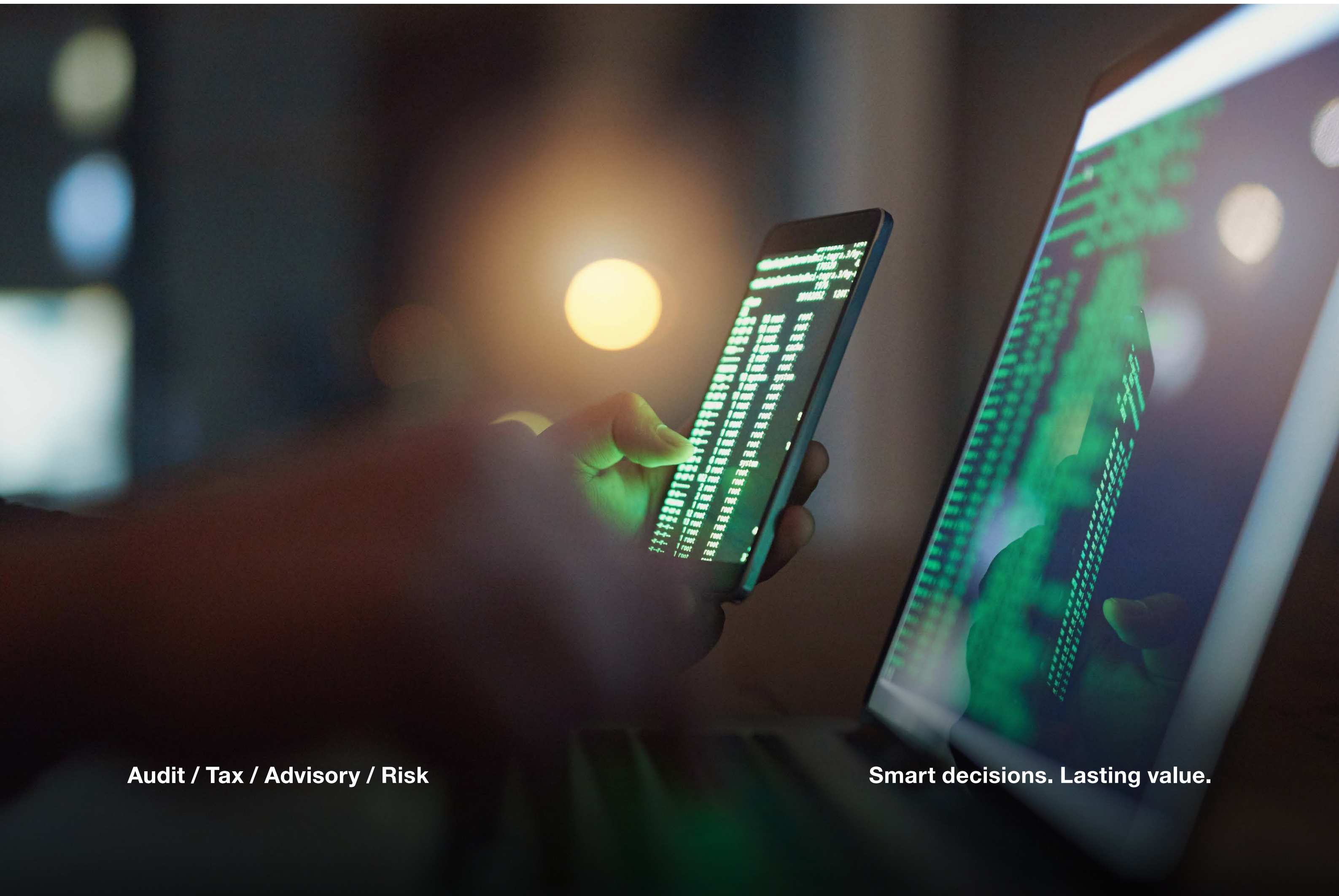
Crowe

KYND

UNIVERSITY OF PORTSMOUTH

Fraud and cybercrime vulnerabilities in the legal sector

Research into the risks impacting the top 200 law firms



Audit / Tax / Advisory / Risk

Smart decisions. Lasting value.

Contents

Key findings

1

Email spoofing

91% of the firms analysed are exposed to having their website addresses spoofed and used to send spam, phishing or otherwise fraudulent emails (either internally or externally).

