



Cyber & Data Liability – An Insurance & Risk Management Overview

Presentation to LUPC & SUPC – 30th April 2020



Insurance | Risk Management | Consulting

Agenda

- Current major factors and trends
- Risk analytics - 'How do you measure your exposure?'
- Outline of the insurance contract and how it operates
- Case Studies

Overview of GDPR Regulations

- **Fines:** 4% of annual global turnover or EUR 20M (whichever is greater)
- **Privacy by Design:** inclusion of data protection from the onset of the designing of systems
- **Consent:** Consent must be freely given, specific, informed and unambiguous
- **Breach Notification:** 72 hour mandatory notification
- **Right to be forgotten:** data erasure








GDPR
General Data Protection Regulation

Insurance market response to GDPR

- Affirmative endorsements explicitly listing GDPR language within policy forms
- It is insurers intention to provide coverage for ICO penalties
- Policies will cover costs relating to defending any such investigation. It remains to be seen whether GDPR fines will be insurable or not, as this will be a matter of insurance/national law, and not down to the ICO.

Industry and sector statistics

Recent surveys support the above and demonstrate that increased on-line activity and reliance and use of data.

-  According to official figures, the public sector, which includes higher education, accounted for 43% of compromised data records over the last two years; a five-fold increase over 2014
-  Almost all universities (87%) have experienced at least one successful cyber attack
-  Over a third (36%) of UK universities are blighted by a successful cyber attack each hour.
-  83% believe cyber attacks are increasing in frequency and sophistication
-  43% have had student data attacked, including dissertation materials and exam results
-  25% have experienced critical intellectual property theft
-  28% have had grant holder research data attacked

Covid-19

Although we're still in the early stages, this global pandemic is changing the way we work, creating various threats and exposures

- Movement towards company wide remote working, with increased use of technology and reorganisation of staff
- Increase in phishing and “watering hole” attacks
- Business Continuity Plans are being put to the test
- Reorganisation of staff and responsibilities
- Increase in 3rd party engagement (NHS, delivering services)

2019 / 2020 claims

Capital One

Data Breach of
over 100M US &
Canadian clients¹

ICO fines¹

- British Airways: £183m
- Marriot: \$123m

Virgin Media

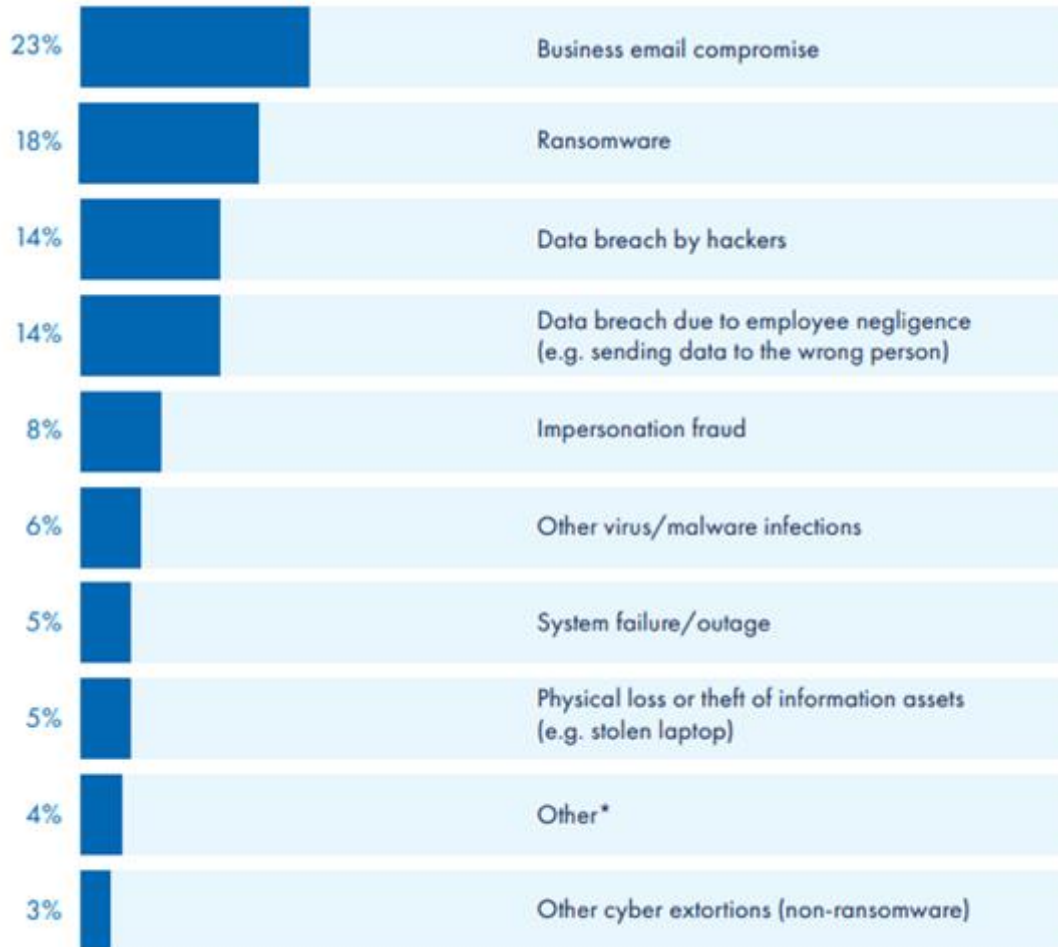
900,000 records
breached due to
simple human error¹

