Data breaches, ransomware and cyber theft should be top-of-mind concerns today for any business. The loss of confidential data can carry a heavy cost, including immediate financial losses, damage to the company's reputation, and exposure to potentially expensive civil litigation.

In the past year, Equifax, Intercontinental Hotels Group, Saks Fifth Avenue, Chipotle, Verizon, Yahoo, Uber and dozens of other high-profile companies were victimized by cyber-attacks.

Today, almost any company or professional firm can be victimized by online criminals looking for easy money. In fact, law and accounting firms are attractive targets because they are involved with escrow accounts, financial settlements and highly confidential matters.
Last year, we were able to prevent a cyber theft involving a wire transfer. After settling a case on behalf of our client, we were expecting to see a large sum deposited in our trust account. When the money didn't arrive, we realized that something was wrong. A hacker had penetrated the sender's network and obtained a copy of the letter notifying our firm about when the funds would be transmitted. The thieves had opened a fraudulent bank account using a similar name, instructed the sender to redirect the money to them and the money was wired to this fraudulent account. Because we insisted on speaking directly with the sender before and after the funds were wired, we were able to successfully intercept the theft and avoid any loss.

In this process we confirmed that because fax messages are analog, not digital, they can actually be more secure than emails or texts. Sometimes a common-sense approach is crucial to foiling the attempted cyber fraud.

Take a team approach

South Florida businesses and professional firms should make cyber security a top priority in their risk management programs. Failure to do so will expose the business to the costs of a data breach, ransomware attack or diverted funds and can go far beyond the immediate losses. A successful cyber attack can disrupt the business, damage customer confidence and lead to expensive litigation, regulatory fines and penalties.
Ideally, cyber security requires a team approach. An information technology (IT) professional should advise on the steps you may need to take to protect your network and digital, mobile and social communication channels. An operational executive can balance those security measures with the need to keep the business operating smoothly and efficiently. A human resources professional can educate and inform employees about safety practices and the changing nature of cyber threats. Most importantly your attorney should also be part of your team to advise on the legal and regulatory aspects of cyber security and data privacy actions. For instance, data breaches of personal information must be reported. Sensitive or secured information, including theft of trade secrets must be reported to regulatory agencies and to shareholders.

Multinationals doing business in other countries may face additional reporting requirements, such as the European Union's new General Data Protection Regulation (GDPR). After May 25, when GDPR

enforcement begins, violations can lead to fines of up to 20 million euros or 4 percent of the company's total worldwide annual turnover in the preceding financial year.

In the U.S., healthcare organizations, banks, credit card companies and other financial service providers may also be subject to legal consequences if personal data on patients, customers or members is compromised.

Law and accounting firms also have a duty to report cyber attacks to The Florida Bar, in keeping with the goal of protecting clients' financial and personal information against hackers. However, some firms have invested more in cyber security measures than others, and clients should discuss this issue with their attorneys. After all, no one wants to see the confidential details of a case or settlement on a public website.

Use best practices

Here are some other best practices, based on our firm's knowledge and experience that can to help reduce your cyber security risks.

- Conduct a cyber security assessment or a formal audit at least once a year. As the old saying goes, "Expect the best, but plan for the worst."
- Focus your security resources on the high-risk areas for your organization, which could range from network configuration to employee training.
- Keep investing in in-house security measures, including firewalls, intrusion detection applications and real-time monitoring.
- Keep patching and updating your operating systems, since outdated software is a favorite avenue for a cyber-attack.
- Protect connected sensors, devices or equipment – the Internet of things (IoT) – from hackers.
- Keep secure backups regularly as a safeguard against a ransomware attack. If someone locks down your system, you can rebuild your network without paying criminals in another country.
- Document your security actions every step of the way. This is vital if you find yourself facing a lawsuit or a regulatory action after a cyber-attack.
- Evaluate your need for cyber insurance. Weigh the cost of coverage versus your potential exposure, and be sure to read the fine print to see what the insurer covers and what might be excluded.
- Consider using an IT services provider to manage your network and data. Outsourcing your security can be a cost-effective strategy for mitigating risk, but ask to see its security policies and practices, and review these documents with your attorney.

Finally, have an attorney review the "fine print" on IT contracts, so you understand who is responsible for data security, and what actions both parties need to take in the event of a data breach or theft. Be prepared for a crisis, and hope those plans never need to be put into action.

Andrew C. Hall is the founder and managing partner of Hall, Lamb, Hall & Leto, P.A., a Miami-based law firm specializing in complex corporate, business, and securities litigation. The firm can be contacted at 2665 S. Bayshore Dr., PH 1 Miami, FL 33133 (305) 374-5030 www.hlhlawfirm.com