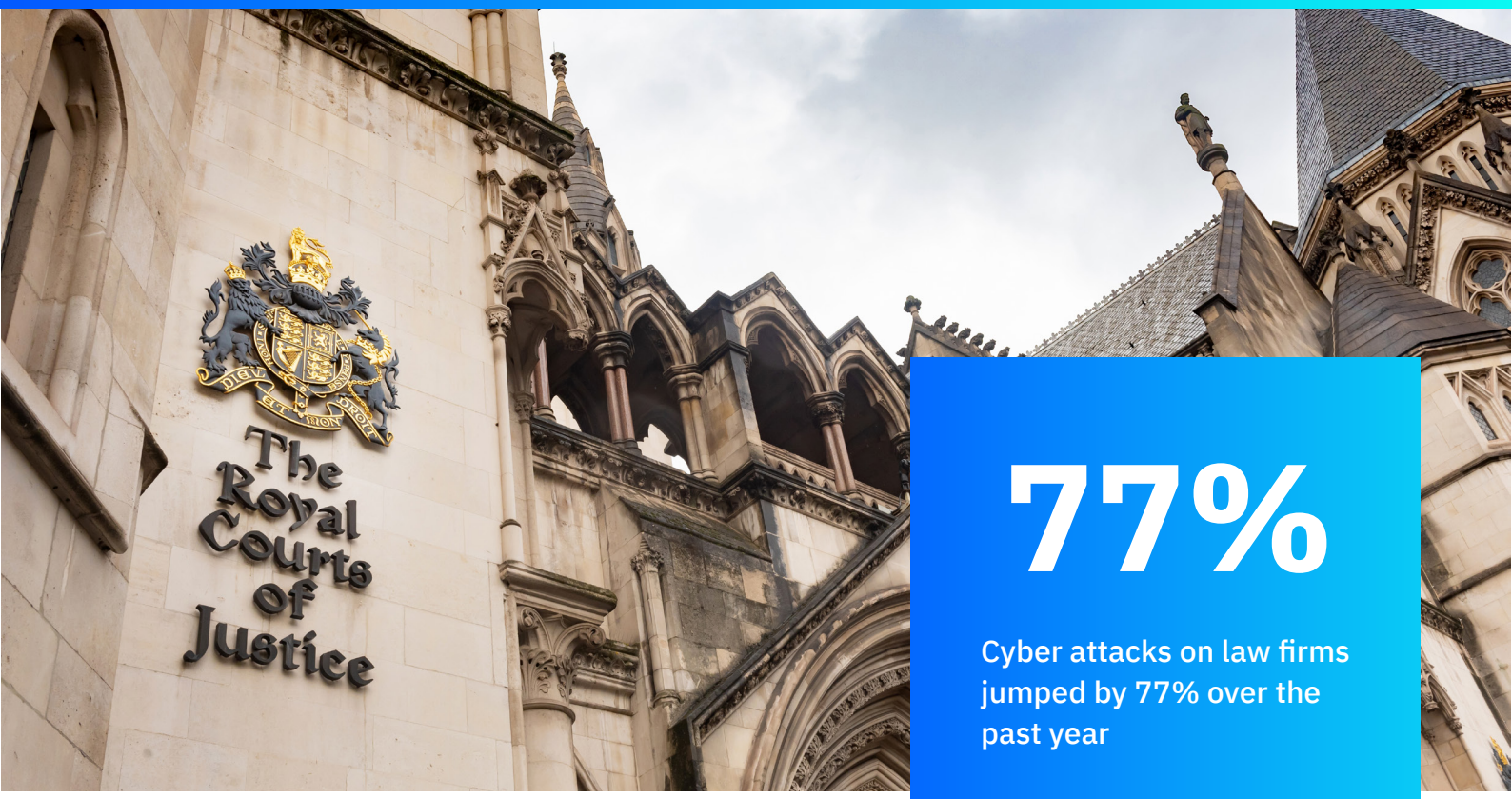
Keeping your world **secure**

Specialist cyber security guidance for law firms



77%

Cyber attacks on law firms jumped by 77% over the past year

Cyber threats to law firms are real, relentless and rapidly advancing.

