Osborne Clarke's 2022 Future of Financial Services

Cybersecurity: how we see cyber risk developing for Financial Services in the next 5 years

26 – January - 3 February 2022

Speakers

Charlie Wedin

Partner
United Kingdom

T +44 117 917 4290
charlie.wedin@osborneclarke.com

Charlie is a partner in our commercial disputes team, and handles large, complex, commercial disputes and investigations, normally with a cross-border element.

Paul Harris

Partner
United Kingdom

T +44 207 105 7441
paul.harris@osborneclarke.com

Paul is a partner in our Financial Institutions Group, advising clients on all financial services regulatory matters, with a particular specialism in advising on payments and fintech-related matters

Nina Lazic

Associate Director
United Kingdom

T +44 20 7105 7400
nina.lazic@osborneclarke.com

Nina is an Associate Director (and solicitor-advocate) in Osborne Clarke's dispute resolution team, with particular expertise in cyber security and technology disputes.

Catherine Hammon

Head of Advisory Knowledge
United Kingdom

T +44 207 105 7438
catherine.hammon@osborneclarke.com

Overview

- **Why does it matter?** Cyber attacks can cripple a business' ability to carry out everyday functions, cause reputational damage, result in financial loss, attract regulatory attention (including significant fines), and result in claims for compensation from customers / employees / data subjects (whether litigation or FOS complaints).
- **Volume of cyber attacks rising rapidly**. From February to April 2020: 238% growth in attacks against the financial sector (globally) & 80% of financial institutions reporting an increase in cyber-attacks (Source: VMWare).
- **Growing sophistication**, with attacks becoming more targeted, co-ordinated, and focussed.
- **In the FS sector**:
    - FS companies are a lucrative target, especially for extortion, given the wealth of data held (financial information, sensitive personal data, confidential business information, insider information, etc).
    - Patchwork of obligations: contractual requirements, alongside regulatory obligations. E.g. Payment Card Industry Data Security Standard (PCI DSS).
    - Not strictly cyber security but, increasing 'customer risk': Liability for consequences of third party fraud – e.g. Authorised Push Payment (APP) fraud. Voluntary refunds at the moment (CRM Code), but calls by Payment Systems Regulatory for mandatory refunds.

What does the future hold?

1. Ransomware attacks

- **What are they & how might they manifest?** Encryption of data / key systems and / or data exfiltration + threat of publication. Can be opportunistic or highly targeted (including post attack through, e.g., targeted approaches to key executives or customers, by way of pressured extortion).
- **Dealing with an incident.** The practicalities (containment, rebuilding, continuity of operations, ascertaining scope, payment?), the legal obligations (notification of regulators and data subjects / customers), the communications (internally, externally), and remediation ('lessons learned').
- **To pay or not to pay?**
    - **Ethical and moral considerations.**
    - **Legal considerations.** Payment of a ransom may not be an offence under UK law unless the firm knows or reasonably suspects that there are connections to terrorism or this would breach sanctions regimes.
    - **Practical considerations.**
    - **What will your regulator(s) think?**

2. Digital transformation

- **For FS incumbents.** Patchwork of (legacy) third party applications and systems, with varying degrees of interconnectivity.

- **For FS disruptors.** No legacy systems, which means the need to create suitable IT infrastructure from scratch.

- Digital transformation provides huge opportunities but also, huge risks:

    - **The right supplier & solution?** How have you assessed the suitability of your vendor? Do they have a proven track record? Does their solution embed cyber security by design? Does their solution have the required connectivity with existing systems? What level of customisation is required for the solution?

    - **The right contract?** Do you know your requirements for the solution? Have your requirements been adequately scoped (with an eye to key cyber security principles)? Who will have responsibility for ensuring the on-going security of the solution once it goes live?

    - **Execution risk.** E.g. inadequate testing, poorly configured production / performance testing environments, rushed migration.

- **And… ongoing supply chain risks.** You are only as strong as your weakest supplier (e.g. Log4j).

3. Developing technologies

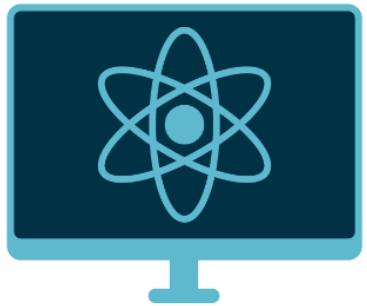
Blockchain, crypto, DeFi etc

- Hacks and exploitation of code errors
- Private vs public blockchains
- Remedy/recompense?

