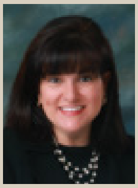

Colleen M. Capossela is the president of CATICPro, Inc., a sister company to CATIC, which offers a variety of insurance and bond products to the legal profession.

Cyber Security: A Necessary Focus

By Colleen M. Capossela

Data breaches, phishing schemes, wire transfer fraud schemes, theft of data, ransomware attacks…the list goes on. Cyberattacks are an everyday reality and a major business risk for any law firm. No longer can security initiatives be ignored with a cyberattack having the potential to devastate your business. There is no sugar coating this matter. If you have not done so already, you need to focus on establishing and implementing security initiatives, protocols, and plans for your operations.

Unfortunately, there are no patterns yet to suggest any one practice is more at risk than another, or that these intrusions focus on larger businesses as opposed to smaller. Some smaller business owners think they are less vulnerable; this is not the case. According to the 2016 State of SMB Cybersecurity report referenced in a recent CNBC article, it was estimated that approximately 50 percent of the small businesses identified had been breached over the past 12 months.[1] While large businesses have the additional resources to focus on cyber security, smaller businesses tend to focus their resources mostly on employees, office space, and health insurance.[2] However, businesses of *all* sizes are vulnerable and are experiencing harmful attacks.

Regardless of the size of your business, you need to determine if you are prepared for the potential significant adverse impact that a cyberattack could have on your firm. Depending on the type of cyberattack involved, the cost to your business could include, but not be limited to: losses due to business interruption, loss of business income, loss of client funds, restoration, re-creation and remediation costs, various expert fees, notification and credit monitoring expenses, ransom requests, public relations costs as well as damages to third parties, and regulatory fines and penalties. In addition, there are ethical concerns regarding disclosure or unauthorized access to client information and compliance with such rules as Rule 1.1 and Rule 1.6 and, of course, there is the concern of loss of good will and reputation.

With the increase in cyberattacks, more regulations are being implemented or modified and more protocols and controls are being put in place resulting in increased demands for attorneys to establish and implement security programs for their operations. Both on the federal and state level, the government is implementing new laws or regulations (or tweaking old ones), to meet public concerns regarding the security of their information. Clients and business partners or affiliates are requesting verification of security measures. Even corporate law departments are making demands on outside counsel. It was reported that the Association of Corporate Counsel released the first set of model cybersecurity practices that it recommends corporate legal departments have their outside counsel follow—and the practices are significant.[3] In-house attorneys had identified cyber security as extremely important and they wanted to be sure that their outside counsel was not the "weak link" regarding their cyber security initiatives.[4]

Given this information, *all* law firms, if they have not done so already, need to take action to mitigate their risks and make cyber security a priority.

There are a number of things that you will need to do to assist in minimizing your risks. The key is to take the time to evaluate your business, understand where you are most vulnerable, and implement strategies to reduce your weaknesses. You need to determine what measures make sense for your particular operations, and you need to put the time into analyzing your business and making it important.

To start, evaluate and understand, 1.) the roles and functions of your staff and work processes; 2.) your technology, equipment, software, and systems utilized; and 3.) the types of data you maintain, its life cycle, locations, and chain of custody. Bottom line, understand the detailed workings of your operations. Then meet with key security professionals to identify what systems, protocols, and procedures would be best to protect your operations. These professionals may include IT security support, forensic technology security specialists, a cyber security privacy attorney, and a cyber insurance carrier. Determine

what types of cyberattacks and intrusions your business is most likely to experience, understand what your obligations and responsibilities are to secure your operations as best you can, and build a security plan that best meets your needs.

Some basic suggestions[5] to consider in discussions with your security professionals when putting the firm's plan together may include:

Technical Measures

Including, but not limited to, implementing strong back-up systems and routinely testing back-up data, regularly updating and patching systems and software, such as installing and enabling the auto-update features in your computer's operating system, using intrusion protection and detection systems, installing anti-virus and anti-malware software as well as proper firewalls that are actively managed, employing encryption and two-factor (multifactor) authentication, and using Virtual Private Network (VPN) especially when connecting to an untrusted network.

