FOIL
FORUM OF INSURANCE LAWYERS
IRELAND

Informing Progress - Shaping the Future

FOIL Ireland learning event

FOIL Ireland Learning Event – Cyber Risks – Claims and Coverage Landscapes

This talk was held on 30th November and was led by **Ronan Lupton SC**, who prior to entering the legal profession had spent 11 years in telecommunications and now practises mainly in media, commercial and chancery law.

The speaker presented a slide showing how full the news media is with items relating to cyber risks, cyber-crime and other cyber related issues. Within the past few days, this had included articles about the risks facing law firms and how things are changing, with regard to the pandemic and issues arising from working from home. In addition, the Law Society had issued an alert about phishing emails (emails purporting to come from a professional but intending to catch-out the unaware and permit the firm's network to be accessed). An example given was of a seemingly legitimate contract being sent through for signature. The issue is such that the Law Society is offering assistance on cyber risk to the profession.

A finding from a recruitment survey was of a higher sense of risk and sensitivity with working from home and facilitating it in a secure way. Many firms surveyed had experienced cyber-attacks. Cyber risk is recognised by firms as one of the major challenges over the next three years.

Forms of cyber interference

Incident vs. breach

We talk at length about incidents and breaches and we use the following definitions:

• **Incident:** A security event that compromises the integrity, confidentiality or availability of an information asset (a computer or a network). It may not result in a data breach.

• **Breach:** An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

Cyber security has its own vocabulary, commonly referred to as **VERIS resources.**

The terms "**threat actor**," "**action**" and "**varieties**" are referenced often in cyber incidents. Those terms are part of the **V**ocabulary for **E**vent **R**ecording and **I**ncident **S**haring (VERIS) a framework designed to allow for a consistent, unequivocal collection of security incident details. Here is how they should be interpreted:

- **Threat actor:** Who is behind the event? This could be the external "bad guy" who launches a phishing campaign or an employee who leaves sensitive documents in their seat back pocket.

- **Action:** What tactics (actions) were used to affect an asset? VERIS uses seven primary categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error, and Environmental. Examples at a high level are hacking a server, malware or influencing human behaviour through a social attack.

- **Variety:** More specific enumerations of higher-level categories, e.g., classifying the external "bad guy" as an organized criminal group or recording Hacking action as SQL injection or brute force.

The speaker's next slide illustrated form of cyber interference and explained the impact of social engineering; basic web application attacks; system intrusion; miscellaneous errors; privilege misuse; lost and stolen assets; denial of service; and 'everything else'.
Reference was made to the source of this material:

https://www.verizon.com/business/resources/reports/dbir/2021/masters guide/

The next slide illustrated patterns of cyber interference incidents over the period 2016-2020. The highest increase in the graph had been in denial of service; followed by basic web application attacks.

As regards data breaches, a similar slide showed a much higher volume of incidents, but denial of service dropped right down. Social engineering was top of this graph; followed again by basic web application attacks. Miscellaneous errors and system intrusion were also high on the graph, showing that it was lower-level members of staff who are using the system who may fall prey to cyber-attacks. This can soon attract the attention of the Data Protection Commissioner.

With Covid and working from home, new forms of threat have become more common, including phishing, ransomware and use of stolen credentials.

What are the risks to law firms and their clients?

Literally, any of the incidents already referred to: it is almost impossible to predict with certainty what form an incident or breach might take, but awareness is key.

Where is the value in a business: in client account; documentation; IP? Where does this all sit between civil and criminal liability? Some breaches have gone both to the civil courts and have resulted in criminal proceedings.

The constant players in cyber discussions are denial of service, basic web application attacks, lost and stolen assets, miscellaneous errors, privilege misuse and everything else continue to apply.

Types of cyber-attack which now seem less important than before include payment card skimmers, crimeware, cyber-espionage, and point of sale fraud.

The major problem areas are social engineering and system intrusion.

Two areas of particular interest on the frequency scale are:

Phishing: This continues to walk hand-in hand with use of stolen credentials in breaches as it has in the past. It is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Ransomware: These actors will first exfiltrate data. Then the data they exfiltrate they will encrypt so that they can threaten to reveal it publicly if the victim does not pay the ransom.

Two examples of cyber interference were then provided.

The first was of a seemingly genuine questionnaire inviting a company to join an EU business register. This resulted in invoices being sent to the account payable department of the company. There are many similar examples, including some being sent to individual, some elderly.

The second example had been sent by 'Credit Analyst' with an Xcel file attachment purporting to be confirmation of payment of an invoice. The currency was in US dollars, so the recipient knew it was suspect and no doubt opening the Xcel file would have injected a code into the recipient's network and cause some form of damage.

