B2 BUSINESS SYSTEMS

ENSURING BETTER SECURITY & COMPLIANCE FOR LAW FIRMS.

Overview of technology helping counter-attack cyber security threats for law firms.

INTRODUCTION

The UK legal sector faces a significant cyber threat. According to the PricewaterhouseCooper (PWC) 2019 Annual Law Firms Survey, **100% of the Top 100 Law Firms** suffered a cyber security incident in 2019[1].

Unsurprisingly, all of the Top 100 Law Firms have reported they are 'somewhat or extremely concerned' about cyber security threats regarding their ambitions and business goals[2]. Cyber criminals target law firms because they hold sensitive client information, handle significant sums and are a key enabler of commercial and business transactions.

A cyber security failing creates a financial burden. The Solicitors Regulation Authority (SRA) report that a small breach costs the average law firm £4,180, rising to £22,700 for larger firms[3]. Firms only fear the impact of Brexit more than cyber-attacks[4].

LEGACY SYSTEMS INCREASE YOUR ATTACK SURFACE AND ARE NOT BUILT FOR TODAY'S REMOTE WORKFORCE

These costs do not include regulatory costs. Under the General Data Protection Regulation (GDPR), the Information Commissioner can fine firms up to €20million or 4% of their global turnover (whichever's higher) if they do not protect personal data. But, focusing only on the financial costs does not show the whole picture. In an industry where client confidentiality is of vital importance, a data breach can cause massive reputational damage.

Not to mention the impact the loss of data or money will have on a client's wellbeing and life. It is not money on a spreadsheet to them; it is their housing deposit, inheritance or life savings. Many firms now believe cyber security is not an IT risk, it is a strategic risk management issue.

IT security is especially important as we move into the new normal and your team members work from anywhere. Your old, fortified perimeter no longer exists. Legacy systems are not built for today's workforce. They increase your attack surface and are slow to react. You need a solution that keeps your data safe and empowers team members to work remotely.

GCHQ has identified the four most significant cyber threats: **phishing; data breaches; ransomware; supply chain compromise**[5]. This guide reveals how law firms can protect their network and enhance their security & compliance in the remote working world when they opt for a dedicated IT Support Provider.

[1, 2 & 4] PWC, 2019 Annual Law Firms Survey, *https://www.pwc.co.uk/industries/business-services/law-firms/survey.html*

[3] SRA, 2020, Risk Outlook Report 19/20, *https://www.sra.org.uk/risk/outlook/risk-outlook-2019-2020/*

[5] National Cyber Security Council, 2018, The Cyber Threat to UK Legal Sector

PROTECTING AT THE ENDPOINT

Phishing is the most common cyber attack impacting law firms.

Cyber criminals favour phishing because it is low effort, high reward. It is adaptable to multiple touch points and can be an email, a text message, a social media post or a phone call. Email is the commonly used method as a malicious email can reach users directly and be smuggled in with the countless benign emails users receive.

With remote workers, accessing a firm's network is even easier. Someone working from home might login using a VPN, exposing their corporate network to a swarm of threats. Hackers scan for VPN signals and attempt to get a foothold in your network. If successful, they can achieve domain user access, steal passwords, disable multi-factor identification and endpoint solutions, before uploading ransomware. All it takes is one bad email to cripple a network.

There are many ways to prevent a phishing attack, especially when team members are working remotely. Many of these methods are well-known, including the need of email scanning and email blocking software. It is also imperative that law firms have clear processes in place that train team members on how to recognise a phishing attempt, and how to respond quickly.

The easiest way to prevent phishing is to stop the bait getting in front of end users. Get instant SPAM protection at the gateway with comprehensive anti-spam service.

Anti-Spam Technology

Set up to support corporate governance or compliance policies, per-user policies or preferences, the latest anti-spam technology uses reputation checks to find out the IP reputation and the reputation of the content, structure, links, images and attachments.

Using real-time reporting, advanced techniques such as adversarial Bayesian filtering, image analysis and gibberish detection can uncover known and new threats hidden in an email. Furthermore, most anti-spams use a cloud-based design to run without affecting firewall processing and network throughput.

Any gathered data, like an IP address, can then be added to an integrated allow or block list. A law firm's IT team can allow or block an IP address at the gateway, granting granular control and protection of the network.

Additionally, flexible junk routing splits junk emails into spam, likely spam, phishing, likely phishing, virus,and likely virus categories. The IT team can then determine if a category should be rejected, tagged, delivered, sent to the user's junk folder or deleted. If sent to the user's junk folder, it is down to the user to "unjunk" emails.

With a next-gen firewall, law firms will also be able to prevent users from entering corporate details into unknown sites.

[6] ITEC, *https://www.itecgroup.co.uk/blog/how-to-prevent-phishing-attacks-and-protect-your-organisation*

FORTIFYING YOUR DATA

The legal sector puts confidentially at the heart of everything. This can make a loss of client information incredibly damaging to a firm's reputation and finances.

In the new world, where everyone is moving away from on-premise protection, the classic perimeter no longer exists. If a phishing attack is successful and you have a data breach, locking down your network with a stack of network gateway appliances anchored in your data centre is now impossible. People no longer work in one place or solely on company-approved devices.

