Cyber Liability: Risks for Professionals and Their Insurers

William Flenley QC[*] & Jake Coleman[†]

Introduction

The last 12 months have seen a remarkable rise in the prominence of cyber-crime. There were allegations that the Russian government had hacked the Democratic National Committee's email system in an attempt to influence the US election. Yahoo revealed that more than a billion users' data might have been compromised by hackers in the largest cyber-attack in history. And, closer to home, a total of 61 NHS organisations across the UK were hit in an unprecedented global ransomware attack.

The issue of cyber-crime, however, is not one that is peculiar to governments and multinational corporations; it is one that professionals and their insurers need to be acutely aware of. That was demonstrated by the hacking of the Panamanian law firm, Mossack Fonseca, and the subsequent release of the 'Panama Papers' in May 2016. The targeting of a firm of lawyers should ring alarm bells for all professionals: Mossack Fonseca appears to have been attacked because of the sensitive information which it held. The nature of all of the professions necessitates the holding of sensitive data, whether it relates to dubious activity or not. This makes professionals prime targets for cyber-criminals.

Even barristers may be subjected to the attention of cyber-criminals. In February 2017 the Bar Council's *Counsel* magazine warned:

> "Cyber security is acknowledged to be one of the greatest threats to business around the world, with a global cost estimated at $445bn, according to the World Economic Forum's 2016 Global Risks Report. The cost has been estimated to have risen by 200% in five years and has been projected to reach $6tn by 2021."

It was perhaps prompted by these statistics that, on 1 November 2016, the Chancellor of the Exchequer announced the government's new National Cyber Security Strategy for protecting the UK economy from cyber-attacks.

In this paper we discuss issues relevant to the liability of professionals who are the subject of cyber-crime. Case law is needed to clarify the extent of a professional's liability, but it seems to us that the most obvious candidates to consider are (1) liability under the Data Protection Act 1998, (2) a failure to take reasonable care to protect confidential information, sounding in breach of contract or negligence, and (3) breach of confidence.

Once some cases have been decided in this area, it may turn out that:

(i) Clients of professionals will have a retainer with the professional, and may therefore be able to rely upon breach of contract, or negligence, as their primary cause of action if the professional has caused damage by breaching guidance on cyber-security; whereas

---

[*]Queen's Counsel at Hailsham Chambers and co-author of "Solicitors' Negligence and Liability" (Flenley & Leech).
[†] Junior Barrister at Hailsham Chambers.

(ii) Those who are not clients may have to rely upon either (a) the provisions of the Data Protection Act 1998, (b) showing a *Hedley Byrne* special relationship so as to give rise to a duty of care in tort, or (c) breach of confidence.

(1) Data Protection Act 1998 – Breach of Statutory Duty

Section 4(4) of the Data Protection Act 1998 ("the Act") places a statutory duty on professionals, as 'data controllers,' to comply with the eight 'Data Protection Principles'. These are listed in Schedule 1 to the Act, and include the following obligation in relation to security, known as the seventh data protection principle:

> "7. **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." [Emphasis added.]

Breach of that statutory duty will afford individuals a right to compensation pursuant to s.13 of the Act.

Is Liability Strict or Fault-Based?

The duty imposed by the seventh data protection principle is fault-based, in that it requires only that "appropriate technical and organisational measures" be taken to protect personal data. Limited clarification of that duty is provided in the Act. With regard to the seventh data protection principle, the Act provides that:

> "9. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—
>
> (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
>
> (b) the nature of the data to be protected".[1]

This would appear to require a classic balancing act between the cost of preventing harm, and the extent of damage likely to occur if there is a breach of data security. It appears similar to the courts' approach when considering liability for negligence.

