Cybersecurity regulation and best practice in the US and UK

Produced in partnership with Jennifer Archie, Lore Leitner and Alexander Stout of Latham and Watkins LLP

Introduction to cybersecurity in financial services firms

In the wake of continued escalations in phishing and denial of service attacks against banks and other financial institutions, financial services firms face a rapidly evolving threat and government regulatory climate. Regulators in the United States have stepped up oversight and expectations for multiple layers of security and obligations to notify national regulators of significant cyber attacks or data breaches. In the United Kingdom, more than 80% of UK companies suffered a security breach in 2014, according to the Government Communications Headquarters (**GCHQ**), a British intelligence agency. PricewaterhouseCoopers has reported that the total number of worldwide security incidents climbed to 42.8m in 2015, a 48% rise from 2013. The compound annual growth rate of security incidents has increased 66% year-on-year since 2009. The Ponemon Institute estimates that, on average in the 2015 financial year, each data breach costs a US company USD$ 6.53m and a UK company US$ 3.72m in damages such as regulatory fines, reputational and commercial risk, and changes to IT infrastructure. Distributed Denial of Service (DDoS) attacks alone reportedly cost banks $100,000 (USD) per hour, and such attacks against the financial industry doubled during Q4 of 2014 to account for 15% of all attacks according to a Verisign report. Banks and brokers, big and small, possess deeply sensitive information and collectively control trillions of dollars, making even the smallest breaches a bonanza for successful hackers. As the legal standard for what is considered reasonable security evolves rapidly, and a raft of new security breach notification requirements are considered across jurisdictions, financial services firms face unprecedented scrutiny over the adequacy of their cybersecurity strategies. UK and US financial services firms acknowledge that cybersecurity has become a persistent, all encompassing business risk, and that they need to take action.

References:

American Banker: Bank Technology News--Banks Lose Up to $100/K Hour to Shorter, More Intense DDoS Attacks

This Practice Note outlines the regulatory roadmap that financial services firms (excluding payment services providers) must navigate in order to ensure a robust, compliant approach to information security management. It outlines key legislative and governmental approaches in the UK and the US, and suggests best practice frameworks for firms to implement integrated, comprehensive, crossborder cybersecurity systems to better protect customers' sensitive information, and better assist firms in meeting their regulatory requirements, in advance of a breach.

Evolving regulatory regime/enforcement

As cyberattacks have become increasingly prevalent, regulatory expectations for robust and comprehensive security management programs, incorporating integrated and fully operational administrative, technical, and physical safeguards and controls have increased as well

Data regulation and enforcement climate in the UK--protecting customer data from disruption, hacks and thefts

As financial services firms hold large quantities of confidential and personal information about their customers' identities, finances and individual transactions, data protection laws are a primary consideration in how data is collected, stored, disclosed and of course, secured against unauthorised access and use. UK law emanated from the Data Protection Act 1998 (DPA 1998) (which is based European Directive 95/46/EC), as well as the common law banker's duty of confidentiality, which extends to all information that the bank has about a customer. In addition, financial services firms will have to comply with various regulatory requirements. The financial regulator, the Financial Conduct Authority (**FCA**), has significantly more power than the data protection regulator, the Information Commissioner's Office (**ICO**), to sanction firms that fail to provide adequate data protection standards. However, the power of the FCA and the ICO cannot be understated.

References:

DPA 1998
Directive 95/46/EC

The protection of customer data is at the heart of the FCA's regulatory approach. As per Principles 2 and 3 of the FCA's Principles for Businesses (**PRIN**), regulated firms must make an appropriate assessment of financial crime risks associated with customer data and apply adequate risk management systems. The Senior Management Arrangements, Systems and Controls (**SYSC**) rules at SYSC 3.2.6R and 6.1.1R require that firms establish and maintain effective systems for countering the risk that the firm might be used to further financial crime, including IT control measures and physical security. Additionally, SYSC stresses the importance of business continuity, and SYSC 3.2.19G stresses that firms should establish appropriate arrangements to ensure that it can continue to function and meet its obligations in the event of an unforeseen interruption. Such arrangements will depend on the scale and complexity of the business, and they must be regularly tested and updated to ensure that they are effective. In the context of operational risk, firms should assess the likelihood and impact of disruptions from unexpected events (SYSC 13.8.5G) and plan to reduce the likelihood of a disruption (by succession planning, systems reliance and dual processing) and the impact of a disruption (by contingency arrangements and insurance) (SYSC 13.8.6G). The FCA also acknowledges the common practice of using an alternative site for recovery in business continuity management but notes that the firm should ensure that the site is appropriate for speed of recovery and adequacy of services and, where the site is shared, a firm should evaluate the risk of multiple calls on shared resources (SYSC 13.8.8G). SYSC 13.4.1G also imposes a regulatory requirement to notify the regulator immediately of any operational risk matter, of which, the regulator would reasonably expect notice, including significant operational loss and failure in systems and controls (SUP 15.3.8G). The regulator has stressed that security should be integral to a firm's operations--it must be part of the firm's strategic planning from the outset, and not incidental or reactionary.

In recent years, given changing consumer patterns and its statutory duty to reduce financial crime, the FCA has focussed its attention on the online world. The FCA and its counterpart the Prudential Regulation Authority (**PRA**) fined the RBS Group £56m (USD$ 88m) in November 2014 for inadequate testing procedures and failing to establish robust IT systems, which gave rise to consumer disruption as over 6.5m customers could not access their accounts online for several weeks. In its 2014 guidance on mobile banking and payments, the FCA noted that the potential for more complex online fraud attacks requires investment in stronger consumer security protections. Prior to this, in 2010 the FCA's predecessor organisation, the Financial Services Authority (**FSA**), fined Zurich Insurance plc £2.275m (USD$ 3.5m) following a loss of 46,000 policyholders' personal information, and for failing to provide adequate protection in a data breach arising from an outsourcing arrangement with another Zurich entity. In July 2009, the FSA fined three HSBC firms £3.2m (USD$ 4.5m) for losing confidential customer information, and failing to adequately secure its systems. In December 2007, the FSA fined Norwich Union Life £1.26m (USD$ 1.9m) for failings in data security controls after allowing access to, and the fraudulent use of customer records.

In line with this increasing regulatory pressure, in March 2014 the UK government launched the UK Computer Emergency Response Team (**CERT-UK**) to develop the UK's cyber resilience to criminal and state sponsored attacks on critical systems. CERT-UK works with multiple stakeholders across industry, government and academia and is responsible for:

- national cybersecurity incident management
- supporting crucial national infrastructure companies with regard to cybersecurity incidents
- promoting cybersecurity awareness; and
- coordinating and collaborating with other national CERTs

Crucially, CERT-UK will also provide advice to help companies prepare for and protect against cybersecurity incidents, including assisting with incident response. CERT-UK evolved out of the November 2011 Cyber Security Strategy which aimed to make the UK 'one of the most secure places in the world to do business in cyberspace' and which, by December 2014, the government had heavily invested in, earmarking £860m to deliver the strategy.

Regulation on the horizon in the UK

In addition to UK data protection and financial regulatory requirements, the European Commission (Commission) and the High Representative of the EU for Foreign Affairs and Security Policy adopted an EU cybersecurity strategy in February 2013. After over two years of debate, it is expected that the Network and Information Security Directive (NISD), which translates the principles of the EU cybersecurity strategy into binding legislation, will be adopted by the end of 2015 or early 2016 and will come into force (through national implementing legislation) in 2017.

The NISD will impose cybersecurity obligations on any 'EU market operator', which is any company that is important to national infrastructure--including banking and financial services firms. The NISD will also impose an obligation on businesses to report any security incidents to the newly established national competent authorities (NCAs). The NCAs will have the investigatory and sanctioning powers, though penalties for non-compliance will be limited to cases of intent or gross negligence. The exact extent and forcefulness of the NCAs powers are, as yet unclear, and will depend on the implementing legislation. But, financial services firms operating in the EU should be aware of the notification requirements which are about to come into force.

