Cyber - From Risks to Claims Including Business Interruption

Wed 22 May 2019

Presenter

Rajen Rajput

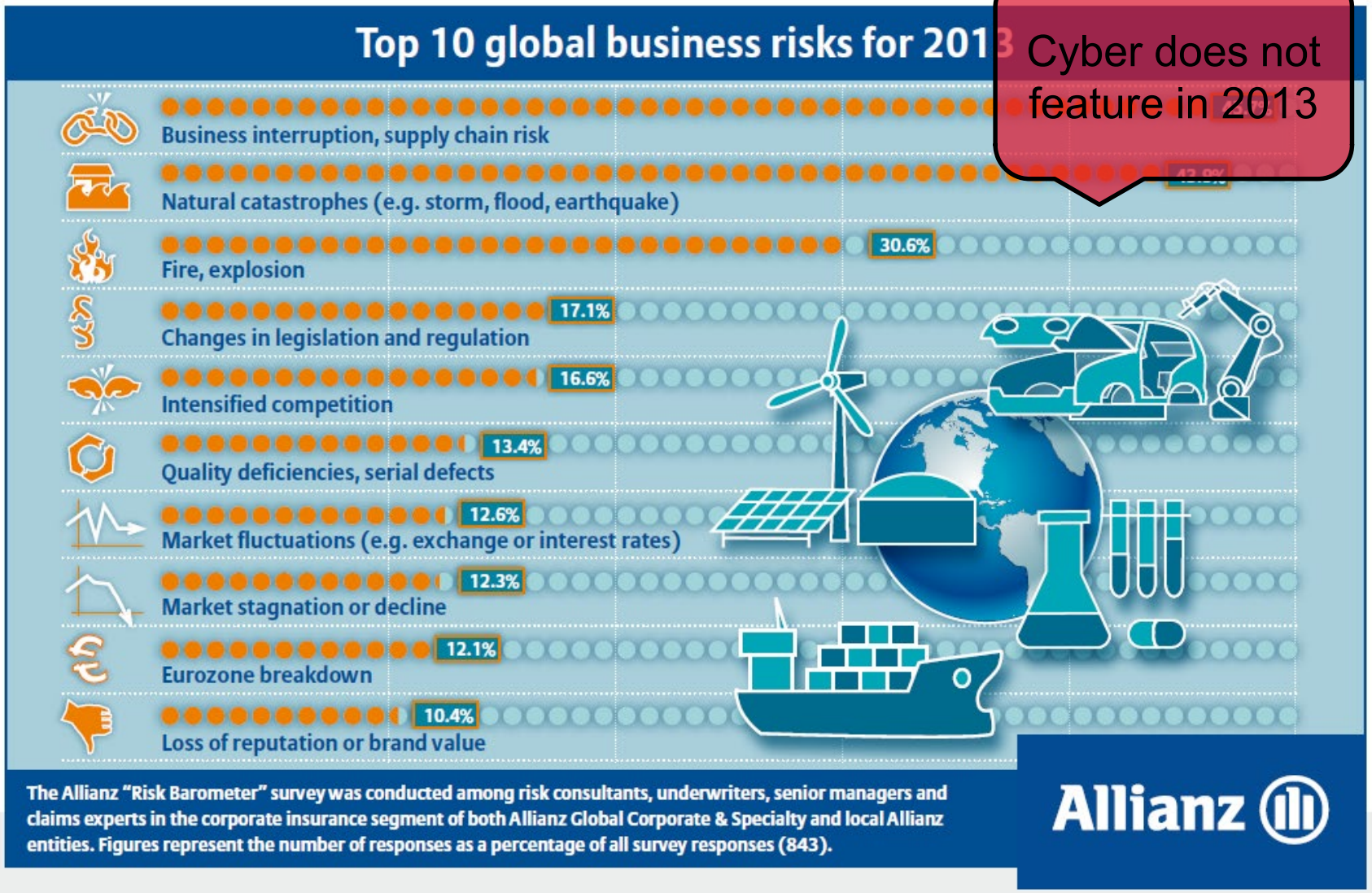
FORENSIC ACCOUNTANTS

Learning Objectives

By attending this event you will gain a further understanding of:

- the growing prominence of cybercrime as a risk to businesses;
- the effects on a business from a cyber breach;
- appreciation of the possible magnitude of economic damage from a cyber attack;
- interpretation of cyber risk policies;
- Business Interruption losses flowing from cyber damage

Cyber Risk in Perspective



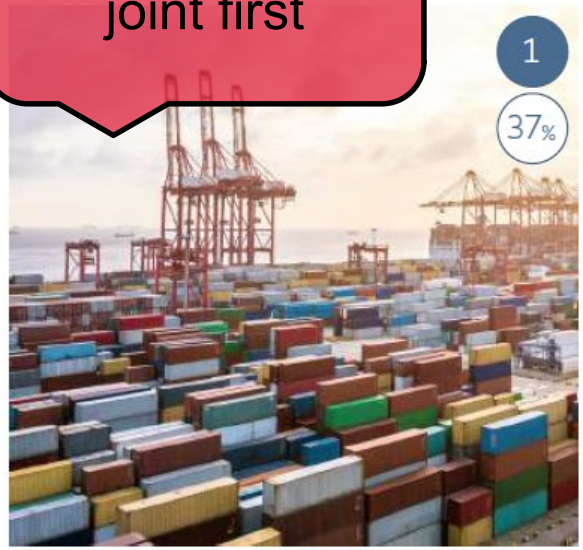
Cyber Risk in Perspective

THE MOST IMPORTANT BUSINESS RISKS IN 2019

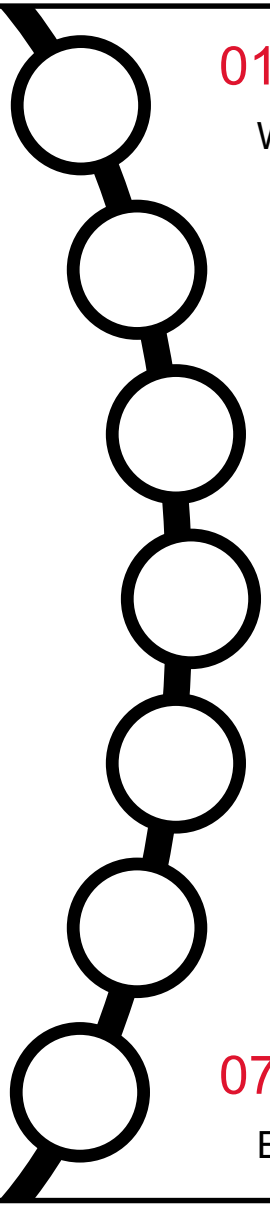
Ranking changes are determined by positions year-on-year, ahead of percentages

Rank		Percent	2018 rank	Trend
1	**Business interruption (incl. supply chain disruption)**	**37%**	1 (42%)	=
2	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)[1]	**37%**	2 (40%)	=
3	Natural catastrophes (e.g. storm, flood, earthquake)	**28%**	3 (30%)	=
4	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**27%**	5 (21%)	▲
5	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuations)	**23%**	4 (22%)	▼
6	Fire, explosion	**19%**	6 (20%)	=
	New technologies (e.g. impact of increasing			

