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

LogRhythm®

The Security Intelligence Company

WWW.LOGRHYTHM.COM

THREAT INSIGHT

Reducing cyber risk in the legal sector

This paper aims to discuss and explore the high-level threat vectors the legal sector faces and then looks into a more granular inspection on key areas of vulnerability and mitigation options.

Contents

Executive summary

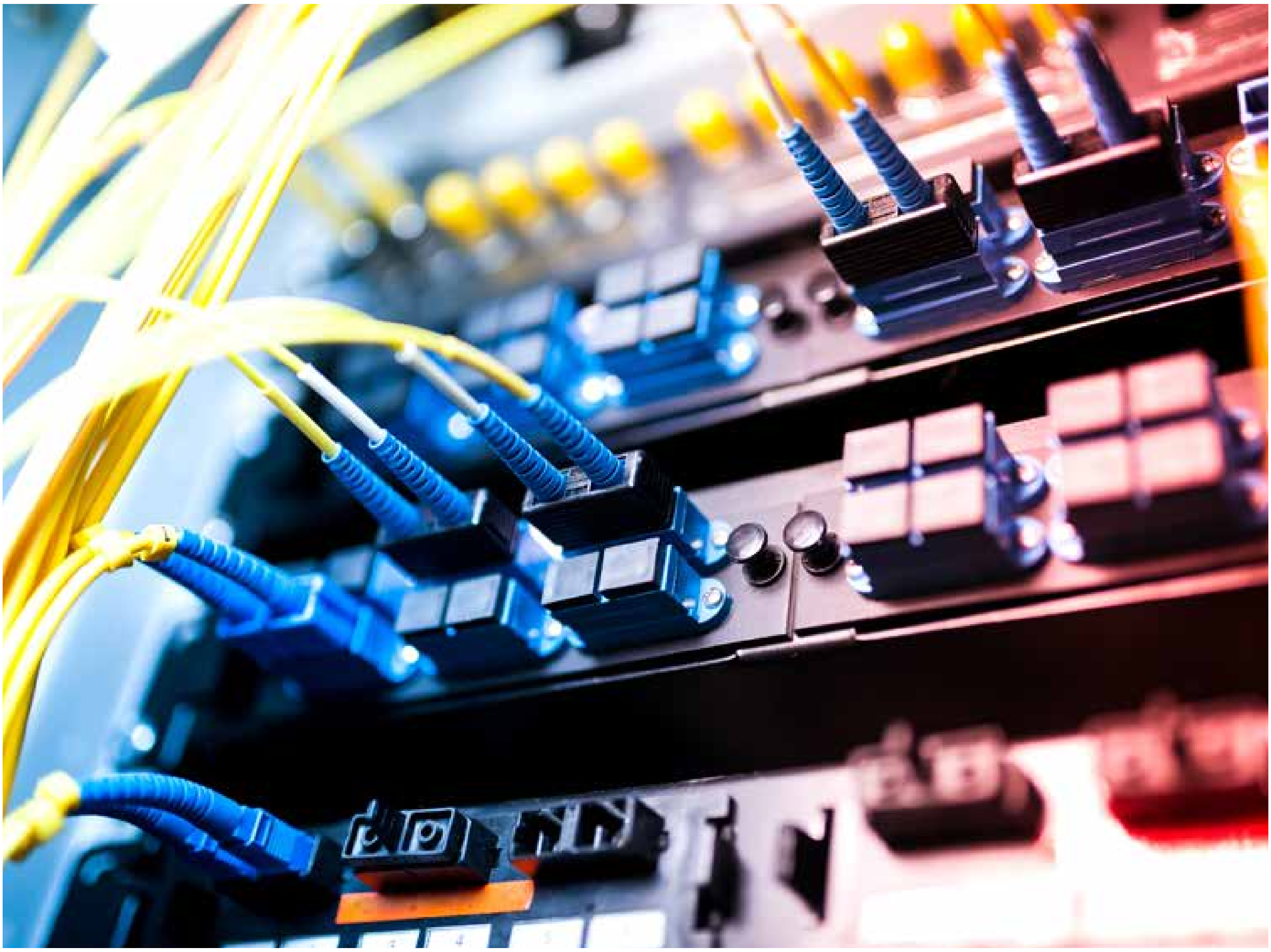
Legal firms operate on a trust basis; it's the cornerstone of their business. If that essential duty of care to their clients is broken, the consequences can be far reaching.

