vmware

No Compromise for UK Financial Services

A report by VMware exploring why the UK financial services sector must develop a robust approach to security, limiting the impact of breaches and providing the best protection for customers

Contents

Foreword

The financial services sector is in the midst of a perfect storm, with shifting market trends disrupting the industry to its very core.

Rampant globalisation, hyper connectivity, heightened customer expectation, evolving work practices, regulatory pressures and an increasing reliance on diverse stakeholder ecosystems are all having significant impact on the companies operating in this sector. These issues are also leading to an exponential rise in the challenges surrounding the protection of data. These are challenges the sector must overcome.

In a recent study conducted by Ponemon, 31 percent of consumers impacted by a breach stated they had discontinued their relationship with the affected organisation, and 65 percent admitted they had lost trust in the business altogether. With new entrants disrupting the financial services market, with no legacy systems, they are able to provide robust, secure and agile platforms built for the market demands expectations and threats. Established players must maintain trust, whilst guarding against an increasingly complex cyberthreat landscape.

In 2017, Russia's Sberbank and the National Bank of Ukraine both fell victim to the WannaCry and Petya ransomware attacks, while Tesco Bank suffered a high profile breach in which £2.5 million was taken from customer accounts in November 2016. And these are just the attacks that made headlines. A study from Accenture suggests a typical financial services organisation will face an average of 85 targeted breach attempts every year.

One of the main reasons such attacks are successful is the often outdated techniques and approach deployed to data security and operations wrapped to support this. Too often this is the result of compromises having to be made between agility and security – at a strategic level but also every single day by those on the front line defending against the threats. The digitisation agenda demands speed and usability, with an intuitive, seamless experience for customers used to a diet of one-touch access and instant information. Yet financial businesses, be they retail banks, brokerages, payments providers or insurance companies, must marry such evolution with stringent regulatory compliance and legacy systems.

Businesses have often been quick to invest in the latest front-end digital platforms, without considering the security ramifications, involving the security team from the on-set, or devoting the same attention to delivering up-to-date protocols and procedures. As cyberthreats evolve, so must the approach to defence.

To understand the scale of the issue, and where IT security professionals who work in the financial services industry believe change is required, we questioned 201 based in the UK, exploring their thoughts on current security practices within their organisation and where they believe they are fighting an uphill battle.

This guide outlines the scale of the job ahead, identifies where common challenges currently lie, and importantly, what the sector must do to develop a fit-for-purpose approach to security which limits the impact of breaches and best protects customers.

Ian Jenkins, Head of Network and Security, UK, VMware.

About this research

VMware commissioned research to explore the cyberthreat challenges the financial services sector faces, covering how prepared IT security professionals feel and how confident they are in their security infrastructure to balance the drive to digitisation. On VMware's behalf, independent research house Opinion Matters questioned 201 UK based IT security professionals who work in the financial services sector in organisations of over 250 employees. The research was carried out in October 2017.

The evolving threat landscape and the digitisation agenda

As holders of significant amounts of data on individuals and organisations, not to mention being gatekeepers to the world's finances, the financial services sector is a prime target for cyber criminals. Therefore, it comes as no surprise to find that they are subject to frequent cyberattacks, with 15 percent of security professionals having to deal with attempts weekly and eight percent daily.

Why is this happening? Only half of those surveyed (49 percent) rated the current security of the IT infrastructure of their organisation as good with 14 percent stating it was only adequate and five percent less than adequate. This suggests security professionals are aware that cybercriminals are evolving faster than the security apparatus designed to stop them but their hands are tied when it comes to making the necessary changes to avert threats. At a time when successful and even attempted cyber-attacks have, according to 56 percent, resulted in a loss of credibility or reputation and 54 percent caused inconvenience to suppliers and customers, financial sector organisations must make changes in order to prevent devastating consequences to their bottom-line.

The challenges facing IT security professionals keen to drive change are significant however – a lack of skills (26 percent), budget and resource (57 percent) and also understanding among senior management (26 percent) were highlighted as impacting how security professionals rated their employers' data security. Even more worryingly, a quarter (25 percent) stated the impact of cybercrime was actually treated as a cost of doing business. Companies must consider the EU's General Data Protection Regulation (GDPR) coming in to force in May 2018, which will apply to all companies selling to and storing customer or citizen personal data in Europe and other continents. With 55 percent of respondents stating both successful and attempted cyberattacks have breached customer confidentiality, such complacency could see financial services organisations facing fines of up to 20 million or 4 percent of annual worldwide turnover. That would be on top of any loss of revenue, reputational damage or reallocation of resource resulting directly from an attack.

15%

admit to suffering **cyberattack attempts weekly** and eight percent daily

A culture of compromise

So what's stopping financial services organisations from sorting out their security and evolving ahead of the threats? Put simply, compromise is a business reality.

