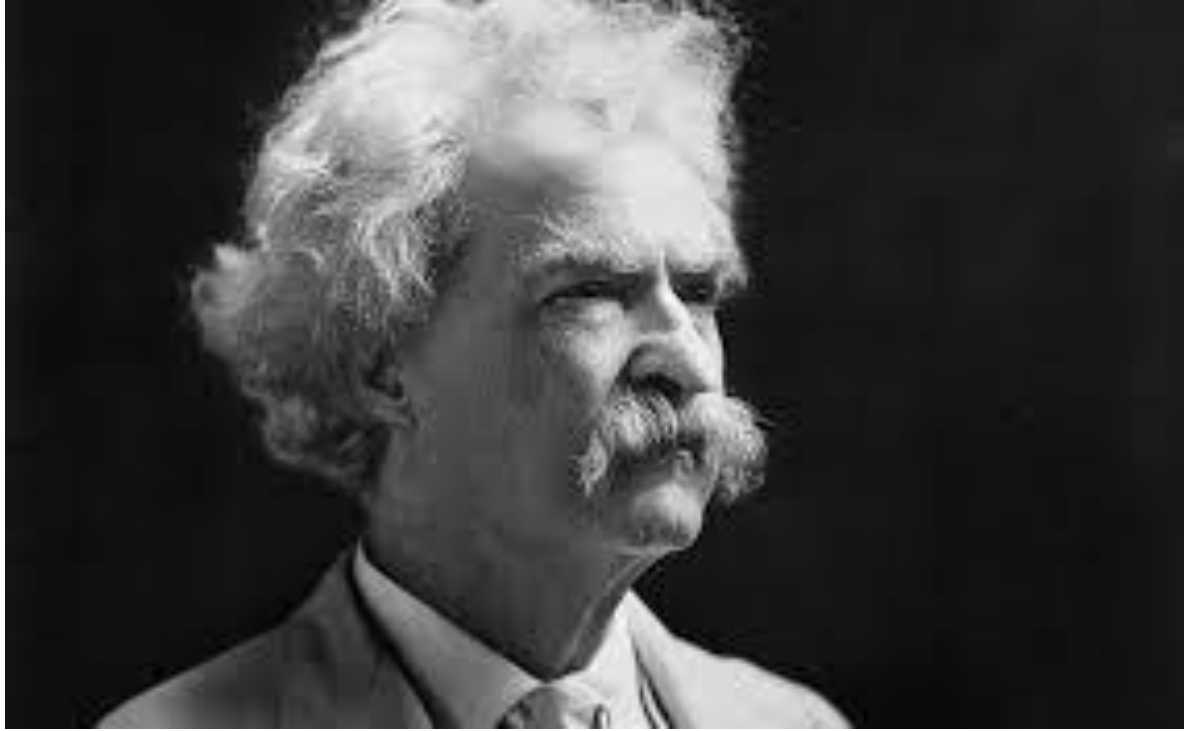




How to sell cyber with the perfect policy for your clients
Richard Hodson November 2017