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

In recent years, the playground where criminals are operating has changed. They're going un-detected and operating passively, leveraging insight into critical information for financial gain or to tarnish reputations. FireEye's recent publication on the 'FIN4' group[2], sheds light on how criminals are passively monitoring legal counsels that have key insight into mergers & acquisitions in order to gain a financial advantage on stocks or on the future of firms' acquisitions.

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 centralised monitoring within the legal sector, in order to reduce cyber risk through quicker detection and response. It examines why security intelligence solutions provide the best of breed for monitoring multiple silos of information and 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.



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.

To translate such impacts to the business has historically been a challenge. However, an illustrative example is shown in fig 1 using a basic risk curve which 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 reality of any organisation with resource constraints is the challenge of addressing risk with high probability of occurrence and the likelihood of high impact.

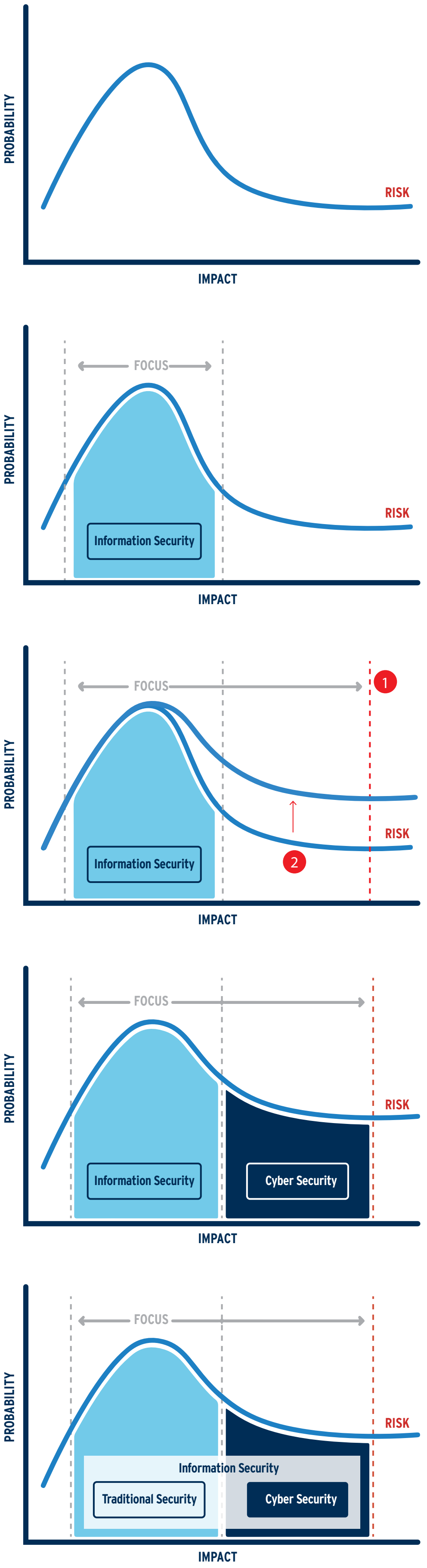
Historically, the 'focus zone' for legal firms looking to reduce their risk exposure had been on just information security which included investments in anti-virus, SPAM control, spyware, basic perimeter defence etc. But as the threat landscape has evolved - and the frequency of attacks have increased - the focus zone has shifted to include cyber security and on risks that historically were deemed unlikely to occur and thus drawing out the focus zone to point 2.

With PwC stating a 66% annual compound growth rate in the number of cyber incidents detected[3] and the office of national statistics now saying that cybercrime is the most prevalent and prolific threat to UK Businesses[4], 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, below cyber security is the sum of efforts invested in addressing cyber risk.

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

Figure 1



An introduction into the security intelligence imperative

The best approach to gaining insight and visibility whilst filtering out unnecessary 'noise' to the most important threats is through advanced Security Intelligence (SI). Just as Business Intelligence (BI) has helped numerous organisations 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 organisations to clearly see the threats that matter.

Across the end-to-end threat detection and response process, there are two key metrics organisations 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 organisation to discover and qualify those threats that could potentially impact the organisation.

- MTTR is the average amount of time it takes an organisation to fully investigate the threat and mitigate any risk presented.

CISO's tip

Cyber attacks can get costly if not resolved quickly. Ponemon's recent study[4] into the cost of a data breach in the UK showed a positive correlation between time to contain attack and the associated costs to the organisation.

With the average attack lasting 31 days and costing on average £358,796, CISOs now have a local tangible metric to show a ROI for SI tools. If a threat is detected and resolved in hours, the business can see improvement and insight into real-time risk mitigation. The report also found that companies using SI technologies were more efficient in detecting and containing cyber attacks. As a result, these companies enjoyed an average cost saving of more than £1.3 million when compared to companies not deploying SI technologies.