With IT security professionals under increasing pressure while also trying to juggle multiple demands from the business, a staggering 90 percent of respondents said they've had to make compromises when protecting their organisation against cyberthreats, having to allocate time or budget to a certain area in the knowledge it could leave other areas exposed. Over half (51 percent) admitted they do this regularly despite best efforts to avoid it.

a huge

90%

say they have to make **compromises**

At the heart of this compromise is the rampant drive towards digitisation and the need to remain relevant. A separate VMware study, this time in the US banking sector, highlighted that respondents most frequently describe their top business focus over the next year as "growing the bank's profile and relationships in the communities it serves." But over a three year horizon, the top business focus becomes "integrating digital and physical channels." And in five years, most bankers say their focus will simply be on "becoming a digital leader".[1]

The push for digitisation is already having an impact – applications and initiatives implemented to improve the customer experience, such as e-banking and mobile applications, were among the most targeted of all types of data or resource, with 30 percent of security professionals stating that these have been targeted, 35 percent admitting they may have been infiltrated and 16 percent certain they had. This increased digital footprint means more opportunities for cybercriminals to find weaknesses.

2 in 3

admit to cyber security practices **'which would shock outsiders'**

One major strategic compromise many financial services organisations said took precedence was prioritising external customer-facing applications: over 71 percent said that their firm focuses security here at the expense of internal systems. The reality is that the days of all-encompassing firewalls are over – the latest threats see these dated practices as no more than a speed bump. Once they have access, a lack of application security means that individual systems can be picked off. A mission critical system may have multiple layers of firewalls between it and the outside world, yet if a marketing application holding customer data is left with less protection, a successful breach may give attackers all they need to then access accounts and money.

To enable IT security professionals to do their job adequately, financial sector organisations need to accelerate their evolution of outdated,

[1] How Technology Will Shape the Bank of the Future. VMware/American Banker October 2017

underfunded security procedures. Too often cybersecurity is perceived as an issue for IT and anti-fraud teams to deal with, when in reality every employee has a role to play.

71%

focus on e-banking and customer applications at the **expense of other systems**

When asked for the most important change respondents would make in the way their organisation approaches cybersecurity, the top answer was investment in skills and training for staff (21 percent).

In the rush for innovation, a digital experience must have security embedded into it from the very start.

21%

say **investment in skills and training for staff** is the most important change they would make to the way their organisation approaches cybersecurity

Innovative security

In the US VMware survey of banking industry professionals, legacy systems were cited as having some impact or a high impact on their institutions' ability to launch new products.[2] In the same vein, security is often cited as holding back innovation, particularly in an industry as heavily regulated as this one.

As previously highlighted, part of the challenge is that many security professionals are wrestling not only with increasing exposure to digital threats as financial services organisations strive to offer customers greater levels of service efficiently, but with having to prevent attacks with legacy security infrastructure and approaches, particularly from senior management.

Over half (53 percent) don't believe their leadership team understands the complexity of threats their business faces today, with two thirds (67 percent) admitting the stress associated with their role is underestimated. Getting management buy-in can also be a significant challenge, with a notable knock-on effect – 62 percent stated their team struggles to get the funding they need for urgent cybersecurity projects.

Yet at the same time, in the banking sector at least, there is significant investment in digital applications and services to deliver tangible results, when 'more than 50 percent of banks with $100 billion or more in assets expect to have commercial implementations of the following major categories of emerging technology: mobile apps, APIs/open banking, artificial intelligence (AI), augmented reality, biometric authentications and blockchain – in the next five years.'[3]

That's a significant disparity, underlining the feeling that financial services organisations' senior management teams may not fully appreciate the current threats, or how best to

counteract them. The focus appears to be on delivering a digital experience with enhanced customer service, without requiring significant physical (and therefore expensive) resource.

Yet this drive for innovation and enhanced consumer experience should not be at the expense of security – or rather, innovation should encompass customer-facing applications at the edge and those that keep data secure. Securing individual applications and systems may seem time-consuming and destined to be ruinously expensive, but the alternative is worse, with both successful and attempted cyberattacks seeing budget taken away from other areas of the business in 26 percent of cases, and time spent by staff on the issue which could have been put to better use in 40 percent of occurrences.

That's why new approaches to security are needed, ones that maximise resources to best effect, rather than, like 74 percent of respondents, spending more and more time fighting small but urgent cyber threats meaning that they can't devote time to protecting against potentially more serious breaches.

From basics like updating software (and therefore mitigating against the likes of the WannaCry-style attacks) to educating beyond the IT team, there are key areas the financial services sector should focus on.