Further, the data controller must take reasonable steps to ensure the reliability of any employee who has access to protected information,[2] and contracts for out-sourcing of data processing must be evidenced in writing.[3]

Although there have been no reported cases construing these provisions, there is a regulatory regime which is likely to be "strong evidence of what the common law requires."[4] That regime includes guidance produced by the Information Commissioner's Office ("ICO"), which, for example, recommends: performing risk assessments; subscribing to the UK Government's 'Cyber Essentials Scheme'; and securing data in the office,

[1] Schedule 1, Part II, para.9.
[2] Sched 1, Part II, para 10.
[3] Sched 1, part II, para.12.
[4] *O'Hare & Anor v Coutts & Co.*, [2016] EWHC 2224 (QB) at [207].

on the move and in the cloud.[5] Similarly, the Solicitors Regulation Authority, Financial Conduct Authority and Institute of Chartered Accountants in England and Wales have all released their own guidance relating to cyber-security. A failure to comply with any of the recommendations contained in those documents may, therefore, render a professional vulnerable not only to admonishment from the ICO or his/her professional regulator, but also to civil liability.

Beyond regulatory guidance, however, it is unclear what courts will require of professionals in their enforcement of the Act. Plainly, case law is required in order to elucidate the precise meaning of the word 'appropriate' in the context of data protection security measures. We may not have to wait too long for that to happen, as there is news of litigation which is likely to examine this area of the law. For instance, a group action is being brought by thousands of staff at Morrisons for the supermarket's alleged failure to prevent a hacker from stealing their bank, salary and national insurance details.[6]

Statutory Defence

Under s.13(3) of the Act, there is also a statutory defence available to data controllers who have acted 'reasonably':

> "(3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was **reasonably required** to comply with the requirement concerned." [Emphasis added.]

Other than placing the burden of proof on the defendant, it is difficult to see what practical difference there is between this defence and the requirement imposed by the seventh data protection principle that data controllers need take only "appropriate technical and organisational measures". It would appear, however, that a professional who puts in place robust security measures, but is nonetheless the victim of a sophisticated cyber-attack, is unlikely to be found liable to a third party under the Act.

Compensation for Breach of Statutory Duty

Section 13 of the Act provides:

> "(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.
>
> (2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for

[5] ICO, 'A Practical Guide to IT Security',https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf.
[6] http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/11957905/Morrisons-sued-by-2000-staff-over-data-breach.html.

that distress if— (a) the individual also suffers damage by reason of the contravention, or (b) the contravention relates to the processing of personal data for the special purposes."

Where pecuniary loss is suffered by an individual consequent upon a failure adequately to protect their personal data, recovery is straightforward. Pecuniary loss amounts to 'damage', [7] and the individual is therefore entitled to compensation under s.13(1).

The position where mere distress is suffered, without pecuniary loss, is more complex. S.13(2) of the Act would appear to preclude the recovery of compensation in such cases, unless it involves a breach relating to one of the 'special purposes', namely journalism, art or literature.[8] The Court of Appeal in *Vidal-Hall v Google*,[9] however, unanimously held that the wording of s.13(2) was incompatible with the EU's Directive on data protection ("the Directive").[10] The court decided that the Directive placed an obligation on the UK to protect its citizens' privacy where personal data is processed, in a manner which did not distinguish between pecuniary and non-pecuniary loss. The Act, in denying a remedy to those who had suffered the latter type of loss, had therefore failed to transpose the requirements of the Directive into UK law. The Court of Appeal therefore held that the provision should be disapplied, as it failed to provide an effective remedy under EU law.[11]

The result is that compensation is available to third parties who suffer mere distress pursuant to a data breach, notwithstanding the existence of s.13(2) of the Act.

The General Data Protection Regulation

Finally, we must mention that the landscape of data protection law is changing. On 25 May 2018, the General Data Protection Regulation ("the GDPR") came into force; as it is a regulation, it is directly effective without further legislation by the UK government. This brings with it numerous significant alterations to the current legislative framework. A full journey through those additions is outside the remit of this paper, however, we note the following:

a) a new 'accountability' data protection principle is added, requiring a data controller to be able to demonstrate compliance with the principles;

b) data controllers must identify, and are therefore well-advised to record, the legal basis on which they process (e.g. hold) personal data; and

c) data subjects have enhanced rights, which include the right to erasure, i.e. the right to be forgotten.