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 organisations MTTD and MTTR and thus 'cyber risk' exposure.

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 and/or tarnish the reputation of law firms.

1. Challenge – mergers & acquisitions – working on behalf of

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 leveraging C-Level information for financial gain.

FIN4 group – techniques

Targets: Top executives & legal organisations working on client mergers and acquisitions.

Cyber-criminal example behaviour:

1) Sends out phishing emails containing a specific tracking ID for each target based on their role, such as partner, or CEO.
2) Attachment to phishing email 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 login to email servers using the stolen credentials. Source of the login is always hidden using Tor, which is not common business practice.

Solution

User Behaviour Analytics (UBA) helps us 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: The impact of a breach is directly related to MTTD and MTTR

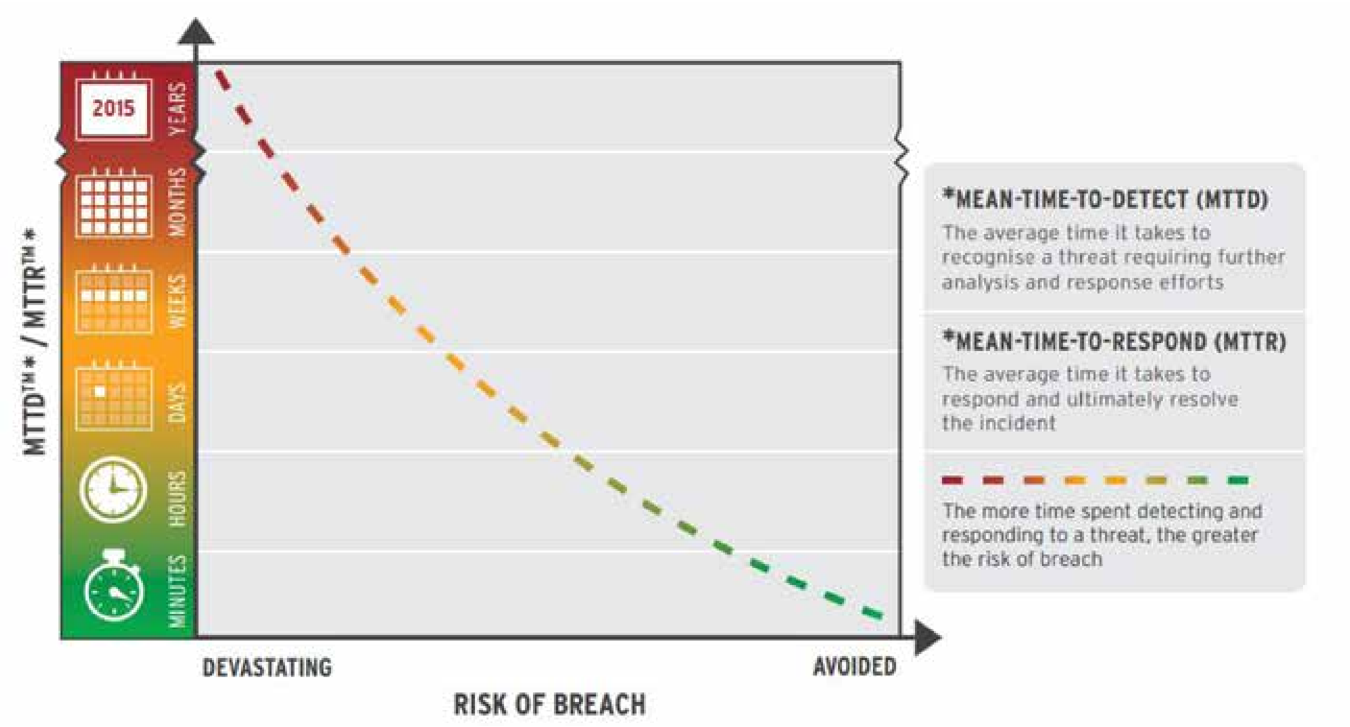
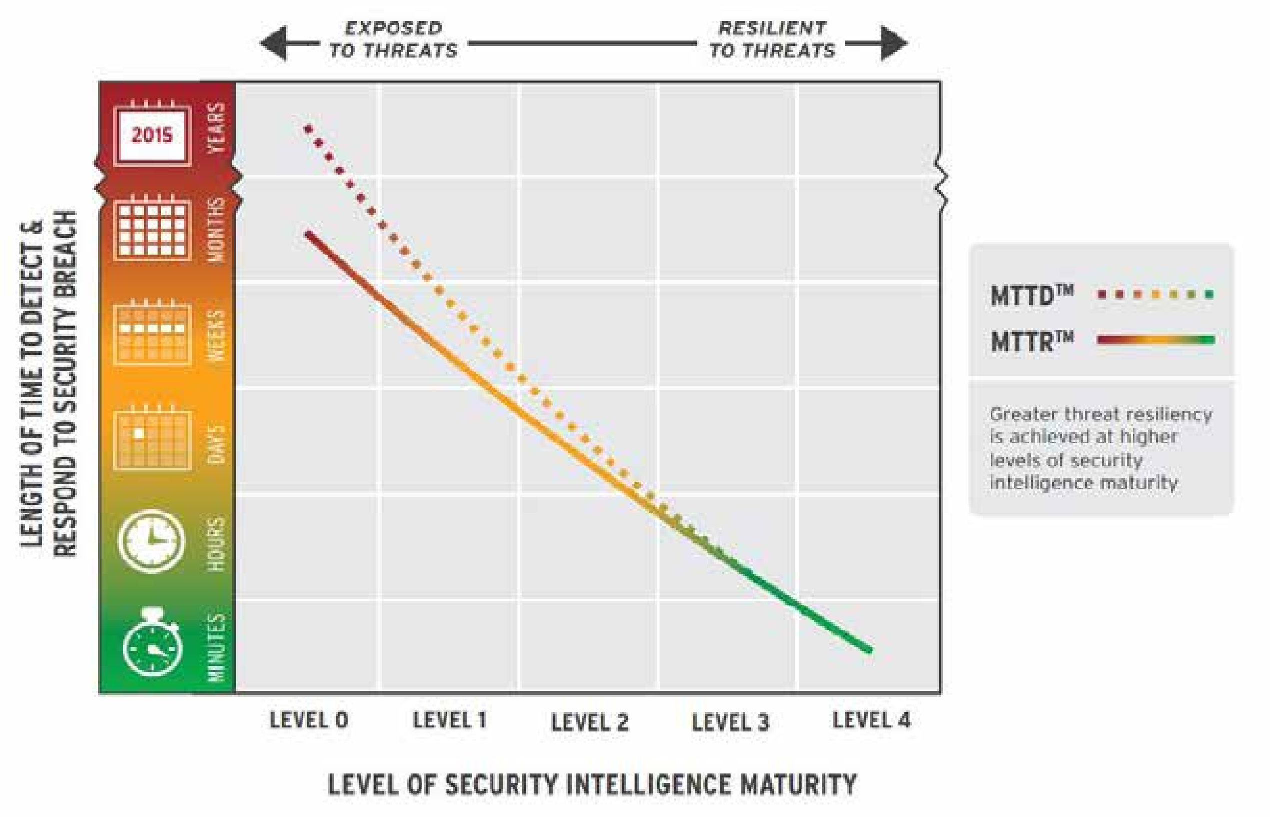


