The London Institute of Banking & Finance

Cyber Security
Special Report

CYBER SECURITY

Find out more at
libf.ac.uk

The dangers of data

Cybercrime is a considerable area of concern for financial institutions around the world. In recent years, Cybercrime activities have facilitated fraud, theft, and invasions of privacy in banking as well as temporarily crippling businesses around the globe including parts of the UK's National Health Service, as the recent "WannaCry" ransomware attack demonstrated.

For financial institutions, who hold some of the most sensitive and personal information on their customers, Cybercrime prevention efforts resemble a near constant digital arms race, with security professionals attempting to pre-empt attacks and hackers who, in turn, create ever more sophisticated software to gain access to customer data and the control of bank digital processes.

The risks to consumers extend beyond their bank accounts being compromised and their money stolen by cyber criminals. Numerous ransomware attacks have seen customers targeted directly, with demands for payments made in exchange for the return of their data. This method, often circumventing the most sophisticated systems banks have in place, relies far more on human error and on scaring customers into paying up. Thus, the challenge for banks is not only in keeping their systems secure, but in educating consumers to ensure that they're able to identify potential threats and take appropriate action to defend themselves.

As stakes increase in the escalating cyber war of hacking, protection development, hacking again, etc. regulators have taken a keen interest. Bank supervisors are likely wondering whether the next banking crisis will be due to risk taking on financial risks or cyber risks. Banks spend a great deal on cyber security. But is it enough? And can banks do it all on their own? Some of the challenges and opportunities are discussed in the articles in this publication. Olivier Kraft, at the Royal United Services Institute, outlines the main threats that banks face. Roy Rubenstein and Ken Wieland discuss some of the technology issues; and David Birch and Frank Stajano look at the human behavioural aspects of cyber security.

Peter D Hahn, *Dean, Henry Grunfeld Professor of Banking*
The London Institute of Banking & Finance

About us

The London Institute of Banking and Finance provides financial education for people at all stages of their lives. From Financial Capability courses for young people to allow them to develop vital money management skills, to cutting edge Higher Education courses for students aiming to pursue a career in banking and finance, to industry-leading qualifications for finance professionals. We advance careers by equipping people with the skills and capability the sector demands, so they can perform more effectively and responsibly. Our qualifications are relevant for a range of roles regardless of experience, and allow individuals to learn in a way that works for them. Our courses are developed and delivered by respected industry practitioners to ensure that they're always of the highest quality.

Content

These articles originally featured in the June/ July 2017 edition of Financial World Magazine, a publication of The London Institute of Banking & Finance in association with CSFI.

The defence never rests

***Olivier Kraft** explains how banks are having to battle increasingly sophisticated cyber criminals and looks at what they are doing to protect their businesses*

Cyber crime poses a considerable challenge to businesses, but that does not mean they are defenceless. The National Cyber Security Centre and the National Crime Agency published a joint report on the cyber threat to UK business in March 2017, setting out steps that businesses can take to enhance cyber security.[1]

Banks are central to this. They face not only the threats that concern all businesses, but also specific risks that require a tailored response. In particular, the criminal use of their information systems in various forms of cyber-enabled financial crime, and the integration of the growing proceeds of cyber crime into the financial system. Each of these has evolved radically in recent years – so should the response from banks and other stakeholders.

A criminal risk turns systemic

Given the amount of customer data and financial information they hold that could have great value for criminals, banks face a high risk of data theft. This may involve directly hacking a bank's information system or fraudulently obtaining the data from customers themselves. The *Cyber Security Breaches Survey 2016* found that businesses in the financial or insurance sectors are nearly twice as likely to suffer from impersonation in emails or online as businesses in other sectors.[2] Stolen data may be used directly by the same criminal (for example to commit identity fraud), or sold to other criminals (for example on the darknet). The thieves are also not just interested in customer data. Criminal hacking into a bank's information systems can target a bank's own assets.

While the challenge of cyber crime is not new for banks, its scale and the extent of public awareness of it are. In February 2016, for example, cyber criminals hacked the SWIFT payment system of the central bank of Bangladesh and instructed transfers from the bank's account with the Federal Reserve Bank of New York. While certain payments were blocked or reversed prior to any withdrawal, it is estimated that Bangladesh Bank lost approximately $81m in that attack.

UK banks have also been targeted. In November 2016, Tesco Bank suffered a cyber attack that led to the theft of £2.5m from customer accounts. These and many other cases over the past year illustrate the growing cyber threat facing banks around the world. The fact that cyber attacks against the banking sector were discussed at the G20 finance ministers' meeting in March is another indication of their potentially significant toll on the financial system.

> *Tesco Bank suffered a cyber attack in November 2016 that led to the theft of £2.5m from customer accounts*

Beyond the cyber attacks

In addition to being direct targets of cyber crime, banks are exposed to a risk of being used to launder the proceeds. Cyber criminals will generally have to make use of money laundering to benefit from their ill-gotten gains. In certain cases, the money-laundering process may rely solely on new payment methods, such as virtual currencies, to circumvent the traditional financial sector. But the banking sector is likely to be involved at a certain stage (eg through deposit of cash by money mules) and directly exposed to illicit funds.

