


FIGHTING FRAUD

03 <i>The threat of fraud is all around us</i> Despite the pervasive threat of fraud, often by skilled online hackers, too few organisations are protected	 06 <i>Beating fraud should be your business</i> An anti-fraud company culture can give businesses a competitive edge	10 <i>Banks broke the law – and the law won</i> Beware the pitfalls of sanctions and regulations governing money laundering	18 <i>Cyber spies are targeting UK business secrets</i> Rogue states launching cyber attacks aim to steal valuable commercial secrets
--	--	---	---



Global Payment and Fraud Management Solutions

Innovate. Optimise. Grow.
ONE connection does it all.



STROZ FRIEDBERG

SEEK TRUTH

FOREWARNED IS FOREARMED. Opportunities expand. Threats multiply. Be ready for both. Our Cyber Response and Resilience teams can help you advance

with confidence, whether you're countering a data breach or securing your network across every touchpoint. Find out how at strozfriedberg.com

Time to strike back at cyber criminals

With almost all business records now created and held on computers, the risk of digital fraud rises each year, but there are counter measures to hit back at the hackers

◆ DIGITAL FRAUD
● NIC FILDES

No matter how many moats, walls and booby traps companies set up around their critical digital information, the bad guys, as they are known in the cyber security industry, seem to get in. Among the most recent victims was Carphone Warehouse which was forced to admit that hackers had gained access to as many as 2.4 million accounts with customer details including names, addresses and bank information. Credit card information stored in an encrypted form could also have been accessed. If there is a common denominator in every data breach, it is the claim by victims that the attack was “sophisticated”. All attacks, whether they are brute-force attempts to take down a web site or a dodgy USB stick that infects a cor-

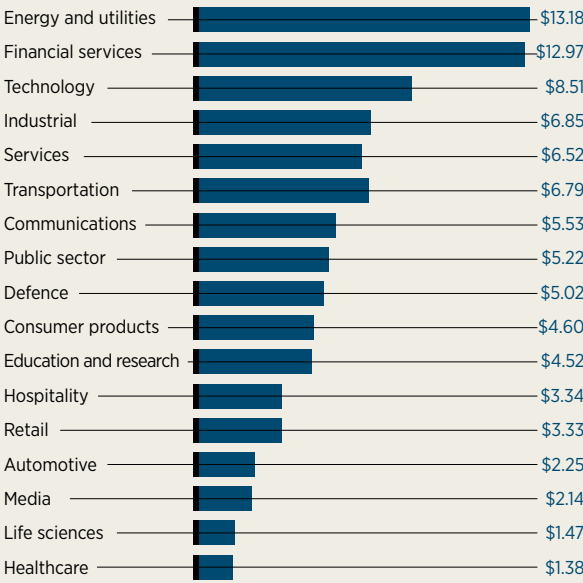
“
With 90 per cent of all business records created and stored electronically, the risk of digital fraud is rising exponentially

porate network, immediately become sophisticated once they succeed. However, Dmitry Bagrov, UK managing director of technology consultants DataArt, doubts that many actually are. “Well they would say that wouldn’t they?” he says, misquoting Mandy Rice-Davies, on the so-called sophistication of an attack once a company realises its systems had been too vulnerable. With 90 per cent of all business records created and stored electronically, the risk of digital fraud is rising exponentially. Yet what is alarming is how unsophisticated most attacks are. “It’s not like *Ocean’s Eleven* – these guys aren’t acrobats,” says Dave Palmer, chief technology officer at Darktrace. “Despite all the talk of armies of bad guys, the majority of people aren’t

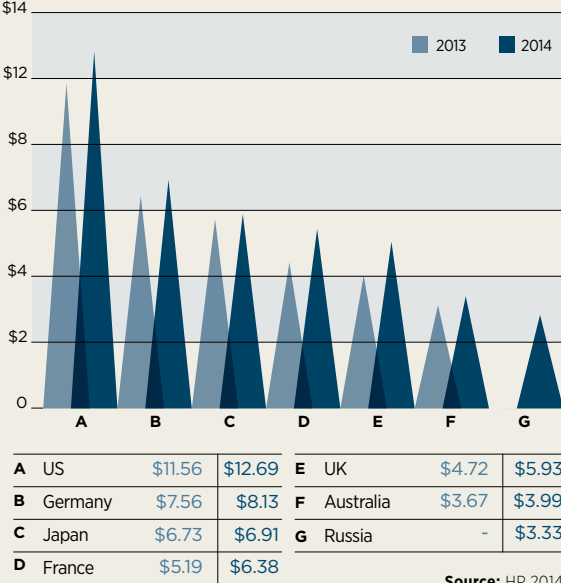


1. Carphone Warehouse admitted in August 2015 that up to 2.4 million customer details had been accessed by hackers
2. Personal details of approximately 77 million Sony PlayStation customers were compromised in a cyber attack in April 2011

AVERAGE ANNUALISED COST OF CYBER CRIME FOR GLOBAL COMPANIES BY SECTOR (\$M)



AVERAGE ANNUALISED COST OF CYBER CRIME FOR A COMPANY BY COUNTRY (\$M)



criminals and the majority of criminals are using basic tools off the shelf. We’re still in the era of low-hanging fruit where tricking people into watching a video or clicking on a link works.” That threat has increased in the age of bring-your-own-device. Staff who take a tablet computer logged into the company network home with them run the risk of inadvertently opening the door to hackers. Mr Palmer notes repeated malware attacks on celebrity chef Jamie Oliver’s website. “How many people are thinking about cyber security when they look up a recipe for fajitas?” he asks. What is changing is the volume of attacks and what the bad guys are trying to do. James Lyne, director of technology strategy at Sophos, says: “We see in excess of 350,000 new pieces of malicious code every day, which means the chances of running into it are very high. What’s more, Sophos sees in excess of 30,000 infected web pages, which are typically small businesses that have been attacked and are now distributing malicious code to their customers. While it is easy to think of these attacks as the result of sexy high-tech hacking, the main attack vectors are still phishing e-mails and infected websites distributing malware.”

To manage cyber risk
you need to plan for it...

We provide the world’s leading organisations with the knowledge, skills, tools and methods to develop the resilience needed to survive today’s evolving cyber security threats.



Find the right solution
for your organisation at
www.securityforum.org

Customer bank details would usually be seen as the Holy Grail for hackers, but company data is now being used for industrial espionage and corporate blackmail. Even IT departments can be fooled into downloading patches that look legitimate but contain malware which can infect a whole organisation.

Darktrace's Mr Palmer says many companies would have experienced internal extortion attempts but that blackmailers are now more likely to come from outside the company. Using ransomware, such as CryptoLocker, means outsiders can threaten to take down a company's systems unless money is paid. Most companies are paying the fees, he reckons, as the cost of having a website go down quickly outweighs the ransom being demanded. "This is digitally enabled criminality," he says.

Another fraud was revealed this month when a web of hackers were found to have made \$100 million by breaking into the computers of business newswires and accessing corporate press releases before they were published. The scale of the fraud, perpetrated by hackers in the United States and Ukraine, shows how valuable non-traditional targets for data theft can be. Why bother selling a credit card number stolen from a company for \$30 if you can get a run on a major piece of breaking news?

“

The starting point for any company needs to be that they have already been hacked and should look for abnormal behaviour on a corporate network

Luke Scanlon, technology lawyer at Pinsent Masons, comments: "This case highlights that too much of the focus of recent discussions has been on privacy rights. It shows that law-makers need to look more at the processes and controls to be put in place to help corporations protect confidential information. The involvement of cyber attacks and hacking in insider-dealing activities highlights a clear area of focus for market regulators along with other prosecuting agencies."

The irony is that for all the horrendous headlines suffered by the corporate victims of attacks, few have been hit as hard as would be expected. People are still buying Sony television sets and playing video games on PlayStation consoles. US shoppers still go to Target and shareholders still believe that people will continue to buy smartphones in Carphone Warehouse given its stock fell a tiny 1 per cent after it admitted it had been hacked.

Companies trying to deal with the relentless attacks – the equivalent of someone rattling the windows and doors of your house every minute of every day – probably feel they need to prepare for the worst. Small steps can, however, make a difference.

"To help thwart the cyber-criminal threat, everyone has to do their part and it's surprisingly simple practices that make the difference – updating the software on your computer, in particular your web browser and popular software such as Adobe Flash, makes a huge difference," says Mr Lyne of Sophos.

TOP 5 TYPES OF CYBER ATTACKS ON COMPANIES

98%

Viruses, worms, Trojans

97%

Malware

59%

Botnets

58%

Web-based attacks

52%

Phishing and social engineering

Source: HP 2014

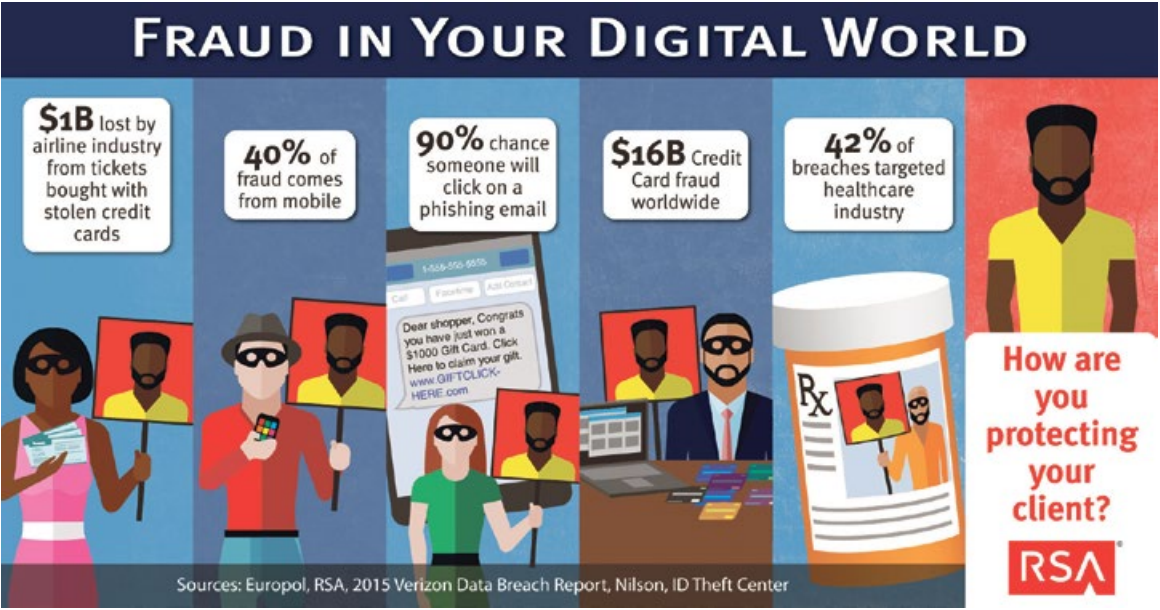
"Running end-point security software and web-filtering software will also help keep your system clean. Finally everyone should be alert to scams. The old adage of 'if it seems too good to be true, it probably is' really does apply here."

Darktrace believes that a more radical approach is needed. The starting point for any company needs to be that they have already been hacked and the best way to deal with it is to look for abnormal behaviour on a corporate network – a random laptop logging on or a worker acting irrationally at an unusual time, for example. Darktrace's software, based on the same pattern-recognition techniques developed by software company Autonomy, acts like a burglar alarm that alerts the IT department to odd behaviour. It also sets "honey traps" for hackers to flush them out before they can cause any damage.

"We need an immune system like we have for the body. We can recognise the symptoms of polio and deal with it – we need the same for cyber security. In ten years, most cyber defence will be based on these principles. You can't just look back and do what worked before. You need to be as flexible as a hacker," Mr Palmer concludes.

Share this article on social media via raconteur.net

COMMERCIAL FEATURE



AS FRAUD LANDSCAPE EVOLVES, SO MUST YOUR RESPONSE...

As fraudsters become more sophisticated, prevention requires complete visibility, says **Rashmi Knowles**, chief security architect, Europe the Middle East and Africa, at **RSA**, the security division of **EMC**



Cyber criminals are more organised than ever. Using online services to commit fraud, known as fraud-as-a-service, opens up the most advanced threat technologies to a wider base of fraudsters.

Because of this your fraud strategy must continuously adapt to protect your customers and digital assets, but that is only half the battle. Consumers demand fast, easy access to accounts, products and services, and do not want their experience interrupted. Any successful strategy must balance an organisation's security requirements with the need for convenient user access. Organisations must aggressively rethink traditional notions about what constitutes a threat and how to defend against it intelligently.

