Advanced 365 Thought Leadership Series

The Future of Data Security in Financial Services

David Smith, Chief Executive
Global Futures and Foresight

www.advanced365.com

Sponsored by Advanced 365

Written by Global Futures & Foresight

Contents

The Future of Data Security in Financial Services:

There is currently a paradox facing financial services providers as the technological and social revolution demands a new approach to customer service that utilises new tools in an ever more customer friendly manner. However, increasing cyber-crime has resulted in new waves of regulation that ostensibly threaten the ability of firms to roll out such consumer facing processes and tools. Those firms that reap the greatest rewards from the ever evolving technology options are those that successfully maintain the balance between these two opposing forces of access and security.

Traditionally, security has focussed on preventing unauthorised access to information but the nature of threats has developed to a point where prevention alone is not sufficient. The average breach inside major companies remains undetected for 229 days and only twenty one percent of attacks are discovered on the same day they are launched. The nature of security breaches has matured, often faster than the traditional prevention solutions: therefore, security must now also evolve to ensure that detection and response mechanisms are in place across an organisation with every member of staff becoming a key part of this detection and response mechanism.

This level of organisational change needed will see several players move outside their comfort zones. New partnerships, internal processes and an acceptance that prevention alone cannot suffice as a cyber-security strategy, are prerequisites for some of the changes, whilst agility and rapid response need to be introduced into this new approach.

Financial Services firms must prioritise their investments of time and money and accept that their security strategy will no longer be about identifying threats and preventing them, but will be about defining areas of risk and developing mitigation strategies to match these.

Whilst many of the trends described in this paper are already visible, the coming decade is likely to be more disruptive. Financial services providers need to overcome the general industry levels of conservatism – both organisationally and technologically – if they are to adapt to the new world and the demands it places on security policies.

Where we are now

A new era of cyber-crime

Cyber-attacks targeting financial services firms are on the rise, with ninety three percent of financial services organisations experiencing cyber-threats in the previous year[1]. Among 758 financial services respondents to a 2015 PwC survey, the average number of information security incidents detected climbed eight percent in 2014 to a record-breaking 4,978 per organisation[2]. Despite this, only seventy percent of executives from financial institutions believe that cyber-security is a strategic risk for their companies[3], yet banks in the UK spend at least £700 million a year on cyber-security[4]. The efficacy of this spend should also be questioned; some eighty eight percent of cyber-security attacks on financial services firms succeed in less than one day, yet only twenty one percent of these attacks are discovered in the same one day time frame[5].

An inconvenient truth

In the words of Scott Vernick, partner at Fox Rothschild, '...there are only two types of companies; those that have been hacked and those that don't know they've been hacked[6].' This inconvenient truth is leading to the realisation that many cyber defences are preparing for yesterday's threat, not tomorrow's. Despite this, security is still seen in some quarters as a short-term function and of little strategic value. Broadly speaking, the notion of cyber-security as a source of competitive advantage in a world built on increasingly complex automated systems is only now starting to become apparent.

Financial losses are increasing - cyber-crime costs the global economy £266 billion and affects more than 800 million people a year[7]. The losses from security attacks, however, may not be as damaging as the potentially greater impact on customer and investor confidence, reputational risk and regulatory impact.

Ever changing regulatory and legislative requirements

The law moves slowly compared to the technology and security fields, but significant and far reaching regulatory changes that have been a long time coming are imminent. Some have already arrived. It is likely these changes will trigger more progressive data protection regulation in other jurisdictions[8].

In June 2014, in a global first, the UK finance industry launched a cyber-security framework for sharing detailed threat intelligence, testing cyber-security and benchmarking financial service providers*. As part of the proposed new accountability provisions, senior managers will be required to take responsibility for all aspects of their business, which includes the security of the technology integral to the effective functioning of the UK's financial systems**.

The EU is currently finalising new General Data Protection regulation that will apply one consistent set of requirements for all organisations that hold data on European citizens. The legislation is very broad and covers many aspects of personal data. Under the proposed legislation, if you suffer a breach of personal data you can incur fines of up to €100 million or five percent of annual turnover[9]. The EU General Data Protection Regulation is expected to reach its final form in 2015[10] and promises to be a great driver of regional market data security spend.

The maturing market

According to a new report by Allied Market Research, the global Internet security market is expected to reach $42.8 billion by 2020, registering a compound annual growth rate (CAGR) of eight percent during the 2014-2020 timeframe[11]. Others forecast double that. ABI Research calculates cyber-security spending for critical infrastructure protection will reach $109 billion globally by 2020[12]. The rationale behind such growth is simple; the value at stake is enormous. It is estimated that the asymmetric effect of a relatively small number of high profile attacks and resultant government regulation could lead to the world capturing less of the $10 trillion - $20 trillion available from big data, mobility, and other innovations by 2020; the ultimate impact could be as much as $3 trillion in lost productivity and growth[13].

* The CBEST framework was developed by the Council of Registered Ethical Security Testers(Crest) and cyber intelligence company Digital Shadows in collaboration with the Bank of England, Her Majesty's Treasury and the Financial Conduct Authority (FCA).

** Although not directly related to cyber security, in November 2014, the FCA and the Prudential Regulation Authority (PRA) fined the RBS Group nearly £60m for IT issues. The FCA was deeply concerned by the actual and potential consumer disruption and, while most firms are not subject to dual oversight, it shows how the PRA will view IT incidents as having the potential to have an adverse effect on the safety and soundness of a firm and the PRA's statutory objectives.

Financial services and cyber-crime: emerging themes

The rising risks of third-party partners

Reimagining the financial industry as an ecosystem is already underway for many executives, as the highly intertwined and increasingly entrepreneurial landscape emerges. However, only sixty two percent of financial services providers surveyed by PwC have established security baselines and standards for external partners, suppliers, and vendors, and just fifty nine percent require business partners to comply with their privacy policies[14]. This suggests that the self-certification process that has traditionally marked many relationships will give way to a more active cyber-risk mitigation and monitoring regime.

As such, organisational boundaries will blur somewhat as some form of standardised security becomes increasingly built in to third party products, services or enabled capabilities. The evolution of the ecosystem is a necessity for the financial industry, and it is likely that cultural fit, with regards to risk will become an increasingly important consideration in choosing with whom to partner.

Reorganising business structures

Booz Allen notes that many of their clients are making a paradigm shift as they accept the futility in relying on a solely preventative approach to security. As a result, more banking institutions are setting up so-called 'fusion centres' that analyse big data from a number of departments, such as cyber-security, fraud and physical security, as well as from third parties[15]. As the type, quantity and complexity of data increases, reorganising business structures to more efficiently combat the shifting threat will increase in importance; enabling improved business intelligence, a more rapid response to threats, reduced costs and ultimately, better leverage of scarce data and science talent.

