

# FIGHTING FRAUD

03

## DON'T LET THE CYBER FRAUDSTERS WIN THE WAR

A cyber-crime wave is engulfing UK companies – so fight back

08

## ROBBERS RIDING 'WILD WEST' WEB

Villainous fraudsters are robbing online shoppers and e-commerce

13

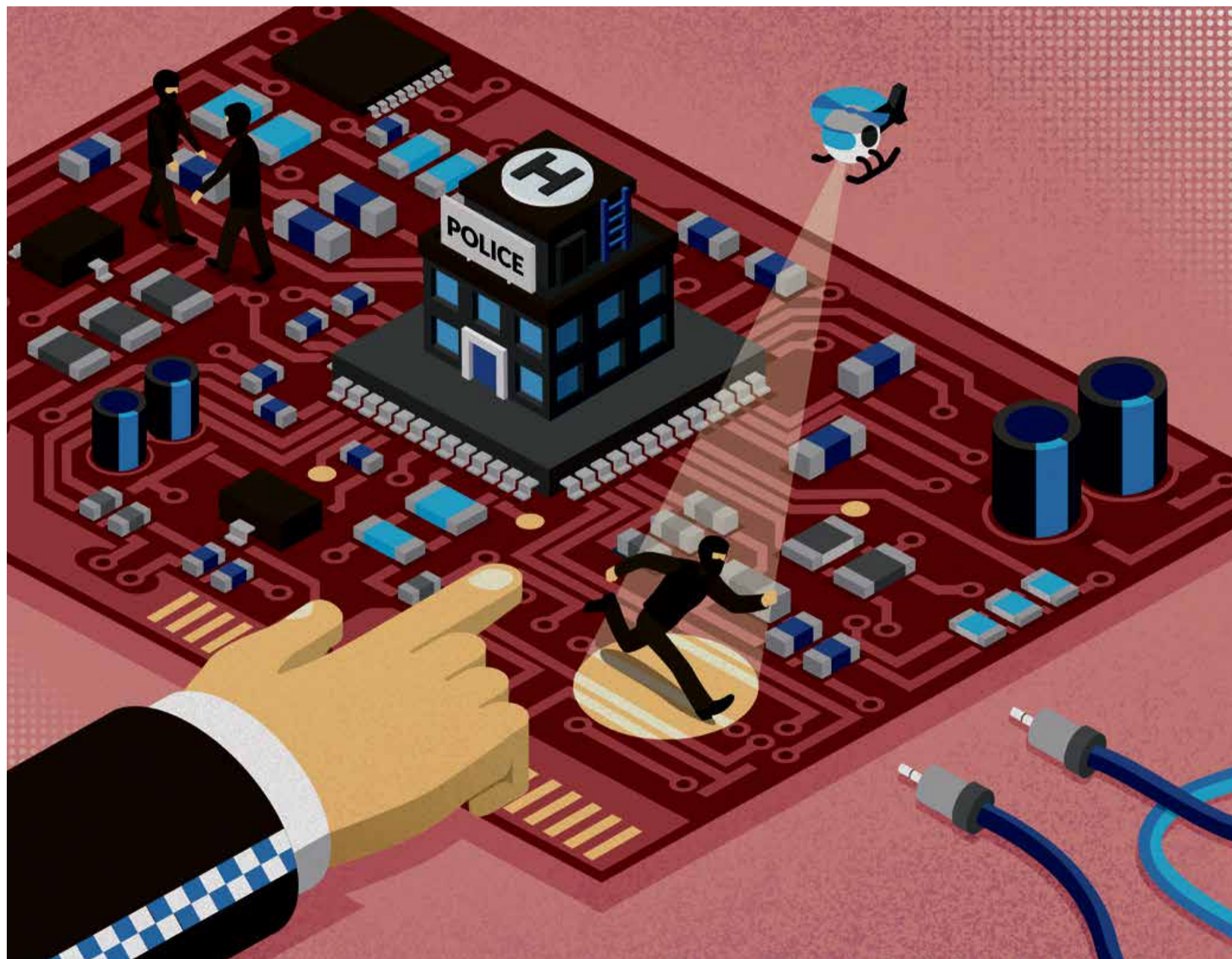
## IS CYBER CRIME A NIGHTMARE SCENARIO?

Chances are cyber crime will get worse before things get better

14

## ANTI-FRAUD TECH FOR THE DIGITAL AGE

Blockchain has the potential to eliminate common online frauds

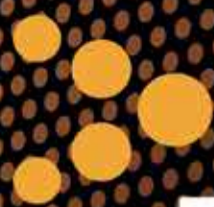


## BUSINESS DRIVEN SECURITY

Find out more about the RSA Security portfolio or take a trial now at [www.rsa.com](http://www.rsa.com)

# RSA®

@RSAEMEA



# BOOST SALES BEAT FRAUD™

ACCEPT MORE ORDERS, FROM MORE PEOPLE, IN MORE PLACES.

With Kount Complete™ you can:

- › Accept More Orders
- › Increase Bottom-Line Profits
- › Reduce Manual Reviews
- › Reduce Fraudulent Chargebacks

Visit [www.kount.com](http://www.kount.com) and download the 2016 Mobile Payments & Fraud Survey Report for free.



# FIGHTING FRAUD

DISTRIBUTED IN  
THE  TIMES

Raconteur	
PUBLISHING MANAGER John Okell	HEAD OF PRODUCTION Natalia Rosek
PRODUCTION EDITOR Benjamin Chiou	DIGITAL CONTENT MANAGER Lorna North
MANAGING EDITOR Peter Archer	DESIGN Samuele Motta Grant Chapman Kellie Jerrard

CONTRIBUTORS

- CHARLES ARTHUR**  
Author of *Digital Wars: Apple, Google, Microsoft and the Battle for the Internet*, he is a freelance science and technology journalist.

**HAZEL DAVIS**  
Freelance business writer, she contributes to *The Times*, *Financial Times*, *The Daily Telegraph* and *The Guardian*.

**DAN MATTHEWS**  
Journalist and author of *The New Rules of Business*, he writes for newspapers, magazines and websites on a range of issues.
- CATHERINE BAKSI**  
Former barrister and *Law Society Gazette* reporter, she is a freelance journalist writing for a broad range of law titles.

**ANTHONY HILTON**  
Author, journalist and broadcaster, he is a former City editor of *The Times* and managing director of *The Evening Standard*.

**DAVEY WINDER**  
Award-winning journalist and author, he specialises in information security, contributing to *Infosecurity* magazine.

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 8616 7400 or e-mail [info@raconteur.net](mailto:info@raconteur.net)

Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, health-care, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at [raconteur.net](http://raconteur.net)

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



# Don't let the cyber fraudsters win the war

A cyber-crime wave is engulfing UK companies, costing billions of pounds and calling for urgent counter measures

OVERVIEW

ANTHONY HILTON

It has long been said that nothing is certain except death and taxes, but perhaps the time has come to add a third certainty – corporate fraud.

A series of reports over the summer showed not only that fraud is more persistent than ever, but there are also more opportunities. The growth of technology, digitalisation, computer networks and the integrated nature of business, with its worldwide supply chains and customer relationships, has bought with it a whole range of new opportunities for corporate misbehaviour.

More money is spent today on compliance and fraud detection than at any time in the past, but the statistics suggest the forces for good are not winning the war.

The most successful criminal act thus far this year – at least among those which are known about – came in February when hackers penetrated the Swift banking network and extracted \$80 million belonging to the central bank of Bangladesh from its account with the Federal Reserve Bank of New York.

But this is in fact only a small part of the tens of billions which are lost every year. Indeed according to a report from accountants PKF Littlejohn, the annual cost of fraud in the UK reached £98 billion in 2015, while the *Global Economic Crime Survey 2016* published by PwC indicated that one in five UK companies had experienced a significant fraud in the last two years.

Globally PwC reported a double-digit percentage increase in crime against companies, with cyber crime the fastest growing segment. Worryingly, the rate of increase in cyber crime was worse in the UK than in most other developed countries.

What criminals get up to is an interesting mixture of the old and the new. Early in August, for example, came a warning that it was now possible to fly a drone close to a building to intercept corporate communications. Most companies have limited wireless security within their office because they assume no criminal can get close enough to compromise their systems.

But a drone adapted as a flying laptop could land on the roof and sit there intercepting guest wi-fi, Bluetooth-connected keyboards, the connections which enable contactless payment cards and much else, as easily in a private building as it could in a public café.

The counter measures are a similar mix of old and new. A business in California specialises in knocking drones out of the sky by bombarding them with radio waves. Police in Holland have a low-tech solution. They have reportedly trained an eagle to swoop and grab them with its talons.

Whole industries are under pressure. According to the World Federation of Advertisers, the marketing departments of corporations could waste more than \$50 billion a year by 2025 because of “the endemic fraud” in digital advertising. Here the problem is that fraudsters have found ways to use a computer to fake the online behaviour of a human. Advertisers normally pay per click and are duped into running campaigns on websites where the only visitors are “bots”, computer programs which pretend to be people.

But the old frauds persist too and on a scale which is chilling. A recent UN report highlights how developing countries have been deprived of billions of dollars by the faking of invoices which cover the export of their commodities. It alleges, for example, that while Zambian accounts showed copper exports worth \$28.9 billion went to Switzerland over the ten years to 2014, none of this showed up in Switzerland’s books. Likewise \$16 billion of copper apparently left Chile for Holland, but there is no record of it arriving. Fake invoices are perhaps the oldest trick in the book, but still obviously effective.

Whatever the source of data, two things stand out for companies to note. The first is that though external fraud captures the headlines, between a third and a half of the discovered crimes are carried out by insiders taking advantage of their trusted relationships and ease of access to sensitive data.

Interestingly long-serving employees are the worst offenders, much more so than juniors, and there has been a marked increase in “silver fraud”, crimes carried out by the over-50s. These are usually people who have been with the company for decades, but feel they are no longer appreciated, are being passed over for promotion and think they earn less than they deserve. PwC reports that 18 per cent of UK frauds were carried out by senior management.

The other thing to note is the haphazard nature of fraud detection. One in five British companies never do a fraud risk assessment while about half carry one out annually. But when it comes to catching people, PwC says 22 per cent were detected by suspicious transaction monitoring, against 14 per cent by the formal fraud risk management system. The three other significant ways frauds were uncovered, each in 8 per cent of cases, were data analytics, internal audit and by accident.

Clearly no one can afford to relax, but it helps to make sure employees have to. One of the oldest, but still most effective, fraud detection devices is to insist everyone takes at least two weeks’ holiday. Even with modern technology, it is hard to conceal a fraud in the UK when lying on a Spanish beach.



1/5

of UK companies experienced a significant fraud in the last two years

Source: PwC 2016

## Cyber criminals are targeting your 'Crown Jewels'

An attack on your mission-critical information can happen at any time



Information  
Security  
Forum

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.