As the National Cyber Security Centre (ncsc.gov.uk) reports, nearly three quarters of the UK's top law firms have been impacted by cyber attacks.

Over the last 12 months, 50% of businesses surveyed had suffered some form of cyber breach or attack[1]. The unthinkable happened to half of the organisations who believed it could never happen to them.

The pressures on you are further increased by an innate belief that law firms can be trusted to preserve the confidentiality of their information. It's great to have that kind of reputation, but worrying to think that one security breach could completely destroy it.

The challenges you face today

Technology is the beating heart of every business and when it stops, we all grind to a halt.

These days, cyber threats come in all shapes and sizes. While some are unbelievably sophisticated, many are quite basic, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked. Taking into account both ends of this spectrum, here are some of the areas where law firms are vulnerable.

- Your current managed service provider (MSP) doesn't provide a reliable security service
- Your internal IT team isn't up-to-date with their knowledge or isn't providing a 24/7 service
- Perhaps, you don't have an internal IT team
- You might have suffered a breach that you don't yet know about
- Your IT, including members' personal devices, have not been kept up to date
- Agreed security policies aren't taken seriously enough at senior levels in your organisation which makes them difficult to enforce
- If the law firms security is compromised, it could have profound consequences for the organisation's reputation
- Business interruption caused by ransomware - what would your firm do if you could not access any case notes, files or client details?
- Data theft is on the rise. How would you survive the publication of client confidential information?

So how good is your cyber security right now? The only way of really knowing is by conducting a discovery audit and penetration testing, working alongside a Managed Security Service Provider (MSSP) expert.

Click here to view the Cyber Security Breaches Survey 2024[1]

Putting the appropriate **defences in place**

Preventing a cyber-attack from happening is considerably more cost-effective and less stressful than having to clear up after one's happened.

Start as you mean to go on by choosing a provider that's accredited with ISO/IEC 27001 or certified with Cyber Essentials or Cyber Essentials Plus. Look for a platform that has been designed with security in mind, not one where it's been bolted on as an afterthought.

If, as is increasingly the case, you're operating in the cloud, adopt a policy of zero trust. (It's better to be safe than sorry.)

Ask yourself the following difficult questions.

01

Do you know exactly who has access to all information?

02

Do you have the right permissions in place?

03

Do you know when information is being shared and to whom?

04

Do you have adequate defences in place to prevent and flag unauthorised access?