However, sixty one percent of financial services respondents cite, 'ensuring that critical data is secure,' as the number one role for IT versus an average of forty six percent for other industries[16]. Information security must evolve from just an IT project to the core of critical business decisions, especially since impactful technology decisions are being made with increased frequency in non IT departments - such as marketing[17] The rise of shadow IT represents a significant barrier to holistic organisation wide prevention policies and responses, and at the very least, increases the need for CMO-CIO collaboration. This is only the most obvious area however, and the need for wider organisational structures to adapt to help optimise security procedures will also become apparent

No wall is high enough

There is a growing acceptance that information will need to be protected at the database and data element level. This raises an interesting question; how does an organisation designate which data is of key importance, and how does it limit the value of (stolen) raw data? If the premise of protection at the micro-level is correct, then approaches to data security will invert; the focus will shift from keeping people out with bigger walls, to a 'defence in depth' risk-based approach around high-risk and high-value repositories.

There are emerging technologies, as explored in figure 2, such as the use of tokenisation that yield raw data useless by adding levels of protection[18], as well as an emerging range of technologies that could provide significant challenges for security providers.

Sixty one percent of financial services respondents cite, ‘ensuring that critical data is secure,’ as the number one role for IT

New payment technologies bring new risks

One such challenge lies in the fundamental way we pay for things. Mass market adoption of Apple Pay is expected to occur in mid to late 2016[19]. The global mobile wallet market is forecast to expand thereafter and reach $5.25 trillion in 2020, with compound annual growth more than doubling each year to 2020[20]. As companies increasingly adopt such payment systems and consumers embrace them, the likelihood for hackers to target underlying technologies such as Near Field Communication (NFC) or Bluetooth, rises. This distributed payment ecosystem should adjust expectations to assume that breaches will occur and build security around the data element. The enormous generation of data in new payment ecosystems also provides the basis of new cyber-security methods.

Big data becomes a key weapon in fighting cyber-crime

Big data represents an interesting mix of opportunities and challenges for those involved in data security. Cybercriminals can hide within big data as well as use big data algorithms in a number of malicious ways (more in figure 3) yet, big data processes and tools also offer a potentially revolutionary way of managing cyber-security. Gartner suggests that big data informed cyber-security could offer numerous benefits[21]. First, it could '...cut down on the noise and false alerts in existing monitoring systems by enriching them with contextual data and applying smarter analytics.' It also promises to correlate the resulting high-priority alerts across monitoring systems to detect patterns of abuse and fraud, and to get the big picture on the security state of the enterprise.

Systems could then pool their internal data and relevant external data into one logical place, and look for known patterns of security violations or fraud. Data scientists will increasingly analyse and correlate security data as well as unstructured business data to reduce the risk of breaches[22]. By profiling accounts, users or other entities, and looking for anomalous transactions against those profiles, big data could enable users to remain agile, and stay ahead of malicious actors and activities. Ultimately, the use of powerful, real-time analytics across multiple data sets – both structured and unstructured – could increase operational efficiency and facilitate faster time-to-remediation[23].

Staffing for success

Possessing the data analytics infrastructure to better adapt to, react and counter threats, is irrelevant if the skills are not available to utilise the output from these systems. The skills gap is growing larger with some governments forecasting that the current demand for security professionals may only be met by 2030[24].

The issue of staff proving critical in cyber-security is brought into focus when one considers their role as the cyber-security threat themselves. Ninety five percent of all financial services security incidents investigated by IBM recognised human error as a contributing factor[25]. PwC notes that in 2014 '...the number of security incidents attributed to insiders—current and former employees, in particular—increased substantially, even as the readiness of financial firms to manage these risks diminished.' In fact, when asked to identify the likely source of security incidents, forty four percent of financial services respondents cited current employees, easily the most commonly named culprit and nine percent higher than all industries' average[26].

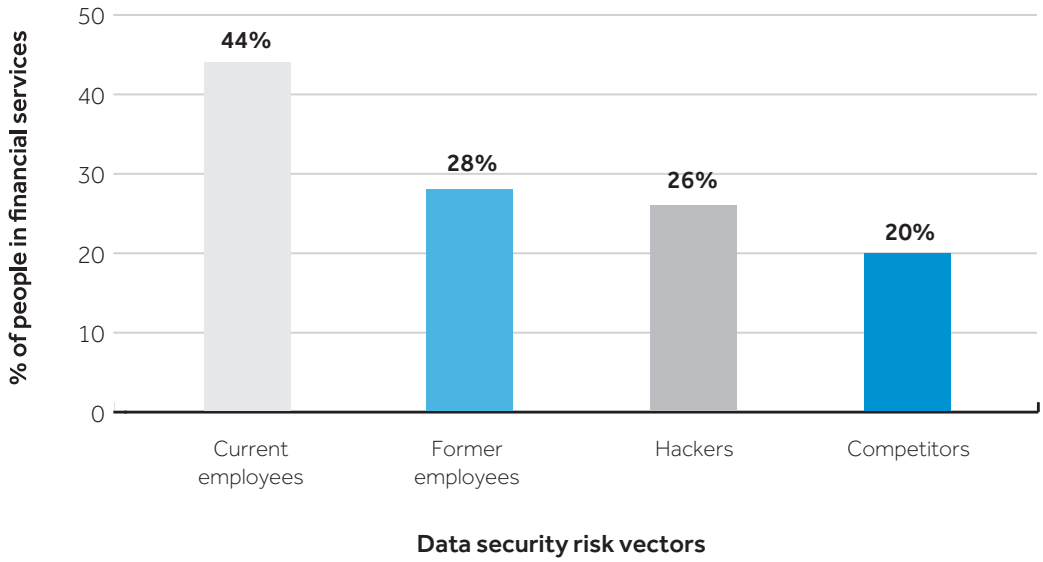
Many businesses do not have an insider-threat program in place; organisations that have an employee training and awareness program dropped to fifty seven percent in 2014 from sixty six percent in 2013[27].

When asked to identify the likely source of security incidents, forty four percent of financial services respondents cited current employees

Breakdown of risk vectors

Of the four most commonly cited risk vectors, employees feature prominently within financial services as can be seen in figure 1[28].

Figure 1: Risk vectors reported by those in FS



What FS players are doing about cyber-security

Sixty percent of executives interviewed by McKinsey think the sophistication or pace of attacks will increase more quickly than the ability of institutions to defend themselves[29]. This clearly underscores the need for some sort of collaborative security approach, although this may prove difficult given that, one in five suspect attacks are coming from direct competitors.