Develop end-to-end protection and find the right solution for your organisation at:

[www.securityforum.org](http://www.securityforum.org)

# Machines can learn how to spot fraud quicker than people

With increasing volumes of online financial transactions, businesses are turning to artificial intelligence to catch fraudsters in the act

### ARTIFICIAL INTELLIGENCE

CHARLES ARTHUR

Identity fraud, in which a slice of your identity ranging from new credit cards to entire bank accounts is taken over by criminals, rose by 49 per cent in 2015 on the previous year. That totalled almost 170,000 cases, according to data collected by Cifas, the financial industry's non-profit fraud advisory service.

The reason for the rise is that more and more we use the internet for financial transactions, but have very few ways to verify our identity without cumbersome systems involving human interaction, which are also vulnerable to fraud.

Cifas' 2015 *Fraudscape* report shows that 86 per cent of identity fraud happened online, with bank accounts and credit or debit cards most targeted, closely followed by loans and communications, typically mobile phone accounts.

Traditionally, companies dealing with such problems have acted after the fact, trying to unravel complex or opportunistic frauds by working back through audit trails. But the speed of online commerce can make it difficult to keep up.

Increasingly, businesses looking to tackle fraud are turning to artificial intelligence (AI), also known as machine-learning, and deploying neural networks because the systems learn in a manner like the brain's own neurons to try to bust fraud.

It is because the AI's view of what is happening is both real time and nuanced that fraudulent transactions and patterns of transactions "look" different from honest ones. Credit card theft is often detected when the stolen card details are used to make a small purchase in the thief's location; if that succeeds, the thief follows it with a much larger one.

The bigger the business, the more applicable such systems will be because they generate more data and machine-learning thrives more on the volume of data than the pure quality of the algorithms they deploy.

Leonard Austin of Ravelin, a London-based startup which applies AI technology to fraud detection for online payments, says: "Given the choice between better algorithms and more data, I'd always rather have the data because algorithms are commoditised already – there are so

many of them to choose from. The better quality data and the more data you have, the more you can predict."

Machine-learning improves with more data because this lets it pick out the differences and similarities between different behaviours. Once told which transactions are genuine and which are fraudulent, the systems can work through them and begin to pick out those which fit either bucket



Businesses looking to tackle fraud are turning to artificial intelligence and deploying neural networks because the systems learn in a manner like the brain's own neurons to try to bust fraud

and predict them in the future when fresh transactions are made. The one risk is if there is undetected fraud in the training data; in effect, that trains the system to ignore that type of fraud in future.

One group with rich sources of data, but also struggling against fraud, is phone carriers or providers, who collectively lose between \$30 billion and \$40 billion to caller fraud every year, according to Cataleya, a Silicon Valley-based startup which is used by a number of carriers around the world.

International calls, which have high costs and involve international money transfer, complicating recovery

of fraudulent transactions, are a particular target, with multiple different fraud methods with exotic names such as false answer supervision, *wangiri* (one ring and cut off) fraud and bypass fraud.

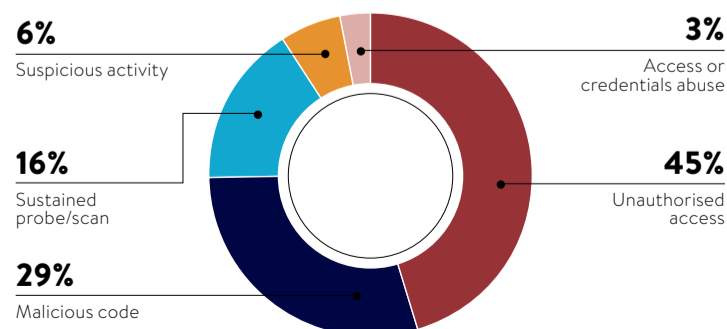
"We could have taken a rule-based approach to detect each kind of fraud," says Jay Jayasimha, Cataleya's chief executive. "But what we have are algorithms that detect abnormalities; they're not looking for fraud as such." That makes them more flexible, but also more useful as new forms of fraud will be unusual, but usually pass undetected by an inflexible rule-based system. Their abnormality, though, will make them stand out, says Mr Jayasimha.

The advantage in using real-time detection is that it catches fraud before it happens and so before billing, he notes. "Traditionally, carriers would have to look at their billing records after the call had completed, which could be one to ten minutes after the call was completed and flagged as suspicious. Then it would have to go to the fraud detection system, which would have to go over the billing records."

Instead, Cataleya's system can recognise fraudulent calls through patterns in the connections of the voice and system data, and even provide the option to disconnect calls recognised as fraudulent.

But detecting card fraud is one of the most important spaces where speed and accuracy matter most. "Any business that sells goods or services online is vulnerable to attack by fraudsters," says Gerry Carr, chief marketing officer at Ravelin. In the UK it's the most common crime,

### MOST FREQUENT CYBER INCIDENTS IN 2015



Source: IBM 2015

COMMERCIAL FEATURE

# TACKLING THE DEEP-ROOTED PROBLEM OF ONLINE FRAUD

*There are ways of protecting and proactively defending your organisation from the increasing number of cyber attacks, says*  
**Charlie Abrahams**, senior vice president of MarkMonitor

**MarkMonitor®**  
PART OF THOMSON REUTERS

It's an unfortunate side effect of the digital world that by searching through the junk mailbox or inbox of any current e-mail account, we would inevitably see evidence of attempts at online fraud. Cases of phishing, the fraudulent practice where e-mails are sent purporting to be from reputable companies to glean personal information from the recipient, have actually risen by 400 per cent in the last couple of years. In the UK alone, such attacks increased by 21 per cent in 2015, costing consumers an estimated £174.4 million.<sup>1</sup>

Phishing is by no means a new scam – the method has been in use for more than 15 years – and fraudsters are changing tactics, looking at new ways to catch out consumers. Targeted fraud that hijacks trusted brands and unsuspecting consumers has been a long-time challenge for companies such as banks or other financial services organisations. However, fraudsters are now focusing their efforts on a range of other sectors. These include industries such as software as a service vendors or companies with cloud-based offerings, telecommunications, retail and internet brands, and many are falling prey to these evolving methods.

The latest Office for National Statistics figures suggest that one in ten of us fall victim to online scams, virus attacks and thefts of bank details every year. The sums stolen are truly spectacular, an eye-opening £193 billion a year – that's 50 per cent more than the annual budget for the entire NHS. The online fraud landscape today has become a tangled web of potential threats and, as well as phishing, business e-mail spoofing scams and malware are also on the rise.

The threats have become more complex to navigate and the risks harder to mitigate with attackers making use of the deep web. The indexed sites on the internet, or surface web, only account for 4 per cent of the data that can be found online.<sup>2</sup> The rest is comprised of the deep web, unindexed content such as webmail pages, company intranets, user databases and pages behind paywalls.<sup>3</sup> The deep web also includes the dark web, which is a series of sites that are visible, but with hidden IP addresses enabling criminals and legitimate users alike to enjoy complete anonymity.<sup>4</sup>



Given the rapidly changing nature of cyber crime, protecting and proactively defending an organisation has never been more important. The first crucial step for businesses is to be fully prepared and adopt a “when” rather than an “if” approach, with the aim of preventing the attacks in advance. Organisations can set up early-warning systems alerting them of new domain registrations, which may misleadingly read like their brand name and may target the brand to host malicious content, before it impacts their customers.

Fraudulent activity can also be detected by using the right intelligence, and proactively monitoring and analysing key intelligence sources to detect phishing and malware activity across e-mail and other digital channels. Businesses need to shut down or restrict access to phishing sites and can partner with an anti-fraud vendor to share their phishing alerts with internet service providers, browsers, e-mail providers and security vendors, helping them block malicious sites at the internet gateway.

Measuring and mitigating cyber crime has to involve understanding the level of activity in these hidden areas of the internet. There are solutions on the market that use leading-edge technology to detect, analyse, mitigate and also provide near real-time alerts for a more comprehensive approach to anti-fraud. Conventional threat analysis requires security experts to search multiple platforms and manually identify threats. MarkMonitor® solutions use automated processes

to monitor and identify threats, and deliver insight into specific threat activity. Leveraging smart robot technology, the solution mimics human behaviour to interact with cyber criminals and infiltrate their networks.

The risk of cyber attacks is real. From a consumer perspective, there are many instances of individuals being targeted and potentially becoming a victim of online fraud. For businesses, proprietary corporate information, trade secrets and employee access credentials are all at risk. Businesses need to be aware of every potential threat to their IP and leverage the technology to monitor, detect and protect their organisation, and unsuspecting consumers, in the deepest, darkest layers of the internet.

**For more information please visit**  
**www.markmonitor.com**

<sup>1</sup> [www.techweekeurope.co.uk/security/cyberwar/uk-phishing-attacks-rise-2015-183964#fZ16pb5p55GHo4ZS.99](http://www.techweekeurope.co.uk/security/cyberwar/uk-phishing-attacks-rise-2015-183964#fZ16pb5p55GHo4ZS.99)

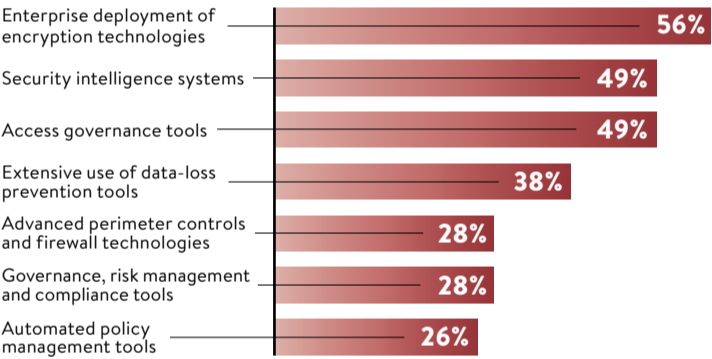
<sup>2</sup> [www.information-age.com/technology/security/123461668/just-tip-iceberg-why-you-should-be-monitoring-deep-web](http://www.information-age.com/technology/security/123461668/just-tip-iceberg-why-you-should-be-monitoring-deep-web)

<sup>3</sup> <http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-beautifulpeople-3593569/>

<sup>4</sup> <http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-beautifulpeople-3593569/>

© 2016 MarkMonitor Inc. All rights reserved. MarkMonitor® is a registered trademark of MarkMonitor Inc., part of the Intellectual Property & Science business of Thomson Reuters. All other trademarks included herein are the property of their respective owners.

## MOST COMMON CYBER SECURITY DEPLOYED BY UK COMPANIES



Source: Hewlett-Packard/Ponemon Institute 2015

with 2.47 million offences recorded in 2015-16.

Traditional systems use rules and business logic to determine whether an attempted transaction is fraudulent. This works, but it's expensive, says Mr Carr, because it is a top-down, expert-led approach, which makes little allowance for variation over time and tends to lead to many manual reviews by humans of transactions flagged as suspicious. That's slow, time-consuming, expensive and also tends not to lead to rules being updated quickly enough to deal both with new fraud patterns and innocent transactions wrongly flagged as fraud.

Ravelin's systems, which are deployed to spot fraud, can be trained with datasets from each customer; even better, they carry some transferability, for example between e-commerce sites. “For businesses where speed, scale and efficiency are paramount, we have to move past manual review,” Mr Carr says.

