Cyril Roux: Cybersecurity and cyber risk

Address by Mr Cyril Roux, Deputy Governor (Financial Regulation) of the Central Bank of Ireland, to the Society of Actuaries in Ireland Risk Management Conference "Cybersecurity and cyber risk", Dublin, 30 September 2015.

* * *

Many thanks to the Society of Actuaries in Ireland for inviting me to address such a distinguished audience of risk and insurance professionals. The conference agenda covers a number of substantial topics, and I am pleased to speak to you about one that is rapidly moving up the Central Bank's supervisory agenda: cybersecurity and cyber risk.

Raising awareness of cybersecurity risk

We know a lot about the financial risks such as interest rate, liquidity and credit risk that contributed to the crisis from which we are emerging. We also know that the next crisis is unlikely to be the same as the last one. That's why we monitor other categories of risks, such as operational risks, faced by supervised firms and by the financial system as a whole. Operational risks come in many guises, and we pay in particular close attention to IT risks.

Financial firms are evermore dependent on their information technology. The share of financial services provided online to their customers continues to grow, and the inner workings of financial firms, as well as their relationships with their vendors and suppliers, are wedded to their information systems. Regulated firms are thus exposed to large scale IT risks on a number of fronts. When part of their IT systems fail, their business is impaired, and, in time, so are their reputation, their finances, and ultimately their survival. Regulated firms perform critical economic functions on behalf of the general public and businesses. Their logical resilience and safety is, if anything, even more important than the security of their business premises. Accordingly, the Central Bank expects regulated firms to have robust governance and policies frameworks around their data and information systems, including their outsourced functions. Regulated firms need to identify, monitor and mitigate their IT risks.

Within that universe of IT risks, I wish to focus today on cyber risk, a growing risk that has serious implications for prudential supervision, consumer protection and financial stability.

The Irish insurance industry appears to share the same view. Cyber risk is at the top of your firms emerging risk concerns, according to the 2015 PwC Insurance Survey. However, not all Irish firms regulated by the Central Bank assess their exposure to cyber risk properly, and not all mitigate risk sufficiently. So today I wish to heighten awareness on the need for firms to be prepared for cyber-attacks and to build resilience to a successful attack. I will also speak about the steps the Central Bank is taking to supervise the way this risk is addressed in regulated firms.

Sources of cybersecurity incidents

Cybersecurity incidents can come from many different sources, but the most common are:

- ***Criminal organisations*** seeking financial gain.
- ***Employees:*** disgruntled employees seeking revenge or motivated by financial gain, or accidental breaches due to human error, failure to follow internal procedures or ineffective internal procedures.
- ***Outsourcing:*** exposure due to control failures in service providers who have access to the firms' systems.

- ***Corporate espionage:*** competitor firms seeking to steal intellectual property or trade secrets.
- ***Hostile nation-states:*** seeking to undermine a rival state's economy.
- ***Ideological groups:*** seeking to damage the financial system.

Even though most firms are potentially at risk, financial firms are particularly targeted because of the criticality of their economic function and the nature and value of their assets. Regulated firms hold financial assets of their clients, in the form of deposits, securities, life insurance contracts and pension accounts, among others. They also hold a treasure trove of personal data, credit card numbers, social security numbers, medical records, and the like. Client assets and personal data are prime targets of cybercrime. To give a recent example, this year, the personal data of 80 million customers of the second largest health insurer in the US was stolen.

Worrying trends in cybercrime

Cybercrime encompasses some recently outlawed activities such as data theft, hacking and disruption of IT services. It also encompasses traditional crime, such as bank heists, fraud, forgery, theft, industrial espionage and ransom. According to Europol the annual financial losses due to online payment fraud now surpass those of payment fraud with physical cards.

Some organised cybercrime groups operate with multiple divisions and specialists in key areas such as management, distribution, hacking, coding, server administration and money laundering. Such cybercrime groups can conduct cyber-attacks of great scale and sophistication, such as advanced persistent threats, which are targeted attacks on specific firms, designed to evade detection and to last for months or even years. Typically it is only when significant damage has already been done that the firm will realize anything is wrong. A recent example is the Carbanak attack, which targeted the money processing services, ATMs and bank accounts of over 100 banks worldwide over a period of two years and may have led to up to $1bn being stolen.

The risk/reward trade-off for cybercrime is very attractive. Cybercriminals know there is a low likelihood of being detected, caught or prosecuted and many attack strategies can be executed cheaply. This has led to a substantial broadening of the attacker base. Due to the proliferation of the cybercrime-as-a-service business model, the cybercrime industry is no longer just the domain of highly skilled IT people. Now a relatively low-skilled cybercriminal can cause significant damage.

Irrespective of size, cybercriminals can use a variety of approaches, some highly technological, such as exploiting previously undiscovered defects in computer software, some relying on human error, such as deception of employees or spear-phishing. It is this human element to which I now turn.