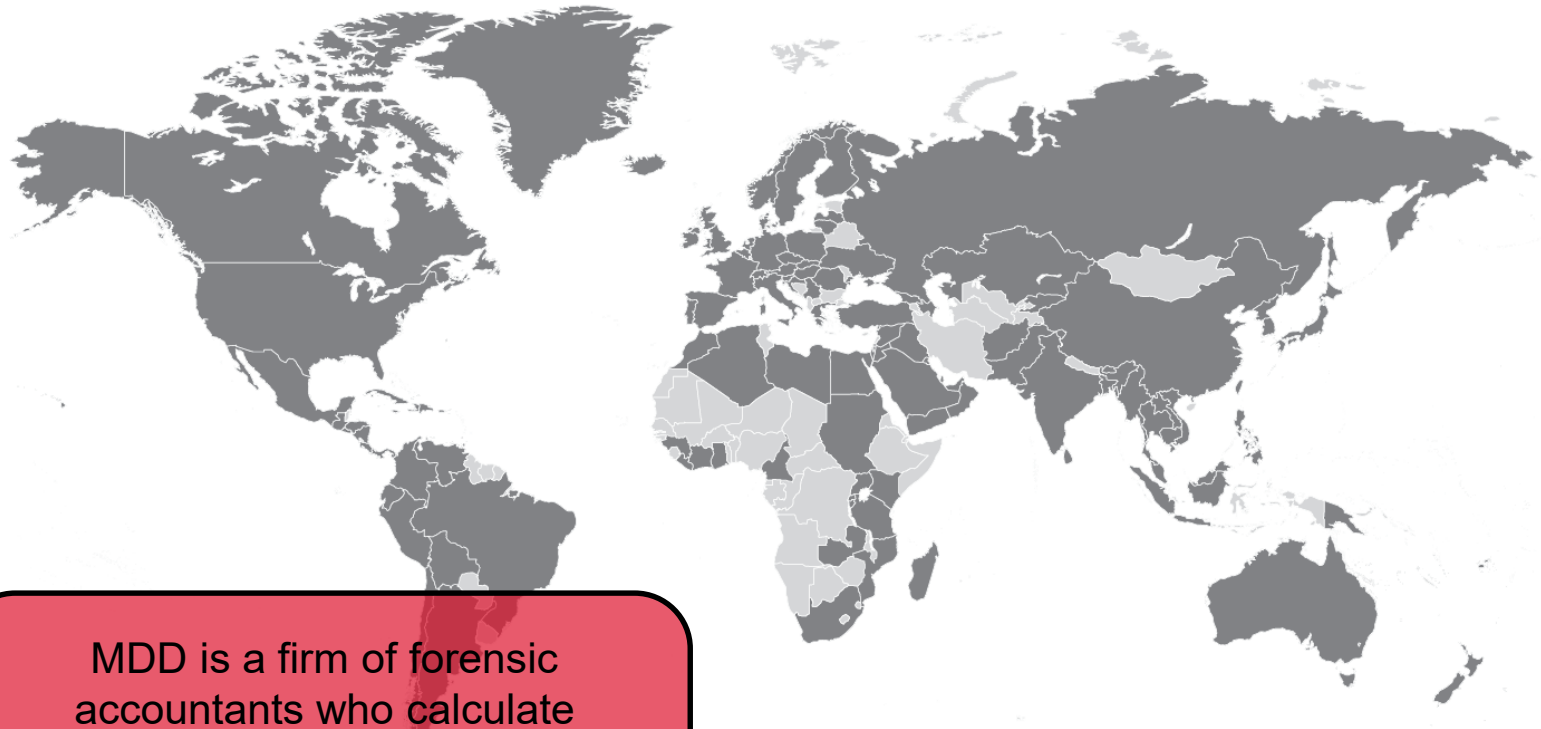
Cyber is now joint first



Contents



01 - Introduction



MDD is a firm of forensic accountants who calculate Business Interruption and cyber MD losses, generally working for insurers, insureds or lawyers.

= Where MDD has worked

01 - Introduction

- Accident Benefits
- Agriculture
- Builders' Risk Claims & Soft Costs Claims
- Business Disputes
- Business Interruption
- Business Valuations
- Catastrophe Services
- Class Actions
- Construction Defect Claims
- Fidelity Claims
- Franchise Litigation
- Fraud & Investigations
- Government Services
- Intellectual Property
- Liability Losses
- Litigation Support
- Lost Profits
- Maritime
- Mining Claims/Refining Claims
- Surety & Funds Control Services
- Toxic Torts
- Transportation
- Valuable Papers

01 - Introduction

- Contingency/ Entertainment
- Cyber Risk
- Disability Compensation & Workers' Compensation
- Divorce & Marital Disputes
- Environmental Damage Claims
- Expropriation
- Extra Expenses/ Increased Costs
- Oil & Gas
- Personal Injury & Wrongful Death
- Physical Damages
- Power Generation
- Products Liability & Product Recall
- Reported Insurance Values
- Stock & Contents
- Subrogation

02 – Cyber Language

03 – Grouping and Simplifying

Obtaining Money

Victim Aware

Ransom

Victim Unaware

CEO-Fraud/Business-Email-Compromise
Invoice fraud
Credential Stuffed Accounts

Obtaining Data

Espionage
Data Leakage

System Damage

Denial of Service
Reduce Computing Power (Efficiency)
Monitor Keystrokes
System Offline

Grouping some of the terms

How Was It Done?

Spyware/keylogger
SQL Injection
Phishing
Vishing
Spear-Phishing
RAM-scraping
USB/Removable-Device
Botnets
Credential-Stuffing
DDoS
Non-Malicious / Unintentional

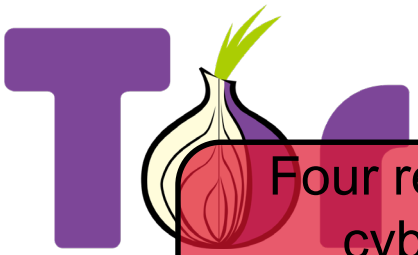
Who Did It?