“Companies in the food delivery, transport and taxi app, and ticketing sectors have all been quick to adapt to machine-learning-based fraud detection, both our own and rivals. They need to process a lot of transactions and they need to do it very quickly, so traditional approaches don't work as

there is a very limited, or no, room for manual review.”

Ravelin reckons it can drive both speed and accuracy. “With all our customers, we look to drive the fraud rate down towards 0.1 per cent,” says Mr Carr. “We've seen fraud rates of 3 per cent and driven it down to 0.9 per cent with a full-blown [machine-learning], rules-based system in place. So there is a multiple factor in terms of accuracy. But accuracy and detection are only interesting in the context of being able to work at the right scale and speed.”

He notes how much the modern landscape has changed, in a world where we hail taxis from smartphones anywhere and no physical money changes hands to pay for the journey, opening up the possibility both of fraud and false positives in detection methods.

“If you can't approve a transaction in milliseconds, then it doesn't matter much how accurate you are,” he concludes. With the velocity of commerce increasing all the time, the need for quicker, better recognition of fraud and non-fraud is becoming not just important, but essential for business survival.

Share this article online via  
**Raconteur.net**

# Rio Olympics shone spotlight on corruption

Bribery and corruption is far from sporting behaviour, but sport has been tainted by greed and wrongdoing

**CORRUPTION**  
CATHERINE BAKSI

As the bright lights fade on the sporting carnival that was Rio 2016, you wonder what the founder of the Games, Baron Pierre de Coubertin, would have made of it. The host nation of the 31st Olympiad does not exactly embody the spirit of fair play, enshrined in de Coubertin's *Olympic Charter*.

The Games shone the world's spotlight on a country in the midst of its biggest corruption scandal, economic recession and a political crisis that has seen its president impeached and more than half its congress under investigation.

At the centre of the storm that has rocked Brazil is the widespread corruption uncovered during *Operação Lava Jato* or Operation Car Wash. It is alleged that executives at state-controlled oil company Petrobras accepted bribes in return for awarding construction contracts at inflated prices, and channelled funds into the accounts of Petrobras executives and politicians, which funded the electoral campaigns of senior Brazilian politicians.

Investigators have uncovered kickbacks of R\$6.4 billion (£1.5 billion), of which R\$2.9 billion (£692 million) has been recovered, but estimate total losses to the state could be more than R\$40 billion (£9.5 billion).

Since March 2014, more than 50 sitting politicians and 18 companies

have faced investigation, and more than 100 individuals have been sentenced, including the former treasurer of Brazil's governing Workers' Party, João Vaccari Neto, and Renato Duque, Petrobras's former head of corporate services.

The speaker of Brazil's lower house of congress, Eduardo Cunha, and the former president Fernando Collor de Mello, who was impeached in 1992, have also been accused of corruption.

To top it off, Dilma Rousseff was impeached as president in August and removed from office following claims of budgetary manipulation.

Set up to tackle the high-level corruption, Brazil's Ministry for Transparency, Monitoring and Control was itself tainted by the brush of corruption and the minister for transparency forced to resign.

Brazil took the biggest tumble in Transparency International's annual Corruption Perceptions Index. Ranked in 76th place in the list of 168 countries, its score, on the scale from 0 (highly corrupt) to 100 (squeaky clean), fell from 43 points in 2014 to 38 in 2015.

While all this may look bad to the observer, Isabel Carvalho, partner in the São Paulo office of international law firm Hogan Lovells, insists that what is happening in Brazil is a good thing and demonstrates a clean-up taking place.

The B in the BRIC list of developing countries, Brazil has the eighth biggest economy in the world. It is not unique in the region for tolerating



01

## OPERATION CAR WASH



Investigators have uncovered kickbacks of R\$6.4 billion (£1.5 billion), of which R\$2.9 billion (£0.7 billion) has been recovered, but estimate total losses to the state could be more than R\$40 billion (£9.5 billion)



Since March 2014, more than 50 sitting politicians and 18 companies have faced investigation, and more than 100 individuals have been sentenced

corrupt practices, but its problem is deep rooted.

One reason for the prevalence of corruption, says Naina Patel, a barrister at London's Blackstone Chambers, is the high level of bureaucracy and regulatory hurdles for doing business, resulting from the large state apparatus that has sought to be an engine of the country's growth and development.

Alberto Luzarraga, partner and co-head of the Latin America practice at international law firm Linklaters, adds: "Historically, the governing bodies of Brazil have had an overly large influence on the economy, particularly on the exploitation of natural resources and the awarding of corresponding development rights."

The country has moved from dictatorship and military rule to democracy within the last century, but has not developed the institutions to control corruption, says Mr Luzarraga.

Also at the heart of this corrupt culture, observes James Ramsden QC, barrister at 39 Essex Chambers, is the immunity of lawmakers and ministers for most acts of corruption.

This immunity, explains Peter Van Veen, director of the business integrity programme at Transparency International, means there is little motivation for senators and others to give up political roles. If they do, they risk coming under the spotlight of prosecutors. "Politics has become a bit of a refuge for the corrupt," he says.

Lack of enforcement has also been a factor, adds Mr Luzarraga, though

this is slowly changing. The trigger for Brazil's clampdown came in the run-up to its hosting of the 2014 World Cup. Hundreds of thousands of citizens took to the streets in protest over the cost of preparing for the football tournament, as the cost of living rose.

The protests turned into a call for a wider clean-up and led to the passing of the anti-corruption law that holds companies responsible for the corrupt practices of employees and introduced leniency agreements, which have been used to great effect during Operation Car Wash.

Ms Carvalho observes: "The anti-corruption law was the only good thing to have come out of the World Cup. Losing 7-1 to Germany was a disaster." The new enforcement regime in Brazil, she says, is changing how people are looking at doing business there. "Due diligence has become much more stringent, and corruption has become a big topic in every mergers and acquisitions transaction."

With the scale of the Car Wash investigation and the efforts of intrep-

## KICKING OUT CORRUPTION IN WORLD FOOTBALL



A bigger deal than even the Olympics, football's World Cup is the most lucrative sporting event in the world. According to FIFA, the 2014 Brazil World Cup generated £3.1 billion through broadcasting rights, marketing, ticket sales, hospitality and licensing rights, and raked in £2 billion profit for FIFA.

The corruption scandal that has engulfed world football's governing body has revealed the ugly side of the beautiful

game. Following investigations into allegations of corruption surrounding the bidding process that controversially awarded the 2018 and 2022 World Cups to Russia and Qatar respectively, 30 FIFA officials and associates were charged over involvement in accepting millions in bribes and kickbacks over more than 20 years.

What happened, says Alex Kelham, managing associate in the sports business group at law firm Lewis Silkin,

was the result of the huge amount of money involved in the commercialisation of the sport. "It became a victim of its own success and provided an opportunity for unscrupulous people to exploit and slice off money on the side," he says.

And it was allowed to happen, because those who administer the multi-billion-pound sport and hand out the lucrative contracts, says Nick De Marco, a sports barrister

at Blackstone Chambers, also regulate the sport.

Darren Roiser, partner in investigations, fraud and compliance at King & Wood Mallesons, adds that FIFA's status as an unincorporated association under Swiss law means it is not subject to the same corporate governance requirements as, for example, UK limited companies.

The beleaguered organisation is making efforts to clean up, reforming its

corporate governance rules and introducing a new four-phase bidding process for the 2026 competition.

What is required, says Crispin Rapinet, global head of investigations into white-collar fraud, at international law firm Hogan Lovells, is a complete culture change and enforcement regime, coupled with greater transparency and accountability, and independent scrutiny of the organisation's operation.



Okan Ozer/Anadolu Agency/Getty Images

id prosecutors, who are bringing US prosecutor-type standards and tactics to the country, Brazil “is a test case of what it takes to bring a country out of a cycle of corruption”, says Lance Croffoot-Suede, a partner in international governance and development practices at Linklaters. While there have been no allegations of corruption in relation to the bidding process for Rio 2016, construction firms that have built some



Cris Faga/NurPhoto/Getty Images



Mario Tama/Getty Images

**01** The Olympics have shone the spotlight on Brazil in the midst of its biggest corruption scandal

**02** Giant balloons depicting former presidents Dilma Rousseff and Inacio Lula Da Silva during protests in São Paulo in April

**03** Rousseff was impeached as president following claims of budgetary manipulation

of the venues have come under the glare of the Car Wash inquiry. And, adds Mr Van Veen, alleged kickbacks tainted every construction deal during the 2014 World Cup.

The organisation of large sports events, as the Organisation for Economic Co-operation and Development’s (OECD) report, *Preventing Corruption and Promoting Business Conduct when Organising Sporting Events*, points out, carries high risks of corruption because of the complex financial arrangements required, often under tight schedules.

The Olympics is not alone in courting sporting scandal. FIFA, the world governing body of football, remains mired in the fallout of allegations of wrongdoing in the bidding process for the 2018 and 2022 World Cups, and the International Association of Athletics Federations has been rocked by revelations of corruption by its officials to cover-up widespread doping.

There is general agreement that all the sporting bodies implicated need to clean up their acts, both in relation to their governance, transparency and accountability, and in the way they organise global events.

Though efforts are being taken to address some of the most egregious wrongdoing, Nick De Marco, a sports barrister at Blackstone Chambers, says that until steps

are taken to establish independent scrutiny and review, the various reforms of sporting bodies “will be only trifling and scandals will repeat themselves”.

More positively, he adds: “Increased pressure from the public, sports fans, politicians and law enforcement agencies means such radical change in the administration of sport is now firmly on the agenda.”

James Ramsden QC, a barrister at 39 Essex Chambers, agrees the outlook will remain bleak until an overarching sports regulator is in place.


“This could form an extension to the existing Court of Arbitration for Sport, but have powers of investigation and oversight in relation to each sport’s governing body that currently submits to the court’s jurisdiction,” he suggests.

Crispin Rapinet, Hogan Lovells’ global head of investigations into white-collar fraud, calls for the development of an international model of best practice and industry guidelines on adequate procedures.

Indeed, the OECD has already produced the *Good Practice Guidance on Internal Controls, Ethics and Compliance*, which it says provides a set of measures that are fully relevant to sports organisations and can stamp out corruption.

“  
At the heart of this corrupt culture is the immunity of lawmakers and ministers for most acts of corruption

Share this article online via [raconteur.net](http://raconteur.net)




the #1 managed cloud company

YOUR BUSINESS.  
OUR EXPERTISE.  
YOUR FUTURE.

Helping you transform your IT to power your business potential.

BETTER SOLUTIONS.  
TOGETHER.

SEARCH FOR  
RACKSPACE FUTURE



# Online robbers are riding the ‘

Developments in online shopping and e-commerce are being exploited by villainous fraudsters often armed only

E-COMMERCE

DAN MATTHEWS

The truism that crime doesn't pay is getting falser by the day. In the pre-digital age, before the era of single-click online payments, the process of fraudulently extracting money from victims was a subtle art honed by experts – and only a handful got away with it.