The speaker highlighted the current increase in phone fraud in Ireland, which was difficult to contain.

The forms of cyber-crime to be aware of

Cybercrime comprises:

• Traditional offences (e.g., fraud, forgery and identity theft);

• Content related offences (e.g., online distribution of child sexual abuse material, hate speech or incitement to commit acts of terrorism); and

• Offences unique to computers and information systems (e.g., attacks against such systems, spread of malware, hacking to steal sensitive, personal or industry data and denial of service attacks to cause financial and/or reputational damage).

• Electronic devices are also used to sell and transfer all sorts of illicit goods and services, from illicit drugs to online child sexual abuse and exploitation materials to lists of stolen credit card numbers.

What do you do?

Solicitor and Client:

• Report to Gardaí – The Garda National Cyber Crime Bureau

• Report to insurer – If appropriate cover in place

• Seek assistance from Law Society - cybersecurity@LawSociety.ie

• Cauterize the incident risk and/or breach

• Where a data breach has occurred, you must notify the DPC furnishing as much detail as possible (GDPR Art 33 contains a 72-hour requirement)

• Engage reputation management / PR consultants to deal with fall out

• Audit security and retain access logs

• Do not pay the ransom where ransomware attack is obvious, or contact has been made with you or the client.

Risk analysis

Staff training – at present, particularly about social engineering.

Policies – privacy and DP

Client profiles and awareness of client sensitivity to the security of their data

Office communications security

Cyber risk is currently very high and steps need to be taken, if not already in place. The Garda National Cyber Crime Bureau has published guidance on online conferencing: the four 'Ps'.

Passwords: change them and make them robust;

Payment: use secure methods;

Permission: limit permissions to trusted individuals/groups;

Participants: limit access by securing links.

Encryption can be used to secure communications.

Building cyber security

1. **Establish** governance and organisation (Deploy meaningful policies)

2**. Identify** what matters most (Assets, whether IP or actual cash)

3. **Understand** the threats (What Threat Actors are you dealing with?) – cyber criminals

4. **Define** your risk appetite (Define what cyber risk could most likely impact you/client?)

5. Focus on **education** and **awareness** (Employee, contractors, and third parties: who has access to systems?)

6. **Implement basic protections** (Anti-malware, up to date patching, MFA, Firewalls, logs)

7. Be able to **detect** an attack (Establish some form of security monitoring protocol)

8. Be prepared to **react** (Have a list of escalations and people to assist)

9. Adopt a **risk-based approach to resilience** (Establish recovery plans/secure back-ups)

10. Implement additional **automated protections** (MFA, Firewalls, Data Loss Prevention Systems)

11. **Challenge and test regularly** (Penetration test, simulate attacks)

12. Create a **cyber risk management** lifecycle (Make managing cyber risk 'business as usual').

Steps required: incident or breach

Triage – notify the relevant bodies and logically follow the process steps discussed above.

Consider having a Confidentiality Ring, allowing data to be looked at by third parties who may not be the company's regular vendors.

Notification planning - handling PR and the media.

Civil applications to the court (e.g., Norwich Pharmacal Orders, injunctive relief).

Precautions

Keeping the GDPR/DPA – ROPA (Record of Processing Activity) which is the first port of call in the event of a cyber breach and when contacting the regulator.

Engage a DPO in the event of a breach (already a requirement) to communicate with the regulator and others.

Actively use storage that is encrypted or that separates sensitive data from less sensitive data

Delete data that is no longer required

General Security, Data Protection and Privacy Policies (MFA, logs on, Firewalls, etc.).

Audit and Audit Frequency (at least twice or three times a year).

Automate, hire consultants or retain in-house staff to handle complex issues.

Legal obligations

GDPR/DPA

• High risk due to follow-on compensation action possibilities (see recent case law below)

• Fining potential - €10m or 2% turnover; €20m or 4% turnover (more sensitive categories)

• Frequent flier breaches:

• Article 5(1)(f) Integrity and confidentiality principle – breached

• Article 24(1) Responsibilities of data controllers – breached

• Article 32 Security of processing – breached

• Cybercrime Legalities

• Report the matter and seek 'early intervention' from law enforcement community.

The position of insurance – counsel's own view only

Experience suggests that cyber cover is costly and is difficult to obtain. Cover should not be conflated with crime cover.

• Cyber cover relates only to – **data**

• Crime cover relates only to – **money and theft**

There can be an overlap in these areas depending on the insurer

Ransomware appears to be an area where insurers are resiling from providing cover. Four New Square and HSE are small in the context of other cyber events (see below).