Insiders
Hobbyists
State-sponsored
Common criminal

04 – Cybercrime on the Rise

Anonymity and Deep Web

Inability to trace crime back to bad actor

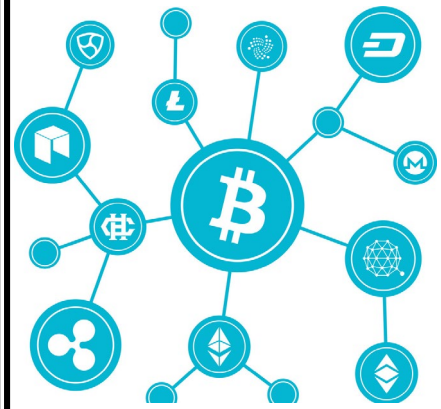


Liquidity

Speed or ease of converting data or information to money

Movement of Funds

Further anonymity once monetised

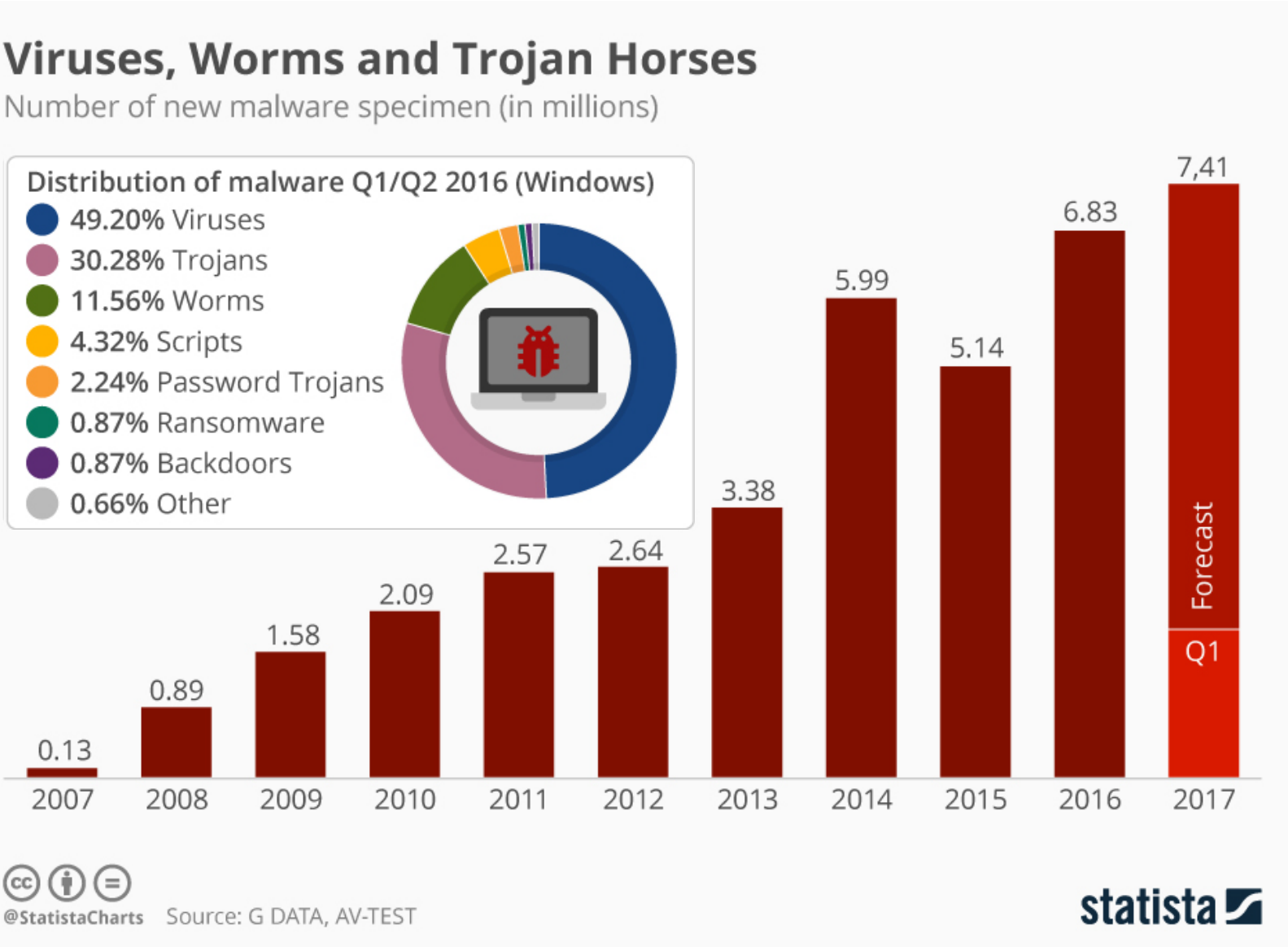


Internet of Things

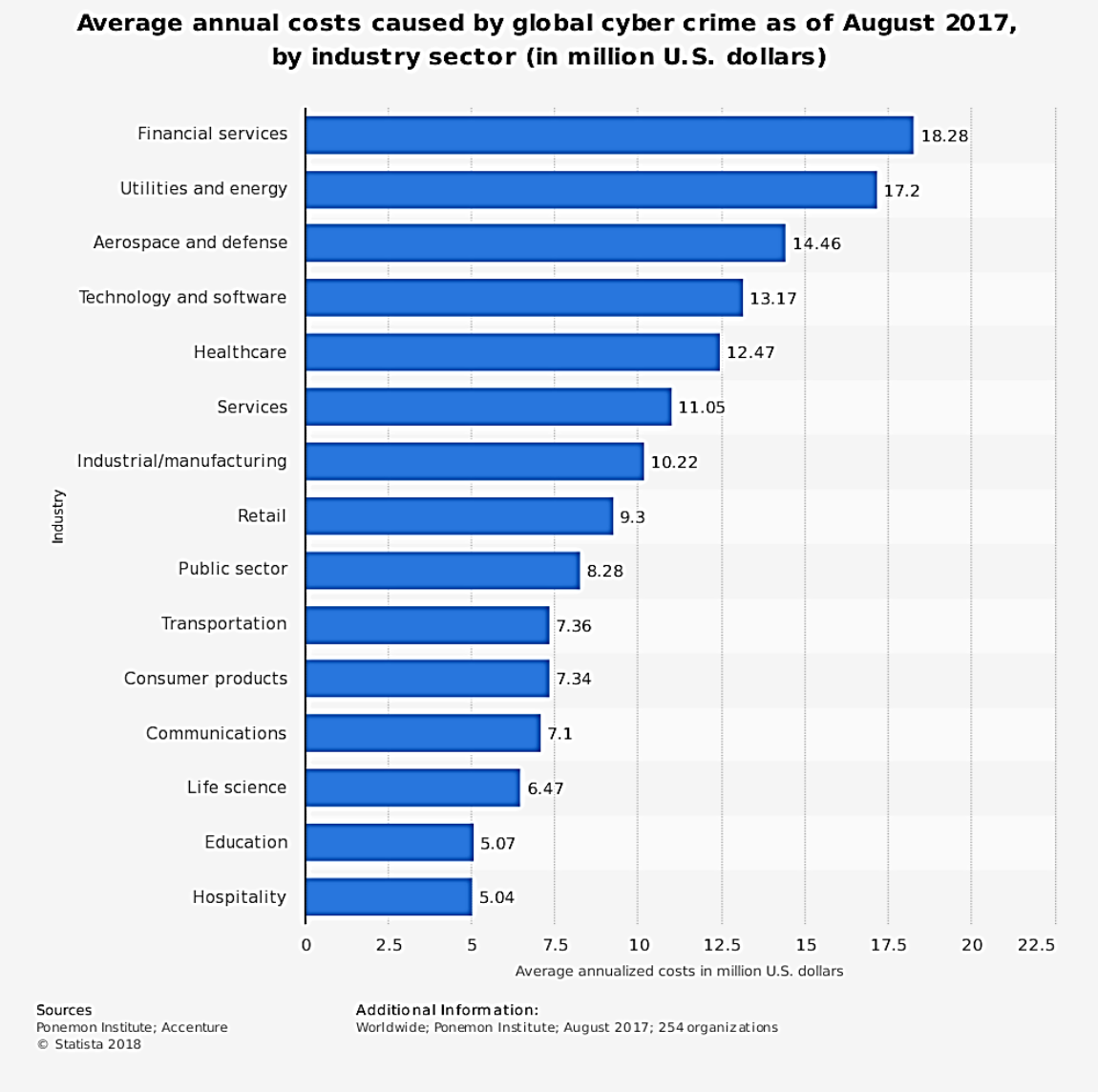
Increasing amount of devices or ‘doorways’

