New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 84
WEDNESDAY, MAY 3, 2017

Outside Counsel

Expert Analysis

For Lawyers and Law Firms: Mitigating Cyber Risks With Right Security Controls

By **Chris Moschovitis**

It is no secret that cyber security risks add complexities that often restrict the process of seamlessly carrying out legal transactions. Law firms need solutions that ensure confidentiality, availability, and integrity of sensitive data to avert significant damages to themselves and their clients. However, law firms should never fall into the trap of thinking that a set of solutions today will deliver them safely from the cyber security threats of tomorrow.

Unfortunately, many lawyers are becoming tone-deaf to the constant narrative of "it's not a matter of if you'll be hacked—it is a matter of when" and are being seduced by vendors that promise "peace of mind." These promises are dangerous and expensive fantasies that deliver a false sense of security. That said, business must go on, and lawyers are all responsible for taking pragmatic steps to mitigate cyber security risk. This can be done by selecting and applying the right security controls for law firms.

First things first: We need to recognize that there is no "one size fits all" solution. Each firm is different and each practice is different. Moreover, each firm and each lawyer have different risk appetites. The right controls for one firm will prove excessive for the next, and not enough for the third. Therefore, the first thing that must be established is what is the risk appetite for the firm and its individual lawyers.

The next thing to do is get a grip on business assets. What, exactly, are the things of value we are trying to protect, and what are the threats against them? Is it a matter of protecting intellectual property? Client data? Classified information? Reputation? Is it a question of physical security? Insider threats? In short, where are the threats coming from?

It is no accident that the National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity leads with "Identify" and not with "Prevent." There is no "Prevent" in cyber security, and the sooner one gets comfortable with that, the sooner one will get to the real work of Identifying, Protecting, Detecting, Responding, and Recovering (the five NIST framework functions) from cyber security events.

Having identified what warrants protection, the real work begins.

CHRIS MOSCHOVITIS *is the chief executive of tmg-emedia and co-author of "History of the Internet: 1843 to the Present." Chris is working on his latest book "Cybersecurity Program Development for Business: The Essential Planning Guide" to be published by Wiley later this year. He can be reached at Chris.Moschovitis@tmg-emedia.com*

Accounting for one' firms risk appetite and armed with one's asset valuation and threat assessments, one is now ready to apply the right controls. Remember: Controls "do" things. They are not some abstract notion, they do-the-do! There are four kinds of controls: Preventive, Detective, Corrective, and Compensatory.

> Law firms need solutions that ensure confidentiality, availability, and integrity of sensitive data to avert significant damages to themselves and their clients.

While there is no "Prevent" in cyber security, it is essential to know that there are preventive controls that are proactive. A preventive control acts like a barrier to an attack. It hasn't prevented the attack, but just like the barrier on the street that hopes to stop the runaway truck from hitting the building: it hopes to prevent an aspect of the attack. Think of it as a locked door. Another example of a preventive control is segregation of duties. One's systems administrator shouldn't know the database password, and the database administrator shouldn't know the systems password. Security awareness training is another excellent example of a preventive control.

Detective controls are easier to understand. They detect. They know the door has been opened (e.g., a motion detector), and they do something about it. Either they close it, or alert someone that the door has been opened. Other examples of detective controls include system's monitoring applications, intrusion detection systems, even anti-virus and anti-malware solutions.

Corrective controls fix or restore the environment. For example, applying the right security patches and upgrades is a corrective control. Restoring your data from backup is another corrective control.

Finally, compensatory controls are those designed to compensate for some of the damage. A disaster recovery site is a compensatory control. Cyber insurance can also be a compensatory control. Even a backup generator, a second set of servers or computers, or the ability to switch over operations at another country, all are compensatory controls.

Keep in mind that there are some solutions that span control classes. For example, an anti-virus/anti-malware solution can be a preventative control, a detective control, and a corrective one all at the same time.

What is the right blend of controls for your organization? As previously noted, it depends on risk appetite, type of asset, type of threat, regulatory environment, budget, and skill-sets. One needs to take all this into consideration in developing a defense-in-depth cyber security strategy.

Remember: Firms have a tremendous advantage over attackers: Lawyers know their firms better than anyone else, and so know what's of value and what needs protection. More than any solution, lawyers should trust themselves and rely on their own judgment and apply pragmatic controls where and when necessary and applicable.