REDUCING CYBER RISK IN THE LEGAL SECTOR
The Blurred Boundaries of Trust

How legal firms can adopt best practice through the adoption of security intelligence tools.

Authors: Mark Baker and Tom Salmon
Contributor: Derry Murphy
Table of Contents

3 Executive Summary

4 Defining Cyber Risk

5 An Introduction into the Security Intelligence Imperative

5 CISO’s Tip

5 Legal-Specific Use Cases
   Mergers and Acquisitions Use Case
   Use Case: Insider Threats
   Use Case: A Disgruntled Employee
   Use Case: Targeted Phishing Emails

8 Conclusion

8 About LogRhythm
Executive Summary

Legal firms operate on a trust basis; it’s the cornerstone of their business. If that essential duty of care to their clients is broken, the consequences can be far reaching.

A recent survey conducted by Oxford Economics and Ponemom stated that, of the firms who had experienced a loss of commercially sensitive data, 61 percent said that this resulted in a loss of competitive advantage.

In recent years, the playground where criminals are operating has changed. They’re going undetected and operating passively—leveraging insight into critical information for financial gain or to tarnish reputations. FireEye’s recent publication on the ‘FIN4’ group, sheds light on how criminals are passively monitoring legal counsels that have key insight into mergers and acquisitions in order to gain a financial advantage on stocks or on the future of firms’ acquisitions.¹

The trustworthiness of internal employees has also become harder to monitor, as the boundary of the network has become blurred, coupled with the emergence of “shadow IT” and the increase in cloud-based file sharing. While cloud-based services can help streamline operations, these can limit the ability for already resource-contained IT security teams to monitor legitimate usage. Therefore, more creative solutions, in line with legal responsibilities, have to be employed.

This paper examines the top five use cases for centralized monitoring within the legal sector, in order to reduce cyber risk through faster detection and response. It examines why security intelligence solutions provide the best of breed for monitoring multiple silos of information. And it discusses how legal IT security teams can leverage their existing investments in point-based security technologies in order to gain valuable insight into malicious activity, while also streamlining operations.

¹ Having the Street? FIN4 likely playing the market - FireEye (Vengerik, Dinnesen et al) 2014
Defining Cyber Risk

Cyber risk isn’t just one particular risk. It varies based on the value and sensitivity of intellectual property and external/internal attack vectors. But for legal firms, it’s predominately client information that is of high value to criminals or ideological attackers.

The primary impact on legal firms is reputational damage, business interruption, cyber extortion and loss of competitive advantage. It’s important to remember that the shift of the risk curve represents an ongoing trend. Very high-impact risks will become increasingly frequent, forcing us to become better at protecting assets and devising creative solutions to mitigate risks.

Translating such impacts to the business has historically been a challenge. However, an illustrative example is shown in Figure 1, using a basic risk curve that demonstrates the interconnectivity between the probability of risk occurrence and its potential impact.

As the risk curve progresses right to the “long tail,” it represents a group of very high-impact risks with a low probability of occurrence. The challenge of addressing risk with high probability of occurrence and the likelihood of high impact is the reality of organizations with resource constraints.

Historically, the “focus zone” for legal firms looking to reduce their risk exposure had been on just information security, which included investments in antivirus, SPAM control, spyware, basic perimeter defense, and so forth. But as the threat landscape has evolved—and the frequency of attacks has increased—the focus zone has shifted to include cybersecurity and risks that historically were deemed unlikely to occur. This has drawn out the focus zone to point 2.

With PwC stating a 66 percent annual compound growth rate in the number of cyber incidents detected² and the Office of National Statistics now saying that cybercrime is the most prevalent and prolific threat to UK Businesses³, the threat landscape has changed and is changing on a daily basis.

This new group of very high-impact risks, commonly referred to cyber risk, now requires close attention. As illustrated, on the right cybersecurity is the sum of efforts invested in addressing cyber risk.

This group of risks includes all sorts of scenarios, organization-specific tailored malware, stolen certificates, spies and informants, exploiting legacy vulnerabilities, attacking third-party providers and advanced persistence threats (APTs).

