

# **Paragon International Insurance Brokers**

## **Protecting the Crown Jewels**

**Expert Forum on Cyber Risk: Reducing Vulnerability to attack  
29<sup>th</sup> January 2016**



# Protecting the Crown Jewels

## Agenda

- What is cyber risk?
- How damaging can cyber risk be to a company?
- How do insurers rate cyber risk?
- What are insurers looking for in terms of cyber risk management

# Introduction

## Paragon International

- Largest independent Cyber Practice in London
- Work with Retail Brokers and Direct Clients
- Commercial, Financial and Professional service firm clients
  - Open Market
  - Facility
- Worked on Largest Cyber Placement in WorldWide Market
- Placed in excess of USD50m in Cyber GWP to London in 2015
- 114 Cyber claims/incidents handled this year

# What is Cyber?

## Depends Who You Ask...

- CYBER is a PREFIX Relating to...
  - Electronic Communication, Networks and Virtual Reality
- CYBER also means...
  - Privacy / Data Breach Insurance
    - Liability to Others
    - Privacy Regulatory Response
  - Security Breach Insurance
    - Liability to Others
    - Network Continuity
      - Data reconstruction, BI, Increased Cost

# Cyber Risk – Not Only a US Risk

TalkTalk

vtech

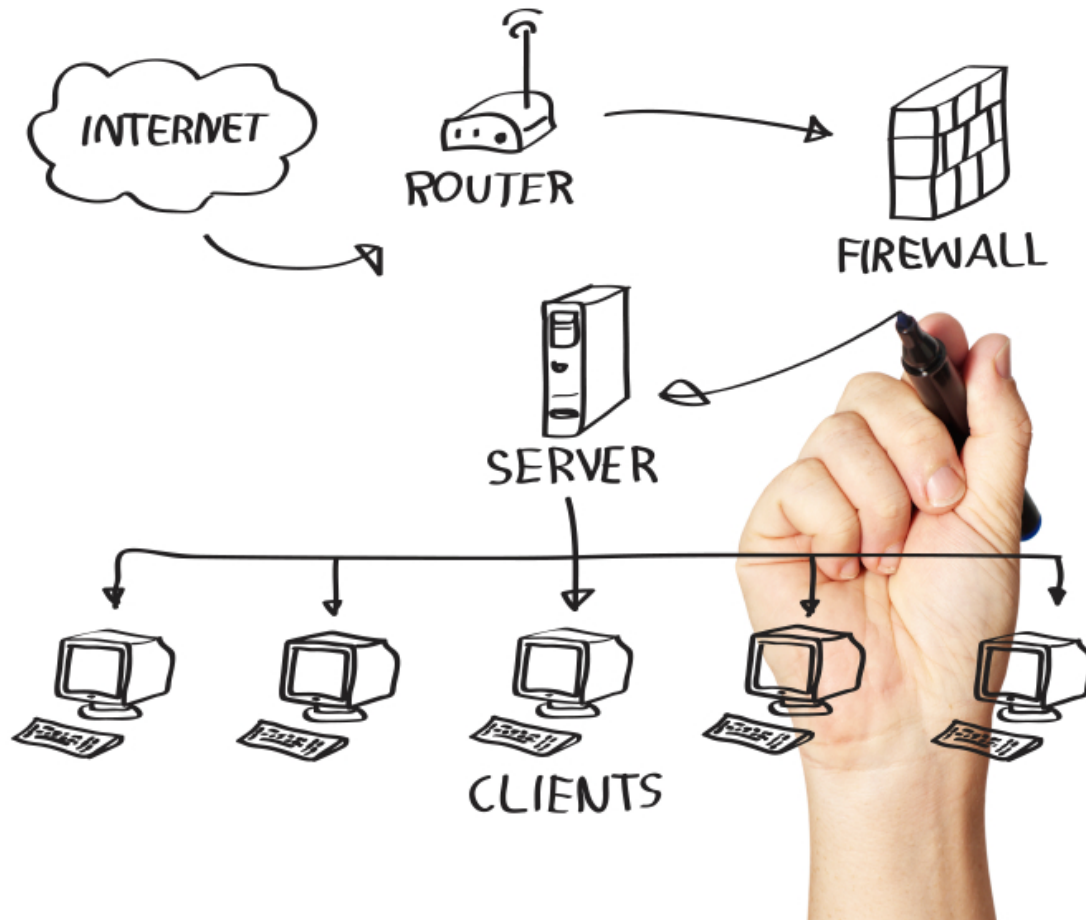
POLISH AIRLINES

LOT

A STAR ALLIANCE MEMBER

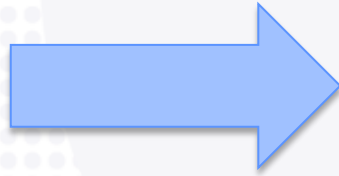


# Cyber Risk – Not Only a Data Breach Risk



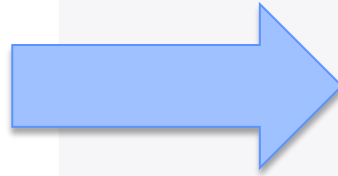


# Cyber Risk – An Evolving Risk



Chip and **PIN**

# Cyber Risk – An Evolving Risk





# Cyber Risk – An Evolving Risk

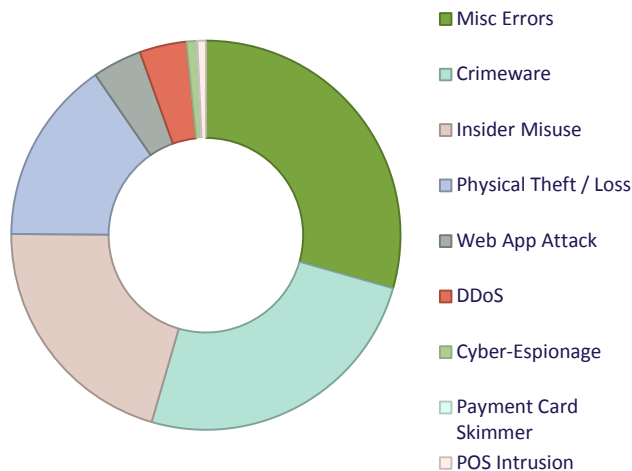


# What Causes Cyber Incidents?

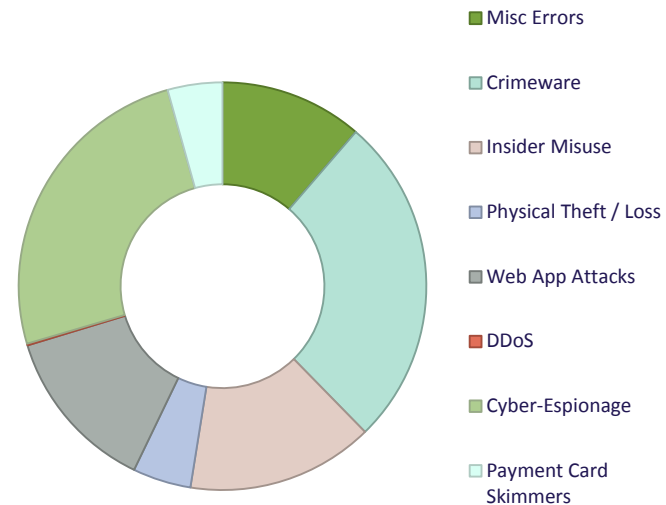
## Some Stats – 2015 VDBIR

While the threats may seem innumerable, infinitely varied, and ever-changing, the reality is... 96% of all 100,000+ incidents collected over the last 10 years fell into nine basic patterns.

