STRIDON

changing perception from within

RISKY BUSINESS

Why law firms need to address a growing cyberthreat challenge

STRIDON

REDUCING RISK AND PROTECTING DATA

Today's law firms are under rising pressure to prioritise cybersecurity and counter malicious attempts to disrupt devices, services and networks.

Introduction

Under pressure to comply with stringent regulatory and legislative[1] obligations to protect the data and assets of clients, legal firms have a duty to maintain the confidentiality, integrity and availability of information held on their IT systems – failure to do so risks punitive fines and lasting reputational damage.

But what cyber-crime now represents is a persistent and growing threat for UK businesses. According to the UK government's recent Cyber Security Breaches Survey 2019[2], 32% of businesses experienced a cyber security breach or attack in the last 12 months – a figure that increases dramatically for medium size (60%) and large businesses (61%) and high income charities (52%).

Law firms in particular have become a popular target for cyber criminals, thanks to the vast amounts of sensitive data and money they hold, and the scale and size of the commercial transactions they handle:

- The SRA[3] reports over £11 million of client money was stolen due to cybercrime in 2016-7
- In 2018[4], 60% of law firms reported an information security incident – up 20% on the previous year.

LAW FIRMS IN PARTICULAR HAVE BECOME A POPULAR TARGET FOR CYBER CRIMINALS

[1] General Data Protection Regulation (GDPR), Data Protection Act 2018

[2] Cyber Security Breaches Survey 2019, Department for Digital, Culture, Media & Sport

[3] Solicitors Regulation Authority

[4] National Cyber Security Centre (July, 2018)

As a consequence, cyber risk and data protection are now a core business concern. And the consequences suffered by a law firm following a cyber-attack could be catastrophic, resulting in:

- Theft of client monies and assets
- Breaches of confidential and sensitive information
- Structural and financial instability
- Disruptions to business continuity
- Reputational damage
- Loss of clients

As law firms become increasingly reliant on digital communications and services to engage and transact more and more online, the protection of information assets and IT infrastructure is now a top priority. Indeed, the ability to innovate safely and grow with confidence depends successfully navigating the threat landscape.

TOP CYBER ATTACK VECTORS

The Law Society's 2018 cybersecurity survey identifies the top three attack vectors experienced by UK law firms as:

81%

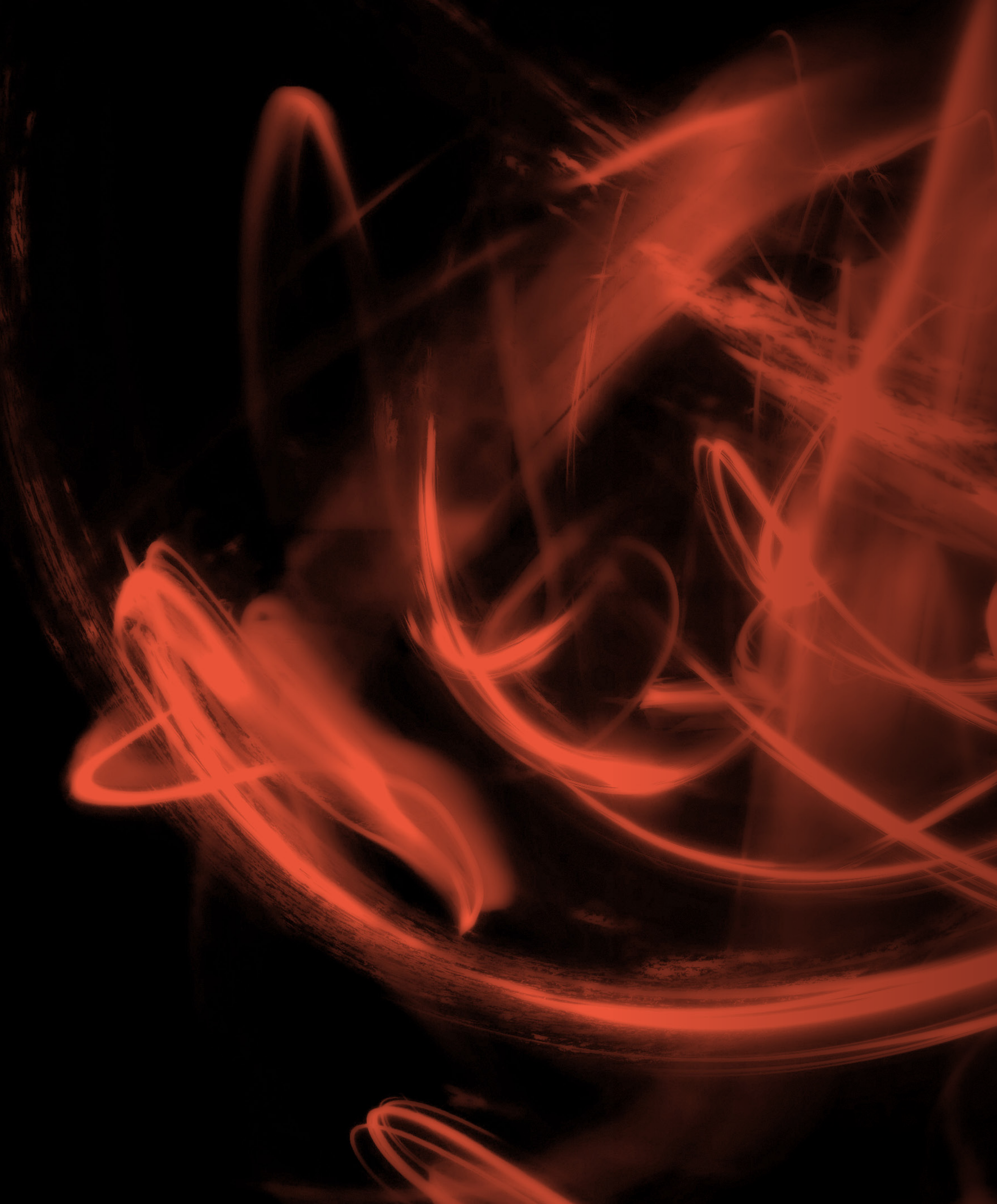
PHISHING EMAILS

53%

SPOOFING

45%

VIRUS, MALWARE AND SPYWARE



Exploring the threat landscape

The financial, reputational and regulatory consequences of cybercrime is significant. Should IT systems crash as a result of an attack, there may be significant disruption to business and client services, as well as the risk of the loss of confidential client information or monies.

But that's not all. The threat landscape is constantly evolving – and data is not the only target. Core systems are being targeted to disrupt organisations. And while data remains a primary target, a new wave of cyberattacks sees data no longer simply being copied but destroyed or changed.

Worse still, cybercriminals are adapting their attacks and using the human layer – the weakest link – as a path to attacks through increased phishing and malicious insiders to target.

THE TOP CYBER AND DATA LOSS THREATS FACED BY UK LAW FIRMS INCLUDE:

1

THREAT

Phishing

A hacker attempts to obtain financial or other confidential information by sending fraudulent emails to people in the firm. Particularly prevalent in areas of practice such as conveyancing, targeted phishing emails and other online scams aimed at law firms are becoming ever more sophisticated.

Appearing to come from legitimate sources, including internal email servers that have been hijacked, recipients are enticed to open an attachment or directed to a facsimile of a trusted website (like a bank's) in a bid to obtain confidential information (passwords, bank details or other sensitive information) or get employees to unintentionally download malicious software (malware) onto their system.

MITIGATION STEPS:

EDUCATE USERS, RESPOND FAST TO INCIDENTS, INITIATE TOOLS TO MITIGATE UNDETECTED PHISHING EMAILS.

