wavenet

EBOOK

Secure the Legal Sector with CyberGuard

Cybersecurity services to protect your networks and data around the clock.

EBOOK

Secure your business with CyberGuard

wavenet

Contents

Introduction

The UK's legal sector is large and diverse, spanning organisations of many shapes and sizes, from small high street solicitor firms to large multinational corporations, self-employed barristers, and barristers' chambers. Law firms are entrusted to safeguard highly confidential, commercially sensitive, and personally identifiable information, making them prime targets for cyber criminals.

In recent years, the widespread adoption of remote working and cloud-based technology has brought about great benefits to the legal sector. However, as technology continues to evolve, the attack surface for potential threats has expanded, leaving law firms exposed to ever more sophisticated cyber threats. With the increasing frequency and sophistication of attacks, the legal sector faces the complex challenge of keeping up.

The National Cyber Security Centre (NCSC) has reported that cyberattacks against law firms are on the rise, from 45% in 2018/19 to 73% in the most recent financial year. The report also stated that attackers are not solely focusing on large multinational firms but on smaller firms as well, as the types of data held – vast amounts of money, information, and client data - are equally valuable. What's worse, last year, Cert-UK, forerunner to the National Cyber Security Centre, published a report into the UK legal sector highlighting the fact that despite the need to be more protected, 35% of firms do not have a cyber mitigation plan in place.

Key concerns that the legal sector have are typically around reputation, critical to the business of law, and financial costs from transaction loss to operational disruption. It is vital that staff are aware of best practice and how to minimise risk, ensuring compliance to the latest laws, standards, and stringent data protection regulations across the sector (SRA Standards & Regulations and the Legal Services Act 2007).

The cyber Security mix

A good security offering for businesses within the legal sector need to contain a mixture of the following services:

- Managed Detection & Response
- Pen-testing
- Incident Response
- Training & Certification
- Security Posture Review
- Managed Firewall

What CyberGuard Can Offer

CyberGuard's professional cyber security solutions have been developed to defend and protect your networks and data around the clock from ever-evolving cyber threats. With over 20 years' experience working within the legal sector, we can provide a complete suite of cyber security services supported by our dedicated team of CREST and CHECK accredited experts, utilising the latest tools and methodologies.

Services include comprehensive intrusion testing and in-depth incident response, strategic security planning and roadmaps, risk assessment, vCISO, security awareness training, certifications, and accreditations.

Challenges to Overcome that the Legal Sector Face

Sophisticated Phishing Attacks

Phishing attacks involve cybercriminals using scam emails, text messages or phone calls to deceive victims into visiting malicious websites. These websites can download malware (such as ransomware or a virus) on victims' computers to steal personal information such as login details or bank details.

In the legal sector, phishing emails hide amongst the huge number of emails that busy users receive every day. They are the most prevalent type of cyberattack against law firms. Cybercriminals have become increasingly skilled at crafting emails that appear authentic, tricking users into revealing sensitive information or clicking malicious links. These attacks present a risk of data breach and reputational damage by compromising sensitive case data and client information.

Business email compromise (BEC) is a form of phishing attack where criminals attempt to trick a senior executive (or budget holder) into transferring funds or revealing sensitive information. Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals and can be even harder to detect.

Crimson Kingsnake BEC Gang

In late 2022, reports emerged that a new threat group called 'Crimson Kingsnake' were conducting large scale business email compromise (BEC) campaigns targeted towards business customers of major law firms. The group aimed to intercept transactions, acquiring funds fraudulently by registering a large number of domains similar to major multinational law firms. They then began sending emails to chase payments for fake invoices.

The emails used legal language to increase the sense of threat and urgency. In some cases, these emails would be followed by a further reply impersonating a known senior individual from the victim organisation, asking that the bill be paid.

Challenges to Overcome that the Legal Sector Face

Ransomware Attacks

Ransomware is malicious software (malware) that prevents you from accessing your computer or the data stored on it. During a ransomware attack, your data is normally encrypted or stolen, rendering it inaccessible. Cybercriminals may demand a ransom for the decryption key or threaten to publish sensitive data online. Given the highly sensitive nature of legal information, ransomware attacks can have severe consequences.