Gil Shapira, worldwide general manager, RSA Fraud and Risk Intelligence, says: "Fraudsters are constantly changing their techniques, and customers change their online behaviour, which limits the ability of traditional fraud strategies to detect evolving threats and their impact."

PROTECTING CUSTOMERS

Gaining broader visibility into your entire online user life cycle as well as shared intelligence around the latest threats is essential, allowing extended analysis of the behaviour of humans and devices so that fraud patterns are quickly detected. As a result, only high-risk activities are interrupted and the normal user's security experience remains transparent.

An intelligence-driven fraud prevention strategy is multi-faceted, spanning user behaviour, device fingerprints, known

fraudulent entities and threats from the underground. To differentiate a genuine customer from a criminal requires an overview across the entire online consumer life cycle from pre-login through transactions to post-login.

“

To differentiate a genuine customer from a criminal requires an overview across the entire online consumer life cycle from pre-login through transactions to post-login

Your solution must work seamlessly across all channels. It must provide expanded choices for integration with new and existing services and technologies, especially when it comes to step-up authentication. You not only need to understand your risk tolerance, but the appropriate security for the digital channel used by your customer. You must also be able to correlate cross-channel activity for login and transactions. For example, if a customer makes a transaction on their laptop followed shortly afterwards by another from a mobile device in another country, this should be flagged.

There are three things organisations should do now to adopt an intelligence-driven fraud prevention strategy.

First, gain broader internal and external visibility to evaluate risk and cyber-crime threats across all online digital channels.

Second, extrapolate insight from the data to understand normal-state behaviour to spot, investigate and root out anomalies that indicate threats based on your unique risk profile, and immediately see which threats are most damaging.


Third, responding to malicious anomalies designates the right corrective action to mitigate the specific threat and enforce controls to initiate a remediation process and operationalise the response.

We're finding organisations that use our fraud and risk intelligence solutions gain visibility into shared intelligence on emerging attacks and threats. They can analyse interactions and transactions to detect anomalies that indicate threats quickly, and take corrective action based on custom-defined threat levels to reduce losses from fraud and undetected breaches. This approach is well positioned to address the ever-changing threats of today and anticipated threats of the future with minimal interruptions to your consumers digital channel experience.


Follow us on twitter: @RSAFraud
Take a journey through a Decade of Fraud and Cyber Crime: www.emc.com/microsites/rsa/timeline/index
Combat fraud with an intelligent driven strategy: www.emc.com/video-collateral/demos/microsites/mediaplayer-video/combating-fraud-threats-intelligent-security-rsa




5 TOP TIPS TO PREVENT FRAUD

- 

Follow up on simple control failures. Seemingly minor bank account errors should be treated as possible red flags not operational glitches.
- 

Dispose of old laptops and PCs without their hard disks. Computers have been traded complete with sensitive company data.
- 

Audit expenses claims on a regular basis. The fear of getting caught will deter employees from trying to abuse the system.
- 

Implement an anonymous whistle-blowing procedure. Being on the ground, employees can see what is going on better than their bosses.
- 

Set password protocols to mitigate cyber-security risks, using letter, number and special character combinations in complex passwords as standard.

Beating fraud is your business

An anti-fraud company culture, backed by staff training and adequate enforcement procedures, can give businesses a competitive advantage by avoiding sometimes substantial losses

◆ FRAUD PREVENTION
● ALISON COLEMAN

The cost of fraud to business has reached alarming levels. New research from chartered accountants PKF Littlejohn and the Centre for Counter Fraud Studies at the University of Portsmouth shows that UK businesses typically lose around 5.6 per cent of their total expenditure to fraud.

Most fraud is high volume, low value and therefore difficult to detect and expensive to investigate. But as Jim Gee, head of forensic and counter fraud services at PKF Littlejohn and the report's co-author, points out, companies that have been successful in reducing the cost of fraud have done so by focusing on pre-empting it by establishing stronger anti-fraud cultures and effective deterrence.

In some sectors, for example financial services, companies have developed robust processes around fraud prevention and made it part of their "business as usual" activities.

Elsewhere, firms are not recognising the benefits of mitigating fraud risk and react only when there has been a breach in their security.

John Smart, UK head of fraud investigation at EY, says: "Activities like launching a new product, entering a new overseas market or relocating parts of the

business can expose firms to additional fraud risks, which they many fail to consider until it's too late. Fraud prevention should be a key consideration at the start of any big corporate change project or any time a business is looking to do something different."

For effective fraud prevention you need to know who your employees and suppliers are, says Andrew Rogoyski, vice president, cyber security services at CGI UK.

"Background checking of new and temporary employees is essential for mitigating the risk of insider fraud. The same approach should be adopted when choosing business suppliers to determine their reliability as a business partner," he says.

In taking a proactive stance on fraud, most businesses will face challenges. One is their lack of real-time visibility into their data, making it difficult to identify readily suspicious behaviour. Another, arguably the most damaging, is that fraud prevention has never been part of the company culture.

Creating a culture where fraud is frowned upon needs to be facilitated by

the right technology, says Chris Baker, managing director of expenses management firm Concur.

"Expenses are a prime example and in many enterprises are the business process that time forgot," he says. "If the way you manage expenses hasn't moved on since the 1970s, the chances are that the culture of slipping in a receipt for Sunday lunch last weekend probably still prevails, too. Your company's culture will only move forward if it is supported by the right technology and tools."

Creating a fraud security-aware culture also comes down to having a clear best-practice policy, good governance and triangulating business systems in order to create the real-time visibility needed to spot any suspicious activity. Quite simply, preventing fraud has to be a "business as usual" process.

According to Phil Beckett, partner at forensic investigation specialist Proven Legal Technologies, the best way of achieving this is to invite the employees to brainstorm ways of defrauding the company and getting around the processes.

He says: "This will highlight any weaknesses that need to be fixed as soon as possible. This process needs regular attention to ensure nothing has changed or been adapted that could open up any risk."

Enhanced monitoring schemes should be implemented to ensure nothing unusual is ignored or missed and that all leads are followed up. The output from this can then help enhance controls in place and everything should be formally documented into a fraud policy.

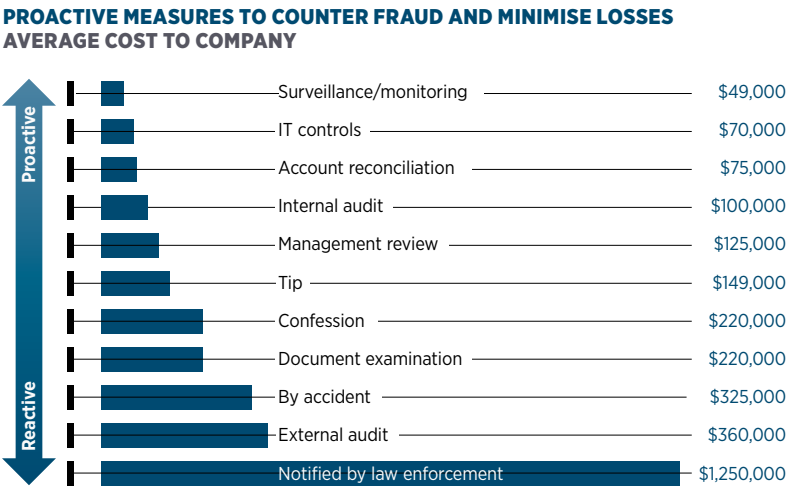
For this to happen, fraud needs to be an open topic of discussion, which some companies may not be comfortable with, their misconception being that talking about it will encourage more individuals to consider doing it.

However, broaching this taboo subject, says EY's Mr Smart, will not only alert people to the issue and the ways in which fraud can present itself, it will also identify the most innovative ways of addressing new fraud threats.

There is an irony that people, deemed a company's most valuable asset, can quite inadvertently be its biggest vulnerability in terms of security. Overlooking the human element is the most common mistake companies make in preventing fraud, says Robert Griffin, chief security architect at security risk solutions provider RSA, so the right training is essential.

"My advice would be to develop a generic security training programme and move on to role-based training as a next step," he says. "Focus on the most valuable assets, and who has access to them, and ensure that your employees understand the importance of protecting them. Walking them through some real-life scenarios will show how a lack of awareness can lead to a security breach."

A strategy of designing weaknesses out of processes and systems, and embedding a strong anti-fraud culture, will also give companies a competitive advantage in reducing their fraud losses.



Source: ACFE 2014

COMMERCIAL FEATURE

TACKLING WELL-ORGANISED CYBER FRAUD

Have you heard the one about the chief financial officer who transferred £250,000 to fraudsters in Hong Kong? Or the imposter “chief executive” who convinced a major media company to send £2 million to his Chinese bank account? Unfortunately, these are not jokes, but actual frauds against real companies – don’t let cyber criminals have the last laugh

STROZ FRIEDBERG

In an age where businesses and individuals exist in an increasingly digital milieu, virtually all fraud is cyber fraud. Even more concerning is that sophisticated, big-ticket cyber fraud is on the rise, backed by an emergent criminal ecosystem capable of coming together rapidly for anonymous collaboration on a single co-ordinated cyber attack – and then disbanding, leaving few clues for organisations and authorities to track.

“Today’s cyber fraud is a professional criminal enterprise that rewards innovation, intelligence and aggression. It outsources avidly and assembles the best talent it can find on a project-by-project basis to achieve very clearly defined goals,” explains Phil Huggins, security expert and vice president of Stroz Friedberg, a cyber crime investigations, intelligence and risk management company.

Firms such as Stroz Friedberg are among the most potent weapons businesses can wield against the rising tide of cyber fraud. They help organisations become more resilient

by improving their ability to recognise and respond to cyber fraud incidents rapidly enough to mitigate serious damage, and by training employees to spot the often subtle signs of an attack.

HOW IT’S DONE: ‘SOCIAL ENGINEERING’ FRAUD

Professional cyber criminals exploit gaps in digital security to perpetrate frauds that are ensnaring a growing number of businesses worldwide. Frequently called social engineering or business e-mail fraud, attacks often start with the collection of publicly available data.

Information gleaned from Facebook or LinkedIn profiles offers cyber criminals the insight they need to compose fraudulent e-mails, which sound familiar and authentic, to company employees. Sometimes, they even target a single individual. Triangulated with information from other sources – articles profiling executives, a company’s website, public filings, online requests for proposals and job



“
Cyber fraud is a professional criminal enterprise that rewards innovation, intelligence and aggression

postings, for example – information is synthesised and used to craft convincing e-mails designed to trick someone into clicking a link or opening an attachment.

That action then results in downloaded malware that can capture a person’s login and password credentials, or otherwise provide access to an organisation’s systems and network.

As they’ve honed their skills, cyber fraudsters have begun hunting bigger game. “In the last few years, cyber criminals have moved on to targeting payroll systems and treasury functions at large corporates. We’ve seen social engineering attacks on chief financial officers and senior accountants, people who can move £1 million or £100 million at a time,” reports Stroz Friedberg’s Mr Huggins.

Stroz Friedberg provides a range of services to battle such fraud, from hack prevention to cyber incident preparedness and response services, including digital forensics, tracing money movement and background checks. Because its professional staff comprises technical experts, former prosecutors and other litigators, and law enforcement agents, Stroz Friedberg works effectively with outside counsel, the C-suite and board members, as well as IT personnel.

DIGITAL TRANSFORMATION ENABLES CYBER FRAUD

As digital transformation sweeps through virtually every industry in the global economy, businesses are digitising all aspects of their operations, from customer interaction to partner relationships in their supply chains. This provides transparency and

enormous efficiencies, but also exposes the corporation, making it more vulnerable to cyber fraud.

This trend is partly to blame for the recent spike in cyber fraud, according to Spencer Lynch, a director of digital forensics at Stroz Friedberg. “We’re no longer talking about businesses that physically hold money, like a bank, but departments that control money-flow at any business. So payroll systems are a huge target right now; criminals are particularly aimed at individuals with access to payroll via their home computers,” says Mr Lynch.

In fact, in one case that recently landed on Mr Lynch’s desk, criminals discovered someone’s corporate login credentials via his home computer. “They used those credentials to access the payroll system, where they created fake employee records. By manipulating that system they were able to receive payment through the company’s normal business processes,” he says.

For a large organisation with hundreds or thousands of employees, it’s hard to spot a small number of new payroll records, let alone identify them as fraudulent, especially if the organisation is not expecting to be targeted.