05

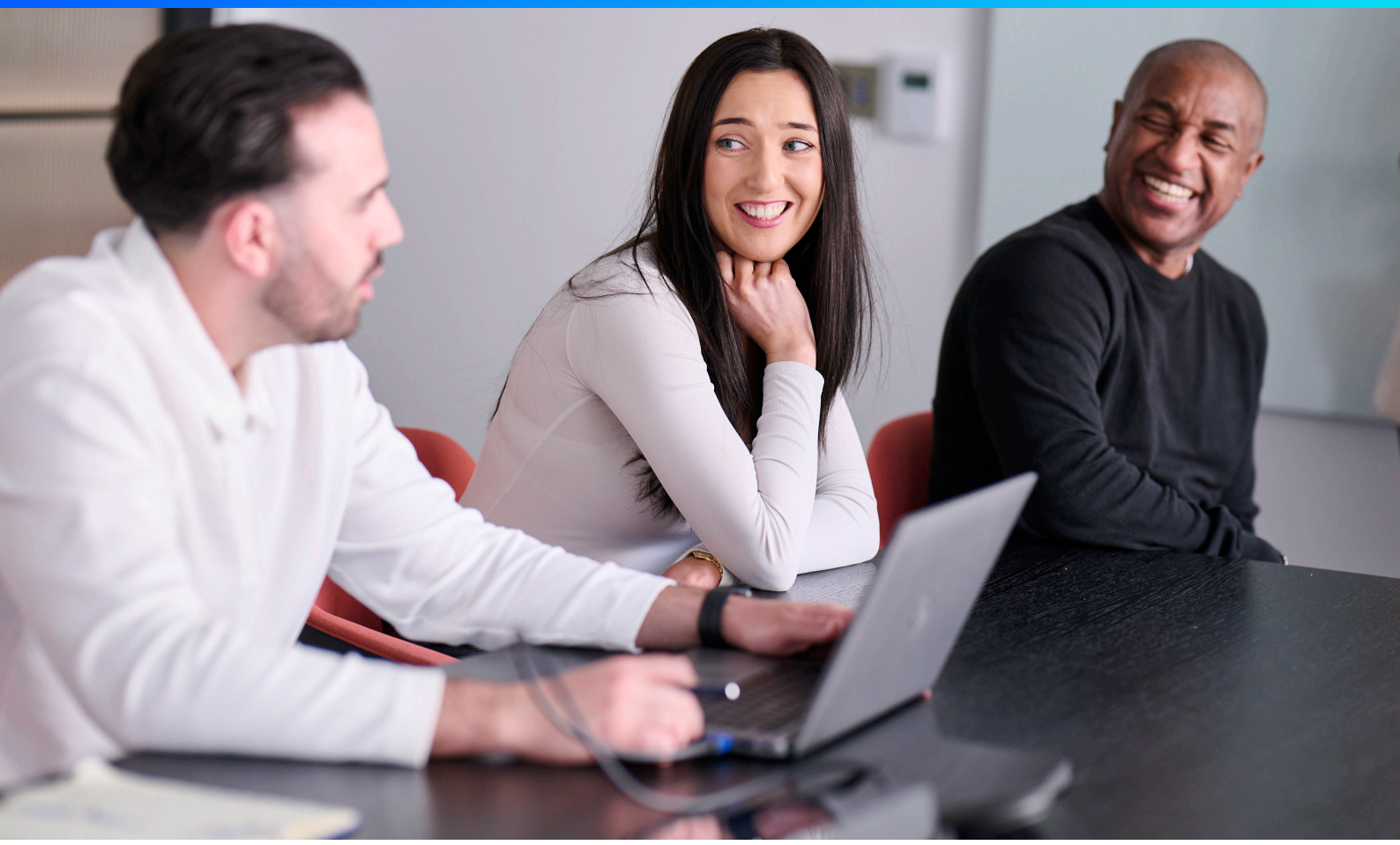
Do you have active cyber security defence 24/7?

The answer to all these questions should be a resounding 'yes'.

If not, you have work to do. (We can help with that.)

Beyond all that, we would recommend encryption for sensitive information on laptops, tablets and mobiles. Otherwise, sensitive information could literally be walking out of your offices on a daily basis.

If your infrastructure uses traditional architecture design, you'll also need to consider firewalls, anti-virus measures, remote working protections, VPNs and granting special permissions, as and when required.



Secure communication with colleagues and clients

If you haven’t embraced modern cloud technology, you’re missing out on some of the most beneficial new developments in collaborative working.

Take advantage of encrypted email to prevent sensitive information from falling into the wrong hands and, for the same reason, ensure shared documents are password protected. (It’s always worth warning first-time users about making the all-too-common mistake of sharing the password and the document in the same email!)

Video conferencing is an essential communication tool you’ll need to address, making sure it’s set up and configured with security in mind.

Your people are your weakest link, but can be your **first line of defence**

All the technology measures we've outlined are vitally important, but your weakest link in terms of cyber security is, without doubt, your users.

Human error is a reality, particularly when individuals are busy. Cyber attackers are acutely aware of this vulnerability and often exploit it. Therefore, it's paramount to equip users with the knowledge and skills to handle data securely. Regularly train them to recognise and resist common tactics employed by threat actors. By fostering a culture of cyber security awareness, you not only mitigate risks but also empower your users to act as the first line of defence against potential breaches.

