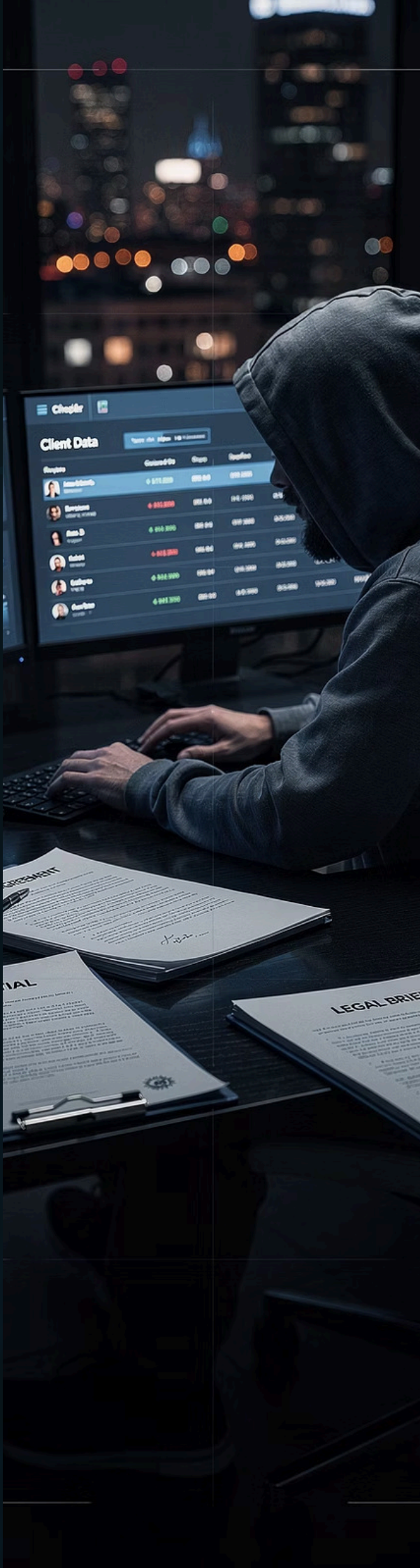
The Top 3 Cybersecurity Priorities - Every Law Firm Must Address

Why the Legal Sector is being Targeted

Law firms are prime targets for organised cybercrime due to their high-value client data, significant financial transactions, and time-critical casework, all of which attract threat actors.

UK threat reports consistently show law firms face high rates of phishing, email compromise, and ransomware. Alarmingly, most initial breaches stem from manipulated employees.

> Cyber criminals do not break into law firms, they are invited in.



Info@cybersecurityaware.net

OPTIMISE

Hello,

Chris Annetts - Former UK Lead Cyber Incident Coordinator at the NCSC and founder of Optimise Cyber Solutions

As the UK's Lead Cyber Incident Coordinator at the NCSC, I guided numerous organisations through severe and intricate cyber incidents. This experience offered a unique insight into the critical elements dictating success or failure against cyber threats.

A critical factor consistently determined the outcome: **the readiness of the people within the organisation.** This proved the ultimate differentiator between rapid recovery and prolonged chaos.

This guide, drawing from first-hand experience, outlines three core priorities to effectively reduce cyber risk for modern law firms, building resilience from the inside out.

Priority 1, Build Human Defence Through Training

The Reality

Over 90% of cyber incidents start with human manipulation. Attackers exploit trust via phishing, fraudulent calls, and impersonation to bypass technical security, leading to costly mistakes.

What This Looks Like in Practice

An urgent email, seemingly from a client, requests a last-minute bank detail change for a high-value transaction. Funds are transferred to a criminal account.

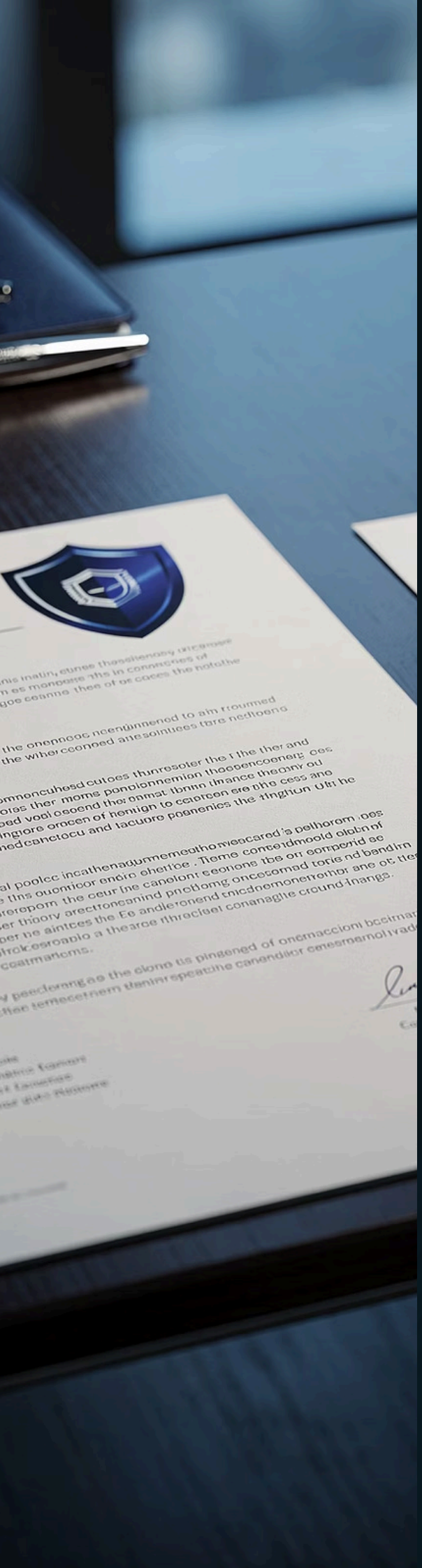
A partner receives a call from a fake IT provider, warning of suspicious activity and requesting immediate verification, capturing login credentials.