CYBER CRIMINALS ARE GETTING SMARTER

In recent years, criminals’ understanding of the financial system has become more sophisticated.

Mr Huggins cites many examples of recent creative fraud activity, including an instance in which cyber criminals breached a company’s accounts payable system and changed payment details for one of their suppliers. Instead of money heading to the supplier, large monthly payments went straight to the fraudsters’ accounts.

Another example unfolded while two family businesses negotiated an acquisition. Having agreed to terms, the seller e-mailed account details to the buyer. But criminals intercepted and the bank details that reached the buyer were not the same as those sent by

the target. Money was paid into the fraudsters’ account and promptly disappeared.

“Cyber criminals’ growing sophistication and perseverance means that areas historically protected by the complexity of transactions are no longer safe. Complexity, in and of itself, is no longer an effective defence,” explains Mr Huggins.

“Criminal groups are incredibly well structured with outsourced networks; they collaborate on a single criminal activity and then may not work together again. It sounds odd, but it’s true. Cyber fraud has evolved into a trust-based business where nobody knows anyone else’s real identity.

“In this ‘dark market’ there are middlemen who essentially work as brokers and project managers, and even offer warranties. If a criminal buys an outsourced service and it doesn’t work, he can get his money back. It’s a very efficient set-up. These are professionals and there is a lot of money at stake.”

Having conducted their own risk assessments, fraudsters set themselves up to be near-untouchable. They locate where policing is patchy, legal recourse is limited and there are no extradition treaties with the countries they target.

To meet this growing cyber fraud challenge, organisations are increasingly turning to specialists such as Stroz Friedberg – experts who are capable of detecting fraudulent activity and helping companies act decisively. Its broad range of cyber capabilities helps organisations increase their enterprise-wide cyber fraud resilience and helps executives make quick decisions on an extensive array of areas to combat criminals.

And the faster companies act when the inevitable occurs, the better they can mitigate risks, limit reputational damage, interact with regulators and reduce direct costs.

@strozfriedberg
strozfriedberg.com

WHEN Can A CYBER FRAUD Strike Your Organisation?

ANYTIME.

Download our complimentary
CYBER PREPAREDNESS CHECKLIST:
www.strozfriedberg.com/prepare

Thwarting market hackers

As online fraudsters increasingly hack into the e-commerce market, merchants are faced with the dual challenge of combating digital crime without adversely impacting on customer experience

◆ E-COMMERCE FRAUD
● DAN BARNES

It is hard to feel sorry for websites. But if you think about them as being a bit like shop owners, it is worth considering that 63 per cent of online merchants are struggling to keep on top of fraud attacks, according to research by payments processing firm Worldpay.

Some have had very public struggles. At the end of 2013, US retail giant Target had 40 million credit and debit card account details stolen by hackers. The upshot was it cost the company \$162 million in costs not covered by insurance.

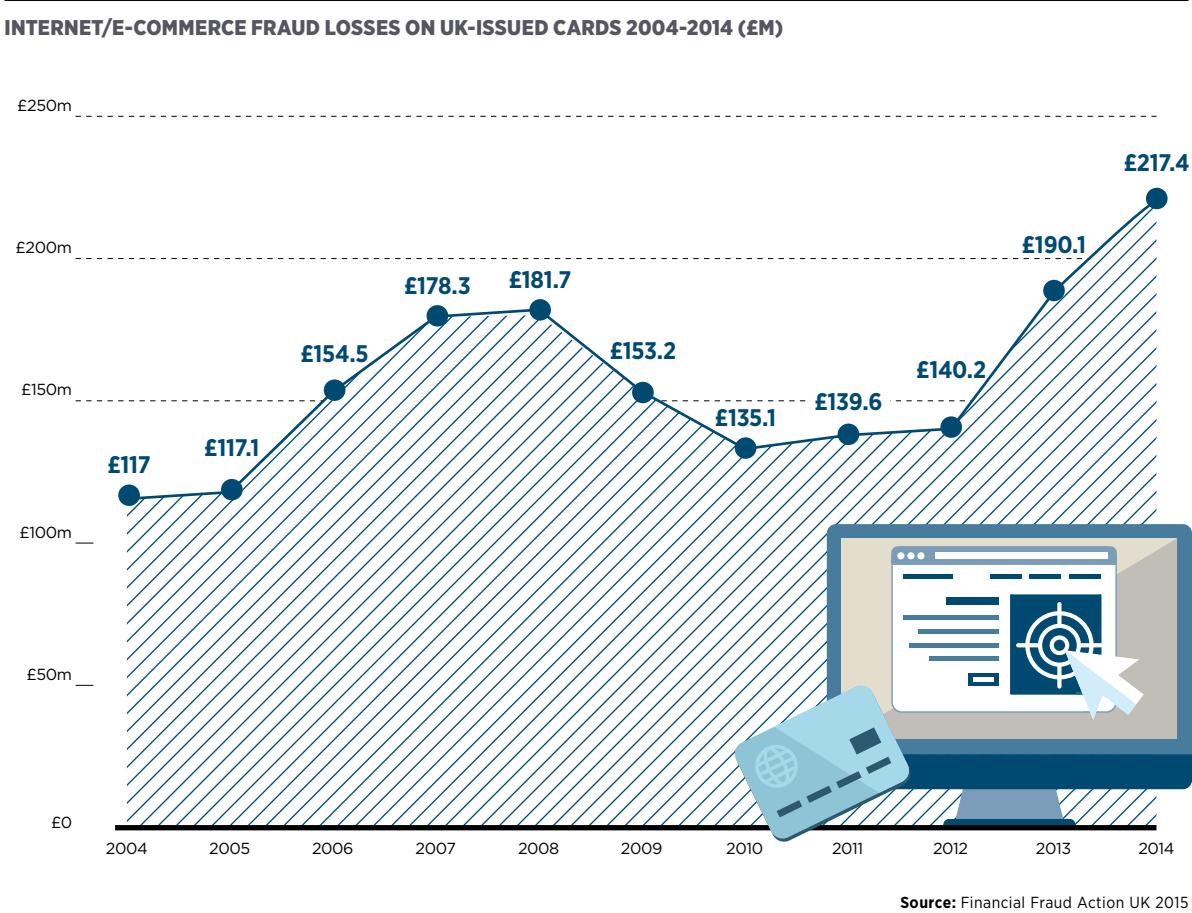
It is, of course, the responsibility of the merchant to keep their goods, cash and customer information secure, but it is also worth remembering they are being targeted by technically minded criminals, while trying to keep pace with a very demanding customer base.

Jackie Barwell, director of fraud product management at payments specialists ACI Worldwide, says: "If you look at a retailer like Next, they have competed to be one of the best in the market at delivery. At one point, if you ordered by 9pm you could get next-day delivery; now it is possible if you order by midnight. There is continual, marketing-led pressure to be the best in order to attract the customer to your website. The fraud team have to try and keep up with that."

The rapid pace of change in terms of channels, payment mechanisms, and capacity for fraudsters to gain access to data and systems makes it hard for the e-commerce merchant's security team to know where there may be a threat and how to counter it. Crucially, the team has to increase security while minimising any negative impact on customer experience. But often there is no real technology discipline around a merchant's operations.

Paul Ducklin, senior security adviser at security software and hardware provider Sophos, was interviewed in a coffee shop with three different means of mobile payments, credit card machine, a computer to update the shop's Facebook page and free wi-fi.

"What could possibly go wrong?" he asks. "The problem is that at a small business like this, there are no IT staff; they are trying to be very convenient and they are trying to be on social media. But at least all the devices are not on one network. The step-up to a small shop is that the accounting system is now on a PC on the same network as a PC to read Facebook and the point-of-sale devices.



Scott Boding, senior director in risk solutions product management at security firm CyberSource, says the use of card-on-file accounts online, which remove the need to re-enter card details into a website, are particularly dangerous. When coupled with the acquisition of non-physical goods, they can be hard to trace. However, he says security measures should not automatically impede the customer experience.

"Ideally they augment customer service, providing additional information for how to handle different situations and quickly speed any customer interaction needed," he says. "If designed holistically, protective strategies can be used to assess risk. Depending on that risk assessment, merchants can then choose to employ a step-up authentication."

The technology that delivers this security can range from a few basic rules, such as picking up when a card issuer reports a card has been declined, to artificial intelligence, learning and spotting unusual spending or behaviour patterns.

At the core is a suite of systems looking for anomalies and providing additional data gathering, says Mr Boding.

"A machine-learning-based system on top of that is essential for identifying complex and subtle fraudster behaviours," he says. "Finally, a flexible rules engine to manage different segments, such as geographies, channels, products and customers, is critical for handling different types of risk appetite."

But to really minimise customer inconvenience, a firm should ensure its e-commerce hygiene is maintained, thereby limiting the ability of criminals to access one part of the business and then run riot through the rest of it. Otherwise customers will get wise, says Mr Ducklin.

"For a lot of merchants, particularly those who run multiple stores and sites, and have an IT team, very little of what they need to do to make e-commerce work is going to be troublesome for their customers," he says. "However, as customers become better informed and realise perhaps the big TVs in a store are running an out-of-date operating system, they are going to be increasingly wary about putting their card or card details into that firm's network."



Forty million target customers had their credit and debit card details stolen in 2013

And we see that attitude extend all the way up to the top [shops]."

Worldpay's research indicates that 77 per cent of merchants say a multi-channel payments approach makes fraud more difficult to identify, manage and prevent, yet nearly 80 per cent of businesses surveyed say alternative payment methods would increase in the next two years. From a technical perspective that offers new points of entry and when a breach occurs in an interconnected environment, the hacker has often crossed a border after which no one ever challenges their right to be where they are.

"Once they were in [at Target], hackers were able to pull off 20,000 thousand smaller intrusions in separate Target stores across the US and implant malware on every point-of-sale register," says Mr Ducklin.

“**Merchants are being targeted by technically minded criminals, while trying to keep pace with a very demanding customer base**”

UK RETAIL FRAUD

12.4p
of every £100 in e-commerce spend is fraudulent

£331.5m

was lost on card purchases online, phone or by mail order in 2014

5%

growth in the number of incidents of card fraud to 1.3m in 2014

33%

of retailers don't have a plan in place to deal with customer credit fraud

81%

of all UK retail fraud by volume is credit or debit card fraud

ACCEPT MORE ORDERS, WITH LESS FRAUD.

Our integrated payment, fraud and security management services can help speed up time-to-market, streamline operations and help you accept payments securely – online and through mobile devices, across the globe.

IF YOU ARE A MERCHANT SELLING ONLINE, WE CAN HELP YOU:

1 **MANAGE MOBILE FRAUD**

Our range of tools can help you to confidently sell through the mobile channel, while managing fraud to the same levels as with traditional eCommerce channels.

Read our report at:
www.cybersource.co.uk/mobilefraud

2 **INCREASE ORDER ACCEPTANCE**

We can help you optimise your fraud management operations to protect the customer experience and accept more genuine orders.

Read our report at:
www.cybersource.co.uk/orderacceptance

3 **MANAGE GLOBAL FRAUD**

Our range of solutions can help you accept orders from international markets with confidence.

Read our report at:
www.cybersource.co.uk/globalfraud

Contact us:
europe@cybersource.co.uk | +44 (0)118 990 7300 | cybersource.co.uk

About CyberSource: CyberSource, a wholly-owned subsidiary of Visa Inc., is a payment management company. Over 400,000 businesses worldwide use CyberSource and Authorise.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. The company is headquartered in Foster City, California and maintains offices throughout the world, with regional headquarters in Singapore, Tokyo, Miami/Sao Paulo and Reading, UK. CyberSource operates in Europe under agreement with Visa Europe. For more information, please visit www.cybersource.co.uk

© 2015 CyberSource Corporation. All rights reserved.

Cleaning up the dirty business

Complying with international sanctions and regulations governing money laundering requires banks and other financial institutions to

◆ MONEY LAUNDERING
● DAN BARNES

When sanctions were imposed on Russia, banks in the UK, elsewhere in the European Union and in the United States became responsible for keeping sanctioned firms, government bodies and individuals outside the banking system. Having the wrong customer can cost a bank much money.

In 2012, HSBC was fined \$1.9 billion by US authorities to settle charges relating to laundering Mexican drug cartel money. In 2014, French bank BNP Paribas was fined almost \$9 billion by American prosecutors for processing payments that broke US sanctions on Cuba, Iran and Sudan. Standard Chartered was fined \$300 million in 2014 for failing to remediate anti-money laundering problems for which it had been fined \$340 million in 2012, related to sanctions on Iran.

