Cyber Threat Response Kit: A Practical Guide for California Law Firms

It might start with a subtle intrusion — perhaps an email that looks legitimate or some malware that goes unnoticed — but before long, your IT infrastructure grinds to a halt, leaving you unable to access important documents, email accounts or case files.

It almost doesn't bear thinking about. But think about it you must, as law firms (and many of their clients) are prime targets for cyberattacks due to the sensitive data they manage.

More than just a technical problem, a cyberattack is a full-scale crisis that affects every aspect of operations, from client relationships to compliance and even the stability of the business. Small and midsize firms, in particular, face the added challenge of having fewer resources to dedicate to security measures.

As with any crisis, a proactive plan prepared during quieter moments is infinitely more effective than scrambling for a solution in the heat of the moment. This downloadable guide will help your firm defend itself and its clients against cyber threats, respond to incidents and ensure compliance with California regulations.

1 How secure is the data you're storing?

No matter the industry, any organization that collects, processes or uses personal information should implement a security plan to ensure its protection. And according to various regulations, enforcement precedents and state and federal laws, this plan must generally be reasonable, appropriate and adequate.

Start by identifying which digital and physical data your firm possesses that needs to be protected, such as information related to employees, clients, health, finances and case files. Compile a list of all the places this data lives, including computer networks, external devices, storage systems, archives and data processing applications. Don't overlook employees' personal devices, as they often contain both law firm and client data.

Next, conduct an audit to reveal vulnerabilities. Asking the following questions for each data source will help you recognize the potential for unauthorized access, alteration, loss, compromise, theft or destruction:

- How does the data come into the firm's possession, or how is it created?
- Where does the firm keep the data?
- How is the data secured?
- Under what circumstances and through which channels does the data leave the firm, and how is it deleted per its document retention policy?

This step can highlight gaps or weaknesses in your policies for document retention or destruction.

For each threat you identify, consider:

- What is the probability of it happening?
- What would be the impact if it does?
- Are the current policies, procedures and safeguards enough to mitigate this threat?

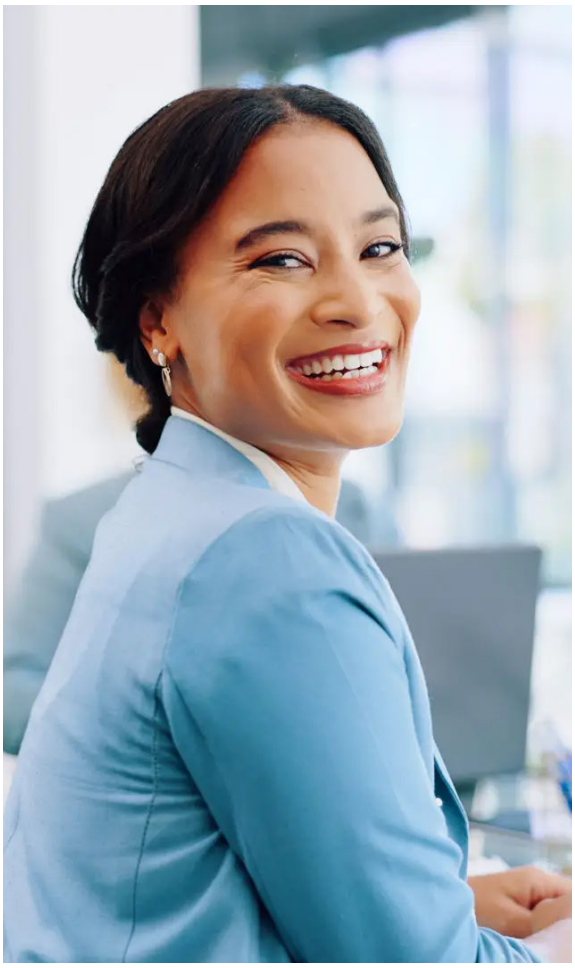
CEB

2 What should be included in your cybersecurity plan?

Now that you've identified the risks, it's time to draft your policies and procedures. While a robust security plan will require input from various departments, you should empower at least one person to oversee its development and implementation, along with regular quality control and updates.

Stick with plain language in these documents to be sure everyone can understand, no matter their level of technical awareness. Also, ensure the policies and procedures conform with the firm's broader objectives and operations to avoid confusion or conflict. It's important to include clear information on disciplinary actions or sanctions for noncompliance.

Your plan should explain what actions will be taken and how policies will be followed to protect data. These measures should match the type of data, the risks it faces and how likely a security issue will happen. CEB's cybersecurity explainer includes a detailed chart connecting specific security measures with their corresponding laws, regulations and guidance.



CEB

Security measures generally fall into three categories:

Physical measures

These are designed to protect the organization's physical computer system and IT networks, such as servers, terminals with access to the system, storage devices and other physical equipment or access points. Different measures might be needed to protect data that is in storage from data that is in transit.