Detecting criminal proceeds has to be part of an effective strategy against cyber crime but poses some difficulties. In particular, the profile of cyber criminals is often different from that of traditional organised crime groups, and the prosecution of transnational cyber crime remains limited, making it difficult to trace proceeds.

How much is involved?

Cyber crime varies significantly in scale, from offences such as phishing, "ransomware" (ie preventing a user from accessing data until a sum of money is paid) or trade in illicit goods on the darknet, to widescale heists such as the ones mentioned already, and attacks on critical national infrastructure. The level of proceeds cannot be estimated precisely: cyber crime is generally considered to be widely under-reported and crime statistics do not always specify whether a crime such as fraud was committed with or without the use of information and communication technology (ICT).

But even in the absence of precise statistics, the proceeds may be assumed to be on the rise. First, the growing number of connected devices (the Internet of Things) and increasingly easy access to criminal software are likely to lead to more cyber crime. That, in turn, will mean more money made from cyber crime. Second, more and more suspicious transaction reports filed by financial institutions point the finger to cyber crime. Consistent with this trend, the European Commission recently submitted a proposal that would require all EU member states to include cyber crime in their list of predicate offences for money laundering.

1. The National Cyber Security Centre and the National Crime Agency (2017), *The Cyber Threat to UK Businesses*. Available at: www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file.

2. HM Government (2016), *Cyber Security Breaches Survey 2016*. Available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf.

Stepping up the response

Banks have long invested significant resources in protecting their information systems. According to the *Cyber Security Breaches Survey 2016,* businesses in the financial and insurance sectors invest more in cyber security on average than businesses in any other sector. Banks have also been cautious in adopting certain new payment methods (eg virtual currencies), taking into account concerns about their potential use for cyber crime, among other risks. But the extent of recent cyber attacks on banks and the increasing risk of money laundering related to cyber crime call for a rapid upgrade of existing strategies.

Banks retain the primary responsibility for ensuring the security of their information systems and data, including through software investment, due diligence on staff, training, reporting of attacks and engagement with customers on cyber security. But internal measures are not enough. Given the complexity and rapidly evolving nature of the threat, with future attacks likely to be novel in both form and scope, a comprehensive partnership between the public and the private sectors is indispensable. In 2015, several large banks launched the Cyber Defence Alliance to share information among themselves and engage with law enforcement agencies on cyber crime. The National Cyber Security Centre, which was launched earlier this year, has a mandate to develop public-private partnerships and help businesses to mitigate the risks they face, including through public guidance, weekly threat reports and the Cyber-Security Information Sharing Partnership. The Financial Conduct Authority highlighted the "increase in volume, scale and complexity" of cyber attacks in its 2017-18 outlook, part of its business plan, and is promoting companies' resilience to such attacks.

Alongside the joint efforts made by the public sector and banks, research into the types of money laundering related to cyber crime will also be needed. Analysing the methods used by criminals to integrate proceeds in the financial sector and identifying potential red flags will allow financial institutions to detect suspicious transactions better. Tracing criminal proceeds is particularly critical when, as in many cases of cyber crime, the underlying offence is committed in another jurisdiction and offenders cannot be easily prosecuted.

> *"The increasing number of connected devices is likely to lead to more cyber crime*

Banks have embraced the endless opportunities provided by ICT, with undeniable benefits for their own internal operations and their customers. The future of those benefits will depend on the banks' ability, in cooperation with the government and business partners, to address the new dimensions of cyber crime and to preserve public trust in the latest technologies. ■

Olivier Kraft *is a research fellow at the Centre for Financial Crime and Security Studies of the Royal United Services Institute. He previously worked on global anti-corruption and anti-money laundering efforts with intergovernmental organisations such as the Financial Action Task Force and the World Bank Group*

A quantum leap in fear

Roy Rubenstein *warns of the threat posed by quantum computing, which could break open the security systems protecting the world's financial data and transactions*

Protecting financial data has always been a cat-and-mouse game. What is different now is that the cat could be de-clawed. Quantum computing, a new form of computer processing, promises to break open the security systems that safeguard much of the world's financial data and transactions.

Quantum computing is expected to be much more powerful than anything currently available because it does not rely on the binary digits 1 or 0 to represent data, but exploits the fact that subatomic particles can exist in more than one state at once.

Experts cannot say with certainty when a fully-fledged quantum computer will exist but, once it does, public key encryption schemes in use today will be breakable. Quantum computer algorithms that can crack such schemes have already been put through their paces.

The good news is that cryptographic techniques resilient to quantum computers exist. And while such "quantum-safe" technologies still need to be constructed, security experts agree that financial institutions must prepare now for a quantum-computer world.

Ticking clock

There is a 50 per cent chance that a quantum computer will exist by 2030, according to Professor Michele Mosca, co-founder of the Institute for Quantum Computing at the University of Waterloo, Canada, and of security company evolutionQ.