The EU's General Data Protection Regulation (GDPR), which is expected to be in agreed form in late 2015 and to take effect in Member States by 2017, also proposes that any personal data breaches are reported to regulators 'without undue delay and, where feasible, not later than 72 hours after having become aware of it'. Such an obligation on data controllers is one of the less controversial aspects of the GDPR, and highlights the paramount importance of data security in the European

regulatory framework.

Regulation in the US

For financial services companies in the US, laws addressing cybersecurity expectations and requirements include the Gramm-Leach-Bliley Act (**GLBA**), the Bank Secrecy Act, the USA PATRIOT Act, the identity theft red flags rule, and Sarbanes-Oxley. Banks are regularly examined on their compliance with these rules, as well as published information security guidelines and bulletins. As a result, the financial services sector in the US is among the most aware, most organised, and most sophisticated industries facing the cyberthreat, yet it is simultaneously amongst the most targeted. As a general matter, banks and other financial institutions, as well as their regulators lead the pack in terms of awareness of evolving risks and threats, and stepping up oversight and controls on cybersecurity.

Addressing the risks that cyberthreats pose to individual banks and to the banking system has been a top priority in the US for the Office of the Comptroller of Currency and the Federal Financial Institutions Examination Council (**FFIEC**). A key initiative was the interagency Cybersecurity Assessment conducted in 2014, which used a new pilot examination work program to assess the cybersecurity preparedness of more than 500 community financial institutions. That pilot assessment resulted in two FFIEC documents. One summarised the general observations from the work done, posed key questions for financial institution management to consider, and provided a list of resources. The second encouraged financial institutions to become members of the Financial Services Information Sharing and Analysis Center (**FS-ISAC**), to facilitate monitoring and awareness of cyber-threats and vulnerabilities. For example, the Office of the Comptroller of the Currency (**OCC**) 2013 guidance bulletin on risk management of third-party relationships re-emphasised the importance of understanding and managing risks associated with third parties, which may also include subcontractors. US banking regulators think the resilience of technology service providers is fundamental to safety and soundness.

For broker dealers and investment advisors, the US Securities & Exchange Commission (**SEC**) is a key regulator. The SEC has been actively raising awareness through public events and reports and conducting audits of broker dealers through the Office of Compliance Inspections and Examinations (**OCIE**). Like bank regulators, the SEC is also very focused upon cyber-risks arising from a firm's management of its third-party vendors, including the firm's practices of auditing and policing the vendors' access to their network. The new cybersecurity requirements are founded in Rule 30 of Regulation SP, which requires regulated firms (in this case, broker-dealers, investment banks, and investment advisors) to safeguard the confidentiality of customer records. The SEC has proposed, but not adopted, more specific cybersecurity rules, but nevertheless exercises significant authority over cyber practices through the OCIE guidelines.

For public companies, the SEC is very focused upon the completeness and accuracy of disclosures to shareholders about cyber-risks and potentially material risks and financial losses, following an attack. The SEC routinely asks filers whether they are currently experiencing attacks or threats to information systems, and to adopt risk factors to state the nature of the threats. The SEC's Division of Corporation Finance's Disclosure Guidance Topic No. 2, contains the critical guidance for disclosure of operational risks, including potential vulnerability to 'unauthorised access, mishandling or misuse, computer viruses or malware, cyber-attacks and other events that could have a security impact on 'your computer' systems'. The guidance states that a registrant may need to include a 'description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material', and provides an analysis of how loss contingencies should be considered for cyber-events.

GLBA or the Financial Services Modernisation Act, was enacted by Congress in 1999 in an effort to provide a forward-looking framework within which 'financial institutions' must proactively protect consumers' non-public financial information. Financial institutions are required by the GLBA to

References:
FINRA--member-regulation
FINRA--Report on Cybersecurity Practices (2015)

> 'establish appropriate standards' to safeguard customer's personal financial information, in order: (i) to insure the security and confidentiality of customer records and information; (ii) to protect against any anticipated threats or hazards to the security or integrity of such records; and (iii) to protect against unauthorised access to or use of such records or information which could result in substantial harm or inconvenience to any customer'.