Cyber Confusion



Mark Twain



Benjamin Disraeli

Lies, Damned Lies and Statistics

What our clients see and hear

Equifax lose 160m records

NHS hit by WannaCry

British Airways IT failure leaves 75,000 stranded

TalkTalk fined £ 400,000

Ashley Maddison

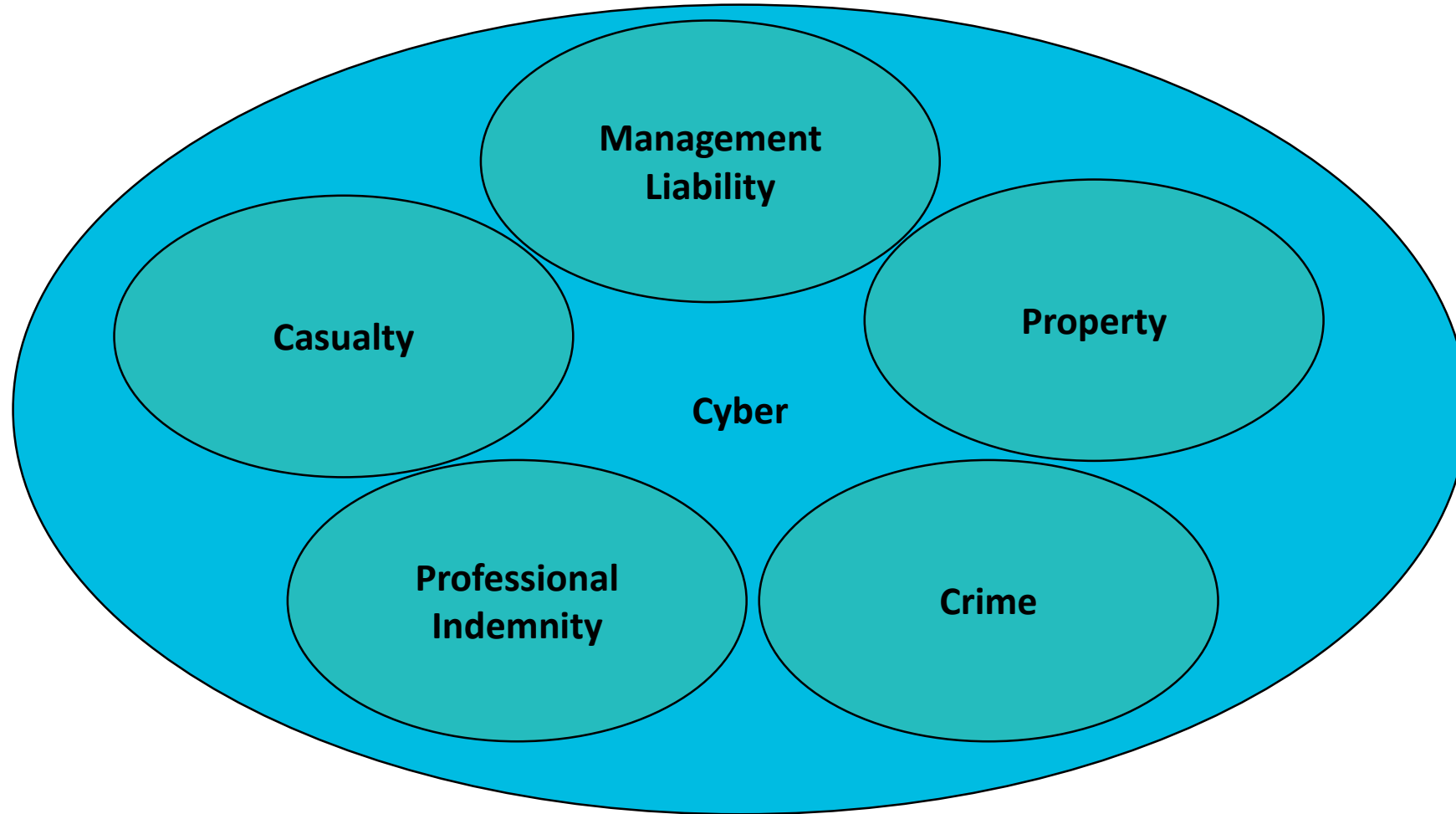
Deloitte Hit By Cyberattack

Who is confident about selling Cyber?

Is there a perfect Cyber Policy?



Cyber is a wrap



What is the anatomy of a cyber event?



Case Study – Loss of third party money

Business: Wool Retailer – Online and Traditional

Turnover: £ 1,904,000

Type of Loss: PayPal theft

Third Party Financial Loss:	£ 22,000
Business Interruption:	£ 12,000
Incident Response:	£ 2,460
IT Forensic Costs:	£ 2,460
PCI Fine:	£ 3,450
PayPal Fine:	£ 7,090
<u>PCI Audit:</u>	<u>£ 1,500*</u>
Total Loss:	£ 50,510
Total Claim	£ 48,010

Insurance Premium: ?????

