Breaking the banks

The threat landscape in the financial sector

Author: Charles Fox, BT Enterprise Architect, Cyber Warfare.

Year: 2015

The shifting threat landscape

Technology is changing the world of finance.

Online banking and mobile apps make managing money simple: in place of postal orders and cheques, people now use smartphones to complete almost £1 billion worth of transactions every day (Banks, 2015). This might be an advantage for both banks and customers, but it also creates a huge opportunity for criminals.

Financial organisations have to embrace the advantages cloud computing and Big Data offer. They need to improve the services they deliver to customers and clients alike — while also realising the potential to reduce operational costs.

However, such a move makes global financial markets (and the fiscal health of nations) even more dependent on the internet. This means cyber criminals and hacktivists become a more dangerous threat with their ability to cripple national infrastructures.

The financial sector in particular is a target for cyber attacks. As transactions change to factor in this new technology, they can leave sensitive data and applications vulnerable to attack. It's no wonder the International Organisation of Securities Commissions (IOSCO) thinks the next financial crisis will come from cyber space. "The issue of cyber resilience is one that we have to be proactive about in terms of making sure the risk management is robust," says Greg Medcraft, Chairman of IOSCO, "cyber crime has a huge potential impact on markets" (Fleming, 2014).

Financial institutions have to act now to avoid falling prey to cyber criminals. Many organisations have made security a board-level issue, which represents an important first step. However, they still have to do more to stay ahead of the hackers and prevent the catastrophic consequences of a serious breach.

Collating up-to-date threat intelligence makes businesses more aware of the attacks headed their way. But organisations also need to know how to interpret the data they have. This makes finding a security partner with the right expertise to collect and analyse intelligence an important task for every financial service provider to complete.

In this white paper, we look at how worldwide economic dependence on the financial sector puts it firmly in the hackers' crosshairs. We highlight the weak spots in security and how new technology can — if it's not secured — present a huge threat to financial organisations.

We see the impact cyber threats can have on an organisation's confidence to bring in new technology. We also look at how the right intelligence and expertise can tackle and eliminate vulnerabilities such as unsecured online banking or emails designed to steal personal data.

Why attack the financial sector?

The financial sector is a lucrative target for criminals. In the US, for example, it accounts for 6.3 per cent of the nation's Gross Domestic Product (GDP) (Konczal, 2014) which works out at over £600 billion.

Trading blows

Cyber threats to the sector often zero-in on the financial exchanges and trading platforms where big deals take place. While many of the details are still classified, we know that, in 2010, traders found Russian military malware on the NASDAQ exchange network (Yang, 2014). The 'flash crash' in the same year caused the Dow Jones to plunge by around 700 points in just minutes — an incident allegedly caused by just one man's automated trades (Clinch, 2015).

Some cyber attacks also exploit the higher-frequency trading systems using sophisticated computing tools to buy and sell shares in fractions of a second. Hackers disrupting these can cause serious trouble for financial markets, leading to falling share prices. Such events cause investors to lose trust. At their worst, they can see companies collapse, people lose jobs and whole economies sink into recession.

A far-reaching threat

And it's not just the financial traders that are under attack. Back in 2011 Heartland Payment Systems — who process Visa, MasterCard, American Express and Discover Card transactions in the US — faced up to costs of $12.6 million when their processing systems were breached.

Another case in May 2011 saw hackers steal personal details from more than 300,000 Citibank customers in the US (Zetter, 2011). And in June that year, the International Monetary Fund (IMF) also reported it had suffered a major breach — thought to be carried out by unknown state-sponsored attackers (BBC News, 2011).

A more recent example saw a breach involving vast amounts of personal data rather than money. In August 2014, hackers attacked the networks of several banks, including J.P. Morgan Chase. They accessed customers' checking and savings account information undetected for over two months. J.P. Morgan estimated the attack affected 76 million households and 7 million small businesses accounts.

These examples have led the financial sector to take more responsibility for its own security. Companies have taken charge of data management, while creating processes designed to protect critical assets and business continuity. They have also worked to understand the motives and methods of hackers, giving themselves a heads up on the latest threats. They still have much to do, though. Wherever cyber threats come from and whoever they target, they can still cause a great deal of damage.