2

Vulnerable services

80.5% of firms were running at least one service, such as an email server or webserver, with a well-known vulnerability that could be exploited by hackers – putting them at high risk of attack from cybercriminals who specifically target services with known vulnerabilities.

3

Out-of-date software

21% of firms had at least one service that was using software which was out of date and no longer supported by the developer, putting them at higher risk of attack and service failure.

4

Certificate issues

23% of firms had at least one security certificate which had expired, been revoked or distrusted. This means clients, prospects or applications would not be able to securely connect to websites using such a certificate.

5

Domain registration risks

79% of firms had at least one domain registered to a personal or individual email address, representing a significant threat to business continuity and domain ownership.

Introduction

There is an epidemic of fraud and cybercrime in the UK and law firms are not immune.

Irrespective of size, law firms attract cybercriminals due to the large amounts of client money, data and sensitive information they hold.

Sensitive client data is highly valuable as it often includes personal, business and commercial information such as medical records, government secrets and divorce papers all of which can be used as blackmail.

The amount of money law firms are losing to cybercrime is increasing. In 2016 the SRA reported that £9.4 million of client money was lost, increasing to £10.7 million in 2017.

The threat is constantly evolving and firms need to continue evaluating and improving their cyber resilience. The National Cyber Security Centre's Legal Threat Report found that 60% of law firms in the UK reported experiencing an attack in 2017; up from 42% in 2013.

Cybercrime is a key issue for law firms.

The SRA recognised the seriousness of the issue, highlighting cybercrime as a key issue for law firms in their Risk Outlook 2018/19 Report. The Law Society found that the majority of law firms are most concerned with cyber threats, with phishing and email spoofing the most common concern.

The impact of a cyber breach could be devastating, including financial loss and reputational damage.

Although law firms are well aware of the issue, basic vulnerabilities persist.

Crowe, KYND and University of Portsmouth's Centre for Counter Fraud Studies undertook research in May 2019 to establish how vulnerable the legal sector is to cybercrime. The research focused on the websites of the top 200 law firms, by revenue, in the UK and examined the cyber risk exposure of each firm at that point in time. The research utilised KYND's pioneering cyber risk management technology.

The KYND technology tracks down all domains relating to an organisation and the externally facing software and services running on those domains. It highlights risks to the organisation relating to domain registration, service vulnerabilities, security certificates and more.

The findings of the research are stark. The vast majority of top 200 UK law firms have significant unaddressed cyber risks.

Key findings

Email spoofing

91% **of the firms analysed are exposed to having their email addresses spoofed and used to send spam, phishing or otherwise fraudulent emails (either internally or externally).**

Standard inbox spam filters and vigilant staff will catch most phishing by spotting an incorrect originating email address. Spoofed emails appear to be sent from a firm's legitimate address and will not be flagged as spam. It is far harder to spot.

Firms at risk of email spoofing do not have the correct email security configurations in place.

Firms using external email security services may mistakenly assume they are protected. Such services can be effective at protecting an organisation from internal spoofing (an organisation's own domains used to send spoof emails to employees) they are not effective at preventing external spoofing (an organisation's domains used to send spoof emails to customers and suppliers).

Incorrect configurations suggest there may be insufficient oversight of cyber security in the organisation or a lack of knowledge and skills to correctly implement the protection that is available.

182 of the 200 firms analysed were wide open to having their domains spoofed and used to send spam, phishing or otherwise fraudulent emails either internally or externally.

Email spoofing can result in:

- exposure to malware and ransomware
- phishing of employees
- phishing of clients.

What can you do?

- Start by creating a statement, known as a Sender Policy Framework (SPF) record, specifying all the infrastructure that sends emails on your behalf.
- Publish the SPF record within a policy known as Domain Message Authentication Reporting and Conformance (DMARC).
- Begin by using your DMARC to monitor emails being sent on your behalf. If you get to this point, well done! You're now aware of any spoofing attempts that are being made on your organisation's email addresses.
- Based on these reports, over time you'll be able to slowly progress your DMARC policy to first warn recipients of illegitimate emails, before progressing further to stop those emails from being received at all!

It's worth noting that many organisations may be on this journey of understanding & monitoring their emails with minimal settings, which is why they are currently spoofable. They'll be aware of any attempts to do so, and in time will be able to refine their settings to become more and more resilient.

