Policy briefing

CII

June 2016

Cyber and the City

A report on cyber risk, 'Cyber and The City', published by TheCityUK and Marsh argues that firms across the industry need to take urgent action on cyber risk to ensure the UK continues to be a secure base for the world's leading financial centre.

Cyber attack is a major new source of systemic risk, as much as market or credit risk. This briefing provides a headline summary of the key aspects of the report which sets out to provide practical steps that firms now take to make themselves and the system safe. The full report can be viewed at: https://www.thecityuk.com/assets/2016/Reports-PDF/Cyber-and-the-city.pdf

Following interviews with a diverse range of City institutions and authorities, analysis on the state of play in cyber risk management and the responses to other risks with the potential for extreme impact, 'Cyber and The City' provides a series of recommendations for financial firms in order to improve their cyber resilience:

Key recommendations for firms
A. Make cyber a standing item on the Board or risk committee agenda;
B. Ensure cyber risk is a part of strategy, investment cases, acquisition and appraisals;
C. Have a broad based team inputting to how cyber risk is managed;
D. Monitor cyber readiness against the ten-point cyber checklist:

Ten-point cyber checklist for boards to consider

- The main cyber threats for the firm have been identified and sized
- There is an action plan to improve defence and response to these threats
- Data assets are mapped and actions to secure them are clear
- Supplier, customer, employee and infrastructure cyber risks are being managed
- The plan includes independent testing against a recognised framework
- The risk appetite statement provides control of cyber concentration risk
- Insurance has been tested for its cyber coverage and counter-party risk
- Preparations have been made to respond to a successful attack
- Cyber insights are being shared and gained from peers
- Regular Board review material is provided to confirm status on the above

Definition

> "Technology risk can be defined as 'any risk of financial loss, disruption or damage to reputation from some form of failure of information technology systems'. Cyber risk relates to attacks which are more likely to be disruptive given their intent to harm."

Cyber attacks

Cyber attacks can be broadly categorised into three areas:

Category	Description
Fraud	Covers the majority of cyber incidents today. This includes attempts at extortion, identity theft and other crimes targeting individual customers or employees. The motive is almost always financial.
Firm take-down	Reflects the more ambitious goals of large-scale data theft, system disruption and damage, in which a particular firm is targeted for personal or political reasons. Several such cases in the UK and around the world have made the headlines.
System failure	An incident affecting multiple institutions, for example a concerted attack on several firms, the failure of the payments system or a failure of the national infrastructure that the financial sector relies on such as the power grid. System failures receive a lot of attention given the scale of the consequences – for instance the cost to the Greek economy of the planned shutdown of its banks for three weeks in 2015 is estimated by the IMF to be 7% of Greek GDP. Responsibility lies with industry bodies and supervisors to make sure that critical infrastructure and pathways are well protected and that communication, contingency and rapid recovery plans are in place.

Characterising the threat of cyber attacks for individual firms

The financial sector is a major target for cyber crime

Financial firms are a major target and vulnerable to attack as they are often large, complex organisations with high concentrations of sensitive data and financial assets, led by high profile names and brands. The wider economy has a critical dependence on these same institutions as vehicles for data storage and transmission.

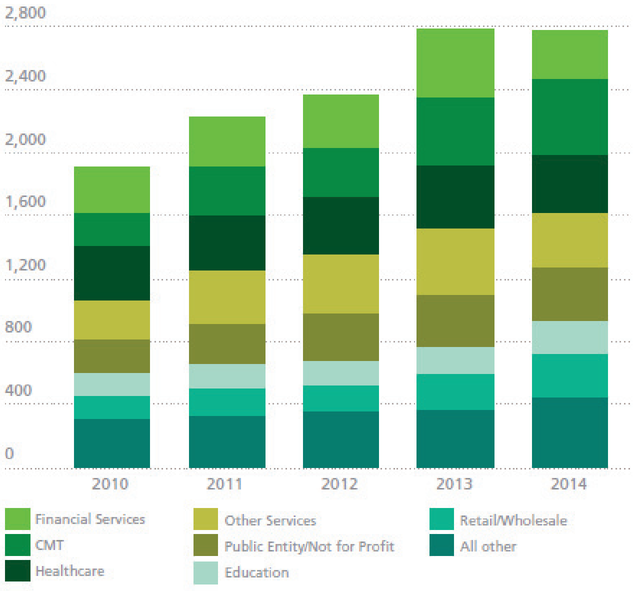
Despite the majority of attacks at present relating to fraud, cyber incidents are one of the few risks with the potential to bring firms down.