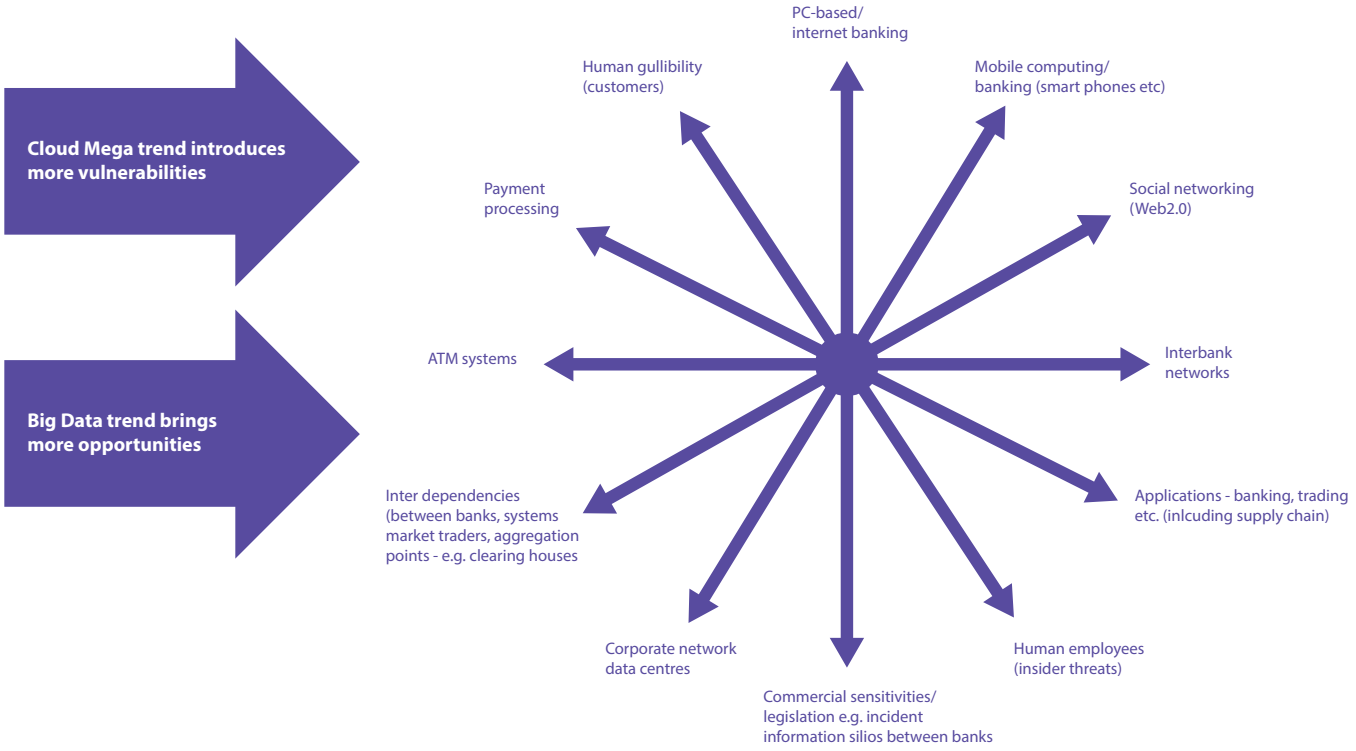
The web of vulnerabilities

The financial sector has developed and grown relatively quickly over the past century. And more recently, the fast rate at which organisations adopt new technology leaves weak spots for hackers to make use of.

Many of these occur where organisations are interacting with customers, like online or mobile banking and ATM systems. Figure 1 shows the common targets for cyber attacks, from data centre weaknesses to the employees themselves potentially flouting security restrictions either by accident or otherwise.

Figure 1.

Web of Cyber Vulnerabilities – Financial Sector



A cyber chain reaction

An interesting part of the web of cyber vulnerabilities? The way financial institutions depend on each other. For instance, many large banks have investment arms that rely on interacting with the stock markets. An attack that affects these stock markets can also have serious consequences for the investment arms, which then affects the retail side of each bank and its customers.

The links between organisations mean that if one organisation suffers a serious breach, it could be disastrous for many — a fact that organisations might not realise. What we call nation state threat actors (hostile countries using cyber warfare) target these links as a way of creating a cyber chain reaction across an entire financial markets infrastructure (FMI).

Many financial institutions guarantee business continuity by spreading their operations across more than one data centre. These mirror a company's data in real-time, preventing downtime if hackers target one data centre.

However, a sophisticated attack would also disrupt the backup (along with any cloud services as well). Corrupting data for a sustained period prevents the organisation from recovering transactions and trades, undermining the trust of the financial institution and the markets themselves.

The problem with people

Financial systems become vulnerable when they interact with individuals, especially as people get used to new technology and ways of working. You almost certainly have antivirus software on your desktop computer, but how well protected are your other devices? Two-thirds of people leave smartphones completely unguarded, not even asking for a passcode before granting access (Henshaw, 2014).

