Fortifying the Legal Firm

Law Firm Strategies for Addressing Evolving Cybersecurity Challenges

Shaped for law | **cts.co.uk**

CTS

Law Firm Strategies for Addressing Evolving Cybersecurity Challenges

CTS, in collaboration with LPM Magazine, conducted an exclusive roundtable discussion that brought together esteemed industry leaders from law firms nationwide. The topic of this event was centred around cybersecurity and what law firm leaders, both technical and non-technical, can do to help keep their firms, data and clients secure.

The discussions centred on these key issues: monitoring the changing security risk and how to review strategy for managing it, deciding where and when to invest in updated or new security before it's too late, and optimum threat response and business continuity planning.

Amongst our roundtable delegates, we were joined by representatives from Amphlett Lissimore, Coles Miller Solicitors, rradar, Sharpe Pritchard and Maurice Turner Gardner.

In its June 2023 report, the National Cyber Security Centre emphasised how evolving work patterns, accelerated by the COVID-19 pandemic, and the rising complexity of cyberattacks have rendered law firms more vulnerable. To kick off the discussion, the roundtable attendees were asked: **"How do you identify and stay updated on emerging security risks?"**

Identifying threats via media monitoring

After a brief mention of a recent news story about a law firm being reprimanded by the ICO due to an unreported data breach, one panellist emphasised the significance of monitoring the news and media as a critical practice for law firms aiming to stay informed about emerging cyber threats. News outlets and media sources offer up-to-the-minute updates on cybersecurity incidents and evolving threats, allowing law firms to gain valuable insights into the tactics used by cybercriminals and, consequently, strengthen their own security measures.

Another participant recommended leveraging online industry resources, like the National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO), for valuable practical guidance. Echoing this sentiment, another delegate championed Cyber Essentials as a valuable resource for law firms lacking Managed Services Provider support or extensive cybersecurity knowledge and experience.

Cyber Essentials, a government-backed program, effectively aids senior leaders in organisations of all sizes to protect against a broad range of common cyberattacks. A Cyber Essentials certification provides law firms with enhanced cybersecurity, increased client trust, regulatory compliance support, a competitive advantage, and streamlined security practices, all contributing to effective risk mitigation.

Artificial Intelligence: obsessed or opposed?

Digging deeper into the discussion of security concerns, the panel was questioned whether they or their respective firms had considered the influence of Artificial Intelligence (AI) on security. The roundtable facilitator also noted a varied response they had observed concerning generative AI, including ChatGPT.

> "Networking events, such as this roundtable, and speaking to similar firms and other industry leaders can be a brilliant way of sharing experiences and strategies and making sure you're on the right track."

ChatGPT, an AI-driven natural language processing tool, facilitates human-like conversations and performs various tasks, including answering questions and assisting with writing tasks, such as emails, essays, and coding. While it holds promising benefits, its potential risks remain uncertain, which is why one delegate's firm has taken a cautious approach by completely blocking the tool on internal work devices. Their concern centres around the challenge of controlling the data that end-users may input and where this data may ultimately be transmitted or stored.

Considering other forms of artificial intelligence, another delegate highlighted their firm's active use of AI technology for enhancing security measures. In their case, the firm has implemented an AI-driven cybersecurity solution, which employs advanced algorithms and machine learning to monitor network traffic and detect unusual patterns or anomalies that may indicate potential security threats. By continuously monitoring network behaviour, the firm can identify both known and emerging threats, thereby fortifying its defence against an evolving landscape of cyberattacks.

Partnering with a Managed Service Provider

Several attendees highlighted the strategic value of their Managed Service Provider (MSP) partnership, with one delegate taking the lead in explaining that their chosen MSP plays a pivotal role in ensuring the security and lockdown of a significant portion of their IT environment. With specialised expertise, their IT partner continuously monitors for emerging security risks and tailors solutions to align with the firm's unique needs and risk profile. This proactive approach significantly enhances the law firm's cybersecurity posture, ensuring readiness to combat both known and emerging risks in the ever-evolving cyber threat landscape.