Famous bank robber Willie Sutton was once asked by a journalist why he targeted banks, his reported response was “because that’s where the money is”. Today the money is in personal data and criminal gangs have developed a host of ways to elicit it.

Online fraud, particularly targeting retailers and their customers, is so prevalent because it’s comparatively easy and safe. Easy because the web provides fertile ground for crime and safe because it’s possible to hide in places the long arm of the law can’t reach.

“Fraudsters of the past had different qualities,” says Nick Mothershaw, an ID and fraud expert at Experian. “They were patient and time rich, with a particular set of skills and unusual equipment. But the advance of technology and the internet has bred a different kind of perpetrator, needing only a laptop, internet connection and a basic understanding of phishing e-mails.”

Twenty years after consumers began adopting the internet in earnest, the web remains a virtual Wild West. It is constantly updating, evolving and expanding, and every new development is an opportunity to exploit.

The techniques used by fraudsters range from curmudgeonly to spectacularly clever. They pose as bank executives or law enforcement in confidence cons, or they simply buy parcels of financial and personal data on the dark web. They set up fake websites that mimic legitimate ones or they piggyback accounts, gently siphoning money over time.

But it’s not all about data. At the simplest level, opportunists can fib to get free products. They order a delivery, then claim a chargeback pretending the items were lost or stolen on route. Some of those who do this don’t even realise they are stealing, so entrenched is fraud in online channels.

At the other end of the scale, international crime syndicates operate in jurisdictions thousands of miles away from where the crime is perpetrated. They exploit loopholes in cross-border payments and overseas deliveries, knowing that fractured international policing is too weak to catch them.

“The rise of the e-commerce offers up manifold opportunities for fraud as retailers look to diversify and innovate across a multichannel model,” says Andy Herrington, head of

cyber professional services for the UK and Ireland at technology company Fujitsu. “Complicating this is the risk of fraud from both the client side and internally.

“Retailers now have complex supply-chain webs whereby goods and transaction may not even pass through their hands. There is also the factor of legitimate sales coming from stolen card details. With this in mind the ‘fraud surface’ is expanding and is currently a growing risk.”

So just how big is the problem? In a word, enormous. High-profile data hacks on Sony’s PlayStation Network, US retailer Target and, in the UK, Kiddicare leaked the personal details of millions of customers. But even these colossal compromises barely scratch the surface.

Vanita Pandey at cyber-crime prevention outfit ThreatMetrix describes the problem as growing exponentially. The company analyses nearly two billion transactions a month from thousands of businesses. Between April and June this year it uncovered 69 million attacks on e-commerce transactions.

That’s in addition to 400 million automated attacks, where an army of zombie computers carry out a pre-programmed synchronised raid. Increasingly these attacks are “low and slow”, according to Ms Pandey, mimicking normal traffic patterns to beat firewalls.

“New account creations and account logins are targeted far more than direct payments in the e-commerce space because fraudsters see the creation or takeover of a legitimate account a better long-term prospect than a single-payment transaction,” she says.

“Gaining access to a legitimate account gives the fraudster access to sensitive credentials as well as a saved credit card in many instances. If they are clever, they can use this multiple times before being detected.”

Darren Thomson, chief technology officer at Symantec, says industry statistics reveal the pressure retailers are being put under. Symantec’s own figures show the sector reported 5,823,654 successful data breaches last year alone.

The cost of these attacks is often absorbed by the victim businesses and is even factored into profit forecasts, such is the seemingly unstoppable march of online fraud. Yet the damage to corporate reputations, consumer confidence and bank balances is getting harder to ignore.

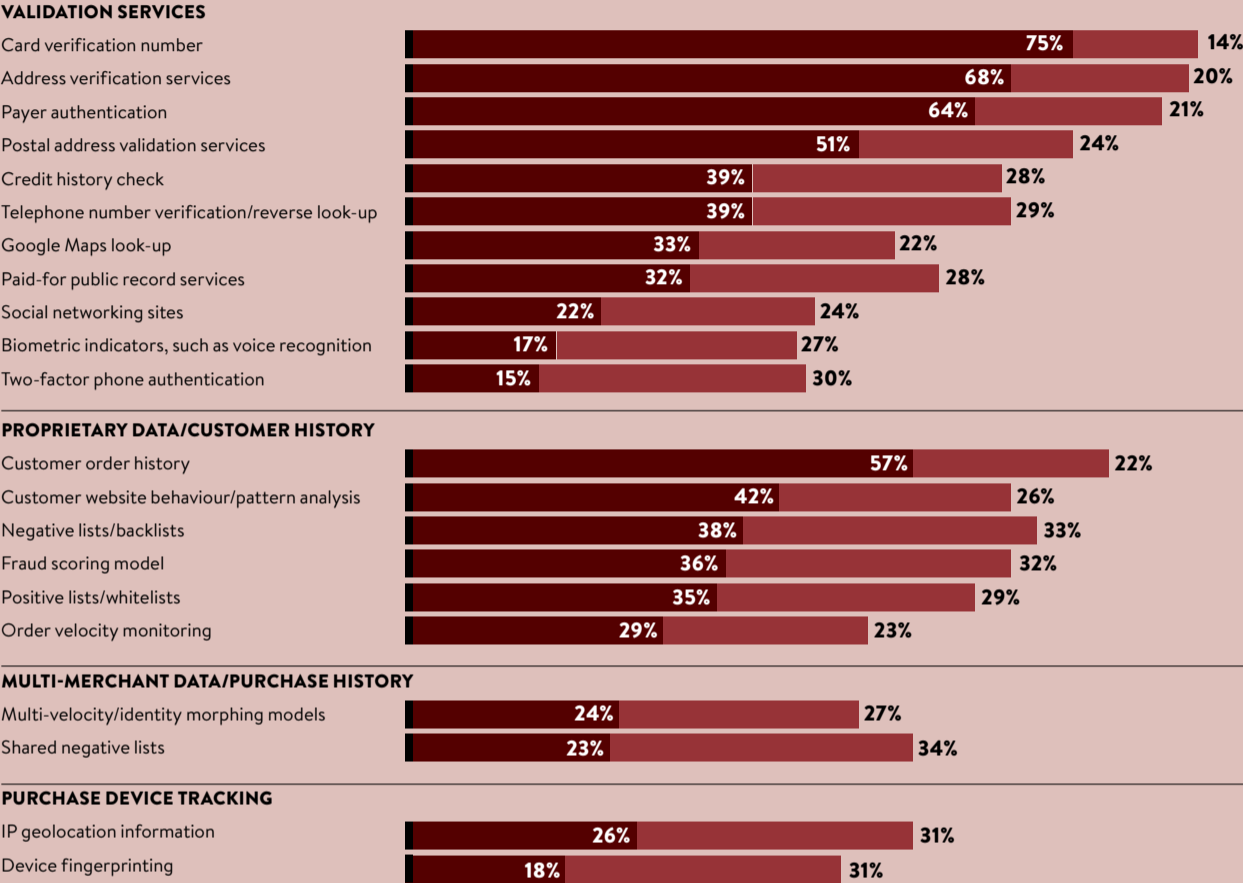
“The highly public attacks and breaches of the last few years rock consumer confidence and cost retailers a huge amount in management, reconciliation and written-off costs,” says Mr Thomson.

Combatting e-commerce fraud is as complex as the frauds themselves. Businesses have to develop protocols

TOOLS USED BY UK E-COMMERCE COMPANIES TO ASSESS PAYMENT FRAUD RISK

● Currently used ● Planning to use in 2017

Source: CyberSource 2016



that can address crimes across the spectrum, from criminal masterminds to low-profile amateurs working from a laptop in a bedroom.

But their attempts to block the bad-dies must be balanced with the equally important requirement to offer a friendly customer experience and a quick, simple user experience that doesn't alienate genuine customers with lots of security procedures.

“The damage to corporate reputations, consumer confidence and bank balances is getting harder to ignore

“The best advice is to work with a payments company that understands e-commerce as well as the specific vertical,” advises Daniel Kornitzer, chief product officer at Paysafe. “They can put a risk programme in place that protects the merchants while avoiding friction for consumers.

“In addition to providing advice and implementing fraud rules, some pay-

ment providers have also designed innovative solutions such as indemnifying merchants against losses, which means retailers effectively outsource their risk management.”

Preparation is key. Mr Kornitzer says retailers should ideally construct a plan with their payment processor long before launching their website. The good ones will have their own fraud teams who can tailor advice to the retailer’s business model.

Tristan Liverpool, director of systems engineering at F5 Networks, says businesses need the technological capability to identify unusual behaviour, such as a regular customer’s card being used on a new device.

It’s also possible to detect new accounts opened for the purpose of committing a fraud, he says. Shared databases can cross-reference information on criminal operations, such as flagged delivery addresses and mobile numbers, as well as highlighting inconsistencies in sales transactions.

Retailers without the budget for sophisticated software have to do a bit more legwork, according to Mr Mothershaw at Experian. Although fraud happens in different ways, there are some signals that are universal.

“A few danger signs include orders involving multiples of high value, desirable goods and delivery ad-

resses that are not valid or do not match to the billing address. Also watch for delivery requests for PO boxes and names that don’t match payment records. A further sign is lots of orders from the same device, especially if they are for different individuals,” he says.

Mr Mothershaw suggests implementing a strong and accurate identity-checking process at the start of the customer life cycle when they sign up for the first time. These may put off some shoppers initially, but once customers are validated, they can get an easy ride for follow-up purchases.

“There needs to be a balance between risk prevention and the experience of the person trying to log-on. The right technology and data can help retailers identify ‘good’ customers as soon as possible and speed them on their way to what they want,” he says.

Fraud is a fast-changing crime, but for all the criminal innovation in this area, fraudsters cannot mask themselves completely. Retailers that educate themselves, use prevention software and partner with experts can stop themselves becoming the low-hanging fruit criminals so love to pick.

