Is 2017 the Year a Leak Sinks Your Firm?

A look into the future for the lessons learned from the "hack" of one major firm.

It was both literally and figuratively a dark and stormy night, at least according to the FBI forensics report. That pinpointed New Year's Eve as the moment when a vast trove of extremely sensitive data was stolen from the firm Krennic, Erso & Tarkin. While the office was quiet and closing, with most out celebrating the eagerly anticipated end of 2016, its servers were subjected to a sophisticated digital heist.

This was not the first time a law firm had experienced a security breach. But what happened next was indeed unprecedented.

First, came the cocky pronouncements from WikiLeaks. That they had obtained "the crown jewels" from an extremely prestigious law firm. That they planned to make tsunami-level waves, releasing information from clients including high-profile financial services firms, high-net-worth individuals, several lobbyist and political non-government organizations, and white-collar criminal defendants.

Further twisting the knife, WikiLeaks stressed that they would be releasing this data slowly, in a manner staged for "maximum impact," as per their stated policies. This was an unpredictable organization, but its agenda wasn't.

The media feeding frenzy that followed was expected. The chain of events that sparked, was not—the wholesale departure, first of clients, then associates, and then partners from the firm.

Whodunnit? And why?

Of course, it wasn't immediately clear what had happened, or why. So, rumors flew. Was it hacking by state actors, bent on continuing subversion of confidence in critical institutions? Or working to pilfer valuable IP for their own business community?

Was it an inside job by someone looking to engage in insider trading on public markets? Was it an associate or staff member, unhappy about firm policies, their bonus, or benefits, looking to do more than just grumble on the usual internal discussion forums? Was it someone with a political agenda, looking to "bring the system down" from within?

Or, most likely of all: Was it simply a horrible accident? A phishing email, accidentally and unwittingly clicked by a well-meaning but careless employee? The storm that started New Year's Eve is still spinning.

Clients are outraged: With multiple practice groups serving a range of individual and corporate clients, many are now frightened and up in arms. In 2016, the legal profession saw a class action lawsuit against a small firm accused of security negligence. And all signs point to something similar brewing here, but on a much larger scale.

Other firms are furious: This was no regional boutique; it had hundreds of lawyers and multiple offices, and it highlighted its professional and compliance capabilities. Now, peers are worried that the negative media coverage is tainting the reputation of the profession as a whole. It's already resulting in more demanding client RFPs and outside counsel guidelines, creating more work, overhead and risk for everyone.

Many calling for new rules: With state-level standards commonly based on ABA Model Rules, law firms have enjoyed a privileged status as a self-regulated profession. Now a chorus of advocates are calling for more uniform standards—covering not only security, but every aspect of professional practice—a potential Pandora's Box.

Lawyers are leaving: As noted, this particular ship in question is already taking on water. And lawyers leaving creates a negative feedback loop, and the end of a once proud and productive law firm.

This article was originally published in the December 2016 edition of LegalTech News.

The Post-Mortem

It took a few news cycles, a few rounds of FBI interviews, and a few closer looks at server logs for enough details to emerge to clarify the mystery. And the story was more complex than any single "gotcha" moment. In this case, a bad actor obtained the credentials of an administrative assistant serving a group of senior partners. Those partners had enough access to enough systems, resulting in extensive extraction of information.

The bad actor? Still unclear if it was someone within the firm, a spy dropping tainted USB drives in the parking lot or sneaking in the front door as the "new guy," or an international agent, virtually crossing continents.

As things settled down, it also became clear that the leak was far from a wholesale extraction of all client and firm data. Ironically, with some still feeling nervous about adopting cloud-based services, in this instance the cloud delivered the silver lining.

As many have highlighted, cloud providers are typically able and incentivized to invest more in information security and ongoing monitoring, as that's a required core competency. The net result is that firms benefit from stronger security protections. And, as it turns out in this instance, the firm was using a cloud-based document management system, with add-on confidentiality and audit software in place set to trip an alarm and lock access when unusual activity levels had been detected.

With the DMS triggered into lockdown mode, the perpetrator was limited to accessing on-premises systems. Unfortunately, the firm was extensively using network file shares for sensitive information and records. The digital assailant's stolen credentials provided broad access to those repositories, and enough damage was done.

Fight the Future:
Lessons and Learning

Predictably, 2017 became another "Year of Security," with tremendous focus on enhancing best practices and building even strong responses. The lessons learned included:

1. Investments in security are never complete. There's constant need to respond to evolving challenges and threats.
2. Prudent incident response planning should include approaches for addressing public and client relations fallout, should the worst occur.
3. The cloud is not a devil; it can actually be an angel offering greater protection.
4. Similarly, the adoption of "hybrid" access models that include default-closed as well as default-open areas, protected by confidentiality management software, is worth serious consideration.
5. Enough can never be said about the importance of educating lawyers and staff to raise their risk awareness. Training, testing and discussion are a critical part of strengthening your firm's "human firewall".
6. On the cultural front, continued emphasis on the sensitive nature of the data firms possess and the commitment everyone within organization must make to protecting it is always worth reinforcing.

Was this story fiction? Or just a future that hasn't happened yet? Either way, the issues and possibilities are quite real…

About the Author:

Dan Bressler is vice president of marketing at Intapp, founder of the Risk Roundtable Initiative and editor of the Law Firm Risk Management blog. In 2015, he was honored by the International Legal Technology Association (ILTA) as its Vendor Thought Leader of the Year.

He can be reached at: Dan.Bressler@intapp.com.