Case law

HSE Ireland

This was a ransomware attack. HSE announced that it had shut down its systems. The timeline was:

13 May 2021 suspicious activity detected

14 May 2021 HSE IT experts noticed deployment of ransomware software, from that point encryption had taken place

Demands made for payment [€20m reported, later reduced to 3 bitcoin €140k.]

Patient data leaked on dark web and published in redacted form by media (Financial Times)

20 May 2021 orders made against '*persons unknown*' restraining any processing, publishing, sharing or selling of stolen data – Cross J

23 June 2021 circa 70% of HSE network back operational

25 June 2021 orders made by O'Connor J against VirusTotal on an *ex parte* basis.

Fall-out

• Extreme reputational risk

• Risk to lives of patients

• A review of the State cybersecurity resources (NCSC) under Minister Ossian Smyth

• Follow-on action high likely from the DPC and at a guess an s.110 statutory inquiry (notification was made in time) with a financial penalty

• Follow-on actions unknown re. patient data compromised

Lesson**:** up to date software patching, operating systems and firewalls.

Four New Square - ransomware attack

• Access to client records – exfiltrate and encrypted

• Demands for payment; if not paid – publish records

• Proceedings taken against '*persons unknown*'

• Privacy Order Steyn J (July) Link:

https://www.judiciary.uk/judgments/new-square-limited-v-person-or persons-unknown-privacy-order/

• Judgment by Nicklin J. (injunctive relief) (September) Link:

https://regmedia.co.uk/2021/09/16/4squarejudgment.pdf

Doorstep Dispensaree

Doorstep Dispensaree primarily provide a pharmacy and medicines distribution service to care homes in the UK. As a result of a separate investigation into their operation by a UK medical authority it came to the ICO's attention that Doorstep Dispensaree had **stored some 500,000 documents relating to personal data in an open and unsecured courtyard**.

Many of the documents had sustained water damage.

On the 17 December 2019 the Information Commissioner's Office in the UK (the "**ICO**") issued its first penalty notice under the General Data Protection Regulation 2016 (the "**GDPR**"). Under the GDPR, the ICO carries out the same supervisory role in the UK as the Data Protection Commission carries out here in Ireland.

The notice issued against Doorstep Dispensaree, **as a data controller, amounted to a fine of £275,000 – approximately €325,000 – and was made on the basis of "*negligent rather than deliberate infringement*" of the GDPR on a number of grounds.**

The infringements made by Doorstep Dispensaree can be generally summarised as arising out of: -

• Failure properly to store medical information (which is special category data under the GDPR); and

• Failure to adopt an appropriate privacy notice.

British Airways

The attacker is believed to have potentially **accessed the personal data of approximately 429,612 customers and staff. This included names, addresses, payment card numbers and CVV numbers of 244,000 BA customers.**

Other details thought to have been accessed include the combined card and **CVV numbers of 77,000 customers and card numbers only for 108,000 customers**.

Usernames and passwords **of BA employee and administrator accounts as well as usernames and PINs of up to 612 BA Executive Club accounts were also potentially accessed**.

Failure to prevent the attack

There were numerous measures BA **could have used to mitigate** or prevent the risk of an attacker being able to access the BA network.

These included:

• limiting access to applications, data and tools to only that which are required to fulfil a user's role

• undertaking rigorous testing, in the form of simulating a cyber-attack, on the business' systems;

• protecting employee and third-party accounts with multi-factor authentication.

Outcome

The Information Commissioner's Office (ICO) has **fined British Airways (BA) £20m for failing to protect the personal and financial details of more than 400,000 of its customers.**

An ICO investigation found the airline was processing a significant amount of personal data without adequate security measures in place. **This failure broke data protection law and, subsequently, BA was the subject of a cyber-attack during 2018, which it did not detect for more than two months**.

ICO investigators found BA **ought to have identified weaknesses in its security and resolved them with security measures that were available at the time.**

Marriot

Marriott estimates that **339 million guest records worldwide were affected following a cyber-attack in 2014 on Starwood Hotels and Resorts Worldwide Inc**. The attack, from an unknown source, remained undetected until **September 2018**, by which time the company had been acquired by Marriott.

In 2014, an unknown attacker installed a **piece of code known as a `web shell' onto a device in the Starwood system giving them the ability to access and edit the contents of this device remotely**. This access was exploited in order to install malware, enabling the attacker to have remote access to the system as a privileged user. As a result, the attacker would have had unrestricted access to the relevant device, and other devices on the network to which that account would have had access.