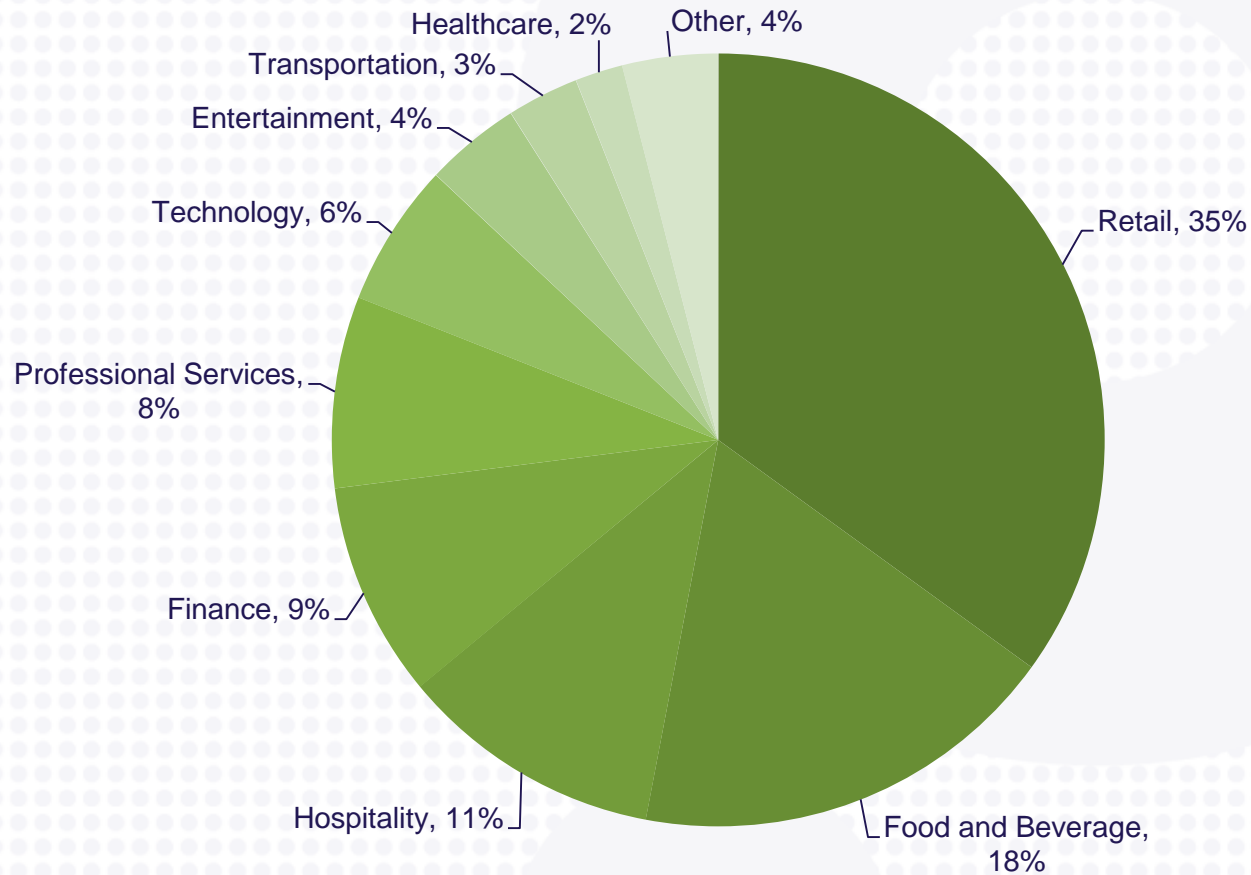
### Security Incidents by Type



### Data Breaches by Type



# Industry Cyber Risks Compromises by Industry



Source: 2014 Trustwave Global Security Report

# The Data Protection Landscape - GDPR

## General Data Protection Regulation

- **Fines** - of up to EUR 20m or 4% of annual global turnover for breaches of the rules
- **Consent** - The new standard will be freely given, specific, informed and “unambiguous” consent
- **Breach notification:**
  - Regulator - “without undue delay” and where feasible within 72 hours.
  - Affected Individuals – only where breaches likely to pose a high risk.
- **Profiling** - Tougher restrictions on the use of profiling
- **Supply chain** - joint and several liability for suppliers (data processors).
- **Data Protection Officers**
- **Other key obligations**

# Cyber Risk

## Consequences

- Data Theft or Disclosure
  - **Confidentiality**: is a *duty of care* of the data holder to consumers, customers and Privacy Regulators
  - Requires resources to bring threat to an end
- Damage
  - **Integrity**: corruption of *data, software, or systems*
  - Requires resources to repair or restore
- Disruption
  - **Availability**: *interruption to business functionality* for a period of time, or *degrade productivity* of commercial operations, transactions, or communications
  - Requires resources to reduce impact of downtime

# The Potential Cost of Cyber Risks

- A hotel company suffered a malware attack. It was estimated that approximately 500,000 customers stayed, dined or used the hotel services at the affected properties during the period of the attack.
- Approximately 5,000 customers of the incident were notified via email. The remaining guests were notified via the hotel's website and through media announcements.

– PFI investigator	\$1,300,000
– Shadow Forensic Investigator	\$300,000
– Data Protection Lawyer	\$1,200,000
– 2 Public Relations Consultants	\$150,000
– Notification and call centre provider	\$110,000
– Credit Monitoring provider	\$160,000
– One Card Brand PCI assessments	\$3,500,000
– Second Card Brand PCI assessment	\$20,000
– Another is yet to issue their assessments	???

<b>Total Costs (so far)</b>	<b>\$6,740,000</b>
-----------------------------	--------------------



# Cyber Insurance

- **Resources and Capital following a Cyber Event**
  - **Forensic Expenses**
    - Detection, repair and restoration of data and networks
  - **Data Breach Notification & Privacy Liability**
    - Costs to comply with requirements to notify customers and offer credit monitoring services, in addition to any ensuing liabilities
  - **Privacy Regulatory**
    - Cost of handling and preparing the response to a data or privacy regulatory investigation, including PCI card brand fines and penalties
  - **Public Relations**
    - Cost of hiring a crisis management team
  - **Business Interruption / Increased Costs of Working**
    - Loss of income (net profit) and increased costs
  - **Cyber Extortion**
    - Crisis management support to manage ransom process, and pay the ransom if unavoidable.
  - **Security Liability**
    - Third party liabilities as a result of a breach of your IT network security