Anti-money laundering or AML covers drug trafficking, corruption, tax fraud and human trafficking, among other criminal activity. Big fines are not even the greatest threat. If a government decides to ban an offending bank from clearing transactions in that country's currency, it can cripple a firm's ability to trade internationally. The US has issued partial bans on clearing dollars before. Given the existential threat this poses to parts of their businesses, going against AML and know-your-customer (KYC) rules is not a good choice.

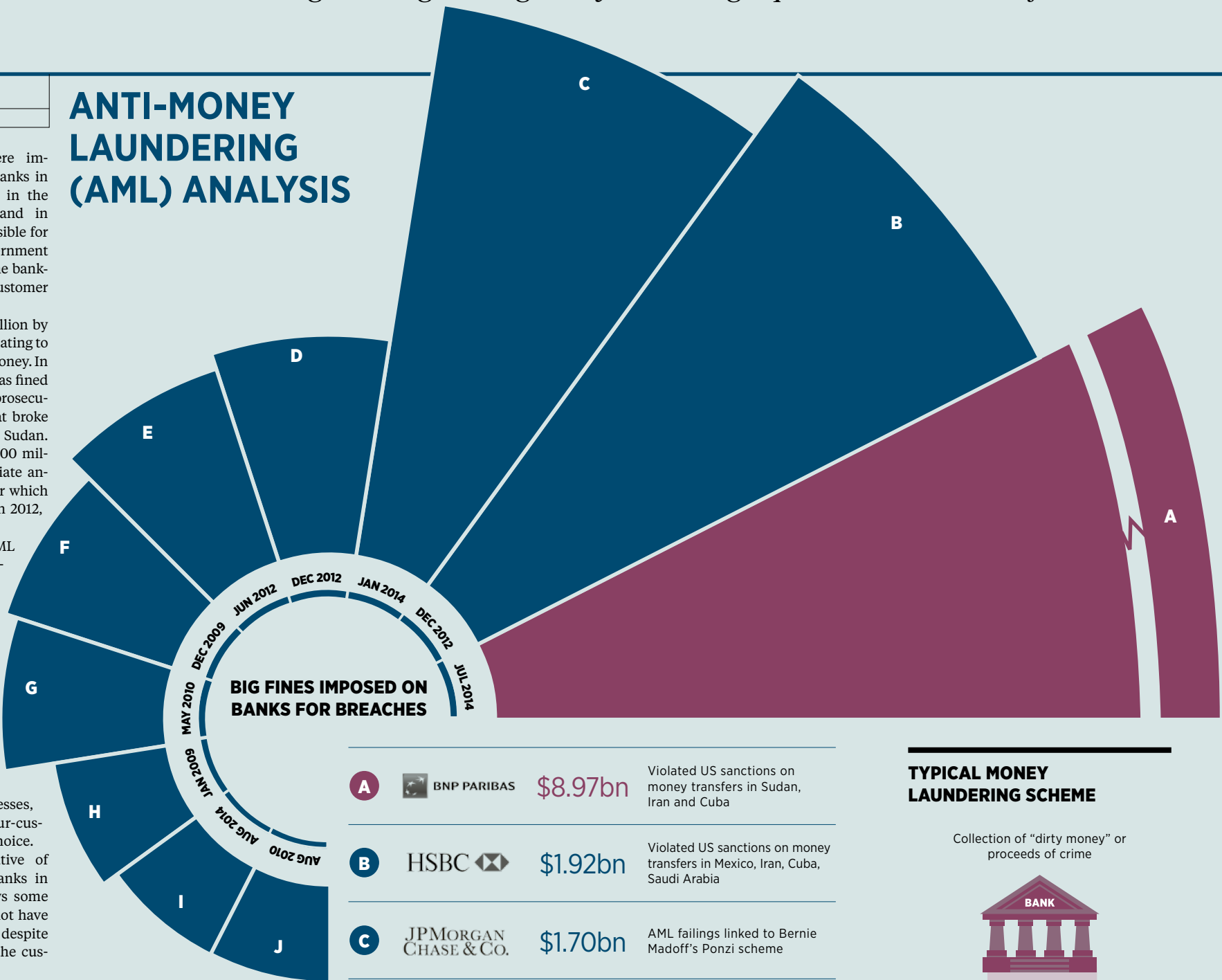
Steve Goldstein, chief executive of Alacra, a firm that supports banks in complying with regulations, says some with substandard processes do not have remedial programmes in place, despite the value that a single view of the customer offers.

"When things change with a client – if the client moves or decides to do business in a new jurisdiction – and that information is not held within the bank, then the bank doesn't really know its customer," he says. "Consequently, the single view of a customer is gaining traction as it also feeds into giving the bank a single view of the customer's credit exposures."

For big sprawling banks, working in multiple countries and with many different divisions and businesses, it is hard to maintain a single view and standard of operation. This is exacerbated by the complexity of the clients that banks deal with.

But banks are not the only businesses through which illicit money can be channelled. In 2015, a report by anti-corruption campaign group Transparency International found that at least £180-million-worth of properties in the UK had been brought under criminal investigation as the suspected proceeds of

ANTI-MONEY LAUNDERING (AML) ANALYSIS



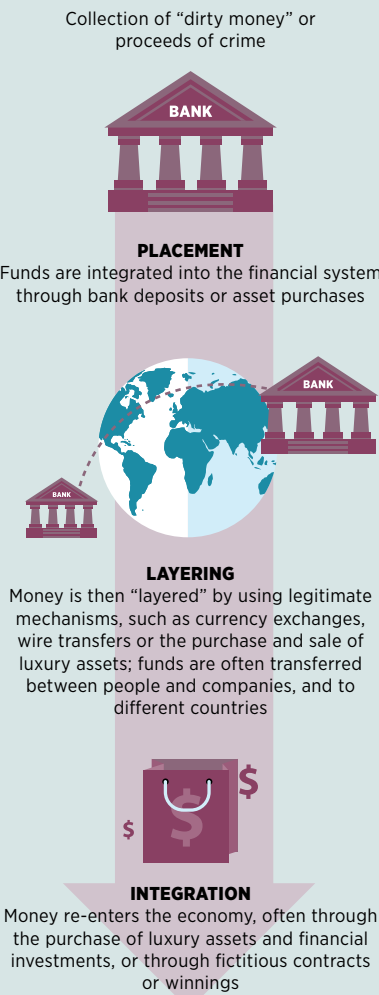
corruption since 2004. However, banks are the target for regulators.

John Cusack, global head, financial crime compliance, and group money laundering reporting officer at Standard Chartered, says: "There are no other organisations in the private sector that contribute as much to the fight against financial crime as banks. Many other organisations that could have regulations applied to them do not and so banks carry a huge amount of responsibility. When we get it badly wrong, we get punished for that and, while we should be held to the standards required, I do think that our contribution should also be recognised."

A huge range of crimes, political judgments and regulations can determine whether or not an entity or customer should be allowed to use a bank. KYC and

“Putting together a single picture of a customer is difficult and proving the identity of a new client is equally challenging”

TYPICAL MONEY LAUNDERING SCHEME



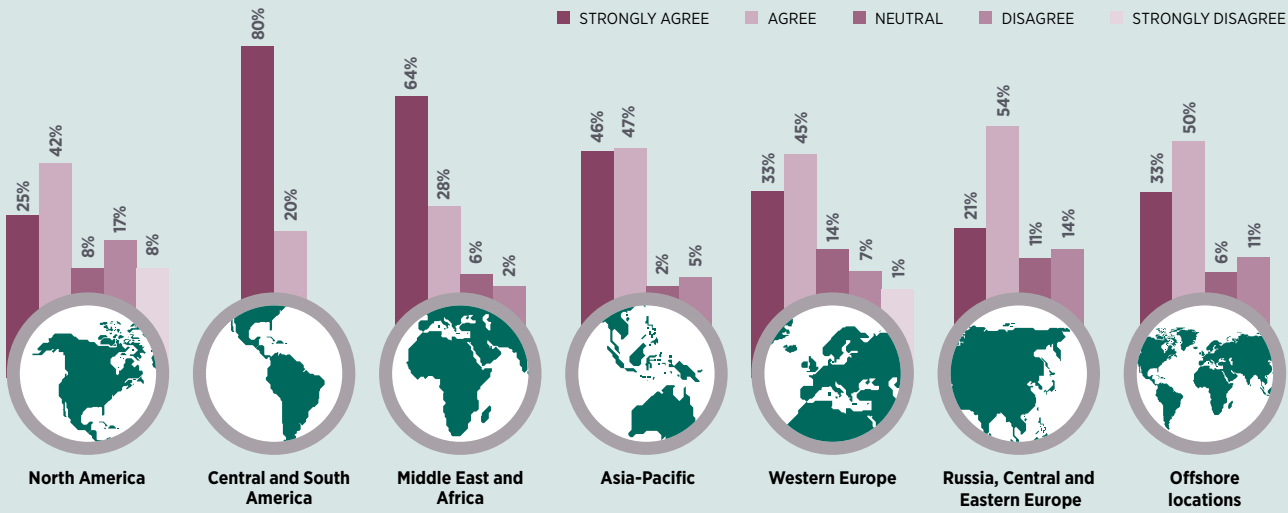
ess of money laundering

ions to be alert to potential pitfalls

WHO NEEDS TO PERFORM AML CHECKS?

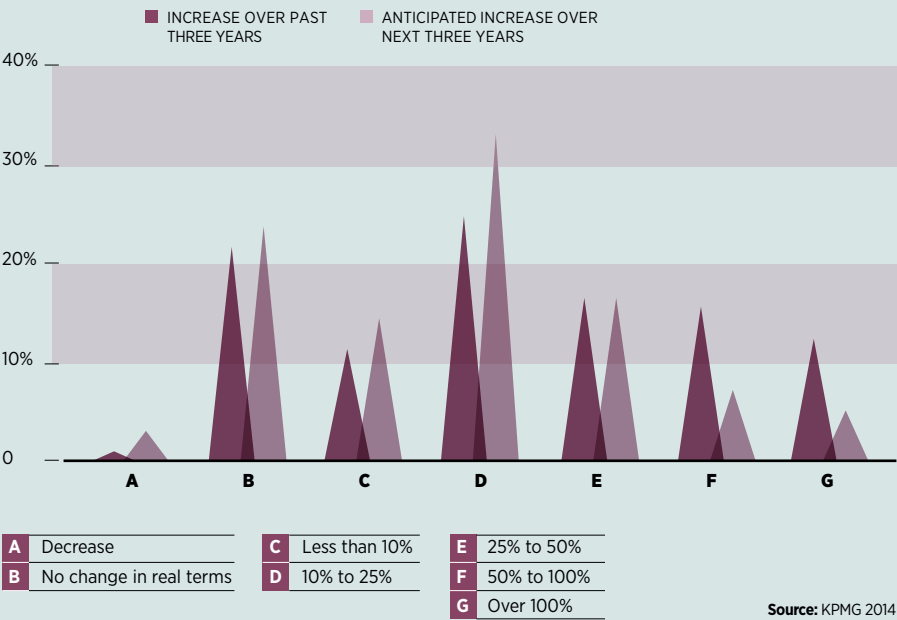
- Accountants
- Credit institutions
- Tax advisers
- Insolvency practioners
- Casinos
- Chartered surveyors
- Automotive dealers
- Financial institutions
- Trust service providers
- Estate agents
- Solicitors
- Jewellers

EXPOSURE TO MONEY LAUNDERING IS CONSIDERED A HIGH-RISK AREA IN BANKS' RISK ASSESSMENT



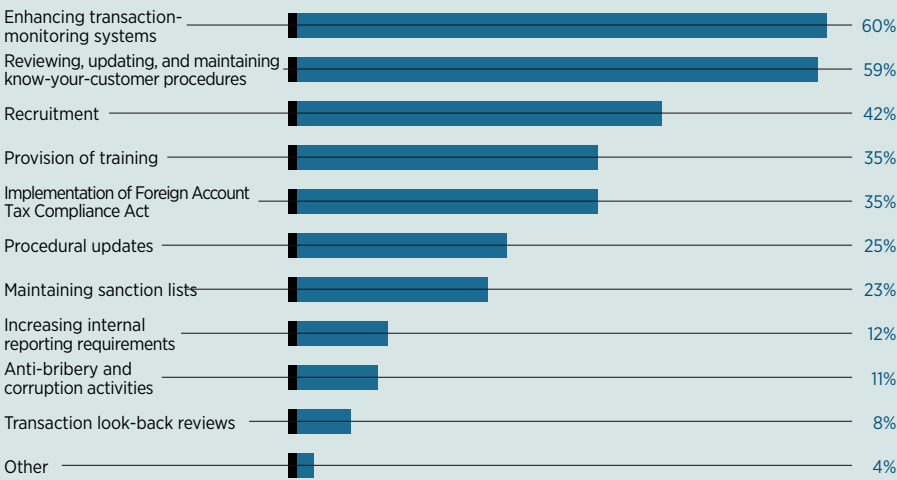
Source: KPMG 2014

CHANGES IN GLOBAL BANKS' AML INVESTMENT



Source: KPMG 2014

WHERE GLOBAL AML BUDGETS ARE FOCUSED



Source: KPMG 2014

headcount, operational tools or systems compared with larger banks, and they often need to deal with a magnitude of requests for different sets of information at different times, creating resource issues and inefficiencies.”