There's also a chance that one poor decision could leave you as the victim of a scam. Between 2013 and 2015, the Carbanak criminal gang used malicious emails to con bank employees and sneak onto their networks (Davis, 2015). Once inside, the gang accessed video surveillance, mimicking staff behaviour to make fraudulent money transfers without raising suspicion. Hitting up to 100 financial organisations in over 30 countries, the gang stole roughly $1 billion.

Identifying the insider threat

And sometimes, it's people on the inside who can cause deliberate malicious breaches. It could be an unhappy employee using privileged access to financial systems — what we call 'insider' threats.

Back in 2007, former HSBC employee Hervé Falciani used his position at the bank to steal files linked to more than 100,000 Swiss accounts (Watchful, 2015). After allegedly failing to sell this data, he eventually passed it on to the French Government. This led to a huge investigation, with the French authorities claiming that HSBC operated a large-scale tax avoidance scheme.

The breach has caused untold damage to the bank's reputation, while its Swiss arm could also be facing a criminal trial (Leigh et al., 2015).

Whether the revelations turn out to be true or not, HSBC offers a devastating example of how an insider threat can wreak havoc.

Within global organisations, internal fraud or security teams need to collect evidence and have an overview of employee activity. This includes telephone, internet and data access. Recording such information for future reference can alert organisations to potentially fraudulent actions. It forms the basis for how financial organisations can use Big Data to eliminate vulnerabilities — a topic we'll look at in greater detail later on.

The financial sector now has a far greater concept of its own vulnerabilities than it once did. Many organisations see cyber resiliency as a top priority and work with partners to share information on the latest threats. This shows the importance of using intelligence to highlight vulnerabilities— and why financial institutions always need to be aware of the new methods hackers develop to breach security.

Tricks of the trade

Hackers use a number of ways to exploit the vulnerabilities in financial organisations. Here are some of the most common attacks companies face:

Phishing

A cyber threat that tricks people into giving away sensitive information like bank details. Scammers send an email threatening to lock customers' (or employees') computers unless they go to a particular website and make a card payment. This site might also infect computers with malware (see Figure 2, threat 11).

Vishing

Financial Fraud Action UK (FFA) said vishing attacks caused losses of at least £23.9 million in 2013 with its mixture of phishing and voice phone calls. Criminals call customers, alerting them to an issue with their bank account — advising them to call the bank immediately. If they do this, however, the hacker hasn't hung up. The scammer can then pretend to represent the bank and capture confidential information.

Smishing

This combines phishing with SMS text messages. Criminals send messages to customers' phones that, if they activate them, infect the phones and lets hackers steal data (see Figure 2, threat 1).

Malware

This is one of the most significant cyber threats, infecting customer and banking systems. Malware installs malicious software on people's computers, often monitoring the keys they type to steal bank details.

Spear phishing

This is where scammers gather information about employees of financial organisations from social networking sites. Hackers then target these people with a phishing attack designed to transfer funds or infect systems with malware (see Figure 2, threat 5).

Distributed denial of service (DDoS)

DDoS attacks are a common way for hackers to exploit network vulnerabilities. They usually target websites, flooding them with huge levels of traffic to overload them and make them unavailable to actual users.

Insider threats

These aren't specifically a cyber vulnerability, but the relative ease with which employees could use malware to infect financial systems is a significant threat. Insider threats can also be responsible for data breaches, as in the prominent case of Edward Snowden in 2013.

Figure 2.

