Browne Jacobson

Cyber and data

13 February 2025

In 2024, the insurance sector had to grapple with significant changes to the cyber security landscape, with new forms of sophisticated cyber attacks targeting financial and confidential information.

Given the increase in complexity of attacks and the risk to clients of losing confidential data, this is a clear concern for law firms and their clients.

The insurance industry will need to adapt to the rapid advancement of cyber attacks. This adaptation is particularly crucial as threat actors increasingly leverage artificial intelligence and machine learning to breach traditional security measures, while simultaneously targeting vulnerabilities in the expanding Internet of Things (IoT) ecosystem.

The recent Synnovis incident serves as a stark reminder that even well-protected organisations can fall victim to determined cyber criminals, highlighting the need for both robust preventive measures and comprehensive incident response strategies. As we examine these challenges, it becomes clear that the intersection of cyber security, data protection, and insurance coverage requires a nuanced understanding of both technical and legal frameworks.

Articles in this section:

The evolving digital battlefield for law firm clients' confidential

Author: Francis Katamba

In 2024, the insurance sector had to grapple with significant changes to the cyber security landscape, with new forms of sophisticated cyber attacks targeting financial and confidential information. Given the increase in complexity of attacks and the risk to clients of losing confidential data, this is a clear concern for law firms and their clients. The insurance industry will need to adapt to the rapid advancement of cyber attacks.

Arup's cyber-attack example and warnings from legal regulators and insurers

In January 2024, an Arup Hong Kong employee was invited to a video conference with the firm's CFO and other colleagues, during which the CFO instructed the employee to transfer HK200m (c. USD25m) to several local bank accounts. The employee left the video call and completed the transactions only to later discover that they had never actually spoken to the CFO or any other colleagues. The video call participants had been deepfakes: video impersonations created by an AI system using publicly available video and audio footage to resemble the CFO and other staff. The entire interaction was an elaborate targeted cyber attack to defraud the company.

Law firms are particularly at risk of being targeted. Unsurprisingly, professional legal bodies and regulators are urging their members to prepare for the unique risks that AI-enhanced cyber attacks pose to firms.

In March, the UK Law Society, in partnership with Travelers Europe published an article warning members that the risk of cyber attacks is especially acute for law firms and that AI-driven attacks could allow cyber criminals to launch far more advanced and fast-acting threats. The UK Law Society's regulatory arm, the Solicitors Regulatory Authority (SRA) updated its anti-money laundering guidance to its members, warning that they should be aware of the increasing risk that remote interactions with clients might be deepfakes. The SRA has been clear that "ultimately the firm is responsible for its own compliance, and this responsibility can never be outsourced".

Cyber attacks on law firms pre-AI

Law firms are prime targets for cyber criminals, who are drawn to both their confidential client information and the substantial client funds they hold.

According to Chaucer, UK law firms reported 226 cyber breaches last year; marking an increase of 36% from the previous year.

Perhaps not surprisingly, government watchdogs like the UK National Cyber Security Centre (NCSC) have been raising awareness, warning firms that they make particularly enticing targets. The special combination of factors such as large caches of client data; well-funded client accounts with frequent, urgent transactions; the severe impact that network downtime can have on billable hours; and the particular importance of trust and reputation to firms are pointed out by the NCSC as reasons law firms may be particularly vulnerable to attacks.

The main types of attacks that the NCSC warned firms they might face will probably be familiar in name if not in nature.

- **Phishing:** Criminals use scam communications to trick employees, often to make recipients visit a website which will then download malware (such as ransomware or a virus) or steal bank details and other personal information (such as login details).
- **Business email compromise:** A targeted form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds or revealing sensitive information by impersonating a representative of the law firm.
- **Ransomware and other malware:** Malicious software mistakenly downloaded onto a network which often results in data being encrypted by the attacker. The attackers will often download the sensitive data and leave a ransom note threatening to publish the data if a ransom isn't paid.
- **Password attacks:** Attackers exploiting vulnerabilities in weak passwords, open systems, and lack of multi-factor authentication.
- **Supply chain attacks:** It is common for firms to outsource their IT and data needs to specialist support companies. Firms are still vulnerable if their supplier has not adequately secured their network.

Despite the warnings, determined cyber criminals still manage to threaten even the largest, most well-resourced firms. Hackers reportedly attacked US firms Kirkland & Ellis, K&L Gates and Proskauer Rose in June last year, along with 50 other multinational corporations. Later in November 2023, hackers targeted Allen & Overy amid its high-profile merger with US firm, Shearman & Stirling.