The structural challenge that exists within firms can also be seen between banks; sharing information between firms is difficult from a legal and operational perspective. Consequently, a new model has sprung up that allows banks to deal with a centralised hub to store and validate data provided.

“The emergence of KYC utility models over the recent past has sought to mutualise the cost of individual data and document collection, in some instances even seeking to standardise the approach and documentation required,” says Mr Taylor.

In 2014, four new utility platforms were launched, run by SWIFT, Markit, US trade processing and clearing firm DTCC, and market data provider Thomson Reuters. Offering a range of centralised hubs, designed to alleviate the fragmentation of data within firms and between firms, they also standardise the data that firms need to ensure the right checks are being run in compliance with the most up-to-date rules. They tackle two of the big challenges banks face – the number of data sources needed to validate potential customers and the pace of change.

In the NICE Actimize survey, 30 per cent of institutions report using between four and six external data sources to augment existing customers’ information, with 27 per cent of institutions using more than seven sources. Also, recent regulatory updates have impacted the approach to KYC of 61 per cent of financial institutions.

Mr Cusack says: “The standards are continuously revised to push them ever higher. Keeping on top of that continuous evolution is the number-one challenge for banks and it is unlikely to ever reverse.”

Both Mr May and Mr Taylor acknowledge their firms’ offerings are not a panacea for banks. However, they point out they are unencumbered by the legacy technology and practices that many banks have, often through the acquisition of smaller banks, which gives their firms greater flexibility to meet new requirements.

“We have an advantage in terms of a fresh infrastructure,” says Mr May. “Our firm’s heritage is in the information data space, so we are very familiar with bringing data feeds together and using those to coalesce a picture of an entity.”

Taking advantage of new operational models could lift the burden for firms who are unlikely to find the pressure from authorities lifting any time soon.

Alacra’s Mr Goldstein concludes: “Regulators see this as an opportunity to acquire money. They have been successful in the past; they are always looking for more money, so I suspect they are not going to stop looking.”



Share this article and infographic on social media via [raconteur.net](#)

Data that entombs a moment in time

When data security is breached, personal details are laid bare and your digital footprint can lead to costly and unforeseen problems

◆ DIGITAL FOOTPRINT
● BEN HAMMERSLEY

It would be easy to be amused by the digital misfortune of others. If you are, the last few months will have been hilarious. There have been countless examples of supermarket and chain-store credit card and customer data loss, not to mention millions of personnel records of the US government stolen from the Office of Personnel Management.

Most recently there have been the profile details, e-mail addresses and usage data of the wannabe adulterers of the Ashley Madison dating site, stolen and then released by blackmailers. Seemingly every week has brought yet another example of a large organisation being infiltrated by hackers, its systems copied and its data exfiltrated.

Darkly amusing, perhaps. Perhaps even, in the case of Ashley Madison, a curious case of moral schadenfreude, of digital comeuppance. You might be tempted to think it's all a little too much like science fiction, too cyberpunk, too Silicon Valley to be something you should worry about. You're probably not, after all, likely to be held to ransom by blackmailing super-criminals or infiltrated by the Chinese secret service any time soon.

But you would be wrong. Even if you're not signed up to a dating site unbeknownst to your spouse or just been made responsible for your company's fraud risk, the simple truth is that one of the key, basic life skills we will all need for the 21st century is an understanding of what we mean when we talk about data. Cyber crime is being recognised as a major concern, yes, but we're yet to comprehend completely how it affects us all.

The story of the internet over the past 20 years has been one of business realising the profound effects of the fundamental nature of data. Data is weird stuff. It costs nothing to copy it and those copies are perfect; it has negligible weight, so moving it is easy; it mixes together with data from other places very nicely; it's very hard to make go away.

We'll touch on these in turn, but let's begin with the mixing. Once you start to record data in one place, it wants to be mixed with data from another. Take an Apple Watch, for example; the one on my wrist takes a measurement of my heart rate at regular moments. My watch also knows where I am, through GPS, and who I have meetings with, through my calendar. Through LinkedIn and other social networks, it can infer a person's real-life identity.

Now, we know that interactions with deeply frustrating people will raise your heart rate, so when you combine all that



Details of more than 33 million accounts were stolen from the website Ashley Madison

TOP 10 MOST FREQUENTLY EXPLOITED CATEGORIES OF WEBSITES IN 2014

1	Technology	21.5%	6	Entertainment	2.6%
2	Hosting	7.3%	7	Shopping	2.5%
3	Blogging	7.1%	8	Illegal	2.4%
4	Business	6.0%	9	Placeholder	2.2%
5	Anonymiser	5.0%	10	Virtual community	1.8%

Source: Symantec 2014

data together, alongside the same data from other smartwatch wearers, we can start to build inferences on how annoying someone is by the physiological effects they trigger.

Useful data; a free idea for an app for anyone who wants to build it and not one that requires any new magical technology, merely connections made between stuff already out there.

With a lack of walls between databases and some published results appearing in the Google index, and we could be destroying reputations.

And destroying them forever, as the Ashley Madison user-base will find when someone turns that illegally released database into a Google-indexable website (something that might already have happened by the time you read this).

Once data has been created and released, it freezes that moment in time. The person you were when the data was created is the person you will always be as far as systems which act on that data are concerned. A foolish decision entombed in data can and will mark you for life. Indeed, that is one of the more subtle arguments against government internet surveillance – it makes it impossible for people to change their minds.

The point here isn't that law enforcement agencies shouldn't be allowed these tools at all – almost everything has its specific and limited place, given proper oversight and a democratic conversation beforehand – but that without those limitations and oversight, we end up with databases that are, because they are all, not only fundamentally insecure, but liable to produce, with that insecurity, deeper problems than they solve.

It is, for example, highly likely that the millions of personnel records of US gov-

ernment employees with security clearances that were breached last year will be checked by those who have them against the Ashley Madison database to ease the blackmail. Two sets of bad IT security combine with a lack of the understanding among the general public that databases will be cracked and choices made in private will not remain so. In an era where most choices are made via weakly secured digital systems, privacy cannot be taken for granted.

We need, as a society, to not only demand and utilise better security practices in the companies and organisations which are large in our lives, but to develop a cultural understanding that without those practices, we risk whole new ways of bringing damage to ourselves and each other.

This is only going to get worse before society learns to deal with it. Technology evolves at a pace that far outstrips the evolution of etiquette. I'm wearing a constant heart-rate monitor, yes, but I've also inadvertently installed video cameras and microphones in most rooms of my house, not least by my bed, where our phones rest at night. My car downloads firmware updates from the internet and my groceries are delivered because of the choices sent from my phone. The lights in my front room, the stereo on the bookshelf and the robot that feeds the cat are all connected and vulnerable, and liable to betray me in a new and unforeseen way. It won't be a surprise that they do, only how they do it.

Being paranoid about the security risk and jettisoning modern technology entirely would be foolish. You would be secure from new and baroque security threats, yes, but you would also be removing yourself from modern society. Instead, we need to live within a new metaphor. Cyber security shouldn't be thought of in terms of walls, fortresses and weaponry to use against an invader. Instead, it should be

considered more in the terms of hygiene and health.

We're going to get sick every so often and sometimes it will be very unpleasant. But if we eat well, wash our hands and don't eat food off the floor, we'll be mostly alright. And when we're not, it is society's responsibility to help us get over it – and not carry the mark of sickness forever more.

“Once data has been created and released, it freezes that moment in time – a foolish decision entombed in data can and will mark you for life”

Share this article on social media via raconteur.net

VALUE OF INFORMATION SOLD ON BLACK MARKET

\$0.50 - \$10
1,000 stolen e-mail addresses

\$0.50 - \$20
Credit card details

\$1 - \$2
Scans of passports

\$2 - \$12
1,000 social network followers

\$7 - \$8
Stolen cloud accounts

\$10 - \$15
Stolen gaming accounts

Source: Symantec 2014

COMMERCIAL FEATURE

DEFEND YOUR ORGANISATION AGAINST CYBER CRIME

Threats from cyber criminals are more sophisticated than ever and as they become faster and smarter, stronger solutions are required for organisations of all sizes in both the public and private sectors



THE ENEMY HAS KILLER INSTINCTS

Cyber crime is highly organised and funded. Once criminals realised that the internet could be used to steal money, either through scams or directly through financial companies' websites, there was no stopping the growing number of attacks.

Even with organisations reportedly spending \$71.1 billion on information security in 2015, they can't keep up with threats changing at a rapid pace. As security software is upgraded, fraudsters work on new ways to exploit weaknesses in an organisation's defences. For IT teams, it's a brutal match-up and for chief executives it's a genuine threat to business.

HELPING SECURITY TEAMS ROLL WITH THE PUNCHES

Hexis Cyber Solutions is a business which leverages years of cyber security expertise to help organisations combat threats infecting their systems. The company's flagship product is HawkEye G, an integrated approach to threat detection, verification and response by leveraging flexible, policy-based responses to mitigate threats before compromise.

The solution leverages end-point and network sensors, as well as third-party integrations such as FireEye and Palo Alto Networks, to detect threats and attacks against a system. From there, the product includes proprietary technology called ThreatSync™ to verify threats against sources including, but not limited to, threat feeds, MD5 files and host heuristics, and sensor data. This results in decreasing the number of ghost alerts and false positives. Through policies, HawkEye G offers automatic or machine-guided remediation tactics including kill process, file quarantine and more.

"The state of play is moving so fast, it's difficult to use hyperbole," says Kane Hardy, Hexis vice president, Europe, Middle East and Africa, explaining the current cyber-crime environment. "In the United States, we see the number of organisations breached increase on an almost weekly basis. It is happening in the government as well other industries, including seemingly benign entities that historically would not expect to be targeted. It's true that no one is really safe from the threat of a breach these days.

“Hexis is an established, global business comprised of a team of highly skilled and experienced cyber security specialists”

"We would be foolish to say it's not happening in the UK too. Financial services organisations are seeing growing numbers of attacks and, in some cases, full-fledged breaches. It could be denial of service attacks, preventing access to business services or it might be a breach where data is actually compromised."

According to Mr Hardy, part of the problem is that organisations fail to keep up with threats that are changing all the time. Often, he says, Hexis is called in to help companies in the midst of an attack even though the targeted company thought they were covered by their existing security systems.

"The threat is progressing at such a rate that old solutions simply don't work. Organisations are deploying the same technologies that were around 20 years ago, while threats are often automated and designed to change instantly and on their own," he says.

HEAVYWEIGHTS DEPLOY CONTINUOUS DETECTION AND RESPONSE

Hexis is an established, global business comprised of a team of highly skilled and experienced cyber-security specialists. The company recruits people with extensive experience in actively defending commercial and government organisations.

"What makes our company unique is that we solve three key problems that security professionals have communicated to us which include lack of complete enterprise visibility, false positives and lack of security professionals. We feel we're ahead of the game and able to offer

organisations tangible return on investment and risk-management value today, something that's really quite scarce with cyber security technology," says Mr Hardy.

"HawkEye G is unique as a total solution that protects both the network and the end-point, as well as integrating with third-party technologies for greater threat intelligence. Everyone will be going in this direction in the next couple of years. But Hexis has something that is truly next generational today."

For IT teams it's a no-brainer. Chief executives and finance directors are on board too, says Mr Hardy. For non-techies, cyber security can be a reluctant investment and, if the product works, there is little sign of a tangible benefit. Like insurance, it's only when security slips that the need becomes clear.

