose of the plan and the types of cyber incidents it covers (data breaches, ransomware, phishing attacks, etc.).
- Define the roles and responsibilities of the team, including internal members (IT, PR, HR, etc.) and external partners like cybersecurity consultants.
- Establish criteria for categorizing incidents by severity and impact.
- Develop a framework for how to identify and report potential incidents (monitoring tools, employee reporting procedures, etc.).
- Outline step-by-step procedures to contain, eradicate, and recover from an incident, including specific protocols for different types of incidents.
- Define internal and external communication strategies during an incident, including templates for notifying stakeholders, clients, and regulatory bodies.
- Address regulatory requirements (GDPR, CCPA, etc.) for reporting incidents and preserving evidence.
- Outline steps to restore systems and data to normal operations, including a post-incident review process to identify lessons learned and improve the plan.
- Detail regular training programs for employees and the incident response team. Include simulated tabletop exercises to test the plan.
- List the tools, technologies, and resources in use across the firm (firewalls, SIEM systems, etc.).
- Define a schedule for reviewing and updating the plan to ensure it remains current with evolving threats and organizational changes.

*Only 34% of law firms have an incident response plan in place. (source: ABA report)*

integreon

### 2. Outline clear data management processes

Effective data management begins with establishing clear and streamlined processes. Start by decluttering your data collection methods. This ensures you are only gathering what is necessary. Excessive or irrelevant data can slow down operations and inflate storage costs unnecessarily.

By focusing on quality over quantity, you can classify and track data more efficiently, maintaining an organized system that allows for faster access and better decision-making.

### 3. Encourage cross-team collaboration

Cross-team collaboration is another critical component of robust data management. Encouraging your firm's IT and InfoSec teams to work closely ensures data security and infrastructure remain top priorities throughout the management process. Legal and communications teams should also be engaged regularly to align with compliance standards and maintain transparency.

By breaking down silos and fostering collaboration, businesses can create a unified approach to data management that minimizes risks.

### 4. Purchase a comprehensive cyber insurance policy

Understanding Cyber Insurance Coverage is an essential component of a viable Cyber Incident Response Plan.

When doing your pre-purchase research, look for coverage for breach response, data restoration, privacy breach notification costs, and data privacy litigation coverage, which some cyber policies offer "Outside the Aggregate Limit" breach response coverage which preserves the policy aggregate limit for class action litigation and other high exposure risk profiles.

### 5. Follow correct data mining protocols

Today there is an increased threat of data breach class actions. In fact, according to the **Duane Morris Class Action Review - 2025**, plaintiffs filed more data breach class actions in 2024 than in any other year, doubling the number filed in 2022.

Effective data mining plays a central role in managing regulatory and litigation risk. The goal is to identify exactly what data was accessed or exfiltrated, no more and no less. To support that, it is essential to:

- Limit the data population by engaging a forensic partner to isolate the impacted data set. This helps reduce scope, cost, and downstream exposure.
- Work closely with breach counsel to ensure compliance with regulatory requirements, such as GDPR and state-level breach notification laws, and to ensure the overall response is legally sound.
- Leverage targeted data mining workflows to quickly identify affected individuals and data types, and document the methodology to support later scrutiny.
- Maintain transparency and ethical rigor throughout the process, especially when interpreting results that could have real-world consequences for affected individuals.

While data mining costs can vary depending on data quality, volume, and complexity, there are proven ways to bring greater cost control and predictability:

- Use advanced culling and pre-processing to reduce the review set before manual analysis begins.
- Secure fixed per-document pricing for the manual review phase to avoid budget overruns.
- Partner with a vendor known for delivering high-quality, defensible work. A well-executed initial pass can eliminate costly rework and reduce the risk of notification errors that may trigger additional liability.

In today's litigation-heavy climate, an unfocused or poorly executed data mining effort is a liability. Performing it diligently by following the steps outlined above is one of the most effective ways to limit future risk exposure.

Today, law firms must invest in both protecting themselves against cyber crime and preparing for an inevitable attack. These recommendations serve as a starting point for developing a solid strategy, but it is most important to see these as moving targets. As technology innovation accelerates, law firms will need to continuously adapt.

For guidance on how to best futureproof your law firm against cyber threats, reach out to the Integreon team at **info@integreon.com**.

integreon

Integreon is a trusted provider of legal and business outsourced services to corporations and law firms worldwide. Through our global delivery centers, we provid expert support for a range of legal, compliance, creative design, and administrative needs, with a proven ability to transform our clients' business performance.

+1 866-312-7023 info@integreon.com

© 2025 Integreon, Inc. or all of its affiliates. All rights reserved.