Evolving exploitation of vulnerabilities by cyber criminals on Retail Banking

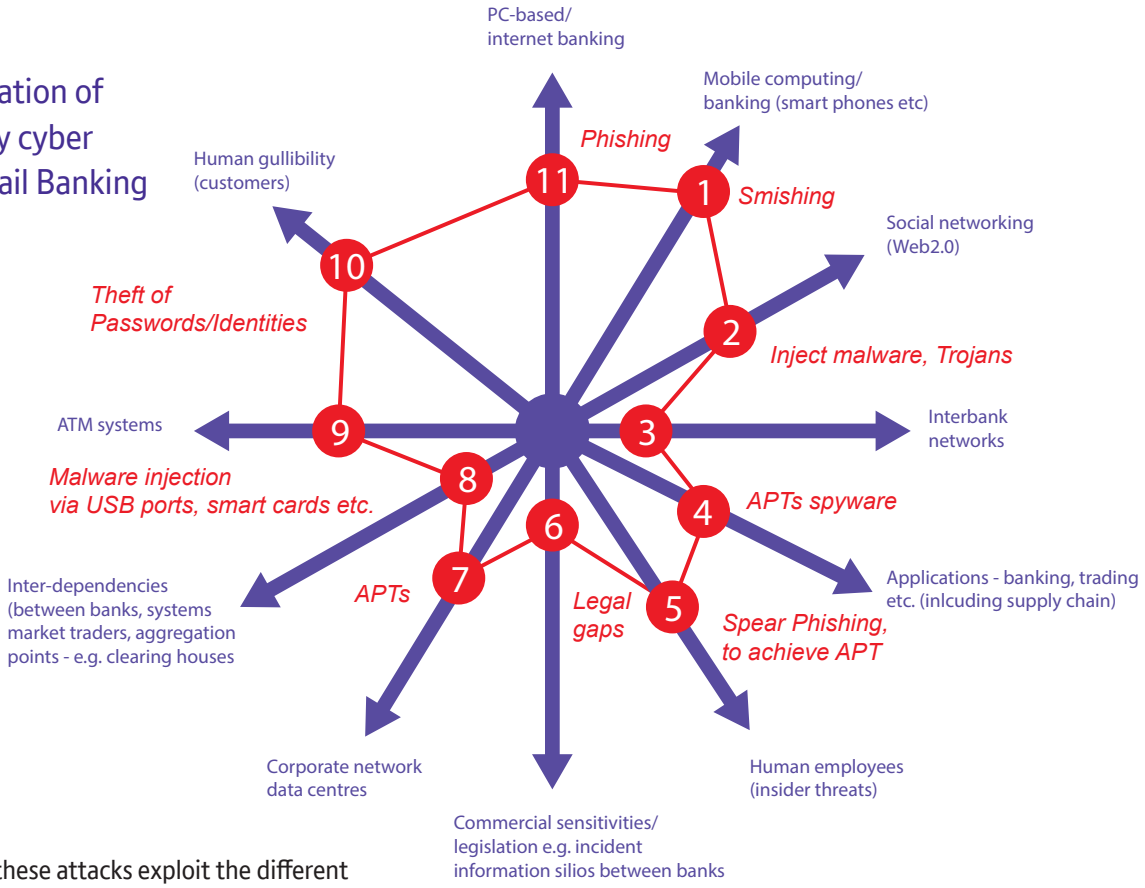
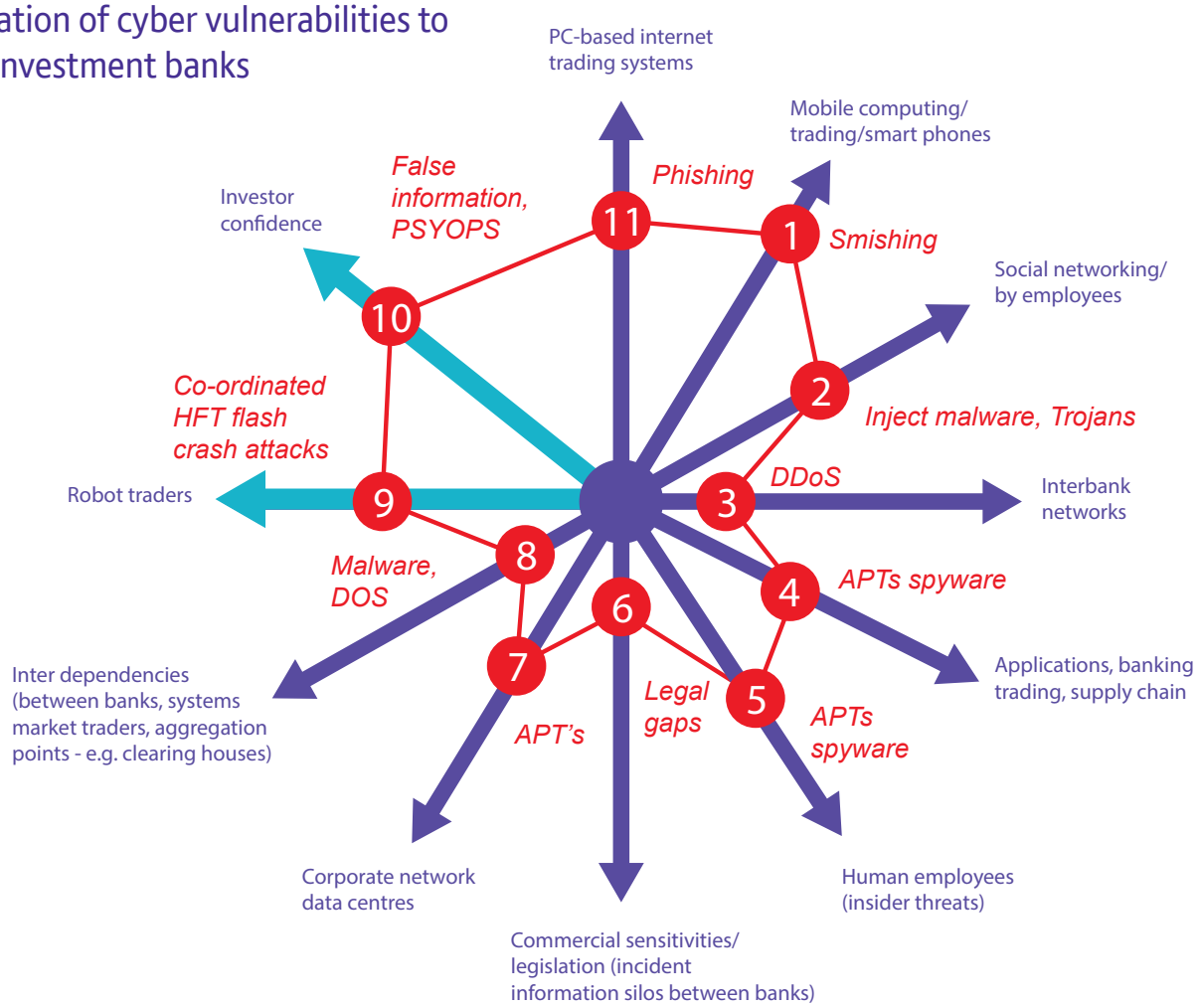


