Make Sure Your Firm's Cybersecurity Insurance Policy Stays Active — and Enforceable

KSHITIIJ KATHURRIA
Chief Strategy and Innovation Officer
iManage

Cybersecurity breaches have become an all-too-common occurrence at all types of businesses, including law firms. Many firms have cybersecurity insurance, but they don't realize they can lose their policy if they do not maintain compliance with its requirements.

As executive managers of the firm, legal administrators are ideally positioned to ensure the firm stays compliant with its cybersecurity insurance policies so they are active and enforceable. Here are 10 ways to make sure your firm's cybersecurity insurance doesn't lapse.

> "Often, risks come from blind spots — areas no one realized were problematic until a breach occurred. Conducting a risk assessment involves uncovering problematic areas and fixing them proactively."

1. Understand the Firm's Technology Infrastructure

Every law firm's IT infrastructure is unique, so securing the firm sufficiently requires a detailed examination of several areas of protection. Some of the firm's technology may be on-premise, traditional desktop hardware and software, while other applications are self-hosted or in the public cloud. The firm has a network and endpoints (desktops, servers) which need to be secured. Lock down user access to both the network and endpoints as well as key applications. Protect against email attacks with email threat protection, encryption and archiving.

2. Conduct a Risk Assessment

Often, risks come from blind spots — areas no one realized were problematic until a breach occurred. Conducting a risk assessment involves uncovering problematic areas and fixing them proactively. Perhaps the firm has passwords — for users or administrators — that never expire. Or the firm owns risky applications that make them vulnerable to

exploitation. Are those applications essential, or could they be replaced with a more secure alternative? Acknowledging these security risks and eliminating them before they cause a crisis simply makes sense.

3. Devise a Business Continuity and Disaster Recovery Strategy

The odds are in favor of the firm facing at least one cybersecurity breach, if not more. Therefore, devising a business continuity and disaster recovery strategy will provide a roadmap the firm can follow if a breach occurs. Business continuity and disaster recovery plans are also helpful in the wake of natural disasters, power outages, health crises or other emergency situations.

4. Develop an Incident Response Plan

When a cybersecurity incident occurs, in the heat of that moment is not the time to make an incident response plan. Instead, create the plan preemptively in calm circumstances. The plan should clearly state how the firm will respond to a cybersecurity incident, step-by-step, and which departments will be involved — all in compliance with the firm's cybersecurity insurance policy.

Some questions your plan should answer:

- Once the security incident is detected, who investigates it?
- When and how does the problem get escalated to the firm's top management?
- When are law enforcement agencies engaged?
- How will the situation be stopped as soon as possible?
- How will it be communicated to the firm's people, its clients, third-party contacts and the public at large?

5. Train Staff to Build Security Awareness

The firm's staff is its greatest asset but also its largest potential liability because human beings make mistakes. Phishing emails, a typical security breach source, have become incredibly convincing and sophisticated, sometimes even tricking IT professionals to give up passwords and sensitive data. Make sure the firm's employees receive specific training regarding cybersecurity risks like phishing to build awareness of existing threats and reduce the chance of user error leading to a breach.

6. Ensure Use of Modern Malware Defense Tools

Some law firms have their own dedicated IT staff, while others rely on systems integration/IT consulting companies to provide technology services.

Regardless of which approach the firm takes, ensure the firm's IT professionals are on board with deploying sufficient malware defense tools. This can include tools such as Next-Generation Antivirus (NGAV), which guards against many threats including malware, viruses and ransomware; Endpoint Detection and Response (EDR), which protects devices from malware threats; and Managed Detection Response (MDR), a security-as-a-service offering which provides resources to help the firm protect itself from cyber threats.

7. Rigorously Adhere to Penetration Testing Schedules

Regular penetration testing allows the firm to discover its vulnerabilities and security holes before bad actors exploit them. Therefore, setting a schedule for penetration testing and adhering to it faithfully is an essential element of cybersecurity maintenance.

8. Encryption Across the Board

Encrypting all emails and documents across the board will go a long way to contributing to the firm's cybersecurity success. Certainly, encryption may have its downsides due to inconvenience, but it is sound business practice to encrypt all communications and documents passing through the firm.

9. Multifactor Authentication

Setting up multifactor authentication is one of the best strategies for firms to prevent unauthorized users from accessing firm email and documents. Users may complain it

is annoying for them to verify their logins on a smartphone or other device. However, this momentary irritation is a small price to pay for the tremendous security benefits multi-factor authentication brings to the firm.

10. Establish Privileged Access Management and Role-based Access Control

Cybersecurity insurance companies are increasingly requiring that companies establish privileged access management and role-based access controls. Firms may like the idea of everyone having access to everything, but this is often not a wise approach. By restricting access to certain information based on roles and access rights, the firm upholds its internal security requirements including attorney/client privilege and government compliance regulations.

By following the 10 steps above, legal administrators can help their firms ward off cybersecurity risks and ensure their cybersecurity insurance policies are active and enforceable.

NEED A BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN? WE'VE GOT A WHITE PAPER FOR THAT

Step 3 above notes the importance of planning for unplanned incidents, such as a cyberattack. If your firm doesn't have a plan in place, *"Business Resiliency: 7 Steps to Successful Incident Management, Business Continuity and Disaster Recovery Planning"* can help you formally put together an action plan for such an event. Download your copy at *alanet.org/whitepapers.*

ABOUT THE AUTHOR

Kshitiij Kathurria is Chief Information Security Officer at Afinety, a managed cloud and IT services provider for law firms.

Kshitij.Kathuria@netgaincloud.com

linkedin.com/in/kshitijkathuria