Fraud and cybercrime vulnerabilities in Independent Schools

Research into the risks impacting 200 Independent Schools

Audit / Tax / Advisory / Risk

Smart decisions. Lasting value.

Contents

Key findings

1

Ransomware risk

34% of schools had at least one external internet service exposed, which would place them at a higher risk of a ransomware attack.

2

Email spoofing

98.5% of schools analysed were exposed to having their email addresses spoofed.

3

Vulnerable services

59.6% of schools were running at least one service, such as an email server or web server, with a well-known vulnerability to a cyber attack.

4

Out of date software

13.6% of schools had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

5

Certificate issues

32.3% of schools had at least one internet security certificate which had expired, been revoked or distrusted.

6

Domain registration risks

33% of schools had at least one domain registered to a personal or individual email address.

Introduction

There has been a surge in fraud and cybercrime in the UK and Independent Schools are not immune.

A survey undertaken in 2019 found that 61% of UK Independent Schools have been targeted for cyber-attacks in the last five years.

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

Increasing integration of technology in the classroom and the recently accelerated shift to on-line learning has created new vulnerabilities which can be exploited by criminals.

Schools also hold sensitive pupil data (including financial details of parents who spend a considerable amount on fees each term). Hackers target schools with data protection measures and social engineering attacks such as phishing.

While data and financial loss are the more tangible risks, it is the subsequent reputational damage this causes that can have the biggest impact as Independent Schools rely on their reputation to attract new students.

Irrespective of size, Independent Schools attract cybercriminals due to their visibility and the opportunity for potential reputational damage as leverage to extract ransom payments.

The impact of a data breach on an Independent School could have significant legal and reputational consequences.

The impacts of a breach could result in an inability to deliver quality teaching to students, and could result in the loss of sensitive personal data.

The amount of money organisations are losing to cybercrime is increasing. Ransomware attacks alone increased by 350% in 2018, with global ransomware damage costs expected to double to £20 billion by 2021.

The threat is constantly evolving and schools need to continue evaluating and improving their cyber resilience. Although schools are well aware of the issue, basic vulnerabilities persist.

Crowe, KYND and the University of Portsmouth's Centre for Counter Fraud Studies undertook research in June 2020 to establish how vulnerable Independent Schools are to cybercrime. The research focused on the internet domains of 200 independent senior schools, and examined the cyber risk exposure of each school at that point in time. The research and its findings are representative of schools across the Independent School sector. 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 the 200 Independent Schools have significant unaddressed cyber risks.

Key findings

The findings of the research undertaken by Crowe, KYND and University of Portsmouth in June 2020 is presented below.

Ransomware risk

34% **of schools had at least one external service exposed, which would place them at a higher risk of a ransomware attack.**

Ransomware is an emerging form of malware that locks the user out of their files or their device, then demands an anonymous online payment to restore access. Such attacks saw a 350% increase in 2018, with global ransomware damage costs predicted to hit £20 billion in 2021, up from £11.5 billion in 2019. This past year bore witness to ransomware impacting organisations large and small, public and private. A more recent twist is not only encryption of the network for a ransom, but if the victim refuses to pay, then the attackers release sensitive data on the internet – turning a ransomware-based disruption into a data breach.

The implication for a school could be a threat to release the personal information held about pupils and parents, for example, name, date of birth, address, unless a ransom is paid. In addition, a ransomware attack could prevent the school from delivering classes to pupils, or even lose data about pupils educational achievements and exam results.

One of the most utilised methods for hackers carrying out ransomware attacks is simply to scan the public internet for specific open ports relating to services, which would allow external access if not securely configured. The open ports can provide hackers with a 'way in' to an organisation.

Commonly exploited services are those used for file sharing or remote access, for example File Transfer Protocol (FTP), Secure Shell (SSH), Server Message Block (SMB) and Remote Desktop Protocol (RDP).

Having these types of service externally exposed can result in ransomware – once target services have been identified, hackers will typically gain access by brute-forcing passwords in order to login as the administrator. They will then encrypt data and demand a ransom payment, typically in cryptocurrency (e.g. Bitcoin) for the school to regain access.

What can you do?
These types of services should not be accessible or visible on the public internet and should immediately be hidden behind a firewall or the port should be closed.

Email spoofing

98.5% **of schools 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 an organisation's legitimate address and will not be flagged as spam. They are far harder to spot.