*Uninsured

Other actual loss examples



Breast Cancer Charity
PBX/Phone Hacking
£ 25,000 Phone Bill
UNINSURED



Accountants
Malware/Keylogger
£ 165,000 Wire Transfers
£ 15,000 IT Forensics

**R
A N
S O M
W A R E
P H I S H
I N G C Y B
E R C R I M E**

Opticians
£ 400 Ransomware
£ 60,000 IT Forensics



Construction Company
CEO Fraud
£ 50,000 Wire Transfer

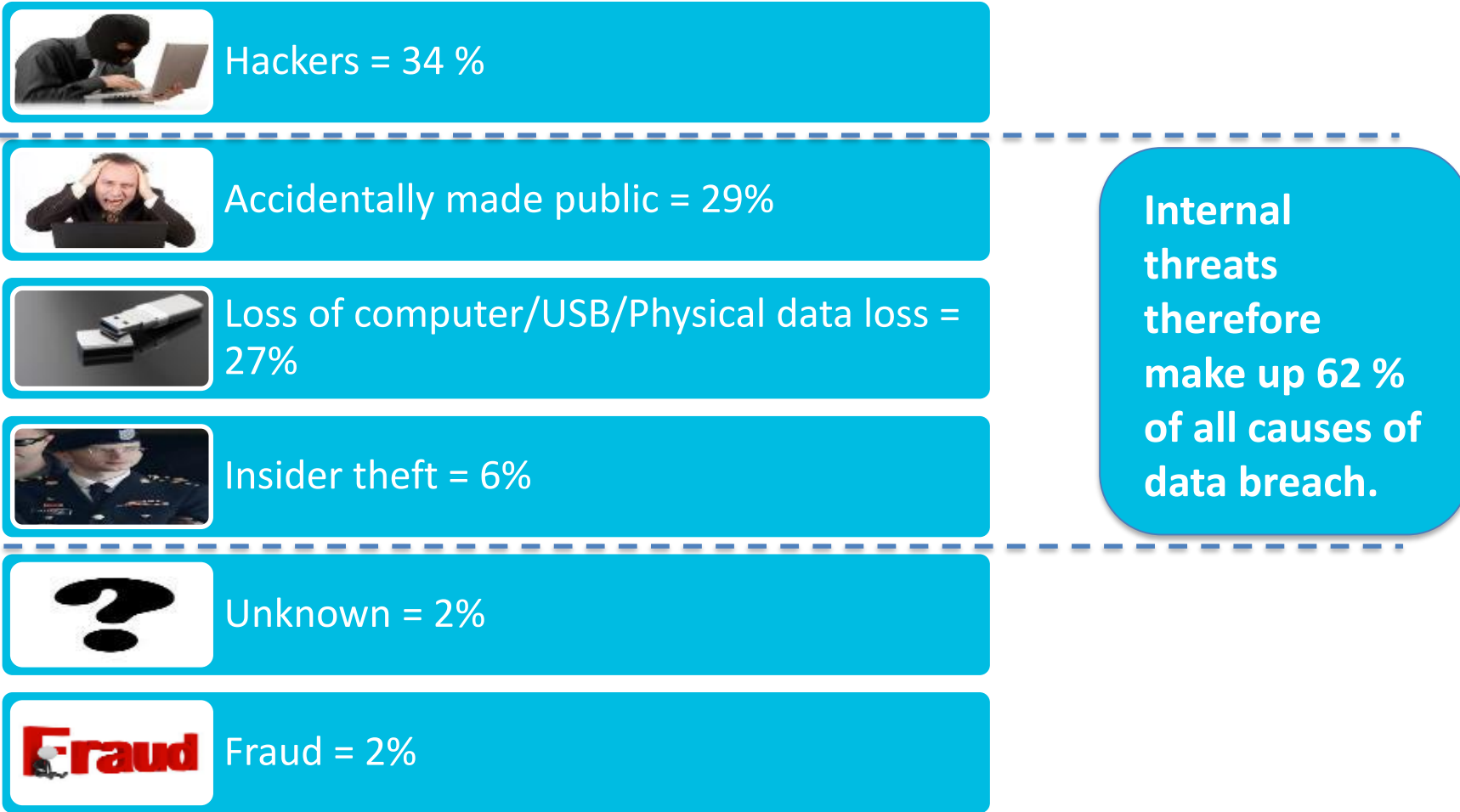
What does cyber cover?