Large companies reported cross-sector gaps in their risk-management capabilities – indeed ninety percent had "nascent" or "developing" capabilities. Only five percent were rated 'mature' overall across the practice areas studied[30]. Perhaps the lack of expertise is due to conceiving cyber-security as a cost with little benefit, as opposed to a strategic driver of business. Worryingly, twenty eight percent of financial services organisations think that the risk of damages from cyber-crime is outweighed by the cost of prevention[31].

Given that cyber-attacks are considered a 'tier one' security threat in the U.K., on par with terrorism and since banks are a key part of the national infrastructure[32], there is considerable state interest in ensuring financial service safety. Plans have been put forward by the U.S. and U.K. governments for systemic penetration testing, which helps simulate attacks and pre-empt weaknesses in defence and detection. Europe's first business accelerator programme focused on cyber-security was launched in London in 2015, with backers aiming to tap into the technology start-up scene and build on links with the UK government[33]. More open sharing of threat details will stand all those participating in better shape.

It is likely that a few organisations will develop a more aggressive approach. Gartner predicts that by 2020, twenty five percent of global enterprises will engage the services of a 'cyber-war mercenary' organisation, including threat intelligence services[34]. Although threat intelligence is currently a costly proposition and an immature market (i.e. lacking measurement parameters, such as reliability of information and risk assessment[35]) as the threat of regulatory induced fines increases in cost, this area could develop significantly.

Banks

In addition to closer government-industry information sharing*, the Financial Crime Alerts Service is designed to allow banks and other financial groups to react faster to major incidents and to learn of the latest techniques being used by fraudsters, cyber-criminals and terrorists[36]. The British Bankers' Association said it was working with its preferred technology partner, BAE Systems Applied Intelligence, to launch the new service in 2015 and is aiming to sign up as many of its members as possible.

A study from recruiters Robert Half revealed that fifty two percent of finance bosses plan to increase spending on cyber-security – with thirty nine percent planning to take on more employees to cope with the extra work, and forty three percent to spend on data analytics tools[37]. Such actions are already being realised. Investment bank JP Morgan is spending a reported $150 million (approximately £90 million) on cyber-security[38], whilst HSBC hired Jonathan Evans, a former head of MI5, in May 2013 to combat financial crime, and the Bank of England hired a geopolitical analyst to understand international tensions[39]. These moves confirm that many now realise that risk is solely a technological issue. Royal Bank of Scotland (RBS) and NatWest customers meanwhile will soon be able to log in to the banks' mobile banking app using their fingerprint[40].

* To prevent the spread of cyber-attacks, banks are also privately sharing information about their own cyber threats and vulnerabilities with other firms, IT analysts and government agencies in real time, on a new government platform called Cisp

Banks that have taken advanced security measures can use a defensive technique, known as 'sandboxing,' to isolate the malicious code of a zero day attack (an attack that exploits a previously unknown vulnerability in a computer application or operating system) before it is executed, then analyse and identify it as malware[41]. Several U.S. banks are gathering data by participating in so called 'carder forums,' where card numbers are sold for $20 to $100 a piece, often in batches of up to one million. Some banks, it transpires, are even engaging in the bidding to ascertain what the hacker knows and the areas of data still vulnerable[42].

Credit card companies

MasterCard has announced additional cyber-security investment of $20 million in 2015, including biometric protection for mobile apps, and early warning alerts on potential threat vectors[43]. In September 2014, MasterCard claimed a ninety eight percent success rate for internal pilot trials of a biometric verification system combining both voice and facial recognition. In the spring of 2015, MasterCard plans to launch Safety Net, an initiative designed to reduce the risk of fraud or cyber-attacks before issuers and processors might notice the threat. The application uses algorithms to score and monitor different channels, geographies, and business sectors, and is designed to intervene only in extreme cases to block fraudulent activity.

In September 2014, Visa launched the Visa Token Service (VTS), which replaces sensitive credit card information, such as the 16-digit account numbers, expiration dates and security codes, with so-called tokens[44]. The tokens are a unique series of numbers that can be used to make payments without exposing actual financial information. Over 500 financial institutions have already started implementing VTS and the service is set to expand, with tech companies and device manufacturers planning to deploy VTS on mobile devices.

Mobile payment applications are also likely to see tokenisation – in fact, the retail industry has expressed its intention to develop a universal standard. Tokenisation has also been embraced by American Express.

Since some of the sources of cyber-risk are relatively prosaic, not all responses require a highly technical component. Using DMARC (Domain-based Message Authentication, Reporting & Conformance) email authentication for example, PayPal detected a significant reduction in the number of phishing email attacks in the last quarter of 2014. When comparing attacks against financial services companies, the percentage against PayPal 'decreased by 14.09 percentage points: from 44.12 percent in 2013 to 30.03 percent in 2014[45].'

Adjacent industries

There are a number of interesting moves by those in similar industries in using cyber-security strategically, which could be adopted by those in financial services to strengthen their understanding of pertinent issues. In 2013 Deloitte joined forces with De Montfort University to launch an MSc in cyber-security whilst PwC established a new partnership with Royal Holloway and sent nine of its security experts on the university's masters programme in information security[46].

The FT also reports that '...to allay clients' fears that professional services firms are taking their own cyber-security seriously, some experts have suggested that the industry should move towards a cyber-security standard, similar to the way that company audits are certified. An alternative solution could be to standardise the cyber-security policies issued by insurance companies, but the market is immature and prohibitively expensive[47].'

MasterCard has announced additional cyber-security investment of $20 million in 2015

The Public View

Cyber-security and public trust

In the U.K., only thirty two percent of people trust their retail banks whilst seventy three percent would be more excited about a new financial services offering from Google/Amazon/Apple/Square/Paypal than their own bank[48]. PwC have gone as far as suggesting that as soon as 2025 to 2030, a market economy could readily exist without banks as we have traditionally known them[49]. The need for banks to redesign their business model is well documented, but doing so with a clearly compelling (and immediate) business proposition is needed.

Others in the financial services ecosystem compare even less favourably than retail banks. Investment banks are only trusted by fifteen percent, whilst a lack of simplicity and customer centricity sees financial advisers poll at twenty eight percent and insurance providers at twenty seven percent[50].

However, fifty two percent trust banks with their private data (c.f. online retailers at 22%) and there would appear to be a strategic opportunity for financial institutions to develop their reputation as trustworthy custodians of customer data. Clearly, the strategic component in data security cannot be overlooked by financial services providers. Perhaps the need to develop competitive advantages through technology is best illustrated by Goldman Sachs decision to start referring to itself as a 'technology company[51].' Such moves, if accompanied by clearly communicated changes in process, could help rebuild trust.

New privacy compact

Booz Allen suggests that '...the next generation of privacy is focused on the halo of information around individuals – the transactional, behavioural and navigational information generated as individuals move and interact through the online and physical world. This information is not currently regulated, yet consumers expect a high level of protection. Companies that manage this well will create a competitive advantage through customer loyalty and insight[52].' In areas where regulation is lacking but customer trust is at stake, financial services providers should enact best (or perhaps most effective) practice for this data as part of their holistic data security strategy.