Figure 2 shows how these attacks exploit the different weak points in financial organisations' cyber security.

Cyber threats to investment banking

Figure 2a.

Exploitation of cyber vulnerabilities to target investment banks



Investment banking faces many of the same threats as retail organisations, but with two key differences. As Figure 2a shows, automated trading processes and investor confidence become important targets for hackers.

Each of these vulnerabilities can have a devastating impact on global markets if exploited. The 2010 'flash crash' mentioned earlier offers the most famous example of this, with markets falling by hundreds of billions of dollars before recovering. This event highlights just how damaging threats to investment banks can be — even when not specifically exploited by cyber criminals or nation states.

Coordinated flash crash attacks

Investment banks rely on their ability to buy and sell stocks and shares faster than any human. To do this, they use high-frequency trading (HFT) algorithms (also known as robot traders) to process huge numbers of transactions in milliseconds. These algorithms give their human controllers a competitive advantage, but they also offer cyber criminals the chance to exploit a dangerous vulnerability (see Figure 2a — threat 9).

Hackers (or rogue traders) can use the superior processing speed of 'predatory' HFT algorithms to trigger (and sustain) a flash crash in markets — inadvertently or not. They also offer nation state threat actors the ability to target specific components of markets. For example, this could involve undermining a country with an economy dependent on its energy sector.

The markets do have some defences against cyber attacks that use HFT algorithms. Following the 2010 flash crash, investment banks put regulatory 'circuit breakers' in place. These trigger when prices reach a pre-determined threshold and cause markets to stop trading, giving banks the time to prevent a crash (as well as the cancellation of legitimate transactions happening after a recovery).

Misinformation attacks on investor confidence

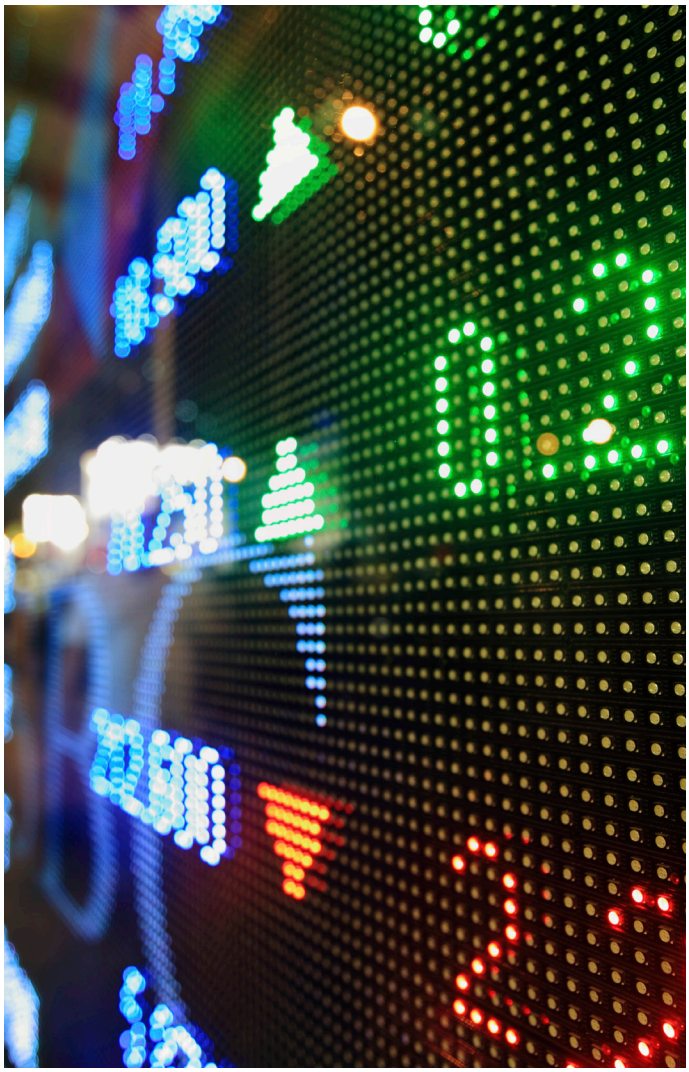
HFT algorithm attacks can also lead to coordinated campaigns to undermine investor confidence. This threat prevents a market's ability to recover in the event of a crash, causing further damage to the economy of the targeted country (see Figure 2a — threat 10).