[7] *Johnson v Medical Defence Union*, [2007] EWCA Civ 262 at [74].
[8] S.3 of the Act.
[9] [2016] QB 1003.
[10] Parliament and Council Directive 95/46/EC.
[11] *Vidal-Hall*, at [79] to [105].

Of course, it is entirely unclear what will remain of the GDPR following the completion of Brexit negotiations. But, given that negotiations are unlikely to be complete until nearer March 2019, professionals plainly must gain awareness of their enhanced obligations under the GDPR.[12]

(2) Contract and Negligence

Retainers may include either an express or an implied term relating to the security of clients' personal data. It seems likely that professionals will often have an implied contractual duty to take reasonable care to safeguard their clients' confidential information. If such a duty exists, then of course it will be necessary, in order to establish liability, to show a failure to exercise reasonable care. Hence it may turn out that the extent of such liability is similar to that of liability under the Data Protection Act.

On the other hand it is possible that an express term of the retainer could hold a professional to a standard higher than that required by the Act. In such a case, claimants are likely to pursue an action for breach of contract as well as under the Act.

Gathering personal data may also amount to an assumption of responsibility,[13] so that the gatherer will be liable in tort for negligently failing to protect that data, either to clients or, conceivably but probably rarely, to third parties.

(3) Breach of Confidence

This is a complicated subject on which various books have been written.[14] The extent of a professional's duty of confidence may depend on the nature of the profession, for instance it appears that solicitors have particularly stringent duties with regard to clients' information.[15] It may be that the touchstone of liability, once confidential information has been received, is unauthorised use of it by the professional. That might mean that a professional who lost a client's information due to a third party stealing it was not liable in breach of confidence.

Can Cyber-Liability Be Excluded?

Clients Acting in the Course of Business

Professionals are generally able to exclude or limit liability for their own negligence to clients acting in the course of their business, unless they are operating on their "written standard terms of business".[16] In the latter

[12] The ICO's publication, *Overview of the General Data Protection Regulation (GDPR)*, is a helpful starting point.
[13] Under *Hedley Byrne v Heller* [1964] principles.
[14] Eg Toulson & Phipps, *Confidentiality*, (3rd ed., 2012).
[15] In relation to solicitors, see ch.6 of Flenley & Leech, *Solicitors' Negligence and Liability* (3rd ed., 2013), which is written by Thomas Grant QC.
[16] Unfair Contract Terms Act 1977, s.3.

circumstance, any term excluding or restricting the professionals' liability for breach of contract will be subject to the reasonableness requirement set out in the Unfair Contract Terms Act 1977 ("UCTA").[17]

Given what is said above about the nature of cyber-liability and the prevalence of cyber-crime, it is plainly highly advisable for professionals at least to attempt to limit their liability.

Clients Not Acting in the Course of Business

Where a client is not acting in the course of his/her business, he/she will benefit from further statutory controls, which inhibit a professional's ability to exclude or limit liability consequent to a data breach to an even greater extent. Those statutory controls apply either under UCTA or the Consumer Rights Act 2015 ("CRA"). A full discussion of the differences between those two regimes is outwith the scope of this paper, but, in essence:

a) exclusion clauses within retainers agreed with consumers before 1 October 2015 are subject to the "reasonableness" test outlined in the Unfair Contract Terms Act 1977 and the "fairness" test set out in the Unfair Terms in Consumer Contract Regulations 1999 ("UTCCRs"); whereas

b) retainers agreed on or after 1 October 2015 are regulated solely by the CRA. S.57(1) of the CRA prevents altogether the total exclusion of liability and s.62 places a requirement of fairness, equivalent to that contained in the UTCCRs, on all terms in a retainer, including clauses limiting a professional's liability.

Under either regime, the following are likely to be highly relevant to any assessment of fairness or reasonableness:

a) the consumer's level of sophistication;

b) the lengths taken in order to bring the existence of the exclusion clause to the attention of the consumer;

c) the availability and cost of insurance against the risk.