New business opportunities for financial security

Identity management

Lloyds is one of a number of banks making an attempt to carve out a place in the burgeoning world of digital identity storage. Lloyds has been working with the Prime Minister's office to test whether it would be possible for banks to vouch for their customers to retailers and government agencies via a simple smartphone app[53].

Barclays has made a separate bid for safeguarding customers' identities by unveiling scanners that identify account holders by their fingers' unique vein patterns, which is more secure and less prone to hacking than fingerprint biometrics. The biometric information is stored in a small egg-shaped device that remains in the customer's possession, rather than being held by the bank. With an appropriate marketing effort, customers may well decide that such services offer value and could serve as the most trustworthy store of personal information.

Cyber insurance

Marsh & McLennan Cos. estimates that the U.S. cyber insurance market could have doubled in 2014 to $2 billion in gross written premiums from an estimated $1 billion in 2013. In Europe, the market is estimated to be less than $150 million, rising by 50 percent to 100 percent annually[54]. The European cyber coverage market could get a sizeable boost from draft EU data protection rules in the works that would force companies to disclose breaches of customer data to them[55]. 'In three to five years, a considerable number of our clients will likely have cyber coverage,' suggests Oliver Dobner of Marsh (German operations)[56].

The dynamics are present for rapid growth; due in part to the rapidly escalating cost of not acting. PwC says that the average loss in reputational or brand value for a company experiencing a data breach can be between $184 million and $330 million, and the collective loss when customer trust is considered can be even higher[57].

By 2020, private firms will be buying cyber-security insurance when they sign up for product liability coverage and other basic policies, suggests the U.S. government[58]. Earlier 2013 forecasts set the cyber insurance market for $5 billion of premiums by 2020 in the U.S. alone but given the rate of growth in 2014, it is likely this estimate is overly conservative[59].

The Future of IT Security and Complience in Financial Services

'In the months and years ahead, what it means to detect and protect in cyber will be redefined,' says Sedar LaBarre, a Principal with Booz Allen[60]. FireEye's CEO David DeWalt suggests that this is because at present, '...companies are spending tens of billions of dollars of their money on a model (antivirus software) that doesn't work[61].' The acceptance that preventative services cannot be solely relied on will be a cornerstone of data security in the future, even as the array of preventative services evolves.

Organisational and even wider ecosystem responses, will form one key tenet of future cyber-security, whilst technology will form the other. One without the other is unlikely to prosper. Threats will grow in frequency and sophistication as new vectors of attack are opened including cloud and mobile computing, big-data analytics, the Internet of Things and artificial intelligence. Such technologies, as hinted at earlier, can also counter these risks, yet no single organisation has the necessary capabilities to mitigate all the risks. Partnerships are therefore critical and must include information-sharing, governance, research and education[62].

Northrop Grumman notes that we will require'... new frameworks for security as a science with the rigour of physics and mathematics. Newton's Laws for cyberspace have not yet been developed[63].' In short, new, as-yet-untested models of security are needed that can deal with new and evolving threats such as deeply embedded advanced persistent threats (APTs) and other variants. Here are several tenets along which new models could be developed[64]:

1) Prioritise information assets based on business risks.

2) Provide differentiated protection based on importance of assets.

3) Deeply integrate security into the technology environment to drive scalability.

4) Deploy active defences to uncover attacks proactively.

5) Test continuously to improve incident responses.

6) Enlist frontline personnel to help them understand the value of information assets.

7) Integrate cyber-resistance into enterprise-wide risk-management and governance processes.

8) Organisations will focus on adapting prevention technologies to be more about containment and data loss mitigation after an initial infection[65].

The acceptance that preventative services cannot be solely relied on will be a cornerstone of data security in the future, even as the array of preventative services evolves

The organisational response

It is, perhaps, natural to view technology, and by extension the IT department, as both the cause and the cure for cyber-security issues. Cyber-attacks exploit technological weak links, yet the belief in ever more sophisticated technology to remedy cyber weakness is also well established.

This would seem well supported by data; the average breach inside a major company goes undetected for 229 days[66]. The financial system and global economy are evolving into real-time constructs yet too many in financial services experience a lag in their security. A purely technological response, suggests Harvard Business Review, ignores the fundamental drivers of information security risk: organisational culture and the behaviours that result from it[67]. Hitherto, security and convenience have been somewhat inversely related - the greater the security provided, the less convenient it is for individuals (customers and employees). However, this could begin to change thanks to both technologies and a shifting organisational perspective of cyber-risk, which has now moved beyond being an operational issue, to one of the top issues corporate boards must face[68]. This will necessitate organisational change; by 2018, IDC estimates, fully seventy five percent of chief security officers (CSO) and chief information security officers (CISOs) will report directly to the CEO, not the CIO[69]. FireEye also believes that '...fewer organisations will run their own security operations centre (SOC).' It also adds that businesses should '...shift from a peacetime to a wartime mindset[70].' For this, strategic use of technology is critical as is an understanding of the limits and challenges of such technologies.

Technological

Future technologies to combat cyber issues

Since the range of security issues is so broad and encompasses highly sophisticated zero-day attacks as well as something as prosaic as working on a laptop in a public area, no single technology has the potential to neutralise all threats. Nevertheless, according to the UK government, '...about eighty percent of known attacks would be defeated by embedding basic information security practices for your people, processes and technology[71].' Emerging and future technologies are listed below in figure 2.

Figure 2: Technologies to help combat cyber-crime

Technology/trend	Description
Big data	Neil Passingham, Technical Solutions Director at HP, believes that security is behind the threat curve. "We need to make the most of big data and the cloud for example. We need to align serious solutions that secure the business" he says. The perimeter needs to shrink to an absolute minimum core data piece, where data simply cannot be breached. Beyond that, the focus must be on advanced encryption techniques, and security analytics that exploit the power of big data[72].
Cognitive computing	Active context-aware and adaptive access controls are all needed[73].
Apps 3.0	Perimeters and firewalls are no longer enough; every app needs to be self-aware and self-protecting[74]. Analyst IDC predicts that by 2017, ninety percent of an enterprise's endpoints will utilise some form of hardware protection to ensure that endpoint integrity is maintained[75]. IDC also suggests that by 2018, twenty five percent of security applications that were previously purchased independently will be incorporated directly into business applications[76]".
Mobile virtualisation	More than 40% of UK businesses had suffered a mobile security breach in the past 12 months (to Nov 2014). Businesses can use mobile virtualization to secure everything that matters -- without impinging upon employee privacy and choice[77].
Tokenisation	"In essence, tokenisation is removing the need for sharing the card number throughout the transaction, and that takes risk out of it," says Jonathan Vaux, director of new payment propositions at Visa[78]
'Bring Your Own Identity'	Bob Olson, vice president of global financial services at Unisys[79] says "There will have to be a shift towards a 'Bring Your Own Identity' approach [with a profile] that leverages biometrics, IP addresses, and analytics on the backend." The challenge for banks in implementing such an authentication approach will be in delivering it across different channels.
Biometrics	Looking towards 2020, 14% of respondents believe that biometrics, such as retina or fingerprint scans, could also become commonplace and 44% say they would be prepared to make payments via biometric scanning. A fifth (19%) would consider paying for goods and services using voice authentication[80].