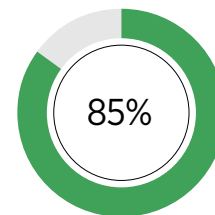
The alternative is a high-level risk to business that is ever-present. This risk threatens business reputation, makes sensitive data leaks possible and can severely damage profitability. Mr Hardy points to the example of the US department store Target, which experts suggest has lost a nine-figure monetary amount due to compromised data.

"It came through a straightforward advanced cyber attack," he says. "It was discovered by tools that are great at discovering attacks, but there were no tools in place to defend and take action against that threat. That's why the business suffered."

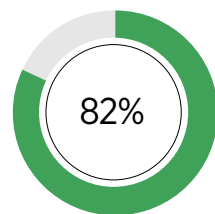
Mr Hardy concludes that Hexis will continue to invest in its product portfolio, including HawkEye G, and will address new threats as they emerge. His advice to organisations planning to avoid what has happened to global corporations is to implement a strategy that incorporates an integrated and active defence – and not one that simply identifies threats.

Get the full case study and more at go2.HexisCyber.com/FightingFraud or e-mail info@hexiscyber.com www.hexiscyber.com

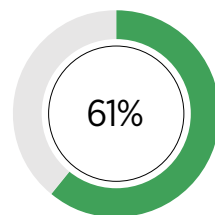
ARE HACKERS HITTING BELOW THE BELT?



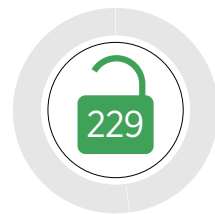
of survey respondents still perform some type of manual log analysis for the identification of threat incidents
Source: 2014 SANS Incident Response Survey



indicated that malware is the most common incident type affecting their organisation
Source: 2014 SANS Incident Response Survey



of all chief executives surveyed are concerned about cyber threats, including lack of data security - up from 48% in 2014
Source: PwC.com CEO Survey



days on average of dwell time for hackers lurking within your environment to steal data before being detected
Source: Mandiant 2014 Threat Report

CASE STUDY

Protection Group International (PGI) is an intelligence-led risk management provider that brings together unique capabilities in the vast field of information security for the commercial, institutional and government sectors.

The in-house security team at PGI faced the same problem that many companies in the UK and around the world are up against – how can we optimise the team we have to be more efficient, yet still improve the security of our systems?

With the shortage of cyber-security professionals only expected to grow over the next five years, PGI decided to take a look at Hexis Cyber Solutions' flagship product HawkEye G.



"HawkEye G enables us to leverage the skilled staff we already have in an even more effective way," explains Brian Lord, PGI managing director. "With the HawkEye G solution, we can be sure that our internal IT infrastructure is even more secure with a 24/7 active cyber-defence posture, without worrying about adding yet more, nearly impossible to find resources. So my defence is improved without the commensurate of delivering it."

Profiling the UK's financial

High-profile cases of financial fraud may help to piece together an identikit picture of criminals who cheat their way to riches

◆ FINANCIAL SERVICES FRAUDSTERS
● CHARLES ORTON-JONES

LIBOR RIGGER
TOM HAYES



The inter-bank lending rate is so obscure even the regulators overlooked it as a possible source of fraud. How on Earth could the Libor be tinkered with? In fact, as Tom Hayes proved, it was a goldmine for unscrupulous traders.

The Libor is the average rate at which banks in London lend to each other. Banks report their daily position in order for an industry average to be estimated. Traders realised there was no verification process. If they held a trading position which could be affected by the Libor, it was simple and profitable to falsify the numbers.

During his trial, Hayes revealed just how lax controls were. He was quoted in 2006 as saying: "Just give the cash desk a Mars bar and they'll set wherever you want."

When rumbled, Hayes openly admitted his activities, but energetically claimed exceptional circumstances. He told the Serious Fraud Office: "We'd had no compliance training. We'd had no rules outlined to us, either internally or externally." The temptation was too great. "Not even Mother Teresa wouldn't manipulate Libor if she was setting it and trading it," Hayes said.

Does he deserve sympathy? Hayes claimed his actions were routine. "I knew I was operating in a grey area. I knew that I probably shouldn't do it but, like I said, I was participating in an industrywide practice at UBS that pre-dated my arrival and post-dated my departure." The judge disagreed. Hayes, 35, was handed down a 14-year prison sentence for his Libor illegality.

DARK-WEB HOST
NICHOLAS WEBBER

Prison deters? Not for this stubborn character. Nicholas Webber was sent to jail for running a criminal website. Once inside, he joined the prison IT course and then set about hacking the prison's IT system. He got caught and his teacher got the boot.

The prison authorities should have known better than to let Webber near a PC. Webber once boasted he was "probably the most-wanted cyber criminal just now" for founding one of the inter-



net's biggest hubs for fraud.

After leaving school, where he was reprimanded for deleting friends' detention records from the school computer, Webber set up GhostMarket, a global auction house for illicitly obtained financial details. Prosecutors claimed GhostMarket hosted 8,000 members, who discussed the manufacture of computer viruses for stealing financial data, for buying and selling stolen credit card details, and to collaborate on more elaborate frauds. Police were able to identify £473,000 of losses

from 3,500 cards sold on GhostMarket, but estimated the true figure could be £15 million.

Webber was undone when using a stolen card to pay for a penthouse suite at the Hilton Hotel in London's Park Lane. He received a five-year sentence for his crimes, but no extra penalty for his shenanigans perpetrated while inside.

GhostMarket is a reminder of how big and lucrative the global fraud after-market has become. Hackers can quickly find buyers for stolen financial data. Sadly, shutting down sites such as GhostMarket has little impact. Replacements rise in their place overnight.

CITY WHIZZ KID
ALEX HOPE



Self-styled foreign exchange trader Alex Hope hit the headlines three years ago when he splashed out £125,000 on a double Nebuchadnezzar-sized bottle of Ace of Spades champagne in a Liverpool nightclub. It arrived to the theme tune from 2001: A Space Odyssey. The picture of him lording it with soap-opera starlets made him famous overnight.

Aged 23, he hired a public relations company to position him as a master of foreign exchange (FX) markets. He was the whizz kid with a seemingly golden touch. His story? He claimed to have started off, at the age of 19, with just £500 and to have doubled this on day one of his FX trading career. He then traded his way to millions.

In truth, he was running a crude, but effective, scam. The publicity sucked in around 100 investors who trusted him with more than £5 million. New investors bailed out earlier ones: a classic Ponzi scheme struc-

PROFILE OF A FRAUDSTER



Is there such a thing as a typical fraudster? It would be convenient if there were. Security agencies and the police would be able to focus their efforts more sharply. Victims could be more wary.

"We've discovered there is an age range at which people become more susceptible to committing fraud," says Mark Kenkre, head of fraud at law

firm DWF, which specialises in complex fraud disputes. "They are in their mid-30s to mid-40s. They tend to be in a position of responsibility, with a degree of autonomy, as this gives them the chance to commit fraud. They have financial pressures. That age range therefore has the opportunity and the motivation." There is a gender factor. "In

terms of our investigations over ten years, we've seen a male bias." And a career factor, too. "Fraudsters tend to be in a position to procure services, so we find them more in finance and sales than other departments. They tend to have been with their company for a period of time, maybe five to ten years. They are embedded."

Naturally, these trends are correlations, not guides. One curious detail is that white-collar criminals often don't see themselves as malefactors. They bend rules or "borrow" funds with a view to repaying them quickly and then escalate from there. It's rarely their fault, so they claim.

In *Dishonest Dollars: The Dynamics of White-Collar Crime*,

Terry L. Leap charts the extraordinary refusal of office workers to admit wrongdoing, even to themselves. "Some perpetrators deny culpability even in the face of overwhelming evidence to the contrary," he writes.

"The defence strategy during the trial of Kenneth Lay and Jeffrey Skilling was simply to deny that any wrongdoing occurred

tricksters

– and end up in jail

ture. Hope filched £2 million. With no qualifications and a paper-thin story, it was only a matter of time before he was nailed.

The Financial Conduct Authority (FCA) investigated him and quickly uncovered his plot. In January, Hope was jailed for seven years. Georgina Philippou, acting director of enforcement and market oversight at the FCA, warned: “He promised fantastic returns but, as is so often the case with unauthorised investment schemes, those who invested ended up with significant losses and the main beneficiary of the scheme was Hope himself. There is a reminder for consumers here that unauthorised investment schemes are often incredibly risky and, if the promised investment returns seem too good to be true, they most probably are.”

BLACKMAILER LEWYS MARTIN

Phishing is a common fraud technique. Hackers create e-mails which look identical to official messages. They send them to the victim, encouraging their target to click on a link and input “login” details. These are then used by the hacker to gain access to the victim’s real account.

Cyber hacker Lewys Martin executed an efficient phishing operation on Halifax bank customers. It is believed he gathered the details of 28,000 customers by using fake e-mails.

Martin then blackmailed Halifax bank, demanding ten bitcoins for every account he had compromised, a total value of £207,000. Halifax bank, owned by Lloyds Banking Group, refused to co-operate and went to the Metropolitan Police Cyber Crime Unit. Martin believed he had covered his tracks by using software to hide his identity. The police quickly broke his cover and arrested him, seizing his machines which were loaded with varied incriminating evidence. He was jailed for four years and two months.

Scotland Yard’s detective chief inspector Jason Tunn said: “We are determined to track down and prosecute cyber criminals who seek to defraud businesses and residents of London. Martin was not able to defeat the bank’s security systems, but instead chose to target his phishing ac-

tivity at retail customers.”

The case illustrates the challenge facing banks. Even if their own systems are foolproof, the naivety of customers can expose the system to a breach.

Fraudsters are known to contact victims by phone, posing as bank staff – a variation known as vishing. There is also an approach via SMS text messages, called smishing.

ROGUE TRADER KWEKU ABODOLI



The triangle of fraud comprises opportunity, motive and rationalisation. Kweku Adoboli’s fraud contained all three elements. The former public schoolboy and son of a United Nations diplomat seemed to be a model citizen. He rose the up the ranks at UBS.

Detective chief inspector Perry Stokes, from City of London Police, said: “To all those around him, Adoboli appeared to be a man on the make whose career prospects and future earnings were taking off. He worked hard, looked the part and seemingly had an answer for everything. But behind this façade lay a trader who was running completely out of control and exposing UBS to huge financial risks on a daily basis.”

Adoboli’s downfall was spread betting on financial markets. He lost money, until his £350,000 wasn’t enough to cover the bills. He resorted to pay-day loans. Then, as so many gamblers do, he chased his losses with increasingly desperate bets. In order to avoid reprimands for his poor performance, he created secret trading accounts. These let him avoid limits on the size of his positions. A six-figure loss grew larger. At one point, Adoboli was at risk of losing £7.4 billion. Jurors were told he was “a gamble or two away from destroying Switzerland’s largest bank for his own gain”.

The loss to UBS was £1.4 billion – the biggest fraud in UK history. Adoboli was sentenced to seven years, in 2012, but has already been released on parole. His story prompted a wide review of compliance rules across the UK and Switzerland.

Share this article on social media via raconteur.net



Expenses Fraud: Three key questions to ask yourself

Expenses fraud is an unfortunate reality for UK businesses of all sizes. Sometimes an employee just doesn’t understand the company’s policy, but in some cases, erroneous claims are made more deliberately. And, with the overall challenge of enforcing policies, fraud is an issue that hits many companies’ finances.

Can you say “yes” to these three questions?

- Does your company have a documented and easy-to-understand expense policy document?
- Do employees and their managers know which claims fall out-of-policy, and do managers return out-of-policy claims to employees with confidence?
- Do you know the warning signs of a fraudulent expense claim?

If you’re not sure you can say “yes” to all the questions, find out how you can avoid expenses fraud at: concur.co.uk/visibility



at Enron. Instead, their attorneys blamed the energy company’s fall on adverse newspaper reports, short-selling investors and a market panic that caused Enron shares to plummet. Even after a Houston jury convicted Lay and Skilling on a total of 26 federal conspiracy and fraud charges, both former CEOs steadfastly maintained their innocence.”

◆ THIRD-PARTY RISK

● CATHERINE BAKSI

Historically, the requirement for local fixers to grease the palms of government officials and business associates to secure lucrative deals was seen as an accepted part of doing business in some foreign jurisdictions.

If any potential wrongdoing came to light by an agent working in a foreign land, company directors sitting on the other side of the world could comfortably deny all knowledge and safely escape censure.