53%

don't believe their leadership team **understands the complexity of threats** their business faces today

74%

spend more time on small but urgent attacks than **protecting against serious breaches**

[2] How Technology Will Shape the Bank of the Future. VMware/American Banker October 2017
[3] How Technology Will Shape the Bank of the Future. VMware/American Banker October 2017

What can be done?
Advice from the experts

"Established players in the financial services sector are being hit by a wave of challenges as digital-native entrants, increased regulation and customer demand force an overhaul of established operations. However, in chasing the digital promise land, they run the risk of overstretching already antiquated security infrastructure. This, combined with expanding digital surface areas, means more opportunities for cybercriminals to find and expose weaknesses. Businesses that are prepared to invest in enhanced user experience must ensure they invest in securing those experiences as well. Failure to do so will only result in catastrophic consequences in the event of a breach."

Ian Jenkins, Head of Network and Security, UK, VMware.

"This past era of compromise towards cybersecurity must end. A revised approach to protecting digital assets, starting at a security by design philosophy, is required to allow IT security professionals to dynamically manage the myriad of threats now faced. This involves understanding that cybersecurity does not begin and end with IT, but is a challenge for the whole organisation. It is also about recognising that adaptive networking, applications and systems are no longer nice to haves, and that cyberhygiene is intrinsic to a company's digital footprint today."

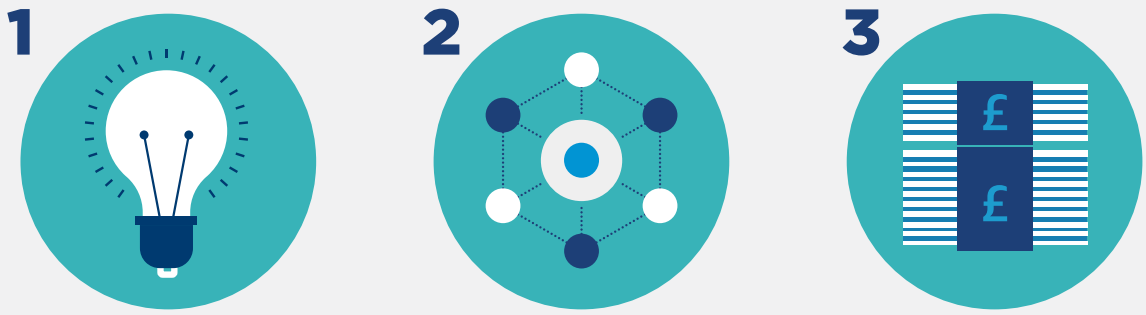
Richard Bennett, Head of Accelerate & Advisory Services, VMware

---

"The financial services sector faces the complex challenge of adopting innovative technologies while ensuring that it is not vulnerable to an evolving cyberthreat landscape. The frequency of cyberattacks against organisations in this sector is only going to increase; customers will not use providers that cannot guarantee the security of their data or finances. WannaCry and Petya have demonstrated the scale and potential for disruption, and attacks of this nature will likely become more commonplace. All IT leaders must have cybersecurity as a top agenda item if they are to benefit from digitisation."

Talal Rajab, Head of Programme, Cyber and National Security, techUK

The **top three** changes security teams want to see implemented are:



Skills and training amongst staff

Better infrastructure

More investment

What are regulatory bodies doing?

The Financial Conduct Authority (FCA), which governs financial services organisations, states that its aim 'is to help firms become more resilient to cyberattacks, while ensuring consumers are protected and market integrity is upheld.'[4] This includes pushing organisations to develop a security culture, covering not just technology but people too. This encapsulates detecting, responding to and recovering from successful cyberattacks, and constantly evolving to meet new threats.

Material cyberattacks must be reported. Such an incident qualifies if it:

- Results in significant loss of data, or the availability or control of IT systems
- Affects a large number of customers
- Results in unauthorised access to, or malicious software present on information and communication systems

More broadly, the aforementioned GDPR has significant implications for all organisations managing customer data, including financial services businesses. Its aim is to allow EU citizens to control their personal data, through:

- Easier access to their data
- A new right to data portability
- A clearer right to erasure ('right to be forgotten')
- Right to know when their personal data has been hacked

Organisations that fail to adequately protect customer data, or are found to be in breach of the regulation, face fines of up to four percent of worldwide turnover. The regulation applies to any business dealing with EU citizens, even if they have no operations in EU member states – as such, it will still apply to UK organisations post-Brexit.

[4] https://www.fca.org.uk/firms/cyber-resilience

Five measures for combatting cyberattacks

Invest in the back as much as the front

The financial services sector has ended up in a state of constant compromise due to a variety of factors, including the drive to digital innovation, seemingly at the expense of complete security. There needs to be balance – digital innovation without security is worthless, but if there is investment in delivering innovative services to customers, there needs to be corresponding investment to deliver the new types of security required. Applying old methods to secure cutting edge propositions will not work – just as customer experience is bedded into these applications and offerings, so should security be.