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

Organisations 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), but 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.

Of the 200 schools analysed, 197 of them (98.5%) had configurations in place that means their domains could be spoofed and used to send spam, phishing or otherwise fraudulent emails either internally or externally.

If a school's email address was spoofed, a hacker could send an email that looks like it came from the school. The email could inform the parent that the school's bank account has changed and fees should be paid to the new bank account. The parent and the school would be out of pocket, and a difficult conversation would be necessary about which side should bear the cost.

Email spoofing can result in:

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

What can you do?
Preventing email spoofing is straightforward and requires that email 'policy' is correctly configured. Email policy configuration is slightly technical and requires the following:

- 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. Getting to this point will mean that you are now aware of any spoofing attempts made on your organisation's email address.
- 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.

Vulnerable services

59.6% **of schools 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.**

New software vulnerabilities are regularly identified and the companies responsible for the software, like Microsoft, disclose the vulnerabilities publicly and provide fixes to address them. Organisations that do not implement the fixes in a timely manner will run vulnerable software, and cybercriminals use publicly available information to identify when an organisation is running such software. The vulnerabilities can then be exploited to attack an organisation.

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

13.6% **of schools 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 school 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

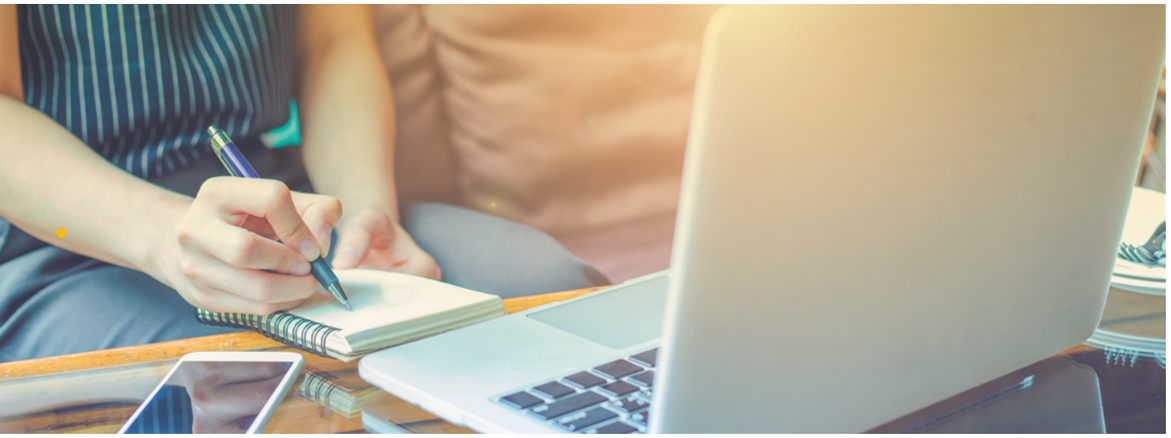
32.3% **of schools had at least one security certificate which had expired, been revoked or distrusted, representing a significant threat to brand reputation.**

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 the continuity of schools operation and also its reputation.

What can you do?
Implement a procedure for reviewing:

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



Domain registration risks

33% **of schools had at least one domain registered to a personal or individual email address, representing a significant threat to the continuity of a schools operation and domain ownership.**

Having school domains registered to a personal (non-school) email address or an individual's school 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 operational continuity.

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

What can you do?

- Register domains using a generic school email address such as info@schoolname.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.

UK Independent School

Fraudsters posed as a parent and sent the school a request to update their parent details (email and telephone) from the parents real email address.

Compromised emails and passwords are sold on the Dark Web for around $2 and accessible via webmail (previous research we carried out into the Dark Web found that one school had 800 compromised emails associated with it for sale).

The school administrator accepted the posed email request as genuine and either directly changed the contact details on the schools database system or passed it to another school employee to do so. The latter case is common as the second employee thinks the request is legitimate as the first employee would have already checked and has sent it to them.

The fraudsters then sent a request for a refund of fees from the new email linked to the schools database The school employee then checked this email address with that on the database and verified it as legitimate against the parent contact details.

In this case the school employee also called the parent to check using the phone number on the school database. However, these details had also been updated on the schools database and the fraudster was able to answer the phone and pose as the parent confirming the request to be genuine and providing bank details for the transfer to take place.