2

THREAT

Ransomware

This type of attack locks users out of systems and prevents them from accessing data. Cyber criminals demand payment for decryption, however, there is no guarantee that paying the ransom will see normal operations return.

The international law firm DLA Piper very publicly fell victim to a largescale ransomware NotPetya attack in June 2017. The financial impact to DLA Piper was estimated in the millions.

While a law firm may not be the intended victim of a ransomware attack, it may well suffer collateral damage if one of its supplier organisations, or a client, is subject to an attack.

MITIGATION STEPS:

KEEP DEVICES (PCS, LAPTOPS, MOBILE DEVICES) AND SOFTWARE (OPERATING SYSTEMS) UPDATED, REGULARLY BACKUP FILES TO A SAFE LOCATION, CONSIDER USING CLOUD SERVICES, IMPLEMENT PREVENTION TOOLS/PROCESSES TO DISRUPT THE DELIVERY AND EXECUTION OF MALICIOUS CODE.

3 THREAT

Data Breaches

Often initiated via a phishing attack, cyber criminals infiltrate a firm's network to steal inside information.

In March 2018 the offshore law firm Mossack Fonesca announced it was closing as a result of the irreversible economic and reputational damage caused by a major data breach, known as the Panama Papers hack, which saw the loss of 2.6TB of data as a result of a poorly secured client portal.

MITIGATION STEPS:

INITIATE A MULTI-LAYERED SECURITY STRATEGY THAT INCLUDES APPLICATION WHITELISTING AND PRIVILEGE MANAGEMENT THAT LIMITS THE PATHWAYS FOR MALWARE TO OBTAIN SENSITIVE DATA. INITIATE SANDBOXING, ENDPOINT SECURITY MANAGEMENT, IDENTITY MANAGEMENT, TRACK AND MONITOR USERS.

4

THREAT

Spoofing

Email modification fraud and business email compromise is one of the most frequently used cyber attack methods used against the legal profession.

Cyber criminals intercept and/or falsify emails between clients and law firms, and bank details are changed to enable the interception and transfer of monies that are then stolen.

MITIGATION STEPS:

STAFF TRAINING, MAINTAIN UPDATED ANTI-VIRUS, ANTISPYWARE AND FIREWALL SOFTWARE, IMPLEMENT TOOLS TO BLOCK PHISHING ATTACKS AND STOP THIRD-PARTY IMPERSONATION OF EMAIL DOMAINS.

5

THREAT

Insider threats

Malicious insider threats from employees or contractors seeking financial gain or with a perceived grievance against a firm represent a major challenge.

Indeed, recent research has found that 56% of breaches are caused by insiders acting either maliciously or accidently. Internal actors may be motivated by sabotage, espionage, insider trading, or activism. Or they may be planning to jump ship to a new role, taking valuable client information with them.

MITIGATION STEPS:

MULTI-FACTOR AUTHENTICATION, IMPLEMENTATION OF USER AND ENTITY BEHAVIOUR ANALYTICS TECHNOLOGIES THAT MONITORS FILES, SYSTEMS AND ORDINARY USER BEHAVIOURS AND PROVIDES ALERTS ON ANOMALOUS BEHAVIOURS (DOWNLOADING OF SENSITIVE INFORMATION, LOGGING IN FROM NEW DEVICES).

