Spotlight

KEY POINTS

- While cybersecurity is a matter of serious concern to the industry, there are no reported cases on liability of financial institutions to clients, following cyberbreaches.
- After a cyberattack, a financial institution may be exposed to liability as matter of English law in contract, tort and under the Data Protection Act 1998.
- Further areas of liability will come via EU law with the General Data Protection Regulation (679/2016/EU), which comes into effect on 25 May 2018, and the Network and Information Security Directive (2016/1148/EU), which is due to be implemented by 9 May 2018.
- The government has stated that it will implement the Network and Information Security Directive despite Brexit but the continuing status of the General Data Protection Regulation will depend on the final terms of the "Great Repeal Bill".
- A financial institution's insurance coverage is, at present, largely a matter of happenstance with the most likely cover being under professional indemnity policies; it is now time for comprehensive cyberpolicies to come into the mainstream.

Authors Sir Richard Aikens and Andrew Dinsmore

The legal implications of cybersecurity breaches for financial institutions

This article considers the potential liabilities and insurance recourses that financial institutions face following a cyberattack from a third party.

INTRODUCTION

Cybersecurity has been a major concern of financial institutions over the last few years. PricewaterhouseCoopers (PwC) estimates that there are between 4,600 and 4,900 detected incidents of cyberbreaches a year.[1]

The main areas of concern over potential cyberbreaches are the increasingly complex technologies, rising threats from foreign nation-states and the consequences of a lack of clear regulatory guidance. It is therefore not surprising that Cybersecurity Ventures estimates that cybersecurity spending, across all sectors, on products and services will exceed US$1trn between 2017 to 2021.[2]

This article will consider (1) a financial institution's exposure to liability, and (2) a financial institution's possible insurance recourses[3] in the following fact pattern: a financial institution is hacked by an anonymous group to obtain data about the institution's clients for non-political reasons which leads to loss in circumstances where they did not have up-to-date security software.[4]

The range of potential losses is broad; by way of example it could include obtaining:

- an individual's account details from which the hacker could interfere with their investments;
- a business's financial statements from which the hacker could decipher its suppliers or customers allowing the hacker to interfere with its business;
- a high-net-worth individual's personal details, for example their address, which is then used for criminal purposes such as a robbery;
- a business's data, for example its email address, which could then be hacked and used to perpetrate further cyberfrauds such as issuing fake invoices to its clients on which the clients react.

THE EXPOSURE TO LIABILITY

The institution may be exposed to liability for such losses in contract, the tort of negligence, for breach of statutory duty and for breach of EU law.

Contract

A cause of action in contract will, of course, depend on the terms of the contract and one can imagine a scenario where there is an express term in its agreement that the institution will maintain up-to-date cybersecurity software or, at least, a term that the institution shall keep the client's information safe.

The more interesting question, for our purposes, is whether or not a court would imply such a term. While the implication of a term will depend on the express terms and the general nature of the parties' agreement, it is certainly conceivable that if the institution had undertaken express obligations in relation to cybersecurity, business necessity requires that a term be implied that they kept up-to-date cybersecurity software. Further, in our view, it is likely that a court would imply a term that the institution would use reasonable care to safeguard their client's information from cyberattack.

To avoid the risk of such an implied term, the institution may wish to include: (i) an express clause either excluding liability or creating a contractual estoppel; or (ii) a specific *force majeure* clause which contemplates such a cyberattack and provides that neither party will be liable to the other for loss in the event of a cyberattack.

A further issue is what damages would be recoverable. The general rule is that a claimant can only recover such loss as is within the reasonable contemplation of the parties at the date of contracting. The damage must not be too "remote" to be recoverable.[5] This therefore requires an assessment of what the client disclosed to the financial institution, when, for example, opening a bank account, and explaining the financial implications of their information being accessed by third parties. While it is generally foreseeable that hacking into a client's account could cause financial loss, there will undoubtedly be difficult issues where the loss is particularly substantial or unusual.

Financial institutions should thus pay close attention to their express terms and if they intend to exclude liability for a cyberattack they should include an express exclusion/*force majeure* clause to this effect and, in the event an action is brought, be aware of possible defences based on remoteness of loss.

