

P03 Cyber crime, bribery and corruption are on the rise

P06 Anti-fraud measures are not optional, they are compulsory

P08 Fraudsters are targeting big money in the financial services



RACONTEUR

24/09/14
#0276

● RACONTEUR.NET
● /COMPANY/RACONTEUR-MEDIA
● /RACONTEUR.NET
● @RACONTEUR



Because some headlines
are not worth making.

Protect your network with F5.

f5.com



Solutions for an application world.



The Resilient Win

Preventative and proactive action against fraud doesn't only ensure business survival; it makes you competitive.

If trust is the most valuable commodity of the information age then a strong reputation is priceless. You can trade on that; you can compete and grow. But when every business is so vulnerable to Internet attack, how strong is the truth behind your reputation? How well can you look after what your customers and partners entrust you with?

With over 200,000 enterprise customers, including 9 of the top 10 banks and 9 of the top 10 defence/aerospace companies, Fortinet is one of the biggest IT security vendors in the world. We've learned truths that would make your toes curl. We also know that the resilient win.

And you can take it as read that cybercriminals are putting a big price on your data, but need only pay pennies of their own finding holes in your defences. There are hard choices to make. You could batten down the hatches, pull down the blinds and kill off your risks. Or you could carry on innovating and embracing change, driving agility in your business; confident that your data, your people and your reputation are safe.

Security Says Yes

According to a new global study commissioned by Fortinet, 54% of CIOs see security as an obstacle to innovation and have either slowed or thrown out new business initiatives because of fraud and other cybersecurity fears. Sadly these aren't businesses enjoying the freedom to achieve their objectives. These are businesses where security likes to say 'no' instead of 'yes'.

Cyber threats are rising in volume and complexity, and your business must have the resilience to face this challenge without changing course.

Such resilience only comes when you commit to a cohesive lifecycle approach to confronting the many facets of today's advanced and persistent threats. This allows you can grow, take advantage of new technologies, be compliant to your regulatory requirements and remain trustworthy in the eyes of your market.

This is Fortinet's Advanced Threat Protection framework. Find out more at www.fortinet.com/ATP

FORTINET®



Distributed in
THE TIMES

Publishing Manager
John Okell

Managing Editor
Peter Archer

Production Manager
Natalia Rosek

Commissioning Editor
James Dean

Design, Infographics & Illustration
The Design Surgery
www.thedesignsurgery.co.uk

Contributors

STEPHEN ARMSTRONG

Contributor to *The Sunday Times*, *London Evening Standard*, *Monocle*, *Wallpaper** and *GQ*, he is also an occasional broadcaster on *BBC Radio 4* and *Radio 2*.

JAMES DEAN

Technology correspondent at *The Times*, he has previously reported on financial crime, and the legal and accountancy professions as a business correspondent.

TOM FOX-BREWSTER

Freelance journalist covering information security, whose work has appeared in *The Guardian* and *WIRED*, he was named BT Security Journalist of the Year in 2012 and 2013.

CHRIS JOHNSTON

Former business news editor at *The Times*, he is now a freelance journalist writing on a wide range of business subjects.

CHARLES ORTON-JONES

Former Professional Publishers Association Business Journalist of the Year, he was editor-at-large of *LondonlovesBusiness.com* and editor of *EuroBusiness* magazine.

EDWIN SMITH

Writer and editor, he has contributed to *The Guardian*, *The Independent*, *The Independent on Sunday*, *The Sunday Telegraph*, *London Evening Standard*, *City AM* and *Private Eye*.

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3428 5230 or e-mail info@raconteur.net

Raconteur Media is a leading European publisher of special interest content and research. It covers a wide range of topics, including business, finance, sustainability, lifestyle and the arts. Its special reports are exclusively published within *The Times*, *The Sunday Times* and *The Week*. www.raconteur.net

The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher.
© Raconteur Media

● RACONTEUR.NET
● [/COMPANY/RACONTEUR-MEDIA](http://COMPANY/RACONTEUR-MEDIA)
● [/RACONTEUR.NET](http://RACONTEUR.NET)
● [@RACONTEUR](https://twitter.com/RACONTEUR)

FIGHTING FRAUD ONLINE:
WWW.RACONTEUR.NET/FIGHTING-FRAUD-2014

P03



Overview



Image: Getty

Cyber crime, bribery and corruption are on the rise as corporate UK seeks to raise its defences against the fraudsters, writes James Dean

Kofi Annan once said: “Corruption, is an insidious plague. It undermines democracy and the rule of law, leads to violations of human rights, distorts markets, erodes the quality of life, and allows organised crime, terrorism and other threats to human security to flourish. This evil phenomenon is found in all countries big and small, rich and poor.”

The then United Nations secretary-general was speaking 11 years ago on the day the UN adopted its convention against corruption. The convention gave impetus to a wave of anti-corruption legislation across UN member states, such as the recent Bribery Act in the UK. The UK and the United States, with its fierce Foreign Corrupt Practices Act, are the two nations leading the way in the fight against corruption at home and abroad. And the agencies that enforce these laws are enjoying something of a renaissance at present, with the US Department of Justice in particular enjoying a string of successful prosecutions.

Bribery and corruption are as old as mankind. The man on the street understands what they are and what effects they have. Such is our comfort with these concepts that the tale of corruption at Enron, the American energy company, can be made into a musical that plays on Broadway and in the West End.

Cyber crime is, though, a very different matter. Highly intelligent

individuals, let alone the average man, have been left fumbling in the wake of the advances in information technology of the last two decades. The vast majority of us simply do not understand how information is being obtained, stored and disseminated in the modern world.

Sometimes these issues hit the headlines, such as the recent news that more than 100 female celebrities had hundreds of intimate photos stolen from their private online accounts. Events like these prompt people to take action – in this case, to take far greater care to protect their cloud computing accounts with stronger passwords or, perhaps, not to take nude selfies on smartphones.

BREACH OF PRIVACY

The women affected by this gross breach of privacy had, it appeared, very little understanding of the technology they were using and how it might be compromised. An even darker side to the story was that the hackers had apparently gone completely undetected as they took what they wanted from the women’s accounts for many years.

Lessons learnt from episodes such as these apply to businesses as much as they do to individuals. It appears that many companies are beginning to act with greater urgency.

The “big four” accountancy firms are somewhat a bellwether for the corporate community. Different practices within these professional

services firms grow and shrink depending on the services required of them from their corporate customers. Within the last year, all four have drastically grown the size of their cyber security practices. EY, for example, said that it would double the size of its practice.

Some recent huge hacks have added to the sense of urgency about shoring up corporate cyber defences. In the largest known leak of personal information, hackers stole 152 million records from 38 million customers of Adobe, the software company, including credit card details, passwords and user names. eBay, the online marketplace, admitted earlier this year that 145 million customer records had been stolen by hackers. According to Risk Based Security, an information security

firm, 822 million personal records were exposed in more than 2,100 attacks globally in 2013.

Some recent huge hacks have added to the sense of urgency about shoring up corporate cyber defences

The fear among businesses of hacking attacks is perhaps the reason that nearly half of all companies believe their cyber security risk has increased in the last year, according to the 2014 *Global Economic Crime Survey* by PwC. This proportion is

the most common of all categories.

In all, more than a third of those surveyed by PwC – 37 per cent – said that they had fallen victim to economic crime in the past year, a rise from the previous year and the year before that. The statistics suggest that, new or old, fraud continues to pervade many corners of corporate life. ■



OLD TRICKS, NEW CONS

Whether it's tricking a victim to give away too much information over the phone or slick computer software which steals sensitive data, cyber fraudsters are pocketing big money, as Tom Fox-Brewster reports

There is a perception among the general population that cyber fraud is some modern esoteric art perpetrated by alpha geeks sitting behind keyboards, clothed in hoodies, hiding in a darkened room. But in reality, present-day fraudsters tend to use old tricks to gain access to people's bank accounts. They can still earn plenty of money by using trusted methods in the cyber realm without having to invest in the latest, sexiest hacking tools, which can cost upwards of £10,000.

Blowing
the Whistle
.....
Page 10



The telephone remains a popular launch pad for identity theft. Using internet-enabled services such as Skype, hackers are able to hide their true identity, while voice manipulation software allows them to tweak the frequency of their speech and easily dupe call centre staff, says Vijay Balasubramanian, chief executive and co-founder of Pindrop Security.

Where relevant some even pretend to have a speech impediment or to be a carer for a disabled caller. Once they have access to people's online accounts and have changed the relevant usernames and passwords, they can quickly shift funds to their own coffers.

In one case, Pindrop looked at the records of a large bank, reviewing 300,000 calls. The bank knew of ten cases where fraudsters had called in, but Pindrop uncovered 115, including one that led to an illicit \$97,000 (£58,000) wire transfer to Cambodia. Most companies think that just 2 per cent of their fraud exposure comes from the phone channel, but in reality it's more like between 30 and 80 per cent, says Mr Balasubramanian.

SOPHISTICATED SCAMS

There are more sophisticated campaigns, ones that have resulted in huge profits for criminals. Considered by US law enforcement to be one of the evil geniuses of the online dark markets, Evgeniy Mikhailovich Bogachev is alleged to have run two of the slicker cybercriminal operations of recent memory, known as Gameover Zeus and Cryptolocker.

The former saw as many as one million PCs infected with the Zeus malware, which siphoned off victims' bank logins. The Cryptolocker "ransomware" encrypted hundreds of thousands of people's files, making them inaccessible before asking for payment to unlock them. Bogachev and his crew were believed to have earned at least \$100 million through such illicit means.

