The cyber threat to banking

A global industry challenge

bba

The voice of banking

In association with

pwc

Foreword

Richard Horne

PwC Partner – Cyber Security

The world has changed over the last few years, especially within banking. Its processes – from retail transactions to market operations – have been transformed by technology and continue to evolve. But there is a very real possibility that the industry's digital dependency could have material impacts for individual banks and even develop into systemic concerns. This report provides valuable insight into some of these emerging risks.

Today's organisations increasingly rely on third party systems in order to provide many of their digital services. Whether it is external data feeds, customer and staff devices or cloud services, banks find themselves having to adapt to relying on systems that are outside their control.

This opportunity has not escaped the attention of criminals, hacktivists and even nation states, who are beginning to harness the speed and scale offered by interconnectedness as weapons of attack.

This is problematic for the industry. Traditional approaches to risk management focused on a single malicious agent, or single points of attack. However, digital attacks can target multiple systems or processes in parallel causing widespread harm. An individual online banking or credit card fraud may be small but their collective impact can be vast – companies face death by a thousand cuts in this new digital age.

Co-dependence between banks for risk management is not new, but they now find themselves extending this dependence to a widening variety of non-bank organisations. This is brought home by the (albeit fleeting) impact on markets following the breach of a market data provider's Twitter account by the Syrian Electronic Army a year ago, and the wide scale impact of the compromise of credit card information from Target's

systems in the US in December – especially when you consider that the latter stemmed from a breach through a refrigeration company.

Interconnected risks therefore require organised responses. The time has passed when banks can take their own approach without regard to the wider system in which they operate.

That's why initiatives such as the Cyber Security Information Sharing Partnership as well as BBA and other banking industry-sponsored information sharing schemes are proving such a valuable channel for managing evolving and emerging cyber threats.

We are all beginning to realise that only a market-wide response can provide serious, long-term answers to the global industry challenges caused by cyber threats to banking.

The cyber threat to banking

A global industry challenge

Issue

In the last 10 years, digital technology has revolutionised economic and social interaction. It has transformed the way we do business, the way we educate ourselves, the way we sell and buy products and the way we share data. Internet use is growing and the methods by which it is accessed are diversifying. Malicious cyber actors are fully aware of this revolution and are taking full advantage of it. Firms have indicated that 2013 saw an exponential increase in cyber-attacks and a recent PwC survey demonstrates that 93 per cent of large organisations last year suffered a security breach.[1]

Defending and countering cyber-attacks whilst keeping up to date with evolving regulations and policy is a complex challenge. Coupled with changing business requirements, speed to market pressures, expansion into emerging markets, business innovation requirements and budget cuts, the challenge for managing cyber risk is significant. Firms are already investing heavily in cyber security. A recent BIS paper indicates that the UK financial sector is already spending over £700 million annually.[2] The issue is also being managed at board level, with 86 per cent of banking and capital market CEOs identifying technological advances as the trend that will have greatest impact on their businesses.[3]

The economic effects of cyber-attacks can reach far beyond simply the loss of financial assets or intellectual property. There are costs associated with loss of client confidence, the opportunity costs of service disruptions, "cleaning up" after cyber incidents and the cost of increased cyber security. More and more, damage to brand and reputation in the

93 per cent of large organisations last year suffered a security breach

the amount annually spent on cyber security in the UK

60 per cent of firms identify the speed of technological change as a threat to their growth prospects

70 per cent of banking and capital market CEOs identify cyber insecurity as a threat to their growth prospects

aftermath of an attack is perceived as a critical risk to firms. In addition, as a key enabler of economic and social development, the banking sector needs to think about the critical infrastructure nature of its operations. PwC report that nearly 60 per cent of firms identify the speed of technological change as a threat to their growth prospects.[4]

Cyber threat actors have a global reach and cyber threat mitigation strategies need to be considered through a global lens. Additionally firm's cyber responsibilities are often split between different departments and this can cause difficulties in not only understanding and prioritising threats but responding to them. More widely the financial sector interconnectedness means that successful attacks on smaller firms or third party supply chains can significantly affect the wider market. Vendors, suppliers, customers and our colleagues are all critical components of a successful business, but come with risks, and successful attacks against these often perceived weaker links will have an indirect impact. The supply chain threat has most recently been demonstrated through the high-profile Target data breach and the identification of the Heartbleed vulnerability. Both examples illustrate the indirect impact of cyber incidents on banks. More than 70 per cent of banking and capital market CEOs identify cyber insecurity as a threat to their growth prospects.[5]