Sharp uptake in Ransomware claims internationally in 2019²:

- Bitpaymer and Ryuk strands (both highly targeted – demand larger ransoms)
- Sodinokibi – single attack can create hundreds of small business victims
- Large Currency Company – £2m paid in ransom, forensics and legal costs still building, BI costs will be in the millions
- Since Jan – over \$750k in Ryuk ransomware payments

Sources: ¹www.bbc.co.uk ²www.coveware.com

What is the cause of claims?



*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

Source of graph: <https://www.aig.co.uk/content/dam/aig/emea/regional-assets/documents/aig-cyber-claims-2019.pdf>

Malware / Ransomware

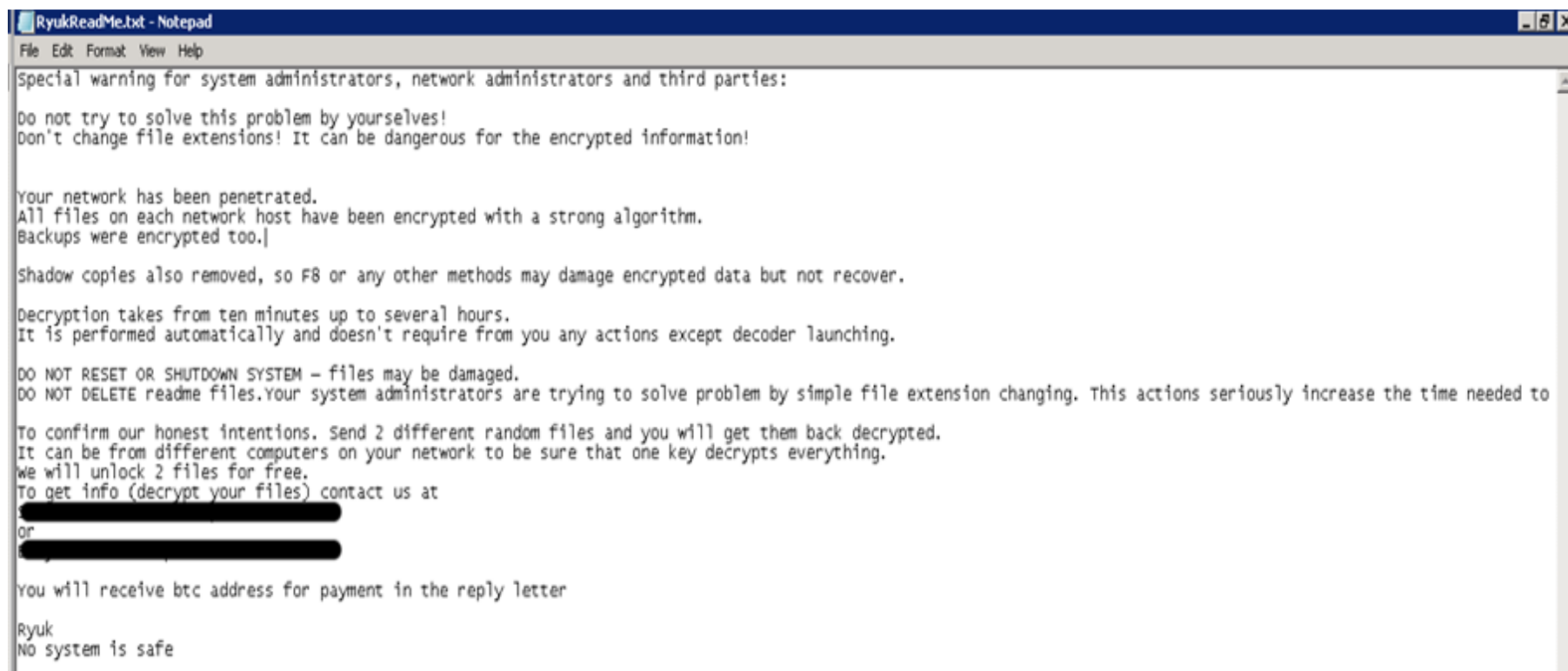
What is Malware?