Kroll, which carries out fraud investigations for businesses, has seen a recent rise in e-mail and social media account takeover, using similar strategies as the Gameover Zeus and Cryptolocker crooks. "In such cases, criminals will compromise e-mail and social media accounts and then send out communications as the true account holder attempting to trick the recipients into an action, such as clicking a link, installing credential-stealing malware or even paying a fake invoice," says E.J. Hilbert, head of cyber investigations at Kroll Europe, Middle East and Africa.

Phishing websites, which look like they're genuine versions of web services, are also common. As the sites appear to be legitimate, users are happy to enter their personal data, not realising they are being duped by identity thieves. Such data, however it is acquired, is often sold on underground web forums, making it more likely the victims' accounts will be compromised. "Trade secrets and the intellectual property of a business can also be targeted," notes Darren Hodder, director at Fraud Consulting.

18,000

phishing attacks took place across Europe, the Middle East and Africa in the first six months of this year, costing organisations \$154 million

31%

of the phishing attacks were in the UK – the highest number – with an estimated loss of \$48 million

47%

of identified fraud transactions originate in the mobile channel, a 68% increase since 2012 and up 29% since 2013

Source: RSA Anti-Fraud Command Center

INSIDE JOBS

Then there are insiders to fret about. "We are increasingly seeing cases where trusted insiders are being used to assist cyber attacks from within the firms themselves," says Paul Walker, head of forensic technology and discovery services at EY.

These moles are either purposefully placed within the target organisation or identified and turned, says Mr Walker. They can then be used to initiate attacks. Certain cases have seen infected USB sticks shoved into company systems installing malicious software or malware on the corporate network to Hoover up information. In other cases, the moles are used to identify weaknesses for subsequent attack.

of technologies such as anti-malware and digital intelligence systems that could help them detect and repel strikes on their infrastructure.

"Businesses need to recognise that they simply cannot protect everything – better to focus on protecting the digital assets that matter the most and would result in a material loss to the business. The first step in this process is understanding what is most important for the business to protect," says Ryan Rubin, managing director and leader of Protiviti's UK security and privacy practice. "Companies will need to accept a degree of inconvenience in areas that matter most. However, if they are honest about the risks they can live with and prioritise the risks they are not willing to accept, solu-



Trade secrets and the intellectual property of a business can also be targeted

"By directly bypassing the firm's security measures and installing malware directly on the target's network, a wealth of information is made available for hackers to steal and distribute, and by use of insider targeting agents, attacks can be stealthy and focused," Mr Walker adds.

One reason why cyber fraudsters are causing such chaos – £266 billion a year in economic damage, according to computer security software company McAfee, though this figure has been disputed – is that many companies are not using adequate tools to respond to attacks. A recent study from consultancy Protiviti revealed that only 10 per cent of organisations are taking full advantage

tions can be implemented to minimise this inconvenience."

Active incident response processes, proactive monitoring and greater "situational awareness" will all help businesses learn normal behaviour and detect anomalies, which may be early indicators of fraud, Mr Rubin adds.

In the case of financial institutions, though, they have to offer high levels of security by necessity and they rely on customers to be vigilant too. When cybercriminals steal money from customer accounts, the cost is passed on to the banks once they hand out compensation. It's not just businesses that have to wise up when it comes to security.

Case Study

PERSONAL DATA AND PORN:
A CASE OF INSIDER FRAUD



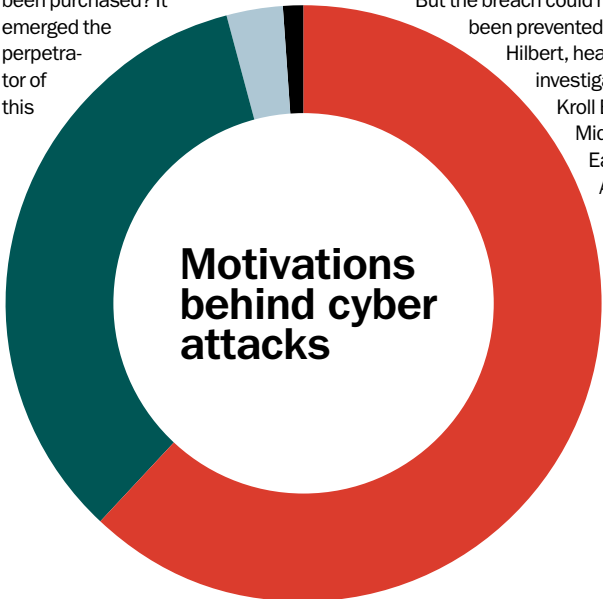
Image: Getty

Privacy-conscious consumers, like criminal hackers, have a reason to target data brokers, organisations whose sole purpose is to collect people's information to sell on to interested parties, primarily marketers. Given the nature of such businesses, company insiders at the brokers might not suffer paroxysms of guilt if they carried out their own attack on their employer's network. A US case tracked by investigators at Kroll in 2012 involved a particularly entrepreneurial employee who chose to use his role and access to company information to make thousands of dollars. Startlingly, the insider had actually contracted Kroll to investigate a missing laptop that contained sensitive data six weeks prior to the start of the investigation into his own activities. The affected company noticed something odd when old equipment, which was supposed to have been decommissioned, was still in use. Why was it still running when new servers, worth as much as \$50,000, had been purchased? It emerged the perpetrator of this

particular fraud had bought up fresh systems so he could use the old ones to store certain business data and sell it off to interested outside parties. He set up websites on the systems for that very purpose, selling background information on his employer's staff to any willing bidders, including hacktivists looking to de-anonymise people they believed to be wrongdoers, according to Kroll. It got worse. Not only had he set up chat forums to discuss deals with potential buyers of the data, he decided to run a pornography site on one of the servers. All this was done using the business' systems, sucking up power and bandwidth, at a further cost to the organisation. Once Kroll had uncovered his activities, swift action was taken to fire the employee and begin criminal proceedings. Everything was kept under the radar, due to the obvious embarrassment the company would have felt, hence the continued anonymity.

But the breach could have easily been prevented, says E.J. Hilbert, head of cyber investigations at Kroll Europe, Middle East and Africa. For starters,

the firm wasn't properly monitoring inbound and outbound connections into the company network. If the firm had layered automated tools designed to pick up on anomalous activity on gateways into the organisation, they would have been alerted to the unauthorised use of corporate computers. The business also gave too much power to the fraudster, granting him access to all information on the network. There were close to zero checks on his activity. Indeed, it was only through an audit of new purchases that suspicions were raised. Mr Hilbert believes the company relied too much on technologies, such as firewalls and intrusion detection systems, to counter threats. "We think tech is going to capture everything for us," he adds. "But don't just rely on the technology... You can't throw a bunch of words at a computer and hope it writes a novel." Handpicked employees also need to be given oversight powers to watch the watchers, he urges. "Trust but verify is the key. Putting the keys to the kingdom in one person's hand is a bad idea," he adds. "You've got to put employees in the position where they are being watched and you don't want to put them in a tempting situation. If you put someone in that situation, they're liable to do something stupid."



- CYBER CRIME 62%
- HACKTIVISM 34%
- CYBER ESPIONAGE 3%
- CYBER WARFARE 1%

Source: hackmaggdon.com, December 2013

How can you keep your digital assets and IP safe from internal and external threats?



Determined hackers, malicious insiders and common errors make it inevitable that high-risk and high-value data will escape.

Protecting information assets requires a new mindset: knowing where important data is stored, understanding what it's worth – from its owners and to the bad guys – and making sure it's protected.

Find out how you can:

- Proactively minimise the opportunities for malicious or accidental breaches of important information
- Recover efficiently from breaches by first targeting the high-risk storage locations
- Quickly close information security gaps before they can be exploited again.

DOWNLOAD A COPY OF OUR WHITE PAPER, "THE GOOD SHEPHERD MODEL FOR CYBERSECURITY" AT NUIX.COM/CYBERSECURITY



Anti-Fraud Strategy

PLAN TO COUNTER FRAUD

Image: Getty



To fight fraud you need an official policy or programme. But what should go in it? Charles Orton-Jones has the answer

Too many firms think an anti-fraud policy is optional. It's not. Let Neill Blundell, head of fraud at law firm Eversheds, scare the life out of you. "Business must implement anti-corruption measures in order to be able to show a defence of 'adequate procedures' under section 7 of the Bribery Act 2010," he says.

"All businesses should be aware that David Green QC, who is the director of the Serious Fraud Office, is currently lobbying to have a section 7-type offence extended for any type of any fraud-related matter. This would mean that a company would need to have a fully implemented anti-fraud programme in order to avoid liability in circumstances where an employee or a third party commits frauds on its behalf. This would mean any type of fraud offence and not just bribery."

So what should this policy state? And how should it be implemented? After all, you don't want your wonderful document rotting in the bottom of a draw.

NO TEMPLATE

The tough news is that there's no template. You can't download one of these things. Bill Trueman, managing director of consultancy UK Fraud and co-founder of Association of Independent Risk and Fraud Advisors, says: "All businesses are different, as well as all business risks." As for the concept of a regular health check: "I am afraid I do not know what one of these is and I go into a lot of businesses, many of them high-street names, to help them with challenges and address issues."

You need a unique, personalised plan. Fortunately, there is a consensus on how this should be drafted. Hitesh Patel, head of forensic

fraud at KMPG, says the trick is to chop the problem into three. "Your policy needs a preventative part, to stop fraud happening to you; a detection part, so you notice when fraud has been committed; and a response strategy. There will be many sub-components, but those are the key three ingredients."