Cyber crime is a risk NOW, and not at some stage in the future

Cyber crime has been described by John McFarlane, Chairman of TheCityUK as a ‘real and present danger’ to the financial and related professional services sector. There is a perception held by some within the industry that cyber crime is a risk that exists at some stage in the future. On the contrary, cyber incidents are increasing in frequency and sophistication as more assets go online and as the cost and expertise needed to launch an attack reduces. According to the report, the number of reported cyber incidents worldwide is expected to grow from 14 billion in 2014 to 24 billion by 2019.

Figure 3

Cyber incidents per industry



Source: Advisen

Cyber crime is not being treated with the seriousness it merits

The threat of cyber crime is not being treated seriously enough across the financial and related professional services sector. In a recent survey of large UK firms, only 30% have cyber in their top 10 risks, 30% stated they have a comprehensive cyber incident response plan, and only 35% have broader functions engaged in it.

Parallels with the financial crisis

There are considerable parallels to the credit crisis. In 2007, UK banks survived due to a financial injection as a remedy of last resort. There would be no such fast acting remedy for a large scale cyber attack where a permanent loss of data may prove to be an irrecoverable event. In addition, when the crisis hit, the banks that were best placed to respond were those where credit-risk was shared across leadership and front-line staff. The risks posed and opportunities afforded by technology can no longer be handled exclusively by specialists, and should be addressed by business leaders in a wide range of contexts such as strategy, acquisitions and appraisals to be able to respond in time to prevent a problem turning into a crisis.

People and processes matter as much as technology

Boards should hold management and not their IT departments responsible for cyber risks. According to the report, only 20% of firms surveyed have broader functions engaged in the issue, suggesting that there is still a tendency for businesses to assume that the best defence against a large scale cyber attack is a strong technology perimeter, or worse - that cyber is dismissed as the domain of the IT department. As 95% of attacks succeed as a result of human error, the major weakness for many organisations are employees that sit inside this technology perimeter. One study quoted by the report found that 73% of companies have been affected by internal information security incidents and that the largest cause of confidential data losses are employees (42%).

It is critical that boards shift the commonly held perception of cyber as a technology and security issue to one that considers it a fundamental enterprise risk to the firm where culture and process are equally as important.

Leaders must plan for a breach, and not just rely on avoidance

According to the report however, only 30% of risk managers in large financial firms interviewed by Marsh for its annual cyber survey in 2015 had a comprehensive cyber incidence response plan – which suggests that leaders are relying on avoidance, rather than putting strategies in place to ensure that the firm is in a position to react in the event of an attack.

The very different experience of firms managing through such breaches demonstrates how good preparation can prevent a problem from turning into a crisis.

Building the UK's cyber security knowledge, skills and capability

In his speech to GCHQ on cyber security in November 2015, George Osborne set out a plan to create a secure environment for UK cyber activity. As part of his announcement of a doubling of related investment to £1.9bn over five years, the Chancellor pledged to improve cyber skills to close 2020's 1.5 million security workforce shortage, identify talent for training and a career in cyber, introduce more apprenticeships and improve extracurricular education. However, Government initiatives will need to be supplemented by the work of individual firms, such as the provision of apprenticeships and work placements for trainees to acquire the hands-on experience they need to move into cyber security roles.

