CLIFFORD
CHANCE

Briefing note October 2015

Cyber crime – a growing threat to financial institutions

Combating cyber crime is now at the top of the agenda for government and industry alike. This is in recognition of the fact that in an increasingly cashless society, the opportunities for cyber-enabled fraud will increase and attract growing criminal interest.[1] In turn this means that financial institutions need "*best-in-class*"[2] protection against cyber crime. The challenges in doing so however were spelt out by the National Strategic Assessment of Serious and Organised Crime 2015 published in June 2015: "*the pace of technological change and the adaptability of the cyber criminal means that law enforcement will always be playing catch-up*."[3] In these circumstances what are the expectations on financial institutions?

Broadly speaking, the response by regulators and authorities across the globe to the increased cyber crime threat is to impose ever greater responsibilities on the victims of cyber attacks.

Some recent steps being taken in the financial sector across the globe to encourage and enforce proper cyber security standards are set out below.

On 15 September 2015, and in light of what it called the rise across the globe in "*the frequency, stealth, sophistication and the potential impact of cyber attacks*", the Hong Kong Monetary Authority ("**HKMA**") wrote to all Chief Executives of all Authorised Institutions ("**AIs**") highlighting the special attention that cyber security warranted. Attached to the letter was a document entitled, "*A credible benchmark of cyber security controls*" which, whilst not being prescriptive of the controls required by AIs, pointed to international standards and other guidance as well as certain areas that AIs may wish to consider in their cyber response.

Given the different motivations behind different cyber attacks, the HKMA said that different risk management measures were likely to be required; and that "*certain conventional risk management philosophy and controls practised by AIs might need to be adjusted or enhanced to cope with the risks*." The HKMA pinpointed four areas that cyber security risk management should cover:

- risk ownership and management accountability – which should cover not only the IT function but all relevant business lines – and which requires a strong security awareness culture within the institution;
- periodic evaluations and monitoring of cyber security controls – given the evolving nature of cyber attacks, the Board should request senior management to evaluate the adequacy of the AI's cyber security controls;
- industry collaboration and contingency planning – intelligence sharing, according to the HKMA, may help the AI and/or other institutions to get ready for possible cyber attacks and contingency planning should be ready to deal with attacks, even catastrophic ones (including e.g. simultaneous attacks to both production and backup IT systems); and
- regular independent assessment and tests – as well as having sufficient cyber security expertise and resources within the AI, the HKMA recommends that

[1] National Strategic Assessment of Serious and Organised Crime 2015 at page 5.
[2] Group Chairman's statement, HSBC, 3 August 2015.
[3] National Strategic Assessment of Serious and Organised Crime 2015 at page 4.

there should be regular independent assessment and possibly penetration tests.

The HKMA said that it would continue to review whether a common framework should be established to benchmark the adequacy of AIs' relevant controls.

This follows on from guidance issued by the Monetary Authority of Singapore on 24 August 2015 to Chief Executive Officers of all financial institutions on "Early Detection of Cyber Intrusions" which highlighted the increasingly sophisticated cyber attacks being perpetrated and the corresponding need for financial institutions to "*continually evolve and improve their ability to anticipate, withstand, detect, and respond to cyber attacks.*"

In the United States, the Securities and Exchange Commission ("**SEC**") is also targeting the financial services industry to underscore the importance of cybersecurity preparedness. In 2014, the SEC's Office of Compliance Inspections and Examinations ("**OCIE**") launched a sweep of the registered investment-adviser and broker-dealer community seeking information regarding the adequacy of registrants' cybersecurity compliance and controls "*to assess cybersecurity preparedness in the securities industry, including firms' ability to protect broker-dealer customer and investment adviser client information.*" In September 2015, OCIE issued a Risk Alert announcing the areas of focus for its second round of the sweep, emphasising the importance of the following issues:

- **Governance and Risk Assessment:** cybersecurity governance and risk assessment processes relative to the key areas of focus discussed below, and the extent to which those processes are reviewed on a regular basis. OCIE is also interested in the level of communication to and involvement of senior management and boards regarding cybersecurity issues.
- **Access Rights and Controls:** adequacy of controls to prevent unauthorized access to systems or information, such as multifactor authentication, and updating access rights based on personnel or system changes. This includes a review of controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation, and tiered access.
- **Data Loss Prevention:** adequacy and efficacy of the implementation of controls in the areas of patch management and system configuration, including monitoring of the network traffic, including potentially unauthorized data transfers via email attachments or uploads and the volume of data transferred outside the firm and verifying the authenticity of a customer request to transfer funds.
- **Vendor Management:** practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms, including how vendor relationships are considered as part of the firm's ongoing risk assessment process.
- **Training:** adequacy of training of employees and vendors, including with respect to the security and confidentiality of customer information and records. Focus on how training is tailored to specific job functions and designed to encourage responsible employee and vendor behaviour, as well as on how the incident response procedures are integrated into regular training programs.
- **Incident Response Plans:** existence of an incident response plan that includes assigned roles and an assessment of system vulnerabilities, including determining which firm data, assets, and services warrant the most protection to help prevent attacks from causing significant harm.