There are some pretty clever additional tools. Phil Beckett, managing director of corporate forensic firm Proven Legal Technologies, says: "You can analyse payments leaving an organisation looking for unusual transactions or patterns of transactions. These can include relatively straightforward

But that's not quite the end. You need an enforcement policy too. Your anti-fraud strategy needs to be implemented companywide. KMPG's Mr Patel says this starts in the boardroom. "You need a champion at board level. They should make statements to be distributed throughout the organisation," he says.

REGULAR TRAINING

Lessons in fraud may need to be annual, in the case of anti-bribery legislation, or more frequent. For technical stuff, shorter lessons are advisable. Sophos Anti-Virus's head of security James Lyne warns: "Box-check exercises get ignored." He suggests: "Regular bite-sized video training and regular live tests to ensure staff know how to behave." Pharmaceutical firm Astellas took three years of lessons to drive home anti-bribery legislation requirements.

A common defect in implementation is staff resistance. Either staff are afraid to air confusion with policy or worried about whistleblowing. Corporate knowledge sharing body CEB suggests creating a Speak Up channel, available 24/7, via a number of routes from e-mail and voice to intranet and in-person. Importantly: "The two most common reasons that employees fail to use the Speak Up route are fear of retaliation and a belief that no action will result from a report," according to CEB.

A strong anti-fraud policy won't mean you are totally secure. No one can guarantee that. But it can mean you are legally in the clear and can react to threats with the minimal damage, which ought to mean you sleep a little easier. 



Your policy needs a preventative part, a detection part and a response strategy

The prevention section starts by listing all the ways your firm could be compromised. For example, telecoms giant Telefonica explores the dangers of physical break-ins, of staff being duped, of digital penetration by hackers and shortcomings in the way it might hold sensitive data. The list includes a provision for "new" threats, which haven't yet emerged.

IT partners will routinely offer help identifying these threats and drafting responses. For example, if you take online payments, then partners such as SagePay and WorldPay provide advice on how fraudsters operate, and how they can be combated by simple methods such as IP address flagging.

Next, establish a strategy for detection. Fraudsters are incentivised to be as unobtrusive as possible. So how will you know you've been hit?

The obvious methods are stock checks and data security patrols.

tests, such as duplicate and round-sum analysis, as well as more complex measures using tests such as Benford's Law, standard deviation and regression analysis." Benford's Law states that the number one occurs 30 per cent of the time in financial data – it's a golden clue for fraud identification.

Santander Bank is experimenting with voice recognition software, provided by Fonetic, which hunts for patterns and key words in conversations. During the Libor scandal, the traders were using code words. Fonetic claims to be able to tally words with transactions to flag up these misdeeds.

Third your policy needs a list of responses. If you lose data what will you do? If your bank account is drained of cash, who will you call? A detailed response strategy will help you respond fast to catastrophes when they strike.

Commercial Feature

Staying ahead of the hackers

The internet has transformed the way we live and work – and nowhere is this more apparent than in financial services, says Fiserv



Mike Urban, portfolio director, financial crime risk management, Fiserv

People can now open accounts, manage their finances and make transactions online, without having to go anywhere near a high street branch. And in recent years, services have moved on to mobile platforms, while other technologies, such as contactless cards, are also changing the way we transact.

This has presented huge opportunities for financial institutions – no longer restricted to geographic regions, countries or local areas – which now have the ability to expand their customer base and grow revenue across the globe.

THREATS AND VULNERABILITIES

But with the internet and other new channels have come fresh opportunities for fraudsters and criminal gangs, who are also able to take advantage of the inherent vulnerabilities of the digital landscape. “They can work together and create affiliations with each other in order to execute different types of crime over the internet, rather than having to physically walk into a branch and hold it up,” says Mike Urban, portfolio director, financial crime risk management, at financial technology firm Fiserv.

Much of the fraud committed comes from data that is openly available over the internet, such as social

media, or which can be accessed through malware or online scams affecting customers. Financial institutions need to ensure they are in a position to identify suspicious trends and prevent incidents from escalating when they do occur.

“Preventing financial crime becomes much more important as your customer base expands in different geographic locations where you might not have a footprint,” says Mr Urban. “Transmitting that information into a system that can continue to track and monitor developments, and identify when particular behaviour is starting to go sideways then becomes mandatory.”

“You need to be able to react to these threats in an automated fashion, rather than relying on a human being to look at it first, slowing the process down even further, especially as criminals are getting quicker all the time.”

PATCHY PICTURE

Many financial institutions have a patchy approach to the threat of fraud. “They have different areas that are focused on particular things,” Mr Urban explains. “Most institutions have a good card fraud programme in place, but that’s just focused on cards. The bigger you are, the harder it becomes to tie everything together. Some institutions may have multiple applications for the same process, depending on acquisitions or where the function is in the organisation.”

Legacy systems are also an issue, he says, with institutions still having to rely on pulling data out of these while needing the flexibility to accommodate other packages as other investments or acquisitions are made.

The solution, says Mr Urban, is a security platform which allows financial institutions to easily integrate legacy systems with the ability to

adapt as new products – and threats – are introduced.

“It needs to be something that can be tailored to unique situations and then changed as required,” he says. “In the long run, it’s more effective because you have a platform where you can easily add new or changing types of crime scenarios, and adjust it as the criminals and the regulations change. Being able to tie all that information together also helps you make a better risk decision. We call it defence in depth.”

CRIMINAL MINDSET

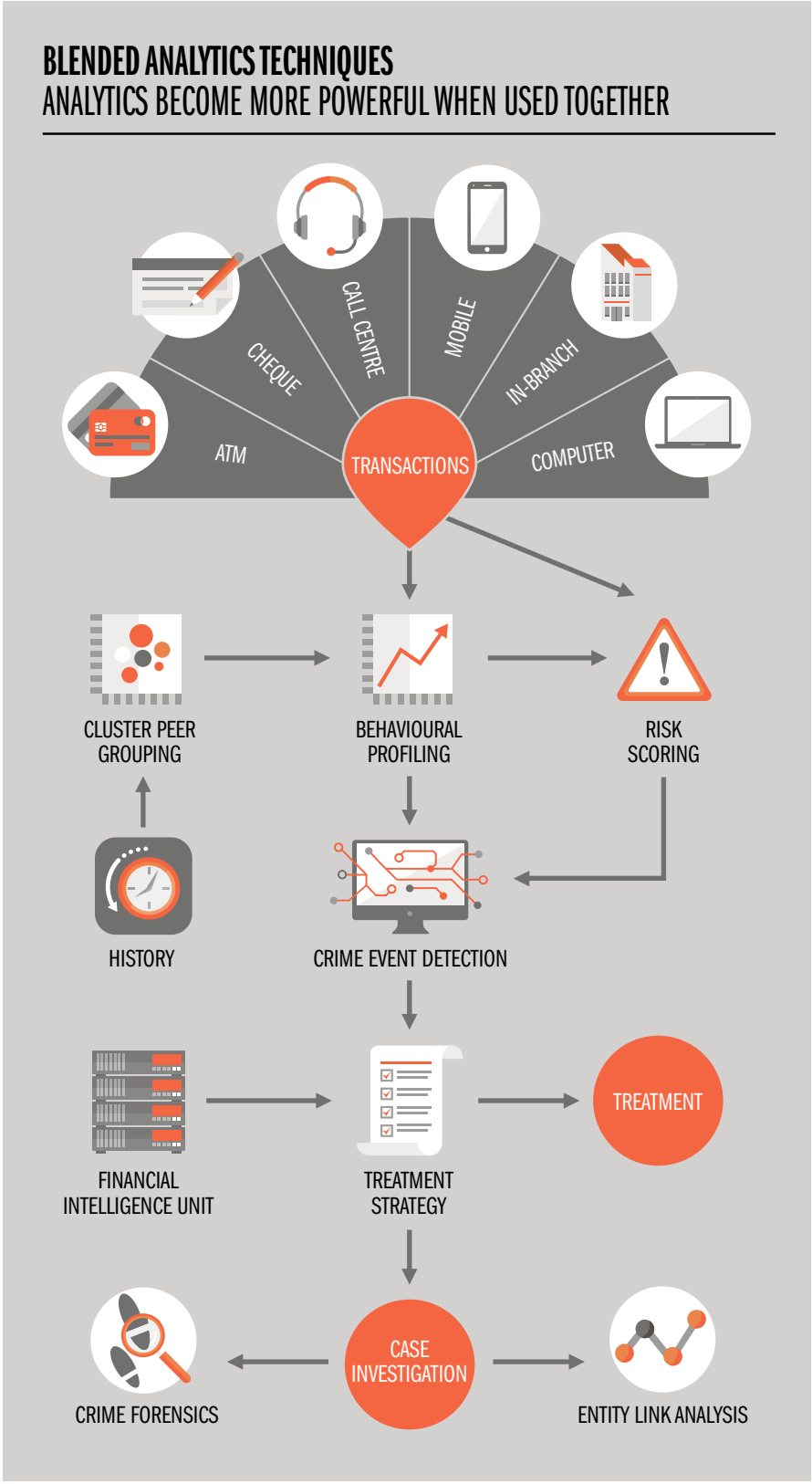
Cases of fraud are only likely to get more aggressive and sophisticated in the future, meaning financial institutions have to start thinking along the same lines as the criminals themselves. “You have to put yourself in the mind of the criminal, during your risk assessments, to identify where they could get in,” says Mr Urban. “You have to be able to react as quickly as they can, even though they don’t have legacy systems and can whip up a piece of malware in a very short time.”

Recent high-profile cases, such as those involving US retailer data breaches, where the credit and debit card details of millions of customers were accessed by hackers, have contributed to a growing awareness of online crime in the public mindset. Mr Urban believes those institutions which can put in place a proven security platform can turn what has up to now been a concern into a strength.