Tort

There is no decided case to the effect that, under the law of the tort of negligence, there is to be imposed a duty of care to maintain cybersecurity software.[6]

When a case does arise based on an allegation that the financial institution was negligent because its cybersecurity was not up to date, a court is likely to analyse whether or not the financial institution could be said to (1) have objectively "assumed responsibility" for so-called "pure economic loss"[7] caused by a data breach in these circumstances and whether the claimant relied on that "assumed responsibility";[8] and/or (2) whether it was (i) foreseeable that there would be loss, (ii) the parties were in a proximate relationship, and (iii) it would be fair, just and reasonable to impose a duty of care in the circumstances;[9] and/or (3) whether "incrementalism" permits an extension of the current ambit of the duty of care.

These three tests are said to complement each other and should achieve the same result;[10] in our view:

(1) As to the "assumption of responsibility", this is likely to turn on the terms of the agreement between the financial institution and the client and what the institution's representatives have previously stated (either in the contract or by a representative of the institution).

(2) As to the threefold test, our view is that (in the scenario contemplated) a court is likely to conclude that loss is the foreseeable consequence of the failure to maintain proper cybersecurity and there is a proximity of relationship; the key issue will therefore be whether it is fair, just and reasonable to impose a duty of care in these circumstances, which is likely to fall back on an analysis of precisely what was agreed and/or said.

(3) As to "incrementalism", it is now commonplace for service providers to be held liable for economic loss caused by their negligence and, in our view, it would be in accordance with the doctrine of "incrementalism" to allow the establishment of this duty in an appropriate case.[11]

Thus, there is a good argument that the courts would hold that there is a duty of care in these circumstances.

As always, however, whether a duty arises in a particular case will turn on its facts. Of course, any duty or liability may be negatived where there is a contract which excludes liability or creates a contractual estoppel against reliance on any state of affairs or representations.

Two final areas of interest are:

(1) the failures that will be required before the duty of reasonable care is broken, which is likely to be a matter of expert IT evidence; and

(2) where the court will draw the line in remoteness of damage.[12]

Breach of statutory duty

As to breach of statutory duty,[13] the key statute will be the Data Protection Act 1998 (DPA 1998) as recently considered in *Vidal-Hall et al v Google* [2016] QB 1003. The Court of Appeal held, albeit in the context of a permission to serve out hearing, that where a private individual brought an action for the misuse of private information, in breach of DPA 1998, the damages under s 13 were not limited to pecuniary loss but could include, for example, emotional distress.[14]

In our view, financial institutions should be aware of the data protection principles included in Sch 1 of the 1998 Act (as given effect by s 4) because a breach of such principles may lead to a private action under s 13; the most likely provision that could found such an action is Sch 1, para 7 which provides that: 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'[15]

As a result, financial institutions should ensure that their data processes and cybersecurity software are up to date as they may be exposed to a damages claim for a failure to do so as being a breach of a statutory duty.

EU law

There are two potential EU regimes on the horizon: (i) General Data Protection Regulation (679/2016/EU) (GDPR);[16] and (ii) the Network and Information Security Directive (2016/1148/EU) (the NIS Directive).[17]

As to the GDPR, this seeks to ensure that organisations are held to high standards when processing personal data and encourages the implementation of national codes of conduct.[18] The focus is on supervisory authorities but Art 79 notes that subjects are entitled to an effective judicial remedy and Art 82 expressly provides for a right to compensation for 'any person who has suffered material or non-material damage as a result of an infringement of this Regulation'.[19]

As to the provisions which could ground such an action:

- We note that Art 5(1)(f) provides that personal data must be processed 'in a manner which ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures';
- Art 24(1) provides that '…the controller shall implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with this Regulation'; and
- Art 32 will place obligations on financial institutions to 'implement appropriate technical and organizational measures to ensure a level of security protection appropriate to the risk…'.

Spotlight

Financial institutions may wish to rely on Art 82(3) which provides an exemption where they were 'not in any way responsible for the event giving rise to the damage'. The phrase 'not in any way' appears to set a high threshold to fall within this exemption and there will be difficult arguments as to (i) whether the relevant "event" is the inadequate software or the act of hacking, and (ii) the causal connection required of "giving rise to".

As to the NIS Directive, this was intended to require companies within the EU member states to ensure that they have suitable IT security mechanisms and is limited to 'critical infrastructure essential for the maintenance of vital economic and societal activities'. Annex II to the current draft includes the banking sector[20] and financial market infrastructures.[21]

It is intended (among other things) to require that EU member states adopt a national strategy on the security of network and information systems[22] and to require that businesses that collect or process the personal data of individuals must implement appropriate technical and organisational measures.[23]

The focus of implementation, contained in Arts 15 and 17, is on the establishment of competent authorities, which indicates that there is no obligation on member states to make provision for a private law cause of action.[24] However, this is only the minimum position[25] and there is no bar on the UK government providing for a private cause of action similar to s 13 of the DPA 1998.