- Malware is an umbrella term for all software or code which is created with malicious intent
- **Malicious Software** = Malware
- Malware includes - viruses, bugs, worms, bots, spyware, adware, Trojans, and... Ransomware

What is Ransomware?

- Ransomware is a sub-set of Malware which is designed to target individuals or organizations
- Ransomware locks access to systems or files by encrypting them
- Attackers then demand a Ransom to provide a decryption key to grant access back to the victim
- Ransoms are typically demanded in cryptocurrencies such as Bitcoin, as they are almost impossible to trace

Malware / Ransomware



```
File Edit Format View Help
Special warning for system administrators, network administrators and third parties:

Do not try to solve this problem by yourselves!
Don't change file extensions! It can be dangerous for the encrypted information!

Your network has been penetrated.
All files on each network host have been encrypted with a strong algorithm.
Backups were encrypted too.]

Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

Decryption takes from ten minutes up to several hours.
It is performed automatically and doesn't require from you any actions except decoder launching.

DO NOT RESET OR SHUTDOWN SYSTEM - files may be damaged.
DO NOT DELETE readme files. Your system administrators are trying to solve problem by simple file extension changing. This actions seriously increase the time needed to

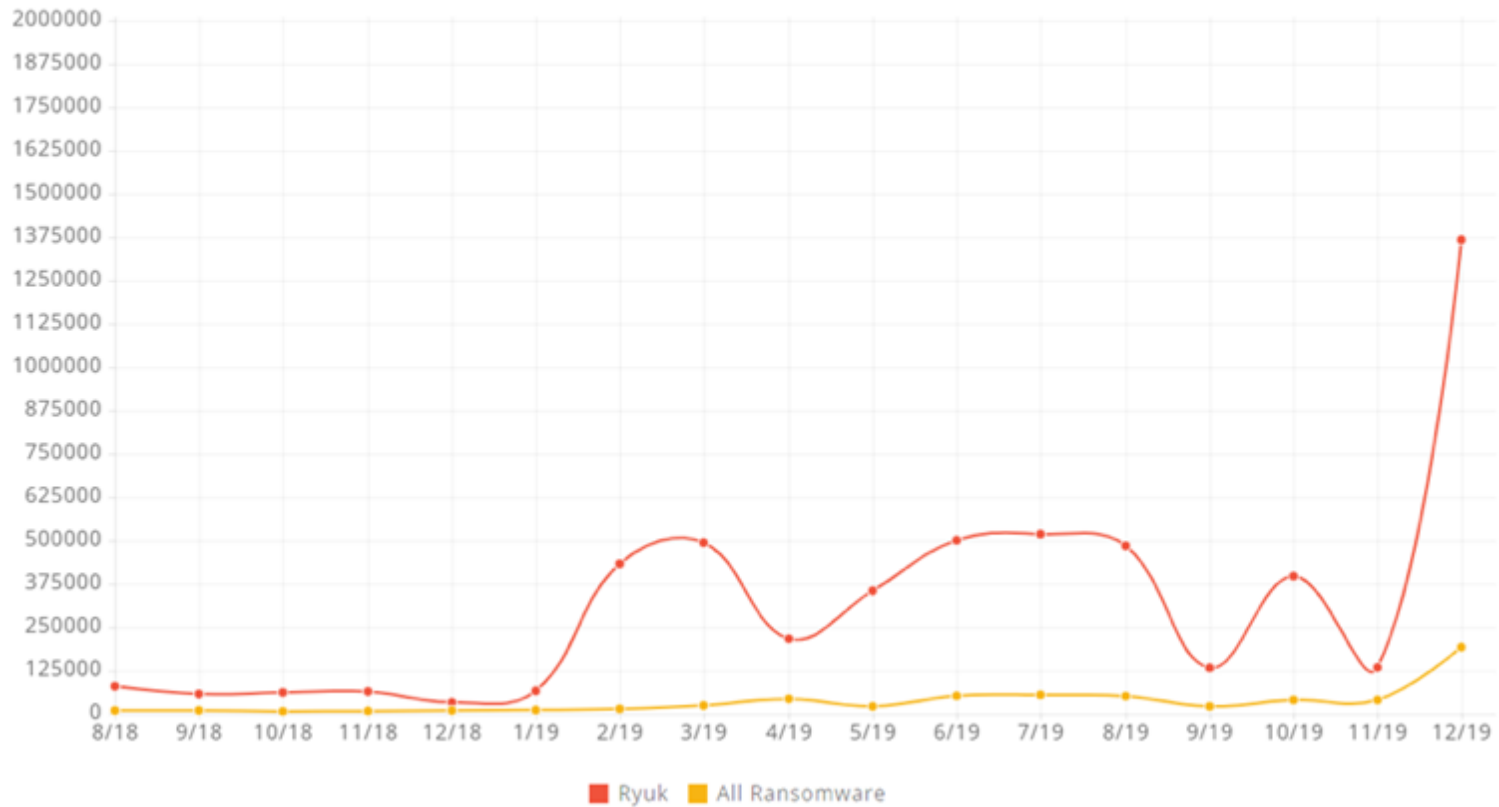
To confirm our honest intentions. Send 2 different random files and you will get them back decrypted.
It can be from different computers on your network to be sure that one key decrypts everything.
we will unlock 2 files for free.
To get info (decrypt your files) contact us at
[REDACTED]
or
[REDACTED]

You will receive btc address for payment in the reply letter

Ryuk
No system is safe
```