Technology/trend	Description
Homomorphic encryption	IBM has been granted a patent on an encryption method that, if implemented, could be revolutionary. It makes it possible to process encrypted data without having to decrypt that data first[81]. A homomorphically encrypted search engine, for instance, could take in encrypted search terms and compare them with an encrypted index of the web[82].
Quantum cryptography	Quantum cryptography is the only known method for transmitting a secret key over long distances that is provably secure in accordance with the well-accepted and many-times-verified laws that govern quantum physics. It works by using photons of light to physically transfer a shared secret between two entities. While these photons might be intercepted by an eavesdropper, they can't be copied, or at least, can't be perfectly copied (cloned)[83].
Polarised security screens	Simple pieces of security such as polarised security screens maintain the level of in-house security on items such as laptops. (The theory is simple: Remove the polarized film from the monitor so that you only see a white backlit screen. Then take this film, cut to fit your spare specs and you can see the screen only when you wear them[84].)
Thin clients	Another technology solution for in-house users is that of thin-clients which provide a virtual operating environment that refreshes each time the user logs off[85].
Advanced forensics	Forensics are moving from a method of simply analysing a cyber-attack after the event, to a tool that can profile the cybercriminal and attack methods – building bio data patterns of criminal and malware activity[86].
New signature based solutions	'Conventional signature-based anti-malware solutions cannot cope with 2013 levels of malware production, let alone those predicted for 2020. New anti-malware solutions, which are already appearing, trap malware at a micro visor level, so it can't enter the organisation at any level or point—and the infected file can be safely extracted. New- generation security protocols will adjust, seek out, and quarantine perceived threats before any system is compromised[87].'
Data elemental protection	'I believe we are headed to a world of highly encrypted information. The innovation is going to be how you manage it. If you can encrypt the information, it won't matter if bad guys steal it, because they can't do anything with it,' says Ted Schlein, general partner at the venture firm Kleiner Perkins Caufield & Byers[88]

The average breach inside a major company goes undetected for 229 days

Future tech threats

Many of these technologies and tools could also be used nefariously. Financial services providers are at various stages of shifting major legacy platforms and protocols and these changes will undoubtedly yield security flaws. The need to leverage new technologies and models is not in dispute, nor is the danger of not renewing major platforms and protocols; yet new vulnerabilities are almost inevitable, even if the status quo were to be maintained[89]. A breakdown of the most prominent technology born threats is included below in figure 3.

Technology/trend	Description
Bring Your Own Technology	Financial services will have to accept that employees will use these devices or be left behind. Their customers are also demanding to be able to interface with them via more digital channels[90].
NFC	'Banks will want to use NFC to introduce new products and fast payment solutions. How will they protect their customers from aggressive targeted attacks and the use of avatar-based—a highly advanced digital creation assembled from numerous stolen aspects of an individual's real identity—attacks?[91]'
Big data and the cloud	In the wrong hands, analytical techniques can generate sophisticated cyber exploits automatically. Massive cloud malware could analyse infrastructure for vulnerabilities and develop attack strategies in seconds[92]. By 2025, most of the data created in the world will move through or be stored in the cloud at some point. Challenges could include highly distributed denial of service attacks using cloud infrastructures as well as a move from device-based to cloud-based botnets, hijacking distributed processing power.
Mobile	Many commentators point out that mobile platforms will become increasingly attractive to hackers and cybercriminals, especially now that mobile payment systems such as Apple Pay are taking off. Websense also thinks that hackers will target mobile devices "not to simply crack a phone code and steal data from the device itself -- but as a vector into the growing data resources that the devices can freely access in the cloud[93]". 80 percent of Internet connections could originate from a mobile device by the year 2025[94].
Self mutating computer virus	Pandoras, the next generation of computer virus attacks, will be self-mutating viruses created to destabilise, confuse and destroy critical electronic infrastructures essential to industry and government. These could be used as offensive or defensive weapons[95].
Botnet of Things / Wearables	Statements made by FBI Assistant Director, Joseph Demarest in January 2015 indicate a major increase in botnet activity. 'The use of botnets is on the rise. Industry experts estimate that botnet attacks have resulted in the overall loss of millions of dollars from financial institutions and other major US businesses,' he said. The advent of IoT will only exacerbate this problem as it introduces billions of new potential bots[96].

Technology/trend	Description
Payments technology	Apple Pay, arguably the most important new name on the increasingly - large mobile payments playing field is already coming under scrutiny in the US where, according to the Guardian, fraud cases relating to it are already costing millions of dollars[97].
Old source code	Not all technological exploits will be born of new innovation. Simple failure to update old source code could have devastating effects. TechRadar suggests that '...in 2015, at least one major breach, a veritable treasure trove of data, will trace its origins to confidential company data improperly transmitted or secured on publicly available cloud storage sites based on old code foundations.'
Biohacking	The term applies to any advanced technique that uses science and technology to improve human output and performance. To many, biohacking is a highly radical, unregulated science. Smart implants will be used for Identification and Authentication of individuals, tasks and services. Identification will include activities like accessing buildings, activating mobile devices, controlling room temperature. Smart implant authentication can be used for authenticating a bank transaction, part of a two factor authentication replacing smartphone PIN codes, activity logging and health monitoring[98].
New types of attacks	The EU-sponsored International Cyber Security Protection Alliance (ICSPA), has predicted that by 2020[99], there will likely exist a mature illicit market for virtual items, both stolen and counterfeit, as well as theft and fraudulent generation of micro payments. High-impact, targeted identity theft and avatar hijack is also deemed likely.

Conclusion

As technology continues to reshape industries and consumer expectations, financial services providers face the unenviable task of embracing innovation and change far reaching enough to provide competitive differentiation, whilst meeting needs for compliance and security[100]. To do this, both organisational change and an appreciation of technological challenges and opportunities are required. Perhaps the most significant change is required to further the ecosystem resilience by sharing threat information with those with common interests and building standards beyond the walls of their organisation.