Also in September 2015, and in its first enforcement action in the cyber arena to date, the SEC imposed a fine of USD 75,000 against investment advisor RT Jones Capital Equities Management for having inadequate cyber security measures to safeguard customer information – and this, despite there being no evidence of financial harm to any individual whose data was compromised. It was found to have failed to have established cyber security policies and procedures reasonably designed to safeguard customer records and information as required under federal securities laws during the period 2009-2013. In July 2013 it fell victim to an attack, traced to China, that compromised the personally identifiable information ("**PII**") of approximately 100,000 individuals, including thousands of the firm's clients. RT Jones had failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cyber security incidents.

In announcing the fine, the Co-Chief of the SEC Enforcement Division's Asset Management Unit

underlined the importance of having proper procedures in place:

"*As we see an increasing barrage of cyber attacks on financial firms, it is important to enforce the safeguards rule even in cases like this when there is no apparent financial harm to clients […] Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs.*"[4]

Mitigating factors were that the firm promptly retained more than one cyber security consulting firm to confirm the attack and determine its scope and also provided notice of the breach to every individual whose PII may have been compromised and offered free identity theft monitoring through a third-party provider.

While the proposed EU Cyber Security Directive is awaited (which is likely to impose reporting obligations on "market operators", and significant sanctions for a failure to report significant incidents) a Standard & Poor's ("**S&P**") report published on 28 September 2015 named cyber security as a substantial emerging risk for the financial sector.[5] S&P viewed the risk to large banks as "*medium*" in view of the "*appropriate steps*" they have taken to mitigate known risks – amongst which are making it "*a high internal priority to install the proper measures to defend against attacks and upping the budget for cyberdefense*". Nevertheless the evolving nature of the threat meant that no cyber defence system was "*fail proof*". S&P set out the questions it was starting to ask bank management teams to ensure they are prepared for a cyber attack before an event actually occurs. These were as follows:

- *How do you measure the exposure and report on cyber-risk?*
- *Do you have a robust, well-documented program to monitor cyber-risks?*
- *How many times was the business the target of a high-level attack during the past year, and how far did it reach in the system?*
- *What areas does the bank feel are still vulnerable to attack?*
- *Does the bank have any third-party vendor oversight? If so, what kind and how much?*
- *What is the bank's readiness with respect to the NIST framework?*
- *How does the bank ward off phishing and diminish the likelihood of having data compromised from an internal breach?*
- *What's the internal phishing success rate?*
- *How long has it typically taken to detect a cyberattack?*
- *What containment procedures are in place if the bank is breached?*
- *Are emergency scenarios test-run?*
- *What software or other techniques are used to monitor attacks?*
- *What kind of expertise about cyberattacks exists on the board of directors?*
- *How much does the bank spend on cybersecurity, and what resources does it devote?*
- *What is the total tech budget this year versus last?*
- *What are the bank's capabilities versus peers, and how are they assessed?*
- *Is there information shared with peers?*
- *Does the bank have any insurance to compensate for a cyberattack?*

It concluded that:

"*A cyber attack is an emerging risk in all industries and could be particularly harmful to the banking industry if malicious attacks prove successful, given the sensitivity to confidence inherent in this industry. We believe banks and regulators have begun to take the initial steps to address the seriousness of the risk. However, we believe the risks of an attack, and the solutions, are only in the initial stages and will be a concern of risk managers and regulators for a long time to come*."

It comes as no surprise that S&P's questions largely mirror those which the HKMA suggests AIs should concentrate on. The focus on financial institutions also makes it more likely that financial institutions will come within the purview of the proposed EU Cyber Security Directive, particularly given the proposal's objectives, which include ensuring that public trust and confidence in network and information services (including online banking) is not undermined.

[4] http://www.sec.gov/news/pressrelease/2015-202.html
[5] "How Ready Are Banks For The Rapidly Rising Threat Of Cyberattack?" S&P Global Credit Portal, 28 September 2015.

Contacts

Carlos Conceicao
Partner, London

E: carlos.conceicao
@cliffordchance.com

Judith Seddon
Partner, London

E: judith.seddon
@cliffordchance.com

David Raskin
Partner, New York

E: david.raskin
@cliffordchance.com

Richard Sharpe
Senior Associate, Hong Kong

E: richard.sharpe
@cliffordchance.com

Jonathan Kewley
Senior Associate, London

E: jonathan.kewley
@cliffordchance.com

Chris Stott
Senior Associate, London

E: chris.stott
@cliffordchance.com