Scope

This paper seeks to provide a view of the current cyber threats targeting the banking industry in order to promote dialogue on collective protection strategies. The cyber challenge will remain complex. Threats will evolve rapidly with the development of new technologies, the ever changing geo-political landscape and, not surprisingly, from our efforts to counter them. The specific threat profile faced by our member banks will also vary according to the nature of their business. Firms will have different cyber security strategies depending on what matters to them and these will be at different stages of development and implementation. We need to be agile as we develop these long term policies, continuously incorporating new ideas as our knowledge increases.

Recommendations

Enhanced exchange of cyber knowledge

As cyber threats evolve, it is essential that banks build their knowledge of emerging risks so that effective mitigation strategies can be put in place. More effective sharing of knowledge and experiences across the banking sector will support such efforts. The BBA, working with members and other partner bodies should consider how the mechanisms for this sharing can be optimised, to support actions by banks against emerging cyber threats. A BBA-led mapping exercise has identified there is a need to provide opportunities for smaller firms to participate in cyber intelligence sharing, attuned to their requirements.

Intensified co-ordination to influence strategic policy

As political focus on cyber issues increases, it is important that the banking sector is proactive in the development of new policies and strategies, to ensure that they reflect industry requirements and experience. At the domestic level continued dialogue with key government departments is required. There is a need for a more joined up international banking industry approach including the European and International Banking Federation to influence and align global regulations.

Measurement of industry wide cyber impacts

A more comprehensive view of the impact of cyber offending against the banking sector would support effective decisions on future resource allocation. Consideration should be given to common measurement methodologies by banks to support the consequent development of industry-wide statistics and analysis by the BBA. Improving measurement and recording practises is critical to understanding the cost and scale of cyber-attacks and how the nature of the problem is evolving over time.

A centre of cyber information

Cyber threats are fast moving and legislative/regulatory changes are likely to develop equally quickly. Similarly a range of international bodies are undertaking initiatives in the cyber field. The BBA can support banking sector cyber professionals by maintaining surveillance of key developments at the UK and international level, and reporting back regularly to members. More widespread and intensive use of the BBA Collaboration system can help member banks to access relevant cyber information quickly and easily.

A global industry approach

A coordinated response is required to prevent and protect banks against cyber-attacks. Comprehensive international level information exchange, ranging from intelligence sharing to best practise, should be considered. The capacity for firms to invest in their ability to share, ingest and process cyber threat intelligence needs support from Board level and initiatives to raise their awareness should be considered.

Malicious activity and motivation

The targeting of bank systems directly to modify, delete and/or steal data

Key criminal capabilities: network intrusion, hackers-for-hire, insiders (witting and unwitting)

Common actors: State-sponsored, criminals, hacktivists

Defending and countering cyber-attacks whilst keeping up to date with evolving regulations and policy is a complex challenge. Coupled with changing business requirements, speed to market pressures, expansion into emerging markets, business innovation requirements and budget cuts, the challenge for managing cyber risk is significant.

The targeted intrusion into a bank's systems is often perceived as the greatest threat due to the malicious actor's ability to not only steal data but modify or delete it. By exploiting software, hardware or human vulnerabilities hackers can gain administrative control of networks which, if abused, could cause catastrophic consequences. If publicised, network security breaches can affect share prices, cause irreparable reputational damage and impact on the stability of the wider financial market. The targeted intrusion of supply chain vendors and other institutions that the financial market relies on for stability (e.g. stock exchange, news agencies for share price information[6]) should also be borne in mind when identifying key cyber risks to your firm. The supply chain threat commonly manifests itself through insecure retail outlets, whereby banks bear the brunt of cost from successful attacks due to card scheme rules.[7] Some firms have invoked "supply chain working groups" to manage risks associated with third parties and others have built comprehensive lists of who supplies what, so that during an incident information and intelligence can be shared with these companies.