Further tools were installed by the attacker to gather login credentials for additional users within the Starwood network. With these credentials, the database storing reservation data for Starwood customers was accessed and exported by the attacker.

The ICO acknowledged that Marriott acted promptly to contact customers and the ICO. It also acted quickly to mitigate the risk of damage suffered by customers, and has since instigated a number of measures to improve the security of its systems.

Outcome

The ICO **fined Marriott International Inc £18.4million** for failing to keep millions of customers' personal data secure.

Ticketmaster

The Information Commissioner's Office (ICO) fined **Ticketmaster UK Limited £1.25million for failing to keep its customers' personal data secure**.

The ICO found that the company failed to put appropriate security measures in place to prevent a cyber-attack on a chat-bot installed on its online payment page.

Ticketmaster's failure to protect customer information is a breach of the General Data Protection Regulation (GDPR).

The data breach, which included **names, payment card numbers, expiry dates and CVV numbers, potentially affected 9.4million of Ticketmaster's customers across Europe including 1.5million in the UK.**

Investigators found that, as a result of the breach, 60,000 payment cards belonging to Barclays Bank customers had been subjected to known fraud. Another 6,000 cards were replaced by Monzo Bank after it suspected fraudulent use.

The ICO found that Ticketmaster failed to:

• Assess the risks of using a chat-bot on its payment page

• Identify and implement appropriate security measures to negate the risks

• Identify the source of suggested fraudulent activity in a timely manner.

Mermaids Charity

The ICO found that an internal email group was created with insufficiently secure settings, **leading to approximately 780 pages of confidential emails to be viewable online for nearly three years.**

This led to **personal information, such as names and email addresses, of 550 people being searchable online**.

The personal data of **24 of those people was sensitive as it revealed how the person was coping and feeling, with a further 15 classified as special category data as mental and physical health and sexual orientation were exposed.**

The ICO's investigation found Mermaids should have applied restricted access to its email group and could have considered pseudonymisation or encryption to add an extra layer of protection to the personal data it held.

Outcome

The Information Commissioner's Office (ICO) has **fined transgender charity Mermaids £25,000 for failing to keep the personal data of its users secure.**

The ICO's investigation began after it received a data breach report from the charity in relation to an internal email group it set up and used from **August 2016 until July 2017** when it was decommissioned.

The charity **only became aware of the breach in June 2019**.

Scottish HIV

The breach of data protection law involved an email to **105 people which included patient advocates representing people living in Scotland with HIV. All the email addresses were visible to all recipients, and 65 of the addresses identified people by name**.

From the personal data disclosed, **an assumption could be made about individuals' HIV status or risk.** An ICO investigation of the February 2020 incident found shortcomings in the charity's email procedures. **These included inadequate staff training, incorrect methods of sending bulk emails by blind carbon copy (bcc) and an inadequate data protection policy.**

It also found that despite the charity's own recognition of the risks in its email distribution and the procurement of a system which enables bulk messages to be sent more securely, it was continuing to use the less secure bcc method seven months later.

Outcome

The Information Commissioner's Office (ICO) fined HIV Scotland £10,000.

Curry's/PC World DSG

An ICO investigation found that **an attacker installed malware on 5,390 tills at DSG's Currys PC World and Dixons Travel stores between July 2017 and April 2018, collecting personal data during the nine-month period before the attack was detected.**

The company's failure to secure the system allowed unauthorised access to **5.6 million payment card details used in transactions and the personal information of approximately 14 million people, including full names, postcodes, email addresses and failed credit checks from internal servers.**

DSG breached the Data Protection Act 1998 by having poor security arrangements and failing to take adequate steps to protect personal data. This included vulnerabilities such as inadequate software patching, absence of a local firewall, and lack of network segregation and routine security testing.

Outcome

The Information Commissioner's Office (ICO) has fined DSG Retail Limited (DSG) £500,000 after a 'point of sale' computer system was compromised as a result of a cyber-attack, affecting at least 14 million people.

There is a follow-on action for compensation in *Warren v DSG*: Saini J – remitting to lower court - https://www.bailii.org/ew/cases/EWHC/QB/2021/2168.html

Mr Justice Saini's decision in sets out in some detail the legal tests to assess negligence and breach of duty pleas which are arguably wholly misplaced in data breach cases.

***De minimis* claims**

Lately, several written decisions concerning GDPR/DPA data breach compensation cases [in the UK] have been remitted to lower courts based on *'de minimis'* assessment and rulings.

