Three perspectives on cyber security for financial services

Financial services firms, when considering how best to prepare themselves against the threat of cyber crime, have more than one perspective that needs to be considered. Firstly, legal requirements, such as Europe's forthcoming Network and Information Security ('NIS') Directive, need to be considered. Information assurance standards like PCI DSS also need consideration. Finally, there is a need to look at the firm's own experience regarding cyber security and the experience of others in the industry. Hans Allnutt, Partner at DAC Beachcroft, Michael Fignon, Manager at Portcullis Computer Security Ltd, and Sandra Cole, UK & International Claims Manager at specialist insurer Beazley, discuss these three perspectives respectively in the context of financial services.

When considering what financial services organisations should be doing to protect themselves against cyber crime, an organisation might consider three perspectives:

(i) Legal: what do legislation, the judiciary and regulators require?

(ii) Information assurance: what security measures are required by standards such as ISO27001 and other industry frameworks?

(iii) Experience: what can the organisation learn from itself, peers and industry?

There is naturally a significant overlap between the three perspectives. Many requirements within the legal and information assurance frameworks follow common sense principles that can be drawn from experience.

However, any organisation would be foolish to focus on just one perspective when considering what it should be doing to protect itself against cyber crime. Each perspective has its flaws: the law is necessarily general in nature, leaving a heavy interpretive burden on an organisation; information assurance standards can be highly prescriptive and objective in nature, endangering an organisation if it prioritises compliance over prevention; and, reliance on experience alone may result in retrospection and a failure to keep up with the pace of technological change.

It is therefore important for organisations to consider the three perspectives. Contributions to this article have therefore been drawn from: a law firm specialising in the legal aspects of data protection and security, an IT and information security specialist, and an insurer that has experience of thousands of data breaches and cyber crime events that have occurred under its cyber insurance policies.

The legal perspective

The legal and regulatory regime that governs financial services' protection against cyber crime has focussed on financial and information risk: the risk of losing money (financial) or data (information) belonging to third parties and customers. As discussed below, the legal and regulatory regime is now widening to tackle how organisations deal with the operational risk from cyber crime.

Most financial services firms are well-versed in the applicable financial and information security laws, but not all firms are well-practised in their application. Laws are constantly being interpreted by regulators, which can make it difficult for firms to remain compliant.

For example, when it comes to the legal requirements of data security in relation to cyber crime, the law as stated is general and subjective. Principle 7 of the Data Protection Act 1998 ('DPA') requires organisations to have in place appropriate technical and organisational measures to prevent the loss of data. In recent years, however, the Information Commissioner's Office ('ICO') has interpreted what 'appropriate' measures are through its own guidance and sanctions.

In May 2014, the ICO issued a report entitled 'Protecting personal data in online services: learning from the mistakes of others.' The report listed eight areas of computer security issues that had frequently arisen in the ICO's investigations. The areas included patch update policies and password salting and hashing. By publishing this report, the ICO highlighted certain technical standards it expected organisations to meet, thereby interpreting the meaning of Principle 7.

The ICO has also used sanctions to publicise good practice. For example when the ICO fined the financially regulated company Staysure £175,000 in March 2015, it expressly referred to the firm's contravention of the Payment Card Industry Data Security Standard ('PCI DSS') by storing unencrypted CVV numbers. In doing so, the ICO sent a clear signal that compliance with Principle 7 includes compliance with PCI DSS.

Whilst it can be challenging, financial services organisations must keep abreast of the ICO's guidance and sanctions in order to ensure that they are adopting best practice in the ICO's eyes. It is no coincidence that the ICO's approach to existing data protection law has similarities with the forthcoming European General Data Protection Regulation ('GDPR'). Those organisations that

follow best practice now will be very well placed when the GDPR comes into effect.

It is important to remember, however, that the DPA and ICO's purpose is the protection of a Data Subject's 'Personal Data' (as defined in the DPA), which is a small fraction of the information targeted by cyber criminals. Compliance with the DPA's requirements on data security alone may leave an organisation exposed to cyber crime that is targeted at assets other than personal data.

The Financial Conduct Authority ('FCA') and Prudential Regulation Authority ('PRA') regulate information and systems that are much wider than just personal data. Like the ICO, the FCA has issued its own guidance[1] in the past but it has not been as detailed as one might have expected. Nevertheless, regulated firms face unlimited fines if they fail to protect adequately against cyber crime.

Recently, both the PRA and FCA have expressed specific interest in cyber risk. On 10 August 2015, the PRA wrote to a number of major insurers with a 28 page questionnaire to examine firms' cyber security and resilience to cyber attacks[2]. The PRA also included questions on behalf of the FCA relating to information exposed to cyber crime.

The PRA's inclusion of cyber 'resilience' marks a trend by regulators to look at operational risk to cyber crime (as opposed to information risk) and the threat it poses to critical national infrastructure. Any financial services firm might wish to consider the questionnaire as an indication of the future of the financial regulators' scrutiny.

The PRA's recent interest in operational cyber risk chimes with Europe's anticipated Network and Information Security ('NIS') Directive, which seeks to impose legal obligations on 'market operators' to secure not only the information that they hold but the networks on which they rely.

Whilst it can be challenging, financial services organisations must keep abreast of the ICO's guidance and sanctions in order to ensure that they are adopting best practice in the ICO's eyes

Whilst the NIS Directive is still proceeding through the legislative process, the UK has already taken steps to implement certain measures including the establishment of Cyber Emergency Response Teams ('CERT') and a platform for sharing cyber threats and vulnerabilities: the Cyber Information Sharing Partnership ('CISP'). Whilst the NIS Directive has yet to be enacted, as with the GDPR regime, financial services firms should engage now with the CERT and CISP so as to be well prepared for any legal change.