But those days are gone. As novelist L.P. Hartley wrote: “The past is a foreign country; they do things differently there.” Jurisdictions across the globe are tightening up laws to eradicate corrupt practices.

In the UK, the Bribery Act 2010 came into force with great fanfare in July 2011. It created a new offence of bribing a foreign public official and, most importantly for companies, a corporate offence of failing to prevent a bribe being paid on their behalf by an “associated” person.

The offences and the extra-territorial effect of the act make it one of the most stringent anti-corruption laws in world, and have made it much harder for companies to turn a blind eye to bribery and corruption.

The legislation catches offences committed anywhere in the world by companies incorporated in the UK or carrying out any part of its business here.

Under section seven, a commercial organisation commits an offence if a person associated with it bribes another person with the intention of obtaining or retaining business or business advantage for that organisation.

“

The Bribery Act catches offences committed anywhere in the world by companies incorporated in the UK or carrying out any part of its business here

”

Associated persons can be individuals or entities who perform services on behalf of the company, be they employees, agents or subsidiaries.

They could range from a sales agent giving back-handers to win commissions, a lawyer bribing a judge to secure an outcome beneficial to the company, or associates acting to speed up administration or secure favourable treatment from tax authorities.

Crucially, knowledge of the bribe on the part of the organisation is not required. Companies can fall foul of the law by failing to have “adequate procedures” in place to prevent bribery.

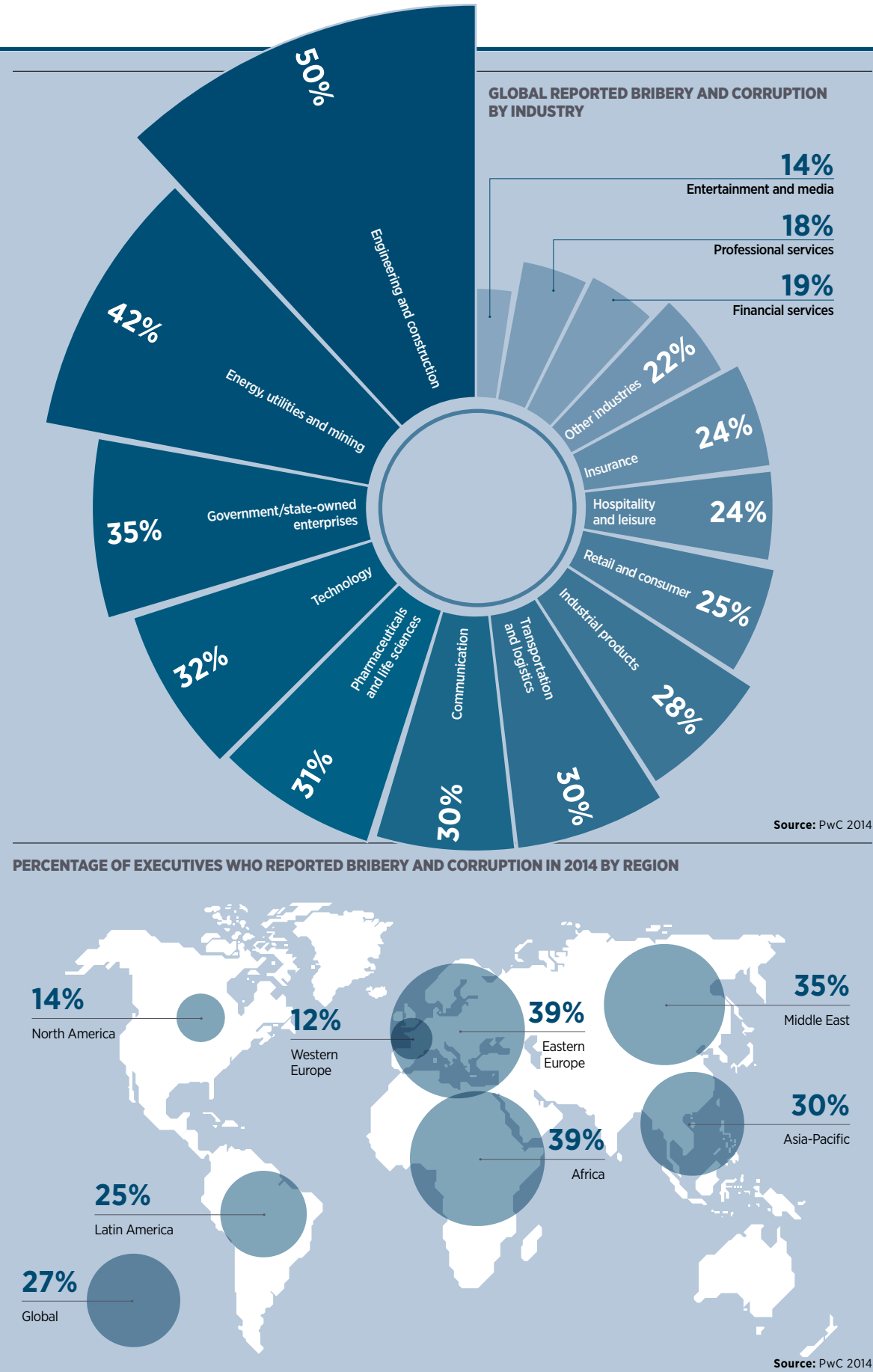
As David McCluskey, partner at boutique London law firm Peters & Peters, says: “It is intended to ensure people work as though they are sitting in central London, not central Africa.”

In emerging markets, such as Brazil, Russia, India and China, the risks in using local representatives or agents can be particularly high.

And corporates cannot afford to be complacent about it. In addition to huge fines and prison sentences, convictions could result in debarment

Perils of third-party corruption abroad

Using agents and partners abroad can open up UK companies to the risk of corruption which is now punishable under stringent international anti-bribery laws



from tendering for public sector contracts and disqualification from being a company director, not to mention the consequential reputational damage and loss of business.

A recent report from accountancy firm Deloitte showed that third-party failure could cause shareholder losses of up to ten times any regulatory fine and share prices to drop by 2.55 per cent.

In recognition of the fact that no anti-bribery regime will be capable of preventing all offences, the act provides a full defence if a company can show it had “adequate procedures” in place to prevent bribery.

Adequate procedures are not defined in the act, but are the subject of government guidance centring around six principles: proportional procedures; top-level commitment; risk assessment; due diligence; communication, including training; and monitoring and review.

Companies have scrambled to put in place compliance regimes, which they hope will afford them protection from prosecution, if those acting on their behalf are caught out.

In reality, says Mr McCluskey: “It means having a visible and well-documented anti-bribery policy effectively disseminated to all staff and agents, a reporting hotline and procedure, with whistle-blower protection, and a hospitality register requirement.”

Every transaction now, says Jonathan Hitchen, partner at international law firm Allen Overy, contains anti-bribery warranties and termination clauses.

In some jurisdictions it is impossible to remove the risk by doing away with agents as in some countries having a local partner is required, notes Jeremy Cole, consultant in the London office of global law firm Hogan Lovells.

“The challenge when entering new markets is to check them [the local partners] out to see if they could cause harm to the company and expose it to criminal prosecution in the UK,” says Mr Cole.

Dan Hyde, partner at London lawyers Howard Kennedy, says: “Organisations need to examine the relationship with any overseas third party carefully and apply due diligence to ensure, as far as possible, they are choosing the right third-party representative and that the risk is not too great.”

Equally as important as looking at new intermediaries, adds Mr Cole, is the need to go back and look over historic relationships that may have been put in place under a less stringent regime.

ANALYSIS: BRIBERY ACT TO DATE



Introduced by the Coalition Government in 2011, the Bribery Act 2010 was the biggest reform of UK anti-corruption law, sweeping away a myriad of disparate and ancient offences, and setting a global gold standard.

The then Justice Secretary Kenneth Clarke heralded it as an “important step forward for both the UK and UK plc”.

He said: “At stake is the principle of free and fair competition, which stands diminished by each bribe offered or accepted.

“Tackling this scourge is a

priority for anyone who cares about the future of business, the developing world or international trade.”

The act introduced four key offences: offering or giving a bribe; accepting a bribe; bribing a public official; and failing to prevent a bribe.

Susannah Cogman, partner at global law firm Herbert Smith Freehills, recalls that when it first came into force, attention focused on fears the legislation might spell the demise of corporate hospitality.

Since then the focus has shifted to the number of prosecutions, or rather the lack of them.

The Crown Prosecution brought the first prosecution in 2011, somewhat ironically against a magistrates’ court clerk who pleaded guilty to taking a £500 bribe for making a speeding charge disappear. Two other cases followed concerning bribes by a man who had failed his driving test and a postgraduate student who had failed a dissertation. Hardly the stuff to send shock waves through UK plc.

And although the Serious Fraud Office (SFO) has secured prosecutions against two tricksters involved in a £23-million scam to dupe investors into putting their money in a biofuel scheme, there have been no corporate prosecutions and no deferred prosecution agreements (DPAs).

However, the SFO confirms there are Bribery Act investigations underway, although it is unable to give “fixed numbers”.

The SFO has further indicated that the first invitation letters have been issued in relation to DPAs and it anticipates two will take place before the end of the year.

Lawyers believe there are many reasons why enforcement activity has been slow.

Ms Cogman points out that the act has only been in force for four years and does not apply retrospectively. In addition, it takes time for offences to come to light and investigations are lengthy.

William Christopher, partner at London law firm Kingsley Napley, compares the UK legislation with the US Foreign and Corrupt Practices Act. “It came into force in 1977, but it took five years before the first prosecution and didn’t get going until the 1990s,” she says.

While the record of enforcement may have been far from impressive, it would be a mistake to judge the act solely on that basis. It has resulted in a sea change in the attitude of corporates to anti-bribery compliance, spawning a mini industry in compliance, and putting the issue high on the agenda of boards of directors.

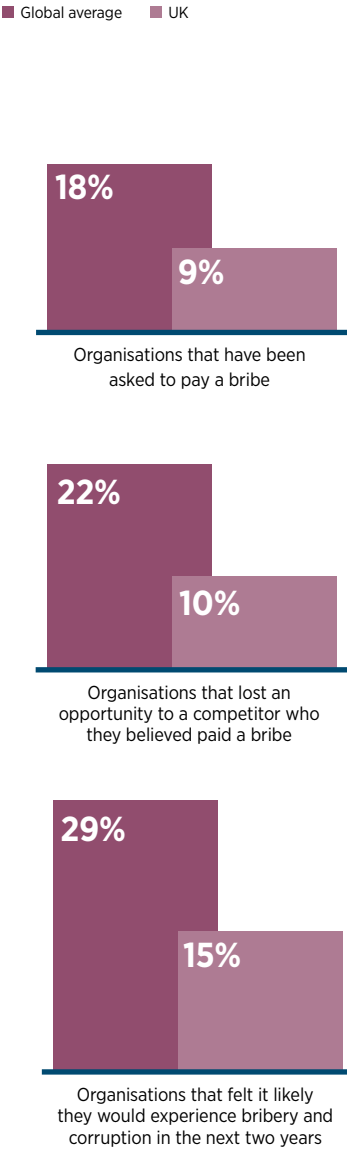
Lawyers are inclined to give the enforcement agencies more time to show their teeth. It remains a credible story for the SFO to say it has a bank of investigations, but warns Jo Edwards, a partner colleague of Mr Christopher at Kingsley Napley: “You can’t keep saying, ‘we’re working on it.’”

The level of due diligence required, explains Michelle de Kluyver, counsel at Allen & Overy, is risk-based and will depend on the jurisdiction and nature of the deal.

Transparency International’s *Corruption Perception Index* is a guide to the jurisdictional risks. It ranks countries and territories based on how corrupt their public sector is perceived to be. In the 2014 table Denmark comes out as the least corrupt country, while at the bottom of the list, ranked in position 174, is Somalia. The UK sits in position 14.

Industries regarded as posing the high-

UK EXPERIENCES LESS BRIBERY THAN THE GLOBAL AVERAGE



Source: PwC 2014

“Companies doing business in the United States need to be alert to the provisions of the US Foreign Corrupt Practices Act, which many view as far more demanding

est risks include energy, mining and defence. Mr McCluskey comments: “Extraction activities tend to take place in areas where the rule of law is non-existent and natural resource has always been ripe for bribery.”

The due diligence, says Mr Hyde, includes assessing the level of corruption in a country, the risk associated with the particular sector, the proposed third party, the level of government involvement, and a myriad of checks to investigate the reputation and reliability of the third party and the transaction contemplated.”

