



## Cyber Security and the impact on insuring your law firm

## Cyber Risk for the Law Sector

While cyber risk and resilience are not unique to the law sector, this sector is seen as a very attractive target for cybercriminals.

The UK legal sector is both large and diverse; it is made up of many organisations from small solicitors to large multinational entities. In early 2023, it was reported that there were more than 32,000 organisations with a combined revenue of more than £43 billion and an employee count of more than 320,000. This makes the legal sector a huge target for cybercriminals. The data that is held along with the management of clients' money and assets means a successful attack can result in a high-value return.

**The Solicitors Regulation Authority (SRA) principles include cyber risk within their standards:**

- Protect client money and assets.
- Act in the best interests of each client; protect client confidentiality.
- Implement Governance, Financial and Risk Management.

The Law Society Scotland has published several whitepapers and continues to educate and help law firms address the significant risks.

**They have shared their 5 legal obligations that should not be ignored:**

- Assess the risk
- Put protections in place
- Regular testing
- GDPR
- Demonstrate compliance

Given the ethical and fiduciary responsibilities that solicitors and lawyers are held to, more so than many other organisations, you can see why this sector is at one of the greatest risks.

In 2022, CERT-UK reported that 65% of UK law firms had been a victim of a cyber incident. Over £4 million of client money was stolen from just 23 UK law firms who reported suffering a cyberattack.

**In summary, the law sector is at high risk due to:**

- Large volumes of financial transactions involve large amounts of money.
- Client-sensitive information is exchanged in significant volumes.
- The diversity of the law sector is made up of many smaller firms unable to invest funding and resources like their larger counterparts.
- Reputation is everything to a law firm.

**What are the greatest risks?**

- Email: the most common attack vector used to deploy many types of attacks including phishing, BEC (business email compromise) and ransomware.
- Ransomware: shifting away from random attacks to targeted attacks from criminals to access specific client-sensitive information.
- Supply chain risk: as law firms increase security, indirect attacks are also increasing. These involve attacking a 3rd party who is an easier target and using them as a stepping stone to attack the intended target.

**Other factors that reduce risk:**

- Culture: a blame culture is needed to ensure early reporting when something goes wrong.
- Employees: your employees are your best line of defence if your IT systems don't stop the threat, so invest in them!
- Risk management: the process needs to include IT systems and infrastructure, and the adoption of best practices to reduce overall risk.
- BCP/DR: business continuity planning (BCP) and disaster recovery (DR) are required to ensure you can continue to operate and/or recover should the worst happen.

## Cyber & Insurance

Before we move into reviewing how cyber risk can impact your ability to obtain or renew your insurance, I want to be clear that Net-Defence is not an insurance expert; our area of expertise lies within cyber resilience and IT.

At its inception, cyber insurance was an additional or complimentary offering on top of other policies such as professional indemnity. This is no longer the case as insurance brokers and insurers have extended their due diligence in the last several years. Some organisations and businesses are now finding they are unable to obtain cyber insurance or, even worse, are unable to renew a policy they have held, in some cases for many years.

The due diligence now often includes demonstrating evidence of best practices in how you are reducing your cyber risk.

If you have insurance or company-specific questions these should be referred to your insurer or broker.

As with any insurance, the cost and coverage are dependent on the controls and security measures you have in place. It is a balance between what coverage you require and the cost you are prepared to pay. Implementation of IT best practices and obtaining relevant certifications can reduce your insurance costs.

If you are not able to meet the insurer's expectations, you may find yourself not being able to obtain insurance or renew a previous policy, even if you have never made a claim.

## Professional Indemnity Insurance (PII)

**This insurance is mandatory for all law firms, and several factors will determine your ability to obtain or renew your policy:**

- Claims history
- Risk management practices
- Areas of practice and expertise
- Disciplinary and regulatory history
- Ability to meet uncovered claims (claims for more than you're insured for)

Risk is present for all work carried out in the legal profession, but this can vary considerably. Below is an idea of the type of legal work, and where the professional indemnity claims come from.