Partnering with a legal specialist offers the assurance of their experience in handling the unique auditing and compliance requirements of law firms, including broader regulations such as GDPR. They should provide specialised services like ISO 27001 and Cyber Essentials PLUS to help law firms to achieve their objectives, all while understanding the intricacies of daily legal processes for tailored support.

The 2022 PwC Law Firms Survey found that the top 100 law firms allocate 0.46% of fee income to cybersecurity. As a result, the roundtable facilitators sought to gain a deeper understanding of **how the panellists' firms determine when and where to invest in updated or new security measures.**

Catalysts for increased investments

One delegate looked back on their firm's approach to cybersecurity investment approximately 3 to 4 years ago, a time when they pinpointed cyberattacks as the primary threat to their business. This recognition triggered a strategic pivot, resulting in a substantial boost in their IT and cybersecurity investments. Recognising the vulnerability of their SME firm, the delegate was acutely aware that the potential financial and reputational repercussions of a security breach were risks they couldn't afford to bear, and so, investment in cybersecurity measures were a necessity.

Similarly, another delegate shared a significant turning point in their firm's approach to security, which came in the wake of the Panama Papers scandal, which sent shockwaves through the legal and financial industries a few years ago. This high-profile incident, which involved the massive leak of confidential documents and data, served as a powerful wake-up call for their firm, who works with high-net-worth individuals and professional practices.

This increase in spending underscores the growing recognition within the legal industry of the critical importance of cybersecurity. As the digital landscape continues to evolve and cyber threats become more sophisticated, law firms are clearly taking proactive steps to safeguard their sensitive data, client information, and intellectual property.

The cost of strategic staffing

Expanding on the earlier discussion about MSP partnerships and the services they offer, one panellist mentioned that their IT partner primarily focuses on the day-to-day management their IT infrastructure but does not provide proactive strategic guidance. Consequently, this firm is actively in the process of hiring for a strategy-based role to address this specific gap in their capabilities.

Recruitment in the competitive legal industry poses a significant financial expenditure due to multiple cost components, including advertising, agency fees, interviews, and potentially higher senior role compensation. These expenses can substantially impact a firm's budget. High demand for legal talent further escalates recruitment costs. The decision to invest in recruitment is both strategic and financial, demanding careful management and consideration of long-term benefits in this competitive sector.

> "It's all about spending your money wisely because frankly, and unfortunately, it isn't a bottomless pit!"

End-user education

A recurring theme throughout the roundtable discussion was the ever-present and significant threat posed by end-users within the realm of cybersecurity. It became abundantly clear that while technological solutions and robust security frameworks are essential components of any cybersecurity strategy, the behaviour and actions of end-users can play a critical role in either enhancing or undermining the overall security posture of a firm.

The unanimous consensus among all the panellists highlighted the value of ongoing and comprehensive training for end-users within a law firm's cybersecurity strategy. The shared opinion was that this mandatory training should begin from day one of an employee's association with the firm and continue in a continuous and evolving manner.

Acknowledging the difficulty of maintaining employee engagement during recurring training sessions, one attendee shared a creative approach implemented by their in-house security team. They introduced gamification into their training regimen, incorporating quizzes, interactive games, and engaging videos. Upon successfully completing these gamified training modules, employees had the opportunity to earn tangible incentives, such as vouchers and monetary rewards.

Undoubtedly, investment in security awareness training is a fundamental step in cultivating a culture of security, stressing the shared responsibility of every individual within the firm in defending against constantly evolving cyber threats.

Due to the nature of the sector, law firms must acknowledge that cyberattacks are not just a possibility but a near certainty—an unavoidable “when” scenario. To get an idea of optimum threat response and business continuity planning, the roundtable attendees were asked: **what measures do you have in place of a breach occurring?**

The value of continuous testing

Defending against hackers demands attention on an hour-by-hour, minute-by-minute basis due to the swiftly changing cybersecurity landscape. All panellists agreed that continuous IT security testing is an indispensable component of a robust cybersecurity strategy. It involves systematically evaluating a firm’s IT environment, infrastructure, and systems to identify vulnerabilities, assess potential risks, and ensure that security measures are effective and up-to-date.