State actors will utilise network intrusion methods as their objective is targeted against the bank directly, commonly referred to as advanced, persistent threats (APTs). State actors commonly engage in espionage, but there have been examples whereby network intrusion techniques have been utilised more 'overtly', to deliver destructive files such as Stuxnet.[8]

The targeted disruption of access to bank networked systems and services

Key criminal capabilities: denial of service, ransomware
Common actors: State-sponsored, criminals, hacktivists

Denial of Service (DoS) attacks are increasing in scale and effectiveness. Over the last 12-months cyber actors have increasingly utilised open

domain name servers to amplify their attacks. A high-profile example of this in 2013 was against Spamhaus, which resulted in the largest recorded DoS attack, reaching over 300 gigabytes per second[9] (the average being approximately 3).[10] Attacks continue to be aimed at the banks' website pages; however a recent DoS attack in Holland against a payment service system[11] demonstrated the indirect impact on banks when supporting infrastructure is successfully targeted. DoS attacks are used for extortion by cyber criminals and have increasingly been used as a distraction tactic to 'tie-up' company IT resources while furthering the actual aim of stealing data or intellectual property. Hostile nations also use DoS capability to prevent access to and the delivery of online services. Hacktivists groups use DoS to raise the profile of their campaign and generate publicity, which ultimately erodes customer confidence by disrupting online services. With multiple services offered via online channels, maintaining availability is critical to the banking sector. Additionally, negative media coverage following a DoS attack can have a significant impact on brand and reputation. Some firms have employed the services of DoS mitigation companies who provide protection to their online sites and content.

Ransomware is similar to DoS as it denies access to services, effectively locking it until a "fee" is paid. This capability is aimed primarily at customers, albeit recent variants have been shown to target businesses directly.[12]

Cyber threat actors have a global reach and cyber threat mitigation strategies need to be considered through a global lens.

The large scale harvesting of personal and business data to commit fraud

Key criminal capabilities: financial trojans, man-in-the-middle attacks, botnets, exploit kits, spam, social engineering
Common actors: Criminals, Terrorist (financing)

Financially motivated crime groups are a growing threat to banks. The growth in the "as-a-service" nature of the marketplace is fuelling an increase in the number of traditional crime groups and individuals drawn into cyber offending. Malicious actors previously entirely removed from cyber offending are attracted by the low risk and potentially high rewards offered by offending online. The availability of professional criminal services for sale, such as coding, the provision of infrastructure, tools and mules, means groups without the requisite technical skills can buy or rent all the required components to commit a cyber-attack against banks and their customers.