- **Low risk:** adjudication, agency, children work, criminal, expert witness, immigration, officers and appointments.
- **Medium risk:** defendant litigation, employment, matrimonial, personal injury, town planning.
- **High Risk:** commercial litigation, estate agency, financial advice, intellectual property, probate, trusts and wills, tax planning.
- **Very high risk:** conveyancing, commercial work (public and non-public companies).

Cyber security and resilience are directly linked to your **risk management processes**.

The good news? Cyber security and resilience are not complex and not as expensive, despite what you might have heard. Preparation and prevention are your best allies in this battle.

## Preparation

**Risk management** is a process that allows risk to be understood and managed proactively, minimising threats and maximising opportunities.

There are many different risk frameworks being used across the world, most of which have the same common elements.

**Steps to any effective risk management process include:**

- Identify the risk.
- Assess business harm, impact and probability
- Calculate overall risk exposure
- Prioritise and treat the risk
- Monitor the risk.

**Business continuity planning** (BCP) is about having a plan to deal with difficult situations so that your organisation can continue to function with as little disruption as possible. This plan needs to account for people, locations and processes based on criticality. The process is designed to understand the critical employees, critical time periods and your dependency on your offices.

**Disaster recovery** (DR) is a plan designed to recover the IT and infrastructure after a disaster. A DR plan comprises recognising crucial IT systems and networks, categorising the RTO, and reporting the activities required to resume, reconstruct, and recover IT systems and networks. DR is part of the overall BCP.

**Recovery Point Objective** (RPO) is the tolerable amount of data the organisation is prepared to lose.

**Recovery Time Objective** (RTO) is the amount of time needed to recover critical systems and applications.

## DR Assessment

The industry standard for assessing IT systems and applications is known globally as the CIA Triad. This is made up of 3 key concepts: Confidentiality, Integrity & Availability.

### Confidentiality (Access Control)

Confidentiality means ensuring that information is accessible only to those authorised to have access.

### Integrity (Accuracy)

Integrity means safeguarding the accuracy and completeness of the information.

### Availability (Accessible)

Availability means ensuring that authorised users have access to information and associated systems when required.

Using a scoring matrix based on 3 points, (High, Medium, Low) each application is assessed separately and then ranked against each other.

Combined, BCP will allow you to keep the organisation operating should the worst happen, while DR will lead the recovery of IT systems & infrastructure.

## Prevent

Risk assessments and action plans are the best way to identify and mitigate risk. This can be done through the Cyber Essentials Scheme, Cyber Assurance Certifications and ISO certifications. These schemes are designed to protect organisations from the most common cyber threats, prevent loss and support recovery.

By ensuring you have “prepare” and “prevent” measures in place you will be able to demonstrate to your insurance broker/insurer you have taken the appropriate action to reduce your cyber and IT risk.

## Cyber Insurance

In years gone by, obtaining cyber insurance was reasonably straightforward. In the last few years, the marketplace has gone through unprecedented changes, impacting insurers and clients across the world.

It has been widely publicised that 2020 & 2021 were very turbulent and significantly unprofitable across the globe. This forced carriers to slow down and, in some cases, halt underwriting new businesses, reducing limits and coverage for renewals.

Just as cyber threats have evolved, so has obtaining insurance against them. Underwriting methodology has transformed, not just with regard to limits and coverage but also minimum controls that an organisation must have in place to deem the risk insurable.

## Changes during 2023

- Gallagher, a global insurance, risk management & consulting firm is reporting rate reductions of between 10% and 30% for organisations that have demonstrated their cyber security and controls.
- Claims continue to increase, but the severity is showing a reduction versus 2022, due to the increased levels of security of their clients.
- Coverage and limits are starting to increase.