When the regulatory circuit breakers stop market activity, traders have the time to realise the danger of the situation. A cyber attack spreading misinformation during this period can have a huge impact on the confidence of investors.

In April 2013, the US stock markets fell by 143 points following a fake tweet sent out from the Associated Press account (Moore & Roberts, 2013). Hackers accessed the account and posted a message reporting explosions at the White House and the injury of Barack Obama. This highlighted the issue of using HFT algorithms that use data from news outlets to make trades.

Securing the stock markets

Even as one-off events, these threats can have serious repercussions for investor confidence, while a series of attacks could make the markets dysfunctional. This shows how the financial sector gains a significant advantage from the technology that automates its trading processes. However, it has to adapt its security procedures to keep pace with the vulnerabilities this creates.



Cyber threats and the cloud

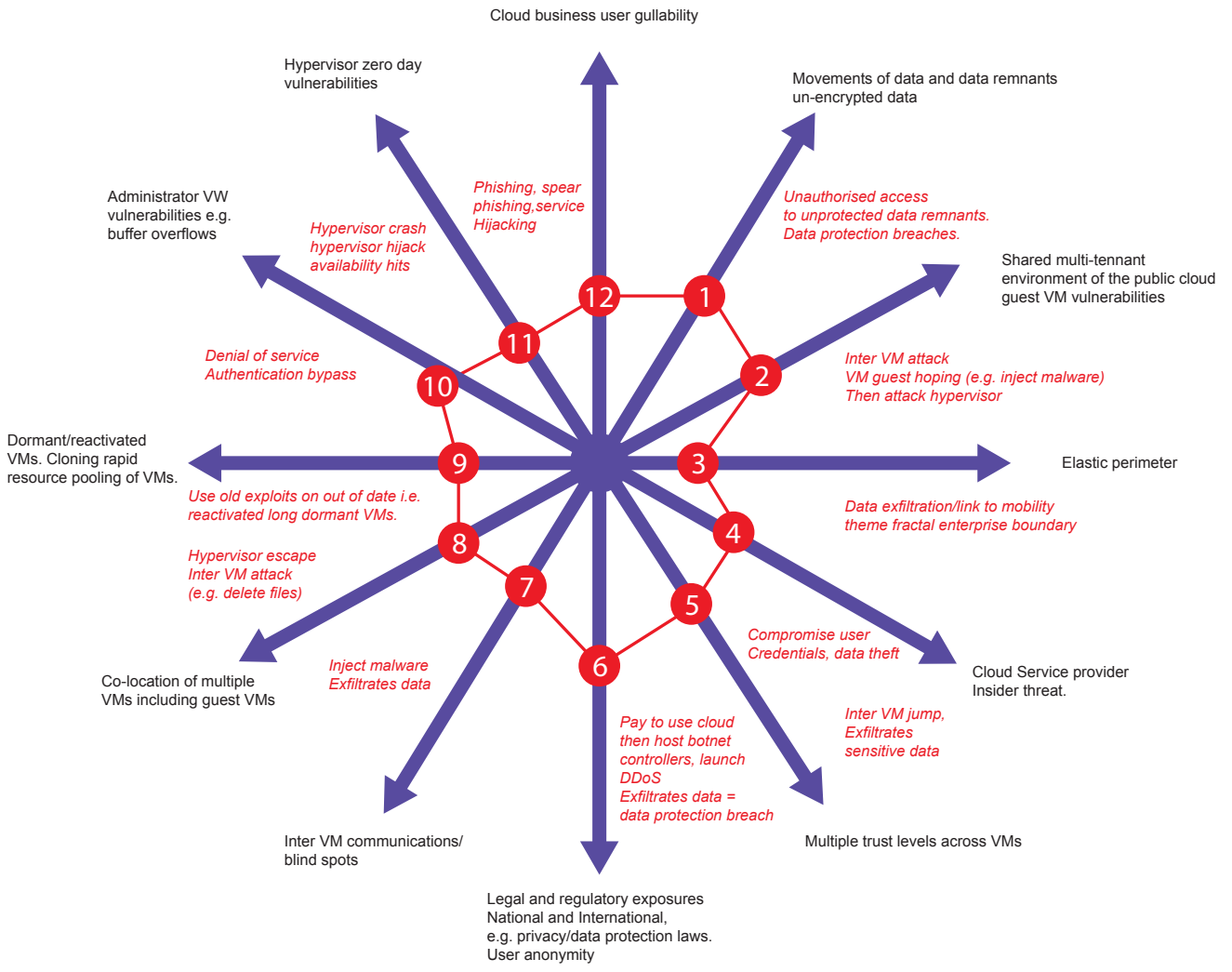
Moving operations (such as website management or credit risk analysis) to the cloud offers financial institutions the chance to cut costs and be more productive. It means they can make key data and apps such as customer relationship management (CRM), data analytics and mobile contactless payment services more accessible across their organisations.