This, says Ms de Kluyver, can range from basic verification and ownership checks to very detailed reports on business and people’s reputations which, adds Mr McCluskey, may have spawned

a “secondary industry of validation of partners and local vendors”.

“Some jurisdictions and sectors may be viewed as posing too great a risk; there are still regions, developed and undeveloped, where grease payments and bribes are deep rooted in both commerce and culture,” says Mr Hyde.

In such circumstances, the ultimate protection, says Mr Hitchen, is to make the tough decision to not do the deal.

Since the UK Bribery Act came into force, there have been no prosecutions brought by the Serious Fraud Office (SFO) against companies. The prosecutor states there are a number of ongoing investigations, including into UK pharmaceutical giant GSK, Rolls-Royce, French energy and transport conglomerate Alstom, and oil and gas company SOMA, although it cannot disclose what they are about.

Aside from the Bribery Act, companies doing business in the United States need to be alert to the provisions of the US Foreign Corrupt Practices Act, which many view as far more demanding. In addition, there is a trend in many countries to take enforcement action locally, either for political or revenue reasons, or through a genuine desire to stamp out corruption.

The SFO’s investigation into GSK followed its fine of \$490 million (£297 million), having been found guilty in China of bribing doctors and hospitals to use its products.

So the anti-corruption climate is hotting up. As Mr Cole at Hogan Lovells concludes: “Major companies doing business around the world must be alive to the fact that they have to look over their shoulder in a number of different directions – a number of anti-bribery laws may apply even though the activity is not taking place in that country.”

Share this article on social media via raconteur.net

Drive change in your users' security behaviour

If phishing is a top security concern for your organisation, try the PhishMe method to lower your users' susceptibility to the most prominent threat vector-email.

PHISHME
www.phishme.com

++

81% of large UK companies suffered a cyber security breach in 2014*

Are you prepared?

-
-
- **Cyber Incident Response Services from MWR InfoSecurity**

The ability to rapidly identify and contain cyber security incidents has a direct influence on the impact of a breach.

MWR's specialist incident response team is equipped with industry leading tools and intelligence to handle any cyber security incident, large or small. Supported by 24/7/365 access to our Emergency Incident Response Hotline, you will never be without the expert support your business needs.

24/7 Cyber Incident Response Hotline:
T: +44 (0) 330 223 3292

To find out more go to:
W: mwr.to/incidentresponse

W: mwrinfosecurity.com

*UK Department for Business Innovation and Skills, 2014



Cyber spies target

States that launch cyber attacks no longer only target other governments and

◆ STATE-SPONSORED CYBER ATTACKS ● DAVEY WINDER

The global *Breach Level Index*, to be published next week by Gemalto, reveals the number of state-sponsored cyber attacks accounted for just 2 per cent of data breach incidents during the first six months of 2015. However, the number of records compromised as a result of those attacks amounted to 42 per cent of the total.

Further, while none of the top-ten breaches from the first half of 2014 were thought to be state sponsored, three in 2015 were. These included the top two breaches at Anthem Insurance and the US Office of Personnel Management.

"State-sponsored attacks were the second highest source of data records loss, with 102.4 million, behind malicious outsiders responsible for 112 million," says Jason Hart, chief technology officer for data protection at Gemalto.

The days of such attacks being targeted purely at government organisations also seem to be over. According to threat forensics specialist FireEye, during the first six months of 2015 there have been considerably more state-sponsored cyber attacks on the private sector (87 per cent) compared with the public sector (13 per cent). The common link between all such attacks is the sensitive nature of the data targeted.

Nick Coleman, the global head of cyber security intelligence services with IBM and a former national reviewer of cyber security for the UK government, explains that all sensitive information "has an economic value and can be sold

as a commodity whether it's health records, credit card information or intellectual property".

The motive behind these attacks, therefore, will fall into one of three groupings: commercial (simple profit motive); strategic (disruption to infrastructure and brand reputation for economic or competitive advantage); and image related (propaganda value of brand damage).

Perhaps the biggest danger for any business, no matter which sector it operates in, is thinking its data isn't sensitive enough to be of any interest. "Companies such as HR outsourcing are seen as a stepping-stone for an attack on more critical

targets," warns Klaus Kursawe, chief scientist at the European Network of Cyber Security.

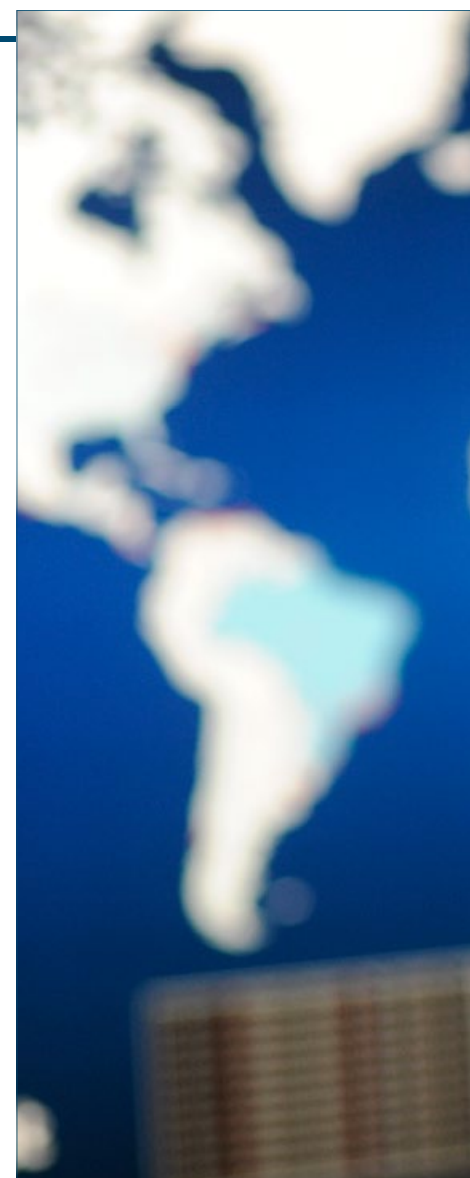
Since the intelligence community now embraces the concept of big data, there is also a tendency to collect as much stolen data as possible and mine it for

usable insights. Then there's the possible advantage of inflicting collateral damage through an attack on the private sector to consider.

"A targeted attack against the finance industry could not only cause significant disruption to the economy, but also stoke civil unrest if it affects enough of the domestic population," says Chris McIntosh, chief executive of security and communications company ViaSat UK and a retired lieutenant colonel in the Royal Signals.

Indeed, Colonel McIntosh argues that cyber is increasingly the first weapon of choice in low-level conflict as it's relatively cheap and very effective. The same arguments come into play when you consider why state-sponsored cyber attacks against organisations are

“Perhaps the biggest danger for any business, no matter which sector it operates in, is thinking its data isn't sensitive enough to be of any interest”



now becoming so commonplace, with the added factor of also being relatively low risk.

"Since a cyber attack is essentially anonymous or at any rate very hard to attribute," he explains, "it's easy for coun-

SECURITY LAPSE LET CHINA IN



In late-2014, a Japanese manufacturing company covering everything from automotive production lines to micro-electronics assembly and with European operations centred in the UK was the target of a suspected state-sponsored attack.

The incident consisted of malicious e-mails containing malware that appeared to have been sent from two long-standing and trusted UK employees to chief design engineers and executives in Japan. The e-mails used social

engineering techniques, based on company product information, to entice the recipients to open and execute a malicious attachment. This contained a remote administration tool or RAT which called back to a Chinese IP address and had resulted in two infected systems that ultimately led to design schematics and advanced earnings reports being stolen.

Following the breach, impacts to the company were felt in stock price variations and over the longer term the company expects further lost earnings potential as design secrets are incorporated into com-

petitor lines. It is likely that because strategic intellectual property had been stolen, the company will have to significantly alter future lines to ensure they remain competitive.

The malicious e-mails had bypassed normal security scanning as they were internal communications, yet the employees concerned had not sent them. MWR InfoSecurity determined that a fake malicious wi-fi access point had been operating near the company's stand at a British trade show, and this intercepted requests to the company domain and then redirected them to a fake Outlook

web access page. From there, the user credentials were stolen as they logged on to their e-mail and later used to conduct the internal targeted attack. The company carried out a thorough investigation to ensure attackers were extracted.

It was determined that the damages in this case were linked to Chinese interests and source indicators were linked to Chinese infrastructure. Since the incident, the company has implemented two-factor e-mail authentication and conducted user-awareness training to help identify malicious redirection of user traffic in the future.

t business secrets

now aim to steal valuable commercial secrets from the private sector



SUSPECTED STATE-SPONSORED MALWARE



Stuxnet
Computer worm discovered in June 2010, designed to disrupt machinery, such as those in nuclear power plants, by attacking industrial programmable logic controllers.



Duqu
Thought to related to the Stuxnet worm and discovered in September 2011, Duqu hunts for information that could be used in attacking industrial control systems.



Flame
Discovered in May 2012, Flame is designed to carry out cyber espionage by stealing computer display contents, files, data and even audio conversations.



Gauss
Discovered in August 2012, Gauss is designed to monitor online banking accounts by stealing browser history, cookies, passwords and system configurations.

tries to publicly deny responsibility for attacks while secretly sanctioning them through state-sponsored groups.”

Colonel Cedric Leighton, former deputy director for training at the National Security Agency, where he oversaw the training of America’s so-called cyber warriors, adds that you shouldn’t underestimate the influence of economic competitive advantage in this uptake of state-sponsored attacks.

“If these countries can develop a product without the sunk R&D costs a Western company would have, then they can offer it to the marketplace at a cheaper price,” he says. “That allows a country like China to continue its economic miracle for a bit longer.”

So we know what is being done and why, but that still leaves the question how does this differ from “traditional” cyber crime? The answer is, surprisingly, not much at all. Verizon’s *Data Breach Investigations Report* series reveals that two thirds of all attacks comprising cyber espionage over the past two years have featured phishing attacks, which usually combine social engineering tactics with malware.

However, state-sponsored attackers are typically more patient than other threat actors. “They don’t mind working slowly

on their target until they are able to gain their trust and successfully install malware on their machine,” says Laurance Dine, managing principal at the Verizon Investigative Response Unit. “This slow and steady approach differentiates state-sponsored attackers.”

It’s a fallacy to think that zero-days are used in every state-sponsored attack,

“
Two thirds of all attacks comprising cyber espionage over the past two years have featured phishing attacks, which usually combine social engineering tactics with malware

and actors will often use much the same criminal methodologies of targeted phishing e-mails and known exploits because they are so generic as not to be easily attributable to any specific group or nation state.

Indeed, Paul Pratley, who is head of investigations and incident response at MWR InfoSecurity, thinks that “only

when a company is highly mature in its security posture, is a high-value target and generic attacks fail, will they [the attackers] resort to using costly zero-day malware developed internally”.

Which just leaves us to ponder what can the average organisation do to detect and deal with state-sponsored attacks? Guillaume Lovet, threat response manager at enterprise security provider Fortinet, puts forward a three-point plan:

1. Make reconnaissance and replication (the identification and reproduction of your defence system) difficult by having complex, hidden, layered and varied defence systems.
2. Limit the attack surface for the initial infection vectors by having up-to-date systems which force an attacker to use less common and more costly zero-day exploits. The attack surface also usually involves people, so employee education is key.
3. Limit the propagation and persistence of the initial attack by having well-segmented networks and meaningful policies. For example, an accountant’s desktop should not have access to the company’s software codebase.

Share this article on social media via raconteur.net

DEATH TAXES CYBER ATTACK

THERE ARE NO LONGER ONLY
2 SURE THINGS IN LIFE

Many security solutions focus wholly on cyber attack prevention, but determined attackers will always find a workaround - prevention alone is not enough.

Countercept is a complete service for detection and response to advanced persistent threats (APT) and cyber attacks, run by one of the only independent security consultancies listed on the CESG Cyber Incident Response (CIR) Scheme. Built around endpoint threat detection and response (ETDR), it is delivered from our operations centre for 24/7 real-time monitoring of your assets.

Find out more:
www.countercept.com
+44 (0) 3302 230 434

COUNTERCEPT



SEEK TRUTH

FIRST YOU SEE WHAT THEY WANT YOU TO SEE. Then you apply world-class cyber forensics and an unmatched zeal for investigation. And soon, the truth is revealed. Learn more at strozfriedberg.com

STROZ FRIEDBERG