As well as ensuring there are enough cyber security experts to perform technical roles, professionals in various other roles within Financial Services should receive training that equips them with a basic understanding of cyber security.

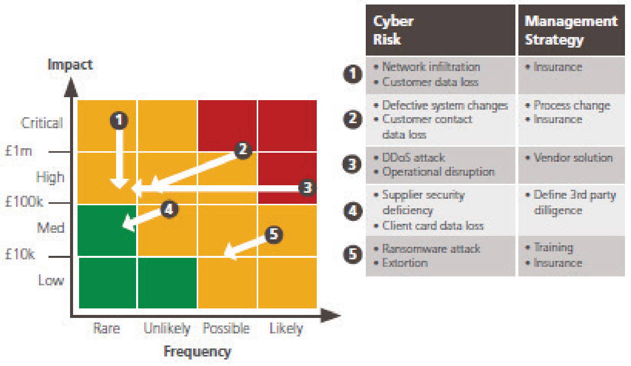
Board Cyber Check-List in more detail

Category	Description
1. The Main cyber threats for the firms have been identified and sized	Firms need to be able to quantify the likely impact of potential risks. As the number of historic cases increase, learning can be drawn from losses with similar consequences. Insurance cover is an example of where the need for remedies has been quantified.
2. There is an action plan to improve defence and response to these threats	This is considered the critical outcome. The focus for board attention should be the actions taken to improve defence and reduce impact. This will help cyber resilience in the absence of helpful KPIs in this area.
3. Data assets are mapped and actions to secure them are clear	Data is often the focus for attackers, and yet few CEOs have a good grasp of what data they hold, how it is used, how secure it is, and who has access to it. Data needs to be understood in the same way as other assets material to the financial well-being of the firm.
4. Supplier, customer, employee and infrastructure cyber risks are being managed	Firms must ensure that standards for cyber security, such as Cyber Essentials accreditation, are being imposed on the supply chain. The relationship between the firm and the customer is dependent upon the provision of secure transaction interfaces on the one hand, and education of the consumer on the other. As cyber security is likely to become an important predictor of firm default, it is recommended that cyber security is added to the core questions such as the bank's credit decision set. Where possible, individual firms need to plan for failure and recovery. Collectively, industry authorities need to ensure that critical infrastructure is being protected and that co-ordinated rapid recovery from attack is possible.
5. The plan includes independent testing against a recognised framework	There are existing frameworks that widen the focus from solely technology to include other sources of risk and defence. The NIST framework already adopted by large banks can be used as a guide to ensure that actions being taken by firms are broad enough to cover the range of risk factors.
6. The risk appetite statement provides control of cyber concentration risk	Risk appetite statements have traditionally restricted the size of a single client or the amount of business conducted in a particular industry or country. However, cyber risk is defined more by the underlying service and technology providers that clients use and the firms they trade with. Existing tools can map these risks and attach them to the balance sheet.
7. Insurance has been tested for its cyber coverage and counter-party risk	Insured firms should review how their policies would respond to scenarios of greatest concern to the firm, and take corrective action in partnership with the insurers if the cover is inadequate for the needs of the firm in the event of an attack.
8. Preparations have been made to respond to a successful attack	It is the responsibility of the board to conduct dry-runs, service recovery plans, communication training and stakeholder management to ensure that the organisation is prepared for an attack. Effective communication has proved crucial to retaining customer confidence in recent cases.
9. Cyber insights are being shared and gained from peers	The board should ensure that the organisation encourages information sharing on cyber risk to extend best practice, and so that there is an awareness of how the firm compares to others.
10. Regular Board review material is provided to confirm status on the above	Reports to the board must be clear, actionable and concentrate on the measures that will make the firm safer (see the diagram below for an example of a board report focussing on the risks and actions taken to mitigate them). Cyber then automatically becomes the responsibility of a non-technical board.