Vulnerable services

80.5% **of firms were running at least one service with a well-known vulnerability – putting them at high risk of attack from cybercriminals who specifically target services with known vulnerabilities.**

Newly discovered software vulnerabilities are disclosed publicly as part of the disclosure and resolution process for software developers. Cybercriminals use these public repositories of software vulnerabilities and identify websites using services with known vulnerabilities.

Running vulnerable services can result in:

- theft of data – hackers can exploit vulnerabilities to directly access sensitive data
- loss of control of website – website owners and visitors can be unaware that the site and traffic to the site has been compromised
- ransomware – a malicious program that removes access to electronic files, usually by encryption
- malware – software specifically designed to disrupt, damage or gain unauthorised access to a computer system also known as a virus, bug or worm.

Out-of-date services

21% **of firms had at least one internet service that was using software which was out of date and no longer supported by its developer, putting them at higher risk of cyber-attack and service failure.**

Older versions of services are no longer supported or maintained by the vendor and any newly discovered vulnerabilities are only patched in the new release versions of the software.

Running old or out-of-date versions of services makes a firm extremely vulnerable to attack and service failure.

Running out-of-date services can have the same impact as running vulnerable services.

What can you do?

- Have a register that includes details of all software used, where it is used, and who is responsible for keeping it up to date.
- Have a procedure to regularly check software is up to date.
- Do not delay or ignore messages to update services when prompted by software providers.

Certificate issues

23% **of firms had at least one security certificate which had expired, been revoked or distrusted, representing a significant threat to brand reputation.**

Visitors to a website with an expired, revoked, invalid or distrusted certificate will see a security warning in their browser and will not be able to visit the site. Applications which use a security certificate to create a secure communication channel to protect data in transit will no longer work if the certificate is expired, revoked, invalid or distrusted.

Out-of-date certificates represent a significant risk to business continuity and reputation.

What can you do?

Implement a procedure for reviewing:

- upcoming certificate expiry date
- when certificates are due to expire
- ensuring certificates are issued by a trusted Certificate Authority.

Domain registration risks

79% **of firms had at least one domain registered to a personal or individual email address, representing a significant threat to business continuity and domain ownership.**

Having firm domains registered to a personal (non-firm) email address or an individual's firm email address makes the individual more prone to social engineering cyber attacks and could also affect the ownership of that domain, representing a risk to business continuity.

If an employee's personal email address is used to set up firm assets, the firm may have difficulties assuming ownership of the assets if the employee leaves.

What can you do?

- Register domains using a generic firm email address such as info@firmname.com.
- Ensure all correspondence to the generic email address is forwarded to more than one employee's inbox.
- Use 'registry lock' and/or two-factor authentication if provided by your registrar. This makes it far harder for an attacker to gain unauthorised access to domain registration data.

Case studies and examples

The case studies below illustrate how the issues identified in this report can have ‘real world’ impacts. Some are for illustrative purposes and others are based on publicly available information.

Email spoofing

Exposure to malware

An example of INTERNAL spoofing

Subject: URGENT: critical security update

From: luke@legal-eagle.co.uk

To: team@legal-eagle.co.uk

Team,

There is a new and critical security flaw in our billing software which we’ve now patched, please immediately download and run the attached package - it will run in the background and only takes a few seconds.

Luke, CTO Legal Eagle UK Ltd

Phishing of clients, customer or suppliers

An example of EXTERNAL spoofing

Subject: APOLOGIES: please login to secure your account

From: geoff.regal@legal-eagle.co.uk

To: any client

____

Dear Client,

I wanted to contact you personally to inform you of a potential breach of information due to a security incident in March 2019. As a precautionary measure we request that you immediately login to change your password.

Geoffrey Regal, CEO Legal Eagle UK Ltd

Phishing of employees

An example of INTERNAL spoofing

Subject: URGENT: late payment on this invoice

From: martin@legal-eagle.co.uk

To: accounts@legal-eagle.co.uk

____

Team,

This invoice is now 2 months overdue & they have got in touch with me personally. Please pay this immediately.

Martin, CFO Legal Eagle UK Ltd

Vulnerable and out-of-date services

NHS WannaCry (Ransomware)

The NHS estimated they lost £92 million as a result of the WannaCry ransomware attack in May 2017. However, the exploit used by the malware had been patched by Microsoft in March 2017. If the NHS had a process for ensuring they kept their services updated to the latest versions they could have avoided this loss.

