Consilio / ADVANCED LEARNING INSTITUTE

Consilio Institute: Practice Guide

SIX DATA PROTECTION STRATEGIES FOR LEGAL TEAMS: MITIGATING RISK, MAINTAINING REPUTATION

Consilio Institute: Practice Guide

SIX DATA PROTECTION STRATEGIES FOR LEGAL TEAMS: MITIGATING RISK, MAINTAINING REPUTATION

TABLE OF CONTENTS

Disclaimers

The information provided in this publication does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this publication are provided for general informational purposes only. While efforts to provide the most recently available information were made, information in this publication may not constitute the most up-to-date legal or other information.This publication contains links to third-party websites. Such links are only for the convenience of the reader; Consilio does not recommend or endorse the contents of the third-party sites.

Readers of this publication should contact their attorney to obtain advice with respect to any particular legal matter. No reader of this publication should act or refrain from acting on the basis of information in this publication– without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation.

Use of this publication, or any of the links or resources contained within, does not create an attorney-client relationship between the reader and the author or Consilio. All liability with respect to actions taken or not taken based on the contents of this publication is expressly disclaimed. The content of this publication is provided "as is." No representations are made that the content is error-free.

SIX DATA PROTECTION STRATEGIES FOR LEGAL TEAMS: MITIGATING RISK, MAINTAINING REPUTATION

No organization is immune from cyber incidents. Although helpful, minimalist data protection practices are often not enough to save organizations from costly data loss and embarrassing reputational damage. Law firms are not immune, either: according to Mandiant, a division of FireEye, 80 of the 100 biggest law firms in the U.S. have been hacked since 2011.

Legal practitioners have real responsibility when it comes to protecting their organizations and their clients from potentially disastrous data breaches, and every day that legal teams don't put proper cyber plans in place, the potential for disaster looms.

Here are six strategies for mitigating the risk of cyber incidents in your organization:

Strategy 1:

Get a Bird's Eye View of Your Entire Operation, Then Fix It

- Is your firm or legal department adequately prepared for a data breach?
- What tools and test protocols do you have in place to protect your data?
- Have you educated your lawyers, associates, and teams to manage data properly? What about your front-line employees?
- If you have already had a data breach, how did you recover from it?
- Are your teams, service providers, and security experts providing effective protection?
- Do you have cyber insurance?

If you don't have the answers to these questions, it's best to work on setting up this basic operational strategy right away. Then take a deeper dive. The best place to start is to know exactly what systems are being used in your organization, what they are used for, and who controls them and keeps the data on them safe. Many organizations have hired outside experts who specialize in data protection to review their internal practices and suggest safety measures.

Strategy 2:

Expand Educational Efforts

Cybersecurity begins in-house and touches every team and every employee. Educating staff with continual, effective data management best practices is the best defense available. For example, teaching employees to spot and quarantine phishing email scams is a simple but eye-opening way to increase data protection. Many information security teams

52% of all security breaches result from human error

"Trends in Information Security," CompTIA 2015

test protocols with fake email blasts to give real-world training examples to employees. This trains them to "pause before opening" potentially harmful emails or attachments — thus making it second nature for each person in an organization to be a more responsible data consumer.

Also, crafting and distributing security policies and procedures, along with the penalties for disobeying them, help show employees how serious your management team is about protecting client data. An effective information security policy should list current practices, protocols, and employee rules for handling all types of client information.

A security policy should cover all data channels, from frequently used apps like email, voicemail, text messages, and internet browsers, to the more technical such as personal computer and workstation network connections, locking and storing laptops, securing mobile phones/devices, managing and changing passwords, remote access codes, and logins to wi-fi networks. Your policies should be open and clear about how your legal team collects, transmits, maintains, and stores data and what the risks are for poor data management. Reviewing, updating, and enforcing your organization's policies on data and how it's managed is your responsibility to your clients.

