THE DAILY RECORD

By: Commentary: Matthew A.S. Esworthy April 29, 2016

Earlier this spring, we learned one of the largest reported data breaches happened not to a government agency, large retailer or multinational corporation, but to an obscure Panamanian law firm. This should come as no surprise, given what we know about cybercrime today.

Professional firms – that is, law, accounting, and consulting firms – have become prime targets for two obvious reasons: 1) with relatively small technology budgets, they maintain weak defenses against intrusions; and 2) their networks contain highly valuable client information that may be used for any number of purposes – insider trading, extortion, or intellectual property theft, to name a few.

There should be no doubt about the threat: it is real, and sooner or later your firm will almost surely be attacked. Prior to the Panama Papers leak, the FBI issued a warning to the legal industry, encouraging firms to bolster their cyber-defenses, and news broke that 48 elite law firms had been targeted by Russian hackers. For months now, security experts have been warning professional firms that they must do more to secure client data.

What exactly should be done? The solution is not merely technological. It cannot be outsourced to a technology vendor. Nor can firms expect to prepare adequately by drafting a new privacy policy and filing it away. Today's pervasive cybersecurity threats demand a comprehensive data-security strategy that is supported and overseen by senior leadership and knowledgeable professionals.

Such a strategy incorporates many component parts, but here are seven basic steps for professional firms that find themselves unprepared:

1. **Involve senior leadership in communicating and enforcing data security policies.** Having partners and executives involved in the communication and enforcement of policy helps immeasurably. Those at the top of the organizational chart are in the best position to deliver the message that data security is a function of excellent client service.

To this end, senior leadership should establish a committee dedicated to data security planning. The committee should include partners as well as IT and administrative staff so that the lines of communication remain open. It can meet regularly to identify vulnerabilities, review and update policies, and discuss developments in cyber risk-management. Many organizations look to the National Institute of Standards and Technology standards as a starting point.

2. **Conduct periodic data-security training for all personnel and encourage basic cyber hygiene.** Training is a critical component of data security strategy. That's because today's threats often stem from human error rather than technological weakness.

Sophisticated hackers have learned that to get around the standard-issue defenses, they need to resort to insidious tactics, such as targeting specific professionals and placing fraudulent phone calls to secretaries in search of information. Intrusions can also take the form of employees or visitors removing sensitive documents, or an employee leaving a file in a café. These low-tech vulnerabilities can be just as troublesome as a hacker infiltrating a network from afar.

To mitigate such threats, firms can plan data-security training for the entire organization. Firms can also enforce measures such as frequently updating passwords, limiting the number of privileged users, making sure all employees update and patch software, regularly scanning for malicious activity and encrypting sensitive data.

3. **Identify sensitive assets.** Among the data-security committee's highest priorities should be identifying and locating the organization's most sensitive data. Who has access to that data? How is it now protected, is it encrypted and what changes should be made, if any? These questions will need to be asked and answered periodically as conditions within the organization change.

4. **Put your defenses to the test.** Given how swiftly threats evolve, professional firms should schedule regular assessments of their data security defenses. What form these assessments take will depend on the organization. For some a monthly scan of their systems for malware will suffice; others may want to enlist the help of a professional

to perform a penetration test. For law firms, penetration testing should always be handled very carefully so as to avoid jeopardizing the attorney-client privilege and work-product protection.

5. **Review third-party contracts.** Cyber audits should also consider a firm's relationships with various service providers, including other professional firms, contractors, and, especially, technology vendors. These third-parties often have access to valuable firm client data. Hence, firms should take reasonable steps to ensure that their providers are acting responsibly to protect their systems and data. In fact, the American Bar Association and the United States Treasury Department recently partnered together to tackle the issue of cyber representations and warranties for third party contracts.

6. **Create and implement an incident response plan.** Given how pervasive cybersecurity threats have become, firm IT departments and administrators should prepare for data breaches. Who will be notified if a breach occurs? How will the data be protected? Who will investigate the leak and how? Who is your law enforcement liaison? Firms can avoid confusion and costly mistakes if they take the time to plan in advance. Enlisting the help of an attorney to quarterback the incident response under the attorney-client privilege is a common approach taken by most large companies. Any plan should be tested to ensure that it works and that all essential players understand their responsibilities.

7. **Get cyber insurance.** Many companies are attempting to mitigate risk with cyber insurance. Notably, most insurers require their customers to engage in sound cyber practices to obtain a policy and coverage in the event of a data breach.

We can be confident that the Panama Papers leak will not be the last to embarrass a professional services firm. In the coming months, other firms will likely be forced to admit to breaches. With reasonable planning, however, any firm can meet today's data security challenges.

Matthew A.S. Esworthy, a partner at Shapiro Sher Guinot & Sandler, serves on the American Bar Association Cybersecurity Legal Task Force and is co-chair of the ABA Criminal Justice Section Cyber Crime Committee. He can be reached at mase@shapirosher.com.