You’ve heard about major cyber attacks on big consumer-facing businesses like Equifax, Target and HBO. As a leader of a professional services firm, you’re thankful you don’t have to worry about ransomware attacks and other cyber crimes. After all, your brand is not in the public spotlight, so you really aren’t a target for cyber criminals.

Right?

Wrong.

Research shows that no business is safe from cyber attacks; these crimes happen to both small and large firms. This means that no matter how buttoned up or under the radar you think your organization is, it is susceptible.

For professional services firms—which typically have mountains of sensitive, highly confidential data—a cyber security breach can be crushing. Think of the information maintained by financial institutions, law firms, architects, engineers or accountants.

For example, a number of high profile law firms have had their systems breached: DLA Piper\(^1\), Cravath Swain & Moore and Weil Gotshal & Manges\(^2\), among others. Big Four consulting firm Deloitte acknowledged in September that it had come under attack by cyber criminals.\(^3\)

Some of these firms are still digging out from under the attack. In Deloitte’s case, as of this writing, they’re still trying to ascertain exactly what was compromised. This is the case more often than not. Determining what was compromised is a time-consuming and expensive undertaking.

While it’s true that these victimized firms are big brands and more frequently targeted by hackers, it’s also fair to say that they have stronger cyber security in place than smaller firms. While a mid-sized law firm or consulting practice might not be quite as asset rich or a target for criminals, the nature of the information these firms hold on their servers makes them enticing targets.

It’s unreasonable to expect a firm’s IT department to keep one step ahead of an entire universe of hackers.

In fact, there’s a strong likelihood that clients are already asking about the state of your cyber security
and your disaster recovery plan. When the breach comes, it is far reaching for every part of the organization. It begins with the initial financial punch in the gut. Consider that ransomware attacks—a type of malicious software designed to block access to a computer system until a sum of money is paid—have resulted in payouts of more than $25 million in ransoms over the last two years. There are also forensic costs to uncover what happened, the pain of business interruption and lost productivity, fees paid for legal advice and other consultants, and of course the significant work that must go in to managing reputation.

In many instances, this last factor—the public relations toll—can create the most long-term pain. The damage to the brand and disintegration of trust can be swift, and there’s no brushing this PR problem under the carpet—full disclosure is the only ethical and legal way forward, which means that everybody will know: clients, prospective clients and competitors. When a professional services firm loses the trust of its clients and others, it is hard to recover that faith.

Professional services firms have 1,000 points of vulnerability—from inadequate server protections to laptops left in taxicabs, employee resistance to updating passwords, to really smart people foolishly opening links in emails from unknown parties.

Your IT Department must do everything it can to repel cyber criminals, or at least to make it difficult enough so that the hackers move on to the next potential victim. But when all is said and done, there is only so much your IT team can do, and smart organizations have cyber insurance policies that will protect them for when the computer system is inevitably hacked.

---

3. [Deloitte](https://www2.deloitte.com), “Deloitte Statement on Cyber Incident”
4. [The Verge](https://www.theverge.com), “Ransomware victims have paid out more than $25 million, Google study finds”

For more information, please call [1.877.426.7779](tel:1.877.426.7779)