In the event that such a private law cause of action is included in the legislation, it will be interesting to see how this will interact with the GDPR and the express provisions for compensation therein.

Conclusion on liability

In conclusion, financial institutions may be exposed to liability as follows:

- for breach of contract and in tort, which will require a close analysis of the parties' understanding and the allocation of risk;
- for breach of the DPA 1998, which could include emotional distress;
- for breach of the GDPR, when it comes into force;
- potentially for breach of the NIS Directive, depending on how it is implemented in the UK.

THE INSURANCE POSITION

Despite the concerns over cybersecurity and the potential exposure to liability for financial institutions, it is surprisingly difficult to find specific "cyberinsurance". While there are two cyberspecific clauses,[26] they seek to exclude liability in specific industries (namely shipping and aviation), as opposed to cover it, and thus provide no comfort for institutions that fail in their obligations to protect their clients from the consequences of a cyberattack.

We will now consider the factual scenario set out above, by reference to typical insurance policies. We argue that it is time for specific cyberinsurance to come into the mainstream.

Professional indemnity insurance

The financial institution may attempt to rely on its professional indemnity insurance, which ordinarily covers a firm for negligence and other wrongdoing in relation to the provision of its services.

While this would most likely cover the simple example noted above, the nature of cybersecurity is so broad and multi-faceted that a situation could easily arise which is not covered. There may well be an exemption from coverage in the event of a cyberattack on the insured.

Thus, while this may provide the most straightforward insurance recourse in some circumstances, it is likely to be a matter of happenstance and financial institutions should not simply assume that all eventualities are covered; rather, they should ensure that specific clauses are included or collateral insurance entered into.

Directors and officers liability insurance

It is likely that the board of a financial institution will have D&O insurance, which generally covers director's liability (plus costs and expenses) following a claim.

The main question will be whether or not the failure to update the security software was an omission of the company or of the individual director and, if the individual, whether it was in the individual's capacity as a board member. The latter requires an analysis of whether security software updates are, or should be, a "board" issue as opposed to an administrative concern of those lower down in the company. These are far from easy questions and may result in a difficult insurance battle unless clear policy wording is used.

As to possible actions:

- A cause of action may be brought by the shareholders for a breach of ss 172 and 174 of the Companies Act 2006, which respectively require that directors promote the success of the company and exercise reasonable care and skill and diligence in the conduct of their role.
- Further, a cause of action may be brought by third parties in the forms noted above.

While directors may think that a way around the problems with D&O cover is to require an indemnity from the company, they will have to contend with ss 232 to 234 of the Companies Act 2006 which provides that directors cannot be indemnified for breaches of duties they owe to the company. Thus, this is unlikely to provide a simple answer to their concerns.

As a result, D&O cover may provide cover but our view is that directors should ensure clear wording in the policy if they seek to rely on such.

Terrorism insurance

It is possible that a financial institution may have terrorism cover, which ordinarily indemnifies the insured against loss which arises from physical damage to the insured property where such damage occurs as a result of terrorism/political violence.

There are a number of problems with relying on a typical terrorism policy in our hypothetical situation:

- there was no political motivation for the cyberattack, which is likely to take this outside the concept of "terrorism";[27]

Biog box
Sir Richard Aikens, based at Brick Court Chambers, is a former Lord Justice of Appeal who now works as an arbitrator in international commercial disputes. He is also a Visiting Professor at King's College London and Queen Mary University of London and one of the editors of *Dicey, Morris & Collins Conflict of Laws*. Email: richard.aikens@brickcourt.co.uk

- the traditional focus of terrorism policies has been to protect against, for example, a terrorist bomb effecting the insured's property and the present case is much more likely to be concerned with pecuniary loss as a result of a law suit; and
- ordinarily, terrorism cover will exclude loss arising from "attacks by electronic means", such as computer hacking or a virus, and is therefore likely to be excluded.

Thus, it is unlikely that the present case would fall within typical terrorism cover.

Public liability insurance

Public liability insurance is primarily concerned with personal injury to third parties which occurs in the course of the conduct of the insured's business and thus would not be relevant here. Further, it is common for such insurance to include a data exclusion, which is likely to include a cyberattack.