Procedural/End User Measures

Including, but not limited to logging user activity; limiting user access; requiring strong, complicated passwords and establishing rules regarding use of passwords; establishing rules regarding use and access of your business systems (include restrictions on Internet use, free WiFi or free web-based e-mail accounts, downloading of random software off Internet, etc.); limiting information provided on social media and on the firm's website, especially job functions and descriptions. Also consider creating and implementing specific policies like a record retention policy, e-mail policy, and wire transfer policy, and creating and implementing an Incident Response Plan for the various intrusions that may impact your business so you know how you will respond if you experience a cyberattack.

Testing/Monitoring Measures

Make sure that what you have created and put in place is actually followed, continues to work, and is changed when needed. Be sure to periodically evaluate what you have put in place and modify when necessary. This is an evolving area, changing all the time, so you need to monitor the effectiveness of what's put in place regularly.

Education/Awareness/ Enforcement Measures

Make sure your employees understand how important security is to your operations and are aware of the dangers by providing regular training and education, and evaluating employees based on compliance. Make it important to your business and be sure to enforce it. All staff needs to help in fighting against a cyberattack. Hackers have turned to looking for ways to "hack people" (trick you or your staff), versus technology in order to access your systems or divert funds. They do this by way of phishing scams. Generally done by e-mail, these scams try to trick you or your employees into clicking on a link allowing access to your systems or transferring funds to a fraudster. Educate everyone in your operations and affiliated with your business on what to watch out for and the practices required to be implemented in your business; everyone in your firm, and working with your firm, needs to be vigilant.

In addition, be sure you have proper insurance coverage to help pay for the expenses and losses that may be incurred by the law firm—transfer some of the risk over to insurance. But remember, insurance is not a substitute for security measures. You still need to make best efforts to secure your operations and implement other risk management initiatives.

When considering insurance options, you may find your traditional policies (professional liability, malpractice, and comprehensive general liability) may not cover, or adequately cover, your losses related to a cyber incident. You may also find that coverage in a business owner's policy or "package policy," is a false sense of security. Reviewing your policies is key in order to reveal what is covered, and to identify exclusions, limitations, and gaps. After review, one may even find that separate cyber and crime policies are necessary. Both may be necessary, for example, because a cyber policy may not extend coverage for wire transfer fraud schemes, and a crime policy may not provide the first party and third-party coverages you are looking for in the event of a data breach.

To determine if you have the types and amount of coverages you want to satisfy your needs and your risk tolerance level, review what you have currently with an insurance professional familiar with cyber and crime coverages. Request a gap analysis. A number of carriers offer cyber and crime coverages, whether in separate policies, endorsements, or "package policies," but the devil is in the details. For example, cyber coverage varies from one provider to the next, and policy forms are not standardized. Crime coverage may not include wire transfer fraud schemes (social engineering or voluntary transfer coverages), unless you purchase a special social engineering endorsement. Make sure the policies you purchase cover the various losses that you anticipate will impact your business. Be sure the situations you are most concerned about are covered, understand the types of costs that are recoverable and to what extent, understand retroactive dates, and understand what terms, limits and sub-limits apply. More than ever you need to read all your policies, understand what you have, what you need, and what you are buying.

The number and variations of security issues and cyberattacks are on the rise; they are not going away. Every business needs to take action to manage its risks. Start by making cyber security risk management a necessary focus in your business. Give it the priority it needs and the resources necessary to manage your risks and sustain business continuity. **CL**

Notes

1. CNBC, Survey Monkey Survey, by Chris Morris, special to CNBC.com, *14 million US businesses are at risk of a hacker threat,* 7/25/17, https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html
2. *Id.*
3. Corporate Counsel, by C. Ryan Barber, *What Companies Can Demand From Law Firms on Data Security,* 3/29/2017, http://www.corpcounsel.com/id=1202782401474/What-Companies-Can-Demand-From-Law-Firms-on-Data-Security.
4. *Id.*
5. Contribution from Robert Jasek, Information Security Manager, CATIC.