Four reasons why cyber crime frequency/severity is rising

04 – Cybercrime on the Rise



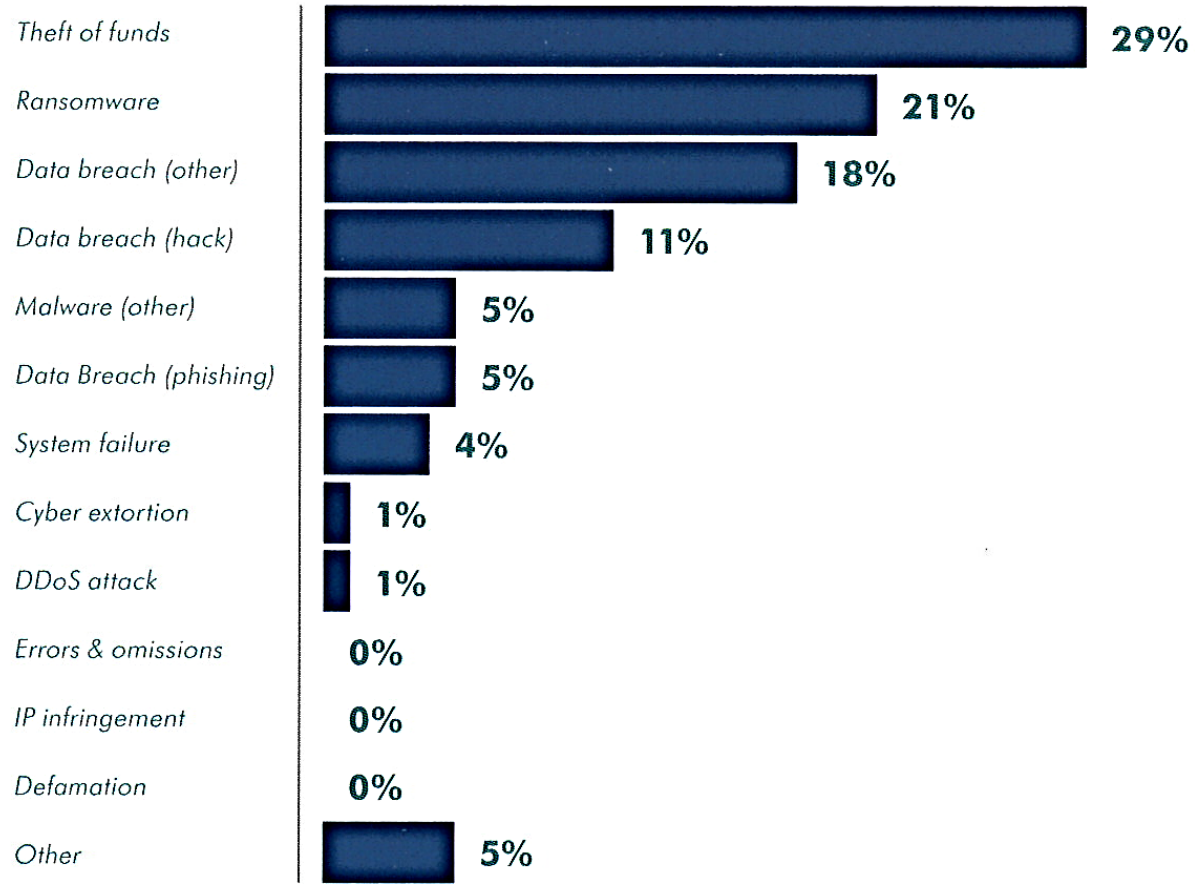
04 – Cybercrime on the Rise



Who is getting hit the hardest?

04 – Cybercrime on the Rise

KEY 2017 CYBER STATISTICS



CFC Underwriting cyber claims statistics, 2017

04 – Cybercrime on the Rise

05 – Who is at Risk?

Large Business (Generalisations)

More data to steal

More money to steal

More personnel to manipulate

Larger status opportunity
(Status for bad actor)

More computers to spread infections

Larger reliance on IT to operate

SME (Generalisations)

Lesser-aware staff in cyber security

Lower IT security and protections
(prevention and detection)

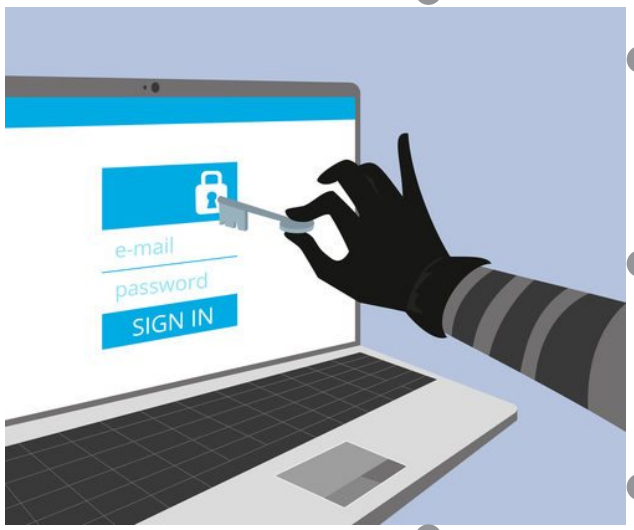
Lower controls on computer policy
(upgrades, personal USBs, personal software)

Older operating systems

47% of small businesses had at least one cyber attack in the past year

Hiscox - Small Business Cyber Risk Report - 2018

06 – Cause and Effect



89 % felt that attacks impacted upon their reputation

26 % were unable to grow in line with previous forecasts

30 % reported a loss of clients

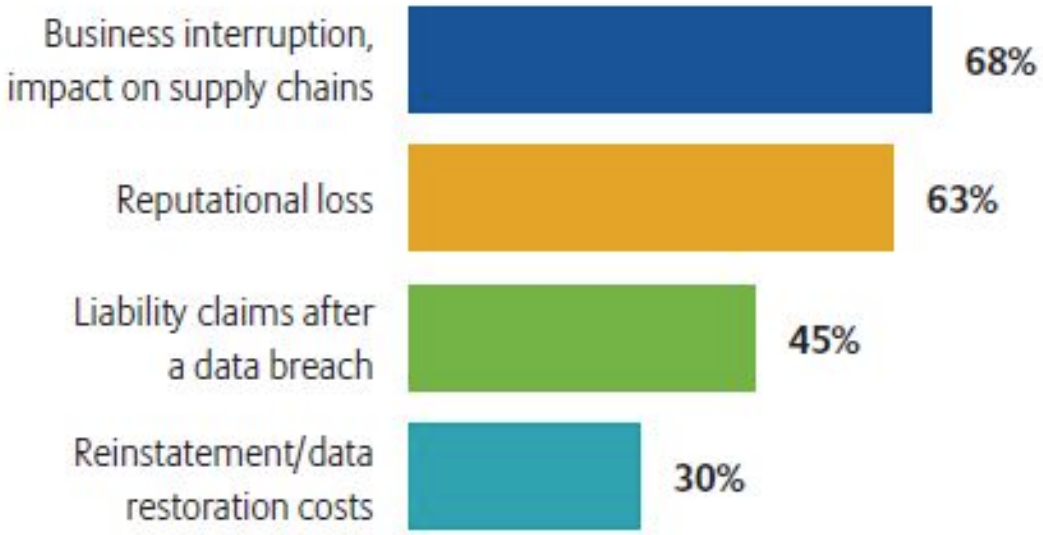
25 % received negative reviews on social media

93 % of businesses suffered operational limitations

Source: Cyber Streetwise campaign and KPMG report of SME victims

06 – Cause and Effect

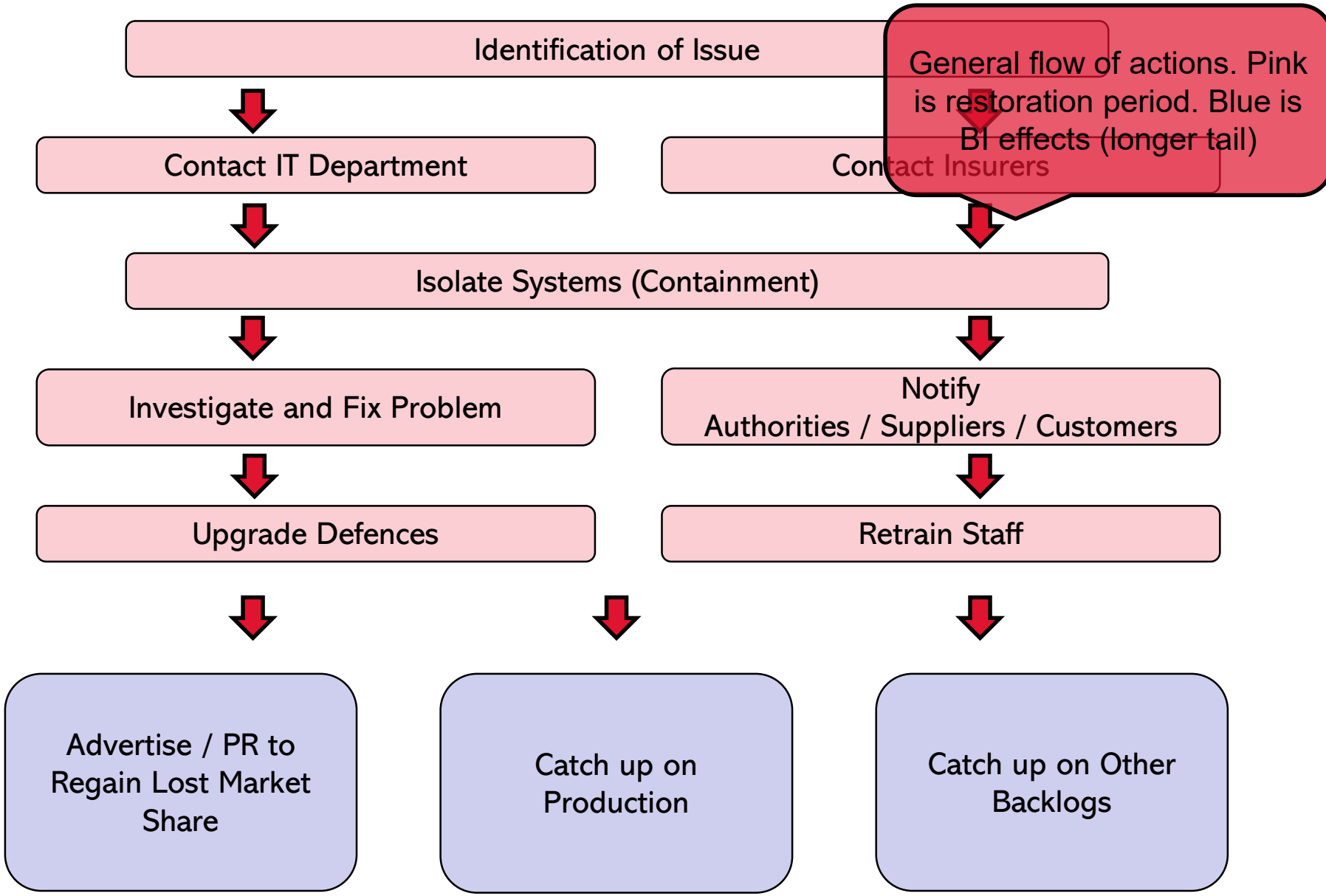
What are the main causes of economic loss after a cyber incident?



Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (446). Up to three answers possible.

Source: Allianz Risk Barometer - 2017

07 – Claim on Policy



07 – Claim on Policy

EXAMPLES OF AVAILABLE CYBER COVER

Costs

- Forensic investigation after a breach
- Legal fees managing the response to a breach
- Notification to affected data subjects
- Notification to ICO or other regulatory body
- Temporary call centre to take enquiries from affected data subjects
- Credit monitoring for affected subjects
- Ransom
- Risk consultancy firm to manage situation
- PR firm - “Crisis containment”
- Repair, restoration or replacement of websites, programs or electronic data
- System repair and possibly repeat event mitigation
- Defend and settle third party claims
- Regulatory investigations and civil penalties
- Claims preparation

Even claims prep may be included - which is a low-risk advantage for the Insured

Loss of Income and ICW

- Cyber business interruption – including due to loss of reputation
- Cyber business interruption – potentially including supply chain

07 – Claim on Policy

Example Wordings For Inclusions

Cyber and Data (mid-2018)

If during the period of insurance, and in the course of your business or advertising after the retroactive date, you discover or suspect a breach has occurred, we will pay all reasonable and necessary:

a. breach forensic costs;
b. outside legal fees you incur in managing your response to the breach;
c. costs you incur to notify each affected data subject of the breach;
d. costs you incur to notify any regulatory body, including the Information Commissioner's Office, of the breach where you are required by any law or regulation to do so;
e. costs you incur to use a third-party call centre to answer enquiries from affected data subjects following notification of the breach to such data subjects; and
f. credit monitoring costs;

Example wording of seemingly wide coverage

07 – Claim on Policy

Example Wordings For Inclusions

Cyber and Data (mid-2018)

If during the period of insurance, and in the course of your business or advertising after the retroactive date, you discover or suspect a breach has occurred, we will pay all reasonable and necessary:

a. breach forensic costs;

b. outside legal fees you incur in managing your response to the breach;

c. costs you incur to notify each affected data subject of the breach;

d. costs you incur to notify any regulatory body, including the Information Commissioner's Office, of the breach where you are required by any law or regulation to do so;

e. costs you incur to use a third-party call centre to answer enquiries from affected data subjects following notification of the breach to such data subjects; and

f. credit monitoring costs;

We will insure **you** for **your** loss of **income**, including where caused by damage to **your** reputation, and any **increased costs of working**, resulting solely and directly from an interruption to **your business** commencing during the **period of insurance** and lasting longer than the **time excess**, due to:

a. the activities of a third-party who specifically targets **you** alone by maliciously blocking electronically the access to **your computer system**, **programmes** or data **you** hold electronically; or

b. a **hacker** who specifically targets **you** alone.

But policy may not respond if cyber attack is general and non-targeted (WannaCry? NotPetya?)

07 – Claim on Policy

Example Wordings For Inclusions

Cyber and Data (mid-2018)

If during the period of insurance, and in the course of your business or advertising after the retroactive date, you discover or suspect a breach has occurred, we will pay all reasonable and necessary:

a. breach forensic costs;

b. outside legal fees you incur in managing your response to the breach;

c. costs you incur to notify each affected data subject of the breach;

d. costs you incur to notify any regulatory body, including the Information Commissioner's Office, of the breach where you are required by any law or regulation to do so;

e. costs you incur to use a third-party call centre to answer enquiries from affected data subjects following notification of the breach to such data subjects; and

f. credit monitoring costs;

We will insure **you** for **your** loss of **income**, including where caused by damage to **your** reputation, and any **increased costs of working**, resulting solely and directly from an interruption to **your business** commencing during the **period of insurance** and lasting longer than the **time excess**, due to:

a. the activities of a third-party who specifically targets **you** alone by maliciously blocking electronically the access to **your computer system**, **programmes** or data **you** hold electronically; or

b. a **hacker** who specifically targets **you** alone.

Service provider

Cyber (mid-2018)

Virus, Hacking and Denial of Service Attack and Business Interruption - We will cover You in respect of costs necessarily and reasonably incurred by You to locate and remove a detectable Virus or Similar Mechanism contained in any Computer Equipment
caused by or resulting from a Virus or Similar Mechanism, Hacking or a Denial of Service Attack directed against You or any Outsourced Service Provider. (*Definition of Outsourced Provider: Any provider of information technology, data hosting or data processing services to You under contract excluding the supply of gas, electricity, water, telecommunication or internet service.)*

07 – Claim on Policy

Example Wordings For Inclusions

Cyber (2019)

Ransom - Following an illegal threat:

1. the reasonable and necessary fees of our appointed consultant, incurred by you with our prior written agreement, for advising you on the handling and negotiation of the ransom demand;
2. the cost of any ransom demand from the third-party or, if the demand is for goods or services, their market value at the time of the surrender; and
3. the amount of any stolen ransom, where such theft occurs at or in transit to the agreed location for payment of the ransom.

Point 3 is interesting

07 – Claim on Policy

Example Wordings For Inclusions

Cyber (2019)
Ransom - Following an illegal threat:
1. the reasonable and necessary fees of our appointed consultant, incurred by you with our prior written agreement, for advising you on the handling and negotiation of the ransom demand;
2. the cost of any ransom demand from the third-party or, if the demand is for goods or services, their market value at the time of the surrender; and
3. the amount of any stolen ransom, where such theft occurs at or in transit to the agreed location for payment of the ransom.

Cyber (2019) (Not wording but on company website)
Business Interruption - this section covers the full supply chain, extending to events that impact the insured's systems, the systems of their technology suppliers as well as those of non-technology suppliers where named.

Supply chain

07 – Claim on Policy

Example Wordings For Inclusions

Cyber (2019)
Ransom - Following an illegal threat:
1. the reasonable and necessary fees of our appointed consultant, incurred by you with our prior written agreement, for advising you on the handling and negotiation of the ransom demand;
2. the cost of any ransom demand from the third-party or, if the demand is for goods or services, their market value at the time of the surrender; and
3. the amount of any stolen ransom, where such theft occurs at or in transit to the agreed location for payment of the ransom.

Cyber (2019) (Not wording but on company website)
Business Interruption - this section covers the full supply chain, extending to events that impact the insured's systems, the systems of their technology suppliers as well as those of non-technology suppliers where named.