Crime and fidelity

Crime and fidelity policies generally cover the insured for first-party loss directly caused by certain types of wrongdoing by employees and third parties and often include 'computer misuse'; however, they are primarily concerned with loss *in specie* and thus the loss of online data and the legal liability for the consequences of that may not fall within standard coverage. In the event that they do fall within such coverage, an issue may be that a failure to update the security software was a breach of warranty which invalidated the insurance.

Insurance Act 2015

The Insurance Act 2015 (the 2015 Act) came into force in August 2016 and will apply to all insurance contracts entered into after that date unless its application has been excluded.[28] A few points relevant to the present discussion are that:

- The insured has to provide the insurer with a 'fair presentation of the risk' (s 3) which, in this context, would most likely require a full presentation of their cybersecurity position and the regularity with which breaches are attempted and whether they have been successful;
- If the insured fails to update its cybersecurity software, it may be in breach of warranty. The effect of such a breach would be to suspend their coverage for the period during which this failure continues (s 10);
- In the event that the insurer fails to pay a claim within a reasonable period of time, they may be liable for breach of an implied term of the contract of insurance (s 13A);[29] although, again, an insurer can contract out of this implied term if they comply with the transparency requirements in s 17 noted above.[30]

Conclusion on insurance

It is clear from the above that whether or not a financial institution is insured is a matter of happenstance by reference to the traditional categories of insurance, with the most likely avenue being professional indemnity cover.

CONCLUSION

In conclusion, there are many potential areas of liability yet very few, if any, clear insurance recourses.

It is likely that cybersecurity and cyberfraud will continue to be of growing concern to financial institutions in future and perhaps it is time for further engagement with the Council for Registered Ethical Security Testers (CREST), a non-profit organisation which provides cybersecurity services such as penetration testing including the Simulated Target Attack and Response programme (STAR) as developed in collaboration with the Bank of England.[31]

Further, the EU Agency for Network and Information Security (ENISA) maintains a cloud certification scheme which aims to assist companies through self-certification or independent assessment thereby building confidence among cloud users.[32] However, it is unclear what role, if any, ENISA will play for parties in the UK following Brexit.

Finally, as to the insurance position, it is time that cyberpolicies come into the mainstream so that policies which concentrate on this risk can address the multiplicity of situations in which liability can arise. This is the growing trend in the United States and in our view the United Kingdom should follow suit. ■

1 See PwC's 'The Global State of Information Security ® Survey 2017' in relation to the financial services sector at https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/financial-services-industry.html

2 See Cybersecurity Venture's 'Cybersecurity Market Report' at https://cybersecurityventures.com/cybersecurity-market-report/

3 For an in-depth analysis of the cyberinsurance market in the maritime context, see the Maritime London paper 'Cyber Risks and Insurance: An Introduction to Cross Class Cyber Liabilities' January 2016 www.maritimelondon.com/wp-content/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf

4 Financial institutions should also be aware of their various regulatory obligations which may apply in the cybersecurity context, for example PRIN 2.1.1(3) of the FCA Handbook which requires, inter alia, that a firm 'take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems' or the FCA Listing Principle 1 which requires that 'A company must take reasonable steps to establish and maintain adequate procedures, systems and controls to enable it to comply with its obligations' as contained in LR 7.2.1 of the FCA Handbook.

5 By this we mean the loss which the law determines is too far removed from the breach to be recoverable despite, on one analysis, having been caused by the breach.

6 There is also an interesting question as to the institution's obligations in bailment which requires an analysis of whether a client has property with the bank, for example if they have gold sovereigns in a safety deposit box, and an interesting

Spotlight

Andrew Dinsmore is a barrister practising from St Philips Stone Chambers in international commercial litigation and arbitration. He regularly acts in banking and financial matters; his recent work includes a number of urgent freezing injunctions and Norwich Pharmacal Orders in the context of cyberfraud.
Email: andrew.dinsmore@stonechambers.com

analysis of what proprietary rights a client has (if any) in their own information.

7 By this we mean a loss which is not related to any property damage or personal injury.

8 *Hedley Byrne & Co. Ltd v Heller & Partners Ltd* [1964] AC 465; *Henderson v Merrett Syndicates Ltd* [1995] 2 AC 145.

9 *Caparo Industries v Dickman* [1990] 2 AC 605.