Malware / Ransomware

RYUK RANSOMWARE: RANSOM AMOUNTS



Source of graph: <https://www.coveware.com>

Risk analytics

How do you measure your exposure?

- An effective and tested Incident Response Plan
- An understanding and management of Data sets
- (Where is data stored/how is it protected/who is authorised to access it?)
- An effective and tested Business Continuity Plan/Disaster Recovery Plan
- Staff training and demonstration of Privacy Policy
- Are your networks secure:- demonstrable from Internal and external pen testing?
- Are Firewalls in place?
- Does the organisation run up-to-date antivirus?
- A good understanding of how your Sensitive Data is secured.
- Is sensitive data encrypted when removed from your premises?
- Are you aware of key outsource service providers and what contracts are in place to indemnify you?
- Do you take credit card payments and is the business PCI compliant?

Aside from the above how is risk managed within your Company?

What is Cyber & Data Liability Insurance?

- Cyber insurance covers the liabilities and losses arising out of the collection of Personally Identifiable Information/Confidential Corporate Information or the damage to networks, systems and databases.
- Policies generally include significant assistance with the incident, which can be essential when faced with reputational damage or regulatory enforcement.
- The term “cyber” implies coverage only for incidents that involve electronic hacking or online activities, when in fact this product is much broader, covering private data and communications in many different formats – paper, digital or otherwise.

What is Cyber & Data Liability Insurance?

- Generally, cyber and data risks fall into first party and third party exposures

Breach response =
panel of experts available
to policyholders

- Breach response lawyers
- IT forensics consultants
- Notification providers
- PR consultants

First party =
your own costs/concerns

- Business interruption
- Extortion from malicious 3rd parties
- Breach response costs

Third party =
litigation from third parties

- Defence costs and damages
- Regulatory costs
- Media liability

Breach Response Costs

SECTION A CYBER LIABILITY



BREACH RESPONSE COSTS

A data breach is the loss, theft or compromise of data. Our cyber policy will cover costs such as notifying your affected customers; offering credit monitoring; setting up call centres for concerned customers; bringing in forensic teams to identify the reason for the data breach; and potentially removing the hacker – or the virus/malware – from your systems.