A one-in-two chance of a fully working quantum computer by 2030 suggests financial institutions have time to prepare, but that is not the case. Since financial companies are required to keep data confidential for many years, quantum-safe protocols need to be in place for the same length of time that confidentiality is mandated *prior* to quantum computing. So, for example, if data must be kept confidential for seven years, quantum-safe techniques need to be in place by 2024 at the latest. Otherwise, cyber criminals need only intercept and store RSA-encrypted data after 2024 and wait until 2030 to have a 50-50 chance of access to sensitive information.

Unsurprisingly, replacing public key infrastructure with quantum-safe technology is itself a multi-year project. First, the new systems must be tested and verified to ensure they meet existing

requirements – not just that their implementation is secure but that their execution times for various applications are satisfactory. Then, all the public key infrastructure needs to be revamped – a considerable undertaking. This means that, if upgrading infrastructure takes five years, companies should be preparing about now if quantum computers arrive by 2030.

Professor Renato Renner, the head of the quantum information theory research group at ETH Zurich, the Swiss science and technology university, sees potential for even more immediate risk. "Having a full-blown quantum computer is not necessarily what you need to breakcryptosystems," he says. In his view, financial companies should be worried that there are already early examples of quantum computers that are stronger than current computers. "It could well be that in five years we have already sufficiently powerful devices that can break RSA cryptosystems," says Renner.

Quantum-safe approaches

Quantum-safe technologies comprise two approaches, one based on maths and another that exploits the laws of physics.

The maths approach delivers new public key algorithms that are designed to be invulnerable to quantum computing, known as post-quantum or quantum-resistant techniques. The US National Institute of Science and Technology is taking submissions for post-quantum algorithms with the goal of standardising a suite of protocols by the early to mid-2020s. These include lattice-based, coding-based, isogenies-based and hash-function-based schemes. (There is no space to try to explain the maths behind these here. The key is that none of them is based on the multiplication of prime numbers and hence susceptible to factoring, which is what quantum computers excel at.)

Nigel Smart, co-founder of Dyadic Security, a software-defined cryptography company, points out that companies are already experimenting with post-quantum lattice schemes. Earlier this year, Google used it in experimental versions of its Chrome browser when talking to its sites. "My betting is that lattice-based systems will win,"says Smart.

The other quantum-safe approach exploits the physics of the very small – quantum mechanics – to secure links so that an eavesdropper on the link cannot steal data. Here particles of light – photons – are used to send the key used to encrypt data (see box on next page) where each photon carries a digital bit of the key.

> *"Financial companies should already be assessing the vulnerabilities of their security systems*

Should an adversary eavesdrop with a photo detector and steal the photon, the photon will not arrive at the other end. Should the hacker be more sophisticated and try to measure the photon before sending it on, here they come up against the laws of physics where measuring a photon changes its parameters.

Given these physical properties of photons, the sender and receiver typically reserve at random a number of the key's photons to detect a potential eavesdropper. If the receiver detects an altered photon, the change suggests the link is compromised.

But quantum key distribution only solves a particular class of problem – for example, protecting data sent across links such as a bank sending information to a data centre for back-up. Moreover, the distances a single photon can travel is a few tens of kilometres. If longer links are needed, intermediate trusted sites are required to regenerate the key, which is expensive and cumbersome.

The technique is also dependent on light and so is not as widely applicable as quantum-resistant techniques. "People are more interested in post-quantum cryptography," claims Smart.

What now?

BT, working with Toshiba and ADVA Optical Networking, the optical transport equipment maker, has demonstrated a quantum-protected link operating at 100 gigabits-per-second.

What is missing still is a little bit more industrialisation," says Andrew Lord, head of optical communications at BT. "Quantum physics is pretty sound but we still need to check that the way this is implemented, there are no ways of breaching it."

Cryptosystems – two ways to secure data

To secure data, special digital "keys" are used to scramble the information. Two encryption schemes are used – based on asymmetric and symmetric keys.

Public key cryptography that uses a public and private key pair is an example of an asymmetric scheme. The public key, as implied by the name, is published with the user's name. Any party wanting to send data securely to the user employs the published public key to scramble the data. Only the recipient, with the associated private key, can decode the sent data. The RSA algorithm is a widely used example. (RSA stands for the initials of the developers: Ron Rivest, Adi Shamir and Leonard Adleman.) A benefit of public key cryptography is that it can be used as a digital signature scheme as well as for protecting data. The downside is that it requires a lot of processing power and is slow even then.

Symmetric schemes, in contrast, are much less demanding to run and use the same key at both link ends to lock and unlock the data. A well-known symmetric key algorithm is the Advanced Encryption Standard, which uses keys up to 256-bits long (AES-256); the more bits, the more secure the encryption.

The issue with the symmetrical scheme is getting the secret key to the recipient without it being compromised. One way is to send a security guard handcuffed to a locked case. A more digital-age approach is to send the secret key over a secure link. Here, public key cryptography can be used; the asymmetric key scheme can be employed to protect the symmetric key transmission prior to secure symmetric communication.

Quantum computing is a potent threat because it undermines both schemes when existing public key cryptography is involved. ■

ID Quantique, the Swiss quantum-safe crypto technology company, supplied one early-adopter bank with its quantum key distribution system as far back as 2007. The bank uses a symmetric key scheme coupled with a quantum key.