Despite the interest of governments and agencies in strengthening cyber-defences, it is likely that it will become harder for financial services to meet new compliance regulation. Emphasis will be firmly made on banks' responsibilities to protect the consumer, bank customers and partners[101]. For this reason, cyber-security is perhaps the most important strategic issue facing financial services providers today and so, Board level engagement is vital. In many cases this may necessitate Board level education and training. Failure to engage sufficiently and the worst case scenario of financial services leaders facing the prospect of uncontrolled international cybercrime, becomes more possible. Failure to invest in data management systems, and of driving behavioural norms within the organisation that assist in meeting compliance rules will not be an option[102].

The data management systems will likely feature an array of big data analytics, intelligent anti-malware techniques, digital forensics and identity science[103]. It is also likely that threat data will be shared more readily between the government and private sector, and amongst private sector companies. Individual organisations must strengthen their data science capacity as the type of data collected and inspected to detect advanced threats will increase in variety and volume[104]. As a result, financial services providers will increasingly come to regard themselves as technology companies and will need to adjust their hiring practices and working environments accordingly.

As with all major paradigm shifts, the biggest challenge is finding an identifiable starting point that initiates the multiple activity strands that are necessary to adjust a firm to the shift. The logical starting point is to assess the maturity of the firm against the various threat vectors by undertaking scenario planning through a series of 'what if' questions relating to each of the vectors. Having established the nature of the risks, the firm should then undertake a complete systems, process and staff audit to identify areas of weakness within each scenario.

The audit must be inclusive of all staff and be the bridgehead into developing a firm-wide culture of awareness and responsibility, with specific changes such as the introduction of security specific KPIs into staff appraisals being examined at this stage. This process will help in the development of a risk-aware culture and management system. Since the threat vector spectrum is so broad, it is essential that security risks and goals are communicated with relevant staff and tools should be implemented to track progress across key metrics, or KPI's[105].

The key phrase here is 'relevant staff.' The concept of cloaking and containing is gaining traction as another key step, which can also be described as the concept of least privileges, or providing the least amount of information that someone needs to do their job. For example, someone who works in human resources or technology should only

have access to what's necessary for HR or technology. Containing the ability of people to navigate certain areas, whilst adding additional restrictions around crown jewels data could significantly reduce the threat from careless or rogue employees or even disgruntled ex-employees. Alerts should be initiated to inform the system of inappropriate access by a given employee. 'The key is for the [bank's] chief information security officer to not trust anybody,' says Unisys' Bob Olson, '...and if you take it from there, you operate with a different mindset[106].'

This mindset would dictate that another critical step is taken, where security is built inside services, by design. The days of implementing services first and security as an afterthought is not only a key vulnerability in information systems[107] but part of a business model that is increasingly unattractive to customers. With data breaches gaining much public attention around the world, carving out a business proposition based on trust in handling data securely could become an option for those with the cultural and technological aptitude.

A key part of this organisational aptitude will come from cyber-security collaboration that extends beyond company walls to address common enemies. This step should involve establishing best practices among its contractors and suppliers – and other stakeholders.

It is clear that successful cyber-security will increasingly require '...the right balance of technology and highly skilled analysts with intelligence tradecraft and data analytics skills[108].' It will also need to be adept in meeting ever tighter compliance and regulatory requirements. The challenge for financial services providers is thus both complex and evolving, but a middle way is almost impossible to entertain – either organisations will transform their notion of security or fall prey to a series of damaging breaches that could ultimately account for their very existence.

References and further reading

1. Source: FT, 2015
http://www.ft.com/intl/cms/s/0/7586e376-a6cc-11e4-8a71-00144feab7de.html#axzz3RGTGiCWR

2. Source: PwC, 2014
http://usblogs.pwc.com/cybersecurity/survey-shows-a-deficit-of-cybersecurity-funding-and-safeguards-in-financial-service/

3. Source: McKinsey, 2014
http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks

4. Source: The Guardian, 2015
http://www.theguardian.com/money/2015/feb/17/how-safe-you-bank-cyber-attack

5. Source: Business Insights, 2014
http://businessinsights.bitdefender.com/financial-services-high-risk-security-by-the-numbers

6. Source: Inside Counsel, 2014
http://www.insidecounsel.com/2014/05/20/planning-for-the-inevitable-cyber-breach

7. Source: TaylorWessing, 2015
http://www.taylorwessing.com/globaldatahub/article_cyber_crime_finance.html

8. Source: Sophos, 2014
http://blogs.sophos.com/2014/12/11/our-top-10-predictions-for-security-threats-in-2015-and-beyond/

9. Source: Sophos, 2014
http://www.sophos.com/en-us/lp/compliancecheck.aspx?cmp=701j0000000KZhGAAW&utm_source=Non-campaign&utm_medium=Cross-link&utm_campaign=CL-CorpBlog

10. Source: CSO Online, 2014
http://www.csoonline.com/article/2857665/data-protection/the-future-of-security-11-predictions-for-2015.html

11. Source: Homeland Security Newswire, 2014
http://www.homelandsecuritynewswire.com/dr20141126-internet-security-market-to-reach-42-8-billion-globally-by-2020

12. Source: ABI Research, 2014
https://www.abiresearch.com/press/us100-billion-cybersecurity-spending-for-critical-

13. Source: TechRepublic, 2014
http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/

14. Source: PwC, 2014
http://usblogs.pwc.com/cybersecurity/survey-shows-a-deficit-of-cybersecurity-funding-and-safeguards-in-financial-service/

15. Source: Bank Info Security, 2015
http://www.bankinfosecurity.com/interviews/2015-trend-big-data-for-threat-analysis-i-2521

16. Source: CA Technologies, 2014
http://blogs.ca.com/2014/03/20/security-and-big-data-loom-large-for-it-among-financial-services-firms/

17. Source: CIO, 2014
http://www.cio.com/article/2825086/cio-role/is-the-cio-cmo-transition-of-power-becoming-a-reality.html

18. Source: Booz Allen, 2014
http://www.boozallen.com/media-center/press-releases/2014/11/booz-allen-releases-annual-financial-services-cyber-trends-for-2

19. Source: GigaOM, 2014
http://research.gigaom.com/2014/11/apple-pay-forecasting-consumer-adoption/

20. Source: Mobile Commerce Insider, 2013
http://www.mobilecommerceinsider.com/topics/mobilecommerceinsider/articles/361991-mobile-wallet-worldwide-market-clear-5-trillion-2020.htm

21. Source: Fierce Big Data, 2014
http://www.fiercebigdata.com/story/big-datas-defense-against-cyber-crime/2014-04-21

22. Source: Security Intelligence, 2013
http://securityintelligence.com/infographic-the-future-of-information-security/#.VPTAHfmacW4

23. Source: Security Week, 2014
http://www.securityweek.com/security-threats-risks-often-neglected-step-child

24. Source: Sophos, 2014
http://blogs.sophos.com/2014/12/11/our-top-10-predictions-for-security-threats-in-2015-and-beyond/