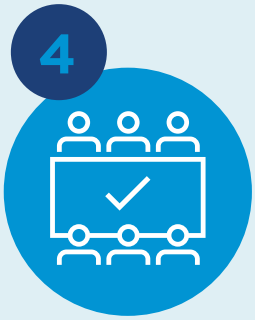
Deploy a security strategy for the present and future, not the past

Approaches to cybersecurity have changed. When an organisation's digital footprint was contained through prescribed corporate devices and limited connected points, an overarching defence made complete sense. However, as footprints expand, and we shift into a hyperconnected reality, security operations face new challenges, from BYOD to a shift towards meeting the customers on their terms.

Implementing a solution focused on a least privilege security model for data center endpoints and providing automated threat detection, response, and remediation to security events is now essential. By focusing on "ensuring good" versus "chasing bad" at data center endpoints, attention is focused on what a workload should be doing. As a result, the lens for seeing malicious activity is more focused and able to narrow the exploitable attack surface of the workload. Encryption, network division to protect data, and ensuring individual application protection are also vital. A new strategy that understands intrusion is inevitable is needed and IT leaders must have accurate visibility of system access, assisted by multi-factor authentication technologies, to ensure that nobody can gain entry unless explicitly granted.

Educate to protect

Awareness of the importance of security and prevention measures is growing amongst security professionals, but there is still much to do. Whether customers or staff, education on the risks and threats of cybersecurity is critical. While the execution may be technology-based, the true weaknesses of any security measure is human – from easy to crack passwords to opening unknown attachments and even credential sharing, updating employees and customers should be as critical as updating software. The focus should be on evolving behaviour, from intern through to C-suite, to prevent unnecessary and avoidable breaches.



Boards need to buy-in to balance

The evidence suggests that senior leadership teams understand that their business lives or dies through its ability to secure its operations. Yet is that commitment to security apparent throughout their decision-making process? True understanding lies in not only accepting the importance of cybersecurity, but understanding how it should be deployed to support, rather than hinder, efforts towards digitisation. Customers want easy-access apps, but they want to know they're protected – a six step process is as detrimental to acceptance as something that's clearly insecure.

Update, update, update

Vendor updates, whether to software, infrastructure or hardware, may sometimes feel like a drain on both time and money. Yet keeping your IT operations up to date is one of the simplest steps to take to ensure that the latest bugs are fixed, patches are rolled out and the threats are neutralised. That goes for all technology, not just anything security or outer-edge focused. WannaCry demonstrated the risk of getting the most out of earlier investments in outdated operating systems – new versions may seem like an exercise in printing money for vendors, but not only does the latest software deliver greater automation to your organisation, it also raises the bar for external threats.

Conclusion

The digital era is here – customers are only going to demand more ways of connecting in manners that suit them. Organisations that are competing against digital-first disruptors need to continue to innovate to keep ahead of the market. In financial services, that cannot be to the detriment of security. For too long an uneasy compromise has existed, but as threats become ever more sophisticated, businesses that become complacent about their security will be the first to suffer. A blemish-free history means only that they were able to counter past threats – the true test will come with future attacks.

A balance needs to be found – one that delivers innovation without exposing customers or their money. Those businesses that strike that balance, whether high street bank, insurance company or investment house, will secure not only their customers' data and finances, but their own future success as well.

For more information about VMware solutions for financial services, please visit: http://learn.vmware.com/UK_FinancialSecurity

About VMware

VMware, a global leader in cloud infrastructure and business mobility, helps customers accelerate their digital transformation. VMware enables enterprises to master a software-defined approach to business and IT with its Cross-Cloud Architecture™ and solutions for the data center, mobility, and security. With 2015 revenue of $6.6 billion, VMware is headquartered in Palo Alto, CA and has over 500,000 customers and 75,000 partners worldwide. VMware and Cross-Cloud Architecture are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and other jurisdictions.

VMware on Security:

VMware helps IT organisations transform security by leveraging a ubiquitous software layer to enable a secure application infrastructure, allowing for granular, micro-segmented security controls aligned to applications. Securing identity and endpoints protects a full range of devices and provides secure connections between applications on devices, data centers and clouds—unifying security, mobility, and networking with east-west traffic inspection and automated remediation against zero day threats. VMware's software layer over infrastructure and the Compliance Reference Architecture Framework streamline compliance by linking software, hardware, regulatory control, and independent audit validation.

VMware UK, Flow 1 & 2 River Park Avenue Staines-Upon-Thames TW18 3FA Tel: 01276 414300 www.vmware.com/uk