Examples include:

- Procedures limiting physical access to electronic information systems and workstations
- Controls on the removal of hardware or electronic media
- Locks and keys on filing cabinets

Technical measures

These security safeguards are incorporated into computer hardware, software and related devices to ensure system availability, authenticate people seeking access, maintain confidentiality and protect the integrity of information stored on or communicated through the system.

Examples include:

- Encryption
- Firewalls
- Antivirus software
- Password and two-factor authentication policies
- Intrusion detection procedures
- Measures to ensure data integrity and confidentiality
- Data encryption for all client communications
- Remote work protocols to secure off-site access
- Regular updates on security patches and software

Administrative measures

These include the policies and procedures underpinning physical and technical security, addressing issues like access to data and contingency planning such as disaster recovery. This may involve the use of audits and a security incident response plan.

Once complete, update your firm's employee handbook with the new cybersecurity plan and require signed acknowledgements from all relevant employees to confirm their receipt and understanding. You might also find that many aspects of the plan could apply to other emergencies, such as an earthquake or fire, so consider integrating those protocols for a more comprehensive response strategy.

3 Have you reviewed all third-party vendors' security measures?

Every relationship with a third-party service provider can expose your firm to potential security risks, so it's important to conduct thorough due diligence before hiring providers to ensure they can safeguard personal data and meet security obligations.

Consider including clauses in your contracts requiring the third party to have the following data security measures in place before you engage them:

- Implement safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the data it creates, receives, maintains or transmits on the firm's behalf.
- Prohibit or control the use of subcontractors.
- Report any security incident it becomes aware of and discipline or terminate the personnel causing or involved in the breach.
- Ensure its policies, procedures and contract-required documentation are accessible for the firm to audit.
- Authorize the firm to terminate the contract if the third party has violated a material term.

4 Are you educating your team?

As the first line of defense, your attorneys and staff must be well-prepared to recognize potential risks. Equip them with the knowledge to avoid cyber threats by regularly communicating security policies and updates through ongoing training sessions and clear, accessible guidelines. Provide the policy in writing, require employees to acknowledge receipt, and host mandatory training sessions and unpack common issues such as phishing and social engineering.

While the serious consequences of security incidents may necessitate disciplinary measures, you might wish to allow anonymous reporting in some instances to ensure attorneys and staff feel safe sharing concerns without fear of retribution.

CEB®

5 Are you incident-ready?

This is the part we hope you never need! Your incident-response plan should outline all the measures that your firm or client will take in the aftermath of a breach, along with relevant information for devising a comprehensive strategy.

Your incident response plan should include:

- Names and emergency contact information of the security response team responsible for technical, legal and communications management
- A clear chain of command for decision-making during a crisis
- Criteria for identifying an incident that triggers a security breach notice requirement and information about breach detection systems
- Information about notification procedures, including who should be notified, the method and timing of delivery and a sample notification letter
- Name and contact information of police, FBI, U.S. Secret Service and detective agencies
- Plans for notifying regulators and credit reporting agencies if a large number of people are affected
- A communication plan, including sample letters to affected individuals, plans for a company statement and a press release. If you work with a PR agency, they can likely provide you with guidance and and will be a trusted ally should an incident occur

6 Which California data privacy laws apply?

Depending on the nature and extent of the cyberattack on your firm or client, various data privacy laws may come into play, including the California Consumer Privacy Act (CCPA) for California residents, the General Data Protection Regulation (GDPR) for EU residents and the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data.

California's security breach disclosure law under Civil Code section 1798.82 requires businesses with personal information about California residents to inform them if their unencrypted personal information may have been accessed by someone without permission. It applies to any person or business that conducts business in the state and owns or licenses computerized data with certain personal information about California residents.

To qualify as a breach under California law, the incident must involve the unauthorized acquisition of computerized data that compromised the security, confidentiality or integrity of personal information. Public information available in government records does not apply.

If the data is encrypted, you might not need to notify people about a security breach. But if someone gains unauthorized access to both the encrypted personal information and the key or password needed to unlock it, the business must inform the affected individuals. This is true if the business has reason to believe the key or password could allow someone to read or use the personal information. If personal information is acquired in good faith — such as to update a customer database or check a client's account status at their request — that doesn't constitute a breach.

If a breach has occurred, you must give notice of it in writing via a notification letter. Emails, online notices or press releases aren't enough to meet compliance requirements unless you can demonstrate that the breach requires notice to more than 5,000,000 California residents, that sending individual notices would cost more than $250,000 or that you don't have enough information to contact each person directly. When one breach affects more than 500 residents, it must be reported to the California Attorney General.

See CEB's practice guide for a sample security breach notification and more information on rules and penalties.

Depending on the firm's clientele and regions served, other state-specific laws might impose notification requirements and penalties for breaches. Ensure your firm knows how to handle data breaches within the framework of these regulations to avoid fines and liability.

7 Consider obtaining cyber insurance

As the risk and potential damage of cyberattacks become more prevalent, having an insurance policy in place can help cover financial losses and liabilities. However, premiums are rising due to increased losses, and many insurers set lower coverage limits to minimize their risk. Policies also tend to have many exclusions, especially for large-scale events like acts of war, and some insurers restrict coverage for critical industries. So, if you encounter any vague language as you review coverage offers, be sure to clarify and negotiate those with the provider.