STRIDON

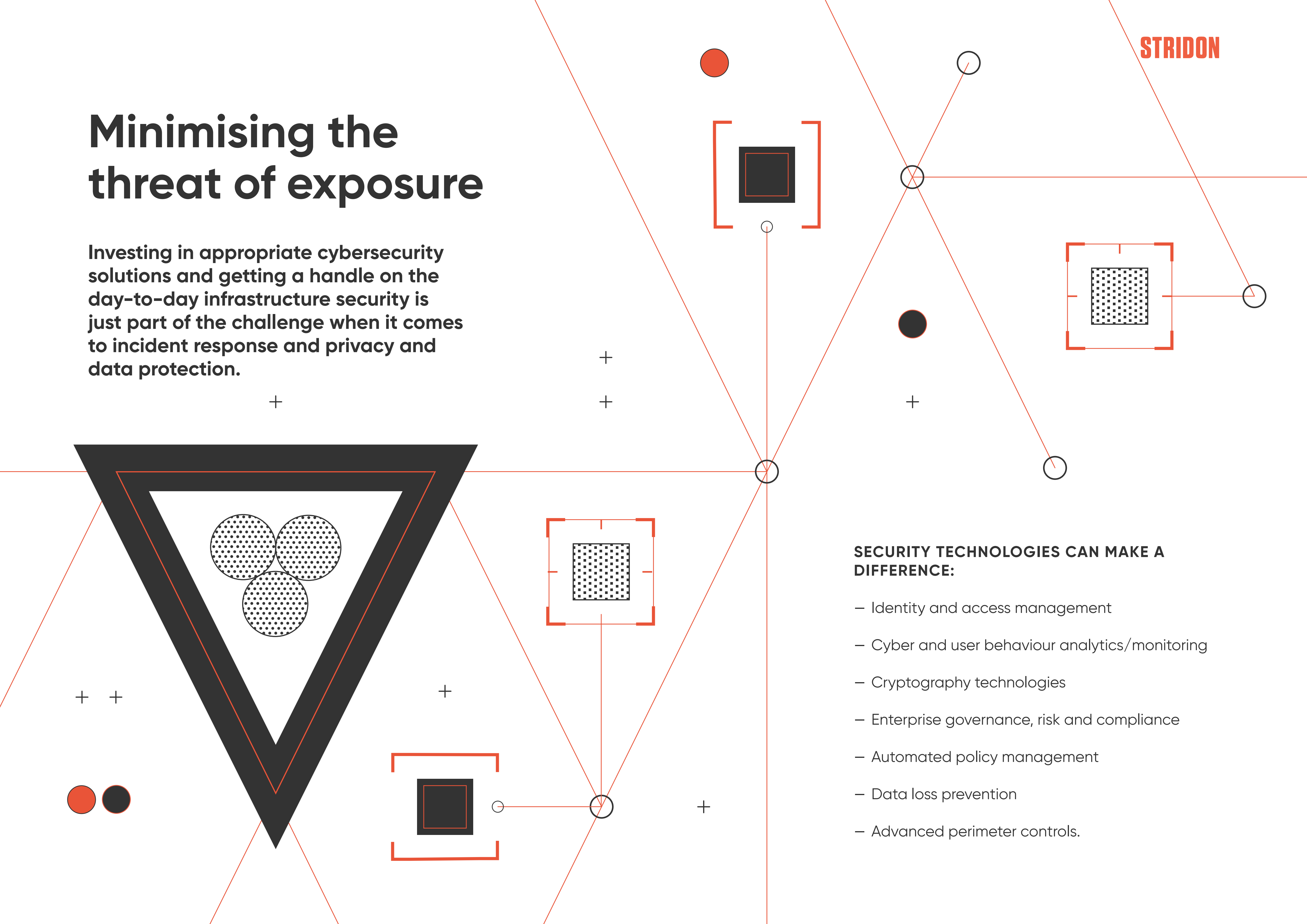
INFORMATION CONCERNS GROWING

Law firms need to carefully evaluate the risk parameters as these apply to their business – the types of clients they handle – and determine the right mix of technologies, policies, procedures and governance that's required.

STRIDON

Minimising the threat of exposure

Investing in appropriate cybersecurity solutions and getting a handle on the day-to-day infrastructure security is just part of the challenge when it comes to incident response and privacy and data protection.



SECURITY TECHNOLOGIES CAN MAKE A DIFFERENCE:

- Identity and access management
- Cyber and user behaviour analytics/monitoring
- Cryptography technologies
- Enterprise governance, risk and compliance
- Automated policy management
- Data loss prevention
- Advanced perimeter controls.