A legal assistant opens a malicious document related to an active case, installing malware and providing access to internal systems and client data.

What Leading Firms Do

Leading firms implement continuous, practical cybersecurity awareness training to help staff recognise manipulation, verify requests, and report concerns. This is reinforced with regular simulated exercises, clear verification procedures, and visible leadership support for secure behaviour.

- Well-trained firms routinely reduce successful attacks by up to 90%.



Priority 2, Protect Insurance and Regulatory Position

The Reality

Cyber insurance no longer offers automatic protection; policies demand clear evidence of ongoing staff training and robust cyber governance to avoid delayed or rejected claims. Firms must satisfy strict regulatory expectations from bodies like the SRA and UK GDPR, alongside increasing client and supply chain scrutiny.

What This Looks Like in Practice

- Incomplete training records after a ransomware attack lead to reduced insurance cover.
- A data breach exposes untrained staff, escalating regulatory investigations.
- Malware from a compromised supplier highlights a lack of evidenced due diligence.

What Leading Firms Do

Leading firms maintain formal training records, conduct regular risk and compliance reviews, and document robust incident response plans. They also embed leadership ownership of cyber risk and meticulously review supplier security, thereby strengthening insurer confidence, their regulatory position, and client trust.

Info@cybersecurityaware.net

Priority 3, Prepare for the Inevitable Incident

The Reality

Every firm will face a cyber incident. The first minutes and hours determine the scale of financial loss, regulatory impact, and reputational damage.

Without preparation, even highly capable teams struggle to make sound decisions under pressure.

What This Looks Like in Practise

Phishing compromises staff account. Delayed reporting leaves systems exposed for days.

Ransomware spreads. Uncoordinated communications disrupt client services, escalating reputational damage.

Confidential case files accessed. Delayed reporting increases regulatory exposure.

What Leading Firms Do

They ensure all staff know how to report incidents, define leadership and response roles, prepare communication templates and escalation routes, rehearse incidents through structured exercises, and establish external support in advance.

Final Guidance for Law Firms

The most effective cybersecurity investment is in your people.

Whilst technology is crucial, trained staff and clear processes determine if a minor disruption becomes a business-threatening crisis.

Protect Clients

Embed cybersecurity awareness into daily operations.

Protect Revenue

Safeguard revenue and financial stability with strong cybersecurity.

Protect Reputation

Maintain reputation by preparing for cyber threats.

Taking Action

- Assess and update staff cybersecurity training.
- Regularly review and test incident response plans.
- Audit cyber insurance for adequate coverage.
- Establish external cybersecurity expert support.

Proactive firms minimise risk, build resilience, and inspire client confidence. Investing in your people is imperative for survival and success, especially as a staggering 95% of all cybersecurity breaches involve human error.

Info@cybersecurityaware.net

Produced by Optimise Cyber Solutions

A Practical Next Step

Many firms reach out after recognising the same challenges described in this guide, rising cyber threats, increasing insurance scrutiny and growing client expectations.

At **Optimise Cyber Solutions**, we are an NCSC accredited company, which specialise in strengthening the human side of cybersecurity for law and professional services firms through tailored awareness training, leadership level incident management exercises and support in building incident response capability from the ground up.

Our programmes are designed and overseen by former UK national cyber incident leadership and delivered by practitioners with real world incident response experience. Training is delivered face to face, live online or through continuous learning programmes to fit the operational needs of each firm.

> For firms looking to take practical steps towards strengthening resilience, we are always happy to have an informal conversation.
>
> Email us on: info@cybersecurityaware.net
>
> Visit us at: www.cybersecurityaware.net
>
> Call us on: 020 4617 7373 or 01226 694040

OPTIMISE

CYBER SOLUTIONS