IN THE REALM OF CYBERSECURITY BREACHES, THE TIMES HAVE BEEN A-CHANGING AND -*ESPECIALLY FOR LAW FIRMS* - NOT AT ALL FOR THE BETTER.

By Scott Larson, CISSP, CISM, CIPP, AME
Larson Security, LLC
& Robert Eisenberg, Managing Director
The Empire Consulting Group

Before the news-grabbing hype of today's "cyber-espionage" Advanced Persistent Threats (APT) and massive, often criminal syndicate-led, credit card data breaches and long before the nefarious activities resulting in recent criminal indictments of Chinese military agents implicated in commercial cyber criminality, the authors began to see large multinationals, that had emerged from massive mergers and acquisitions, together with their prominent outside law firms, becoming cybersecurity targets in the late 1990's. However, such activities, in those early days of cyber lawlessness, were the exception to the more commonplace network intrusions and theft of intellectual property cases of the time. Credit cards and long distance calling cards have always been a target of criminals, but the more "talented" cybersecurity bad actors of some 15 years ago were harbingers of much worse things to come. Indeed, the cyber pirates who were collecting proprietary data from and eavesdropping upon law firms and corporations were highly sophisticated for that era, although they were – thankfully - few in number. That was then, when one of the co-authors, Scott Larson, supervised the Computer Investigations and Infrastructure Protection Program at the Federal Bureau of Investigation (FBI). Fast forward 15 plus years to today and Scott will tell you that this higher level of sophistication on the part of attackers has become all too common.

And, in fact, unlike that earlier era and given the global reach of the Internet, premier law firms of today have become "Tier One" targets for cybersecurity threats.

It is not that many firms are unschooled in the realm of Electronically Stored Information (ESI). Law firms understand segmentation of data to avoid potential conflicts. Moreover, for many law firms, client engagement databases and systems for "Conflicts Checks" are well established. Unfortunately, the same tools and vigor that are being applied to a firm's conflicts and engagement management arenas are, frequently, not being utilized for the information security and data protection ecosystem of these same law firms.

Why not?

Naturally enough, law firms have focused their technical personnel and other resources on litigation, conflict management and eDiscovery and many have been successful in these arenas. However, much less focus is being dedicated to what is referred to as the "Security Maturity Model (SMM). On the other hand, clients are becoming increasingly concerned with SMM and at present expect law firms to be as familiar with advanced data security issues, as they are with more "traditional" legal services. In the realm of Regulatory and Reputational Risk,clients are now requiring HIPAA Business Associate (BA) or ISO27002 Information Security Management System (ISMS) audits to meet the needs of their businesses. Also sought is the ability to aid in compliance with Payment Card Industry Data Security Standard (PCIDSS), HIPAA/HITECH Act and the EU Data Protection Act. Also expected is strict compliance

with a growing plethora of contractual obligations compelling outside counsel to assure that all appropriate protective measures are in place.

An additional factor in compelling both clients and law firms to confront a fraught state of reality in the cybersecurity field is the persistence of what is referred to as "The Advanced Persistent Threat" (APT).[1] We have seen this threat grow exponentially during the last ten years, well before Google's public disclosure of Operation Aurora in 2010[2] made APT a common acronym within the information security lexicon. Law firms, internal patent repositories and other holders of intellectual property are the primary targets of adversaries utilizing APT.

What issues should be primarily addressed and what should be done by a law firm or other organization to meet these potential threats?

To begin with, merely scanning systems for security vulnerabilities on a reactive and intermittent basis is not sufficient. Indeed, vulnerability scanning on an annual or even quarterly basis for external and internal network purposes does not provide proper safeguards. Rather, configuration management, network segmentation (protecting the entity's "golden eggs"), and network security monitoring within firewalls and switches are essential for mid-to-large size organizations. That is not to say that scanning and perimeter security are unnecessary. It just, frequently, is not good enough. The problem is that the anti-virus software utilized for security (recent studies have revealed that such software detects less than 40% of incidents) and newly developed "shiny" appliances like log aggregation systems known as Security Incident Event Management (SIEM) Systems are expensive and, what's worse, the events that are detected are frequently ignored due to a lack of trained personnel or an organization's information security analyst that has been re-assigned for another priority. Fortunately, however, an organization will need to rely much less upon such costly and occasionally ineffective technology if regularly scheduled network security monitoring and other routinely engaged cyber-investigatory services are deployed.

As mentioned, the appliances that are presently touted are inevitably very costly and some are of questionable efficacy. The new hot security tool of today is an appliance with "intelligent" logical and historical indictors to aid in network defense. These are both almost prohibitively expensive and may have a limited useful life. Rather, it is suggested that an organization start small, but systematically, in securing its cybersecurity environment; get a "health check" first, before the organization invests in any "heavy machinery". First, look to leverage the systems and personnel already in place with a "doctor" who makes house calls to your office.

Moreover, hire trusted individuals to access and review an organization's data. One should be cautious of the Big Data enterprises who claim to have every solution for an organization's cybersecurity needs. Seek a smaller, , adaptive, well-trained group with a multi-discipline range to advise you for whatever

---

[1] **Advanced Persistent Threat** (**APT**) is a set of clandestine and continuous computer hacking assaults, targeting a specific entity. APT usually targets organizations and nations for business and political motives. APT processes require a high degree of covertness over an extended period of time and often turn the victims IT infrastructure into a digital espionage collection station that "phones home" via a covert data channel(s).

[22] **Operation Aurora** was a cyber-attack conducted by advanced persistent threat actors originating from, in or near Beijing, China and believed to be affiliated with the Chinese military. The recent indictment of five Chinese military hackers by a grand jury on May 19, 2014 in western Pennsylvania (USDC, W. Penn., Criminal No. 14-118) underscores the prevalence and severity of the threat.

comes your way. The group you select should help find solutions whether internally or by leveraging outside resources.

Finally, develop a plan to conduct a Security Gap Analysis for the law firm before an incident occurs or a major client determines your security does not measure up to your competition.