Share this article online via Raconteur.net

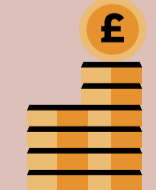
TOP COUNTRY



NIGERIA  
42%

ESTIMATED E

Source: Financial F

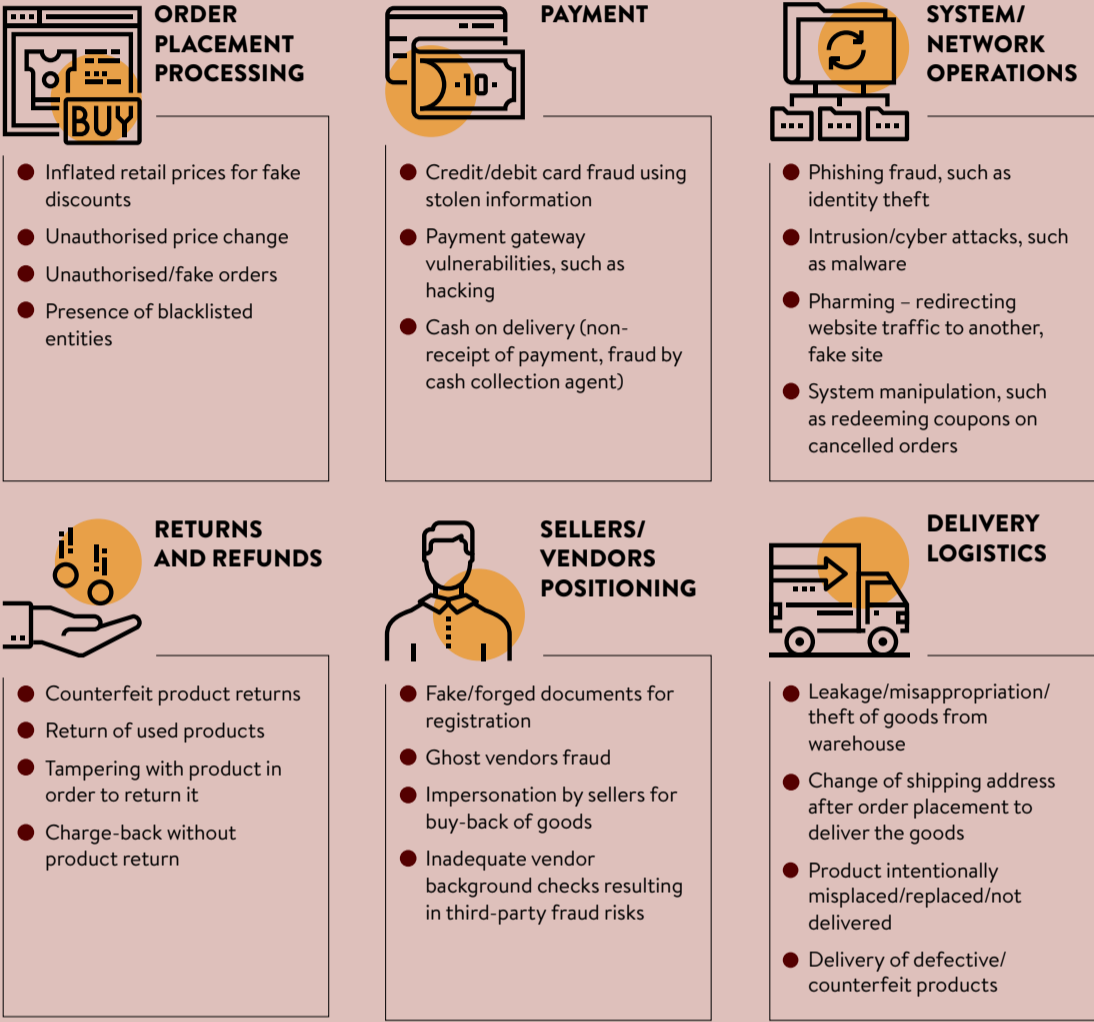


2006  
£154.5M

# 'Wild West' worldwide web

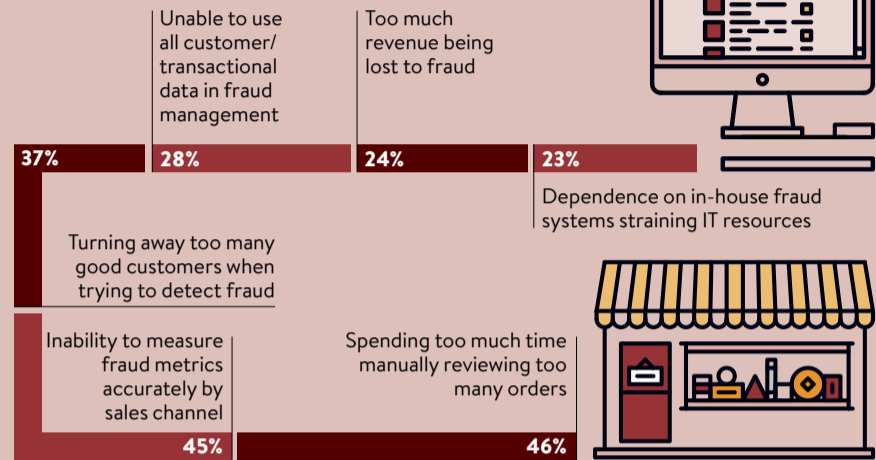
with a laptop, internet connection and phishing e-mail

## E-COMMERCE FRAUD-RISK LANDSCAPE



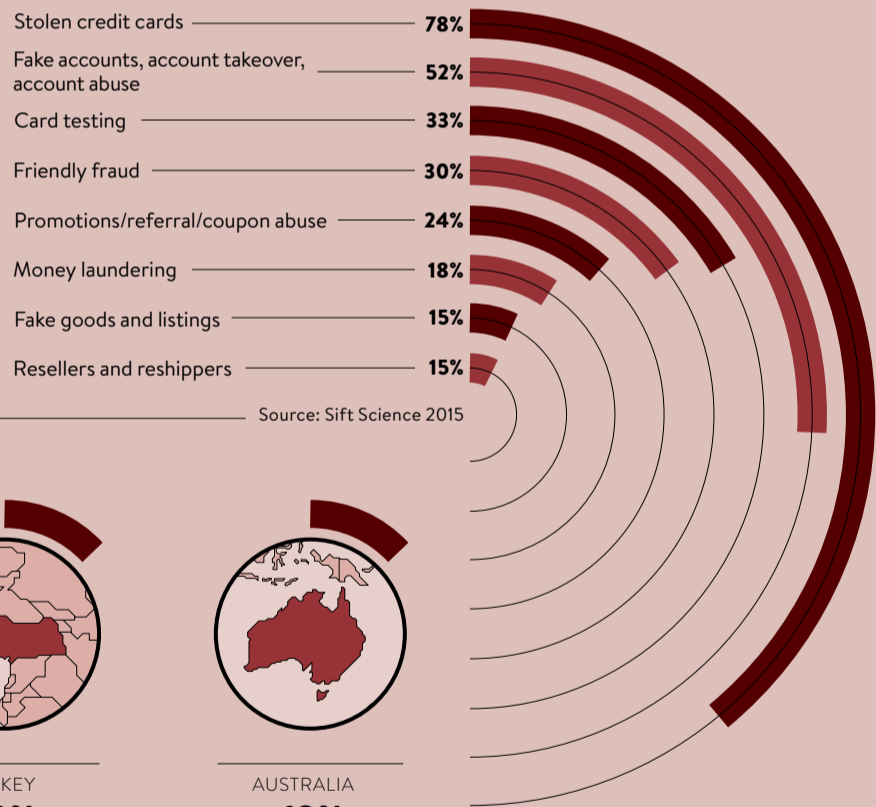
Source: Deloitte 2016

## FRAUD CHALLENGES OF GREATEST CONCERN TO UK E-COMMERCE COMPANIES



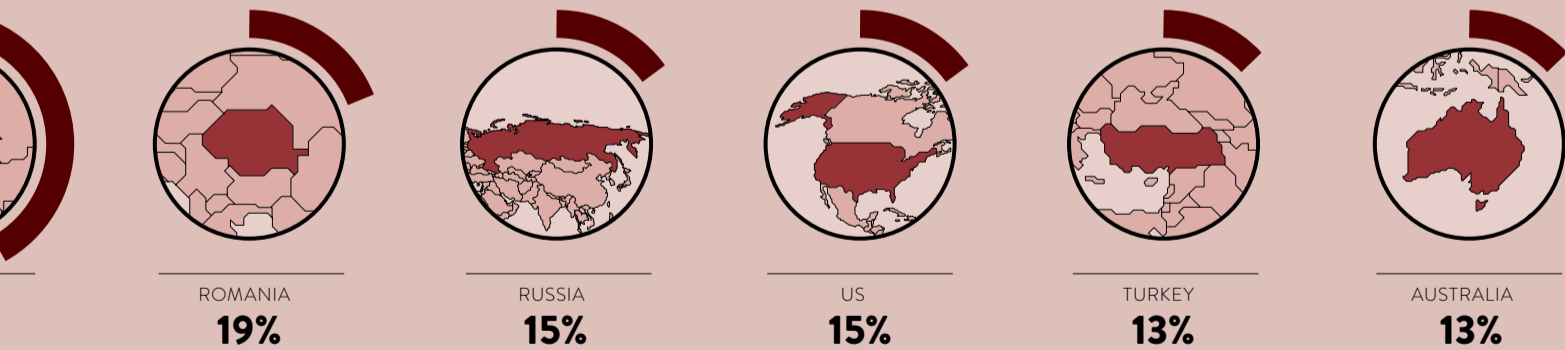
Source: CyberSource 2016

## PREVALENCE OF CERTAIN FRAUD TYPES FACING UK E-COMMERCE COMPANIES



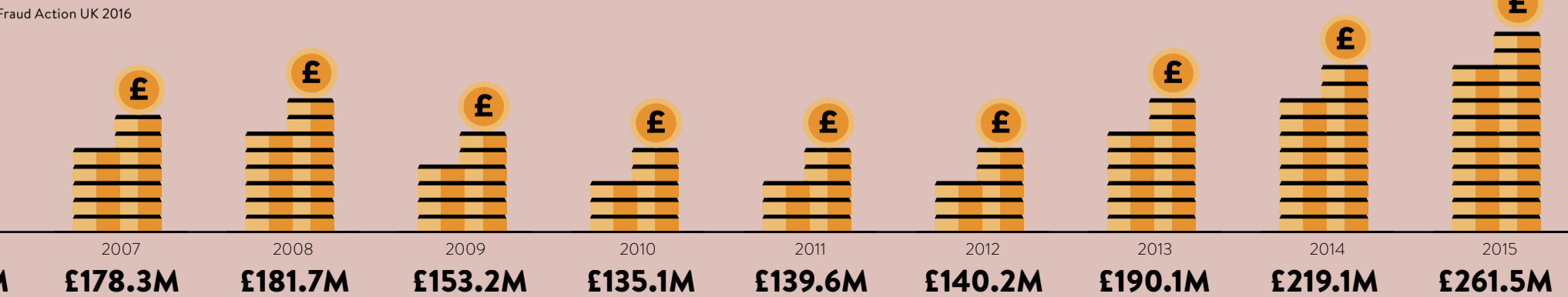
Source: Sift Science 2015

## COUNTRIES BLOCKED BY UK MERCHANTS DUE TO HIGH FRAUD RATES



Source: CyberSource 2016

## E-COMMERCE FRAUD LOSSES ON UK-ISSUED CARDS, 2006-2015



Fraud Action UK 2016

SMALLER FIRMS  
HAZEL DAVIS

Research from SAS and the Centre for Economics and Business has shown that efficiencies gained by businesses through better fraud detection tools could total £290 million from 2015 to 2020.

The trouble is that many small and medium-sized enterprises (SMEs) rely solely on the fraud detection provided by their payment gateway, says Gerry Carr, chief marketing officer at anti-fraud startup Ravelin. “The main job of a payment gateway is to validate your customer’s credit card details securely, and make sure the funds are available for the payment and you get paid.

“As they only typically see the payment page activity, because they simply need to approve or decline a transaction, they are not able to see all the events in the customer journey, thus limiting their ability to provide end-to-end fraud protection.”

