Cyber Insurance: Global developments, claim examples and limitations on coverage

Shabnam Karim, Senior Associate, Clyde & Co LLP

27 February 2018

Introduction

Overview of presentation

1. Putting cyber insurance into context; the environment in which businesses operate globally and locally
2. Global and local claim examples
3. The basis of liability relating to cyber/ data breach in the UAE
4. Cyber Insurance: Key issues and considerations in cyber policies
   - *Business interruption*
   - *Cyber extortion*
   - *Cloud service providers*
   - *Physical damage*

Setting the context; the environment in which businesses operate

The increased threat of data and breaches and cyber attacks

- Increase in data stored electronically/ digitisation of assets; move away from paper, including regional hospital records
- Increased globalisation/ complexity of operation; i.e. data stored in multiple jurisdictions; possibly with outsourced providers
- Big organisation can be a hodgepodge of technologies; some dated software and some new; both potentially insecure
- Smart devices/ the Internet of Things
- More sophisticated hackers and state-sponsored attacks

Setting the context; the environment in which businesses operate

How are businesses being targeted?

- Point of sale intrusions (malware into a retailer's credit card processing system, credit card information then sent outside of the network)
- Disgruntled or former employees (See the Morrisons' example where employee personal details were posted online)
- Insider misuse of passwords or privileges
- Loss or threat of encrypted devices
- Software vulnerability attacks (exploiting a security hole to install malware)
- Phishing attacks/ employee negligence
- Ransomware
- Distributed denial of service attacks

Setting the context; the environment in which businesses operate

Who are the biggest global targets?

Verizon DBIR (2016 data breach investigation report

– Professional services firm

– Healthcare

– Finance

– Retail

– Small businesses

Recent Claim examples- Global

1. **WannaCry Attack**
2. **NotPetya Attack**
3. **California hospital; malware which encrypted patient records**
4. **Equifax breach**
5. **Uber hack- data stolen of 57 million customers (made public in November 2017)**

Recent Claim examples- Local

Data and statistics not commonly available

1. Cyber criminals stole almost DH 4 billion from victims in the UAE in 2017 (Norton security insights report)
2. Saudi petrochemical plant a victim of the Triton hack in 2017; hackers gained control to a safety shut off system
3. Cyber attack in Saudi disrupting government computers
4. Khalifa Bin Salman Port in Bahrain; operations of terminal disrupted in June 2017
5. Saudi Aramco- historic
6. Bank of Muscat- historic
7. Gulf Air – facebook page hacked by political activists

Statistics for the UAE

- In 2015, Dubai Police received 1,011 reports of cyber crimes totalling losses of more than AED 40.5 million
- UAE 8th most targeted country globally and 1st in MENA for spear-phishing (Gulf News September 2017).
- 2nd most targeted country in MENA for ransomware attacks
- SME organisations in the UAE are more vulnerable to attacks and targeted repeatedly for spear-phishing attacks- Symantec's Internet Security Threat Report

An overview of relevant laws in the UAE

No specific privacy laws, but general laws apply:

- UAE constitution, Article 31: general concept of privacy
- UAE Penal Code, Article 378: offence to publish news, pictures or comments pertaining to the secrets of a person's private or family life
- UAE Penal Code, Article 379: offence to disclose a secret that you are entrusted with, by reason of your "profession or craft"
- DIFC Data Protection Law 2012; breaches may attract fines between USD 5,000 and USD 25,000
- Impact of GDPR; comes into force 25 May 2018

An overview of relevant laws in the UAE

UAE Cyber Crimes Law (Federal Law No 5 of 2012, as amended)

- First comprehensive cyber law in the Middle East
- Imprisonment and/or Fines for acts such as hacking for changing, copying, deleting, disclosing and publishing any data/ information obtained illegally; imprisonment of at least six months and/or a fine of not less than AED 150,000 and not more than AED 750,000;
- Fines and/or Imprisonment for financial cyber crimes (such as accessing credit card details/ bank accounts)

Liability imposed on management

- Civil Code provisions on vicarious liability for acts of employees
- Companies Law; duties of directors
- Criminal/police complaints against management individuals?