Maersk - NotPetya (Malware)

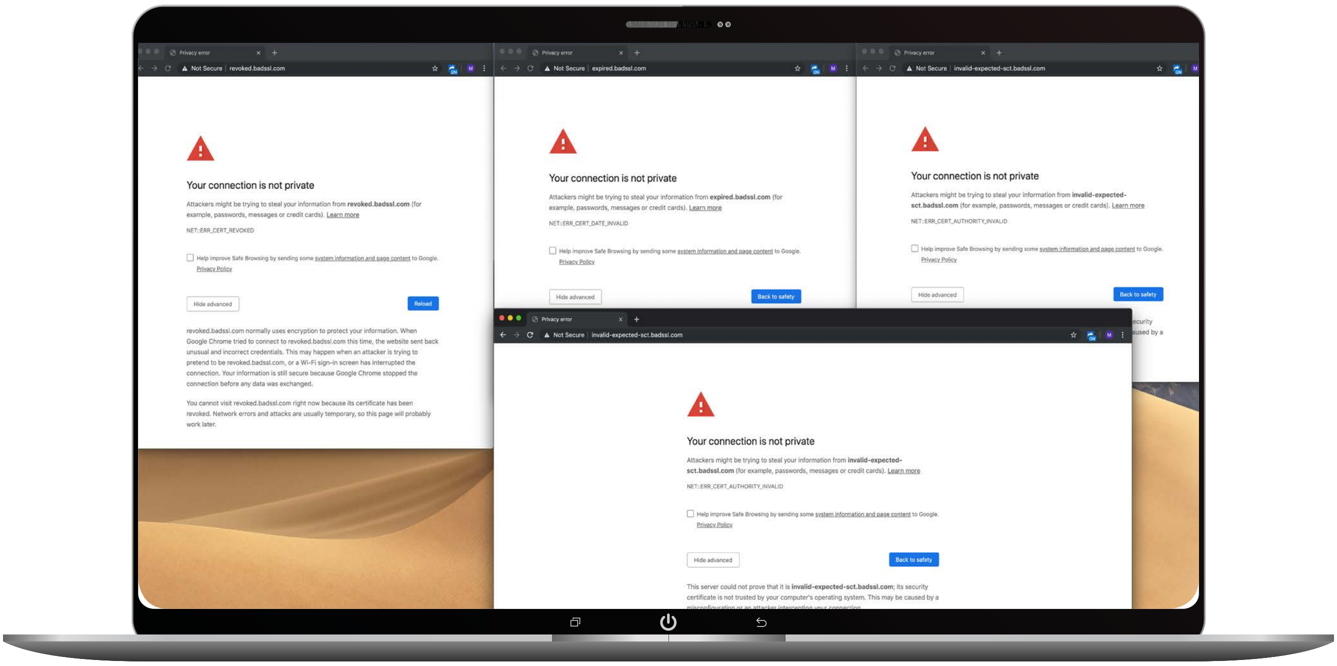
The NotPetya attack of June 2017 exploited the exact same vulnerability as the WannaCry attack earlier in the year. Maersk estimated that they lost $300 million as a result of that attack. Just like the NHS, had they kept their services updated this loss could have been avoided.

Equifax (Theft of data)

This data breach reported in September 2017 exposed records of 145.5 million US citizens in the UK (including dates of birth, addresses, phone numbers, emails and credit card data). The hackers made use of a well known vulnerability in a piece of web software that had been patched in March 2017.

Certificate issues

Below are examples of the types of warning messages displayed by web browsers when there is a problem with a website's security certificate. If your website has similiar problems to the ones below, it will not be accessible to clients.



Your connection is not private

Attackers might be trying to steal your information from **revoked.badssl.com** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_REVOKED

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

revoked.badssl.com normally uses encryption to protect your information. When Google Chrome tried to connect to revoked.badssl.com this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be revoked.badssl.com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Google Chrome stopped the connection before any data was exchanged.

You cannot visit revoked.badssl.com right now because its certificate has been revoked. Network errors and attacks are usually temporary, so this page will probably work later.

Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

Your connection is not private

Attackers might be trying to steal your information from **invalid-expected-sct.badssl.com** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

Your connection is not private

Attackers might be trying to steal your information from **invalid-expected-sct.badssl.com** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy Policy

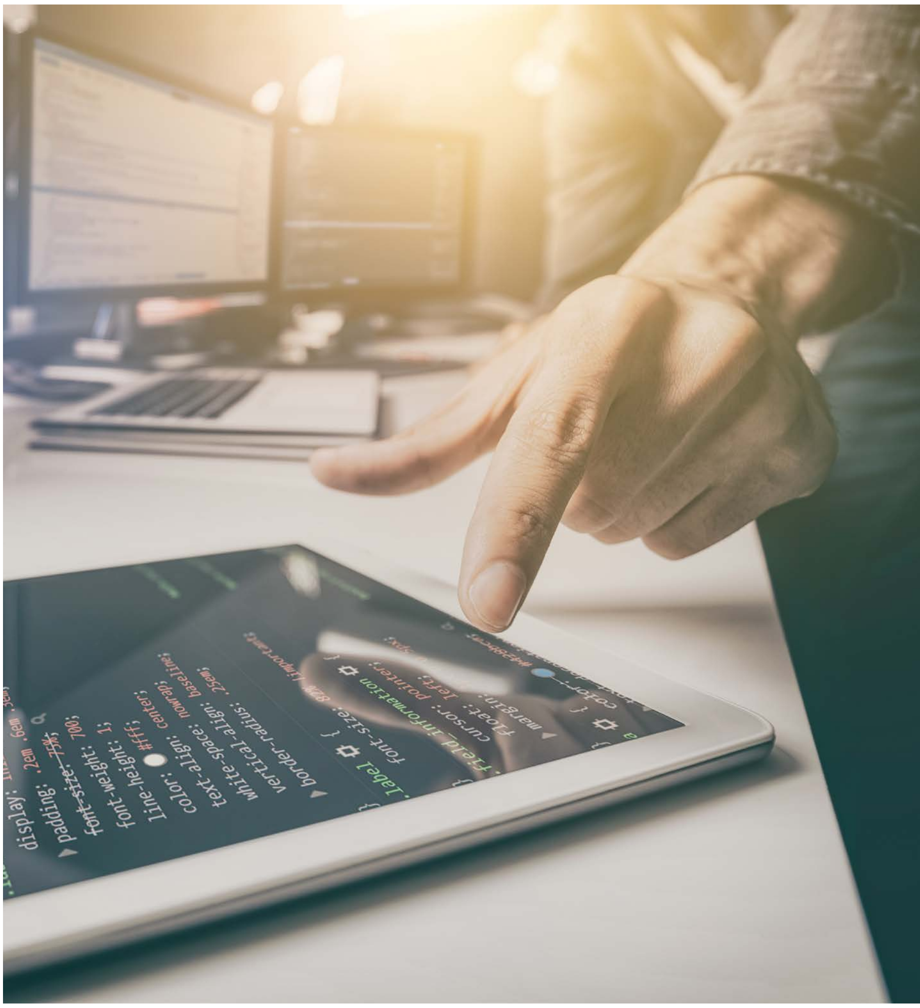
This server could not prove that it is **invalid-expected-sct.badssl.com**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Domain registration risks

In a cyber attack in October 2016, hackers were able to hijack a major Brazilian bank's entire online footprint by gaining access to their website domain registration details. It is believed that the hackers gained access to the bank's domain registration details via a simple social engineering attack.

With these details the hackers changed the Domain Name System (DNS) registrations of all 36 of the bank's online properties, commandeering the bank's desktop and mobile website domains. One weekend afternoon, they rerouted all of the bank's online customers to perfectly reconstructed fakes of the bank's properties.

In essence, the hackers became the bank and absolutely all of the bank's online operations were under the attackers' control for five to six hours causing significant financial loss and reputational damage to the bank.



What should law firms do?

Keeping pace with the evolution of cyber threats is becoming increasingly challenging.

The cyber landscape changes by the second and is weighted in favour of cybercriminals; making it difficult for law firms to maintain effective cyber security.

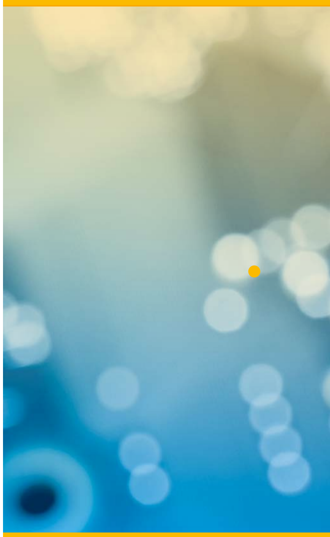
In addition cyber risks can seem complex and senior management may not have the technical skills necessary to interrogate their IT supplier/team about the firm's cyber security and vulnerabilities.