“Everyone is aware of fraud in a way that maybe they weren’t five or ten years ago,” he says. “Often customers who are impacted by fraud will actually leave the institution and go elsewhere. Those who can deliver a better customer experience will minimise the risk of losing revenue and damaging the bottom line.”

The financial crime platform offered by Fiserv is used by more than 1,000 clients in over 70 countries around the world and can empower clients to add or change detection scenarios in response to emerging threats.

For more information visit www.financialcrimerisk.fiserv.com



With the internet and other new channels have come fresh opportunities for fraudsters and criminal gangs

Financial Services Fraud

FRAUDSTERS TARGET FINANCIAL SERVICES

Most fraud is committed within the financial services sector, causing significant loss of revenues, reputation and customer confidence, writes **Chris Johnston**

Scan the pages of almost any newspaper personal finance section or website and readers will find tales of woe and misery from the victims of financial fraudsters. These stories relate how scams, such as phishing, vishing and others, are used on a daily basis to transfer five-figure sums into accounts controlled by fraudsters, and despite attempts to crack down on such practices, they keep on occurring.

The Office for National Statistics has estimated there are as many as 3.8 million incidents of bank and credit card fraud annually in Britain, while Financial Fraud Action (FFA) says losses on UK cards rose by 16 per cent to £450 million in 2013.

FFA spokesman Craig Jones says that following the introduction of chip and PIN for credit and debit cards and other improvements in security, criminals are resorting to variations of deception crimes to trick people into disclosing their financial details. "Vishing for example – where fraudsters ring members of the public and ask them for personal details while pretending to be from their bank or the police – has become an increasing problem," he says.

Even financial professionals can fall victim to such scams, as Charterhouse accountants of Harrow, north-west London, found earlier this year when it was defrauded of more than £80,000. Because staff were tricked into divulging security information over the phone, Nat-West has refused to compensate the firm, which employs 28 people.

The resulting animosity in situations such as these means financial fraud is an ever-growing problem both for financial institutions as well as their customers. Nic Carrington, a partner in Deloitte's forensic and dispute services division, says the scale of financial fraud has increased considerably in recent years. "People just keep on trying to find holes and, if they're lucky, they only need a few successes to achieve

very good returns. It's a big issue for banks," he says.

As well as trying to combat "external" fraud, which can also extend to sophisticated cyber attacks launched by criminals based abroad, financial institutions must remain hyper-vigilant to scams committed either by their own staff or with their co-operation.

People just keep on trying to find holes and, if they're lucky, they only need a few successes to achieve very good returns

Since the financial crisis struck, banks and other financial companies have been forced by regulators to keep a much closer eye on their inner workings in a bid to combat rogue traders, such as Jérôme Kerviel, whose unauthorised trades cost Société Générale almost €5 billion in 2008 and threatened its very survival.

RISK AND COMPLIANCE

Some big banks now have as many as 10 per cent of their staff in risk and compliance roles, which is a significant shift given that these employees are not direct sources of profit. "The regulatory agenda now is such that there is a real obligation on the institutions to report to the authorities... there's an acceptance that the culture of financial services has somewhat changed – things have just moved on," according to Mr Carrington.

One consequence of this shift has been a move by financial institutions to analyse data in a predictive way to help identify unusual patterns of transactions or behaviour by staff. Rather than relying on "red flags", there has been a move towards more sophisticated forms of analysis to reveal suspi-

TACKLING CARD FRAUD

Overseas fraud using UK cards, 2010-13

UK-ISSUED CARDS OR CARD DETAILS USED FRAUDULENTLY OVERSEAS

■ 2010
■ 2011
■ 2012
■ 2013

CANADA

4%

US

22%

BRAZIL

6%

LUXEMBOURG

4% 7% 10%

IRELAND

3% 5% 9%

FRANCE

5% 8% 9%

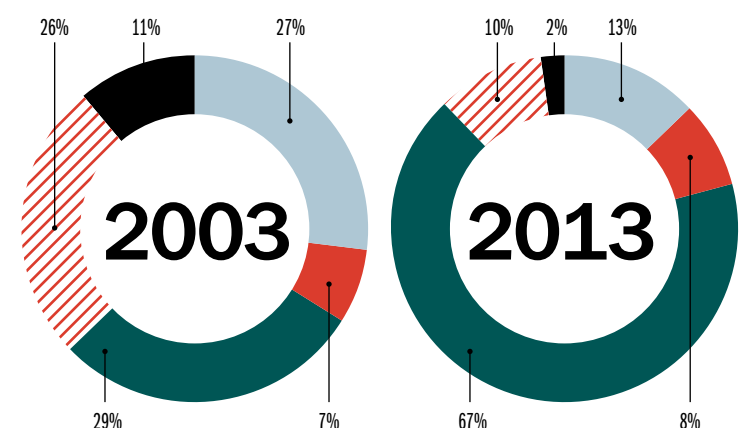
SOUTH AFRICA

5%

Card fraud losses by type

(AS PERCENTAGE OF TOTAL LOSSES)

■ LOST/STOLEN CARD
■ CARD ID THEFT
■ REMOTE PURCHASE
■ COUNTERFEIT CARD
■ MAIL NON-RECEIPT



cious activity. However, seeking to analyse the sheer volume of transactions in financial services remains one of the difficulties in trying to identify rogue employees or suspicious actions.

When fraud is exposed, financial institutions often use firms such as BDO to reveal exactly what took place and why controls failed. Richard Shave, head of financial services

investigations at BDO, says his firm has been called on to examine a number of cases involving collusion by bank employees with external solicitors and valuers to make fraudulent property loans.

He says it is impossible to know how many instances of fraud, either internal or external, are not being detected, but the increased regulatory scrutiny means that fewer

are now likely to slip through the net. "The level of data mining that the banks are doing now will have contributed to the increased levels of detection of fraud in financial services," says Mr Shave. "Banks are throwing a lot of money at their compliance teams."

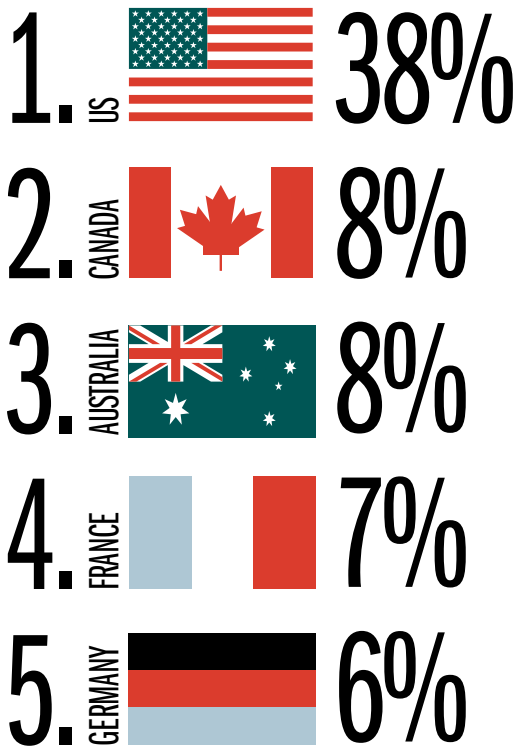
Money laundering is another issue confronting financial institutions given that several have been

Opinion

Source: Financial Fraud Action 2014

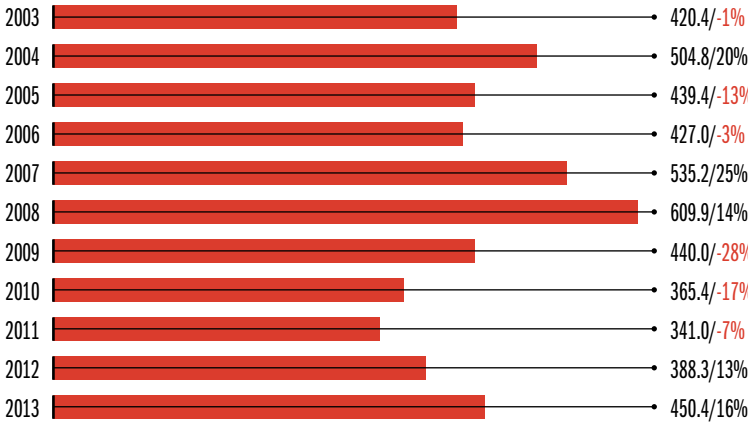
Fraud in the UK using foreign cards, 2013

LOSSES ARE SHOWN AS A PERCENTAGE OF TOTAL FRAUD AT UK MERCHANTS ON FOREIGN-ISSUED CARDS




Fraud losses on UK-issued cards, 2003-13

(GROSS IN US\$ MILLIONS/
% CHANGE FROM PREVIOUS YEAR)



heavily penalised by regulators on both sides of the Atlantic in recent years. HSBC was fined a record \$1.9 billion (£1.2 billion) by US regulators in December 2012 for allowing Mexican drug barons, among others, to use its accounts to launder funds. The bank subsequently spent almost \$300 million upgrading its systems to prevent such failures in the future.

How institutions react in the first few hours after a fraud has been exposed can be critical in terms of tracking down the culprits, he believes, and some have better procedures in place than others for dealing with the aftermath. Risk assessment is a key part of the fraud reduction process, but in Mr Carrington's view not every institution is taking sufficient steps to


identify where the potential vulnerabilities lie in their systems. "If you don't know what's possible, then you don't necessarily put in the controls to cover it – there is more that could be done," he says. 