# How do insurers rate cyber risk?

- Industry / turnover
- Data – amount and type
- Reliance on IT network for operations
- IT Security, Policies and Procedures
  - Compliance with regulations (Data Protection Act, Industry PCI, etc)
  - Employee training
  - Firewalls, Encryption, IDS
  - Access controls
- Readiness to deal with an incident
- Cyber risk culture – internally and externally
- Claims experience

# What insurers' approach is to Cyber Insurance

- Insurers know you are a target and you will be attacked or someone could make a mistake which leads to a cyber loss
- Great IT security is a license to buy insurance
- Insurance is for the low frequency, high severity claims

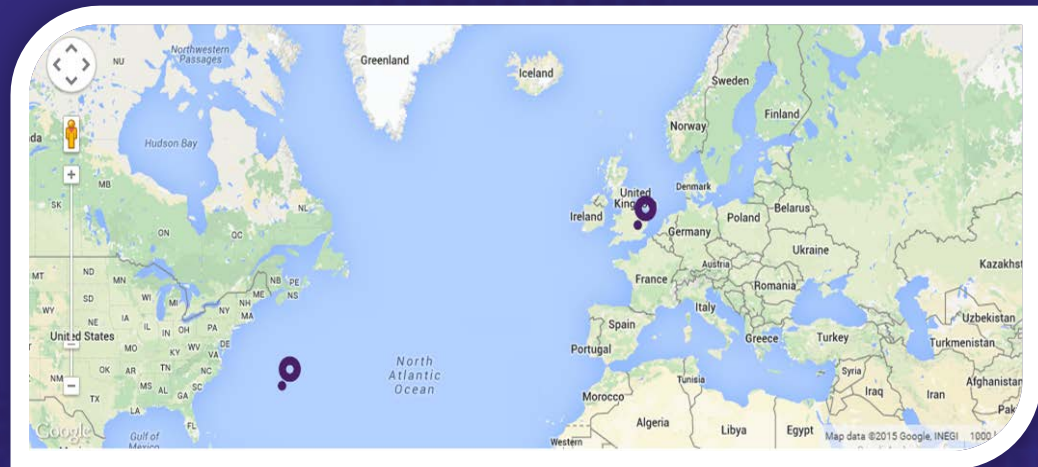
# What are insurers looking for in terms of cyber risk management

- IT Security
  - Encryption, Industry Standards, Access Management, Patch Management
- Are you ready for a breach?
  - Having a tested response plan in place which details how you will respond to a breach can make your response more efficient and effective
- Are you considering and managing cyber risks at an organisational level?
  - It is a myth that cyber risks are only the responsibility of the IT department
- Have you considered the Human Element?
  - The Verizon, 2015 Data Breach Investigations Report, which collected information on 100,000+ incidents over the last 10 years, shows that 50% of breaches within organisations in 2014 were caused by human error
- Supply chain management
  - Auditing and restriction of access

# Contact us

Paragon International Insurance Brokers Ltd  
140 Leadenhall Street  
London EC3V 4QT, England  
T +44 20 7280 8200  
F +44 20 7280 8270  
[www.paragonbrokers.com](http://www.paragonbrokers.com)

Paragon Brokers (Bermuda) Ltd  
LOM Building, 27 Reid Street  
Hamilton HM11, Bermuda  
T +1 292 0875  
F +1 292 8343  
[www.paragonbrokers.com](http://www.paragonbrokers.com)



Paragon International Insurance Brokers Ltd . Authorised and Regulated by the Financial Conduct Authority. Accredited Lloyd's Broker. Paragon International Insurance Brokers Ltd, 140 Leadenhall Street, London, EC3V 4QT. Registered in England. Company No. 3215272. Paragon Brokers (Bermuda) Ltd. LOM Building, 27 Reid Street, Hamilton HM 11, Bermuda. Registration No.33838. Paragon Brokers (Bermuda) Ltd is authorised and regulated by the Bermuda Monetary Authority.

## **Basic Copyright Notice & Disclaimer**

**©2016 This presentation is copyright protected. All rights reserved.** You may download or print out a hard copy for your private or internal use. You are not permitted to create any modifications or derivatives of this presentation without the prior written permission of the copyright owner.

This presentation is for information purposes only and contains non-binding indications. Any opinions or views expressed are of the author and do not necessarily represent those of Swiss Re. Swiss Re makes no warranties or representations as to the accuracy, comprehensiveness, timeliness or suitability of this presentation for a particular purpose. Anyone shall at its own risk interpret and employ this presentation without relying on it in isolation. In no event will Swiss Re be liable for any loss or damages of any kind, including any direct, indirect or consequential damages, arising out of or in connection with the use of this presentation.