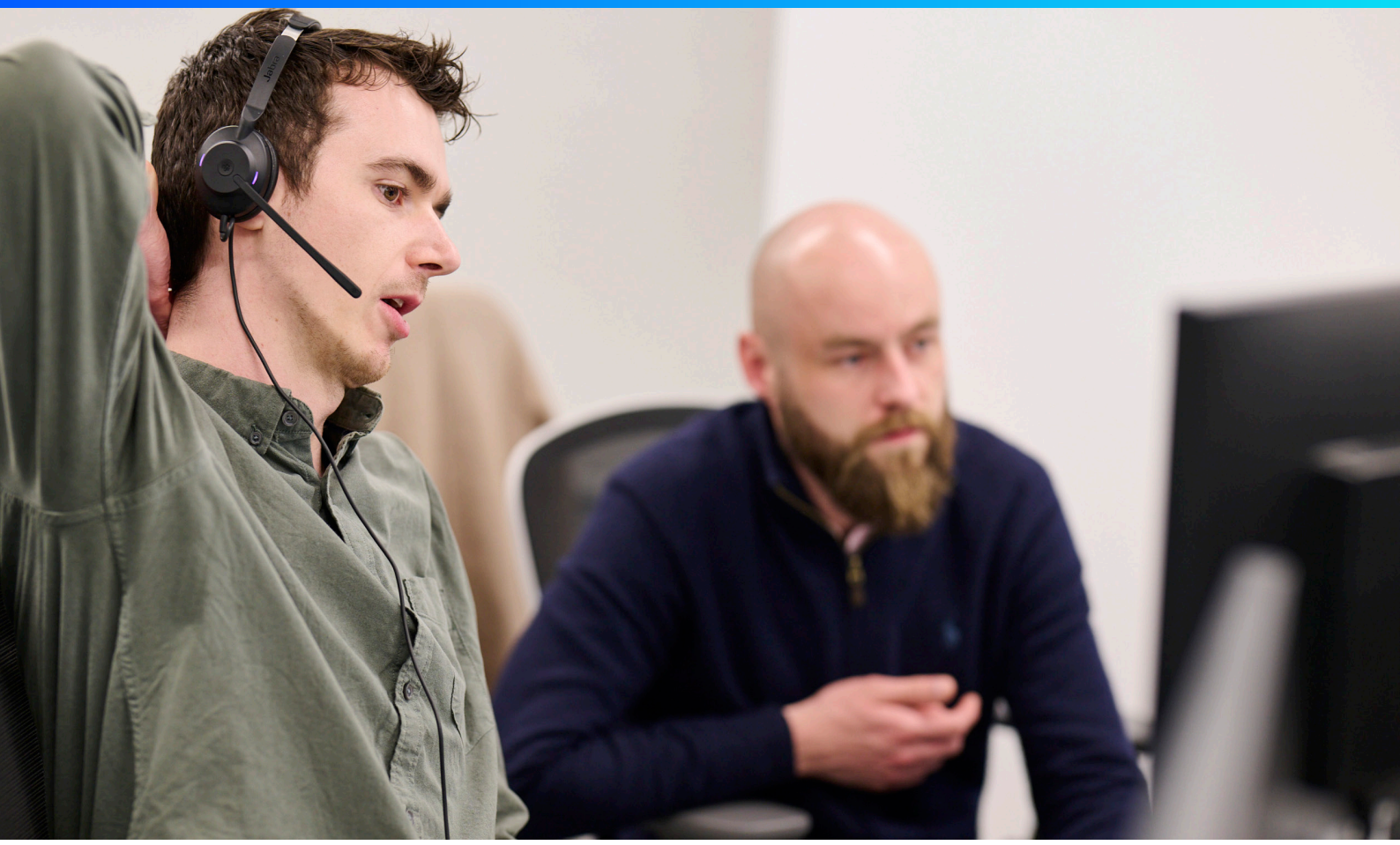
Continuous 'nudge' training is more effective than big annual refresher courses, which can easily be forgotten by the end of the month.