Law firms will also need to take positive action to implement effective policies and procedures to deal with cybercrime and create a culture of cybersecurity awareness. At a very minimum, some elementary best practices will also need to be in place, such as:

- Multi-factor authentication to prevent the widespread access/downloading of sensitive information
- Stringent document management controls and access logs (includes client accounts)
- Frequent updates/immediate patching of systems
- Secure logs that are protected from potential hackers and can be interrogated should a breach occur, to understand the extent/pattern of the event.

Ultimately, business continuity depends on the establishment of strong foundations that minimise exposure to cybercrime and the threats that can stem from cyber security failures.

This should include a bullet proof business resilience, data backup, and disaster recovery strategy that ensures the firm experiences minimum downtime – and can return to business as usual operations as quickly as possible.

But with law firms facing increasing pressure to hold the line on operational IT costs while simultaneously improving how they manage risk, a growing number of progressive firms are taking a managed services approach to ensure they can stay ahead of threats and address the daily challenges of their unique IT environments.

Generating strategic outcomes

Many law firms are discovering a hard truth: they simply do not have the resources to invest at the scale to keep pace with their growing technology needs.

That represents a major challenge for IT leaders that want to focus on a law firm's technology investments in a way that aligns with its overall business strategy – so that the IT function can become an engine of growth:

- Assisting emerging practice areas to win more clients
- Deploying new client engagement and collaboration technologies
- Driving operational efficiencies across practice groups that improve a firm's competitiveness in the marketplace
- Adapting to new client demands by enabling adaptive and agile IT environments that support fast changing requirements.

The managed IT service model enables law firms to turn over day-to-day IT infrastructure requirements to a specialist expert provider who can undertake these tasks at a lower cost, and with greater efficiency.

With the right IT partner in place, law firms are able to improve infrastructure stability, technology support, data security and disaster recovery, while achieving significant cost efficiencies. All of which enables IT leaders to redirect resources to focus more keenly on revenue-supporting activities and initiating new and transformative in-house capabilities.

THE BUSINESS VALUE OF MANAGED SERVICES

- Instant access to IT skills and expertise in new and emerging technologies
- Access to specialised toolsets, operations automation and administration
- Improved system availability, security and responsiveness
- Continuous management of security infrastructure and network security policies, secure access management and authenticated device administration
- Constant monitoring and reporting on the extended IT environment
- Risk mitigation that reduces the incidence of downtime and average recovery times
- Faster innovation that supports operational and business productivity gains
- 24/7 support for users
- Predictable monthly costs.

Under increasing pressure to protect client data, law firms need to initiate broader process and policy shifts – like conducting regular IT security audits, initiating augmented vendor governance and management strategies – as well as considering how existing systems can be leveraged or enhanced to support future services and optimise productivity.