Independent verification should be obtained irrespective of the technical capacity of a law firm's IT team.

Independent verification of a firm's cyber security posture reveals vulnerabilities that could be exploited by hackers. It also provides firms with reassurance that their cybersecurity is being effectively managed.

Crowe can help you to:

- obtain comprehensive insight into your firm's cyber risk exposure
- address specific vulnerabilities in your externally facing IT infrastructure that could be exploited by hackers
- identify whether any of your firm's email addresses have been compromised
- take actions to prevent exploitation of potential cyber risks.



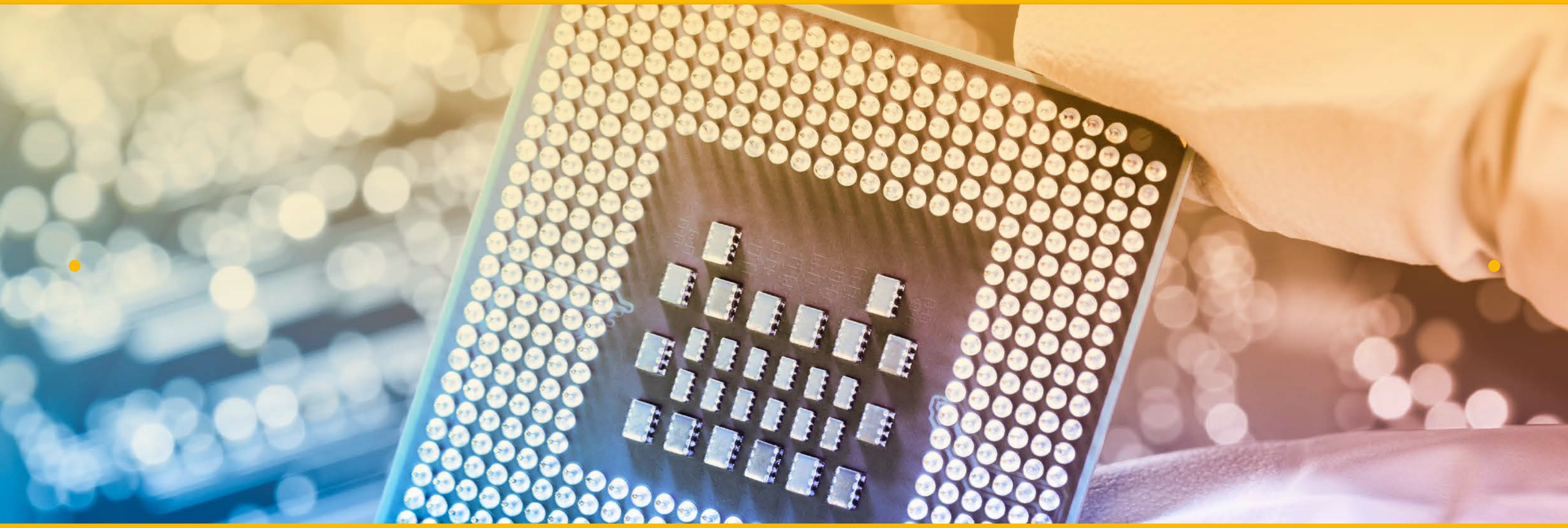
How we can help

If you are concerned the findings of this research relate to your firm, Crowe can provide the independent verification necessary to ensure your firm is protected.

We have extensive experience of working with law firms so we understand the importance of adding value where it matters most to help you to make smart decisions that have lasting value.

For more information and a no obligation discussion please contact us:

Jim Gee
Partner
National Head of Forensic Services
jim.gee@crowe.co.uk
+44 (0)20 7842 7239



Organisations and authors profile

Jim Gee,

Partner and National Head of
Forensic Services, Crowe UK

Visiting Professor and Chair of the Centre for
Counter Fraud Studies, University of Portsmouth

Jim is a Partner and National Head of Forensic Services at Crowe UK. He is also Visiting Professor at the University of Portsmouth and Chair of the Centre for Counter Fraud Studies (Europe's leading centre for research into fraud and related issues) and Chair of the UK Fraud Costs Measurement Committee (a cross-sector body) which, each year, develops and publishes the UK Annual Fraud Indicator.