KEEP YOUR MONEY SAFE



It is not only the banks job to fight fraud, it's yours too, says **Chris Skinner**, chairman of the Financial Services Club

UK banks and card companies work on a basic model of acceptable risk when it comes to bank account fraud. That was the reason for the introduction of chip and PIN, a scheme that cost UK retailers. A decade ago, when this scheme was introduced, card fraud was anticipated to double within five years as the use of a magnetic stripe payment with a signature was massively insecure.

no longer need to enter a Verified by Visa or MasterCard SecureCode when making an online purchase if you are using your usual computer at home. That is because the card firms recognise it is your normal internet location and device that is making the purchase, so they assume you are secure with this. Nevertheless, we are starting to see some changes, especially when passwords are being regularly compromised. It was only a few months ago that everyone was told to change their passwords when the Heartbleed bug was discovered. Similarly, large and trusted websites and web services, such as eBay and Adobe, have had password files stolen in the last year, causing many of us to start using multiple, instantly forgettable passwords. That has to change and it is. If you use the latest iPhone or Samsung Galaxy smartphone, both will take fingerprints for authentication of transactions. If you are a Barclays Bank customer, you can authorise actions securely just using your voice on the phone, as they have rolled out voice biometric authentication this year. These and other developments will continue as banks are always trying to be one step ahead of the criminals when it comes to fraud and, based upon the last ten years of statistics, they're not doing a bad job of it. It is a shame that most customers are not, as almost half use the same password for all their logins, especially among younger demographics, with the most common passwords being princess, password and 123456. Therefore, if you are one of the people with these passwords, do everyone a favour and start protecting yourself online a little bit too. 

 With all the concerns about identity theft, card fraud, online scams and more, we are kept pretty safe by our financial system

The impact of chip and PIN was significant and best illustrated by the fact that the rate of fraud today is less than it was ten years ago, even with the rise of the mobile, social internet. Fraud losses on UK cards totalled £450.4 million in 2013 compared with £411 million in 2003. The 2013 figure is deceptive, as it represents a 16 per cent rise on the 2012 total of £388.3 million, a lower figure than a decade before. That seems pretty incredible when the number of cards issued has increased dramatically from 42 million cardholders in 2013 to 47 million now, as has spending. Card spending today is more than £530 billion annually. In other words, with all the concerns about identity theft, card fraud, online scams and more, we are kept pretty safe by our financial system. You have probably noticed that alongside chip and PIN and secure keys for online services, you have other checks and balances on your account that is changing over time. A good example is that you



Whistleblowers

CALLING TIME ON DIRTY DEEDS

Stories of whistleblowing can be like espionage thrillers, shining light into dark corners of the corporate world where the stakes are high, writes **Edwin Smith**

For a practice that has historically been associated with confidentiality clauses and shadowy backroom deals, whistleblowing has enjoyed an unusual amount of publicity of late. Much of this, of course, is because of the sensational case of the American government security contractor turned whistleblower Edward Snowden. But the corporate world has seen the issue thrust under the spotlight too.

In the UK, the Financial Conduct Authority (FCA) has made an effort to set out its stall since superseding the Financial Services Authority in April 2013. Data released earlier this year showed that the average number of whistleblowing reports received by the FCA was 38 per cent higher than its predecessor. It had also opened 50 per cent more investigations.

and exemplary corporate governance, the powers that be have been eager to show they are paying attention to insider reports of fraud and other malfeasance.

This has been most clearly illustrated by the recent case of an anonymous whistleblower at the Chinese arm of the British pharmaceutical giant GlaxoSmithKline (GSK). What's more, the story has a plot that would be at home in the pages of an airport thriller.

The chain of events began in January 2013 with an e-mail to GSK's London-based chief executive Andrew Witty from an anonymous source, who had knowledge of the company's Chinese operation. The e-mail alleged that the firm's standard marketing practices in the region "constitute bribery in the vast majority of cases", and

GSK later revealed it had investigated the claims using external legal and audit expertise, and that some fraudulent behaviour had been identified. This, the company said, "resulted in employee dismissals and further changes to our monitoring procedures in China". But GSK also said the investigation "did not find evidence to substantiate the specific allegations made in the e-mails".

SEX AND BRIBERY CLAIMS

However, perhaps the most extraordinary thing about the incident was that, along with the allegations of bribery and other wrongdoing, the whistleblower's e-mail included a sex tape – a video of GSK China chief Mark Reilly and his longterm Chinese girlfriend that was filmed in his apartment, which Mr Reilly says, was recorded without his knowledge.

In response, the company tasked investigator Peter Humphry with uncovering the identity of the whistleblower. But Mr Humphry and his American wife were later charged by a Chinese court for illegally buying information relating to their work. In August this year, the pair were sentenced to a combined total of four-and-a-half years in prison and fines of £35,000.

In another twist, Mr Humphry went on to reveal, in a statement released from prison before his trial, that when he offered to investigate the bribery allegations in addition to establishing the source of

GlaxoSmithKline in China was at the centre of bribery charges after a whistleblower went public

tape, GSK instructed him that the claims in question had been shown to be false.

However, when he finally saw the whistleblower's original e-mail, just weeks before his own arrest, he described the allegations it contained as "totally credible".

In an e-mail to colleagues he wrote: "I can only assume that they didn't give them to us because they were afraid we would find the allegations credible and start verifying them... Actually I do believe every word of these allegations. They are totally credible."

GSK, for its part, said that while wrongdoing by its employees in China had been uncovered, the perpetrators had not been acting on instructions from the company.

Four highranking GSK executives were detained by Chinese police in connection with the case and, according to reports, Mr Reilly was also "effectively detained" as the ruling Communist Party continued an anticorruption campaign under the leadership of Xi Jinping. It was

announced in May that GSK would also be investigated by the Serious Fraud Office in the UK.

INCREASED AWARENESS

Michael Ruck, a financial services litigation specialist at law firm Pinsent Masons and former FCA lawyer, says the case is symptomatic of a wider trend. "There are clearly issues that GSK will now be addressing," he says. "But, more widely, there has been an increased awareness of bribery, corruption, money laundering and policies to counter these practices. I've noticed it particularly in the last six months or so."

Mr Ruck adds that changing international attitudes to bribery and fraud may force certain companies to rethink the way that they do business. "Historically the risk of being caught out and having sanctions implemented would have been fairly small. So, on a commercial basis, firms may have taken one decision in the past. But now we're at a point where the risks are much greater. I'm



Lots of employers take this very seriously, but certain organisations and certain industries rely on conducting business in a certain way

Meanwhile, in the United States, where whistleblowers are eligible for financial incentives, the Securities Exchange Commission recently made its highest-ever award to a whistleblower, of \$14 million. Even in China, a country, fairly or not, seldom associated with transparency

detailed the way in which illegal payments were allegedly made to doctors and other officials in a bid to push the company's products. It named specific doctors and hospitals, and quoted senior executives at the company and their private e-mail accounts.



FRAUD: NOT A SINGLE RISK, AN ECOSYSTEM

We help you look at the bigger picture, in a global context, applying our expert knowledge of crime and fraud to help you to mitigate the threats to your business.

For further details on Marsh's commercial crime insurance product, please contact:

Dean White

+44 (0)20 7357 2205
dean.white@marsh.com

Alexandra Chittock

+44 (0)20 7357 2291
alexandra.chittock@marsh.com

Marsh Ltd is authorised and regulated by the Financial Conduct Authority.
Copyright © 2014 Marsh Ltd All rights reserved.



Commercial Feature

Technology must keep up with third-party risk

In a world of growing regulation, companies need to move from manual to automated risk management processes, says **Daniel Kline**, managing director, Europe, Middle East and Africa, for ethics and compliance solutions provider NAVEX Global



Image: Getty

not sure the same commercial decision would still stand. Particularly overseas, [sanctions] will be used as a political tool as well," he says.

Professor David Lewis, convener of the International Whistleblowing Research Network, points out that, while the majority of corporates have a whistleblowing procedure in place, this doesn't guarantee that best practice will be followed or that disclosures from concerned employees are always treated with the gravity they merit. Professor Lewis says: "Lots of employers take this very seriously, but certain organisations and certain industries rely on conducting business in a certain way. If they get caught out on occasion, and have to pay off a whistleblower or pay a fine, it's viewed as a cost to the business."

BIG FINES, BIGGER PROFITS

He adds that even apparently big fines, in the tens of millions, need to be seen in the context of the profits of the multinationals that pay them, which often run into the tens of billions of dollars.

Public scepticism regarding company procedures should be tempered by the realisation that only a certain type of case tends to hit the headlines. "Of course, the media highlights cases where whistleblowers get crucified or go to tribunals. What the media doesn't bring out is successful whistleblowing [that remains internal and confidential within a company] because that's not a story. It's not in anyone's interest to demonstrate when it has worked," says Professor Lewis.

If they are not commonplace, highprofile cases involving multinationals do raise important issues.

In 2011, Michael Woodford, the new British chief executive of Japanese camera manufacturer Olympus, resigned just two months into his role amid worries over \$1 billion of improper payments made by the business to conceal its losses. Eventually the entire board resigned and Mr Woodford received a £10-million settlement, but not before his concerns had fallen on deaf ears within the company and he had fled to London for fear that his life was at risk.

When internal investigations arise from whistleblowing, they must almost always be carried out by the companies themselves or agencies in their employ. So it's not difficult to imagine how the dynamic could result in conflicts of interest. However, Professor Lewis warns that any truly independent ombudsman would have to be funded somehow and the question of when an ombudsman would be brought into action would be difficult to resolve. "It's a thorny problem," he says.

But the publicity surrounding prominent corporate cases such as these may prove to have positive consequences for businesses – if only as cautionary tales.