As a result of the incident the school implemented multi-factor authentication on its systems and strengthened controls on changes to parent contact details. These changes will prevent the same issue in the future.

UK Independent School

A school in Dorset was hit by a ransomware attack in 2019. The malware arrived by email and resulted in the infection of the school's IT network.

The ransomware resulted in the loss of a year's GCSE coursework.

Travelex

Over the New Year of 2019 to 2020, Travelex became the victim of a ransomware attack that took their online operations down for almost a month, leaving their customers and those of several major high street banks (Sainsbury's, RBS, Lloyds, Barclays, HSBC and Tesco) unable to access online orders or retrieve refunds for their travel money. Travelex had allowed Remote Desktop Protocol (RDP) to be accessible over the public internet, which meant that hackers were able to directly access computers on the Travelex network and 'brute-force' passwords. The attackers obtained and encrypted over 5GB of customer data before deleting the backups and demanding Travelex pay a ransom of £4.6 million to regain access. To date it is not clear whether Travelex has paid the ransom.

Email spoofing

Exposure to malware

An example of **INTERNAL** spoofing: In this email, the cyber criminal wants the person receiving the email to download and run malware.

Subject: URGENT: critical security update

From: luke@london-school.co.uk

To: team@london-school.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, Head of IT, London School

Phishing of clients, customer or suppliers

An example of **EXTERNAL** spoofing: In this email, the cyber criminal wants to obtain the login username and password by directing the email recipient to a false login page.

Subject: APOLOGIES: please login to secure your account

From: geoff.regal@london-school.co.uk

To: any client

_____

Dear Parent,

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, Headmaster, London School

Phishing of employees

An example of **INTERNAL** spoofing: In this email, the cyber criminal is attempting to trick the email recipient into paying the invoice into the criminal's bank account.

Subject: URGENT: late payment on this invoice

From: martin@london-school.co.uk

To: accounts@london-school.co.uk

_____

Team,

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

Martin, Bursar, London School

Vulnerable and out-of-date services

NHS WannaCry (Ransomware)

The NHS estimated it 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)

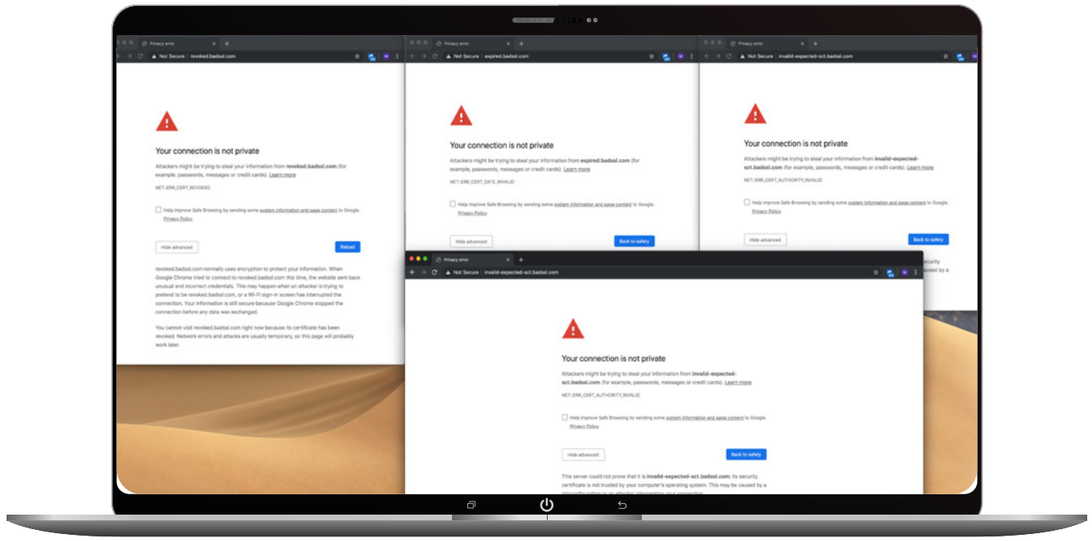
The NotPetya attack of June 2017 exploited the exact same vulnerability as the WannaCry attack earlier in the year. Maersk estimated that it lost $300 million as a result of that attack. Just like the NHS, had they kept their services updated this loss could have been avoided.

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 parents and students.