Ravelin’s own analysis shows that a mature business with a fraud solution in place would expect to drive fraud down to less than 0.5 per cent at its peak. But in the period between kick-off and maturity, that is during the high growth period for SMEs, the level of fraud can reach 5 to 9 per cent of all transactions and represent an even larger slice of revenue, as fraudsters tend to spend more, which can hit an SME even harder.

“While it can be easy for an SME to spot a customer buying large numbers of items in quick succession, it’s more difficult to spot multiple accounts making relatively small purchases across an extended period of time. Spotting these connected purchases is not easy and can seriously damage a business’ bottom line,” says Mr Carr.

Sundeep Tengur, fraud solutions and financial crimes specialist at SAS, says: “Fraud has evolved from simple and opportunistic modus operandi to more complex and patient scenarios. Fraudsters are becoming increasingly sophisticated and often hide within complex networks where



STAFF AWARENESS  
ABOUT SECURITY  
SURVEY OF SMALL UK BUSINESSES



Source: PwC 2015

# Size doesn’t always matter in a breach

Fraud is as much of a threat to smaller firms as big businesses, so why are they lagging behind in prevention?

look to have regular fraud risk assessments, and seek to develop an anti-fraud culture and policies within the business. A focus on increasing the perception that fraud will be investigated, detected and not tolerated is a good place to start.”

Scott Zoldi, chief analytics officer at FICO, which uses predictive analytics and data science to improve operational decisions, says ongoing checks should be in place. “Regularly review what information you store. Check over what information is being stored on your servers and verify that any confidential or monetary data is sufficiently protected,” says Mr Zoldi.


He suggests using managed security services: “Advances in cyber-security technology, including the use of more sophisticated analytics, can be difficult to keep on top of. Managed security services can ensure you are as well protected as larger firms.”


Mr Zoldi also suggests a disaster recovery plan. This, he says, should include: “Who to call when something bad happens, off-site back-up in order to recover from fire, flood, physical theft and hackers, and records of what, if anything, your insurance policy covers from down time and other costs associated with hackers.”


It’s important to do your data homework. Mr Zoldi says: “Collect computing logs and occasionally review them because they will prove valuable during incident response, helping you to learn what your computers normally do, respond to cyber attacks more quickly and potentially spot hackers before a damaging breach.”


“Managed security services can ensure you are as well protected as larger firms


TOP 10 IT SECURITY TIPS FOR SMALL BUSINESSES


- 


01 Assess the threats and risks
- 


02 Get in line with cyber essentials
- 


03 Secure your data on the move/in the office
- 


04 Secure your data in the cloud
- 

05 Back up your data
- 

06 Train your staff
- 

07 Keep an eye out for problems
- 

08 Implement an IT security/incident management policy
- 

09 Minimise your data – delete out-of-date/inaccurate data
- 

10 Review any IT contractors

Source: Information Commissioner’s Office 2016

businesses. “Also contributing to the rising velocity of fraud is the proliferation of online services and the anonymity those digital channels provide to consumers,” says Mr Tengur. “For example, when making insurance claims, it’s easy to inflate the value of a damaged or stolen item or to add a few additional items to the claim, therefore resulting in what’s often referred to as ‘soft fraud’.”

Organisations must be in a constant state of readiness, he says, and this requires a multi-layered and pragmatic strategy. “It is critical that organisations adopt a holistic approach that encompasses data management and fraud detection, as well as robust policies and strict internal governance,” says Mr Tengur.

Fraud can affect business in a multitude of ways, not just financial. “In the case of an SME that itself is implicated in a fraud, perhaps bribery to secure a contract, it could find itself the subject of an SFO [Serious Fraud Office] or other regulatory investigation,” says Alex Jay, partner at Gowling WLG, counter-fraud specialist and a

member of the independent Fraud Advisory Panel.

The costs of responding to and addressing such an investigation, both financially and reputationally, can be severe. Mr Jay says: “For company directors or senior management personnel, failing to implement anti-fraud measures or control such risks could also give rise to criticism or even claims against them in severe cases.”

Training is crucial, but he says: “Any training programme should be considered with input from a variety of areas of the business and preferably with the assistance of anti-fraud professionals to ensure it is fit for purpose. An SME should



sage Pay

*KNOW YOUR BUSINESS*  
**KNOW YOUR  
ENEMIES**

**Take the fight to fraudsters** with Sage Pay. Don't give them room to strike, restrict their tactics and safeguard your business **with advanced fraud screening tools as standard** from Sage Pay.

---

*Speak to a Fraud expert today*

**0845 485 7898**

**#domorebusiness**  
[www.sagepay.co.uk](http://www.sagepay.co.uk)

## COMMERCIAL FEATURE

# RANSOMWARE: THE FAST-GROWING CYBER THREAT EVERY ORGANISATION MUST FIGHT

*A new initiative, launched by Europol and Kaspersky Lab, among others, aims to combat the growing threat of potentially devastating ransomware*



**R**ansomware is on the increase as hackers become more sophisticated, audacious and professional. While the majority of traditional attacks involve seizing data and then finding ways to cash that data in, with ransomware cyber criminals can earn money at once. It is a type of malware in which hackers lock the victims' computer or encrypt their data and demand a ransom in order to allow the victim to regain control over the affected device or files.

This summer the Dutch National Police, Europol, Intel Security and Kaspersky Lab, one of the four biggest endpoint security vendors in the world (IDC rating, 2015i), joined forces to launch a new weapon in the battle to combat this type of cyber crime.

No More Ransom – [www.nomoreransom.org](http://www.nomoreransom.org) – is a new online portal aimed at informing the public about the dangers of ransomware and helping victims to recover their data without having to pay the cyber criminals. The website allows victims to report a crime, directly connecting with Europol's overview of national reporting mechanisms.

Kaspersky Lab research, based on Kaspersky Security Network statistics, shows an almost six-fold increase in ransomware attacks on businesses, from 27,000 in 2014-15 to 158,600 in 2015-16. Shade, for example, is a ransomware-type Trojan that emerged in late-2014. Spread via malicious websites and infected e-mail attachments, after getting into the user's system, Shade

encrypts files stored on the machine and creates a text document containing the ransom note and instructions from cyber criminals on what the user should do to get their personal files back. It's just one of many examples of ransomware.

"This form of attack, which first appeared around 2005, became less common for a while, but then about three years ago it came back with a vengeance," says David Emm, Kaspersky Lab's principal security researcher. "It's grown massively since then. Hackers make far fewer mistakes these days and those who fall victim to it are often unable to get their data back unless they have a backup. In a few cases it can be decrypted."

Worryingly, ransomware hackers are becoming more professional. "Over the last decade attacks have become more organised and less speculative because criminals are realising they can make serious money from it," says Kirill Slavin, Kaspersky Lab's general manager for the UK and Ireland. The company has identified 26,000 encryptor modifications, which is ransomware code that encrypts data.

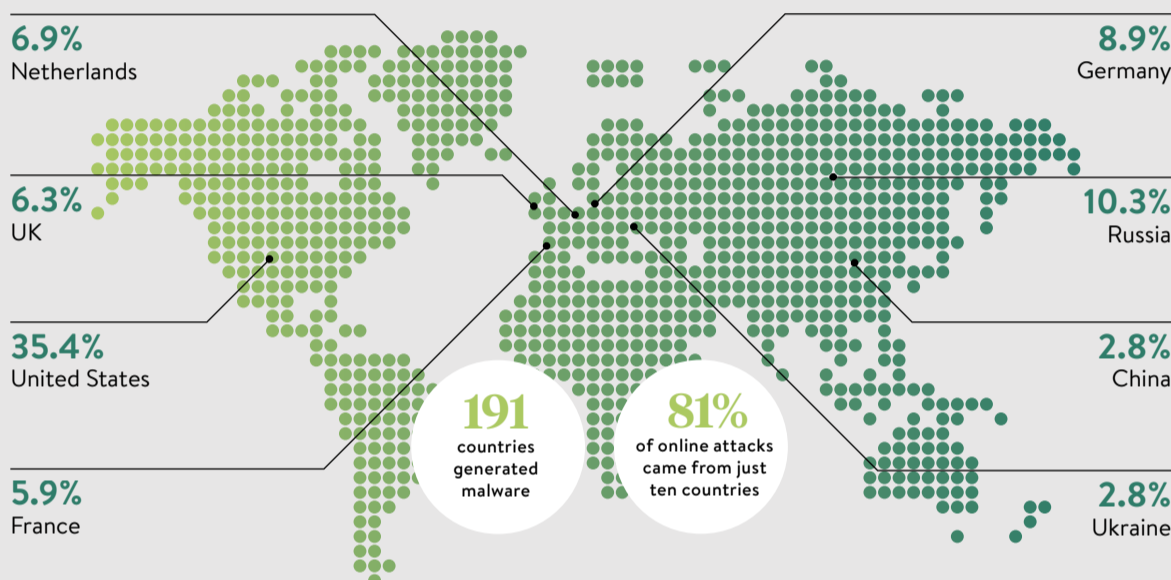
"Moving forward, we expect it to reach the same sort of proportions as we've seen for banking malware," he says. "These people are entrepreneurs and this underground market is a reflection of legitimate markets. There are individual contractors, small and medium-sized enterprises, and large businesses. You find people who manage networks and those who write code. There are value-added resellers and affiliate programmes where criminals receive commission on malware that they distribute."

A ransom can cost the victim an average of £230, he points out, but one big hack could reach a ransom of hundreds of thousands of pounds. Attackers will scale their ransom demands depending on who they think they're dealing with. In some cases, every day the victim delays payment, the demand is increased.

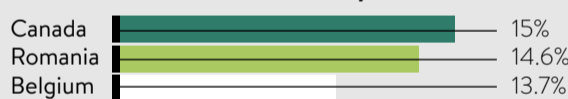
Smaller businesses are particularly at risk. According to Kaspersky Lab's IT Security Risks 2016 survey, nearly 42 per cent of small and medium-sized businesses (SMBs) fell victim to ransomware in the last 12 months. Over a third (34 per cent) paid the ransom, but one in five weren't able to recover their data, even after the demands of cyber criminals were met. Those that pay, warns Kaspersky Lab, may well find themselves targeted again.

## 171,895,830 ONLINE ATTACKS BLOCKED BY KASPERSKY LAB IN SECOND QUARTER OF 2016

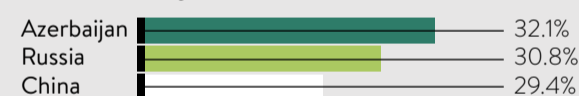
Top countries of origin for malware



### Safest countries for online activity



### Countries at highest risk of internet infection



There is plenty of scope for ransomware to develop and diversify. "Ransomware hackers are going after smartphones – in 2015, 17 per cent of attacks were on the Android platform," says Mr Emm. There are also concerns about the fast-growing internet of things, the system that connects machines to each other via the internet. "Your office's central heating system could be controlled through an app, so what happens if it's suddenly switched off during the middle of winter? Major machinery might not work and even cars with their increasing computer technology could be affected. We've already seen proof of concept of this," he says.