REAL-WORLD EVENT:

- The insured discovered that an unidentified third party had uploaded files to their system, which allowed them to corrupt the insured's information files.
- Data obtained included private, personally identifiable information, including credit card information.
- The third party made fraudulent charges on multiple accounts.
- The insured was required to notify the affected individuals. Given the discovery of the fraudulent charges, the insured offered affected individuals an opportunity to obtain credit monitoring.
- The insured also wanted to manage the breach in the media to demonstrate decisive, responsible action so a public relations expert was brought in to assist.

The costs related to all of the above were covered under the Breach Response Costs section of the policy.

Regulatory Defence Costs

SECTION A CYBER LIABILITY



REGULATORY DEFENCE COSTS

These are the legal costs incurred to comply with any regulatory action taken against you following a data breach.

REAL-WORLD EVENT:

- An insured healthcare provider misplaced multiple drives that contained personal healthcare information for over one million patients.
- It was unknown whether the drives were lost, stolen or destroyed. The insured was required to notify the affected individuals, as well as the department of Health and Human Services (HHS).
- HHS opened an investigation into the incident and fined the insured healthcare provider for failing to protect the information.

Cover under this section paid for the legal fees incurred by the Insured in connection with responding to the HHS investigation and inquires. It also provided coverage for the fine assessed and imposed by HHS.

Security and Privacy Liability

SECTION A CYBER LIABILITY



SECURITY AND PRIVACY LIABILITY

This covers your liability in the event you suffer a data breach and you find yourself sued by affected customers or employees. This includes theft or altering of data, virus or malware, denial of service and other loss of data from your systems.

REAL-WORLD EVENT:

- An insured boutique retailer emailed a group of customers to promote a sale with special discounts.
- Intending to attach a copy of the flyer detailing the discounts, the insured instead attached a copy of a spreadsheet that contained a customer list, including customer names, addresses and credit card information – an easy mistake to make.
- The insured was required to notify all affected customers of the error and offer credit monitoring. The costs for this were covered under the Breach Response Costs section of the policy.

Several of the affected individuals filed a lawsuit against the insured and cover for legal costs and indemnification was provided for the insured under the Security and Privacy Liability section of the policy.

Cyber Extortion

SECTION A CYBER LIABILITY



CYBER EXTORTION

These are the costs you may incur should a hacker steal data from your systems and then demand a ransom to avoid leaking the information. The software tool the hacker uses in this case is called 'ransomware'.

REAL-WORLD EVENT:

- A small healthcare clinic discovered that an unauthorised third party had gained remote access to a server that contained electronic medical records.
- The third party posted a message on the server stating that the information on the server had been encrypted and could only be accessed with a password that would be supplied if the insured made a ransom payment.

The insured worked with law enforcement and determined that the payment should be made. The payment constituted Cyber Extortion Monies under the policy and the sum was reimbursed.

Multimedia Liability

SECTION A CYBER LIABILITY



MULTIMEDIA LIABILITY

This covers your liability in the event you are sued as a result of information provided within your multimedia channels – for example on your website, Twitter feed or Facebook page. Typical examples would be breach of copyright, libel or slander, plagiarism or defamation.

REAL-WORLD EVENT:

- The insured began a blog to share information to customers and the public. It's a common thing.
- The blog page contained a logo/image that was similar to a design that had been copyrighted by another party.
- The other party sent a 'Cease & Desist' letter to the insured demanding that they remove the image from the blog.

Discussions between the parties failed and the other party resorted to law. Costs were covered for breach of copyright under the Multimedia Insuring Clause in our policy.

Cyber Business Interruption

SECTION B CYBER BUSINESS INTERRUPTION



CYBER BUSINESS INTERRUPTION

(DEPENDENT BUSINESS INTERRUPTION INCLUDED)

1. Cyber Business Interruption

- Business interruption is the income a business can lose as a result of a network disruption to the insured's systems.
- Many companies now outsource business critical IT processes like card payment processing or data storage.
- To make sure such events are covered we have written dependent business interruption into our cyber insurance cover.
- This indemnifies the insured customer for loss of income due to a vendor, such as a payment processor, suffering a service outage due to network disruption.