The dawn of the AI cyber attack and the initial response of legal regulators

Predictably, just as it seems that watchdogs and firms are getting to grips with the 'traditional' cyber attack methods and hardening systems against them, a new threat emerges.

It is impossible to read any press without coming across a multitude of articles about the enormous potential to use new and developing AI systems to increase productivity at work. Leading AI developers are already adapting their models for the legal market and testing them with legal services providers, such as OpenAI and PwC, and reportedly 26% of legal professionals are using large language models at least once a month.

Unfortunately, but perhaps unsurprisingly, cyber criminals have been quick to adopt various forms of new AI technology to their advantage. Last year, the NCSC published its predictions about the near-term impact of AI on cyber crime through 2025.

Cyber attackers are expected to increasingly leverage AI to enhance the effectiveness of their existing tactics:

- **Phishing:** AI will significantly improve the success of social engineering, particularly through generative AI.
- **Ransomware delivery:** Attackers are already using AI to boost the effectiveness and efficiency of phishing attempts that deliver ransomware and other malware.
- **Ransomware development:** AI has the potential to generate malware capable of evading detection by current security filters, according to the NCSC.
- **Exploitation of stolen data:** The NCSC warn that AI's ability to quickly summarise data will likely enable cyber attackers to identify and target high-value assets, amplifying the damage caused by attacks in the next two years.

- **Source of AI attacks:** The NCSC also cautioned that most sophisticated attacks are likely to come from “highly capable state actors” with the resources and data necessary to create their own AI models.

Even more worryingly, as the Arup example demonstrated, cyber criminals are using AI tools to attack organisations in completely new ways. The UK Cabinet Office has published guidance warning the public about an expected surge in deepfake disinformation to mislead the public about candidates and the elections. Obviously, this novel method of attack will not be limited to the public sector; in an article published in May, Deloitte highlighted reporting that the fintech sector has seen a 700% increase in deepfake and predicted that fraud losses from generative AI could experience rapid growth reaching US$40bn in the United States by 2027 from US$12bn in 2023.

Looking ahead

Insurers and their law firm policyholders must be aware of the ever-evolving cyber security landscape to appreciate the new forms of cyber attacks and to understand how law firms are putting controls in place to mitigate against any potential cyber breaches.

To properly evaluate an insurance claim after a cyber attack, it’s crucial to understand the technical details of how the breach occurred and how it was handled, including the response measures taken and security controls in place.

Synnovis: lessons from a recent cyber attack

Author: David Henderson

The 2024 Synnovis ransomware attack highlights practical steps companies can take when facing a potential cyber threat, offering key guidance for victims and critical considerations for response. When assessing insurance claims related to such incidents, the ‘prepare, respond, and recover’ framework serves as a valuable tool for evaluating how well a company managed the risks and aftermath of an attack.

What should I do if I think I am a victim of the recent NHS ransomware attack?

In 2024 the NHS was again the victim of a ransomware attack; a type of cyber attack where criminals prevent users from accessing their device and the data stored on it (usually by encryption) before demanding a ransom payment to restore access.

In the event of a potential cyber attack, the information and response measures detailed in the Synnovis cyber incident documentation can be extremely useful. For further guidance on safeguarding against ransomware, the NCSC website provides additional resources.

Why are the legal risks associated with ransomware particularly hard to manage?

From a legal perspective, managing the risk of ransomware is very complex. Ransomware attacks present the usual regulatory challenges associated with having to apply ‘appropriate’ security measures and other controls to protect personal data. However, this complexity is intensified by the fact that the Information Commissioner’s Office (ICO), and other regulators, are opposed to the making of payments to cyber criminals. Even though, in some cases, this may be the only way to recover critical data. Complicating matters further, there is also a risk that the payment of ransomware demands could in certain circumstances breach money laundering, terrorist financing, sanctions or other very serious criminal laws.

What should companies consider when implementing a plan to deal with these risks?

The only way for organisations to manage their cyber security risks responsibly is to have in place a plan that is risk-based, proportionate and tailored to their organisation’s needs.

This plan should consider the ransomware and clearly set out the steps they have taken to:

- **Prepare** for and minimise their exposure to cyber attacks;
- **Respond** to and minimise the impact of a successful cyber attack; and
- **Recover** from and learn the lessons from cyber attacks, incidents and near misses.

As with all data protection and cyber risks, many of the issues that result from a breach are predictable. However, making the right decisions in the aftermath of a breach is much more difficult and stressful, as organisations often find themselves struggling to determine

the best course of action.

