Law firms are a TOP TARGET FOR CYBERCRIME

In response to large enterprises embracing new technologies to detect and respond to security incidents, attackers have shifted their focus to organizations who have existing relationships and often access to the intended victim.

Law firms and contract lawyers have become ripe targets as they have continued access to sensitive information in the form of contracts and correspondence. Law firms have been warned in recent years that their systems have been attacked and that the attacks will likely escalate and intensify.

For example, in 2016, the FBI alerted international law firms of insider trading schemes that rely on information from law firm breaches. In December 2016, federal prosecutors had charged three Chinese citizens for hacking into law firm computers in 2014 and 2015 to **steal information to the tune of $4 million**.

With the constant warning drum beat coming from the federal government, audit community and American Bar Association, law firm networks are a veritable treasure chest of data:

- Firms maintain a tremendous amount of highly confidential information regarding financial information, trade secrets, technology IP, M&A data; from a cyber criminal's vantage point, this information is currency.
- Law firms can act as a beach head for attacks against your client or another firm or see you as an end to a mean.

Law firms have common law duties to protect client information as well as contractual and regulatory obligations related to the health, financial or other personally identifiable data they collect. Failure to comply with these obligations can constitute unethical or unlawful conduct. Thus, many law firms are now aiming to achieve security that goes beyond minimum measures as a matter of sound professional practice and client service.

BLUVECTOR®

STAY AHEAD OF THE THREAT. BluVector has reinvented the network intrusion detection system with patented machine learning and speculative execution engines so that it can finally defend the network against even the newest and most sophisticated cyberattacks.

Before your next breach, visit **www.bluvector.io**

73%
of large law firms had fallen victim to a breach

30%
of attacks resulted in loss of billable time†

COST OF A BREACH

Security breaches result in negative publicity, a lack of client trust and even lead to civil action. Given the sensitivity of client-attorney correspondence, it is vital that firms protect their correspondence, private documentation, and any client Personally Identifiable Information (PII).

Quantifying the impact of a breach within the legal industry is not a simple task. One would have to analyze:

- Cost of downtime, inability to bill or service clients
- Disciplinary actions, cost associated with malpractice
- Loss of important information/files
- Reputation loss, loss of client(s) and prospective clients
- Cost of breach investigation and required notification
- Fines for failure to adhere to state law

† *2015 American Bar Association Legal Technology Survey Report*