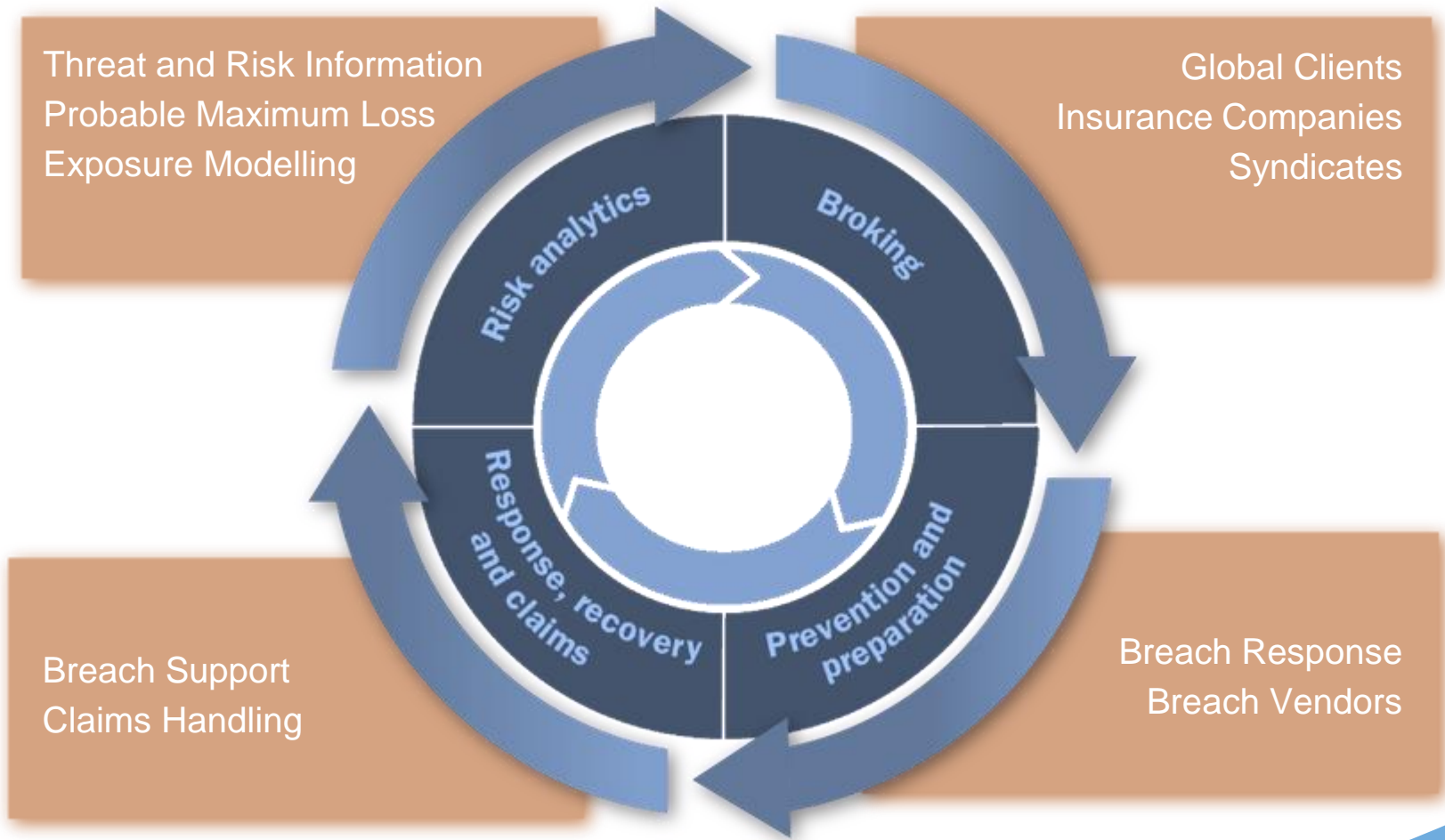
2. Digital Asset Restoration

This covers the costs incurred by the insured to restore affected data – called 'Digital Assets' in the trade – after a breach event or if security is compromised.

3. Cyber Reputation Business Income Loss

This covers earnings loss due to the loss of current or future customers within 12 months from a data breach or network interruption event.

Overview of underwriting requirements and rationale



Examples



Example 1: Ransomware

- US higher education institute became aware of infection of both RYUK Ransomware and TrickBot trojan malware
 - N.B. TrickBot and Emotet malware are precursors to RYUK, so always take immediate action if these variants of malware are detected
- RYUK Ransomware demand was for over \$4m
- Client engaged with Crypsis for IT Forensics
- Fortunately the client had adequate backups and was able restore the majority of systems without paying the ransom
- However – incurred over \$800k of expenses already

HEI Example 2

What happened?