Employee risk: Insider-Threat and Human Error

People can be the most vulnerable and unpredictable part of a firm's tech infrastructure.

There are two main types of employee driven cybersecurity risk: Insider-Threat and Human Error. Disgruntled current and ex-employees can be a significant source of security risk due to their knowledge of firms' systems and data assets. They may have a strong personal motivation to damage the firm or hold it to ransom. While security or IT staff might be the obvious cases, other examples include staff with access to valuable intellectual property, senior management or sales staff with client data. Financial firms have long managed the risk of employee fraud through separation of duties, two-person authorisation and access limitations. Similar controls around high-value data and systems are needed.

For instance, firms have to ensure that access rights are reconfigured when an employee leaves or moves internally. Firms should ensure that employees have at any moment only the access rights they need to carry on their job.

Accidental and/or non-malicious employee security breaches accounted for around 25% of data breaches in 2013 and 2014. Often the breach occurs for well-intentioned reasons such as an employee wanting to work on something from home and sending a document to their personal email or copying data onto a USB drive, or when employees use external systems or software. If an IT system cannot give employees what they need to do their job, they tend to seek out their own solutions e.g. use of personal equipment/devices. This introduces security risks, as such shadow IT operates outside of the firm's protected systems.

Outsourcing risk

Let me now turn to outsourcing. Financial services firms will often outsource critical functions, for example payment processing, IT, clearing and settlement, website management etc. This means that a firm's IT security depends in part on the quality of IT security of its third party service providers. Providers typically have access to sensitive data and/or some of the firm's systems. If a provider is hacked or compromised with malicious software this opens up the likelihood that the firm's data or systems will also be exposed.

Many large high profile firms have been successfully attacked this way. A prominent example is the US retailer Target in 2013, where 40 million customer debit and credit card records were stolen as well as personally identifiable information on 70 million customers, through IT security lapses of its heating and air conditioning vendor.

Firms should seek to mitigate this risk by carefully selecting and managing service providers and by incorporating cybersecurity and data protection requirements into third party contracts from the outset. However, many firms do not perform due diligence on the security infrastructure of their vendors nor require them to meet minimum security standards.

Cyber insurance market

Cyber risk creates insurance opportunities. Although the market is currently quite small in terms of premium size (estimated at $2 billion), it is a growing one.[1]

Several insurance companies have launched corporate policies and have accompanied their offers of contractual cover with a suite of services, such as assessment of exposure, advice for managing and mitigating the risks, and loss management. In so doing, the insurance industry performs a valuable service, similar to the traditional management of fire risks of business premises.

However, there are significant challenges for this new insurance offering. Underwriting cannot rely on long-run loss and exposure data for pricing, measuring profitability, capital allocation and risk management. In any case, the nature and scale of cyber risk is evolving so rapidly that it is questionable whether whatever historic loss data there is, could be useful for forecasting future losses. New classes of risk are always a challenge to underwrite.

Furthermore, as we have seen on the effect of the floods in Thailand on business interruption policies, there are also challenges in measuring risk accumulation due to the length of supply chains. A cyber-attack can have unexpected knock-on effects within the insured's business which could trigger several independent policies. Other issues include the potential that there may be unintended and unidentified exposure overlap between standard business policies and stand-alone cyber policies and issues around the definitions and scope of cover.

---

[1] Marsh Risk Management Research: Benchmarking Trends March 2015.

Potential systemic risks need to be better understood

The next big financial shock will arise from a succession of successful cyber-attacks on financial services firms. This is the prediction of Greg Medcraft, Chairman of the International Organisation of Securities Commissions (IOSCO). In 2014, 33% of financial industry survey respondents ranked cyber-attacks as the number one systemic risk to the broader economy.

Such concerns are a welcome development as it means the risk is being considered before it materializes. The complex interconnectedness of financial institutions and markets means that the financial system is only as strong as the weakest link in the chain. This is why the presence of cyber security risks in one firm could potentially give rise to systemic failure. So far we have not had a cyber-event that led to systemic problems but it may be only a matter of time. A seemingly manageable security incident at a single firm could cascade quickly to the broader financial sector. Consider for example a simultaneous, coordinated attack on several Global Systemically Important Banks or critical financial infrastructure providers (such as a stock exchange or a central counterparty clearing house). This could have a yet unknown domino-effect on those firms' counterparties which could have the potential to lead to a systemic shock in the financial system.[2]

Given the complex, rapidly changing and borderless nature of cybercrime, no single firm or regulator can successfully tackle the risk alone. Cybercrime's international nature will require a collaborative response from governments, regulators and industry. Let me tell you what we are doing at the Central Bank about it.