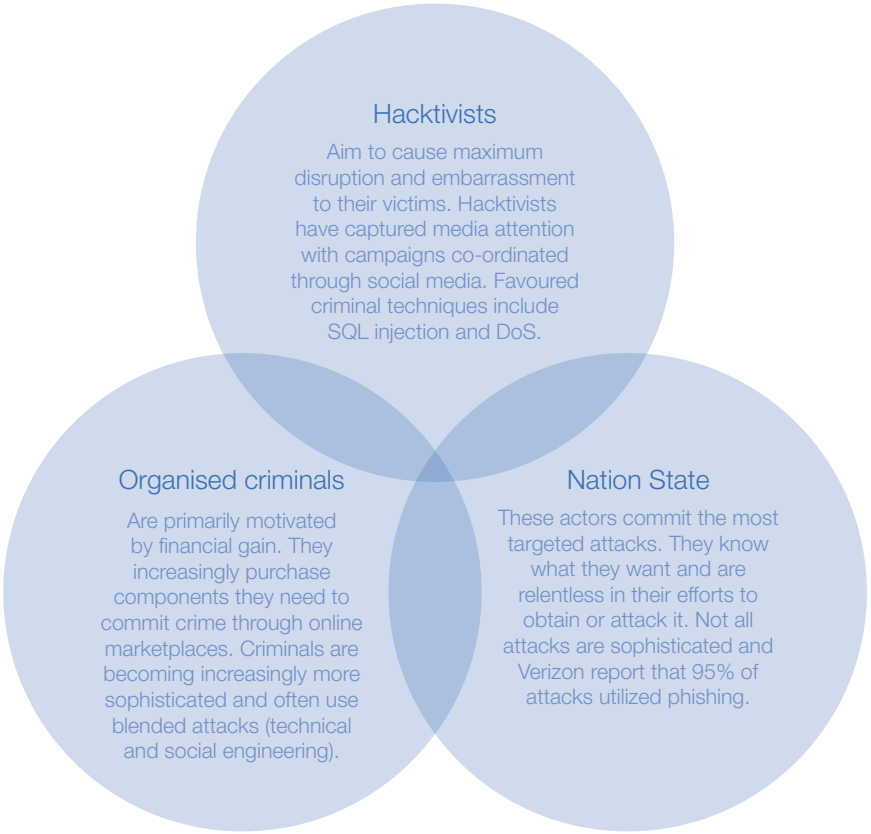
Malicious actors and modus operandi

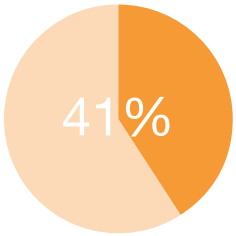
There is an international element to the cyber security threat. Cyber threat actors operate within the virtual environment, and as such are not constrained by real-world boundaries. Cyber threat actors have shown themselves to be capable of adapting quickly to the rapid pace of technological change, taking full advantage of the convergence of internet-enabled technologies to develop new and bespoke attack vectors. They also respond directly to the widely differing legal and regulatory

regimes in place within different countries and take advantage of the loose, often still developing, international policy.

The following diagram outlines the three main categories of malicious actors involved in cyber-attacks and illustrates that there are no clear lines between the perpetrators. The threat is dynamic and alliances will form, disband and re-form to suit the needs of those involved. This agility is essential to the success of malicious actors thus our agility to counter it is more important than ever.

Figure 1: The three main categories of malicious actors involved in cyber-attacks





of economic crimes are committed by employees within an organisation

Whichever category they belong to, threat actors will generally look to exploit the 'path of least resistance'. As technological systems and controls improve, people are increasingly seen as the weakest link. Employees at all levels within an organisation can act as insiders wittingly or unwittingly. They can either use their access to systems to assist malicious actors in conducting attacks or to compromise systems for their own gain. Threat actors are increasingly employing targeted social engineering techniques, such as spear-phishing, to trick individuals with access to key systems to inadvertently act as insiders. Insiders present a potent threat due to their privileged position with access to systems and knowledge of procedures. A recent PwC survey suggests 41 per cent of economic crime was committed by employees within an organisation.[13]

Political instability is often a trigger for cyber-attacks. The recent Russia and Ukraine crisis not only had a huge impact on banks' sanction obligations but also caused a wave of retaliation cyber-attacks from

Russian and Ukrainian groups. Another well-reported example of politically motivated cyber-attacks were committed against US banks in 2013 by the Muslim hacktivist group al-Qassam Cyber in retaliation for the posting to YouTube of a film that mocks the founder of Islam. Again in 2013 South Korea suffered a cyber-attack that impacted on payment services and cash machines that is suspected to be part of their ongoing dispute with the North – interestingly in this example the Anonymous hacktivist collective 'claimed' the attack, although South Korean officials suggest this was false.

Threats will evolve rapidly with the development of new technologies, the ever changing geo-political landscape and, not surprisingly, from our efforts to counter them.

Common tools and techniques

Malware

The development and deployment of financial Trojan malware is a key threat. The credentials harvested from customers and banks compromised IT systems are subsequently used for fraud. Financial Trojans of particular concern over the last 12-months continue to be variants of Zeus. The online availability of Trojan source code is a significant risk and the release of the Carberp source code in June 2013 could spawn an increase in variants for sale on criminal forums, as occurred when the Zeus code was released in 2011. Point of sale and mobile malware attacks are causing increasing concern to banks, especially when criminals chase higher returns by targeting high-value accounts held by corporate or business clients.

Social engineering

Due to the improvements in online authentication methods, such as two-factor or out-of-channel, malware campaigns are increasingly paired with social engineering tactics, commonly through voice or email (vishing and phishing).[14] Social engineering is still generally targeted at customers, although there have been examples of criminals targeting bank employees directly utilising their online accesses or by tricking them into installing physical devices to networks. Firms also need to be vigilant when engaging in corporate social media, information derived from these open channels can be used by criminals looking to gain a foothold within companies.

Deployment techniques

The deployment of malware is optimised through the use of exploit kits. The exploit kits automate the process of identifying vulnerabilities in victims' web browsers and plug-ins (notably java and adobe) to enable the installation of malware. Less technical methods such as email, online adverts and social media are also being used to deliver malware directly (e.g. via attachments) or indirectly (e.g. through hyperlinks to compromised websites).