Disruption to routine business operations can be costly to legal practices, both in terms of billable hours lost due to outages and costs to clients that depend on them. This makes legal practices of particular interest to extort money in return for the restoration of IT services.

The dark web has become a breeding ground for cybercriminals offering 'Malware as a Service' and 'Ransomware as a Service', allowing even those less knowledgeable to purchase and deploy sophisticated malware or ransomware with ease.

4 New Square

In 2021, Barristers Chambers 4 New Square were targeted by a ransomware attack. This affected the operation of critical IT systems and involved the exfiltration of sensitive data. Luckily, they were able to recover from their backups.

The investigation showed that no publication of data took place. Cyber insurers deployed a team shortly after the attack to isolate the systems, stop the attack and preserve the data. A significant GDPR data review was subsequently carried out to ensure proper notifications were made to any potentially affected clients.

The key lessons learned from this attack was that all plans should be tested. Although the response to the attack was successful and there was no significant disruption to clients in the immediate aftermath, had the plans in place been tested, recovery may have been quicker and smoother.

Challenges to Overcome that the Legal Sector Face

Password Attacks

Access to data, systems and services need to be protected. A strong approach to identity and access management will make it hard for criminals to pretend they are legitimate, whilst keeping it as simple as possible for legitimate users to access what they need.

Credentials are often re-used across multiple sites and services. This could allow a criminal to access work accounts if the password is disclosed, for instance, in a data breach. Weak and common passwords are easier to uncover, making it quicker for attackers to access law firm systems. Multi-factor authentication (MFA) adds an additional authentication step when logging into a system which makes it harder for an attacker to access systems, even if they have access to a valid account and password.

With the growing use of cloud systems to store confidential data, misconfiguration of these systems can leave data accessible to anyone. Attackers are very good at searching the internet to find open access data sources. By not restricting account permissions to data and services, attackers have the opportunity to use compromised accounts to access more sensitive data and move onto other critical systems.

Remote working

The traditional IT setup in law firms used to involve employees working from a centralised office with a single firewall protecting the entire network. Access to sensitive data was limited, and data protection was relatively straightforward.

The widespread adoption of remote working and cloud services may have increased productivity across the legal sector, but it also exposes law firms to the risk of insecure home networks. Today, employees work from various locations, including home, cafes, and while on the move. Employees accessing company networks and applications from personal devices may unknowingly introduce vulnerabilities. This decentralisation has opened multiple entry points for potential attackers, increasing the overall attack surface of law firms. Cybercriminals are constantly exploiting vulnerabilities in home routers, making it essential for firms to educate their employees on securing home networks.

Financial Loss and Downtime

In many areas of law, from mergers and acquisitions to conveyancing, law firms handle significant financial transactions. The time-sensitive nature of these transactions creates an attractive environment for cybercriminals to intercept funds in transit. The SRA reported that in 2020 75% of the solicitor firms they visited had been the target of a cyberattack.

The consequences of a successful cyberattack on a law firm can be devastating. The average cost of a cyberattack for an SME is £138,000, with industry wide costs averaging £628,000. Downtime resulting from attacks can stretch up to 21 days, leading to significant financial loss and reputational damage. In 2021, a city law firm reported they had lost client data as a result of a cyberattack which wiped almost 8% share value within an hour of the statement.

To protect themselves and their clients, law firms must adopt robust cyber security measures, such as zero-trust methodologies and conditional access policies. Staying informed about the latest cyber security trends and working with reputable IT security providers are crucial steps in safeguarding sensitive data and maintaining client trust in the digital age. To ensure compliance to the latest laws, standards and GDPR best practices, staff should be knowledgeable about cyber threats and how to minimise risk.

The solution

In the legal sector, cyber security in not an option, it's a necessity. Protecting client data, maintaining trust, and ensuring compliance with data protection regulations are paramount. Wavenet's CyberGuard solution provides the very latest in cybersecurity services. With so many threat variations and the potential of multiple security gaps, law firms must remain vigilant and employ best practices to safeguard their digital assets. CyberGuard gives peace of mind that your security is in good, experienced hands.