## Looking Forward

- **Underwriting:** due diligence and focus on IT controls will continue.
- **Limits:** caps will continue to be reduced, especially when adequate IT controls are not in place.
- **Price:** the cost of insurance is likely to be driven down by competition, hoping to recover from 2021/2022 losses.
- **Coverage:** exclusions are forecasted to increase, particularly if you are not able to demonstrate your controls.
- **State of the market:** it remains unstable and in a constant state of flux, which will impact those looking to insure against cyber criminals.

**Cyber Insurance** is designed to cover against a cyber event. This is a malicious action or an accidental event on an organisation's digital systems, data or technology.

**Impact of an event:**

- **Non-physical:** compromise of the confidentiality, integrity and/or the availability of digital systems, data and or technology.
- **Physical:** property damage and/or bodily harm and injury.

**Consequence of an event:**

- Loss of income
- Extortion/ransom demands
- Fines and penalties
- Negligence
- Shareholder litigation
- 1st party costs (insurance)
- 3rd party liability (if the organisation is sued)

The **due diligence** process includes a review of your Cyber Resilience. These are 12 key information security controls. While they have been established for several years and considered best practices, many organisations have not adopted them.

**The 12 controls are as follows:**

- **Multi-factor Authentication:** Additional electronic identity authentication.
- **End Point Detection & Response (EDR):** A solution to detect and respond to attacks on endpoint devices (e.g. anti-virus).
- **Back-ups:** Secure, encrypted backups, stored in a separate and secure location. Tested (monthly) for recovery.
- **Privileged Access Management (PAM):** An information security mechanism that safeguards identities with special access or capabilities beyond regular users.
- **Network Protection:** Network security protects your network and data from breaches, intrusions and other threats.
- **Email filtering & web security:** Email scanning for undesired content, categorising (e.g. spam, junk, viruses and malware) and taking specific actions (e.g. block, move to junk). Web filtering is restricting access to certain websites or those that have malicious content.
- **Patch & Vulnerability Management:** Vulnerability management refers to the process of discovering, identifying, cataloguing, remediating, and mitigating vulnerabilities found in software or hardware. Patch management refers to the process of identifying, testing, deploying, and verifying patches for operating systems and applications found on devices.
- **Cyber Incident response planning & testing:** Incident response is a term used to describe the process by which an organisation handles a data breach or cyberattack, including the way the organisation attempts to manage the consequences of the attack or breach.
- **Cyber security awareness training and phishing testing:** Information Security Awareness Training: your employees are your best line of defence if your IT systems don't stop the threat. Simulated phishing and other email-based attacks test and educate your employees.
- **Hardening Techniques including remote desktop protocol (RDP):** Hardening techniques are processes to reduce means of attack by taking specific actions (e.g. turning off non-essential services). Remote desktop protocol (RDP) is a secure connection that enables IT support to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers.
- **End of life management:** Protocols and processes to ensure that, when hardware and software are no longer maintained or supported, it is removed/replaced.
- **Vendor/digital supply chain risk management:** Processes to identify, assess and mitigate risk in your end-to-end supply chain with the intention to prevent issues and loss mitigation if issues do occur.

The 12 controls are assessed as part of risk assessments completed through Cyber Essentials Scheme and IASME Cyber Assurance Certifications, designed to protect organisations from the most common cyber threats and loss of IT.

## What is not covered by cyber insurance?

Cyber insurance does not transfer all risk, and it is not a substitute for having robust cyber risk management in place.

It will allow some costs from an incident to be recovered, it can provide specialist support to manage the immediate crisis and can sometimes allow a ransom payment to be made.

**There are a number of issues that will not be resolved by having insurance in place. These include:**

- The cost of time lost in resolving the issue
- The cost of loss of ability to operate/ fee earners being unable to work
- Loss of reputation
- Impact on explaining to clients that their data has been breached
- Time lost in reporting the incident to the Information Commissioner's Office (ICO), the Solicitors Regulation Authority (SRA) and law enforcement agencies

The National Cyber Security Centre (NCSC) notes that: "cyber insurance will not instantly solve all of your cybersecurity issues, and it will not prevent a cyber breach/attack. Just as homeowners with household insurance are expected to have adequate security measures in place, organisations must continue to put measures in place to protect what they care about."