"You can think of it as adding an additional layer of quantum security on top of everything you already have," says Kelly Richdale, ID Quantique's vice-president of quantum-safe security.

"Quantum key distribution has provable security. You know it will be safe against a quantum computer if implemented correctly," she says. "With post-quantum algorithms, it is a race against time, since in the future there may be new quantum attacks that could render them as vulnerable as RSA."

Andersen Cheng, chief executive of start-up PQ Solutions, a security company with products including secure communication using post-quantum technology, argues that both quantum-resistant and quantum key distribution will be needed. "You can use both but quantum key distribution on its own is not enough and it is expensive," he says.

What next?

Mosca says that leading financial services companies are aware of the threat posed by quantum computing but their strategies vary: some point to more pressing priorities while others want to know what they can buy now to solve the problem.

He disagrees with both extreme approaches. Financial companies should, in his view, already be assessing the vulnerabilities of their systems. "Most organisations do not have a detailed map of where all their information assets are and which business functions rely on which crypto algorithms," he says.

Companies should also plan for their systems to change a lot over the next decade. That is why it is premature to settle on a solution now since it will probably need upgrading. And they must test quantum-resistant algorithms. "We don't have a winner yet," says Mosca.

Most importantly, financial institutions cannot afford to delay. "Do you really want to be in the catch-up game and hope someone else will solve the problem for you?" asks Mosca. ■

Roy Rubenstein *is a technology writer who has been covering the telecoms and semiconductor industries for more than 20 years. He is editor of Gazettabyte and co-author of the recent book, Silicon Photonics: fueling the next information revolution*

Keeping one step ahead

Software that makes networks 'programmable' could be an important weapon in the armoury against cyber attacks and transform the shape of banking, writes ***Ken Wieland***

At the Mobile World Congress in 2015, Francisco González, the chairman of Spanish bank BBVA, told the audience: "BBVA will be a software company in the future." This was not the announcement of a radical change of sector, but of the expectation that software will determine the future shape of banking.

One reason for this expectation is that software is set to change networking itself. Software-defined networking (SDN) is one of the most talked about network technologies, along with network functions virtualisation (NFV). Both mean that banks will no longer be constrained by hardware capabilities. Listen to some telecommunication companies (telcos) and their equipment suppliers, and SDN and NFV are set to change the way financial institutions do business.

A recent report by consultancy Ovum – *Creating the Future Network for the Digital Financial Institution* – concluded that a move towards software-defined networks is necessary for some compelling reasons. These include the holy grail of cuts in operating costs, but also, the report argues, more sure-footed regulatory compliance and tighter control on security – prospects sure to interest financial services.

More agile networks, it adds, would also facilitate digital services that put banks on a level footing with companies such as Amazon, Google and Netflix, which have revolutionised customer service expectations.

Banks face a new world of digital competition. Open banking, for example, could, in principle, reduce them to utility pipes operating secure payment services while those companies that react quickly with enticing new products take the lion's share of margins. What will save them, in theory at least, is agility. But quickly and securely bringing new products on-stream in an industry that relies on the confidence and trust of its customers, and has to meet stringent regulatory requirements, is a tall order.

"Our customers are focused on cost, agility and risk," says Tony Evans, managing director of global financial services at Juniper Networks, a US network security and performance company. He argues that software-defined networks can tick all three boxes. A cynic might point out that he would say that but it is clear that banks are facing potentially major business upheavals and patching up existing systems is unlikely to be optimal. Daniel Mayo, Ovum's chief analyst on financial services technology, warns that any move towards SDN cannot be done in a piecemeal way. The technology is disruptive and transformative, and requires significant capital expenditure.

This poses an awkward dilemma for financial institutions. How do you reconcile a strong focus on cost control with a network capital expenditure splurge and, probably, a radical internal reorganisation that could open up new security vulnerabilities?

Safety first

The notion of "programming" the data centre or wide area network (WAN) according to certain policies lies at the heart of SDN. "The reason why SDN is so important is because you can have centralised policy control," explains Winston Carrera, chief technology officer of global banking and financial markets at BT Global Services. "Processes can be automated."

In a non-SDN environment, an IT administrator who wants, say, to reserve data centre resources for mission-critical apps at times of peak demand, or to route data traffic across the network in a certain way to fulfil compliance, has to hand-crank each network element involved in the service. That is a laborious and time-consuming process and one prone to "fat finger" mistakes.

SDN not only seems to promise a way out of the silos and ancient operating systems that bedevil some banks, it would cut operating costs through automation and tighten security by reducing the risk of human error. Once the rules are set, the system instantly starts using them. In principle, artificial intelligence (AI) could also be used to implement a self-learning system, making the SDN both robust and reactive.

What might trouble financial companies contemplating a move to software-defined networking, however, is the heavy reliance on the so-called "SDN controller".

The controller is responsible for centralised policy enforcement and, in the words of Carrera, has as an "omnipresent view of what you do". It has access to all databases needed to go about its business of setting and implementing policies.

In an SDN world, if the controller were compromised, it could wreak havoc on a bank's operations. Carrera says no financial institution has had its fingers burnt in this way, not least because telcos do not expose the SDN controller directly to the "outside world". Are telcos and equipment suppliers downplaying the risk?