10 See *Commissioners of Customs and Excise v Barclays Bank Plc* [2007] 1 AC 181. Lord Bingham noted at §8 that all three tests provide for a duty in the majority of cases; a position Lord Mance shared at §83.

11 In *Commissioners of Customs and Excise v Barclays Bank Plc*, Lord Bingham noted at §7 that incrementalism alone would not be sufficient and Lord Mance described it at §93 as an 'important cross-check on any other approach'; see further, Buxton LJ in *Islington LBC v UCL Hospital NHS Trust* [2005] EWCA Civ 596, §27.

12 On remoteness of loss in "pure economic loss" cases in tort, Clerk & Lindsell, *On Torts*, 21st edn, §2-177 notes that: 'It is arguable that the scope of duty test should be seen as the key element in the application of the remoteness principle to pure economic loss. What the defendant can reasonably contemplate as a consequence of his breach must depend upon the scope or purpose of his duty. If the risk of the particular kind of damage fell outside the purpose of the defendant's duty, then however foreseeable that risk in general terms, it would not fall within the reasonable contemplation of the defendant. Whether the scope of the duty is seen as an independent test or as the key element in the concept of remoteness, it has had a major impact in limiting tortious liability for pure economic loss.'

13 See generally, Clerk & Lindsell, *On Torts*, 21st edn, Ch. 9.

14 In this regard, it is important to note that the DPA 1998 expressly provides for a private law cause of action; if it did not, the presumption is that a statute is not actionable but the court would consider whether Parliament intended to give the individual a private law cause of action if the statute imposes an obligation on the defendant for the protection of a class of individuals.

15 See further Sch 2, para 9, which makes specific reference to the implementation of technological security measures.

16 This is due to come into effect in EU member states from 25 May 2018 and the UK government has confirmed that it will implement its provisions irrespective of its continued membership of the EU.

17 This was adopted by the EU on 6 July 2016 and must be implemented by EU member states by 9 May 2018; thus, it will be implemented before the planned departure of the UK from the EU.

18 See Art 40ff.

19 Art 82(6) then expressly provides that the right to compensation is to be brought in the courts referred to in Art 79(2).

20 Annex II(3).

21 Annex II(4).

22 See Art 7.

23 See Arts 14 and 16.

24 Art 21 also notes the role that penalties, as opposed to private compensation, are to play in the regime.

25 Art 3 states that '...Member States may adopt or maintain provisions with a view to achieving a high level of security of network and information systems.'

26 The CL380 "Institute Cyber Attack Exclusion Clause", which often attaches to the ITV-Hulls (01/10/83) policy in a shipping context, and the AVN48B "War hi-jacking and other perils exclusion clause (Aviation)", which often attaches to an AVN1D or AVN1C policy in the aviation context.

27 See the definition given in s 1 of the Terrorism Act 2000 in the context of fire insurance; the definition used has been 'any use of violence for the purpose of putting the public or any section of the public in fear': *MacGillivray on Insurance*, 13th edn, §28-033.

28 Insurers can only exclude the 2015 Act in non-consumer insurance and to do so they will have to comply with the transparency requirements of s 17; namely, they have to take sufficient steps to draw the disadvantageous term to the insured's attention before the contract is entered into or the variation agreed. Even then not all sections can be excluded, eg s 9.

29 Section 13A was introduced by s 28 of the Enterprise Act 2016 earlier this year.

30 See s 16A, as introduced by s 29 of the Enterprise Act 2016.

31 See further ISO standards on information security management systems, the most well known of which is the ISO/IEC 27001: 013.

32 See the EU Commission's paper, *Unleashing the Potential of Cloud Computing in Europe*, published on 27 February 2012, COM(2012) 529, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

Further Reading:

- The New York State Cybersecurity Regulation: lessons for UK-regulated firms? (2017) 6 JIBFL 373.
- What can be done to mitigate cyber risk? (2015) 6 JIBFL 353.
- LexisPSL: Banking & Finance: Cyber-attacks on banks: the consequences of a loss of access to bank records.

Further Information

- Maritime London paper 'Cyber Risks and Insurance: An Introduction to Cross Class Cyber Liabilities' January 2016: www.maritimelondon.com/wp-content/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf
- PwC's 'The Global State of Information Security Survey 2017' in relation to the financial services sector at: https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/financial-services-industry.html
- See Cybersecurity Venture's 'Cybersecurity Market Report' at https://cybersecurityventures.com/cybersecurity-market-report/