Cyber Insurance

Introduction

- Lloyds Emerging Risks Report 2017: The global cyber market is worth between USD 3 - 3.5 billion; by 2020, some estimate it could be worth USD 7.5 billion;
- Demand for cyber insurance anticipated to increase penetration globally when GDRP comes into force
- AON Benfield 2016 report estimates that 85% of premium is for US risk

Cyber Insurance

Key coverage considerations

- **Data breach costs** (hiring IT forensics, legal representation, notification costs. PR consultants, credit monitoring costs and call centre services)
- **Business Interruption**

  Example wording:

  "We shall indemnify you for income loss and associated extra expense, in excess of the Retention, incurred during the period of restoration as a direct result of the total or partial interruption of your network for a period longer than the waiting period caused by a network security breach first discovered by you and notified to us during the policy period or any Extended Reporting Period, provided that such network security breach first occurs on or after the retroactive date."

Business interruption

Triggers for cover and issues that may arise:

- “Income loss” and “associated extra expenses”
- “Incurred during the period of restoration”
- “direct result of the total or partial interruption of your network”- *note no cover for BI events caused by service providers*
- “for a period longer than the waiting period”- *common for a waiting period for coverage to trigger*
- “caused by a network security breach”- *are network outages due to internal errors and omissions covered or must the threat be from an external* actor?

Cyber extortion

There is usually cover for this; ransomware is common in the UAE

Example wording:

"Extortion Loss means any:

(i) monies paid by an Insured with the Insurer's prior written consent to prevent or end an Extortion Threat; or

(ii) Professional Fees for independent advisors to conduct an investigation to determine the cause of an Extortion Threat."

"Extortion Threat means any threat or connected series of threats, for the purpose of demanding monies, communicated to the Insured to prevent or end a Security Threat."

Cyber extortion

Issues that may arise:

- Subject to insurers' prior approval
- Could the affected system be remediated for a lesser amount than the demand?
- Could remediation be achieved without payment of ransom?
- Payment in crypto currency
- Could a ransom payment be terrorist financing? Under UK legislation, if the victim of the cyber attack knows or reasonably suspects that the attackers are linked to terrorism then payments to these attackers illegal.

Cloud service provider hack?

Who could be affected by a cloud service provider outage? Agregation considerations?

- The cloud service provider
- Customers of the cloud service provider
- Customers of the customers in the form of service interruptions coming from the impaired servers

Possible secondary effects?

- Property damage or loss of life where life critical functions were hosted in the cloud, such as healthcare records or alarm systems
- Knock-on business effects; e.g. online news provider was impacted when customers didn’t get their news, paid advertisers lost visibility
- Could companies whose services are heavily reliant on cloud service providers be sued by customers/ investors?

Physical damage exclusion

Some policies exclude bodily injury and property damage

Example wording:

“"Bodily Injury and Property Damage any:

(i) physical injury, sickness, disease or death; and if arising out of the foregoing, nervous shock, emotional distress, mental anguish or mental injury, other than mental anguish or mental injury arising from any breach of Data Protection Legislation by the Company; or

(ii) loss or destruction of tangible property, other than Third Party Data, or loss of use thereof, or the physical theft or loss of the Company’s Assets"

Physical damage exclusion

Issues that may arise:

- German steel mill – cyber attack on the network led to physical damage
- Use of smart devices; pacemakers could be tampered with;
- Mobile Apps providing GPS tracking for hikers could leave hikers stranded
- Hackers have demonstrated their ability to hack car washes, manually controlling the machinery with the ability to crush a car
- Does your CGL Policies cover this instead or is there a cyber exclusion to that?

Questions?

Shabnam Karim

Senior Associate | Clyde & Co

Direct Dial: +971 4 384 4373

PO Box 7001 | Rolex Tower | Sheikh Zayed Road | Dubai, UAE

Main +971 4 384 4000 | Fax +971 4 384 4004 | www.clydeco.com

CLYDE&CO

375
Partners

2000
Legal professionals worldwide

3600
Total Staff

50+
Offices in 20 countries