Patrick Donegan, principal analyst at HardenStance, a cyber security consultancy, thinks not. "The risk of SDN controller compromise is certainly real. But, in fairness, I do think most vendors understand that very well," he says. "For example, Nokia has been working with leading security vendors like Palo Alto Networks and Clavister to drive its SDN security roadmap." Donegan also points out a recent announcement by Juniper Networks to add five new security vendor partners to support its SDN strategy.

He agrees, too, that SDN – through automation and centralised policy-setting – opens up new opportunities to strengthen cyber security: "Let's not forget that it was a 'fat finger' error that caused the massive Amazon Web Services outage a few months ago." (In March, AWS suffered a domino failure of websites it was supporting when an employee who was debugging the billing system made a mistake.)

SDN also allows a more intelligent approach to managing network security. Particular traffic flows deemed higher risk can be shunted into an intrusion detection system – or quarantined – for what is called, in security circles, "deep packet inspection". Lower-risk traffic can be allowed to flow more freely.

Many in the finance sector seem sold on the SDN promise of clever ways to fend off data breaches. In a global SDN/NFV survey of 100 institutions undertaken by Ovum, better security was hailed as one of the main drivers for future adoption.

Some may argue that a non-SDN world can have advantages when it comes to security, since each bank's network will retain its own idiosyncrasies. Outsiders find such networks difficult to navigate, which means intruders can be at a loss. There is, more importantly, also no single point of weakness. SDN proponents will need to address these objections to change if the technology is take root in the banking sector.

SDN collaboration

If financial companies are to gain the full benefits of SDN, and if telcos and their suppliers are to tap successfully into this still nascent market, Donegan advises both camps to work closely together.

> *"Greater automation can help eliminate security breaches caused by 'fat finger' errors*

"There's still a learning curve to be gone through on the part of both customers and providers," he says. "Some banks may be expecting some security features served up at a faster rate than the industry is able to deliver them. And that's fine – they're pushing the envelope as they should be. SDN also drives the need for change in the internal processes of both the provider and the end customer to derive the available performance and security benefits. The responsibility for closing the gap in alignment lies on both sides."

Although it is still early days for SDN, Mayo says he already sees "some movement" towards software-defined networks in the financial sector. It suggests that longer-term thinking is beginning to make headway. Along with a growing shift towards a hybrid cloud strategy, where banks show a greater willingness to park non-critical applications in the public cloud to reduce costs, Mayo sees SDN as a key ingredient for a leaner and more successful financial services sector. ■

Ken Wieland *is a freelance telecoms writer with more than 20 years' experience covering the fixed and mobile markets. He is a regular contributor to various trade publications and author of extended reports for The Economist Group*

Time to stage Sister Act

Ignore Big Brother. ***David Birch*** *argues that banks should take on the role of Little Sister and use their apps to deliver both security and privacy to customers*

George Orwell got it all so wrong. Remember his vision of Big Brother? Some giant government computer system that would put big-screen TVs in all of our living rooms and use some nightmare always-on version of Skype to connect us permanently to the home secretary? It all seems so quaint now, not least because of our considerable post-war experiences of large-scale government IT projects. It would never have worked as the book imagined because it would have been abandoned halfway through, with billions of pounds down the drain (I would not say wasted, of course, because much of it would have gone to consultants), and the call centre would have been outsourced to the Far East so you could dob in your neighbours 24/7.

There are all sorts of things that Orwell did not see – such as chatbots and the internet, laser beams and "reality" TV. But what he got really wrong was the central conception that it would be the government spying on us when, as it has turned out, it does not need to bother because we are spying on each other, all the time.

The police cannot arrest anyone, an airline cannot "deplane" someone, a footballer cannot have a punch-up on a night out, and a member of the House of Lords cannot snort cocaine without someone recording it on their smartphone and posting it all over Snapgram or Facechat, or whatever is in fad at the time.

Everybody is doing it. It is not revolutionary socialism or social media that is the lever disrupting the old order, it is the mobile phone. In a few short years, it has turned into a combination of remote control for the real world and a Swiss army knife for the virtual one. You cannot leave home without it, whereas I regularly leave home without my American Express card (because I have it loaded into my iPhone by ApplePay).

I have, essentially, volunteered to be tracked and traced wherever I go in return for what Sam Lessin, when he was the head of identity at Facebook, memorably told me was a superpower. And he was right. The ability to communicate instantly with anyone else on the planet, to connect with any or all of the information that mankind has to offer, and (soon) my own artificial intelligence, is indeed a superpower. There is no other way to describe it.

The problem for banks is that they are not making much use of their superpowers. Our mobile phones generate a torrent of data that banks could simultaneously use and protect. Not so much Big Brother, more a sort of Little Sister who generally keeps her mouth shut but occasionally blabs to mum and dad (and the Financial Conduct Authority) if you do something that you should not. She looks after your data, but as data protection regulation becomes ever tighter and more complex so your data, or what I should more properly be calling your personally identifiable information, is turning into a kind of toxic waste that nobody wants to hold. This is precisely why the financial services industry should seize the opportunity to be the Little Sister that delivers both security and privacy to its customers.