Cyber (2019)
Business Interruption - We will pay your:
i. loss of income;
ii. increased costs of working; and
iii. additional increased costs of working …

Occasionally written on income basis rather than GP – which reduces underinsurance problems and simplifies claim calculation/explanation

Income definition - The total income of your business, less any savings resulting from the reduced costs and expenses.

07 – Claim on Policy

Example Wordings For Exclusions

Cyber and Data (mid-2018)

1. any loss, theft, damage, destruction or loss of use of any tangible property. However, this exclusion does not apply to data.
2. any individual **hacker** within the definition of **you**.
3. any failure or interruption of service provided by an internet service provider, telecommunications provider, **cloud provider** but not including the hosting of hardware and software that **you** own, or other utility provider.

Exclusion for property

07 – Claim on Policy

Example Wordings For Exclusions

Cyber and Data (mid-2018)

1. any loss, theft, damage, destruction or loss of use of any tangible property. However, this exclusion does not apply to data.
2. any individual **hacker** within the definition of **you**.
3. any failure or interruption of service provided by an internet service provider, telecommunications provider, **cloud provider** but not including the hosting of hardware and software that **you** own, or other utility provider.

credit monitoring costs unless:

a. arising from a **breach** of a **data subject**'s National Insurance number, driver's licence number or other government issued identification number that can be used, in combination with other information, to open a new financial account;

Monitoring costs example which is dependant on what info was taken

07 – Claim on Policy

Example Wordings For Exclusions

Cyber and Data (mid-2018)

1. any loss, theft, damage, destruction or loss of use of any tangible property. However, this exclusion does not apply to data.
2. any individual **hacker** within the definition of **you**.
3. any failure or interruption of service provided by an internet service provider, telecommunications provider, **cloud provider** but not including the hosting of hardware and software that **you** own, or other utility provider.

credit monitoring costs unless:

a. arising from a **breach** of a **data subject**'s National Insurance number, driver's licence number or other government issued identification number that can be used, in combination with other information, to open a new financial account; or

Cyber Cover (mid-2018)

Patent

Any patent being infringed (broken, limited or undermined) without the patent holder's permission.

07 – Claim on Policy

Example Wordings For Exclusions

Cyber and Data (mid-2018)

1. any loss, theft, damage, destruction or loss of use of any tangible property. However, this exclusion does not apply to data.
2. any individual **hacker** within the definition of **you**.
3. any failure or interruption of service provided by an internet service provider, telecommunications provider, **cloud provider** but not including the hosting of hardware and software that **you** own, or other utility provider.

credit monitoring costs unless:

a. arising from a **breach** of a **data subject**'s National Insurance number, driver's licence number or other government issued identification number that can be used, in combination with other information, to open a new financial account; or

Cyber Cover (mid-2018)

Patent

Any patent being infringed (broken, limited or undermined) without the patent holder's permission.

Cyber Cover (mid-2018)

Hack by director or partner – We will not make any payment for any claim, loss or any other liability under this section directly or indirectly due to (i) any individual hacker within the definition of **you**

*Definition of **you:** any person who was, is or during the period of insurance becomes your partner, director, trustee, in-house counsel or senior manager in actual control of your operations…*

Length of Indemnity

Variances in BI Indemnity Period

- **Cyber and Data (mid-2018)**
  - The period, in months, beginning at the date the interruption to **your business** commences and lasting for the period during which **your income** is affected as a result of such interruption, but for no longer than the number of months shown in the schedule.

- **Cyber and Commercial Crime (mid-2018)**
  - Reduction of Business Income sustained by the Insured during a Period of Restoration due to the interruption of the Insured's business operations. (Period of Restoration: *the period beginning with the date that business operations have first been interrupted and ending on the earlier of: 1. the date when the business operations have been restored substantially to the level of operation that existed prior to the interruption; or 2. three hundred and sixty five (365) days after the business operations have first been interrupted.*

Be careful as indemnity period definitions are not always the same, and may be ambiguous

Services Provided

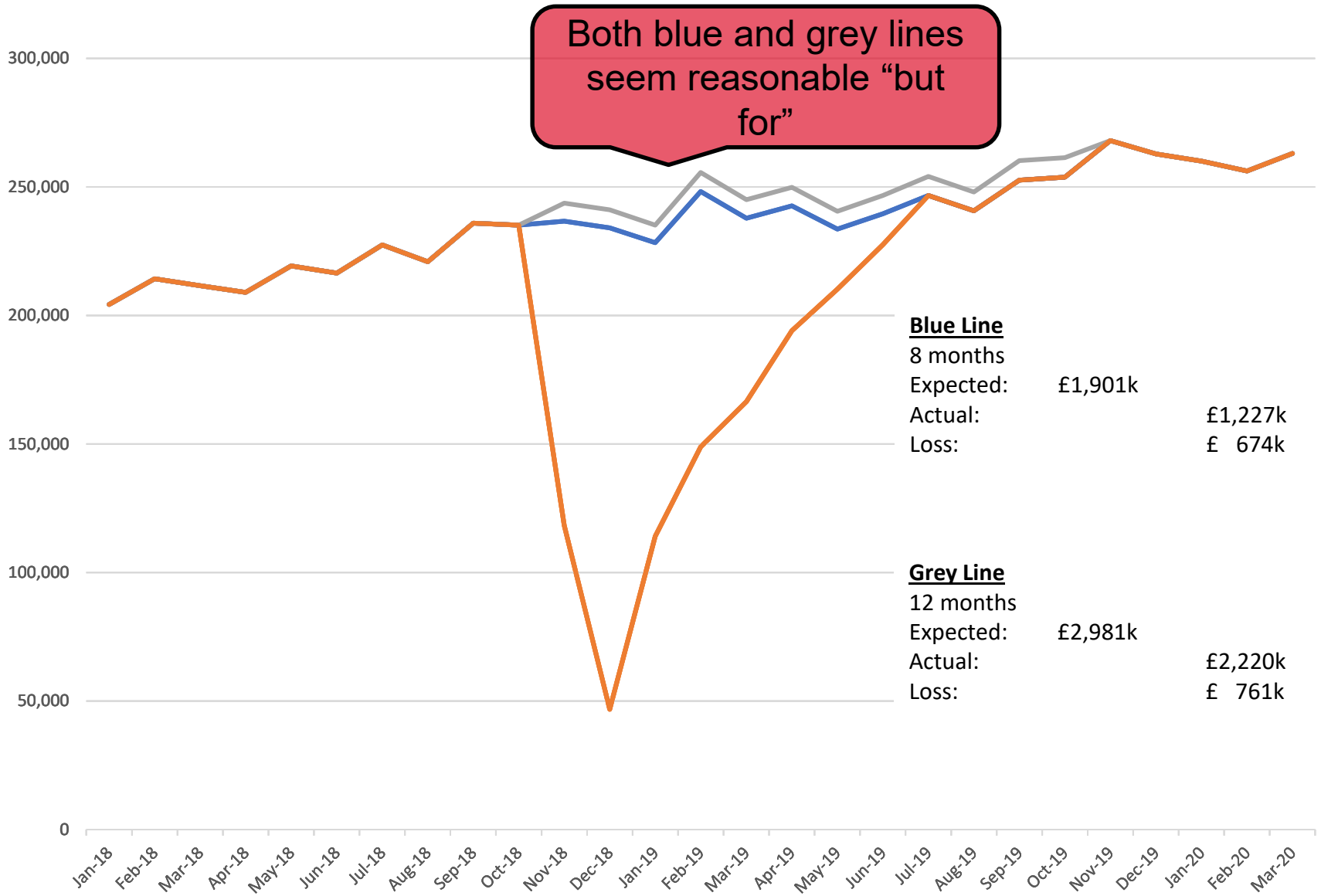
Depending on cyber cover purchased, the premium is almost like a retainer for these professional services

Categories of Costs or Losses

Objective	Subjective
IT costs for identifying and containing problem	Increase in security (betterment)
IT costs for rebuilding/reconfiguring servers or websites	Loss of profit / earnings
PR and advertising	
Temporary call centre costs	
Notification costs	
Cost of ransom	
Retraining staff costs	