By chance, the Insured became aware of suspicious files contained on a web-server. The client retained forensic IT experts to conduct an investigation following which it was identified that the server had been compromised with a number of Web Shells and access had been obtained from a variety of IP addresses.

Based on the outcome of the forensic findings, the Insured sought legal advice in respect of its reporting obligations.

What was the outcome?

The webserver was connected to a data base that hosted the university's events booking system. The bookings dated back many years and related to a wide variety of bookings, from sports pitches to concerts.

Fortunately, there was no evidence that the data had been accessed or exfiltrated despite the Web Shells being present. On this basis, the legal representatives were able to advise the client that there was no breach and therefore no legal liability.

HEI Example 2

Breakdown of costs

Involvement of Forensics and Legal Advice.

Forensic IT consultant had been retained and was on site for over a week to review the breach and report findings.

Daily rate of £5k comes to costs incurred of £30k

Legal experts retained for over two weeks to advise the Insured on methods for response and liability

Retention and costs incurred totalling of £20k

Total 1st Party Costs incurred to the insured £50k

HEI Example 3

What happened?

The webserver was connected to a data base that hosted all the university's events booking system and details of union membership groups. The bookings dated back many years and related to a wide variety of bookings, from sports pitches to concerts.

Unfortunately , there was clear evidence that the data had been accessed or exfiltrated by the hackers but it was unclear on the exact details and volume of data lost.

On this basis, the legal representatives appointed are retained to advise the Insured on how to handle the breach and potential legal liability.

What type of data was affected?

To establish this the IT Forensic firm retained by the Insured are required to stay on site for a longer period of time. The report and conclusion take over two weeks to conclude at a cost incurred of £50k.

After a deep dive it becomes apparent that records for over 150,000 past and present students have been lost including details of personal email, payment methods, interests/hobbies, and union membership groups.

HEI Example 3

Notification obligations

- GDPR - Mandatory notification to the ICO within 72 hours
- Established that you must notify the affected individuals:

What are you going to say?

The appointed Legal representatives assist the Insured to produce an FAQ sheet, including an answer as to what, if any, compensation/ID theft protection will be offered. At this stage, the university has to grapple with the questions over why they had the old data.

How will you tell the data subjects?

Email can end up in junk email folders or worse be spoofed so it is advised to use traditional mail. The legal representatives assist the Insured to draft letters and a PR firm is appointed to co-ordinate the campaign including the 80p/letter costs. That's £120,000 in one go in one week for just the notification.

HEI Example 3

How do people get more information?

As a result of the letter correspondence there is a frequent or significant outlay of staff to accommodate the increased number of queries coming into the University.

There are scenarios where a call centre is required but in this scenario the University are capable of routing calls via a specific reception/admin team.

What are you liable for?

The loss of information is, in some cases, deemed emotionally distressing and the University is sued by individuals for the harm caused.

The scenarios derived from the information lost that links students to specific Unions or membership groups. For example a student may not wish to have details of their membership to the LGBTQ group breached and a lawsuit citing emotional distress is plausible.

What Regulatory fines will you incur?

After investigation by the ICO the university is viewed as having handled the claim in an effective and responsible manner but is nonetheless guilty of negligence in the first instance.

A fine of £90k is administered by the ICO.

HEI Example 3

Breakdown of costs

1st party costs

The Breach Response services provided by legal representatives over the course of the months following the claim equate to over **£40k** in legal fees.

The forensic team retained comes to costs of **£50k** in fees.

£120,000 in costs to provide notification letters to those affected.

ICO fines at **£90k**

Total 1st party costs **£300k**

3rd party costs

The liability associated to the emotional distress outlined takes longer to settle but the legal fees in defence incurred are clear. This can cost above **£500** an hour to retain a Partner in Privacy law at a leading firm.

Assuming there are over 1000 plaintiffs in a group litigation order aiming for **£2000** in minimum compensation Insurers could place a maximum loss reserve on the claim of **£2M** awaiting the outcome. This is without allocating costs incurred in legal fees.

Thank you!

Any questions?

Phil Webster
07717 802518
phil_webster@ajg.com

Education Practice
Station Square
One Gloucester Street
Swindon, SN1 1GW



Gallagher

Insurance | Risk Management | Consulting