When it comes to dealing with whistleblowing within a business, Professor Lewis says: "The short answer is to take it seriously. Whistleblowers tend not to be crackpots these days," he says. So if an individual is serious and not acting out of malice, it may well be advisable for the employer to deal with the problem before it escalates.

"Because of the price to be paid," Professor Lewis adds, "commercial organisations know that it's in their own interest to get their act together." ■

Third-party risk management has never been as top-of-mind with business leaders around the world as it is today.

A barrage of negative headlines about well-known organisations dealing with third-party-related violations, along with legislation such as the US Foreign Corrupt Practices Act and the UK Bribery Act, tighter regulations, stricter enforcement and more severe sanctions are helping catapult this issue to the top of the must-address list for C-suites, boards and compliance professionals alike.



Time and resource constraints mean many risk management programmes cannot perform continuous monitoring manually

In addition to pressure brought on by increasingly stringent legislation and regulations, and the penalties they can bring, consumers and employees are demanding greater transparency and more rigorous corporate social responsibility.

According to research by the European Commission, 56 per cent of the public believe corruption has increased in recent years. *The Dow Jones State of Anti-Corruption Compliance Survey* of compliance professionals from more than 350 companies worldwide found that 71 per cent had stopped or delayed working with a business partner because of concerns about anti-corruption regulations.

WHY IS THE THIRD-PARTY RISK MANAGEMENT PROCESS SO DIFFICULT TO MANAGE?

Compliance professionals managing third-party risk are faced with greater challenges than ever before. Baseline screening and enhanced due diligence for all of an organisation's third parties, including product sourcing, contracted services and outsourced process providers, has become the "new normal".

For many organisations this spike in workload and the complexity of the information needed to stay within the bounds of the law means that manual processes are already, or soon will be, no longer viable. Time and resource constraints mean many risk management programmes cannot perform continuous monitoring manually – and therefore the results of risk assessments are both incomplete and quickly outdated.

AUTOMATION IS CRUCIAL FOR EFFECTIVE THIRD-PARTY RISK MANAGEMENT

A growing number of companies from all sectors are realising that third-party risk management software transforms the risk management function from an archaic, ineffective process to a centralised, predictive and exponentially more effective and efficient function.

Automated approaches allow organisations to right-size their resources, taking a limited approach for low-

risk business partners and applying more resources to those with the highest risk levels, while continuously monitoring all third parties for changes in risk exposure.

Technology-enabled approaches also help ensure customisable, defined risk-mitigation policies. This streamlines and standardises the risk mitigation actions that need to happen among internal staff and third parties around the world, even across business units and geographies, to address any red flags effectively.

CONFIDENTLY MANAGING THIRD-PARTY RISK BRINGS GREATER PEACE OF MIND

With an automated third-party risk platform, such as the one offered by NAVEX Global, leaders of organisations can gain peace of mind knowing their global due diligence programmes are comprehensive and scalable. The platform also creates a permanent audit trail to prove compliance to boards of directors, auditors, regulators and shareholders. In addition, housing all third-party identity, discovery and due diligence information in one online repository enables greater consistency, and dramatically drives down overall costs.

The increasing complexity of third-party risk management is growing. However, those organisations that make an investment in ensuring they are familiar with the latest regulations and have a system in place to manage risk can be confident they are compliant, protected and better able to grow – and prosper in today's global economy.

For more information please visit
www.navexglobal.com

NAVEX GLOBAL™
The Ethics and Compliance Experts

71%

of 350 companies surveyed had stopped or delayed working with a business partner because of concerns about anti-corruption regulations

Third-Party Risk



NO BRIBES PLEASE, WE'RE BRITISH

Image: Getty

When a company expands into new territories, especially emerging markets, bribery and corruption is a significant risk of doing business through local third-party representatives, as **James Dean** reports

It was heralded as the new law that would put Britain at the forefront of the fight against corporate corruption. “Bribery blights lives,” Kenneth Clarke, then Justice Secretary, said shortly before the new Bribery Act came into force on July 1, 2011. “At stake is the principle of free and fair competition, which stands diminished by each bribe offered or accepted.”

E-Commerce Fraud
Page 14


Nonetheless, more than three years on, not a single company has been prosecuted under the new law. Despite this, David Green, the director of the Serious Fraud Office (SFO), has disclosed that his agency is investigating a number of alleged bribery offences which, if they come to fruition, will be prosecuted under the new law. “Watch this space,” he said. “We have cases under development.”

Companies found guilty of a Bribery Act offence can be hit with staggering fines and might be blocked

from tendering for public contracts. The loss of revenue and damage to a company’s reputation could also help to put it out of business.

Two elements of the new law are particularly important for companies. The act creates the corporate offence of bribing a foreign public official in order to obtain or retain business. It also creates an offence of failing to prevent bribery. These offences cover any company that is deemed to be doing business in the UK.

ADEQUATE CONTROLS

One of the most significant elements of the offence of failing to prevent bribery is that the company does not need to know that a bribe has been paid by one of its employees or agents. The company can fall foul of the legislation simply by failing to have “adequate controls” in place to prevent bribery. As a result, companies have been forced to put in place controls to prevent bribery by any individual that represents them, including “fixers” and other third-party agents, wherever they are in the world.

Satindar Dogra, a partner at law firm Linklaters, says companies have had to be particu-

311

companies and individuals sanctioned since 1999 under the Organisation for Economic Co-operation and Development's Anti-Bribery Convention

Source: OECD

€1.24bn

record sanction against a company for foreign bribery

Source: OECD

\$1trn

paid in bribes globally each year

Source: World Bank

larly cautious when they use the services of third-party agents in emerging markets and other high-risk jurisdictions.

“Companies seek to manage their risks by ensuring that appropriate vetting and due diligence has been carried out on such agents; that agents receive anti-bribery training or have their own developed code of conduct; and that there are appropriate anti-bribery warranties and termination rights in the contractual documents,” he says. “Where due diligence raises red flags, a satisfactory explanation of the red flags is required, failing which a company would be ill-advised to proceed with the agent in question.”

What makes “adequate” anti-bribery controls is a moot point, says lawyer Dan Hyde, a partner at HowardKennedyFsi. Adequacy is highly subjective and is not defined in the Bribery Act, although the government has published guidance on the matter.

“Adequate procedures would certainly involve having a bespoke anti-bribery policy that was effectively disseminated and actively implemented,” Mr Hyde says. Staff must be readily primed to notify management when red flags arise, he advises.

Mr Hyde recommends that companies need to examine their relationships with third-party agents overseas “to ensure, as far as possible, they are choosing the right third-party representative and that the risk is not too great”. This due diligence would include assessing the level of corruption in a country, in the agent and in the home government. There should also be “myriad” checks on the reputation and reliability of the agent, and the transaction they are being asked to complete. “Some jurisdictions and sectors may be viewed as posing too great a risk,” he says.

Problems with third-party agents abroad can be amplified if a company does business in the United States and is therefore subject to the punitive provisions of the Foreign Corrupt Practices Act (FCPA). According to Mondaq, the online information service, FCPA investigations and prosecutions resolved last year involved alleged corrupt conduct on every continent except Australia and Antarctica. A large number of the actions involved the oil and gas industries, but enforcement actions also targeted the financial services, technology and medical sectors.

GlaxoSmithKline, the British pharmaceutical company, is currently under investigation by both the SFO and the US Department of Justice over allegations of bribery in China. Last year Chinese police accused GSK of channelling as much as ¥3 billion (£280 million) in bribes to encourage doctors to use its products. Similar allegations later surfaced regarding GSK’s sales practices in Poland, Iraq, Lebanon and Jordan. The SFO opened a criminal inquiry into GSK’s sales practices in May this year after the US Justice Department launched its own probe.



Some jurisdictions and sectors may be viewed as posing too great a risk

GSK says it is “committed to operating its business to the highest ethical standards” and will continue to co-operate fully with the SFO while the agency carries out its investigation. GSK says it has overhauled its operations in China and has unveiled a global policy to stop paying doctors in the manner alleged.

However, if the SFO’s investigation into GSK was to lead to a prosecution, the drugmaker could be the first company to be prosecuted under the Bribery Act. ■



Commercial Feature

Security analytics for cyber-fraud prevention

Businesses owe it to their customers to have the technical solutions to combat cyber attackers, says **Darren Anstee**, director of solutions architects at Arbor Networks



Almost every day, the news contains reports of businesses being compromised by cyber threats. Often, when intellectual property or customer information is stolen during an attack, this data can be used to carry out, or assist in, fraudulent activities.

When this occurs, customers can accuse organisations of inadequate preparation and lack of care, and there can be significant cost and reputational impact. When it comes to dealing with cyber incidents – whether an intentional or unintentional breach – it is important to be as prepared as possible. But is this actually the case in businesses today?

Research conducted by the Economist Intelligence Unit and sponsored by Arbor Networks has shown that nearly three quarters of companies don't feel fully prepared should a cyber incident take place. The two top areas of concern are an organisation's ability to predict the business impact of an incident accurately and their ability actually to detect an incident within 24 hours of it occurring.

The same research also shows that organisations are experiencing more cyber-security incidents now than in previous years and board-level executives are beginning to understand both the consequences of a successful breach and the increasing likelihood that this will occur. Security, risk and compliance should now be a concern for everyone within an organisation, from board level down.

So, how are businesses falling victim to cyber attacks? Well, when it comes to security, there are two types of organisation: those that have already been targeted and those that will be targeted. In the past, some organisations have simply assumed that the worst will

not happen to them and just under two thirds of organisations actually have an incident handling plan or team in place. This does appear to be on the rise though, which is encouraging.