In short, financial services firms should monitor regulatory guidance closely in order to ensure that they have adequate measures in place to protect the information they hold from cyber crime. Those sufficiently influential financial institutions should also focus on protecting their operational functions from cyber crime so as to be ready for the NIS Directive and PRA scrutiny if applicable.

Information assurance perspective

Information assurance through security testing has long been a cornerstone of good practice within the financial services sector. However, that good practice has been largely led by external and internal audit functions requiring third party assurance and the firm's own view of the appropriate level of testing and assurance that is required. The matter of which partners delivered these services was also largely at the discretion of the firm, with no standards initially, relying on word of mouth and past experience rather than a simple benchmark standard.

As time went on, acceptable baselines of what should be done from both a test and assurance perspective evolved, with BS7799/ISO27001, PCI DSS[3] (often followed as a minimum baseline even if full certification was not required) and open source methodologies such as OSSTMM[4] and OWASP[5] being required to allow some form of benchmarking and repeatability. Financial services, like most other non-government sectors then adopted CESG's CHECK standard[6] as the minimum level of skill required by a security testing organisation. This undoubtedly raised the level of expertise of those security professionals working on behalf of financial services and continued an evolution of testing levels that were responding to the growing sophistication of threat actors - from script kiddies and trophy hunters to organised crime and nation states.

It is the evolution of the threat actor that has driven the latest developments of ever increasing levels of depth and sophistication of information assurance and security testing. These latest standards are an indication of the perpetual arms race between the cyber criminal and cyber defender and financial services should be wary of falling too far behind.

In May 2014 the financial services sector took a further step forward with the introduction of the CBEST standard[7] and its adoption by the most systemically important financial institutions to the UK economy. The standard, created by the Bank of England with support from certain IT security companies, takes an approach designed to test and measure a firm's maturity to real world cyber attacks. The CBEST approach uses 'Red Teams' that are intelligence-led, open-scope, risk-managed and realistic to attack an organisation's

systems. The Red Team engagements exercise a firm's people, technologies and processes.

The CBEST standard was launched following an initial roll-out to certain financial institutions. Certain themes may be drawn from the initial roll-out:

(i) CBEST is designed to assess the maturity and ability of a firm to protect those assets and information deemed to be systemically important. Historically such systems were excluded from a traditional assurance assessment based on their importance but that approach left organisations vulnerable to cyber criminals.

(ii) It is not a system-by-system audit but an evidenced-based review of how an organisation's systems are vulnerable to attack using realistic attack patterns created from an extensive threat intelligence gathering process.

(iii) CBEST is not seen as a pass or fail test of technical controls. Firms will already understand how quickly they can respond to an outage on the trading floor or after a terrorist alert/attack and CBEST promotes understanding of the equivalent detection and response process for a successful cyber attack. Through Red Team feedback and post-attack engagement, an organisation stands to learn much more from the experience than previous security reviews.

(iv) CBEST should drive organisational awareness of security and feed a cycle of improvement and development with measurable key performance indicators.

The CBEST standard will inevitably have its limitations and critics, but its success over many other assurance systems lies in assessing and taking risks, not simply assessing the potential risk.

The Financial Policy Committee has, through the Financial Stability Report[8], confirmed that CBEST is here to stay. As CBEST develops, it is expected that the standard will be rolled out to other banks, insurers and other financial institutions. If not already subject to it, financial services organisations should certainly consider the CBEST standard when protecting themselves against cyber crime.

The experience perspective

It is often said that a price cannot be put on experience and that is particularly true in the case of cyber incidents and data breaches. One can slavishly follow legal requirements and assurance but it is simply not possible to be risk free when it comes to cyber crime.

Organisations need to ensure that they not only employ the technical measures referred to above but also stress test how they will respond when a breach does happen. A data breach isn't always a disaster but mishandling it is.

How an organisation responds to an incident has a direct impact on a number of critical issues: the relevant regulator's response to the incident; shareholder reaction; customer/client confidence and overall market reputation. Companies need to have a well-structured incident response plan that has been tested in a simulated breach exercise: there is no point having a plan if the organisation does not have experience of practising it in a crisis.

Organisations should ensure that there is a designated incident response team, including key stakeholders such as the company's CISO, Head of IT and Director of Communications as a minimum, but they also need to plan for absences and the fact that incidents often occur outside usual working routine. This means having out-of-office contact information for the incident response team and designated back-up personnel in case the primary team is unavailable. Finally, but perhaps most importantly, companies need to engage experienced service providers who know how to respond to a breach. This is most easily achieved through specialised insurance policies that have designated service provider panels. In the midst of a crisis, a company needs immediate access to IT security consultants, lawyers, PR representatives and notification agents who have guided companies through a breach time and time again. This will become increasingly important after the introduction of the EU GDPR. A current draft requires companies to provide notice of a breach to regulators in as little as 24 hours.

Hans Allnutt Partner
DAC Beachcroft, London
Michael Fignon Manager
Portcullis Computer Security Ltd
Sandra Cole UK & International Claims Manager
Beazley
hallnutt@dacbeachcroft.com
MJF@portcullis-security.com
sandra.cole@beazley.com

1. http://www.fca.org.uk/your-fca/documents/fsa-data-security-factsheet
2. http://www.bankofengland.co.uk/pra/Documents/about/insuranceletter100815.pdf
3. Payment Card Industry Data Security Standard.
4. Open Source Security Testing Methodology Manual.
5. Open Web Application Security Project.
6. CHECK standard definition (launched in 1999).
7. CBEST is not an abbreviation.
8. http://www.bankofengland.co.uk/publications/Pages/fsr/2015/jul.aspx