With proper preparation, you can mitigate risk. And, if the worst does happen, you can recover. By prioritising cyber security, the legal sector can continue to serve clients with confidence, knowing that their sensitive information is secure. Wavenet's CyberGuard solution offer a range of services to help you strengthen your security from all angles.

We protect our customers from end-to-end through: Security Testing, Managed Detect & Respond Services, Security Awareness Training and Cyber Certification. We also provide reassurance in the event of an attack through fast and effective Cyber Incident Response.

Our cybersecurity services give you:

- Peace of mind with UK-based, 24/7 monitoring and response
- Intelligence-based analysis for better visibility of threats
- A proactive approach to security
- Help from trusted CREST and CHECK-accredited professionals

Benefits:

- Improve visibility with our Threat Intelligence
- Proactively monitor your infrastructure
- 24/7 UK Security Operations Centre (SOC)
- Support from a cyber security incident response team (CSIRT)

We work with leading technology providers in the cybersecurity sector, including:

Microsoft Security | paloalto NETWORKS | Qualys. | KnowBe4 Human error. Conquered. | CROWDSTRIKE

Our Services

Managed Security Operation Centre

At the heart of our cybersecurity efforts lies our UK based 24/7 Security Operations Centre (SOC). This dedicated team comprised of seasoned and accredited cybersecurity experts diligently sift through a multitude of alerts from various sources.

There are many advantages for the legal sector to choose our SOC. Foremost is the capability to detect and counteract security threats in real-time, curtailing any potential to inflict substantive damage or result in financial losses. With vigilant eyes on networks, systems, and applications, our SOC ensures that deviations and questionable activities are swiftly detected and addressed.

Features and benefits:

- Threat Detection and Response
- Incident Management
- Proactive Threat Hunting
- Enhanced Incident Response Time
- Better visibility
- Reduced costs

Our SOC delivers the following MDR services

Managed SIEM

Our state-of-the-art SIEM solutions, powered by Microsoft Sentinel, ensures a comprehensive view of your security landscape. Through intelligent log analysis and event correlation, we spotlight unusual patterns and behaviours, facilitating quicker incident response and better threat visibility.

Managed EDR

We recognise the need for a layered defense strategy so by integrating industry leaders like Microsoft Defender and CrowdStrike, our Endpoint Detection and Response (EDR) service, offers unmatched precision in pinpointing and neutralising threats at endpoint level.

Managed XDR

Extended Detection and Response (XDR) is a unified defence against incidents that span endpoints, identities, email, collaboration tools and cloud applications. By monitoring diverse attack surfaces and analysing the overall threat landscape, XDR provides a higher level of protection against emerging and sophisticated threats to the legal sector.

Managed NDR

Network Detection and Response (NDR) platforms capture network metadata by continuously analysing network traffic and behaviour. It enables security teams to respond quickly and prevent potential breaches or damage.

Managed Firewalls

Arobust perimeter is fundamental to cybersecurity. Our managed firewalls not only act as your law firms first line of defence against intruders but are also continually updated and fine-tuned to adapt to evolving threat patterns.

Managed Vulnerability Scanning

Our proactive vulnerability scanning solution delves into your systems, networks, and applications, identifying potential weak points. This ensures you can act pre-emptively, fortifying vulnerabilities before they can be exploited.

Incident response

When faced with a cyber incident, time is of the essence. Wavenet's Cyber Security Incident Response (CSIR) is CREST approved, a testament to our unparallel expertise in the field. In the aftermath of a cyberattack, our primary focus is on swift containment to protect the law firm's reputation, recovery of data, and ensuring minimal business disruption.

Our CSIR service encompasses:

- Rapid Response: Efficiently addressing security incidents to prevent further damage.
- ExpertAnalysis: Identifying the nature and scope of the breach, ensuring informed decisions at every step.
- Recovery and Restoration: Re-establishing the integrity of your systems and getting your operations back on track.
- Post-Incident Review: Analysing the incident to provide actionable insights, bolstering your defences for the future.