BI is subjective and requires supporting info to help quantify

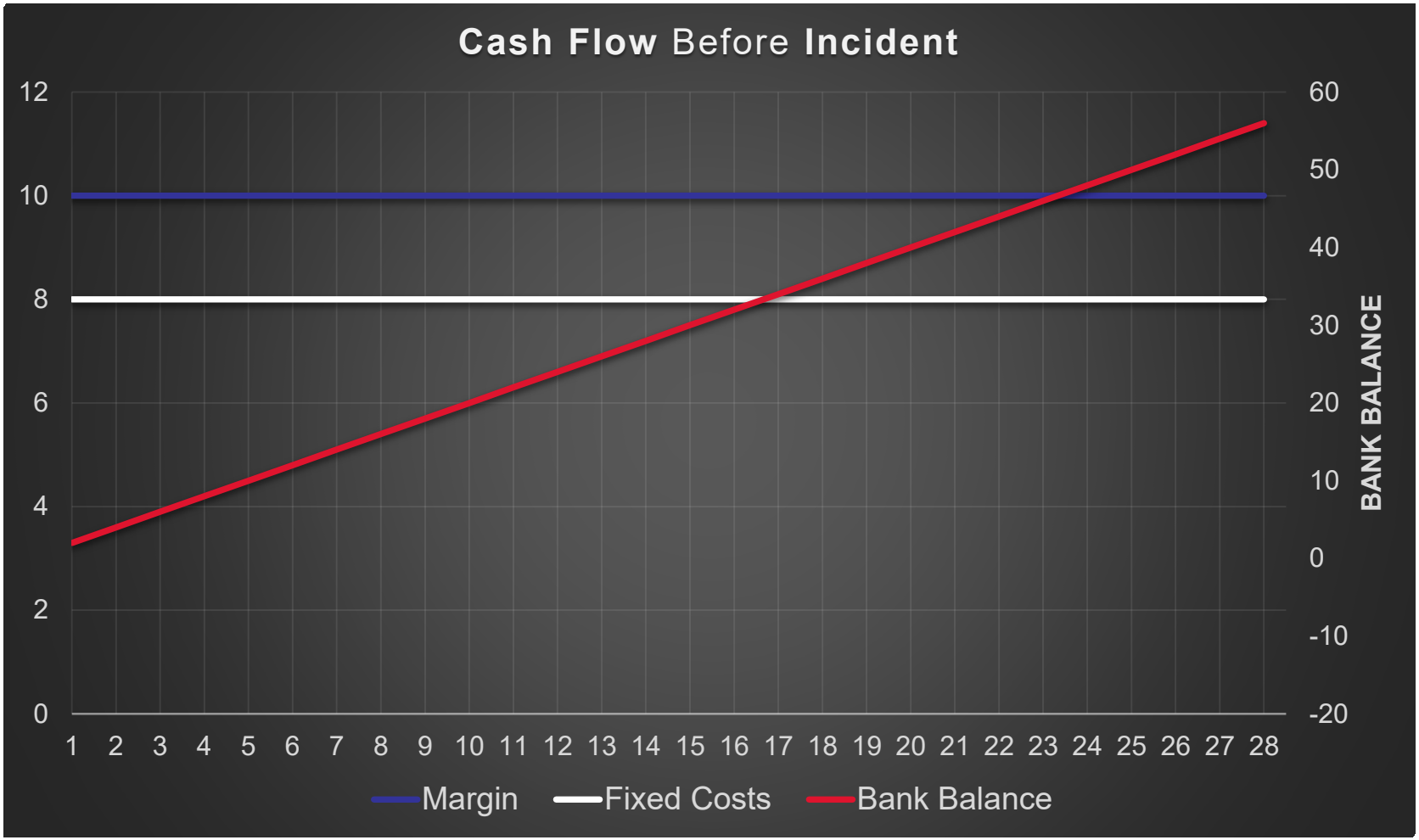
Example Subjectivity



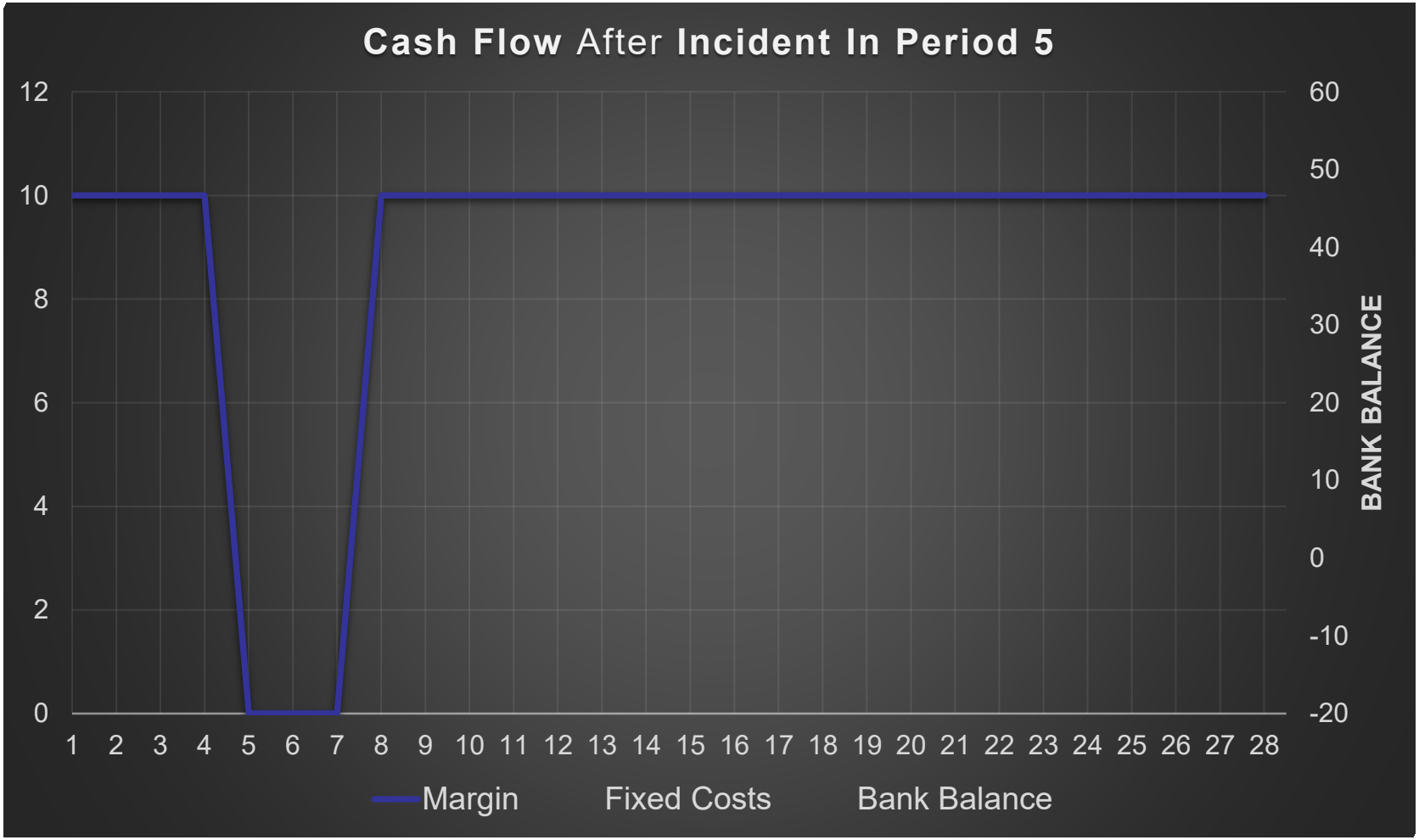
Supporting Subjectivities

- Sales by Customer / Region / Product
- Monthly Profit and Loss Accounts
- VAT Returns
- Annual Accounts
- Budgets and Forecasts
- Production Data
- Explanations to Outliers
- Correspondences with Potential Customers
- Contracts and Agreements
- Industry Data or Statistics
- Data on Web Traffic
- Data on Link Clicks
- Conversion of Web-Visits/Clicks to Purchase
- Information on Bottlenecks