Recounting some security testing carried out at their firm, one of the delegates shared that, in an effort to gauge the resilience of their cybersecurity defences, they decided to employ password-cracking software to simulate potential attacks on their active passwords. The outcome of this thorough testing was both eye-opening and concerning: approximately half of the firm’s passwords succumbed to the password-cracking software within a mere two days.

Another described how their firm carries out period penetration testing (pen testing) once a quarter. They highlighted its significance in helping to identify and address security weaknesses, evaluating the effectiveness of security controls, and testing incident response capabilities.

> “I kind of consider pen testing sort of like a car’s MOT - it’s useful at the time but could be out of date five minutes after. However, it gives a good sense check and keeps the internal security team on its toes.”

Read the fine print

Circling back to the recent incident involving a law firm’s data breach, attributed to inadequate cybersecurity measures and confusion surrounding breach reporting responsibilities, numerous panellists underscored the significance of conducting thorough reviews of Managed Service Provider (MSP) and supplier contracts. This advice is particularly relevant when law firms engage with multiple suppliers operating in the same domain. Law firms must have a strong grasp of each party’s responsibilities and the extent of coverage within these contracts, to ensure there aren’t any gaps through which threats may enter.

Cyber insurance was another topic that all delegates deemed a vital element of staying prepared for a breach. However, it was acknowledged that obtaining cyber insurance has become more challenging for law firms due to the escalating threat landscape and the surge in cyberattacks. Insurers now require rigorous cybersecurity measures and comprehensive risk assessments before offering coverage, primarily driven by the increasing costs associated with breaches and the potential for extensive financial and reputational harm.

Furthermore, firms with insurance must fully understand the scope and restrictions of their coverage, including the types of incidents covered and financial limits, as well as make sure they are informed about the breach response process to maximise the benefits of their policy while avoiding potential pitfalls that could result in voided coverage or denied claims.

Responding to an incident

Highlighting the need for breach preparedness, one delegate stressed the importance of law firms having a strong incident response plan in place.

While the legal sector is taking a notable step forward, with approximately 2-in-5 firms having an incident management process in place, it's important to note that this remains the least addressed area in the Government's 10 Steps to Cyber Security guidance across organisations.

The plan must outline procedures for detecting, reporting, and classifying incidents, as well as immediate response actions and a communication strategy for both internal and external parties. Legal and regulatory compliance, technical response measures, evidence handling, recovery, and post-incident analysis should also be specified.

Such a plan serves as a structured framework for early detection and mitigation of security incidents, ensuring clear communication, legal compliance, and the preservation of crucial evidence. It enables firms to effectively recover from breaches, learn from the experience, and, ultimately, regain client trust.

Business continuity comeback

Finally, as the roundtable concluded, the conversation shifted from incident response to business continuity, in particular the creation, testing and execution of a Business Continuity Plan (BCP).

Establishing a robust Business Continuity Plan (BCP) goes beyond merely drafting a strategy on paper. It involves the critical phase of practical implementation and live testing – a necessary step for instilling confidence, not only within your law firm but also among your clients.

When there's an active threat or crisis situation, the ability to demonstrate a well-executed BCP becomes paramount. In today's landscape, where security threats are prevalent, panels and clients are increasingly seeking concrete evidence of effective BCPs. They want assurance that firms can not only prevent but also efficiently recover from disasters or disruptions. Live testing serves as a tangible validation of your firm's readiness and resilience, reassuring both internal stakeholders and clients that your Business Continuity Plan is primed for action when needed.

CTS

Head Office
7450 Daresbury Park
Daresbury
Cheshire
WA4 4BS

London Office
33-39 Bowling Green Lane
London
EC1R 0BJ

0345 872 4400

hello@cts.co.uk

www.cts.co.uk