Recent central bank initiatives to address cybersecurity

While information security has been on the Central Bank's agenda for quite some time, this year we have intensified our efforts on cybersecurity through a number of initiatives:

- Cyber risk is being considered in the FLAOR/ORSA reviews of insurance firms and as part of the supervisory engagement with firms. This scrutiny will evolve in a Solvency II context in 2016;
- We established a banking IT risk inspection team with resources recruited in early 2015. This team is undertaking inspections of IT risk in banks which will include cybersecurity risk assessments;
- The Single Supervisory Mechanism (SSM) issued questionnaires to banks to assess the management of cybersecurity risk and we are in the process of reviewing the Irish banks' submissions. In addition, as part of our auditor assurance work, we are looking at cyber risk governance in banks.
- We performed a themed review of the management of operational risk around cybersecurity within the investment firm and fund services industry. The review examined firms' control environments (including policies and procedures) designed to detect and prevent cybersecurity breaches as well as board oversight of cybersecurity. Our findings were communicated to the funds industry last week in a letter to firms. Included in the letter were examples of best practice that firms should consider.

The Central Bank is at an early stage of its work to address cyber risk. Our work will continue to evolve. This risk cuts across many Central Bank divisions including Insurance, Banking, Markets, Anti-Money Laundering, Financial Stability and Consumer Protection. Cybersecurity has serious implications for prudential, systemic and consumer risks, and thus an integrated

---

[2] IOSCO suggest a number of plausible cyber-attack scenarios which could have systemic implications in the paper: ''Cybercrime, securities markets and systemic risk', July, 2013, IOSCO & WFE Joint Staff Working Paper.

supervisory approach is essential. We are bringing together a senior cross-directorate cyber group so that we can have a holistic view of this risk which will inform our overall supervisory strategy.

Central Bank expectations of firms

I would like to share with you our current expectations on the management of cyber risk in regulated firms.

We do acknowledge that an effective cybersecurity programme should be reflective of the size, business model, nature and sensitivity of the firm's critical assets. That being said, there are a number of common themes that are pertinent to most or all firms.

- ***The Board should have a good understanding of the main risks:*** The Board needs to have sufficient knowledge and understanding of cybersecurity risk to be able to effectively challenge senior management on the security strategy. Boards should understand what the firm's critical assets are, how they are shared with external parties and the potential loss or damage to the firm in the event of a data or systems breach.
- ***Cybersecurity risk should be considered within the firm's overall risk appetite and business strategy***. This is not simply an IT problem.
- ***Perform risk assessments and intrusion tests:*** Firms should perform cybersecurity risk assessments on a regular basis. Such assessments should include identification of critical assets and commissioned intrusion tests. They need to be performed frequently enough to capture changes in new systems, new product offerings or new security threats.
- ***Prepare for the successful attacks***: build resilience through distributed architecture and multiple lines of defense and prepare to mitigate the impact on customers.
- ***Manage vendor risk:*** Firms should perform cybersecurity due diligence on prospective and existing outsourced service providers and incorporate cybersecurity and data protection provisions into outsourcing agreements.
- ***Gather information and follow best practices:*** Firms should follow and apply industry standards to their cybersecurity risk management frameworks as appropriate for the scale and nature of their business and participate in industry information sharing groups.
- ***Educate staff:*** Firms should provide regular security awareness training to all staff. Firms should address the "human factor" by cultivating an environment of security awareness throughout the firm and providing regular security awareness training to all staff. Without good security awareness training, each staff member becomes a weak link from a security perspective.
- ***Have robust IT policies, procedures and technical controls are put in place:*** That includes incident reporting and response plans, recovery and business continuity plans, patch management, and employee access rights.
- ***Consider buying cyber-insurance:*** Firms may consider evaluating the possibility of using cyber-insurance as a partial risk mitigation strategy.

Looking ahead

The Central Bank intends to sharpen its focus on the cybersecurity threat. We are committed to building up our knowledge and expertise. In line with the rapidly evolving nature of cyber risk, the Central Bank's regulatory expectations will be evolving.

Supervisors have an important role in fostering robust oversight of cybersecurity risks, even though the onus is on the firms to manage these risks. Our approach needs to be agile. We will adopt a multi-pronged approach where we use the range of tools at our disposal, including thematic reviews, inspections of supervised firms, independent reviews by the internal audit team or external third parties, issuing guidance and working to raise awareness and educate industry and consumers on cybersecurity issues.

A single regulator cannot successfully tackle this threat alone. The threat does not stop at national borders. There needs to be a united and coordinated approach among regulators and to this end, we are working closely with the ECB/SSM as well as international counterparts, the EBA and regulatory bodies to achieve this.

Cyber risk will be a permanent feature of business and regulatory life. We will actively engage with industry to ensure the regulated firms address this risk. We intend to publish, in the coming months, an initial paper on cybersecurity risk. In this paper, we will share our current thinking and our supervisory experience of this risk, and lay out our expectations towards regulated firms.

Thank you for your attention. I wish you an interesting and fruitful conference.