Cyber insurance policies generally cover:

- Costs incurred for remediation in response to a cyber incident
- Expenses related to ransomware attacks, including ransom payments
- Loss of income and expenses exceeding normal operations as a result of a cyberattack
- Liability arising out of claims arising from the data loss or breach
- This may include defense and judgment or settlement costs for liability over a failure to properly maintain personal or corporate data or violation of privacy rights
- Independent contractors and business associates (i.e., outsources or vendors) who process the insured's data
- Fines or penalties imposed by law or regulation, including costs associated with investigating, defending and paying for or settling regulatory actions
- Additional payment card industry (PCI) fines and penalties, including forensic services investigating noncompliance with PCI standards

The Federal Trade Commission (FTC) also recommends obtaining coverage that includes:

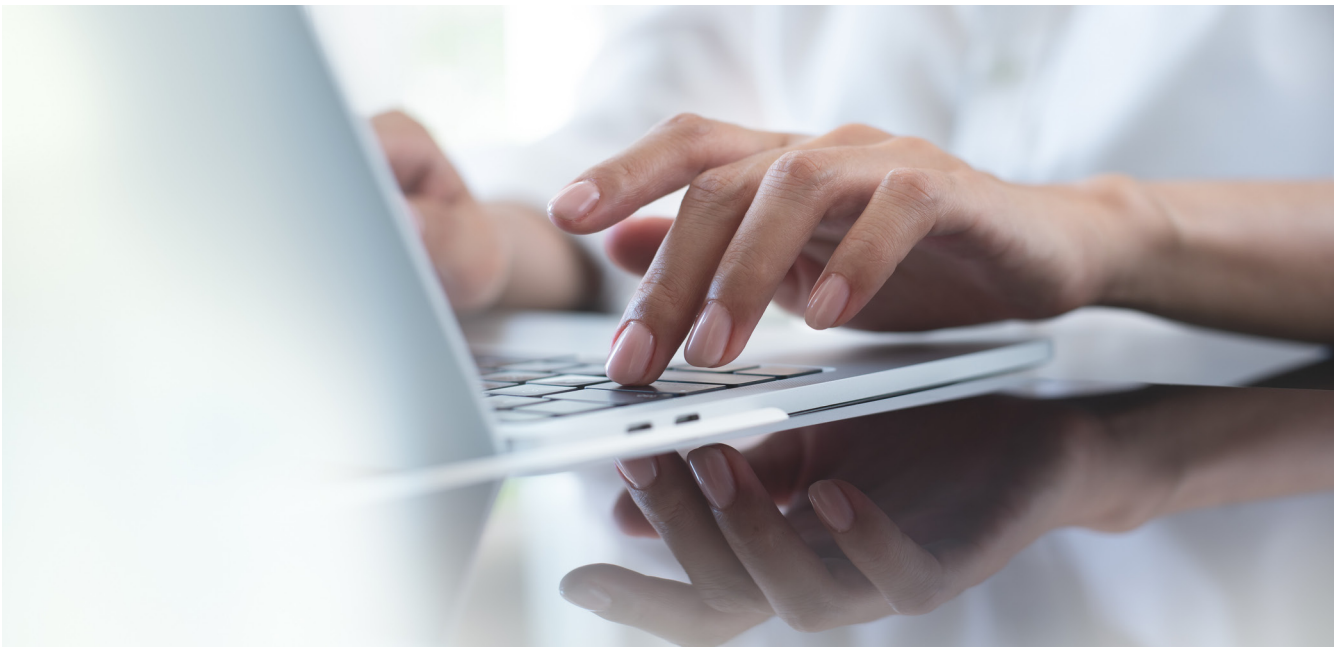
- Cyber attacks that occur anywhere in the world
- Terrorist acts
- Duty to defend
- Coverage in excess of any other applicable insurance policy the company may already have
- A breach hotline available at all times and year-round
- Third-party coverage that includes losses for defamation, copyright or trademark infringement, other costs related to litigation and accounting costs

8 Conduct regular audits, tests and updates

As your business and technology evolve, so should your risk assessments. Regularly reviewing and updating your security measures ensures they remain effective against new threats and vulnerabilities, helping you stay ahead of potential cyberattacks.

These tests can range from sending test "phishing" emails to employees to contracting a third party to evaluate compliance with your security protocols. It's also a good idea to check *DailyNews* regularly for relevant updates.

While we hope you never have to implement your incident response plan, getting ready now will minimize any damage and disruption if the worst happens. Having a clear, well-rehearsed plan in place can reduce downtime, safeguard your most sensitive data and demonstrate compliance for clients and regulators.



Find out how CEB can guide your cyber threat decision-making by scheduling a demo.

CEB

Contact us at 1-800-232-3444 or visit us online to learn more.

CEB is a registered trademark of Continuing Education of the Bar - California (CEB). © The Regents of the University of California, 2024. All rights reserved.