IR retainer services

For law firms seeking added peace of mind, we offer IR Retainer Services. With this, you will not only be prepared for potential incidents but also assured of priority response, ensuring even swifter action and mitigation in the event of an unforeseen breach.

Features and benefits:

Crest Accredited

Incident Management

Proactive Threat Hunting

Enhanced Incident Response Time

Service Excellence

Penetration testing services

Penetration Testing, also known as “Pen Testing”, is a simulated cyberattack carried out by in-house experts to assess the security of a computer system. By simulating real-world attack scenarios, our CREST accredited team can identify weaknesses in your system’s defences, such as misconfigurations, outdated software, or insecure network settings. They can then create an efficient defence plan against hacking attempts.

Our pen testing services include:

- Infrastructure Assessment
- Mobile and Web Application Security
- Red Team Assessment
- PCI DSS Assessment
- Stolen Device Assessment
- Physical Security Assessment
- GDPR Assessments

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CREST

Features and benefits:

- Identify Potential Vulnerabilities
- Proactive Security
- Risk Mitigation
- Compliance and Regulations
- Incident Response Planning
- Stakeholder Confidence

Who we work with

Large Law Firms

Helping senior managers to ensure that cyber resilience and risk management are embedded throughout the organisation, including people, systems, processes, and technologies.

Small High Street Solicitors

Helping to secure sensitive case and client data, networks, and systems, complying with data protection regulations and ensuring the continuity of critical services.

Sole Practitioners & Self Employed

Helping to protect data and networks with cost-effective solutions tailored to your specific needs.

Customer quotes

Lincoln's Inn London

pride themselves on building strong, long-term client relationships based on trust, discretion, integrity and results. To transform from an office-based business to a flexible, secure remote working enterprise they needed a secure hosted cloud platform so their 130-strong workforce could access the business critical applications.

Nebula, a ready-built Cloud platform allowed Wavenet to design and deliver a suite of nine Citrix servers on a secure hosted platform and with additional licencing applied enabled all staff to have full functionality of their 'office based' applications and work safely and efficiently wherever they were based.

Farrer & Co

is one of the UK's most prestigious, well known and respected law firms and prides itself on superb customer service. They required a network infrastructure that would deliver the modern touch to match their commitment to customer service , improve the productivity of their 450 staff, that was robust and secure to guarantee the integrity of the sensitive case information they handled for their clients.

Wavenet migrated their existing Cisco/Meraki infrastructure to a bespoke Extreme Networks solution that improved employee productivity and customer experience.

The Honourable Society of Lincoln's Inn

FARRER&Co

> When you've built a reputation like that of Farrer & Co. it's important you are able to uphold it. At the same time, in an increasingly technology-driven business environment, they couldn't afford not to look at how they can deliver a modern experience for clients and staff; through the deployment of Extreme Networks switching and management solutions, they have been able to do just that. Extreme Networks Management Centre allows for the entire network to be viewed by a single pane of glass, simplifying management and improving visibility. By deploying Extreme Networks switching, wireless and management, the team at Farrer and Co. can focus on delivering the level of service that has set them apart for so long.
>
> Andrew Blewitt Senior Account Executive Extreme Networks

GET STARTED

Build business resilience and improve your security strategy with Wavenet.

CyberGuard Technologies is the security division of Wavenet. We provide a suite of fully managed end-to-end security services from a 24/7 UK Security Operations Centre. Our cyber defences protect the legal sector from the potential devastation of cyberattacks, defending finances, identity, reputation, data, and confidential information.

We provide cybersecurity, communications and technology-managed services that grow with your law firm – giving you the confidence that when you work with us, your business will be future proofed. Our focus is on finding the right cybersecurity solutions so you can focus on what matters most to your firm.

Talk to us

WAVENET.CO.UK

0333 234 0011

Wavenet Limited
One Central Boulevard
Blythe Valley Park
Solihull, West Midlands
B90 8BG

cyberguard@wavenet.co.uk

wavenet

Networking
& Connectivity

Unified
Communications
& Voice

Contact Centres

Mobile Solutions
& IoT

IT, Cloud
& Technology

Network
Intelligence

Cyberguard