Strategy 3:

Implement the Best Cyber Tools Available

Legal teams and information security personnel should work closely together to lock out hackers and intruders as much as possible before any crisis occurs. One simple step is to ensure effective malware protection is installed on every device the organization uses. Then, add stronger defense tools that provide comprehensive protection across all your platforms and cloud services. It's important to add tools that give complete visibility into your multiplatform environment that unify Security Information and Event Management (SIEM) and Extended Detection and Response (XDR).

Review your processes for blocking potential security threats and tackling information security such as patch management, virus protection, firewall configuration, and web and email gateway monitoring. It can be expensive to maintain up-to-date tools for the highest level of protection, but the costs of losing reputation and trust because of a data breach are always far higher. It's best to look at what is working, what isn't working, and what could be improved, removed, or left alone.

> Consider also the need to **bring third parties into the planning process.** Outside vendors, or those with insight into your networks, **may be impacted** by your data breach.

Strategy 4:

Invest in Good Cyber Insurance

Cybersecurity experts agree that cyber insurance is a must for all legal entities. And the more the better. It's key to really understand what your insurance policy covers, what are the retentions, what panel counsel to use, and how to immediately receive breach counseling if an issue occurs.

Another good practice around insurance is to predetermine or engage forensic investigators before an issue occurs. Having them in place makes reacting to a breach much easier, and their engagement can be covered under insurance.

Implementing strong security controls helps stay ahead of cybercrime, unintentional breaches, bad actions, ransomware, and viruses.

Strategy 5:

Have a Crisis Scenario/Recovery Plan Ready to Go

Don't get caught in a data breach situation without having a detailed plan to lean on. You want to make sure IT and legal teams work in sync throughout the process. The plan needs concrete information about who will manage each phase of the crisis, from locking down servers and reviewing logs, to interviewing IT employees to managing communications with stakeholders.

Consider also the need to bring third parties into the planning process. Outside vendors, or those with insight into your networks, may be impacted by your data breach (or you by theirs). Third parties can include vendors, service providers, clients, and others.

Ensure your vendors and service providers also have disaster recovery plans in place, and make sure they provide them to you on a regular basis. It's important to stay on top of vendor relationships and to add regular due diligence testing protocols into your crisis plan. Vendors should know that your organization will require regular security audits, penetration testing, review of logs, etc., as part of your crisis scenario.

Your recovery plan document is only as good as the information inside it, so be sure to review it regularly to ensure it fits your growing organization.

Also, be sure to provide all detail about which employees, experts, and leaders are in charge of each plan step. That way, no one is waiting for instructions during a crisis. Set up regular check-in meetings to be sure everyone is kept informed during the crucial first 72 hours of a crisis.

Strategy 6:

Provide Comfort to Clients and Customers Wherever Possible

With data breaches and cybercrime on the rise, it's important for you to know what your ethical, regulatory, and legal responsibilities are to your clients, customers, partners, and employees — as well as any reporting requirements to regulatory agencies. Client data your organization maintains should be classified by the type it is: personal, financial, general, etc. Specific security controls should be placed around each type of data, how it is kept and for how long, how it is used, and why it is needed.

The need for data security protection only increases as large-scale breaches become standard day-to-day occurrences. Implementing strong security controls helps stay ahead of cybercrime, unintentional breaches, bad actions, ransomware, and viruses. The keys to maintaining control include vigilance, open-ended communication, and using the latest tools that prevent data loss.

RECOVERING FROM A DATA BREACH

If your organization experiences a data breach, you must take immediate action. Here are some steps that the Federal Trade Commission (FTC) suggests taking to help alleviate future issues:

1. **Lock down your operations immediately.**
   - Prepare/launch a team of internal and external experts in security
   - Take affected servers offline
   - Restrict access to areas where a breach may have occurred
   - Speak to outside counsel who specialize in data breaches to determine liability
   - Do not destroy evidence — but remove any hacked information from your website or public social media accounts
2. **Fix vulnerable areas.**
   - Consider changing service providers
   - Review all computer network setups, policies, and current protection plans
3. **Communicate with clients, law enforcement, employees, and stakeholders.**
   - Contact law enforcement as soon as possible
   - Know your jurisdiction's regulations for contacting clients and corporate stakeholders