Tackling the issues of **remote working**

To ensure secure remote working, it's essential to adopt a multi-layered approach that integrates both technological solutions and best practices. Harness controls like device encryption to safeguard your hardware's stored information, VPNs to ensure a protected connection when accessing Chambers' resources and multi-factor authentication to add an additional layer of verification. Even if a device gets compromised, these measures will act as a robust line of defence, ensuring the data remains uncompromised.

As with all areas of cyber security, keep all users up to date with regular security training updates so they are aware of the latest tactics being used by cybercriminals.

Bearing in mind the threat landscape is constantly evolving, you might want to enlist the support of a Managed Security Service Provider (MSSP) with proven experience working within the legal sector.



What if the **unthinkable happens?**

Don’t just wait till the inevitable happens – be as prepared as you possibly can be. For a start, you should work on developing a company culture that gives you the best chance of nipping any future attacks in the bud.

Cultivate a culture of awareness and support where there’s no fault in raising false alarms, and where mistakes and accidental errors won’t be met with blame or criticism. By establishing this open and non-judgemental environment, you are empowering users to promptly report any concerning incidents, such as clicking on a suspicious link, without hesitation.

Then, it’s a case of putting a Business Continuity Plan (BCP) in place to guide you through a worst-case scenario.

That might include:

- Establishing alternative communication channels that your organisation could use if email or Teams suddenly become unavailable.
- Putting backup systems in place that are separate from your main systems and are tested regularly. (Tip: don’t keep your BCP and emergency credentials on the main network!)

In the event of an incident, recovery time is critical as you set about restoring your capability to function. If you feel out of your depth with all this, you’re better off engaging with experts sooner, rather than later, to help you put effective defences in place.

Why you need **Cyber Essentials accreditation**

Cyber Essentials is an effective, Government-backed scheme that will help you protect your law firm against a whole range of the most common cyber-attacks.

It ensures you meet a recognised national standard and can help build trust with existing and prospective clients. An assessment also helps provide a gap analysis that you can use as a way to get to where you need to be.

You'll find full details on how you can become accredited at About Cyber Essentials - NCSC.GOV.UK.

The requirements for an assessment include firewalls, secure configuration, security update management, user access control and malware protection.

To ensure a smooth transition through the Cyber Essentials process, law firms may want to enlist the support of a qualified cyber security company, such as Ekco. We can help you understand all the assessment questions and what steps you need to take to achieve certification.

Who is **Ekco**?

As cyber security experts serving the legal sector in the UK and across the globe, we deliver the strategic insight, tools and software needed to protect your business against emerging cyber threats.

We stop at nothing to keep you moving forward. Ensuring your business stays secure, connected and organised, wherever you are, whatever hour of the day it is. Above all, we're about making people's lives easier.

Based in Holborn Gate, our London team is supported by 100+ engineers and a 24/7 SOC team. Our dedicated team has experience working in the Chambers and legal market and we are well aware that you operate differently from other parts of the legal sector.

Unashamedly client-centric, we pride ourselves on building strong relationships based on much more than an anonymous voice at the end of a phone line.

Need help with your cyber security?

If you would like to ask questions about any aspect covered in this brochure, or you would like advice on cyber security issues within the legal sector, please contact us at **info@ek.co** or at **www.ek.co/contact**

Keeping your world **secure**

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

UKAS MANAGEMENT SYSTEMS 8289 ISO 27001 INFORMATION SECURITY MANAGEMENT

UKAS MANAGEMENT SYSTEMS 8289 ISO 9001 QUALITY MANAGEMENT

UKAS MANAGEMENT SYSTEMS 8289 ISO 14001 ENVIRONMENTAL MANAGEMENT