Every firm and broker that sells securities to the public in the United States must be licensed and registered the Financial Industry Regulatory Authority, Inc. (**FINRA**), a self-regulatory organisation. The Member Regulation (Risk Oversight and Operational Regulation and Sales Practice) arm of FINRA regularly examines all firms to determine compliance with FINRA's rules and those of the SEC and the Municipal Securities Rule-making Board (**MSRB**). FINRA has made cybersecurity a focus of its recent audits and standards setting actions, most notably by conducting a targeted examination of the industry in 2014. FINRA's Report on Cybersecurity Practices (February, 2015), while not setting any new industry rules, explicitly lays out best practices for the industry, making clear the expectation that firms prioritise cybersecurity by devoting sufficient resources to manage the evolving risks. The FINRA also regularly issues information security bulletins, alerting member firms and brokers to specific attack behaviours and risks, and passing along means to detect and respond to such threats.

Investigating and responding to major denial of service attacks or advanced persistent threat events and restoring security to the network can easily lead to direct expenses in the tens of millions of dollars. Financial institutions also face potential civil liability to affected customers, shareholders, and companies damaged directly or indirectly by the loss of security, following serious attacks.

Being prepared to respond to major attacks

As firms face increased threats from cyber-attacks, numerous agencies have outlined cybersecurity guidelines, including the International Chamber of Commerce, the UK's Department of Business, Innovation & Skills, the British Cabinet Office, and in the US, FFIEC and the US National Institute of Standards and Technology (**NIST**). The Bank of England (**BoE**), the UK's central bank, has also issued guidance on cyber-security matters, introducing the CBEST framework to identify areas where the financial sector could be vulnerable to cyber-attacks, using government and commercial intelligence to identify potential attackers and to implement better practices after systems testing. See BoE's CBEST webpage for more information. Key common elements in these guides, as informed by our experience in advising large enterprises recovering from major attacks, include those listed below.

Risk assessments

Following a disciplined risk-assessment process is the first step for any risk mitigation program. Certain classes of cyberattackers actively focus on gaining access to financial networks, are extremely persistent and use advanced means to access and attempt to steal or damage data. Such attackers plant multiple means of unauthorised access throughout an enterprise to include entrenched malware, 'backdoors' and the misuse of legitimate credentials (ie usernames and passwords). They attempt to move around the internal network by hiding in the noise of normal everyday network traffic. In order to have the best chances of preventing or more realistically, quickly discovering and interrupting an attack, sophisticated financial institutions use advanced boundary and malware defence tools that not only detect clearly known artefacts (Indicators of Compromise, or **IOCs**), but also provide the ability to analyse network activity to search for patterns of anomalous or suspicious activities. Malware science is imperfect, because attackers change and evolve their tactics. Technical, administrative, and physical measures must be scaled to these very serious risks, as well as many other diverse attack means and methods.

The requirements to follow a formal, documented risk-assessment and mitigation process are particularly critical following any breach. In this sense, the first step to prepare for a breach is to have properly scoped and carried out this preventative process. Post-attack, regulators and affected parties frequently second guess--often with a strong hindsight bias--whether pre-breach risk assessments and mitigation efforts were sufficient. While regulators often deny a 'punish the victim' mentality, the reality of many high profile cyber-attacks can lead to that result, simply because the organisation was deemed too vulnerable to the attack, in highly foreseeable (ie preventable) ways. The organisation may be judged and have failed at avoiding an attack or leakage. Proper risk-assessment methodology therefore should generally follow accepted risk-assessment practices, and be fully documented, and consistently optimised as the threat environment morphs and evolves.