Figure 1. Risk Curve of the Probability of Risk and Potential Impact

³ 2015 Cost of Cyber Crime Study: United Kingdom - Ponemon Institute October 2015
An Introduction into the Security Intelligence Imperative

The best approach to gaining insight and visibility while filtering out unnecessary noise to the most important threats is through advanced security intelligence (SI). Just as business intelligence (BI) has helped numerous organizations clear the fog of too many points of seemingly extraneous business data to find previously unknown business opportunities, SI does much the same thing with threat information, enabling organizations to clearly see the threats that matter.

Across the end-to-end threat detection and response process, there are two key metrics organizations should measure and strive to improve: their mean time to detect (MTTD) and mean time to respond (MTTR).

- MTTD is the average amount of time it takes an organization to discover and qualify those threats that could potentially impact the organization.
- MTTR is the average amount of time it takes an organization to fully investigate the threat and mitigate any risk presented.

CISO’s Tip

The main objective of SI is to deliver the right information, at the right time, with the appropriate context, to significantly decrease the amount of time it takes to detect and respond to damaging cyber threats. In other words, to significantly improve an organization’s MTTD and MTTR.

Legal-Specific Use Cases

Legal firms find themselves becoming an ever-increasing target for cyber threats. The threats, which can emanate internally or externally, are most likely to be from criminal or ideological groups looking to profit from or tarnish the reputation of law firms.

Mergers and Acquisitions Use Case

In today’s business environment, cyber-criminals are looking to get ahead of the curve by gaining access to sensitive information. For law firms, particularly the FIN4 group highlighted by FireEye, this means using C-Level information for financial gain. Some examples of cyber criminal behavior include:

1. Sending phishing emails containing a specific tracking ID for each target based on their role, such as partner, or CEO.
2. Sending an attachment to a phishing email that contains a malicious Microsoft Word document. When opened, a number of actions happen:
   - Creates email rules to automatically delete any incoming emails trying to warn about phishing or security.
   - Creates a prompt that looks like the Microsoft Outlook “Please re-enter your login credentials” screen.
   - Stolen credentials are sent to one of a few pre-determined servers.
   - Criminals log in to email servers using the stolen credentials. The source of the log in is always hidden using Tor, which is not common business practice.

User Behavior Analytics (UBA) helps discover and respond to the threat of FIN4:

- Monitor Microsoft Exchange email rules for the specific FIN4 rules.
- Monitor network traffic using an application aware forensic tool to discover connection to implicated servers and hosts.
- Monitor access to public-facing services, such as email, from Tor—either from known Tor exit nodes or by application identification of incoming internet traffic.
- Monitor incoming network requests from specific browser strings always used by the automated tools employed by criminals in the FIN4 network.

Figure 2: MTTD and MTTR shrink as security intelligence capabilities grow more mature
Use Case: Insider Threats

You might think that insider theft, lawsuits and foreign espionage were descriptors to Tom Clancy’s next novel, but these are the facts arising from recent data thefts from American Superconductor by Sinovel. An American Superconductor employee in Austria was accused of stealing valuable software that controls turbines and giving it to Sinovel Wind Group—a Chinese competitor.

Putting aside the international ramifications of this case, insider theft is a real factor for any business, particularly legal firms, based on the nature of their business. It was highlighted by the Law Firm File Sharing survey that 77 percent of firms rely on a confidentiality statement to secure communication, and nearly half admitted to using free cloud-based file sharing services such as Dropbox to transmit privileged information.⁴

Typical methods of exfiltration are USB devices, cloud data syncing services such as Dropbox, self-emailing files to personal addresses and even printing. In all of these instances, the employee is using technology to perform the theft or leak. However, their employment is what is granting them the access needed to carry out their activities.

Based on our experience today, business operations and productivity should be of the utmost importance, and security solutions should not be an impediment to these. Therefore passive monitoring, rather than prevention, should be adopted initially to highlight breaches or to highlight violations outside of corporate policy.

Unfortunately, many insider leaks and breaches are discovered after the event has occurred. This leaves a likely expensive investigation and potential litigation. Monitoring insider threat is vital in a CISO’s agenda to be able to reinforce policy into practice.

