McGOWAN
Program Administrators

Protect Your Law Firm with a Cyber Risk Management Plan

Attorneys and law firms are prime targets for cyberattacks due to the confidential information they safeguard on behalf of their clients. Such data may include financial details, trade secrets, or even personal information like medical records or social security numbers. And yet, many law firms are unprepared to defend against a cyberattack and have no response plan in place.

The incidence of cybercrime continues to climb year after year, and firms face dire consequences from lack of preparation—high financial costs, diminished reputation, and exposure to malpractice suits, to name a few.

By outlining a risk management plan and selecting an appropriate cybersecurity insurance policy for support, you can mitigate the threat of security breaches.

Assessing risk with a data audit

According to a recent opinion by the American Bar Association (ABA), cyberattacks are an imminent threat to law firms. But how vulnerable is your firm? Performing a data audit enables you to account for the flow of sensitive data and pinpoint where the most significant weaknesses lie and how to address them.

During a data audit, you will gain valuable insight into what data is stored, how it is stored and protected, and who has access. You will also learn what information third-party vendors have access to, how they use it, and most importantly, how they protect it.

It is advisable to work with an outside cybersecurity firm to achieve this. However, you can conduct an independent data audit. Begin with a list of questions:

- How is sensitive data collected?
- How is sensitive data stored?
- How is data protected?
- Who has access to it?
- Where are the potential weaknesses?
- Are all my passwords secure?
- How are passwords stored and remembered?
- How are mobile devices and laptops secured?

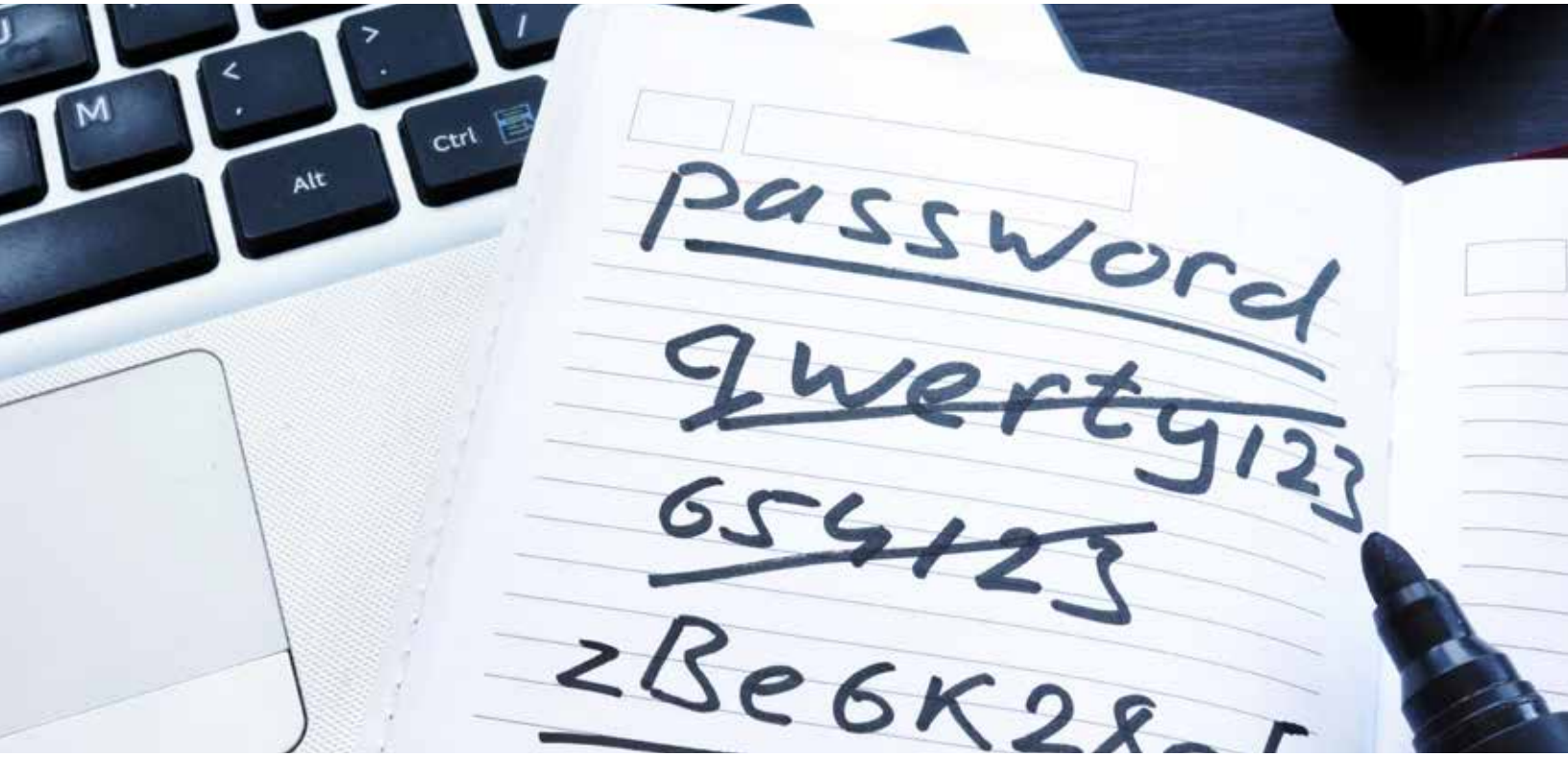
Once you have a clear idea of potential threats and weaknesses, it is time to devise a plan.