## Summary

**The law sector is high risk due to:**

- Large volumes of financial transactions involving large amounts of money
- Client sensitive information is exchanged in significant volumes
- During/post COVID-19: Moving to online, digital and remote platforms for daily operations and remote working.

**What are the greatest risks:**

- Email: According to the SRA, four out of five cybercrimes reported involved email
- Ransomware: shifting away from random attacks to targeted attacks by criminals to access specific client sensitive information
- 3rd parties & providers: as law firms increase security, indirect attacks are also increasing. These involve attacking a 3rd party who is an easier target and using them as a stepping stone to attack the intended target

**Other factors that increase risk:**

- Culture: a no-blame culture is needed to ensure early reporting when something goes wrong
- Employees: your employees are your best line of defence if your IT systems don't stop the threat
- Risk Management: process needs to extend to include IT systems and infrastructure and the adoption of best practices to reduce overall risk
- BCP/DR: business continuity planning (BCP) and disaster recovery (DR) are required to ensure you can continue to operate and/or recover should the worst happen.

## Cyber Risk

Cyber risk is the chance of exposing business information and communication systems to an unauthorised person or circumstances capable of causing loss or damage.

Risk implies the likelihood or probability of an event occurring.

Therefore, combined, this is the risk-based probability of a bad event happening to your business's information systems, leading to the loss of confidentiality, integrity or availability of your system.

Risk can originate from anywhere, including an attack, 3rd party vendors/suppliers with weak security, internally from a rogue employee, by accident or from failure to adopt security best practices.

## Prepare

Implement a **Risk Management** process to manage risk proactively, minimising threats.

**Steps to any effective risk management process:**

- Identify the risk
- Assess business harm, impact and probability
- Calculate overall risk exposure
- Prioritise and treat the risk
- Monitor the risk

Implement **Business Continuity Planning (BCP)** and **Disaster Recovery (DR)**. BCP will allow you to keep the organisation operating should the worst happen, while DR will lead the recovery of IT systems & infrastructure.

## Prevent & Certify

**Prevent:** risk assessments and action plans are the best way to identify risk and mitigate this. This can be done through the Cyber Essentials Scheme and IASME Cyber Assurance Certifications.

**Cyber Essentials Certification** gives you peace of mind that your defences will protect your business against the vast majority of common cyber-attacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

Cyber Essentials Plus gives you the added reassurance of an independent assessment.

**Scope/Controls:**

- Firewalls
- Secure Configuration
- User Access Control
- Malware Protection
- Security Update Management

The IASME Cyber Assurance was developed over several years during a government-funded project to create a cyber security standard which would be an affordable and achievable alternative to the international standard, ISO 27001.

The IASME Cyber Assurance standard allows the small companies in a supply chain to demonstrate their level of cyber security for a realistic cost and indicates that they are taking good steps to properly protect their customers' information.

The IASME Cyber Assurance level 2 gives you the added reassurance of an independent assessment.

**Scope/Controls:**

- Risk Assessment
- Backup
- Policies
- Incident Management
- Data Protection
- Operation Management

When obtaining insurance, the due diligence process includes a review of your Cyber Resilience. These include 12 key information security controls, which are embedded within Cyber Essentials and Cyber Assurance certifications. Remember, having insurance does not prevent you from being attacked, nor will it recover all of the costs related to an incident.

Protect your law firm with Cyber Essentials certification. Our expert team can guide you through the process, ensuring your firm is equipped to mitigate cyber threats and safeguard sensitive data. Contact us today to learn more about how Cyber Essentials can benefit your practice.