Uncovering new vulnerabilities

To get the most from their cloud services, financial organisations need to get their head around cloud security. Moving data and applications to external data centres opens companies' networks up to a range of new cyber threats.

Figure 3 shows how moving to the cloud makes financial organisations more vulnerable to cyber attacks. From unauthorised data access to denial of service, there are many ways for hackers to steal information from the cloud or prevent companies from using essential apps.

Cyber Threat perspective on Cloud – The Web of Threats



Multiplying the issue

It's one thing to be aware of the threats, but managing cloud vulnerabilities can prove challenging when financial institutions use a mixture of public and private cloud services (known as hybrid cloud). This means they often have to turn to multiple suppliers — and potentially create new weak spots.

When looking for cloud suppliers, it's important to pick a partner you can trust — as well as thinking about how you plan to manage each service.

Federated Trust model

One option? Choose suppliers that are part of a Federated Trust. This means you can use the same configuration settings and account details across multiple systems run by different providers.

With this model, you can be sure your cloud services will work alongside each other, but you might find yourself locked in to using the vendors you originally chose. This could cause problems if your suppliers don't meet your expectations for cloud security.

Cloud of Clouds

Alternatively, you can turn to the Cloud of Clouds model and contract directly with different independent cloud service providers. This gives you a lot more freedom to choose the suppliers and applications that work for your organisation — especially when it comes to security. However, it is difficult to make sure different systems from various suppliers can work together, leaving gaps for hackers to take advantage of.

Avoiding cloud cover

Many financial organisations know there are security risks involved with moving to the cloud. Six out of ten see data confidentiality as an issue, while more than half are similarly worried about how cloud services will match compliance requirements (Donnelly, 2015).

The danger is that these concerns could prevent companies from investing in cloud services, causing them to miss the chance to improve their businesses. With a better idea of the common vulnerabilities, it's easier for the financial sector to focus on how to get the cloud security they need.

Cyber threats and Big Data

The other new technology to have made a splash in the financial sector is Big Data. Nine out of ten organisations are looking to use it more to help them achieve business goals (Banham, 2015). It involves bringing together large volumes of data, then using that to spot patterns. This is especially useful when it comes to the huge amounts of trading information financial companies deal with.

Using Big Data, the finance sector can significantly improve how it detects and prevents fraud. Many financial organisations are using real-time analysis that allows them to spot threats much more quickly. They can then bolster their cyber defences wherever they need to and make sure attacks don't turn into serious security breaches.

Keeping customers safe

A common example of Big Data in action is the way organisations can track customer behaviour. You might have received a phone call from your bank while on holiday abroad. Having spotted you were making transactions in an unusual location, the bank called to check they had nothing to do with fraudulent activity.

This is a basic form of monitoring data patterns. With Big Data, banks can bring open-source information into the picture, checking things like social media before spending time and resources trying to make contact with a customer. It also means they can react quicker when a fraud happens.

Tackling the insider threat

Big Data also gives financial organisations the ability to tackle insider threats. Building a pattern of employee behaviour means companies can easily spot malicious behaviour. If, for instance, someone in the HR department at a retail bank unexpectedly starts to access customer files, this activity won't slip through the net. Organisations can catch it in real time and deal with it.

Financial organisations can be much more confident in their security if they know they can spot threats straight away with Big Data.

Big Data, big opportunities

Big Data is an important tool the financial sector can use to manage the risks presented by cloud computing. The trick, though, is having the right information to hand. In this way, intelligence on the latest threats is becoming a key part of cyber security. It helps organisations to know what to look out for and be more successful in preventing attacks.

Raising awareness, lowering risks

From cyber criminals and terrorists to nation state threat actors and their proxies, a wide range of hackers target the financial sector. This is because of the money it handles and the importance it has to the global economy.