There are steps law firms can take to meet GDPR compliance and mitigate any potential data breaches including hiring practices, managing data correctly and educating team members on how to respond quickly in case of a breach.

Next-Generation Firewalls

From a technology standpoint, the best way to fortify your data is to barricade it behind advanced, next-generation firewalls.

Instead of reacting to threats, next-gen firewalls proactively seek & destroy potential malicious attacks. Law firms
can stay ahead of cyber criminals by leveraging machine learning for real-time and inline zero-day protection.

The proactive threat detection inspects all traffic including applications, threats and content that tie traffic to a user regardless of their location or device type. Advanced sandboxing techniques employed by the next-gen firewalls make this detection safe and reliable.

Next-gen firewalls also include **application IDs** to accommodate the rise in SaaS and the fact that your team members often use unapproved applications to complete their jobs[7]. **URL filtering** prevents phishing, while **IoT security** tracks traffic from any unauthorised devices (e.g. a team member's personal phone). This makes a user an integral part of your firm's enterprise security policy.

Granular Control

Using deep packet inspection, your law firm's IT team can gain heightened visibility as the firewalls report back who is accessing what application, from what device, and from where. This is logged into your syslog service to help minimise remediation time if a breach happens, and to react quickly to anomalous activity.

Additionally, granular control is granted with programmes only allowing authorised users to access certain sections of the network. This reduces lateral movement on the network and minimises exposure to critical business resources.

Zero Trust

According to The Industry Security Forum, over half of all data breaches are caused by insiders. With Zero Trust practices and strategies, next-gen firewalls provide complete visibility into traffic, verify users, devices and applications, enforce policies across networks,
endpoints and clouds, and deliver context-based reports.

[7] ITEC, 2019, Rebel Tech, *https://hello.itecgroup.co.uk/download-research*

[8] ISF, 2018, Managing Insider Threat: Briefing Paper, *https://www.securityforum.org/research/managing-the-insf-briefing-paper/*

PREVENTION-FIRST STRATEGY

GCHQ identifies ransomware as the third most significant cyber threat facing law firms.

Ransomware prevents users from accessing certain documents, data and files unless a fee is paid. Paying does not necessarily mean the hacker will release the data.

In 2019, ransomware caused business delays in 27% of UK businesses[9]. A strike could leave you unable to access your data for a long period, slowing down transactions and increasing costs and complaints.

IT heads can protect their law firm from ransomware by keeping their software updated, patching security flaws and by being careful about what software, hardware and applications they allow onto the network.

However, it's predicted more than 40 billion devices will connect to networks by 2025[10], and coupled with the rise in remote working, this makes tracing your network perimeter hard. It's always changing as team members connect from anywhere at any time on any device.

PREVENTION-FIRST STRATEGY

By switching to a prevention-first strategy, IT teams can reduce the number of IT tickets being raised and successfully manage the network from a centralised location.

Ransomware attacks start at team member computers. Attackers then need to move through your network piece by piece. AI-driven threat detection is built into the next-gen firewalls to run local analysis and behaviour threat detection. Moreover, zero trust software will contain the ransomware, stopping hackers from accessing critical files.

With cloud-delivered deployment and management, the protection agent detects and responds to threats quickly. Law firms can run powerful, scalable prevention with a simplified user experience.

[9] SRA, 2020, Risk Outlook Report 19/20, *https://www.sra.org.uk/risk/outlook/risk-outlook-2019-2020/*

[10] Palo Alto

OUR IT SUPPORT SPECIALISTS

Supply chain compromises are a massive threat to a law firm's security and compliance. The biggest issue when working with a third-party supplier is if they will adequately secure the systems that hold your data. The increasing use of digital technologies to deliver legal services will likely build more avenues for exploitation.

As the sector starts embracing remote working, It is important law firms have confidence in their managed services partner.

OUR CREDENTIALS

We keep all customer data safe and comply to multiple international and national IT Security regulations including Cyber Essentials Plus, ISO 14001 and ISO 27001. The London Data Centre also complies with ISO 22301 and OHSAS 18001.

IT SECURITY SERVICES

As part of your Managed IT Support, we help protect your IT estate from cyber crime, and make sure your security complies with regulatory demands.

Network Security: halt unauthorised access with automated threat detection and prevention in the shifting landscape

Internet Security: next-gen software firewalls, anti-malware and anti-spyware protect from browser-borne attacks

Cloud Security: specialist and comprehensive cloud security options including the ability to enforce hundreds of out-the-box governance policies to ensure security and compliance

Endpoint Security: protects at a device level, getting law firm's ready for remote working and BYOD

IT SUPPORT SECURITY PILLARS

Once you enter a Managed IT Support Service with us we stress test your network as part of our security dedication.

We've made regular penetration testing, 24/7 monitoring, disaster recovery and daily backup checks core elements of our Managed IT Service.

Find out more: www.B2.ltd/IT/

IT SUPPORT AT A GLANCE

24/7 IT Support Help Desk, 7 Days a Week

24/7 Performance Monitoring

Proactive Risk Identification

Root-cause analysis

xerox™