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 its 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 schools 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 schools 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 organisation's cyber security and vulnerabilities.

Independent verification should be obtained irrespective of the technical capacity of your school's IT team.

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

Schools should consider whether IT systems are configured securely and what forms of assurance are available to governors and trustees. Third party suppliers, and the systems provided by third party suppliers, can introduce cyber and information security risks. Schools should have processes in place to identify and assess the risks posed by third party suppliers, and a procedure to manage those risks. Cybercrime is so common that schools should consider that it is a matter of time before their is a serious incident of some sort. Schools should have an incident response plan in place and should undertake different scenario exercises to test the plan. An organisation's response to an incident has a significant bearing on an incident's impact and how quickly an organisation can recover.

Crowe can help you to:

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

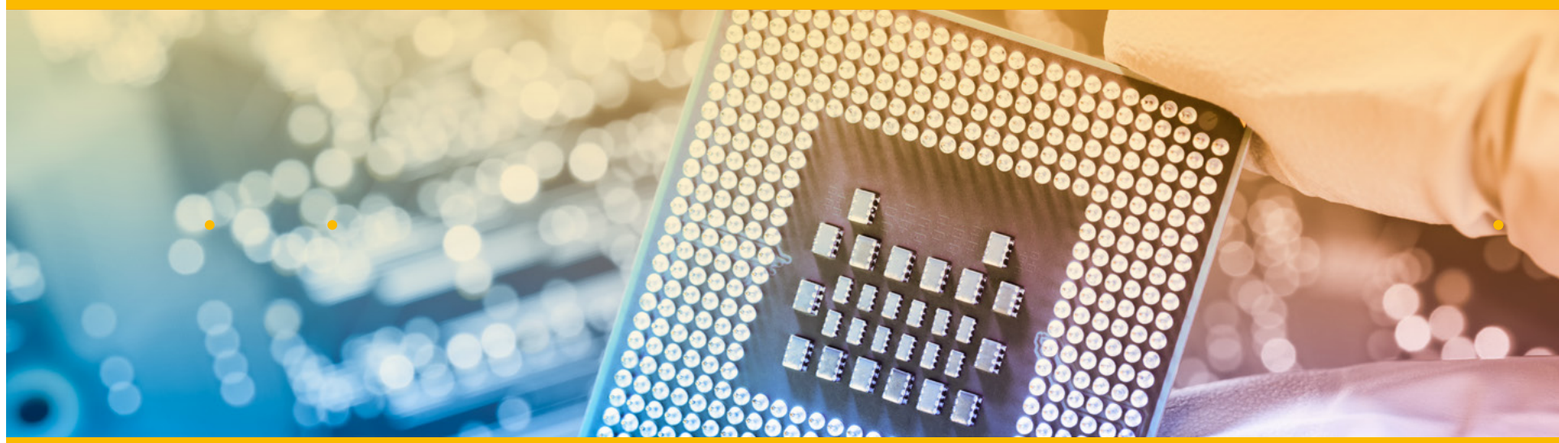
How we can help

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

We have extensive experience of working with Independent Schools 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.

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

Find out more about Crowe's Forensic Services team:
www.crowe.com/uk/croweuk/services/advisory/forensic-services

Eoghan Daly

Director of Forensic Services, Crowe UK

Eoghan is the Director of Forensic Services at Crowe UK and leads the firm's cyber security work. He has worked with organsiations across many sectors to help them improve how they manage cyber and information security.

In addition to his cyber security work, Eoghan works with organisations to strengthen their fraud resilience, and if fraud is suspected, to investigate what happened and what recovery options are available. In addition to his work in the private sector, Eoghan's advice has informed government policy in the UK and Ireland, and also in various parts of the European Union.

Find out more about Crowe's Forensic Services team:
www.crowe.com/uk/croweuk/services/advisory/forensic-services

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 organisations 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) Melanie has produced ground breaking reports on cyber, is a keynote speaker and works wth the government advising on cyber policy and laws.

Find out more about KYND:
www.kynd.io/

UNIVERSITY OF PORTSMOUTH

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.

Find out more about the Centre for Counter Fraud Studies:
www.port.ac.uk/research/research-centres-and-groups/centre-for-counter-fraud-studies

Crowe

Start the conversation

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

Eoghan Daly
Director, Forensic Services
eoghan.daly@crowe.co.uk
+44 (0)20 7842 7219

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