25. Source: IBM, 2014
http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03046usen/SEW03046USEN.PDF

26. Source: Business Insights, 2014
http://businessinsights.bitdefender.com/financial-services-high-risk-security-by-the-numbers

27. Source: PwC, 2014
http://usblogs.pwc.com/cybersecurity/survey-shows-a-deficit-of-cybersecurity-funding-and-safeguards-in-financial-service/

References and further reading

28. Source: Business Insights, 2014
http://businessinsights.bitdefender.com/financial-services-high-risk-security-by-the-numbers

29. Source: McKinsey, 2014
http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks

30. Source: McKinsey, 2014
http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks

31. Source: eWeek, 2014
http://www.eweek.com/small-business/financial-institutions-under-constant-threat-from-cyber-criminals.html

32. Source: CNBC, 2015
http://www.cnbc.com/id/102344021#.

33. Source: FT, 2015
http://www.ft.com/intl/cms/s/0/7586e376-a6cc-11e4-8a71-00144feab7de.html#axzz3RGTGiCWR

34. Source: Security Week, 2014
http://www.securityweek.com/security-threats-risks-often-neglected-step-child

35. Source: Security Week, 2014
http://www.securityweek.com/security-threats-risks-often-neglected-step-child

36. Source: FT, 2015
http://www.ft.com/intl/cms/s/0/15630060-433f-11e4-be3f-00144feabdc0.html#axzz3RGTGiCWR

37. Source: SC Magazine, 2014
http://www.scmagazineuk.com/bank-bosses-finally-get-the-memo-on-cyber-security/article/356853/

38. Source: SC Magazine, 2014
http://www.scmagazineuk.com/bank-bosses-finally-get-the-memo-on-cyber-security/article/356853/

39. Source: SC Magazine, 2014
http://www.scmagazineuk.com/bank-bosses-finally-get-the-memo-on-cyber-security/article/356853/

40. Source: Computer Weekly, 2015
http://www.computerweekly.com/news/2240240587/RBS-uses-Apple-fingerprint-authentication-for-mobile-banking

41. Source: The Guardian, 2015
http://www.theguardian.com/money/2015/feb/17/how-safe-you-bank-cyber-attack

42. Source: SC Magazine, 2014
http://www.scmagazineuk.com/bank-bosses-finally-get-the-memo-on-cyber-security/article/356853/

43. Source: FinExtra, 2015
http://www.finextra.com/news/fullstory.aspx?newsitemid=27000

44. Source: Security Week, 2015
http://www.securityweek.com/mastercard-visa-introduce-new-cybersecurity-enhancements

45. Source: Pymnts, 2015
http://www.pymnts.com/news/2015/paypal-amps-up-cybersecurity-plans/#.VOuOJ_macW4

46. Source: FT, 2015
http://www.ft.com/intl/cms/s/0/270d2894-ecb5-11e3-a754-00144feabdc0.html#axzz3RGTGiCWR

47. Source: FT, 2015
http://www.ft.com/intl/cms/s/0/270d2894-ecb5-11e3-a754-00144feabdc0.html#axzz3RGTGiCWR

48. Source: Payment Eye, 2014
http://www.paymenteye.com/2014/08/12/mobile-payments-key-trends-for-2015-2/

49. Source: PwC, 2014
http://www.pwc.com/et_EE/EE/publications/assets/pub/pwc-the-future-shape-of-banking.pdf

50. Source: PwC, 2014
http://pwc.blogs.com/press_room/2014/10/pwc-research-financial-services-industry-faces-bigger-problem-than-lack-of-trust-apathy.html

51. Source: FT, 2014
http://www.ft.com/intl/cms/s/0/bbfb86a6-3424-11e4-b81c-00144feabdc0.html#axzz3SCPbQ0Nm

52. Source: Trade Arabia, 2014
http://www.tradearabia.com/news/REAL_271336.html

53. Source: FT, 2014
http://www.ft.com/intl/cms/s/0/bbfb86a6-3424-11e4-b81c-00144feabdc0.html#axzz3SCPbQ0Nm

54. Source: Bloomberg, 2014
http://www.bloomberg.com/news/articles/2014-10-08/lloyd-s-ceo-sees-cyber-insurance-to-surge-after-attacks

55. Source: Reuters, 2014
http://www.reuters.com/article/2014/07/14/us-insurance-cybersecurity-idUSKBN0FJ0B820140714

56. Source Wall Street Journal, 2015
http://blogs.wsj.com/digits/2015/01/28/cyber-insurance-demand-said-rising-in-europe/

57. Source: VPN Creative, 2014
http://vpncreative.net/2014/07/14/insurance-companies-major-cyber-risks/

58. Source: NextGov, 2014
http://www.nextgov.com/cybersecurity/2014/09/wh-official-cyber-coverage-will-be-basic-insurance-policy-2020/93503/

59. Source: Advisen, 2013
http://news.advisen.com/documents/proprietary_content/201310231909_001/NEWS_CRIC_24_Oct_Jim_Blinn.html

60. Source: Booz Allen, 2014
http://www.boozallen.com/media-center/press-releases/2014/11/booz-allen-releases-annual-financial-services-cyber-trends-for-2

61. Source: Forbes, 2014
http://www.forbes.com/sites/sap/2014/01/09/the-future-of-global-cyber-security-is-in-the-cloud/

62. Source: Northrop Grumman, retrieved 2015
http://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Literature/NG_Advertorial_Raconteur.pdf

63. Source: Northrop Grumman, retrieved 2015
http://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Literature/NG_Advertorial_Raconteur.pdf

64. Source: Tech Republic, 2014
http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/

65. Source: Patriot Tech, 2014
http://patriot-tech.com/predictions-future-of-cyber-security/

66. Source: KPCB, 2014
http://www.kpcb.com/blog/venture-capitalist-ted-schlein-on-the-future-of-cybersecurity

67. Source: Harvard Business Review, 2015
https://hbr.org/2015/02/the-enemies-of-data-security-convenience-and-collaboration

68. Source: World Economic Forum, 2015
https://agenda.weforum.org/2015/02/5-economic-principles-of-cyber-security/?utm_content=buffer081a1&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

69. Source: ZdNet, 2015
http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

70. Source: ZdNet, 2015
http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

71. Source: Morrison Foerster, 2013
http://media.mofo.com/files/Uploads/Images/130814-Botnets.pdf

72. Source: Business Value Exchange, 2014
http://businessvalueexchange.com/blog/2014/03/21/financial-services-overwhelmed-cyber-crime-tech-conservatism/

