LogRhythm®
The Security Intelligence Company

The case for better defence

Cybersecurity and legal firms

LogRhythm
The Security Intelligence Company

Opening argument

The law is the basis of civilisation and provides the rules that determine how we live, how we do business, and how we protect all that society has built. Law firms ensure that businesses and individuals have the help they need to navigate this complex system.

Robes, panelled offices and long shelves of law books may be the layperson's stereotype of a law firm, but make no mistake, law firms are 21st-century organisations and they face 21st-century threats. Many firms are partner-led and have been slow to adopt best practice in cybersecurity. As a result, they can be a little behind the security maturity curve and are only now taking the journey to more sophisticated monitoring.

Technology allows legal firms to manage complex compliance requirements, track and share documents, streamline handling of funds, and manage billing, among other benefits. Such technology is essential.

Unfortunately, too many firms are guilty of neglecting security best practice. Law Journal Newsletters reported that a full third of respondents had no incident response plan[1]. Given that 62 per cent of law firms were estimated to have been the victim of a cyberattack in 2015[2], this is particularly concerning. Added to that, the Information Commissioner's Office reported a 32 per cent increase in data breaches in the legal sector in 2015, accounting for 4.5 per cent of all UK data breaches[2].

Evidence

Changing the security practices and culture of any company can be difficult and doesn't come without cost. A firm needs to carry out due diligence before taking such action. This will ensure the evidence supports the need, helping secure buy-in from senior management.

When legal firms are subject to successful cyberattacks, the results can be damaging both to the company, its clients and its reputation.

Prestigious global firm Cravath Swaine & Moore is known for representing Disney in its recent acquisition of 21st Century Fox and Time-Warner in its acquisition of AT&T. The firm also made headlines in 2016 for a data breach[3].

Treasure chest

Law firms must keep huge amounts of records and those records remain relevant for a very long time. The storehouse is immense. Some of the data cyberattackers could be seeking includes:

- Litigation information
- Merger and acquisition information
- Trade secrets
- Intellectual property
- Financial details on both corporate and personal clients
- Medical information
- Details of divorces, prenuptial agreements, adoptions, paternity and other sensitive personal information

[1] Most Firms Feel Assured in Cybersecurity Abilities, But Is That False Confidence?
http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/01/01/most-firms-feel-assured-in-cybersecurity-abilities-but-is-that-false-confidence/
[2] Cyber threats to the legal sector and implications to UK businesses
https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-threats-to-the-legal-sector-and-implications-to-UK-businesses.pdf
[3] China Stole Data from Major US Law Firms
http://fortune.com/2016/12/07/china-law-firms/

LogRhythm
The Security Intelligence Company

No firm needs this kind of publicity. There are suggestions that targeted 'spear phishing' attacks allowed the culprits to gain access to corporate email accounts.

Mossack Fonseca, the Panamanian legal firm at the centre of the massive Panama Papers leak, clearly demonstrates the damage a cyberattack can cause. The firm closed more than three dozen offices worldwide after losing 11.5 million records in a cybersecurity breach, according to one of its founders[4].

These attacks illustrate clearly what is at risk. Law firms hold large amounts of sensitive and valuable data. If a potential client sees a firm as a weak link and believes the firm cannot keep their data secure, the client will go elsewhere. In addition to reputational damage, such leaks may also lead to liability claims against offending firms.

Smaller firms cannot ignore the risks either. In fact, smaller client bases, lower revenues and limited resources can result in the firm being unlikely to survive a breach.

Law firms also need visibility of what users are doing with critical data across their organisation, particularly global firms that are becoming increasingly diverse as they make acquisitions. For example, if an employee from an acquired company shares sensitive information on an online storage platform, they would be failing to safeguard the data in an appropriate way and are likely to be violating protocols.

Like many industries, the legal sector also faces a security skills shortage, meaning there is a need for tools that let security teams do more with less.

Concluding argument

Law firms can't afford to be behind in information security. Firewalls and intruder prevention are only the beginning. Maintaining good IT hygiene is crucial. Mossack Fonseca, it was discovered, was using out-of-date software with known security vulnerabilities[5]. While this was careless, user and entity behaviour analytics (UEBA) can help detect unusual activity and flag it for response, or respond automatically. Of course, this works even better if your systems are all up-to-date.

Security information and event management (SIEM), working in tandem with UEBA, brings organisation-wide security data together to provide a complete picture of security-related

[4] Panama Papers fallout: Mossack Fonseca law firm shuts dozens of offices after leak reveals how world's wealthiest people stash their cash
http://www.scmp.com/news/world/article/2105236/panama-papers-fallout-mossack-fonseca-law-firm-shuts-dozens-of-fices-after
[5] From Encrypted Drives To Amazon's Cloud — The Amazing Flight Of The Panama Papers
https://www.forbes.com/sites/thomasbrewster/2016/04/05/panama-papers-amazon-encryption-epic-leak/#629e-7f833a34

Don't get hooked
Email and social media are targets for attackers seeking to penetrate your network. Firewalls won't block hackers with valid passwords.