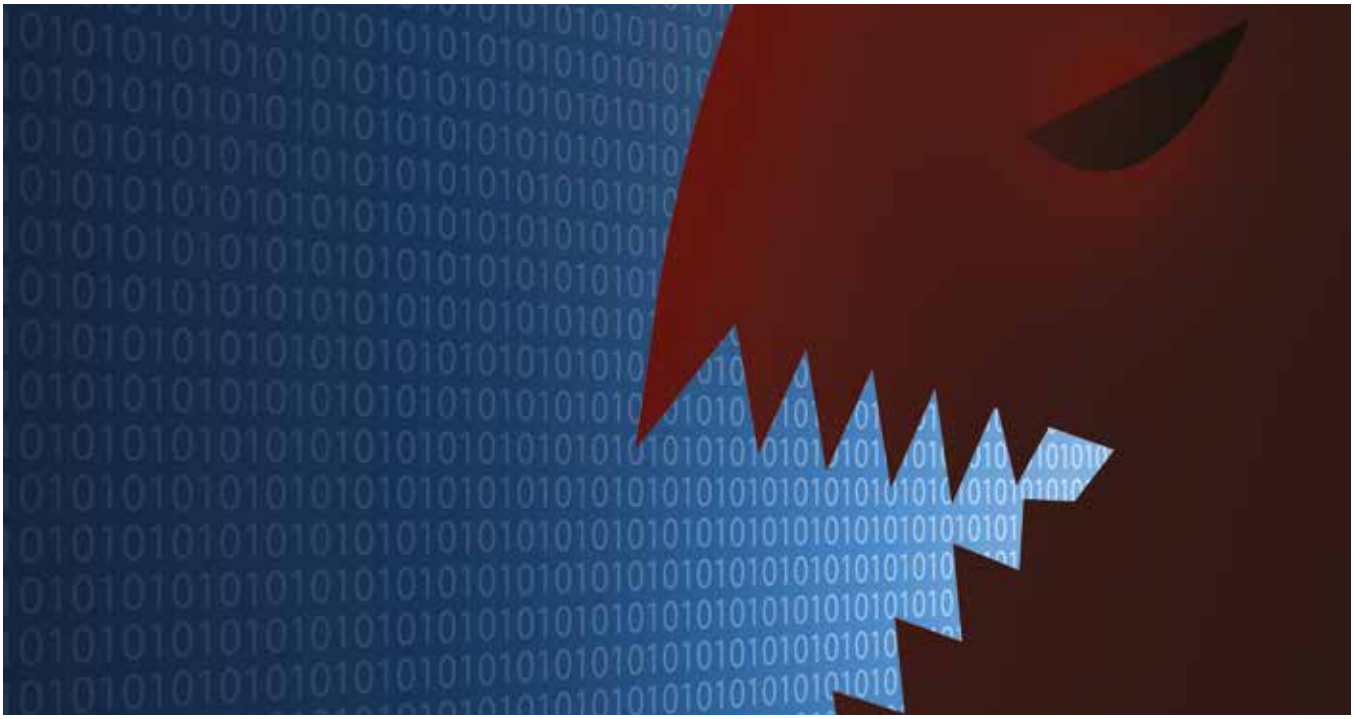
Yes, this is a cyber security challenge and it could all go horribly wrong but, as things stand, the way banks use data is not going particularly right. I can illustrate this with three quick stories.

I was in New York and went to an ATM to get some money. The transaction was declined, falling foul of my bank's well-meaning anti-fraud supercomputer. The next day, I was woken at 4am (ie 9am UK time) by the bank's fraud service calling to ask me if I really was in New York. I did not think anything of it at the time because I was too sleepy. When I woke up, I did wonder if the bank app that is on my phone and that I use all the time might have mentioned to the ATM host that I was in the US in general, New York in particular, and at an ATM specifically.

My second story occurred in London. I was walking down the street when I got a call from a service provider. The first question I was asked was something along the lines of "what is your name and the first line of your address?" but I did not answer because it sounded a bit like the Windows Support people who ring me at home all the time.

Instead I asked for a phone number so I could call them back, but they could not give it to me because they were a call centre. So I asked how I could be sure it was them and they could not come up with a suggestion. Yet all the time that this waste of my time and their money was unfurling, their app was on my phone. If the marketing department, the call centre and the mobile app could be linked through some sort of interconnecting network, then when the call centre rings me with a marketing message, the app could pop up on the phone and say "hey, so-and-so is calling now, can you put your thumb on something to prove it's you". Problem solved – mutual authentication that complies with the directive on strong customer authentication.

In the third story, I was in Woking when I called my bank to enquire about a new service. Not to order anything, I just had a question about business bank accounts. As is normal when you phone a bank that you have been with for many years, they first ask you to authenticate yourself using a selection of publicly available information (eg date of birth and mother's maiden name) and then ask you a series of questions to which they already know the answer. In this case, they also asked me something to do with the countries that I have been working in recently. There was no way I could remember all the countries I have worked in over the past few months, but why should I?



The bank already knows, since my phone and all the financial applications that I use all the time had been with me.