For example, in *Marplace (No.512) Ltd v Chaffe Street*,[18] a firm of solicitors successfully limited their liability in negligence to £20m. The clause was found to have been reasonable for three reasons: first, because the claimant was a sophisticated and wealthy client; secondly, because the claimant was aware of the term and it had not been forced upon him; and thirdly, because the limit of £20m had been selected on appropriate commercial principles including the level of insurance cover available and its cost.

A court's analysis of an exclusion clause will, of course, be highly fact-sensitive. Professionals should therefore consider their need for an exclusion/limitation clause on a case-by-case basis where that is possible.

[17] In s.11.
[18] [2006] EWHC 1919 (Ch).

Claimants Who Are Not Party to a Retainer

Professionals frequently hold sensitive information relating not only to their clients but also to other individuals and entities, on whose behalf they are not instructed. In the absence of any contractual relationship, it is clearly impossible to exclude liability for losses suffered by those individuals and entities pursuant to a data breach. That said, it is possible that careful drafting may help in preventing the court from holding that a professional owed a duty to such third parties in the first place.

Conclusion

Cyber-liability poses significant risks to all professionals and consequently therefore to their insurers. There is great uncertainty as to the standard to which professionals will be held in their attempts to protect third parties' data, although we can expect clarification in the coming years. In particular, different considerations may apply depending on whether there is, or is not, a contract between the professional and claimant. In the meantime, attempts must be made to limit liability where the law permits.

APPENDIX

Two Examples of Possible Incidences of Cyber-Crime in relation to Solicitors, taken from the Solicitors Regulation Authority website

Fraudsters intercept solicitor-client emails to steal money

The following case illustrates why firms and clients should consider following up on unusual communications, using independent and established means.

Mrs A was being advised by XYZ Solicitors in the purchase of a buy-to-let property.

The day before she was due to send the purchase money to the solicitors, Mrs A emailed them to confirm details of the firm's bank account. She received two replies, both seemingly from her solicitor.

The first email contained the correct bank details. The second email, received minutes later, contained details of an account in the name of XYZ Solicitors but with a different bank. The email explained that the firm was having issues with their usual bank, and asked Mrs A to use their alternate account. This email was sent by fraudsters.

Mrs A called her bank and arranged for the funds to be transferred within 24 hours. She emailed the law firm to confirm this. This email, along with others sent by Mrs A and her solicitors, was deleted to prevent detection. The fraudsters also sent emails to both parties, assuring them that everything was fine.

Three days elapsed, during which time the fraudsters transferred the money abroad. They did this through several smaller transfers to avoid questions from their bank.

The fraud came to light only when XYZ Solicitors called Mrs A to find out what was happening. By the time the fraudsters' banking provider had been alerted, all the money was gone. Mrs A's bank refused to refund her as they had acted on her instructions, leaving her to bear the loss.

It emerged that the fraudsters had hacked into the firm's email server, possibly by taking advantage of an outdated anti-virus, internet browser or operating system. They had used a bank account in the name of the law firm to make the fraud appear legitimate.

Fraudsters instruct solicitor by pretending to be the client

The following case illustrates the importance of maintaining secure systems, and the harm that can arise to clients if firms fail to do this.

Miss A was acting for a client in the sale of a property. On the day the proceeds of the sale were to be paid into the firm's client account, Miss A received a message from her client's email address. It contained instructions to transfer the funds to the client after receipt, including details of a bank account in the client's name.

After the funds cleared into the firm's client account, Miss A transferred the funds as instructed.

The next day, the client called Miss A to ask whether the firm had received the proceeds from the sale. Miss A replied that the funds had been transferred to the client's personal account, as instructed in the email. However, the client denied emailing instructions to Miss A. They both contacted the bank to which the funds had been sent, only to be told that the funds had subsequently been transferred abroad.

It appeared from the firm's investigation that a fraudster had hacked into the client's email account and sent the instructions to Miss A, under the guise of being the actual client.

This was a sophisticated fraud which would have required knowledge of the identity of Miss A's client, the type of matter Miss A was dealing with, and the stage the matter had reached. The fraudsters may have obtained this information by using malicious software that allowed them access to the firm's systems.