During more than 25 years as a forensic specialist, Jim has advised Ministers, Parliamentary Select Committees and the Attorney-General, as well as national and multi-national companies, major public sector organisations and some of the most prominent charities. To date he has worked with clients from 41 countries.

He specialises in helping organisations to reduce the cost and incidence of fraud through strengthening the resilience to fraud of relevant processes and systems.

KYND

Melanie Hayes

Chief Marketing Officer and Co-Founder of KYND

Melanie Hayes is the Chief Marketing Officer and co-founder KYND. Using pioneering technology KYND helps keep businesses safe from the growing threat of cyber attacks. The KYND technology tracks down all domains relating to an organisation and the externally facing software and services running on those domains. It highlights risks to the organisation relating to domain registration, service vulnerabilities, security certificates and more.

Starting her career at a prestigious UK retailer where she produced the industry's first e-commerce website Melanie has now gained over 18 years' experience in the technology, food and retail sectors. Working across the globe and most recently for Experian (EMEA) she has produced ground breaking reports on cyber; focusing on the industrialisation of cyber threats, dark web monitoring and the growth and costs of identity fraud.

Professor Mark Button,

Director of the Centre for Counter Fraud Studies at the Institute of Criminal Justice Studies, University of Portsmouth

Mark is Director of the Centre for Counter Fraud Studies at the Institute of Criminal Justice Studies, University of Portsmouth. Mark has written extensively on counter fraud and private policing issues, publishing many articles, chapters and completing eight books with one forthcoming.

Some of Mark's most significant research projects include leading the research on behalf of the National Fraud Authority and ACPO on fraud victims; the Nuffield Foundation on alternatives to criminal prosecution, the Department for International Development on fraud measurement, Acromas (AA and Saga) on 'Cash-for-Crash fraudsters', the Midlands Fraud Forum and Eversheds on 'Sanctioning Fraudsters'.

Mark has acted as a consultant for the United Nations Office on Drugs and Crime and on Civilian Private Security Services. He also holds the position of Head of Secretariat of the Counter Fraud Professional Accreditation Board and is a former director of the Security Institute. Before joining the University of Portsmouth Mark was a Research Assistant to the Rt. Hon. Bruce George MP specialising in policing, security and home affairs issues. Mark completed his undergraduate studies at the University of Exeter, his Masters at the University of Warwick and his Doctorate at the London School of Economics.

Appendices

Findings by turnover

	>£100m	>£50m-£100m	>£25m-£50m	<£10m-£25m	£1m-£10m
Percentage of firms exposed to having their website addresses spoofed either internally or externally	82.5%	81.0%	97.7%	88.8%	100.0%
Percentage of firms running at least one service, such as an email server or webserver, with a well-known vulnerability	92.5%	85.7%	81.8%	74.2%	60.0%
Percentage of firms with at least one service that was using software which was out of date	37.5%	28.6%	18.2%	13.5%	20.0%
Percentage of firms with at least one security certificate which had expired, been revoked or distrusted	47.5%	33.3%	18.2%	11.2%	40.0%
Percentage of firms with at least one domain registered to a personal or individual email address	87.5%	85.7%	86.4%	71.9%	40.0%

Findings by location

	London HQ	HQ outside of London
Percentage of services with known vulnerability (average)	15%	19%
Percentage of services out of date (average)	2%	1%
Percentage of certificates expired, distrusted, invalid or revoked (average)	7%	4%
Percentage of domains registered to personal or individual email (average)	37%	42%

Crowe

Start the conversation

Jim Gee
Partner, National Head
of Forensic Services
jim.gee@crowe.co.uk
+44 (0)20 7842 7239

About Us

Crowe UK is a national audit, tax, advisory and risk firm with global reach and local expertise. We are an independent member of Crowe Global, the eighth largest accounting network in the world. With exceptional knowledge of the business environment, our professionals share one commitment, to deliver excellence.

We are trusted by thousands of clients for our specialist advice, our ability to make smart decisions and our readiness to provide lasting value. Our broad technical expertise and deep market knowledge means we are well placed to offer insight and pragmatic advice to all the organisations and individuals with whom we work. Close working relationships are at the heart of our effective service delivery.

www.crowe.co.uk

@CroweUK

Crowe U.K. LLP is a member of Crowe Global, a Swiss verein. Each member firm of Crowe Global is a separate and independent legal entity.
Crowe U.K. LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global.