73. Source: Gartner, 2014
http://www.gartner.com/newsroom/id/2867917

74. Source: Gartner, 2014
http://www.gartner.com/newsroom/id/2867917

75. Source: ZdNet, 2015
http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

76. Source: ZdNet, 2015
http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

77. Source: Network Computing, 2014
http://www.networkcomputing.com/wireless-infrastructure/mobile-virtualization-the-future-of-security/a/d-id/1318324

78. Source: Gizmodo, 2015
http://www.gizmodo.co.uk/2015/03/visa-apple-pay-bio-hacking-privacy-and-protecting-your-money/

79. Source: Bank Tech, 2015
http://www.banktech.com/security/how-fraud-and-cyber-security-will-evolve-in-2015/a/d-id/1318489

80. Source: Banking Tech, 2015
http://www.bankingtech.com/277312/fraud-fears-holding-back-consumer-acceptance-of-mobile-payments/

81. Source: Info World, 2014
http://www.infoworld.com/article/2609755/encryption/ibm-s-homomorphic-encryption-could-revolutionize-security.html

82. Source: Wired, 2014
http://www.wired.com/2014/11/hacker-lexicon-homomorphic-encryption/

83. Source: Wired, 2014
http://www.wired.com/2014/09/quantum-key-distribution/

84. Source: LinkedIn, 2015
https://www.linkedin.com/pulse/data-information-security-ill-show-you-mine-ah-whatever-paul-kuiken

85. Source: LinkedIn, 2015
https://www.linkedin.com/pulse/data-information-security-ill-show-you-mine-ah-whatever-paul-kuiken

86. Source: Business Value Exchange, 2014
http://businessvalueexchange.com/blog/2014/03/21/financial-services-overwhelmed-cyber-crime-tech-conservatism/

87. Source: HP, 2014
http://www8.hp.com/h20195/V2/getpdf.aspx/4AA5-1187EEW.pdf?ver=1.0

88. Source: KPCB, 2014
http://www.kpcb.com/blog/venture-capitalist-ted-schlein-on-the-future-of-cybersecurity

89. Source: Deloitte, 2014
http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-Transformingcybersecurity-021114.pdf

90. Source: Business Value Exchange, 2014
http://businessvalueexchange.com/blog/2014/03/21/financial-services-overwhelmed-cyber-crime-tech-conservatism/

91. Source: HP, 2014
http://www8.hp.com/h20195/V2/getpdf.aspx/4AA5-1187EEW.pdf?ver=1.0

92. Source: Northrop Grumman, retrieved 2015
http://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Literature/NG_Advertorial_Raconteur.pdf

93. Source: ZdNet, 2015
http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

94. Source: Microsoft, 2014
http://www.microsoft.com/security/cybersecurity/cyberspace2025/#chapter-1

95. Source: Institute for Global Futures, retrieved 2015
http://www.globalfuturist.com/about-igf/top-ten-trends/trends-in-security.html

96. Source: IT Pro Portal, 2015
http://www.itproportal.com/2015/01/08/internet-things-breeding-botnet-army-watching-sleeping-baby/

97. Source: Gizmodo, 2015
http://www.gizmodo.co.uk/2015/03/visa-apple-pay-bio-hacking-privacy-and-protecting-your-money/

98. Source: Security Affairs, 2015
http://securityaffairs.co/wordpress/33743/hacking/bio-hacking-security-risk-future-now.html

99. Source: Business Value Exchange, 2014
http://businessvalueexchange.com/blog/2014/03/21/financial-services-overwhelmed-cyber-crime-tech-conservatism/

100. Source: Global Banking and Finance, 2014
http://www.globalbankingandfinance.com/financial-services-sector-in-the-race-to-embrace-technology/

101. Source: Business Value Exchange, 2014
http://businessvalueexchange.com/blog/2014/03/21/financial-services-overwhelmed-cyber-crime-tech-conservatism/

102. Source: HP, 2014
http://www8.hp.com/h20195/V2/getpdf.aspx/4AA5-1187EEW.pdf?ver=1.0

103. Source: Business Value Exchange, 2014
http://businessvalueexchange.com/blog/2014/03/21/financial-services-overwhelmed-cyber-crime-tech-conservatism/

104. Source: Security Intelligence (IBM), 2013
http://securityintelligence.com/infographic-the-future-of-information-security/#.VPTAHfmacW4

105. Source: IBM, 2014
http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03046usen/SEW03046USEN.PDF

106. Source: Wall Street and Tech, 2015
http://www.wallstreetandtech.com/security/
morgan-stanley-data-theft-exposes-insider-threat-and-need-for-more-restrictions/d/d-id/1318623

107. Source: IBM, 2014
http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03046usen/SEW03046USEN.PDF

108. Source: Business Insights, 2014
http://businessinsights.bitdefender.com/financial-services-high-risk-security-by-the-numbers

About Advanced 365

Advanced 365 is a leading UK based provider of CIO Advisory, Business Innovation Solutions and Managed Services. Over 250 organisations rely on our expertise and service excellence to improve their operational efficiencies, control costs, and capitalise on digital business opportunities.

Advanced 365 Business Innovation has over 25 years' experience as a leading provider of pioneering software solutions, with tens of thousands of organisations using our products and services. We enable our customers to increase business value and maintain competitive advantage by maximising the potential of existing data and applications, combining core systems with latest technologies.

Within our CIO Advisory Practice, we work with CIOs, CFOs and other senior managers to address immediate and long term opportunities and issues such as:

- Business and Financial Alignment.
- Operational Transformation.
- Technical Strategy.

Advanced 365's relationship with David Smith is one of many relationships we have with prominent industry leaders to ensure we can provide the very best ideas, innovation and thought leadership in the industry to our clients.

About Global Futures and Foresight

Global Futures and Foresight (GFF) is a strategic futures research organisation. The aim of GFF is to develop views of the future to help their clients embrace change with more certainty, thereby releasing the full power of their creativity and innovation. GFF helps its clients to reduce their risk of being blindsided by change and to be better enabled to adapt to the fast changing world. GFF clients number some of the largest and most prestigious firms from around the world including: NATO, HSBC, RBS, Lloyds, More Than, e-sure, Allianz, Travelers, QBE, Acord, Kraft, Mars, Steria, CSC, Unisys, Cisco, Microsoft, Siemens, Advanced 365, Equinix, Fineos, Experian, KPMG, Deloitte, Ernst & Young, PWC, Cap Gemini, Celent, Royal Mail, Bausch & Lomb, Linpac, Heinz, SAS airlines, Philips and many other businesses and academic institutions.

www.thegff.com

For more information:

Advanced 365 Limited, registered in England, company number 2124540.
Registered office: 230 City Road London EC1V 2TT
t: +44 (0)20 7880 8888 **e:** info@advanced365.com **w:** www.advanced365.com

www.advanced365.com

Advanced 365