Figure 3: MTTD and MTTR shrink as security intelligence capabilities grow more mature



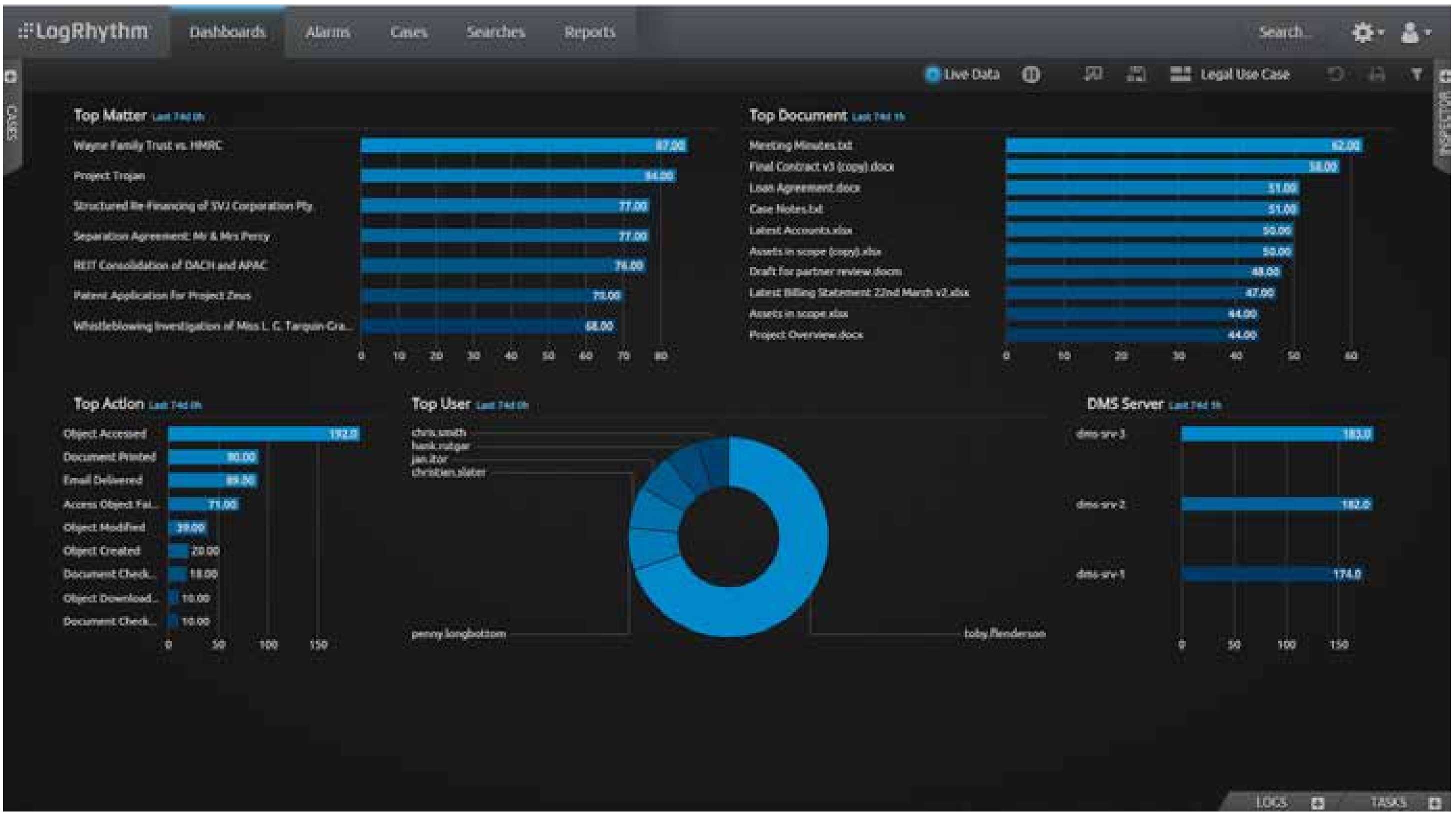


Figure 4 – LogRhythm Dashboard demonstrating insight into document management system activity

2. Insider threat

You might think that insider theft, law suits 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[1] that 77% 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.

Typical methods of exfiltration are USB devices, cloud data syncing services like Dropbox, self-emailing files to personal addresses and even printing. In all of these instances, the employee is using technology to actually 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 CISOs 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 centralised visibility
- Multiple 'point' based technologies or multiple dashboards
- No centralised intelligence
- No holistic analytics applied on large datasets

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

In Figure 4, we can see a clear overview of user activity. By applying user behaviour analytics we can understand when one employee significantly moves out of profile – exporting, printing, changing, downloading large volumes of data that they should not access on a daily basis.

3. Disgruntled employee

Leaving employees – monitoring best practice

When an employee hands in their notice it is critical to perform both retroactive analysis and real-time analytics on their behaviour. 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

4. Targeted phishing emails

Phishing emails represent a real and significant threat to all organisations. The legal sector in particular relies heavily on email for communication internally and with external parties. Most workers can empathise 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 and CFO (or other high placed controllers of finance/payments).

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 meta-data 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 organisation such as connpany.com rather than company.com - did you notice the double n instead of m?
- 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

Analysing 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 maximise investment in security technology is centralised 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 & MTTR is reduced in two ways. Firstly by adding another silo and communication layer to their solution and secondly, the risk 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 organisations around the globe to rapidly detect, respond to and neutralise damaging cyber threats.

The company's award-winning platform unifies next-generation SIEM, log management, network and endpoint monitoring and forensics, and security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence.

Find us

LogRhythm Ltd.
Clarion House
Norreys Drive
Maidenhead
SL6 4FL, UK

Contact us

Tel: 01628 918 300
Email: uk-team@logrhythm.com

References

1- Cyber-attacks: Effects on UK Companies July 2014 – Oxford Economics

2- Having the Street? FIN4 likely playing the market - FireEye (Vengerik, Dinnesen et al) 2014

3- Source: PwC, The Global State of Information Security Survey 2015

4- 2015 Cost of Cyber Crime Study: United Kingdom - Ponemon Institute October 2015

http://www.lexisnexis.com/law-firm-practice-management/document-security/document-security-report.pdf