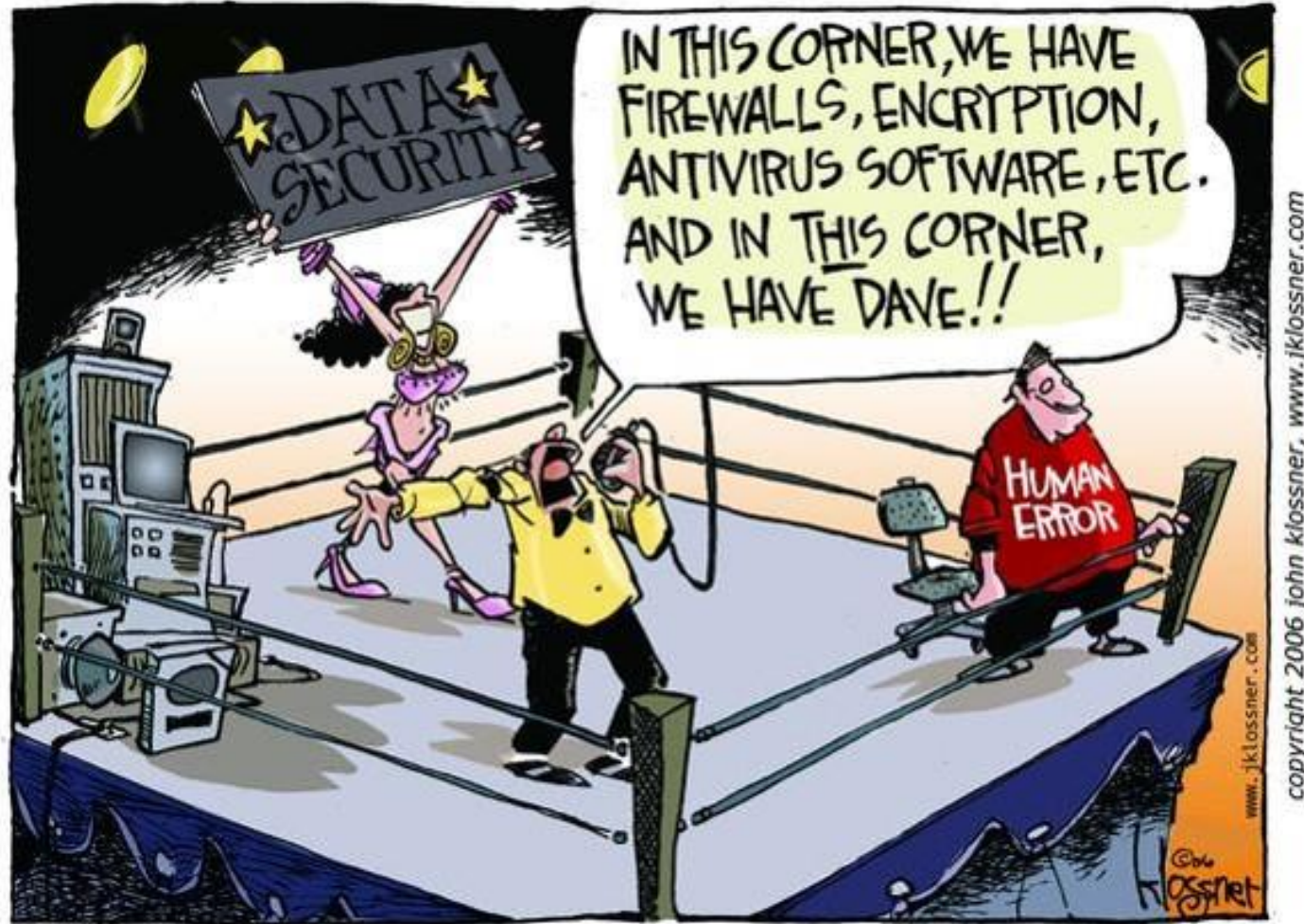
Some First Party “Cyber” Losses	Third Party “Cyber” Liability Examples
System damage	Privacy claims for breach of personally identifiable information
Loss of Profits/Revenue	Claims for direct financial loss
Forensic costs	Breach of confidentiality
Regulatory investigations	Defamation, libel, slander
Notification costs	Intellectual property infringement
Contractual fines/penalties	Transmission of virus
Cyber crime (theft, extortion, telephone hacking, phishing scams)	Claims from Financial institutions
Public relations/Mitigation	