Decryption is one of the most effective tools for rescuing a victim and Kaspersky Lab has the ability to decrypt about 30 per cent of ransomware, but prevention is better than cure. Patch, protect and backup is the advice from the company. Organisations should ensure they install updates and keep in regular contact with their vendor.

"People don't routinely backup their data or they do so with a device which is left connected to the computer and this can be vulnerable to a ransomware attack. Make use

of the cloud and have an offline backup," says Mr Emm, "or backup to a local storage device and then disconnect it." Staff behaviour can also be an issue. "Don't give everyone administrative rights over the system – only the rights they need to do their job," he says.

In 2015 Kaspersky Lab's solutions protected 443,920 users and corporate customers worldwide from crypto-ransomware, depriving cyber criminals of nearly \$53million in illegal earnings. In August it launched the Kaspersky Anti-Ransomware Tool for Business, free software that offers complementary security to protect corporate users from ransomware.

To identify ransomware behaviour patterns and protect Windows-based endpoints, Kaspersky Anti-Ransomware Tool for Business leverages two innovative technologies,



Ransomware hackers are going after smartphones – in 2015, 17 per cent of attacks were on the Android platform

Kaspersky Security Network and System Watcher. System Watcher's unique capabilities include the ability to block and rollback harmful changes.

While experts advise businesses to use a variety of additional protection technologies and approaches to protect themselves, Kaspersky Anti-Ransomware Tool for Business provides complementary security to those companies that do not have advanced Kaspersky Lab security solutions. Kaspersky Anti-Ransomware Tool for Business is able to protect against crypto-malware, a form of ransomware that can infiltrate and encrypt an entire network, including its backups, within minutes.

As the ransomware criminals become more innovative and well resourced than ever before, the challenge for organisations is to ensure they too keep ahead of the curve. "Everyone has a responsibility and a role to play in combating this fast-growing and devastating form of cyber crime," says Mr Emm. "We're proud to be leading that fight."

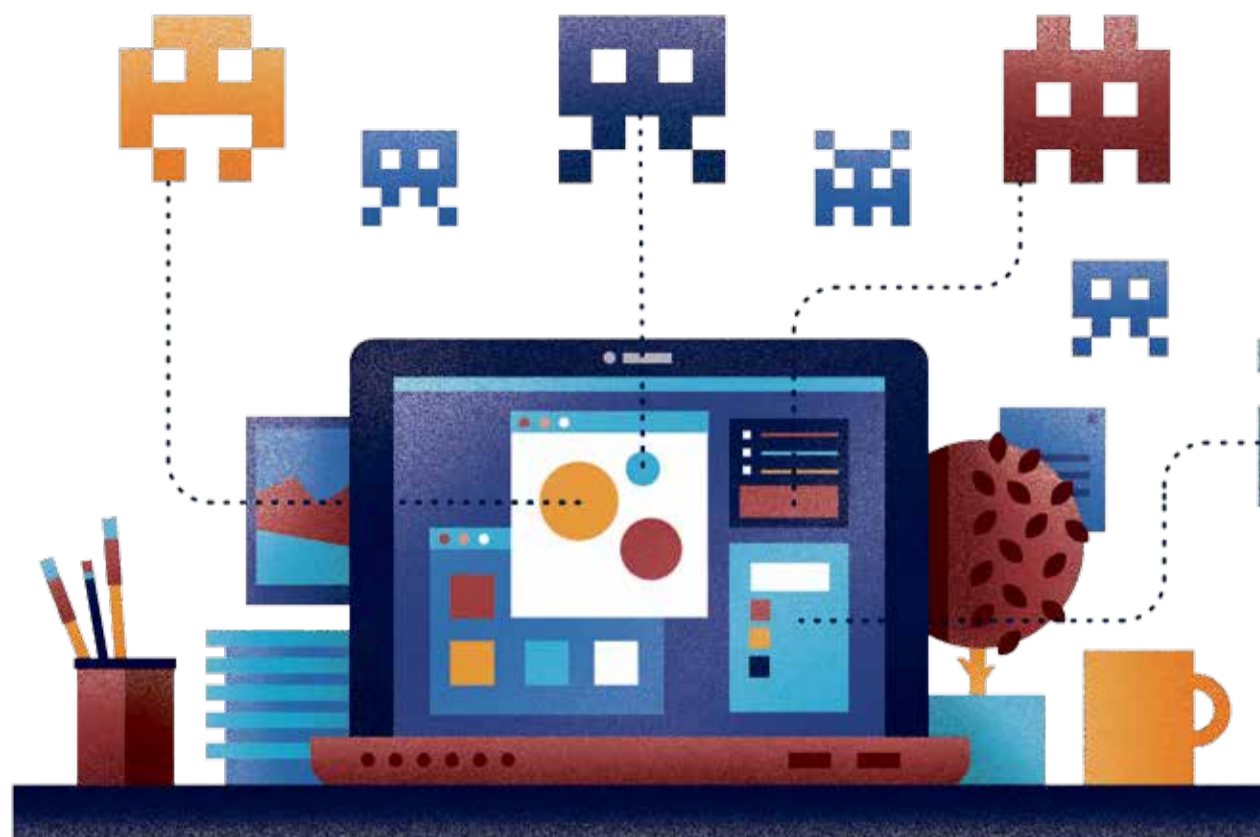
For more information please visit [www.kaspersky.co.uk](http://www.kaspersky.co.uk) or [www.nomoreransom.org](http://www.nomoreransom.org)

**42%**  
of SMBs fell victim to ransomware in the last 12 months

**34%**  
of these paid the ransom

**1 in 5**  
weren't able to recover their data, even after the demands of cybercriminals were met

Source: Kaspersky Lab's IT Security Risks 2016



# Is future cyber crime a nightmare scenario?

Chances are cyber crime is going to get worse before things get better and the hacker hunters fight back

**CYBER CRIME**  
DAVEY WINDER

Cyber crime, according to the National Crime Agency (NCA) *Cyber Crime Assessment 2016* report, accounted for 53 per cent of all crimes in 2015.

Cameron Brown, an independent cyber defence adviser, who has conducted research into emerging trends in cyber-crime offending, warns that opportunities to earn a living through cyber crime "will propel the disenfranchised and those in lower income bands to pursue a life of crime given the low risk and potential high yields".

Mr Brown insists that cyber crime will continue to grow into a highly lucrative and well organised enterprise, seeking competitive advantage with the aid of sophisticated cyber operations. Operations that include research and development, with cyber criminals becoming increasingly innovative as far as the threats they can leverage are concerned.

Jamie Saunders, director of the NCA National Cyber Crime Unit, argues that "senior members of UK business must think seriously about ways they can improve their defences and help law enforcement in the fight against cyber crime". And that means they must think seriously about the shape those future threats will take.

To determine the future shape of the threat landscape, we must first look at the seeds which have

already taken root, starting with ransomware. Security vendor Malwarebytes has a honeypot to attract unwitting attackers and says in December 2015, 17 per cent of exploit payloads were categorised as ransomware; by May

2016 this had risen 259 per cent to 61 per cent.

Ransomware already dominates the threatscape, but it's going to get much worse according to Liviu Arsene, senior e-threat analyst at Bitdefender, who predicts "ransomware-like attacks will become more prevalent with the integration of internet of things (IoT) and smart sensors into our daily lives".

“By 2040 more crime will be committed by machines than by humans”



**53%**

Cyber crime accounted for 53 per cent of all crimes in 2015

Source: National Crime Agency 2016



**5.8m**

fraud and computer misuse offences were recorded during 2015 across England and Wales

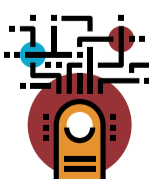
Source: Office for National Statistics 2016



**44%**

of UK businesses hit by economic crime over the last two years were impacted by cyber crime - up by 20 per cent from 2014

Source: PwC 2016



**20x**

more likely for an individual to be robbed online by overseas perpetrators than held up in the street

Source: Office for National Statistics 2016

Mr Arsene envisions a scenario where a smart home or office is held hostage and the owners are asked to pay a fee to regain access to lights and appliances, for example.

Raj Samani, chief technology officer, Europe, the Middle East and Africa (EMEA), at Intel Security, works with the NCA and the Europol European Cybercrime Centre as an adviser. He sees ransomware spreading to transport with the arrival of ever-smarter cars. "It's only a matter of time before we see instances of people left helpless, unable to drive their cars unless they pay up a ransom," he warns, adding, "we're not talking driverless cars here, just a standard modern vehicle with connectivity capabilities."

Connectivity, in particular the increasingly connected world of devices that is heralded by the IoT, will be front and centre of any emergent threatscape. Strip away the lack of secure thinking during the design process and organisations are left vulnerable to cyber attack.

Indeed, one vulnerability can often rule them all. "Our researchers discovered vulnerabilities in a supervisory control and data acquisition solution used in the Large Hadron Collider, several European airports, nuclear power plants in Iran, the largest pipelines, water supply systems, trains and chemical plants in several countries," Alex Mathews, EMEA technical manager at Positive Technologies, reveals. In the same way, a single vulnerability in a web application can provide direct access to corporate infrastructures of myriad companies.

Predicting the future of cyber crime isn't all about evolution though, there has to be some revolution in there. This calls for some serious security future-gazing and that inevitably means robots.

"As the workforce moves towards more automation, we could find 35 per cent of jobs now done by humans have been replaced by robots," says Tracey Follows, chief strategy and innovation officer at The Future Laboratory. "Futurists have been forecasting a sharp rise in lone-wolf terror attacks for years. But once robots can be hacked to become suicide-bombing machines, lone-robot attacks could become a real thing."

What's more, according to Ms Follows, artificial intelligence and machine-learning could enable robots to self-programme criminal activity. "My forecast would be that by 2040 more crime will be

committed by machines than by humans," she says.

Driverless cars will be our transportation reality in the years to come and that's another opportunity for cyber crime right there. "If you can convince the vehicle its GPS telemetry is wrong with a signal jammer," says Aaron Yates, chief executive at Berea, "you will be able to pilfer vehicles at leisure." But if you think driverless cars are problematical, what about delivery drones? Already being tested by the likes of Amazon, what if delivery drones were hijacked and deliveries stolen? What if they were herded by the hundreds into flying bot armies? Art Swift, president of the prpl Foundation, fears drones could be dropped on to a motorway or flown into a plane on take-off.

And it's not just drones that could be herded by hackers, humans could be as well. Darren Thomson, chief technology officer of Symantec, predicts that cyber criminals could take down an entire railway by hacking the information display boards.

"No one knows where to go for their train, the station atrium would fill up causing a physical or terrorist risk for that space," says Mr Thomson. "We are becoming so reliant on technology that it could potentially be used to pool people in a particular place."

Future-gazing would not be complete,

though, without mention of quantum computers. "In about a decade we may reach a tipping point in the world of cryptography, as a practical quantum computer will become a reality," says Michael Scott, chief cryptographer at MIRACL.