Botnets

Botnets provide the industrial scale of much of the online fraud threat. Botnets are versatile tools that are created through the successful deployment of malware, once established botnets can facilitate further infections, denial of service attacks and anonymisation of criminal activities. Spam botnets are a global problem and often perceived as a mere nuisance. However, they are increasingly being used to facilitate

malware deployment directly (i.e. via attachments). Customer confidence and bank reputation in delivering online services can be damaged from spam campaigns, so their threat should not be underestimated. Firms have observed that spam is becoming increasingly difficult to detect as not only are the emails well-crafted but the sender address often spoofed from a familiar contact to make it appear even more legitimate.

Regulatory response and challenges in responding

Political focus on the issue of cyber security has increased. International authorities such as the United Nations and International Banking Federation are considering whether new legal instruments are needed for cyber matters. Specifically the European Union Network and Information Security Directive sets out mandatory data breach reporting regulations on the financial sector and the recent Financial Action Task Force meeting indicated that they will be providing guidance on virtual currencies this year. The Singaporean regulators have already legislated for mandatory data breach reporting within an hour of identifying it. This demonstrates that international standard and legislative bodies are fast moving into the cyber realm.

Governments are reinforcing the importance of cyber security; treating it as a national security priority and investing in it, despite these times of austerity. National and international initiatives such as cyber information sharing forums, private and public task-force models, setting cyber security standards and industry-wide cyber exercises are evidence of this.

Inconsistency of capability poses a risk to collective response. In a challenging economic environment, some BBA members have invested significantly in cyber threat mitigation capabilities. However, responding to a large-scale, systemic threat is beyond the capability of any single organisation. What's required is significant investment, by individual organisations and as part of a collective response.

To date information sharing on cyber threats has proved successful. Many BBA members participate in sector and cross-sector collaboration initiatives, however, some do not and this needs to change. Whilst this can be in part explained by the sensitivities of some of the issues, there is also an element of lack of awareness and cultural resistance. This means some firms do not have the required level of information to defend against current threats. As threat actors will target the weakest link, this weakens the sector's ability to defend the system as a whole.

Innovation is crucial to the survival of the banking industry and BBA members are constantly looking for ways to harness new technology to enable more efficient and effective services. In a highly competitive market, the desire and need to rapidly generate new products makes delivering comprehensive security controls for these products a formidable challenge.

To allow efficient resource allocation, an effective industry cyber threat mitigation strategy requires a good understanding of the impact of the threats. At present there are no industry wide statistics to accurately reflect this impact. Given the wide variety in the business profiles of BBA members, there will always be some differences in the approaches adopted. However, common, high level methodologies, indicators and

taxonomy could help support the development of industry-wide statistics. BBA members recognise the importance of regulator engagement in cyber risk management. A collaborative approach is essential to success; a shared view on priorities and a clear understanding of regulatory expectations would help banks to better develop their strategies and controls.

Endnotes

1. PwC 2013 Information Security Breach Survey
2. www.gov.uk/government/uploads/system/uploads/attachment_data/file/244978/bis-13-1206-network-and-information-security-directive-impact-assessment.pdf
3. PwC 2014 Annual Global CEO Survey
4. PwC 2014 Annual Global CEO Survey
5. PwC 2014 Annual Global CEO Survey
6. www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall
7. www.which.co.uk/consumer-rights/problem/how-do-i-use-chargeback
8. mashable.com/category/stuxnet/
9. blog.cloudflare.com/the-ddos-that-almost-broke-the-internet
10. www.news.softpedia.com/news/2-64-Gbps-Average-Size-of-DDOS-Attacks-Launched-in-2013-391974.shtml
11. www.infosecurity-magazine.com/view/31663/dutch-banking-system-ddosd/
12. www.nationalcrimeagency.gov.uk/news/256-alert-mass-spamming-event-targeting-uk-computer-users
13. PwC 2014 Global Economic Crime Survey
14. www.nationalcrimeagency.gov.uk/publications/207-nca-strategic-assessment-of-serious-and-organised-crime/file

www.bba.org.uk
BBA
Pinners Hall
105–108 Old Broad Street
London, EC2N 1EX
United Kingdom