CLIFFORD
CHANCE

>THOUGHT
LEADERSHIP>

CYBER SECURITY
LEGAL AND REGULATORY CONSIDERATIONS

CYBER SECURITY AND INFORMATION MANAGEMENT – LEGAL AND REGULATORY CONSIDERATIONS

Banks and other financial institutions are acutely aware of their vulnerability to cyber attacks and security lapses. These attacks can be directly damaging to their businesses and reputation, but can also raise legal and regulatory issues that need to be anticipated and addressed. Increasingly, banks are subject to express obligations to keep data secure and to inform affected individuals and regulators in the case of a breach. Here, Clifford Chance experts consider these issues and look at how banks can both defend against, and respond to, cyber security lapses.

Although many of us hold the view that cyber attacks and security breaches are things that happen to others, most financial institutions are constantly under some sort of cyber attack. That fact is driving an expectation among regulators that this topic should be front of mind and should be the subject of frequent board-level discussion. Carlos Conceicao, a contentious regulatory partner at Clifford Chance in London, says: "Regulators now have clear expectations around who should be considering these risks, and where the responsibility should lie for addressing them."

One of the biggest challenges that financial institutions face when dealing with cyber security is the impact of making systems more accessible to customers. Institutions are under commercial and governmental pressure to increase the use of mobile and electronic banking while protecting systems from attack.

What is cyber security?

Cyber security refers to policies and technologies that are used to protect data from unauthorised or unintended access, deletion, alteration or destruction. The most obvious cyber threats include: the disruption of business operations, for example, through denial of service attacks; the theft, destruction or publication of commercially sensitive data; and attacks on a business's reputation and customer goodwill.

> "Regulators now have clear expectations around who should be considering these risks, and where the responsibility should lie for addressing them."
>
> **Carlos Conceicao**, Partner, Clifford Chance, London

The perpetrators of cyber attacks generally fall into one of four categories:

- **Criminal** – involving the fraud and/or theft of valuable data. The UK government estimates the cost of cyber theft for UK companies to exceed £30 billion to date.
- **State sponsored** – involving governments accessing military secrets or sensitive commercial information, or seeking to cause disruption, as in the North Korea attack on Sony Pictures.
- **Hacktivism** – by individuals or groups, such as the targeting of banks by Occupy Wall Street in 2011, and the threat by Anonymous to shut down banks' social media pages in 2013.
- **Insider** – involving current or former employees, either stealing corporate assets or breaching confidence.

While these challenges are not new, technology has advanced in such a way that it has become much easier for people to acquire hacking tools and initiate attacks. At the same time, the amount of data being stored and transmitted over networks has increased exponentially. The consequences of cyber security breaches have become more severe, with financial institutions exposed to serious reputational risk, and customers, employees and shareholders becoming much more litigious in this space.

"Legislators see all this happening," says Alvin Khodabaks, a Clifford Chance telecommunications, media and technology partner based in Amsterdam, "and are moving fast to develop laws and improve business and national security. But the processes take a long time and the risk is increasing quickly."

In Europe, a new Cyber Security Directive will be in place in the next two or three years, which will be challenging for many businesses, introducing fines linked to a percentage of global revenue for serious cyber breaches.

Legal risk

Legislation around cyber security is developing differently on either side of the Atlantic. In Europe, one of the key areas of risk is regulatory – where there are sector-specific rules, such as those from the Financial Conduct Authority (FCA), as well as European legislation in the form of evolving data privacy rules and up-coming cyber regulation.

In the United States, contractual legal risk is also an issue, particularly if customers' personal data is compromised, as this can result in a very real threat of class action litigation. There are often confidentiality and performance obligations

> "Legislators are moving fast to develop laws and improve business and national security. But the processes take a long time and the risk is increasing quickly."
>
> **Alvin Khodabaks**, Partner, Clifford Chance, Amsterdam

under customer/supplier contracts, while there is also a growing need for due diligence of an M&A target's security measures, alongside warranty protection and disclosures.

Finally, when it comes to staff, there are obligations owed to employees regarding personal data; directors have fiduciary duties to take cyber security seriously, and efforts need to be made to reduce risk through training and clear protocols and policies.

Regulatory exposure: the United Kingdom

In the UK, the Information Commissioner is responsible for enforcement of the Data Protection Act, which implements the European regime on how secure data should be and how organisations should respond to incidents. Under current law there is no general obligation to notify losses of personal data, but guidance suggests serious breaches should be reported, with factors taken into consideration including the technical resources of the victim company. Certain communications providers do have to notify the Commissioner of personal data breaches, and under proposed new EU regulation a compulsory breach notification is likely to be introduced in the next two or three years.

In the financial services sector, however, data security issues are left in the jurisdiction of the FCA and the Prudential Regulation Authority, as experts on the sector and because of their unlimited power to fine (the Information Commissioner is subject to a cap on fines of £500,000). These regulators have established general principles, such as that institutions must have adequate systems and controls in place, which have been used to discipline firms for data loss/IT systems failures. Firms must also report matters to the regulator which could have a significant adverse impact on their reputation which requires firms to report any such issues.

Richard Jones, Clifford Chance's director of data privacy, says: "Financial services firms are in a different position, because they have a regulator that expects to be informed of any breach."