Where can I find out more?

There is so much information on the internet it is often difficult to know where to begin. A good starting point for GCs, DPOs, in-house lawyers and others grappling with the data protection compliance aspects of ransomware is to consult the ICO website.

Building truly effective governance and compliance is a team effort that will only succeed if specialist expertise across multiple disciplines (legal, IT, risk, HR etc.) is combined with strong leadership and commitment at all levels of an organisation.

The NCSC Cyber Security Toolkit for Boards provides another valuable resource to help build or improve upon a cohesive approach to managing cyber risks at an enterprise level.

Implications for insurers

While the advice above is targeted at companies, it can also be valuable for insurers, particularly in their underwriting. Underwriters should carefully consider their proposers' response strategies in the event of a cyber attack. For example, does the proposer follow the 'prepare, respond, recover' approach, and do they have a response protocol prepared that allows them to react quickly to any cyber attacks. This will be crucial to minimising the impact of an incident. If the proposer has had a previous attack, considering the company's preparation, how it responded to minimise the impact, and how it is recovering from the cyber breach will go a long way to highlight how seriously the company took the risk when assessing any subsequent claims.

Mandatory cyber security requirements for businesses in the 'Internet of Things' (IoT) supply chain

Author: David Henderson

In 2024, new cyber security legislation came into effect mandating cyber security standards for IoT devices. Businesses involved in the manufacture, import or distribution of consumer-facing IoT devices may need to implement mandatory cyber security controls or face a range of penalties under the UK Product Security & Telecommunications Infrastructure (Product Security) regime (PTSI regime). This guidance explains which businesses might be caught by the new PTSI Regime, what they must do to comply, and the potential legal consequences if they don't meet their statutory requirements.

Policyholders and brokers should consider whether losses arising from non-compliance with PTSI standards are covered by their current policy wording.

The PTSI regime

The regime came into effect on 29 April 2024 and comprises two pieces of legislation:

- PTSI Act 2022; and
- PTSI (Security Requirements for Relevant Connectable Products) Regulations 2023.

Scope of the PTSI regime

The regime applies to manufacturers (or their UK representatives), importers and distributors ("relevant persons") of certain consumer connectable products that can connect to the internet or other networks and can transmit and receive digital data ("relevant connectable products"). Commonly referred to as IoT or smart devices, relevant connectable products include devices such as smartphones, smart TVs, smart speakers, connected baby monitors and connected alarm systems.

Products such as charge points for electric vehicles, medical devices, smart meter products and personal computers may be exempted from the regime. However, this should always be assessed carefully as it may depend on the precise use case. For example, tablet computers that can connect to cellular networks may be caught by the regime.

Compliance with the PTSI regime

Manufacturers of relevant connected products will be required to ensure, amongst other things that:

- Security requirements are met, including the use of passwords that meet prescribed standards;
- Statements of compliance are published which confirm that applicable security requirements have been met;

- Cyber security issues are monitored and, where appropriate, investigated, dealt with and reported on.

Importers, distributors and authorised representatives are also required to support compliance with the regime and all relevant persons must take reasonable steps to prevent non-compliant products being supplied to consumers.

Penalties for non-compliance

The PTSI regime gives the Secretary of State for the Department for Science, Innovation Technology (DSIT) considerable enforcement powers, including the ability to withdraw products from the market and impose fines of up to £10 million or 4% of worldwide turnover in the previous accounting year (whichever is greater).

However, the Office for Product Safety & Standards (OPSS) which will act as the enforcement authority for the new regime has explained that its approach will be pragmatic, proportionate and aligned with its Enforcement Policy.

Next steps

The stated policy objective of the PTSI regime is to ensure that businesses in this space reflect good practices set out in the European Telecommunications Standards Institute (ETSI) guidelines, and the UK government's Code of Practice for consumer IoT security.

For companies involved, directly or indirectly, in the supply of IoT devices or other consumer-facing connectable products, it is important that they understand whether they are in scope of the PTSI regime, and any obligations or potential liability for non-compliance this might trigger and discuss this with their broker. Equally, insurers should be mindful of this potential new liability for their policyholders.

Previous
Management liability

Next
Medical malpractice

Underwriting and policy wordings →

Regulatory →

Contact

Francis Katamba

Partner

francis.katamba@brownejacobson.com

+44 (0)330 045 2725

David Henderson

Principal Associate

david.henderson@brownejacobson.com

+44 (0)20 7337 1023

Related expertise

Digital and data

Financial services and insurance advisory

Insurance claims defence