Example Cyber board reporting

Cyber Risk Heat Map

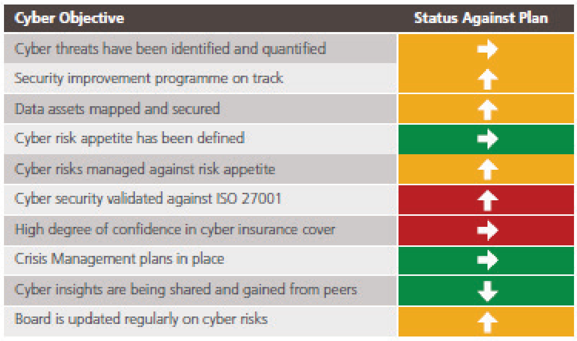
Risk management strategies in place for key risks



	Cyber Risk	Management Strategy
1	• Network infiltration • Customer data loss	• Insurance
2	• Defective system changes • Customer contact data loss	• Process change • Insurance
3	• DDoS attack • Operational disruption	• Vendor solution
4	• Supplier security deficiency • Client card data loss	• Define 3rd party diligence
5	• Ransomware attack • Extortion	• Training • Insurance

Progress against Cyber Objectives

Progress being made all major cyber objectives



Cyber Objective	Status Against Plan
Cyber threats have been identified and quantified	🟧 →
Security improvement programme on track	🟧 ↑
Data assets mapped and secured	🟧 ↑
Cyber risk appetite has been defined	🟩 →
Cyber risks managed against risk appetite	🟧 ↑
Cyber security validated against ISO 27001	🟥 ↑
High degree of confidence in cyber insurance cover	🟥 →
Crisis Management plans in place	🟩 →
Cyber insights are being shared and gained from peers	🟩 ↓
Board is updated regularly on cyber risks	🟧 ↑

Conclusion

The threat of cyber attack itself is broad in nature – from the shift in traditional fraud to cyber channels that constitute the majority of attacks today, to the much rarer sophisticated attempts to destabilise whole firms and wider economy. This threat should not be dismissed given the fragility of customer trust in the integrity of the financial services they rely upon, and the attractiveness of financial firms to attackers.

In the assessment of the report authors, the trajectory of cyber risk will follow the same path as that of credit risk preceding the financial crisis. The most resilient to attack will be those within the financial and professional services sector that have a shared appreciation of cyber risk across leadership and front-line staff. The lead that Government has taken on cyber security up until now is an indication of the potentially systemic nature of this risk - but it is now the responsibility of boards to challenge management on the treatment of cyber risk through the 10 point checklist proposed in the report. To a certain extent, cyber safety is about displacement. If one firm is harder to attack, it is likely that the attacker will go elsewhere. The same can be extrapolated to a sector, a city and a country.

Links to other useful materials

‘Making Sense of Cyber Insurance: A Guide for SMEs’ produced by the ABI (May 2016):

https://www.abi.org.uk/~/media/Files/Documents/Publications/Public/2016/Cyber%20Insurance/Making%20Sense%20of%20Cyber%20Insurance%20A%20Guide%20for%20SMEs.pdf

‘Cyber Essentials’ launched by the Government (April 2014) to guide businesses in protecting themselves against cyber threats. The Cabinet Office estimates that 80% of breaches would not occur if the Cyber Essentials advice was taken on board and implemented. For further information see:

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Lawrence Finkle
CII Group Policy & Public Affairs
June 2016

The CII is the world’s leading professional organisation for insurance and financial services, with over 120,000 members in 150 countries. We are committed to maintaining the highest standards of technical expertise and ethical conduct in the profession through research, education and accreditation. In 2012 we are celebrating our Centenary as a Chartered body.

For more information on the CII and its policy and public affairs function, including examples of the range of issues in financial services and insurance that we cover, please see: www.cii.co.uk/policy.

Please do not hesitate to contact us: Lawrence Finkle, tel 020 7417 3586; email address Lawrence.finkle@cii.co.uk