Phishing:
Phishing involves sending an email or social network message impersonating a reputable firm. These messages usually have links to spoof web or social media pages that aim to capture passwords, personal data or financial details. Phishing attacks are often indiscriminate, casting a wide net.

Spear phishing:
This variant resembles phishing but involves targeting specific individuals or companies. Attackers will research targets and use the information they do have to try to convince the target they are the legitimate entity they are impersonating. This may include offering details about the target's postal address, employer or partial account numbers.

Whaling:
Whaling attacks are highly targeted, usually on CEOs and other high-level executives. They are carefully crafted to appear real and urgent. It may take the form of legal documents or an important financial matter. The messages will link to sites carefully tailored for high-level executives. Due to the authority and access these targets possess, a successful hit can be extremely damaging.

'Friday afternoon fraud':
This type of attack targets communications between solicitors and clients finalising the conveyancing process. Criminals intercept conversations and convince clients to pay property deposits into the wrong accounts. As the fraud often takes place at the end of the week (hence the 'Friday afternoon' reference) the fraudulent transactions can remain undetected over the weekend.

LogRhythm
The Security Intelligence Company

activity across networks. This enables a holistic view of security monitoring and compliance reporting, providing efficiencies in an environment where security skills are often in short supply.

Unfortunately, systems are not the only vulnerability a law firm faces. Staff can also pose a security risk, whether intentionally or unintentionally. Staff at Mossack Fonseca and Cravath Swaine & Moore may not have intended to cause harm when they fell for phishing attacks, but they did. They are also likely to have violated corporate cybersecurity protocols when they fell for those attacks.

Peer to Peer, published by the International Legal Technology Association, suggests staff failing to comply with IT security policy may be a matter of culture[6]. A company's security culture needs to be communicated, reinforced, monitored and coached to. It needs to be a clear priority. User monitoring and targeted training can ensure that cybersecurity is not just a yearly box to tick but a living part of a firm.

Some insiders, however, are malicious. Whether for financial gain, corporate espionage, or simply out of spite, staff can use their status to access, copy, compromise, or share data. For example, a staff member may access files in a firm's mergers and acquisitions practice, though they do not work in that department, attempting to use insider information for personal gain. This puts the client, the deal and the firm's reputation at risk and could have regulatory repercussions as well. Proper monitoring and UEBA can not only detect this behaviour, it can also automatically shut it down until it can be investigated.

Verdict

LogRhythm's NextGen SIEM Platform monitors your environment to detect malicious activity and enable a rapid response. Its embedded UEBA solution provides deep visibility into user activity, helping detect insider threats, compromised accounts, privileged account abuse, and other user-based threats. Security automation and orchestration (SAO) frees up time so in-house IT teams can focus on other important tasks and improving operational efficiency.

Network and data monitoring also support reports to verify activities and security for regulatory compliance and auditing requirements. In addition, LogRhythm's centralised solutions for dedicated log management and SIEM are designed for quick deployment and scalability.

In your defence

LogRhythm understands what law firms do and what they need to keep their businesses running smoothly, securely and profitably.

That's why LogRhythm brings everything to bear to defend those firms:

- SIEM
- UEBA (empowered by LogRhythm Cloud AI)
- Network monitoring
- Compliance reporting

[6] Understanding Your Organization's Security Culture Needs To Be at the Top of Your To-Do List
http://epubs.iltanet.org/i/900970-fall-2017/47

LogRhythm
The Security Intelligence Company

Law firms face intense regulatory and compliance oversight, as well as expectations from clients that they can demonstrate that robust processes and policies are in place for data protection, privacy and information security. Successful audits start with good records and LogRhythm's solutions support auditing requirements through Compliance Automation Suites with embedded content, and enable long-term and secure data storage as well as wizard-based data recovery.

LogRhythm's behavioural analytics extends to machine learning across long periods of time to establish baselines of normal user behaviour through our cloud-based AI offering. This enables unusual patterns of behaviour to be identified automatically and risk-based alerts indicating users that should be investigated further.

Together, LogRhythm's offerings provide law firms with industry-leading automation, compliance and auditing support, comprehensive reporting, and protection against advanced threats. With LogRhythm, the defence never rests.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralising damaging cyberthreats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA) and security automation and orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations centre (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

"LogRhythm provides real-time actionable intelligence within a single pane of glass based on events across my entire infrastructure and allows me to quickly isolate unusual network behaviour by a user, machine or network device."

Jason Riggins, network administrator, Kansas Medical Mutual Insurance Company

LogRhythm®

The Security Intelligence Company

Security. Made Smarter.

Contact us

UK: **+44 (0)1628 918 330**
Germany: **+49 89 919292 - 200**
Middle East & North Africa: **+971 55 6422224**
europe@logrhythm.com | **www.logrhythm.com**