What is the number one cause for lost data in any organisation?

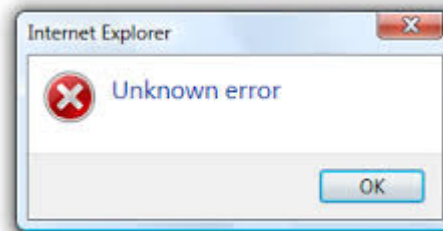
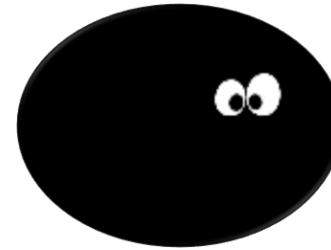
- a) Malicious employee – Insider job
- b) Loss of Laptop/USB or paper files
- c) Accidentally made public – e.g. Reply all?
- d) Hacker

Answer





Case Study – Outsourced service provider



Case Study – Outsourced service provider.



- Limited Liability
- Consequential loss exclusion
- No responsibility for data

But I back up my systems



Average dwell time in 2016 - 99 days

Dwell time = the number of days that a threat “lives” in a system before detection

Caveat Emptor – Not all cyber policies are created equal!

- Liability only policies
- Cover excludes Outsourced Service Providers (OSP's)
- Jurisdictional Issues
- **Terrorism exclusion**
- **Non-specific virus' or virus in the wild exclusion**
- Policies that only cover electronic data
- Policies that do not cover loss of Employee Data
- Systemic risk exclusion/sublimit



Beware of the Exclusions

Virus in the wild exclusion

- *any computer virus that was not specifically targeted to your system.*

Terrorism

- *Act(s), including but not limited to the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organisation(s) committed for political, religious, ideological or similar purposes including the intention to influence any government and/or to put the public, or any section of the public, in fear*

Electronic Data Exclusion

- *the loss or distortion of any data held electronically by you.*

Aren't I already covered

Property & Business Interruption Policies: Data is an intangible asset and is not covered by current property policies, therefore also no business interruption cover.

General Liability & Employers Liability Policies cover property damage or bodily injury. No cover for Financial Loss.

Computer Policies also respond to physical loss damage. Some do include some cover for hacking and virus.

Professional Indemnity policies respond to claims stemming from the ordinary course of your business.

Crime/Fidelity policies cover first party losses following theft, no cover for third party claims.

Other benefits

- Liability Mitigation – See GDPR
- Reducing liability to Directors and Officers
- Triage: Who you going to call?



Cyber & General Data Protection Regulation - GDPR

- Fines & Penalties probably uninsurable
- Mandatory reporting periods to the ICO
- Personal Liability for individuals

Elizabeth Denham, Information Commissioner August/September 2017

“Fines can be avoided if organisations are open and honest and report without undue delay, which works alongside the basic transparency principles of the GDPR”

UKGLOBAL