1. *Rolfe & Ors v Veale Wasbrough Vizards LLP* [2021] EWHC 2809 (QB) (07 September 2021) link: Rolfe & Ors v Veale Wasbrough Vizards LLP [2021] EWHC 2809 (QB) (07 September 2021) (bailii.org)

2. *Johnson v Eastlight Community Homes L*td [2021] EWHC 3069 (QB) (16 November 2021) Link: Johnson v Eastlight Community Homes Ltd [2021] EWHC 3069 (QB) (16 November 2021) (bailii.org)

Follow-on Claims

Follow-on compensation claims – of note:

• *Lloyd v Google* – Leggatt LJ (10 November 2021): Lloyd v Google LLC [2021] UKSC 50 (10 November 2021) (bailii.org)

Two points emerge:

• Indication of position re. class actions under GDPR

• Requirement to plead / show loss and damage to claim compensation. Order 15 Rule 1 RSC ("*the same transaction*") is narrower in scope than Rule 19.6 CPR ("*the same interest*") (the narrowest procedure in Lloyd) and that in *Greffrath*, O'Moore J properly declined to broaden O.15, R1, so that it can't reach R19.6CPR. Interesting from a class action point of view. Link: Greffrath & ORS v Greymountain Management Ltd (In Liquidation) & ORS. (Approved) [2020] IEHC 284 (12 June 2020) (bailii.org)

Follow-on Claims Ireland

Follow-on compensation claims – of note:

• *Collins v FBD Insurance plc* (High Court – Feeney J): Collins -v- FBD Insurance Plc [2013] IEHC 137 (14 March 2013) (bailii.org)

• *Murphy v Callanan* (Supreme Court – Baker J): Murphy v Callanan & others [2013] IESC 30 (19 June 2013) (bailii.org)

• *Shawl Property Investments v A & B* (Court of Appeal – Whelan J *obiter* strict liability "*it is necessary to have regard to the principle of proportionality in evaluating claims for breaches of* [the GDPR]" par 133): Shawl Property Investments Ltd v A. and B. (Unapproved) [2021] IECA 218 (30 July 2021) (bailii.org)

Áine Davis – AON

Insurers are aware of what is happening and how it is happening and they are working very hard to stay ahead of those threat factors. Everyone is feeling the impact of this type of activity. Attacks can last for months or years, with the attackers choosing their moment. It is crucial in the event of an attack to follow the steps outlined by the previous speaker. The last thing to do is just pay a ransom, without getting help. It has to be borne in mind that the cyber attacker will still have the stolen data and the regulator must be made aware of this.

Insurers are learning more every day and are paying multi-million-euro claims.

The insurer's involvement starts at first response, when the attack on the system is notified. The insurer's cyber experts will immediately become involved and give advice, looking at all aspects of the incident. They then assist to manage the claim, mitigate the loss and get the company back up and running.

Given the nature and frequency of cyber-attacks, insurers are becoming more cautious. They want to see that anyone to whom they provide cover has taken all steps possible to minimise the risk of an attack succeeding. Proposal forms will ask a very large number of detailed questions (the speaker had seen 180 asked), as it is now a very in-depth process. Insurers are also likely to carry out permissible scanning of a proposer's systems.

There has been a 400% increase in ransomware activity in the last two years. Cyber-attacks are now at the top of the list of companies' concerns, having displaced Brexit. The impact of Covid and the move to working from home has provided an ideal opportunity for cyber-attackers: members of staff who never used IT were suddenly at least using email.

Cyber liability insurance can definitely assist but insurers will wish to ensure that a company has invested in its IT infrastructure before providing cover. Outside of the presentation, the speaker is happy to provide further information to anyone who contacts her.

Q&A

From the point of view of a firm of solicitors, the Four Square case (barristers' chambers) was of particular concern and suggested that in the event of a claim the focus might be on whether there had been negligence. Is having a competent outside consultant to review IT systems a way to reduce that risk?

Ronan Lupton agreed with that proposition: there is a difference between inadvertence and negligence. This includes checking on how third parties with whom a firm deals are handling data and making sure devices are encrypted. The larger the firm, the greater the risk of breaches, because there are more people.

Áine added that however robust a system may be, there was always the risk of someone pressing a button an infecting the whole system and creating a data breach. It might, however, mitigate the penalty if, otherwise, everything had been done right.

Ronan; it is often human error that permits an attack but this may be by someone in IT not doing their job, to a very junior member of staff making a mistake.

Áine confirmed that the standard professional negligence insurance policy will not pick-up on most cyber claims and in reality, a stand-alone policy is required. However, this dovetails with cover for crime.