The bank app does not only know who I am and where I am, it knows what I have been doing. It knows everything about me but does not seem able to do much with this data. But it should. The combination of the bank and the mobile operator really ought to deliver something special. For example, the end of PINs because of continuous passive authentication: software running in the mobile phone that checks how I hold the phone, where I go, what I do, how I type and so on. The next time the bank calls, there should be no question of asking me for my mother's maiden name or my PIN because the phone will already know whether it is me or not.

> *The bank app does not only know who I am and where I am, it also knows what I have been doing*

There is no doubt that cyber attacks are a threat to banks, but they are arguably also an opportunity. Banks are trusted as the repositories of our money and that means we are also likely to trust them to hold, and use, sensitive data. Yes, it is true that other companies may be actively fed with more details of our lives – banks are unlikely to know the cat's name without looking at Facebook – but the data that banks collect are data most of us would probably not broadcast.

If you want to know whether I am over 18, whether I am in the UK or not, whether I have travelled to the US in the past month, whether I have bought anything in Waitrose recently, whether I have children at university, whether I have car insurance or whether I play golf… The bank application on my phone already knows and it can attest to a variety of facts about me (with my consent) while keeping all this information safely locked up back in the bank vault. ■

David Birch *is a director of the secure electronic transactions consultancy, Consult Hyperion, and a visiting lecturer at the University of Surrey. He is an internationally recognised thought leader in digital identity and digital money, one of Wired magazine's top 15 global sources of business information and a research fellow at the CSFI*

To err is all too human

***Frank Stajano** discusses the human factor behind cyber attacks and explains what can be done to make a company's computer network more secure*

Is it true that humans are the weakest link in computer security? To simplify the discussion, let us start by leaving them aside. How easy is it for a malicious attacker to get into a corporate network without exploiting its users? It depends. If the attacker's objective is to penetrate any random network in order to attack other targets (for example using it as a base for phishing or spamming), then they will certainly find one that is vulnerable. If, on the other hand, their objective is to penetrate a specific network because of the assets it contains (for example for financial fraud, industrial espionage, extortion or sabotage), then penetration might range from very easy to very difficult, depending on how competently that network is protected.

The first lesson here is that most bad guys do not care about you in particular: your first concern should simply be to avoid being an easy target. When the script kiddies fire off their scanning programs, performing the electronic equivalent of rattling the handles of all the doors in the neighbourhood, you just do not want your own door to open right away. Let them attack someone else. As a baseline, ask your security experts to configure your systems securely, to keep the security patches up to date and to monitor for intrusions. (You have competent security experts you trust, right? OK, we could all do with a few more.)

The second lesson is that it is essentially impossible to make a system totally invulnerable: with enough resources, any system can be penetrated. With government-class "advanced persistent threat" attackers, who have access to zero-day vulnerabilities ("zero-day" meaning that the vulnerability has never been flagged up, so there is no time to mitigate it), and who can inject a trojan into the firmware of the routers you just bought before they are shipped to your premises, all bets are off. There are countermeasures to such threats but are they worth it? Do not ask for invulnerable security: it requires military-style operational security practices that would make it impossible to get any productive commercial work done, and it comes with infinite cost, such as designing and fabricating your own microprocessors, chipsets and motherboards (witness the major security vulnerability discovered in May and affecting essentially every Intel platform built between 2008 and 2017).

So, the third and most important basic lesson is that information security is not cryptography but risk management. The only mature approach to security is to start with an assessment of what your assets are, how valuable they are to you, how valuable they are to potential attackers (not the same thing), how easy they are to compromise, how expensive they are to defend, and so forth. And then to decide, as a strategic board-level decision, how risk-seeking or risk-averse you are, and how much you are willing to invest in preventive measures (a potentially unnecessary but certain expense) to avert the possibility of being successfully attacked – a loss that might or might not happen.

But let us go back to our original question. It is true that the prevalent network attacks today, phishing and ransomware, are computer-aided frauds that target humans rather than machines. This often prompts the comment that it is those pesky users (your employees) who make the system insecure. I believe this is a wrong-headed attitude that will not make your company safer.

A few years ago, I partnered with Paul Wilson,[1] co-author and star of the popular TV series *The Real Hustle*, to investigate the psychological foundation for frauds and scams. Many of the hundreds of scams we considered worked by exploiting a handful of psychological traits that are part of human nature. As you might expect, most of today's computer-based frauds exploit the same psychological traits, which were around long before computers. For example, according to what we called "the social compliance principle", society trains us not to question authority, and fraudsters exploit this ("I am your bank and, if you do not verify your login now, we will close your account").

> *It is essentially impossible to make a system totally invulnerable – any system can be penetrated*

Another trait, the "herd principle", suggests that, when a situation looks dodgy, we feel reassured if many others are engaging in it. Fraudsters, therefore, surround us with accomplices who engage confidently in the suspicious behaviour and implicitly reassure us that it is all legitimate. Think fake reviews on restaurant-rating websites. Subtle manipulation of swing voters is a more ominous example that is topical nowadays, with the involvement of Cambridge Analytica in the Brexit and Trump campaigns.

