Issued 8/4/17

Hackers are Aggressively Targeting Law Firms' Data

Behind every splashy headline is a legal industry that's duking it out – helping to support entrepreneurs and big corporations in a power struggle to dominate their industry. From patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use.

This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence. For an example of this, look no further than the Panama Papers – "…an unprecedented leak of 11.5m files from the database of the world's fourth biggest offshore law firm, Mossack Fonseca." This was devastating, but it is only one example among many. Just a few weeks ago news broke that a ransomware attack was successfully executed against yet another multinational firm - DLA Piper.

This ransomware attack left the firm, with estimated revenues of $2.5 billion, completely without access to its own data. "Law firms are the subject of targeted attacks for one simple reason," says John Sweeney, President ofLogicForce. "Their servers hold incredibly valuable information. That includes businesses' IP, medical records, bank information, even government secrets. For hackers looking for information they can monetize, there is no better place to start." These headlines, buried among the others,

make it clear that the legal industry is facing an unprecedented cyber-security challenge. And solving this problem starts with helping firms realize they've been victims. 40% of firms did not know they were breached in 2016 The Law Firm Cybersecurity Scorecard includes an array of assessments - from cyber defenses, crisis management procedures, and post-hack responses. The report comes to a chilling conclusion: "…40% of surveyed law firms had experienced a data breach in 2016 and did not know about it." Part of the challenge is the skyrocketing cost of cybersecurity. Hiring an in-house team simply isn't feasible for most firms. Instead they rely on consumer-grade technology that is ill-equipped for the threats they are facing.

The solution, as we've seen in many industries, is to outsource cybersecurity to trusted firms that can offer heavy-hitting, managed solutions at an affordable rate. SaaS (Software as a Service) is long overdue in this space, and thankfully it's becoming more and more available. Real-time industry expertise is an important part of the solution – something software alone can't handle. Today's hackers hold a strategic advantage because of the growing numbers of devices and associated vulnerabilities. Every access point is a potential breach. A knowledgeable, sophisticated team can create security solutions specially crafted to meet the challenges that law firms face.

One of the greatest challenges in modern security is the Internet of Things (IoT). Everything from the appliances in the breakroom to the smartphones in the pockets of employees create dynamic networks – communicating information in a way that opens up opportunities to hackers. The threat goes beyond teams. An individual attorney uses a plethora of electronic devices, all networked together to provide a more streamlined work environment. And human intelligence, served up to hackers through social media, only makes targeted cyber-attacks easier. There are things

attorneys and other legal professionals can do to start upping their defenses.

1) The American Bar Association has published a comprehensive guide for law firms [link] – including both methods for preventing and responding to cyber-attacks.

2) Firm managers need to create a data security plan that speaks to every member of their team. Educate employees on strategies for identifying phishing attacks and other dangerous threats aimed at fooling people into compromising networks.

3) Engage outside IT security experts and have risk assessments completed on a regular basis. If you can identify vulnerabilities, you can put a plan in place to minimize or eliminate them.

4) Communicate and enforce a password policy that limits access and requires authorized users to regularly change their credentials.

5) Conduct a weekly check for patches or other updates to computer security software.

6) Develop a comprehensive breach response plan. After you've been hacked, it will be too late to develop a competent response that protects the Firm's reputation.

7) Make sure your employees are trained to recognize and avoid cyber threats.