Putting plans and training in place is hugely important to an organisation's ability to respond. People and processes have a significant part to play; educating employees on the types of threats that are out there and how to spot them can be extremely helpful. Regularly exercising incident handling plans and teams is also crucial, but multiple research reports have found this is often something that is overlooked.

One key question that many ask is how do attackers actually get through the defences organisations have in place: are businesses simply not taking this seriously enough? The issue here is that securing a modern network and service architecture is not simple. We all take for granted our laptops, palmtops, extranet access to business partners, cloud services, home-working and so on, but all these things make it much more difficult to fully control data and security within an organisation. And that is before you even start to consider the complexity and sophistication of the tools and techniques now available to hackers.



and the whole area of prevention versus detection has become a hot topic within the security industry.

Organisations are now starting to look at how they can be quicker in detecting threats that have made it inside their networks and through their defences – as this is something we should now expect. Traditional security architectures tend to involve layered solutions at the organisation perimeter; once a threat has made it through this perimeter many organisations have very limited threat detection capabilities. Security strategies are changing though and experience is driving organisations to focus more on being able to detect and analyse threats that are already inside their networks much more quickly.

One issue here is that the skills to analyse threats can also be in short supply in many organisations and lev-

Analytics solutions are becoming an increasingly important tool for incident-handling teams. These solutions allow visibility into network traffic and user activities spanning days, weeks and even months, and the best of these solutions allow the user to navigate through all this information in real time. These solutions can drastically speed up both the identification of a problem, its investigation and the resolution, minimising the impact to a business and reducing the risk that attackers will make off with customer data or business intellectual property.

Cyber attacks are now a threat for all organisation types and being prepared is key. Having the appropriate technical solutions, which make the most of available resources, is important, but so is training and process implementation. Looking again at the research conducted by the Economist Intelligence Unit, and sponsored by Arbor Networks, two thirds of surveyed organisations felt that being able to respond well to a security incident could actually enhance their business reputation – more than that though, being able to respond well is something businesses owe to their customers.



Analytics solutions are becoming an increasingly important tool for incident-handling teams

People are a key weak point, with mediocre passwords, phishing and watering hole-style attacks continuing to be successful in giving attackers a foothold within businesses. Once an attacker is inside they can often remain there undetected for a lengthy period. Organisations have traditionally focused their security on preventing threats from entering their networks

eraging specialist services to augment internal resources is becoming increasingly common. Solution vendors are aware of this skills shortfall and have made tools available that are more graphical in nature, fewer screens full of columns, rows and so on, making it easier for specialists to spot trends as well as unusual or suspicious activities over longer time frames.

For more information please visit
www.arbornetworks.com

ARBOR
NETWORKS

Expenses Fraud:

It's more common than you think



Photo: birdpavilions.com

According to research conducted by YouGov on behalf of Concur, expenses fraud is more common than you might think.

- 20% of UK employees feel it would be 'easy' to use the expenses process to 'claim money for their own benefit'
- Only 30% of expense processors are able to take the time to check the legitimacy of every receipt
- Less than 1% of employee claims are ever rejected or queried by a manager

Expenses fraud is an unfortunate reality for businesses of all sizes in the UK. Sometimes it's just a case of an employee not understanding the company's policy, but some erroneous claims are done more deliberately. And with controllers admitting to not being able to enforce policy across the board, it's an issue that hits the heart of most companies' finances.

Ask yourself: can you say "yes" to these three questions?

- Does your company have a documented and understandable expenses policy?
- Do employees and their managers know which claims fall out-of-policy, and are managers able to return claims confidently?
- Do you know how to spot the warning signs of a fraudulent expense claim?

If you're not sure you can say "yes" to all the questions above, find out how you could by visiting www.concur.co.uk or contacting us on **01753 501 444**.

We've helped more than 20,000 businesses of all sizes gain better control and visibility of their expenses process, including more than 30% of the FTSE 100 companies.

About Concur

Concur® is a leading provider of integrated travel and expense management solutions. Our web-based and mobile solutions help companies and their employees control costs and save time. Our open platform enables the entire travel and expense ecosystem of customers, suppliers, and developers to access and extend the Concur T&E cloud. Concur systems adapt to individual employee preferences and scale to meet the needs of companies from small to large. Learn more at www.concur.co.uk or on the concur.co.uk/blog.



FIGHTING FRAUD
24/09/14
EDITION #0276

📞 RACONTEUR.NET
📧 /COMPANY/RACONTEUR-MEDIA
📱 /RACONTEUR.NET
📧 @RACONTEUR

E-Commerce Fraud

COMBATTING CYBER CROOKS

Smartphones and social networking sites have created new opportunities for cyber criminals, but how can companies mitigate the threat to e-commerce without alienating consumers with restricting security. **Stephen Armstrong** investigates



Are cyber criminals winning the online security arms race? A recent study from computer security software company McAfee and the Centre for Strategic and International Studies suggests they might be.

Estimates of global losses due to online crime were worth \$445 billion for 2013 – on par with the trade in illegal drugs. Given that cyber crime is indoors work with no heavy lifting and you can scope a shop with a laptop rather than a 20 strong gang, its popularity is unlikely to wane any time soon.

"Cyber criminals are innovating faster than most of us," warns security expert Keren Elezari from Gigaom Research. "They are extremely organised and surprisingly sophisticated. They're even crowdfunding their malware development."

She describes one smart trick that appears to be a message from Facebook warning of unlawful attempts to access someone's Facebook account and urging that person to download a security app to their phone, which in reality allows gangs to steal bank PIN codes.

For online retailers, this can seem terrifying. On the one hand, fraud threats loom. If bank and credit card fraud were included in the annual *Crime Survey for England and Wales*, the estimated number of crimes would jump by 50 per cent,

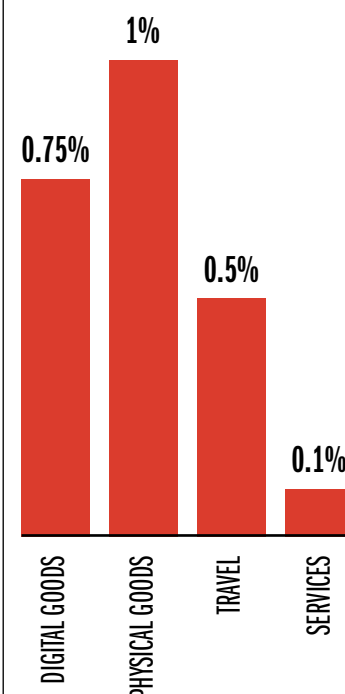
taking the total from 7.3 million to 11 million offences a year. On the other hand, customer checkout abandonment rates currently hover at roughly 33 per cent, according to research from the UK's online retail association IMRG. The last thing any site needs is another barrier to a successful customer experience.

"Visa had fraud rates of 1 per cent when they created the complex Verified by Visa password system, which ruined the shopping experience for the honest 99 per cent," says Sebastian Siemiatkowski from mobile payments platform Klarna. "Nobody outside the payments industry cares about the problems of the payments industry. They just want to click 'buy'."

Mr Siemiatkowski says that, in the vast majority of cases, Klarna can assess a customer's risk using their e-mail address or postcode instead of a long sign-in process. And risk management is a burgeoning industry. In Canada, for example, a company called SecureKey links online banking with government identity services. The digital charge card Affirm, launched by PayPal co-founder Max Levchin, offers a "digital tab", authenticating consumers with Facebook and other social and data signals to assess risk.

"I think we'll move to a point in the future where information needs to be encrypted in transit and encrypted at