Other psychological buttons that the fraudsters might push include greed, distraction, time pressure and, cynically, our kindness. The exact set of exploitable psychological vulnerabilities is not so important. What does matter is that the hundreds of frauds we examined all exploited combinations of the same few psychological vulnerabilities. The crucial insight is that these vulnerabilities are part of human nature, and that they are there for a reason.

Why did medieval suits of armour have joints? Were they not

1. Stajano F and Wilson P (2011), 'Understanding Scam Victims: seven principles for systems security'. *Communications of the ACM*, 70-75. Available at: http://dl.acm.org/citation.cfm?id=1897872.

the weak point that enemy swordsmen always targeted? Yes, but without joints you could not move. With psychological vulnerabilities, it is similar: each exists for some good reason. We react to time pressure by switching to quick heuristics rather than full logical reasoning because that is what saved our ancestors from becoming lunch when they heard the roar of the sabre-toothed tiger.

The most important lesson for the security engineer is that you cannot hope to remove the vulnerability just by telling users what they should do, especially against an adaptive adversary who will invent a different scenario to trigger the same reaction. An explanation, or blaming the user's gullibility, will not change human nature and will not get the desired results. A better solution is to design the system with the expectation that users will continue to be human: the technical defence must protect the system even if users react to well-crafted malicious stimuli according to those predictable failure modes.

Is it possible to manage internet security without restricting the sites that can be accessed? Sure. This may not apply to basic and repetitive jobs but, where appropriate, productivity and morale are increased by empowering team members to take the right decisions: the warning ("we rate this site as 80 per cent likely to be fraudulent; are you sure you wish to proceed?") might be coupled with a logged and explicit assumption of responsibility ("please explain why you need to access the site despite the warning, and click here to accept responsibility for the consequences").

A similar approach, without the logging, is used by the Firefox web browser: when a user attempts to open a website that others have reported as fraudulent, the browser instead puts up a red page with a conspicuous warning. It is still possible to proceed to the website if desired, but it cannot happen inadvertently. Similarly, Firefox makes it difficult to visit a website whose Transport Layer Security certificate (a cryptographic protocol that provides communication security over a computer network) fails to verify, except if users confirm they know what they are doing by clicking the correct sequence of options in a purposefully technical dialog box.

A useful guideline to protect your system, while acknowledging the existence of these universal psychological vulnerabilities, is to be parsimonious in imposing security policies on your employees. Security measures are "a tax on the honest": something annoying that gets in the way of employees doing their work.[2]

Analysis of user response to security policies suggests that every person had a "compliance budget": a finite amount of goodwill that is gradually depleted every time they comply with some annoying corporate policy. Once it runs out, the person becomes fed up and stops cooperating. Spend that budget wisely and do not annoy your employees with trivia, such as gratuitous password requests that interrupt the workflow, if you want them to have some goodwill left to comply with the policy items that really matter.

To conclude, here are three parting thoughts for security, three important goals to which I have wholeheartedly devoted my academic and entrepreneurial efforts.

First, we need more security experts. In addition to my university teaching, with support from academia, government and industry, I started two hacking competitions, Inter-ACE and Cambridge 2 Cambridge, to raise a new generation of skilled cyber defenders.

> *"Many of the scams worked by exploiting a handful of psychological traits that are part of human nature*

Second, computer people have a moral duty to build a digital society that is secure and fair for its citizens. I embarked on a crusade to eliminate passwords because we cannot give people an impossible task and blame them for not completing it. We are now turning this project into an open-source start-up, Pico – a hardware token that relieves the user from having to remember passwords and PINs .

Last but not least, users are a crucial component of the system. My message to system architects is that, rather than blaming users, understanding and accepting human nature is a necessary step towards making systems truly secure. ■

Frank Stajano *is a tenured academic at the Faculty of Computer Science and Technology of the University of Cambridge, where he is the head of the Academic Centre of Excellence in Cyber Security Research. He is a founding director of two cyber security start-ups, Cambridge Cyber and Pico Authentication, and a founder of the Inter-ACE and Cambridge 2 Cambridge cyber security competitions*

2. Beautement A, Sasse M and Wonham M (2008), 'The Compliance Budget: managing security behaviour in organisations'. *New Security Paradigms Workshop*, 47-58. Available at: http://dl.acm.org/citation.cfm?id=1595684.

The London Institute of Banking & Finance

JIBS EVENTS

London Financial Crime Prevention & Compliance Symposium

Hosted by The London Institute of Banking & Finance (LIBF) and JIBS Events, this inaugural thought-leadership symposium offers the valuable opportunity to reflect upon the key challenges faced by the financial services industry, whilst also equipping delegates with enhanced awareness of the compliance requirements in the fight against financial crime.

Agenda to include:

- London's role in preventing international economic crime
- OPBAS: Developments in the UK AML framework
- Preventing terrorist financing from the frontline perspective
- The role of the Office of Financial Sanctions Implementation (OFSI)
- The Criminal Finances Bill – key considerations for financial services professionals

Available discounts:

20% for members of: LIBF

10% for members of: ACAMS, ICA, ICSA, IoD and STEP

07/09/2017	09:00-17:00	CPD 7	£595	Grange Tower Bridge Hotel

Find out more and book online: www.LondonSymposium.com