Another relevant regulator in the UK is the London Stock Exchange (LSE), which requires that listed companies consider whether disclosure of major developments affecting them is required on the exchange. Knowledge of a significant cyber attack may constitute insider information which needs to be disclosed.

The EU Cyber Security Directive

The new EU Cyber Security Directive is not yet in its final form and is unlikely to come into effect before 2017, at which point it will need to be implemented into the laws of each EU member state. Member states will have to adopt a network and information security (NIS) strategy, designate a national NIS authority to implement the directive, and set up a computer emergency response team to handle risks and incidents. Most significantly, they will be obliged to ensure market

"Financial services firms are in a different position, because they have a regulator that expects to be informed of any breach."

Richard Jones, Director of Data Privacy, Clifford Chance, London

operators put in place appropriate security measures, and that they report significant incidents to national authorities.

The directive is targeting critical infrastructure operators, such as energy and transport firms, and it remains to be seen whether financial institutions will fall within the scope of that definition. If they do, there will be new obligations which go beyond those already imposed by the FCA, to adopt risk management practices and report breaches to national authorities, who may publicise incidents if that is thought to be in the public interest.

"It is going to lead to a new administrative burden, increased costs of compliance, and new technical standards and obligations," says Jones. "But for now, to a large extent, institutions just need to watch this space."

Regulatory structure: The United States

In the US, cyber security is a national priority, with huge pressure on government agencies and the private sector to respond to the threat. There are an array of regulators approaching the issue from different perspectives, and these generally fall into three camps. First, the Department for Homeland Security, the Federal Bureau of Investigation, the Department of Defence and the National Security Agency are all focused on cyber as a national security issue, looking at state actors, activists and terrorists. Their main desire with respect to the private sector is to get as much information about hacking activity as possible, and to encourage self reporting.

Secondly, the Federal Trade Commission and the attorney generals in the 50 states are approaching the topic as a consumer protection issue, and so instead of treating banks like victims, are treating them as perpetrators that need to tighten up systems. David Raskin, a Clifford Chance regulatory enforcement partner in New York, says, "That's a serious problem when it comes to disclosure, because who is going to help the government catch people who are hacking systems if that information is going to be used against them in an enforcement action or as part of a class action?"

Finally, the Securities and Exchange Commission and FINRA, the financial industry regulator, fall somewhere in-between. Raskin says: "The SEC wants disclosure from firms who have been attacked, but at the same time has also brought enforcement actions against firms whose systems are viewed as deficient in some way."

Despite these divergent approaches, the US has developed a common standard in the form of the National Institute of Standards and Technology (NIST) Framework. This voluntary set of best practices focuses on critical infrastructure but applies to all companies, and is the result of a collaborative effort to develop tools for boards to use in addressing the issue.

> "The SEC wants disclosure from firms who have been attacked, but at the same time has also brought enforcement actions against firms whose systems are viewed as deficient in some way."
>
> **David Raskin**, Partner, Clifford Chance, New York

The framework identifies the key elements of an effective cyber security policy (core functions) and the basis for self-assessment (implementation tiers and profile); thus, it is divided into three sections:

Core Functions
Identify threats
Protect the system
Detect threats
Respond to threats
Recovery
Implementation Tiers
Partial
Risk informed
Repeatable
Adaptive
Profile
Compare the "current" and "goal" profile to understand what changes need to be implemented

On the enforcement side, the Federal Trade Commission has emerged as the *de facto* cyber security regulator despite having no formal grant of cyber authority. It has settled over 50 cyber actions over the last 12 years, but is not authorised to collect financial penalties. Meanwhile the state attorney generals have an independent power to investigate, along with notification laws, data security laws and private rights of enforcement that are not coordinated with the federal government.

Going forward, the Department for Homeland Security is taking on a bigger role in this space and may yet set federal standards, but there remains a threat within the threat because of too many regulators taking conflicting approaches.

Proposed legislation would provide legal immunity for companies that share cyber information with the Department for Homeland Security, which would be a positive step.

Raskin says Europeans can learn lessons from the US situation: "Generally it's fair to say that, when it comes to enforcement trends, it is smart for people in Europe to pay attention to the US, because behaviour tends to drift from the US to here."

Certainly institutions all over the world are exposed to operational, reputational and legal risks with respect to cyber security now, and need to address these issues.

In practice, all this means three things for financial institutions:

- **Board-level engagement** in this area is critical, because regulators are expecting to see challenges on the part of board members in relation to issues of cyber security;
- **Risk assessments** should be on a proactive rather than reactive basis, looking at threats from both a resilience and a business continuity perspective;
- **Monitoring arrangements** should be in place, regularly testing systems and controls.

CLIFFORD CHANCE CONTACTS

Carlos Conceicao
Partner, London
T: +44 20 7006 8281
E: carlos.conceicao@cliffordchance.com

Richard Jones
Director of Data Privacy, London
T: +44 20 7006 8238
E: richard.jones@cliffordchance.com

Jonathan Kewley
Senior Associate, London
T: +44 20 7006 3629
E: jonathan.kewley@cliffordchance.com

Alvin Khodabaks
Partner, Amsterdam
T: +31 20711 9374
E: alvin.khodabaks@cliffordchance.com

Lena Ng
Counsel, Singapore
T: +65 6410 2215
E: lena.ng@cliffordchance.com

David Raskin
Partner, New York
T: +1 212878 3438
E: david.raskin@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

J201505270047298