Artificial Intelligence

- Arms race
- Cloud services

Quantum computing



- Time frame?
- ***"… appropriate technical and organisational measures** to ensure a level of security appropriate to the risk…"*

4. Growing (& continuing) regulatory scrutiny (GDPR & DPA 2018)

- **Core security requirement:**
    - "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement* ***appropriate technical and organisational measures*** *to ensure a level of security appropriate to the risk…*" (Article 32(1) GDPR, emphasis added)
    - Evolving standard (not static).
- **Notification obligations, for "personal data breaches":**
    - **Article 33 GDPR.** Notification required "*unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*".
    - **Article 34 GDPR.** Notification required if "*likely to result in a high risk to the rights and freedoms of natural persons*"
- **Monetary penalties.** £17.5m or 4% of total annual worldwide turnover. To date: £22m for BA, £20.45m for Marriott, £1.4m for Ticketmaster, £585k for Cabinet Office, and £320k for Doorstep Dispensaree (+2 others)

4. Growing (& continuing) regulatory scrutiny (FSMA & handbooks)

- Senior Management, Arrangements, Systems and Controls sourcebook (SYSC) of the FCA Handbook: Firms should have effective, proportionate and risk-based systems and controls in place to ensure they cannot be used for financial crime.

- **Notification obligations.**

    - Principle 11 of FCA's Principles for businesses requires firms to deal with their regulators in an open and co-operative way, and disclose appropriately anything relating to the firm of which the regulators would reasonably expect notice.

    - FCA guidance in cyber context: FCA regulated firms must notify the FCA as soon as it is aware of a 'material' cyber incident. An incident could be material if:
        - it could or does result in significant loss of data, or the availability or control of IT systems
        - it affects a significant number of customers and could result in serious harm to them, such as theft of personal data
        - it could or does result in someone getting unauthorised access to data and altering it, or
        - malicious software is present on information and IT systems.

    - EBA guidelines on major incidents reporting (PSD2).

- **Enforcement.** Enforcement for firms that do not have adequate cyber security systems and controls in place or who fail to notify. No maximum for fine that can be levied. To date: £16.4 million for Tesco Bank.

- **Changes to SYSC (operational resilience).**

4. Growing (& continuing) regulatory scrutiny (ICO and / or FCA?)

- **FCA / ICO Memorandum of Understanding**: "*the most appropriate body*" will lead, notification to each other of "*significant developments*", matters can be referred to the other for action, investigations can be carried out by both (in parallel).

- In practice:

    - Notify both, keep both informed.

    - ICO usually takes lead if high volume of personal data.

- Potential for 'double jeopardy', but none so far.

5. A rising tide of customer complaints and claims (GDPR & DPA 2018)

- **Compensation available,** for material or non-material damage (Article 82(1) GDPR), where non-material damage includes distress (s.168, DPA 2018).
- Key case: *Lloyd v Google:* Lloyd sought compensation for "*loss of control*" damages, for both himself and an estimated 4.5 million iPhone users, via a representative claim under CPR 19.6. Supreme Court: DPA 1998 provides right to compensation for material damage (e.g. financial loss) or distress. No entitlement, under DPA 1998, to compensation for "loss of control".
- Other useful cases to stem the tide: *Warren v DSG Retail Limited, Rolfe v VWV, Johnson v Eastlight, Ashley v Amplifon.*
- BUT: ICO's position in *Lloyd v Google*…

5. A rising tide of customer complaints and claims (FSMA & DISP)

An easier route for compensation and / or driving settlement?

- **Financial Ombudsman Service.**
  - Customers entitled to escalate complaint.
  - Currently: Firms are not required to pay a case fees for the first 25 cases referred to the FOS in a financial year. **A case fee of £750 (per complaint)** is payable by firms which receive over 25 complaints.
  - Proposals: The FOS has proposed to reduce the number of 'free' cases from 25 to 3.
- **Impact on litigation.** If a customer accepts a favourable decision by the Ombudsman, the customer will be unable to claim additional damages in subsequent civil court proceedings if the claim is relates to the same cause of action, based on the same facts.
- **Consumer Redress Schemes.** The FCA has rule-making powers to require a firm to establish and operate a consumer redress scheme…

Any questions?

About Osborne Clarke

Our global connections and 'best friends'

Through a network of 'best friends' we extend our reach across the globe, particularly in North America, EMEA & Asia Pacific. We have worked closely with like-minded firms in over 100 countries. We'll find the right local partner for you and wherever that may be, we will make sure that you receive the Osborne Clarke level of service.

Europe

Belgium: Brussels

France: Paris

Germany: Berlin, Cologne, Hamburg, Munich

Italy: Busto Arsizio, Milan, Rome

The Netherlands: Amsterdam

Spain: Barcelona, Madrid, Zaragoza

Sweden: Stockholm

UK: Bristol, London, Reading

USA

New York, San Francisco, Silicon Valley

Asia

China: Shanghai

India*: Bangalore, Mumbai, New Delhi

Singapore

925+

talented lawyers working with

270+

expert partners in

25

international locations* advising across

8

core sectors with

1

client-centred approach

*Services in India are provided by a relationship firm