The reality for law firms is that without the ability to know exactly what is happening across your IT estate and understanding what “normal” activity looks like, you’re behind the curve. Aiding this is the following:

• No centralized visibility
• Multiple point-based technologies or multiple dashboards
• No centralized intelligence
• No holistic analytics applied on large datasets

Understanding the behavior and activity of users is key to profiling risk. Organizational-specific profiles pave the way for minimal false positives and maximum return on investment.

In Figure 3, an overview of user activity is clear. By applying user behavior analytics (UBA), one can understand when one employee significantly moves out of profile—exporting, printing, changing or downloading large volumes of data that they should not access on a daily basis.

---

⁴ Cyber-attacks: Effects on UK Companies July 2014 - Oxford Economics
Use Case: A Disgruntled Employee

When an employee hands in their notice, it is critical to perform both retroactive analysis and real-time analytics on their behavior. Once they show their intent to leave the business, they must be viewed as potentially more willing than most to take intellectual property with them.

A good process for leaving employees includes:

- Reviewing at least 30 days of internet access:
  - Have they uploaded any large files to sharing websites such as Dropbox?
  - Are they regularly using external email accounts such as Gmail?
  - Are they using platforms with integrating file exchange such as Facebook?

- Reviewing DMS and file server activity:
  - Have they accessed an unusually large amount of files?
  - How many times did they access more sensitive and critical information before leaving compared to a normal week, or another employee?

- Enable real-time alerts and daily reports on leaving employees:
  - Abnormal increases in access to sensitive data
  - Unusual working patterns
  - Use of removable media, file sharing, document exchange, large email attachments

Use Case: Targeted Phishing Emails

Phishing emails represent a real and significant threat to all organizations. The legal sector, in particular, relies heavily on email for communication internally and with external parties. Most workers can empathize with the commonly raised complaint of too many emails coming in.

You may have heard the term “whaling.” This refers to sending well-crafted emails to very high-value targets such as partners, CEOs or CFOs.

Criminals take advantage of this by crafting well-written phishing emails. They hope that, due to the sheer volume of emails received each day, a busy senior executive is less likely to spot a small spelling error or notice a minor difference to the sending email address.

Catching phishing emails requires real-time analysis of the entire email—both the visible message and the invisible metadata used by computer systems to route and process emails around the world. Some of the key indicators present in phishing emails are:

- HTML links with a different target than the displayed URL
- Emails coming from domains very similar to your organization, such as connpany.com rather than company.com.
- Emails with a Reply-To field set to return emails to a different recipient than the original sender
- Any emails coming from non-trusted email servers
- Emails that have bounced through many relays and proxies to disguise the original sender

Analyzing emails for these traits increases the chances of catching and stopping phishing attacks before they progress to an impacting event.
Conclusion
CISOs in the legal sector need to be aware of the potential impact of a broad range of threats. Historical investments in point-based solutions are becoming less valuable as attacks evolve and adversaries apply new techniques to disrupt and damage legal firms.

A key trend to maximize investment in security technology is centralized monitoring and real-time analytics. By combining these two approaches, law firms can detect a wide range of threats, and respond to them quickly. Reducing cyber risk involves adopting creative solutions in order to reduce frequency and impact. Having a solution in place where those driving the platform understand the environment in which they operate is a huge advantage to adopting and responding to specific legal targeted threats in real time.

Those who have outsourced without laying the right log management foundation will find that their MTTD and MTTR is reduced in two ways. Firstly by adding another silo and communication layer to their solution. Secondly, the risk is of that third-party not truly understanding the context of your environment and adapting to the constant change of the business.

About LogRhythm
LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company’s patented award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner’s SIEM Magic Quadrant report for five consecutive years, named a ‘Champion’ in Info-Tech Research Group’s 2014-15 SIEM Vendor Landscape report, received SC Labs ‘Recommended’ 5-Star rating for SIEM and UTM for 2016.

LogRhythm is headquartered in Boulder, Colorado, with operations throughout North and South America, Europe and the Asia Pacific region.

To learn how LogRhythm can help your firm reduce cyber risk by detecting and responding to threats faster, visit www.logrhythm.com.