Key risk-assessment steps may include:

- **Identify reasonably foreseeable internal and external threats** that could result in unauthorised disclosure, misuse, alteration, or destruction of customer information or customer information systems. For financial institutions, the key attack risks include:
  - nation state attacks for economic or political gain
  - financially motivated organised criminal attacks, with the ultimate objective of identity theft, fraud, or stock market manipulation
  - hacktivists seeking attention or changes in commercial or government policies, and
  - disgruntled insiders seeking to inflict harm or secure financial benefits
- **Assess the likelihood and potential damage of these threats, taking into consideration vulnerabilities and attack vectors,** as well as the sensitivity of the targeted information. Examples of common attack vectors for financial institutions include:
  - destructive malware (ie which wipes or destroys data)
  - customised attacks targeting investment strategies, account numbers, social security numbers, intellectual, fraudulent wire transfers
  - spear phishing and social engineering to gain access to credentials or data, and
  - account takeovers
- **Assess the sufficiency of technical measures, policies, procedures, information systems and other arrangements in place to mitigate risks:**
  - **Technical measures,** including a 'defence in depth' strategy, where advanced tools examine network traffic as it passes and alerts human response teams (who usually act on alerts on 24/7 basis) to unremediated known malware, anomalous activity or patterns suggestive of malware or attack. Security alerts from tools protecting critical assets such as domain controllers, hosts on the network, key systems and applications, and routers and switches, for example, need to be aggregated, prioritised, indexed, and rendered searchable, usually through a security incident event manager. Encryption of data at rest, in motion, and in use is also commonly deployed.
  - Examples of expected **administrative measures** include the written policies and procedures--generally propounded by the IT function--governing complexity of passwords, access controls, background checks for workforce, rigorous selection and supervision of service providers and contractors with access to sensitive

systems or data (see below), recording/tracking of computer inventory, change management, device and media controls, and the like. Financial institutions are routinely examined and audited on the basis of the completeness and adequacy of these written policies.

- Examples of expected **physical measures** include restricting physical access to data centres and premises to necessary personnel in possession of electronic access credentials, dual authentication access readers at entrance doors of sensitive areas (ie include PIN pads or biometric readers), mandatory routine changes of PINs, individualised badging, escorts for all authorised visitors (ie maintenance or other vendors), deadbolt or other locks, motion-activated colour cameras, video monitoring for sensitive areas, locked server racks, controls logs, secure automated backup processes, tight inventory and secure decommissioning controls for unnecessary or outdated computer equipment, and regular reviews of alarm and physical access control systems.

Governance--pre-staging breach prevention and response expertise

From a governance standpoint, preparedness for a major data breach means first and foremost having the right people--internally and externally--**pre-staged** for rapid, expert response to a data breach crisis. This means at a minimum that internal subject matter experts sit on the board, and across functional areas, including not just information technology staff and leadership, but also within the communications, legal, insurance, customer relations, regulatory compliance and other pertinent departments. The Board should be fully engaged on information security budgets, roles and responsibilities, top level policies, risk and incident reporting. Internal audit, risk, or other specially designated committees are often appointed, with embedded technology expertise. SEC Commissioner, Luis Aguilar, provided specific guidance to directors of public companies as to what they can and should be doing to oversee cybersecurity in a speech concerning Cyber-Risk given in 2014.

Outside experts are also critical in a major attack. External experts should typically be identified and prepared in advance, in at least the following areas: technical investigation and remediation; **legal** advice; and **crisis communications.**

Chain of command confusion abounds in a crisis, unless careful preparations have been completed. Pre-staging these resources will ensure that decision-making aligns with pre-agreed responsibilities. Each member of the steering committee or crisis team will understand his or her role, and be empowered to make decisions and advise the group. Timing of response in a crisis is key. Poorly defined lines of decision-making authority on matters as simple as who is on what sorts of calls about the event create risk of inefficiencies, delays, loss of privilege and potentially errors in judgment.