Average % of orders later resulting in fraud



Source: CyberSource, 2013 UK eCommerce Report

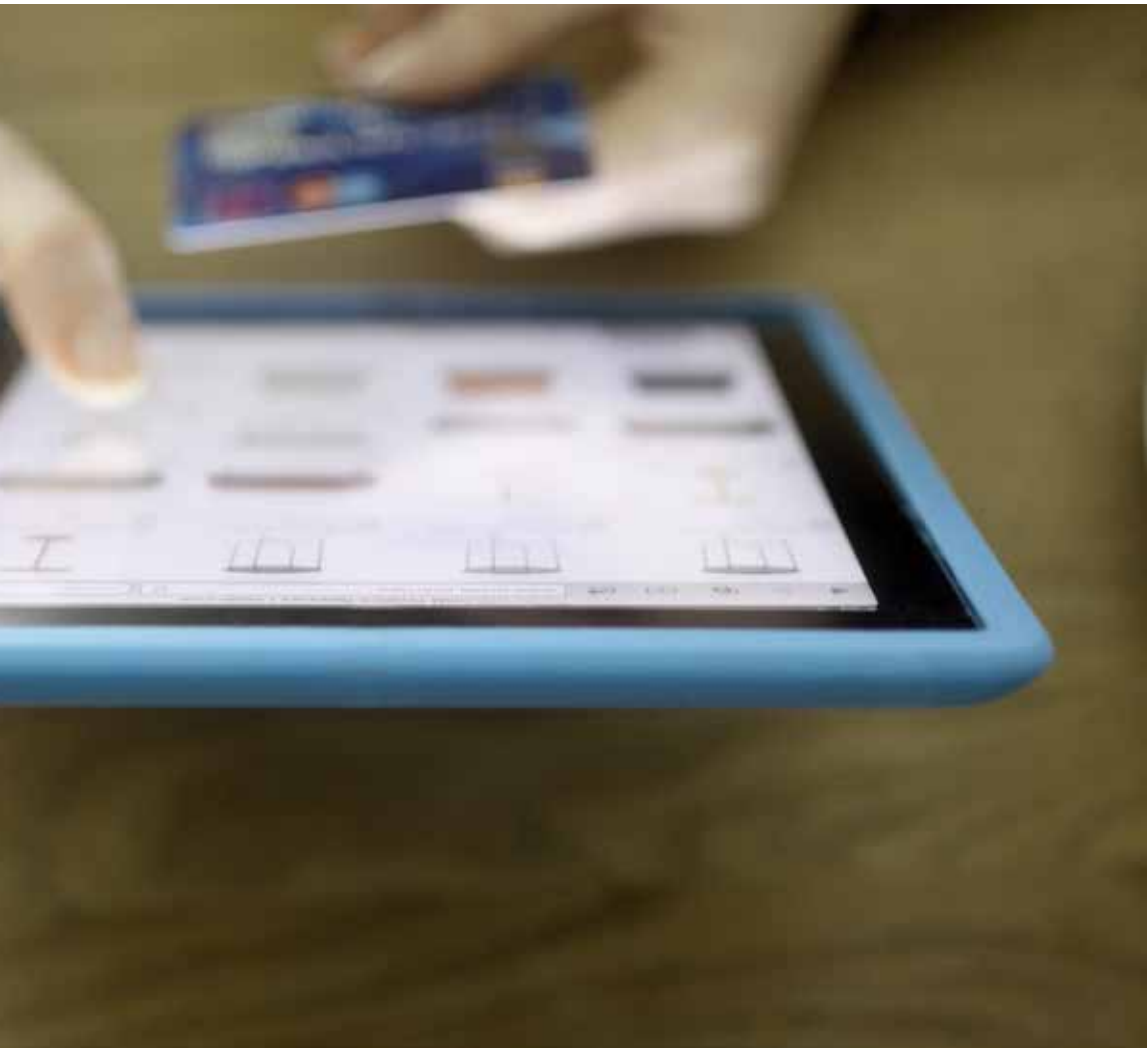


Image: Getty

rest,” says Andy Schmidt, research director at financial risk consultancy and member-based advisory service CEB. “At the moment it’s mainly banks that underpin identity management and fraud protection for the entire payments industry and they’re going to resist that expense if they’re expected to do so for countless new players who don’t want to pay them for the service. The liability is huge, the upside decreasing.”


COST BORNE BY RETAILERS

All of these solutions, however, come at a cost and that cost is borne by the retailer. In the UK, most of the online card verification systems, such as Verified by Visa or 3D Secure, have been in place almost as long as chip and PIN payments, and while the systems were clunky at launch, they’re becoming evermore sophisticated.

Indeed, Mark Cobbett at the UK Cards Association warns retailers not to panic. “The techniques may seem more complicated but, with fraud, criminals have been doing the same basic things for the past 300 years – counterfeiting, copying and pickpocketing,” he says. “The internet can seem more alarming because every incident is grouped together and easy to record, rather than dotted across high streets around the country. In fact, e-commerce fraud is worth 6p in every £100, while online retailers have re-

duced the risk of shoplifting, which can account for 7 or 8 per cent.”

He suggests retailers start with some time-worn principles to keep themselves safe. First know your customer, second don’t get too greedy – if an unexpected bulk purchase seems too good to be true, that’s because it might be – and third lock up your warehouse with strong security. Online this means software that spots unusual shopping patterns, alerts unusual deals and keeps out hackers.

 **E-commerce fraud is worth 6p in every £100, while online retailers have reduced the risk of shoplifting, which can account for 7 or 8 per cent**


Companies such as Experian, 192.com and Ethica can help here, especially for smaller retailers. They gather groups of retailers together, and share information and customer data, making fraud easier to record and predict. And verification systems are becoming less clunky; at launch, customers would be forced on to dedicated sites to enter complex passwords – that’s changing.

Richard Collard, an online fraud expert at IBM, points out that change needs to come quickly as, faced with

tight verification, crooks are turning to “man in the middle” scams, setting up fake pages and e-mailing people to enter their banking passcodes. The sooner verification is entirely on the retailer site, the better.

Graham Goodwin, financial crime manager at insurance giant Towergate and former Metropolitan Police Fraud Squad detective, says the big drive by criminals is data breaches, where crooks break into companies secure servers and can hide for up to 200 days harvesting card informa-

tion. There are some five or six massive breaches every week, according to Forbes.com *Data Breach Bulletin*.

Even here, IBM’s Mr Collard sees hope. Software can usually spot unusual spending patterns, as anyone who’s received a call from their card company checking the past few purchases knows. The key, says Ms Elezari of Gigaom Research, is collaboration – just as in life, you’ll get more done if you talk to each other. 

Feeling the collar of corporate criminals

Digital forensics experts investigating white collar crime.



Fighting white collar crime begins with prevention, but when litigation does arise digital forensics expertise can mean the difference between a conviction and a criminal walking free.

CY4OR Legal’s highly experienced team are able to unlock evidence from a range of digital sources, including:

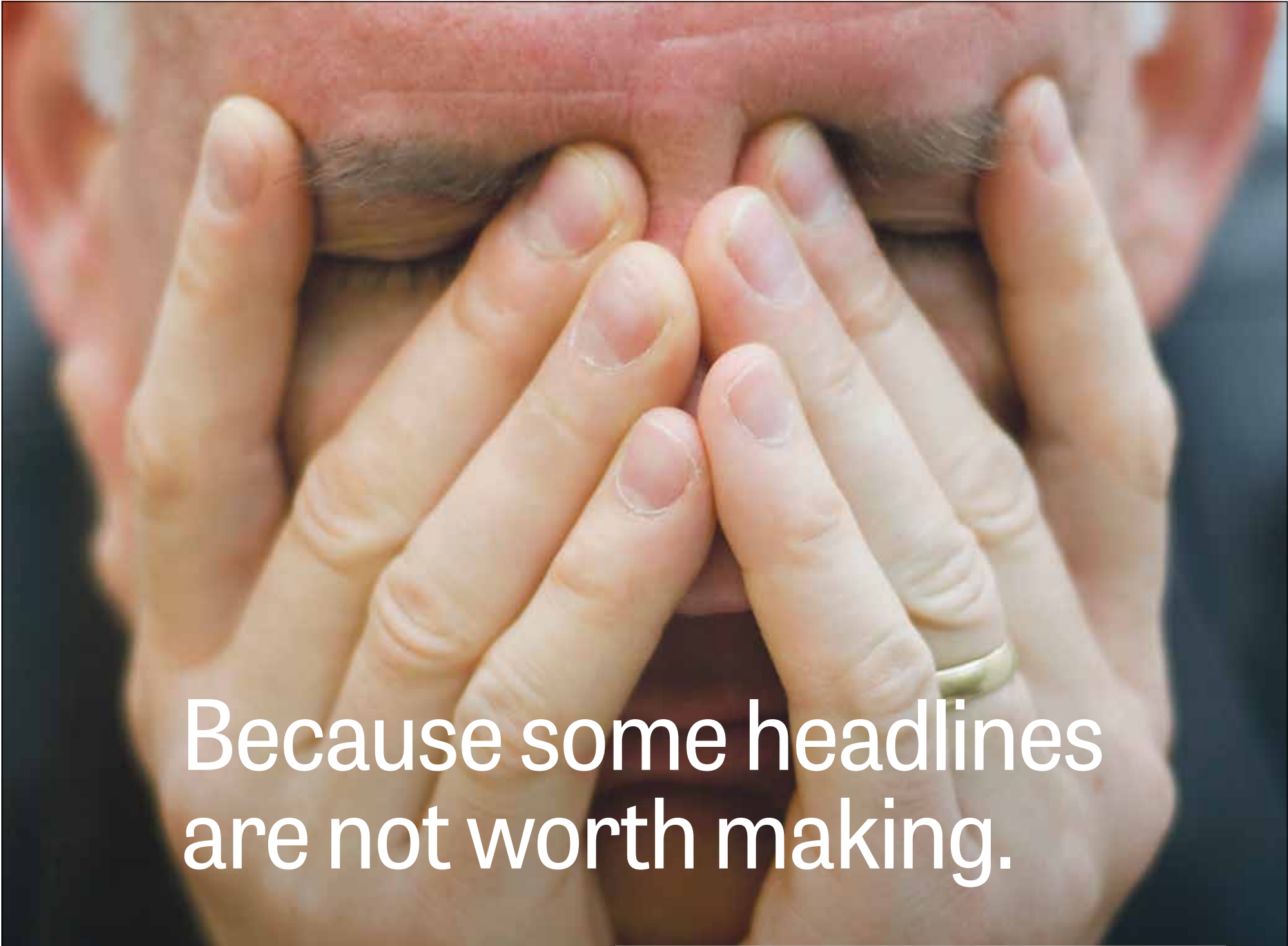
- E-mails, voicemails and SMS
- Mobile phone records
- Internet activity and metadata
- Audio and video
- Computer systems

CY4OR Legal is at the leading edge of digital forensics, discretely and professionally conducting investigations for law firms, in-house legal teams and government agencies on multi-site and multi-jurisdictional cases.

CY4OR
experts in digital evidence

Talk to us today about how we can help you investigate corporate fraud.

0845 163 8695
enquiries@cy4or.co.uk
www.cy4or.co.uk



Because some headlines
are not worth making.

Rebuilding trust is expensive. Protect your network with F5.

Your business-critical applications represent your company and your strategic advantage. A cyber attack can knock out those applications—while taking down your reputation and your revenue.

Deployed across a range of organizations, from enterprises to mobile network operators, F5® security solutions block a wide range of attacks while ensuring valid customers and employees have access to the applications that matter most.

Secure your brand from today's sophisticated attacks. **With F5, it's possible.**

f5.com



Solutions for an application world.