There are also a number of vulnerabilities in financial institutions for these hackers to exploit. Companies face significant threats that they need to predict, detect and manage to avoid disastrous consequences such as losing revenue, suffering damage to reputations or even market crashes.

Picking the perfect partner

Many organisations share concerns about the security of cloud computing. Also, most companies don't have the skills or resources to analyse Big Data and react to security incidents in real time. But acknowledging these limitations is the first step to eliminating vulnerabilities and improving cyber security.

Working with a dedicated security partner means financial organisations can counter the risks of cloud computing while taking advantage of Big Data analysis. They can also tackle the occasions when individuals (whether employees or customers) get in the way of cyber security, implementing policies to prevent accidental and malicious insider threats.

An intelligent solution

To get the most from new technology, financial institutions need to use the expertise of an experienced team who can bring them the latest threat intelligence. This gives companies the best chance of discovering vulnerabilities before the hackers do, and can equip themselves to defend against all manner of attack.

Cyber threats are no reason for the financial sector to avoid adopting new technologies. Financial organisations should select a strong security partner to help manage the risks — a security partner that can predict threats and keep hackers out of their networks.

Bibliography

Banham, R. (2015). 4 Ways Financial Institutions Can Bank On Big Data In 2015. [Online] Available at: http://www.forbes.com/sites/centurylink/2015/04/14/4-ways-financial-institutions-can-bank-on-big-data-in-2015/ [Accessed 21 May 2015].

Banks, R. (2015). Mobile is the new banking branch. [Online] Available at: http://www.mobileindustryreview.com/2015/03/mobile-is-the-new-banking-branch.html [Accessed 15 June 2015].

BBC News. (2011). Government 'may have hacked IMF'. [Online] Available at: http://www.bbc.co.uk/news/technology-13748488 [Accessed 21 May 2015].

Clinch, M. (2015). 'Flash crash' trader told he poses a 'clear flight risk'. [Online] Available at: http://www.cnbc.com/id/102693235 [Accessed 21 May 2015].

Davis, O. (2015). Hackers Steal $1 Billion In Biggest Bank Heist In History: Could They Take Down The Whole System Next Time? [Online] Available at: http://www.ibtimes.com/hackers-steal-1-billion-biggest-bank-heist-history-could-they-take-down-whole-system-1818010 [Accessed 21 May 2015].

Donnelly, C. (2015). Financial sector cloud adoption on the rise despite security concerns. [Online] Available at: http://www.computerweekly.com/news/2240241763/Financial-sector-cloud-adoption-on-the-rise-despite-security-concerns [Accessed 21 May 2015].

Fleming, S. (2014). Market watchdog warns on danger of cyber attack. [Online] Available at: http://www.ft.com/cms/s/0/82519604-2b8f-11e4-a03c-00144feabdc0.html#axzz3agufzATc [Accessed 21 May 2015].

Henshaw, S. (2014). Two Thirds of British Smartphone Users Failing to Implement Basic Security Settings. [Online] Available at: https://www.tigermobiles.com/2014/07/smartphone-users-failing-implement-basic-security-settings/ [Accessed 21 May 2015].

Konczal, M. (2014). Frenzied Financialization. [Online] Available at: http://www.washingtonmonthly.com/magazine/novemberdecember_2014/features/frenzied_financialization052714.php?page=all [Accessed 21 May 2015].

Leigh, D. Ball, J. Garside, J. & Pegg, D. (2015). HSBC files timeline: from Swiss bank leak to fallout. [Online] Available at: http://www.theguardian.com/business/2015/feb/11/hsbc-files-timeline-from-swiss-bank-leak-to-fallout [Accessed 21 May 2015].

Moore, H. & Roberts, D. (2013). AP Twitter hack causes panic on Wall Street and sends Dow plunging. [Online] Available at: http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall [Accessed 15 June 2015].

Watchful. (2015). Falciani, a Warning to Insider Threat. [Online] Available at: https://www.watchfulsoftware.com/en/news-events/blog/posts/falciani-a-warning-to-insider-threat [Accessed 21 May 2015].

World Bank. (n.d.). Data - GDP. [Online] Available at: http://data.worldbank.org/indicator/NY.GDP.MKTP.CD [Accessed 21 May 2015].

Yang, S. (2014). The Massive Hack Of The Nasdaq That Has Wall Street Terrified Of Cyber Attacks. [Online] Available at: http://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7?IR=T [Accessed 21 May 2015].

Zetter, K. (2011). Citi Credit Card Hack Bigger Than Originally Disclosed. [Online] Available at: http://www.wired.com/2011/06/citibank-hacked/ [Accessed 21 May 2015].

Offices worldwide