This means that most current methods of cryptography would be rendered useless overnight. "It's not unfeasible that hackers could decrypt all the sensitive information we currently store on the internet - banking details, tax records, identities, corporate and legal data - with enormous repercussions," says Mr Scott.

We will leave the final word to ex-FBI counter-terrorism operative and current national security strategist at Carbon Black, Eric O'Neill, who doesn't think this necessarily means an unhappy ending as far as the victimisation of business is concerned.

"In the near future, predators will become the prey," Mr O'Neill predicts, as security teams increasingly become proactive in hunting for threats. "As the good guys become more active in remediating threats before hackers launch their attacks, espionage and digital fraud will become far less economically beneficial for the bad guys, giving us a far better chance of keeping them out."

“Hackers could decrypt sensitive information on the internet with enormous repercussions”

Share this article online via raconteur.net



# Don't just know your customer. Trust them

Prevent fraud and abuse for your web-scale business with real-time machine learning.


✓ ESTABLISHED ACCOUNT

✓ UNIQUE DEVICE ID

✓ VERIFIED EMAIL

✓ SUCCESSFUL TX

✓ SUBSCRIBED TO NEWSLETTER



# An anti-fraud technology for the digital age

Blockchain has the potential to eliminate common frauds perpetrated online and help secure financial services from cyber hackers

**BLOCKCHAIN**  
DAN MATTHEWS

Blockchain is a technology in its infancy, but it is steadily transforming the financial relationships between people and businesses globally. Alex Tapscott, co-author of the book *Blockchain Revolution*, compares it to the emerging internet in 1993.

Back then, had you tried to strike up a conversation in a pub about the web's potential, there wouldn't have been many takers. The same is true today of blockchain technology, which some have heard of, but few have had the chance to get to grips with.

That's partly because it is technical and complicated, based on mathematical algorithms and digital protocols, and partly because there aren't that many practical uses for it yet, certainly not from an everyday consumer's point of view.

Its complexity defies layman's explanations, but Mr Tapscott sums it up as "a vast, globally distributed ledger where anyone, anywhere can move, store and manage any kind of asset, from money and securities to intellectual property and votes".

Assets can be moved "securely and privately without a trusted intermediary like a bank or government". It is, he says, "the first digital medium for value just as the internet was the first for information".

Brian Donegan, head of e-business operations at the Department of Economic Development for the Isle of Man government, describes it more prosaically as like a "giant

global spreadsheet that runs on millions of computers".

Meanwhile, David Treat, managing director of financial services at Accenture, says it is "a technology which enables people to confidently and securely share access to data because they are able to prove to themselves mathematically that it hasn't been tampered with".

Blockchain is a vast, globally distributed ledger where anyone, anywhere can move, store and manage any kind of asset, from money and securities to intellectual property and votes

Essentially, the blockchain is a database just like any other, but with a few unique qualities that make it very interesting to people fighting fraud in online transactions. Digital banking and payments services are developing quickly, yet the security that underpins them must keep up with the speed and openness of the new services.

According to Gareth Stephens at identity data intelligence specialists GBG, it opens up a world of opportu-



nities that were impossible before its arrival. The central technology is extremely secure, some would say impenetrable, and it can be completely decentralised so no one can claim ownership.

"Any participant, across geographies and institutions, can collaboratively make changes to the ledger and these changes are reflected across all copies of the ledger in a matter of minutes," he says.


Unlike an owned security system, one created by a company and licensed to, say, a bank, the blockchain's distributed ledger is diffuse and there is no obvious place for a fraudster to start chipping away.

"It is not centralised and that is important, therefore there is no single point of failure," explains Dr Kevin Curran, senior member of the Institute of Electrical and Electronic Engineers and reader in computer science at Ulster University.


"It is composed of data structure blocks where each block holds batches of individual transactions and the results of any blockchain executables. All of these blocks contain a timestamp and a link to a previous block. The blockchain therefore serves as a public ledger of transactions which cannot be reversed."

Or at least not quite. According to Mr Tapscott, in order to mess with a blockchain-based cryptocurrency, such as bitcoin, a hacker would have to access simultaneously every sin-


## WHAT IS BLOCKCHAIN TECHNOLOGY?




A digital ledger that keeps a record of all transactions taking place on a peer-to-peer network




All information transferred via blockchain is encrypted and every occurrence recorded, meaning it cannot be altered



It is decentralised, so there's no need for any central, certifying authority



It can be used for much more than the transfer of currency; contracts, records and other kinds of data can be shared



Encrypted information can be shared across multiple providers without risk of a privacy breach

Source: IoT World News



Carlos Osorio/Toronto Star via Getty Images

**LEFT**  
Alex Tapscott, co-author of *Blockchain Revolution*, compares the advent of blockchain to the emerging internet in 1993

gle computer on the ledger, an act requiring the same computing power as a googol or ten to the power of one hundred googles.

Coming back down to Earth for a moment, this essentially means blockchain has the potential to eliminate common frauds perpetrated online, such as “double spend”, where two payments are made close together to dupe merchants into thinking they have been paid, when the money has actually been sent to a second digital wallet owned by the fraudster.

There are other benefits too, for example the blockchain would all but eliminate transaction fees, reduce infrastructure costs for financial firms, eliminate the need for time-draining middlemen and overseers, enable micro-payments of less than a penny and it is capable of proving value exchanges relating to just about anything, from a painting to a vote.

Is there a downside? Of course there is. For one the blockchain is immature and, while the core technology is secure, attempts to layer services on top have engineered vulnerabilities that hackers have exploited with some ease.

For a secure currency, bitcoin gets stolen an awful lot. In August the media reported the theft of \$78 million worth of the currency, 120,000 bitcoin, from the Hong Kong-based exchange Bitfinex, causing an instantaneous 20 per cent drop in its value.

The exchange was forced to cease trading, phone the police and shave more than a third of the value from customer accounts in order to make up for losses.

In June, around \$50 million in ether, the second most widely traded cryptocurrency, was swiped from under the nose of a venture capital fund called the Decentralised Autonomous Organisation,

which uses the Ethereum blockchain. The creator of Ethereum said the hacker had seized upon a “recursive calling vulnerability” in its code. Well we all could have told him that.

The lesson is that things built on the blockchain aren’t necessarily as safe as the chain itself. There is a lack of specialists qualified to work with the technology and it will take time to educate and train enough people to make consumer-ready services.

The Isle of Man has launched an ICT University to help address the problem. Mr Donegan says it is needed to “educate the next generation of blockchain developers, which the industry needs to ensure its success continues at the right pace”.

But the main challenges to creating a consumer blockchain are related to its implementation and do not necessarily detract from the central idea itself. According to Mr Treat at Accenture, things could pick up pace next year.

“Financial services is one of the most mature sectors in experimenting with the technology and there are a few success stories, such as Nasdaq Linq, but they remain on a relatively small scale. Implementations are expected to accelerate moving into 2017,” he says.

For now, the blockchain remains a future technology, not sci-fi and not quite sci-fact either. But its scope for eliminating theft coupled with its potential to increase the speed and efficiency of transactions makes it a tantalising prospect.

The next five years will make or break the blockchain, but don’t bet your bitcoins against it becoming the most important anti-fraud technology for the digital age.

“  
The main challenges to creating a consumer blockchain are related to its implementation and do not necessarily detract from the central idea itself

Share this article online via [raconteur.net](http://raconteur.net)

COMMERCIAL FEATURE



# BRAND, BUSINESS AND FRAUD

*Phishing and fraud are most often associated with financial and banking industries, but these days nobody is safe, says **Lori MacVittie**, principal technical evangelist at F5 Networks*

Irrespective of workplace, chances are there are cyber criminals lying in wait to Hoover up both individual and corporate credentials, whether it is through phishing or malware deposited on corporate assets by the simple act of browsing.

OK, you don’t let corporate users browse those kinds of sites. But do you let them browse the *BBC*? *Newsweek*? *The New York Times*? How about *MSN*? All were recently victims of malvertising, where bad guys use top-tier sites to distribute malware-laden online ads through online advertising companies.

Worryingly, a mere 25 per cent of real-world malware is caught by anti-viruses, according to the *Five Habits of Highly Successful Malware*. And, although employee security awareness sessions can have an impact, a recent study shows that 50 per cent of victims still can’t resist opening questionable e-mails and clicking on the link within an hour.

“  
There are tools that address the threats from phishing and malware – a lot of them

Then there’s the ongoing headache of employees in the workplace accessing their financial institutions online, where phishing and malware are rampant.

Research from IDC indicates 30 to 40 per cent of workplace internet access is spent on non-work related activities. This may be why our F5 Security Operations Center (SOC),

which has experts monitoring and analysing real-time threats 24/7, observed that phishing attempts were significantly higher during the week than at the weekend. Monday, in particular, seems a very popular day to go phishing.

Other challenges to contend with include employees accessing corporate assets through an SSL VPN (secure sockets layer virtual private network) or other “protected” portals from outside the corporate walls. The malware that’s sitting in their browser right now doesn’t really care whether it’s grabbing corporate or consumer-related credentials. They’re all worth something to the attacker and, as long as they went to all the effort to infect that device in the first place, why not grab everything on offer?

The reality is that nobody can rest easy; it’s a short step from cybersecurity ignorance to having your name in headlines for the wrong reasons and reputation in tatters. You also have to consider the potential of social media-fuelled noise that can quickly turn pristine brands into mocking memes.

Taking your eye off the ball can come at an eye-watering price. In addition to the reputational hits and their consequences, heavy costs and resources are needed to root out every instance of malware and backdoors, even after a single successful phishing expedition. For example, desktops need to be wiped and reinstalled to eliminate those that got in from drive-by downloads or malvertising. The clean-up process is uncomfortable, whichever way you slice it.

The good news is there are tools that address the threats from phishing and malware – a lot of them. The thing is they are generally categorised as “anti-fraud”, and mentioned in



Lori MacVittie, principal technical evangelist F5 Networks

the context of finance and banking and other money-based industries. But these solutions aren’t peculiar to finance and banking. There’s nothing magical about the way those industries interact with customers that makes anti-fraud only applicable to protecting them.

By adopting the correct solutions, any industry can combat web fraud and the web apps and technologies that trick, deceive and coerce individuals into giving up their credentials.

What the best web fraud solutions do is actively to seek out and prevent the theft of credentials that ultimately assist attackers in breaching security. Whether the attackers are after cash or data is irrelevant. Once they’re collecting credentials, they’re collecting any credentials. And that should be a concern for business in any industry.

For more information please visit [f5.com](http://f5.com), [www.linkedin.com/company/f5-networks](http://www.linkedin.com/company/f5-networks) or contact [@F5NetworksEMEA](https://twitter.com/F5NetworksEMEA) on twitter



sage Pay

YOU CAN'T AFFORD  
TO IGNORE  
**FRAUD**

Safeguard your business  
**with advanced fraud  
screening tools as  
standard** from Sage Pay.

---

Speak to a Fraud expert today

**0845 485 7898**

**#domorebusiness**  
[www.sagepay.co.uk](http://www.sagepay.co.uk)