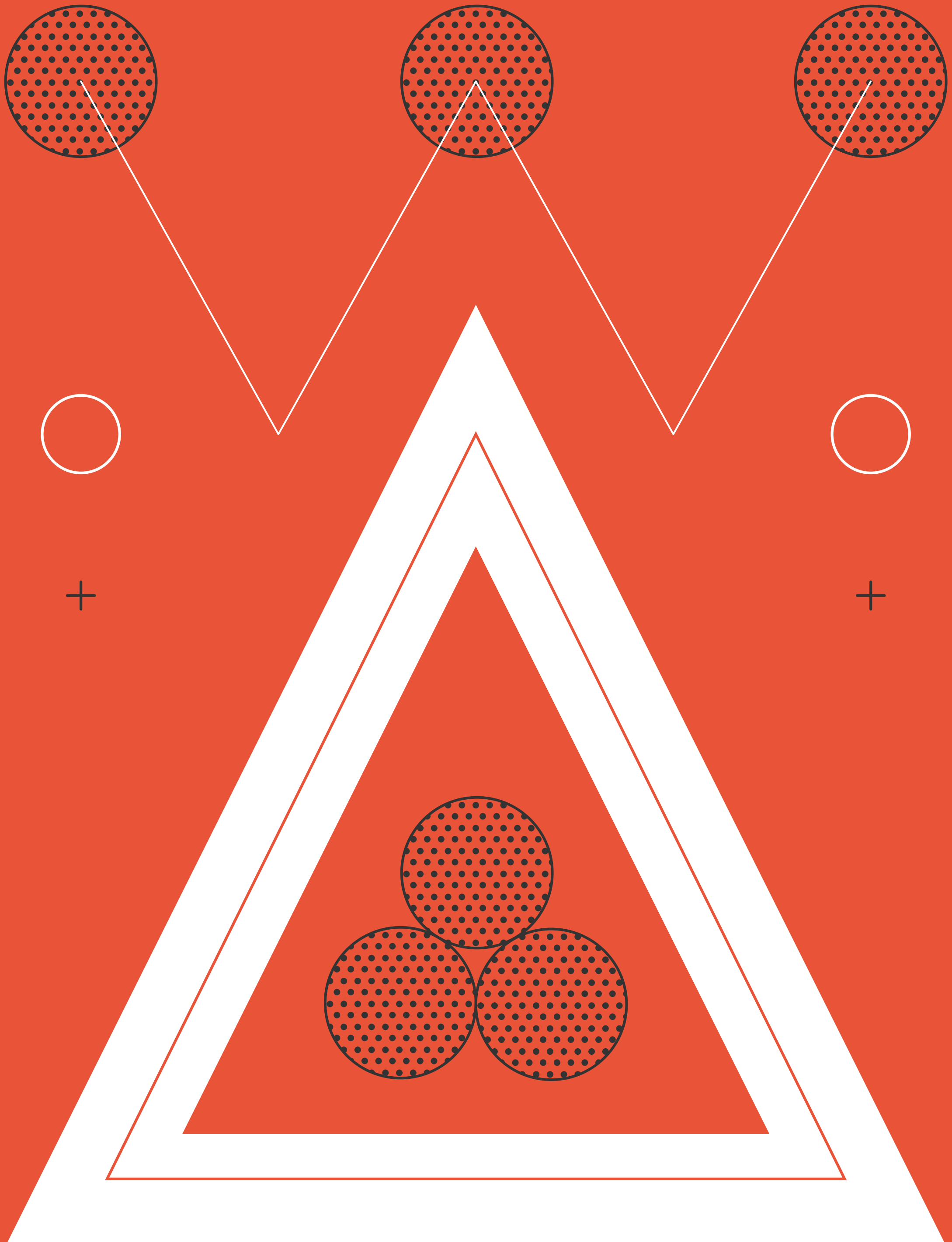
STRIDON - HELPING LAW FIRMS FOCUS ON BUSINESS

At Stridon, we know that keeping pace with monitoring, maintaining, upgrading and securing systems is a day-to-day challenge. Which is why our managed services are designed to support law firms with the complexities of delivering, supporting and managing highly reliable and secure IT systems.

But it doesn't end there. As a strategic IT partner and trusted advisor, we go beyond simply managing workloads to help organisations unlock value from their IT investments and actively manage governance, security and regulatory compliance.

Working alongside IT leaders, we focus on ensuring:

- IT functions are aligned with the broader strategic goals of the firm
- Appropriate strategies are in place to reduce risk and optimise service/system availability
- The risk-free and rapid deployment of new client service and employee productivity models that don't compromise governance or compliance frameworks
- Initiating creative approaches that enable law firms to leverage internal efficiencies and accomplish more, with less
- Clarity on investments and strategies that strengthen organisational defences and ensure that sensitive data is safeguarded against risk – both external and internal



STRIDON

STRIDON

LET'S TALK

T/ +44 (0)20 3006 2140

E/ ideas@stridon.co.uk

W/ stridon.co.uk