- **Technical advisors.** Major attacks are automated and premeditated. In the advanced persistent threat scenario, changes to the computing environment or access to information transmitted across the network to which the attacker has unlimited access may prematurely alert to the attacker the discovery of their malicious activity and exacerbate the scope, duration and impact of the attack. Before taking investigative or remedial steps, many experienced security advisors therefore recommend that the attack be well identified, and that complex, and effective, plans to permanently eradicate the unauthorised access should be ready for execution, before the attacker is alerted to discovery.
- **Legal advisors.** Similarly, if expert legal advice is not sought-internally or externally--legal mistakes may also occur including notification errors (inaccurate or speculative information released, wrong people notified, wrong benefits offered), failures of documentation (auditable trail), loss of attorney-client or other legal privileges, over or undersharing with affected companies or individuals or regulators, shareholders, regulators, or loss of criminal evidence. Whether to notify law enforcement, affected data subjects, affected commercial partners, regulators, data protection authorities voluntarily, or if required, what to include in any such notice, is often a complicated, multi-jurisdictional, multi-stakeholder process. The facts necessary to form a correct legal judgment about these matters change and evolve daily, even hourly, in a major attack scenario. Similarly, unexpected issues can arise in the course of the technical attack recovery, such as the need to rapidly apply and follow confidentiality and data protection laws, notwithstanding an urgent need to deploy advanced forensic and monitoring tools of traffic traversing the corporate network.
- **Crisis communications experts.** Large financial institutions typically have highly-experienced communications experts on their staff, leading substantial departments. A major cyber-attack is a discreet category of 'crisis', with diverse causes and PR challenges, that requires targeted preparation. Many financial institutions have found that augmenting the internal team with outside experts with experience on major breaches in the same industry is very valuable. Media training specific to data breach scenarios is also common.

In addition, global enterprises holding large databases of sensitive personal financial or other information often pre-identify **vendors to handle automated notices and call centre support** for affected customers. When identified in advance, like other experts, these vendors can pre-stage their services to align with data-breach risks and scenarios, enabling a very rapid response in the event of an attack.

Vendor selection and supervision

An April 2015 survey of 40 banks by New York's superintendent of financial services found that only about a third require their outside vendors to notify them of any breach to their own networks, which could in turn compromise confidential information of the bank and its customers. Fewer than half the banks surveyed said they conducted regular on-site inspections to make sure the vendors they hire--like providers of outsourced technology functions, accounting firms, law firms--are using adequate security measures. About half require vendors to provide a warranty that their products and data streams are secure and virus-free. The survey of banks also found that financial firms in the US lag behind their counterparts in Europe when it comes to adding protections to safeguard information that is shared with third-party firms. The report stated that European banks were better at requiring vendors and other outside parties to use multifactor authentication.

Financial institutions should exercise appropriate due diligence in selecting service providers, require service providers by contract to implement appropriate security controls, agree to non-disclosure provisions regarding the institution's systems and data, and monitor and supervise these relationships over the life of the agreement.

Audits and testing

Hackers and cyber attackers are quick to expose online vulnerabilities. It is important to ensure that financial services firms invest in testing the robustness of their security, and have capacity to create patches or rewrite code to fix potential entry points for malicious actors at short notice.

Information sharing

In the US, the financial services sector has established a voluntary organisation to share cybersecurity alert and response information. Known as the Financial Service Information Sharing and Analysis Center (**FS-ISAC**), this organisation collects threat intelligence from across its membership and from the US Department of Homeland Security, and distributes that information to its members in real-time. Because cyber-incidents are often replicated across the industry, belonging to the FS-ISAC or its equivalent organisations in the UK, such as the Cyber Security Information Sharing Partnership (**CiSP**), can provide advanced notice of the sorts of threats currently being fought off by peer firms, that may soon impact a firm.

Cyber insurance

According to a March 2015 report by the UK Cabinet Office, 10% of UK firms have some form of cyber cover and only 2% of large UK businesses have standalone cyber-insurance products. Indeed the market, while quickly growing, is still in its infancy, with relatively expensive products and relatively poor discounts for good behaviour. Nevertheless, a number of tailored products are emerging and, given the expense of data breaches, the option of cyber insurance may be a prudent investment for financial services firms. According to an underwriting manager for cyber, technology and media at Lloyd's syndicate Barbican, the market for cyber insurance had experienced a 50% increase in insurance submissions during the first three months of the year, when compared to the same period in 2014, with 70% being first time purchasers.

References:
IT Security Guru--70% of cyber insurance applicants are new, says Lloyd's of London

Conclusion

The financial services industry is at the epicentre of the escalating global cyber assault on private enterprise. Regulators on both sides of the Atlantic have awoken to the seriousness of these threats, both to individual consumers and to the world economy, and are placing increasing demands on the industry to prepare itself and defend networks.