Creating a cyberattack response plan

Drawing up the response plan involves thinking through every aspect of a hypothetical data leak. Here are some general best practices outlined by the ABA to get you started. Once you have the basics down, you can tailor your plan to your firm's unique needs.

- **Containment:** Once a breach is discovered, the most urgent priority is to isolate the exposed systems to prevent further exposure and the spread of viruses or malware to other networks.
- **Audit:** Assess the damage and the extent of the breach to determine what data may have been exposed and ensure that no other systems have been affected.
- **Purge:** Completely delete any files that may have been affected by the breach.
- **Log details:** Make detailed notes about the attack. These notes may be used as evidence in court.
- **Public Notice:** ABA states that the law firm must notify affected parties promptly after a data breach.
- **Contact Police:** Inform authorities as soon as feasibly possible. The same attack may also target other firms or businesses.
- **Recovery:** The ABA recommends developing an in-depth recovery plan. Clearly define employee roles during the recovery phase. Efficiency and speed are crucial to minimizing damage and returning operations to normal.
- **Lessons Learned:** Conduct an "after-action review" with your team. Delve into what went well and what should be improved.
- **Update:** Continuously improve your systems and update the cyberattack response plan based on lessons learned.

Once you have outlined your response plan, the next step is ensuring that the firm's employees understand and implement the plan.



Creating a culture of cyber responsibility

It is essential to foster a culture of cyber responsibility at your firm.

Ideally, firm employees are involved in conducting the data audit, creating the response plan, and having clear ideas of how to implement the plan. Regardless of department, all firm employees should be made aware of the plan and how to implement it. Procedures should be reviewed regularly–monthly at first, and then quarterly as your staff becomes familiar with the plan.

Continue to foster cyber responsibility by investing in IT training for staff. This can ensure that your employees are knowledgeable about current trends and threats in cybersecurity. Cybercriminals are constantly evolving new techniques and becoming more sophisticated.

Another critical strategy is stressing every day "cyber hygiene." Examples include enforcing secure passwords, encrypting data, and regularly updating software.

Disaster recovery plan vs. cyberattack recovery plan

A disaster recovery plan may also be helpful in the aftermath of a breach. While both disaster recovery plans and cyber recovery plans aim to help a law firm return to normal operations after a cyberattack, the focus of each is slightly different.

- **Disaster recovery plans** prioritize continuity of business operations in the event of an attack.
- **Cyber recovery plans** revolve around data management and defending against future attacks.

A firm can successfully recover from a cyberattack without a disaster recovery plan, but it's recommended that you have both in place.

How cyber insurance can help

A cyberattack or data breach is an inevitability at a law firm. How prepared is your firm? By following the tips in this guide, your firm can mitigate much of the risk. Unfortunately, there is no guaranteed way to prevent a cyberattack.

Having the right cyber insurance plan offsets risk and the costs of recovering from a cyberattack. McGowan Program Administrators Lawyers Professional Liability Insurance provides reliable coverage for cyberattack-related expenses such as the cost of notifying clients of a breach, computer forensics, and defense costs if civil suits are filed as a result of a data breach.

Are you ready to improve your law firm's safeguards against cybercrime? Contact McGowan today to get started.

McGOWAN
Program Administrators

Contact us:

McGowan Program Administrators
20595 Lorain Road
Fairview Park, OH 44126

Jason M. Adams | National Production Underwriter – Lawyers Professional Liability Program
Email: jmadams@mcgowanprograms.com | Phone: 800-545-1538 x3682 | Cell: 440-829-3233

www.McGowanPrograms.com