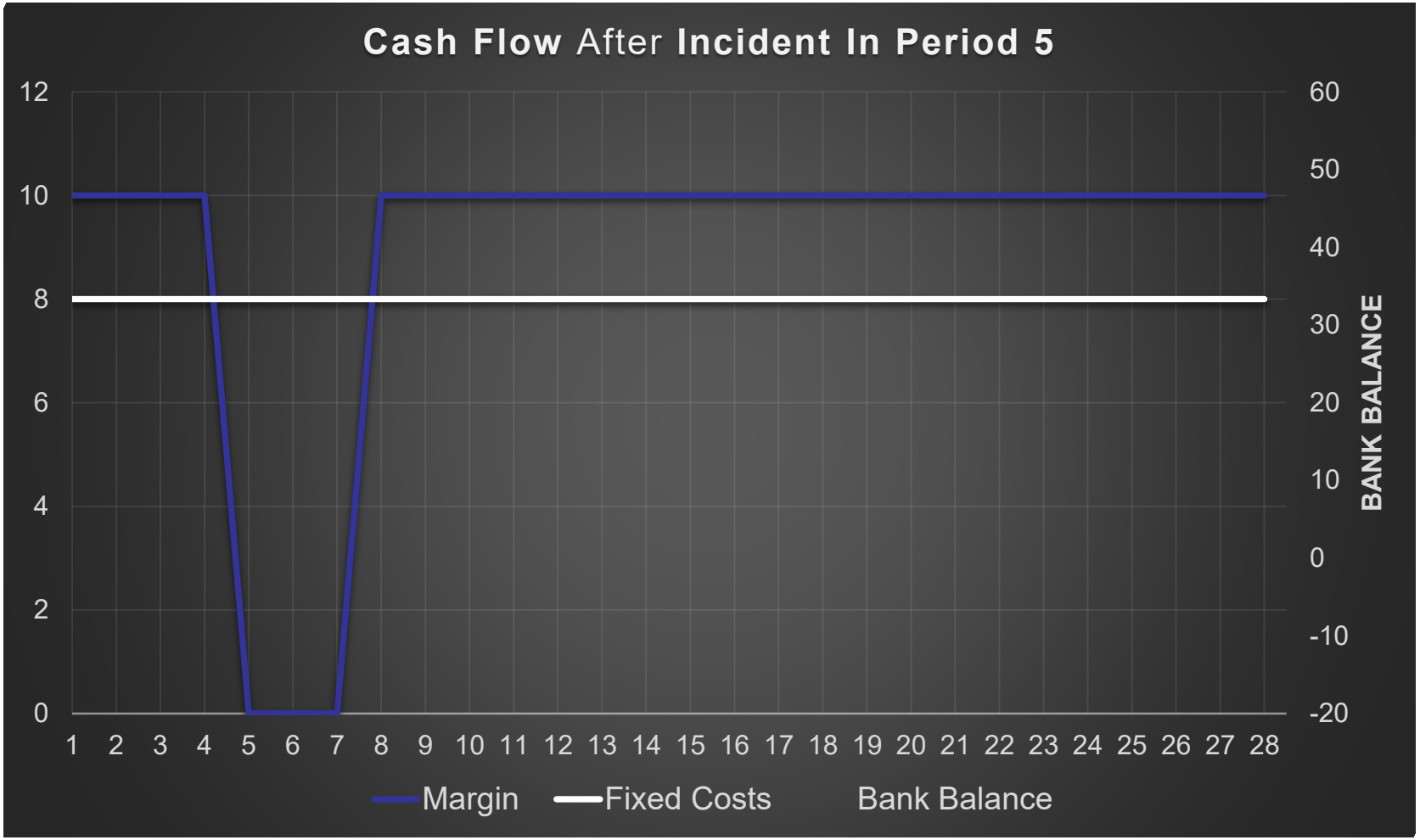
Importance of Cash Flow



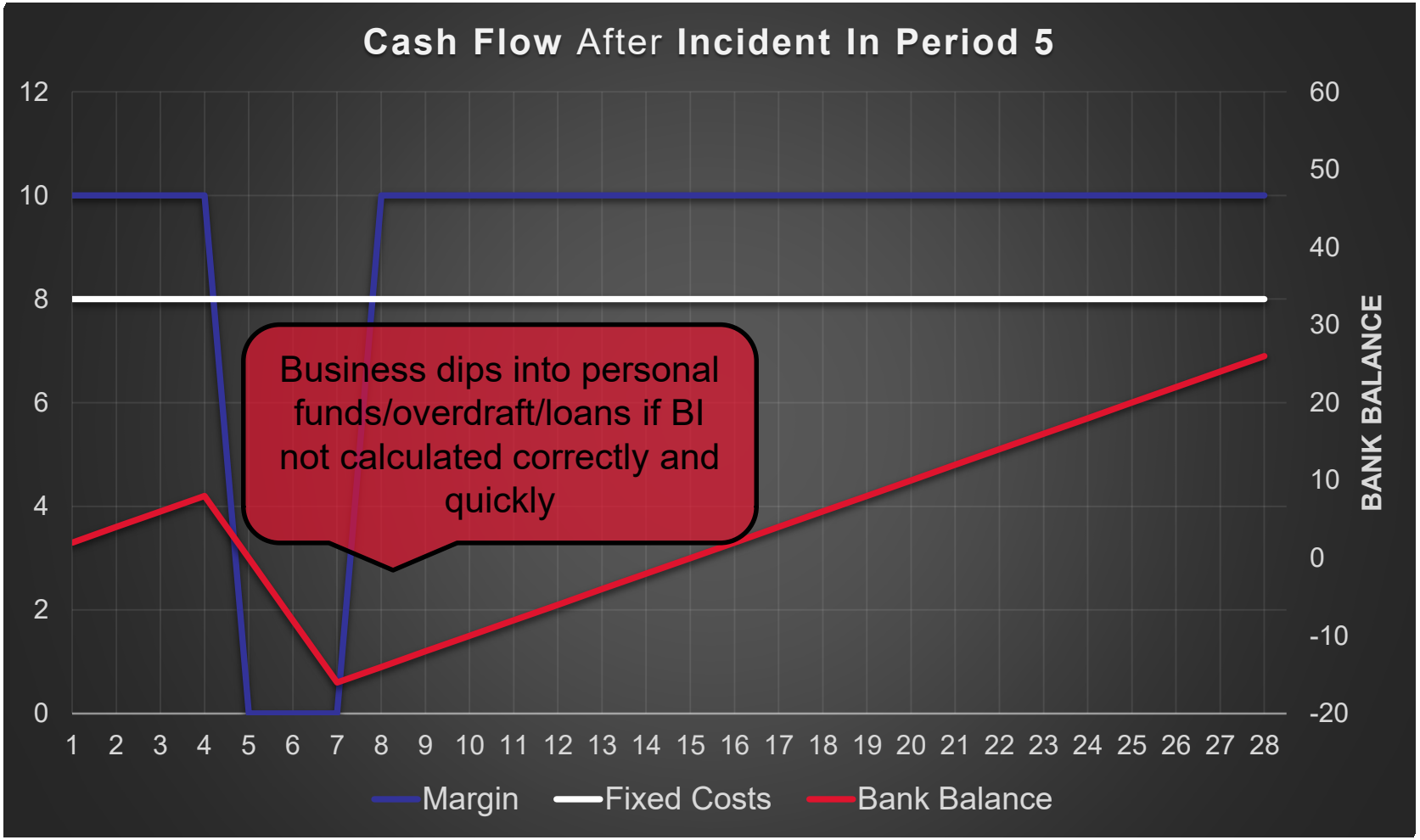
Importance of Cash Flow



Importance of Cash Flow

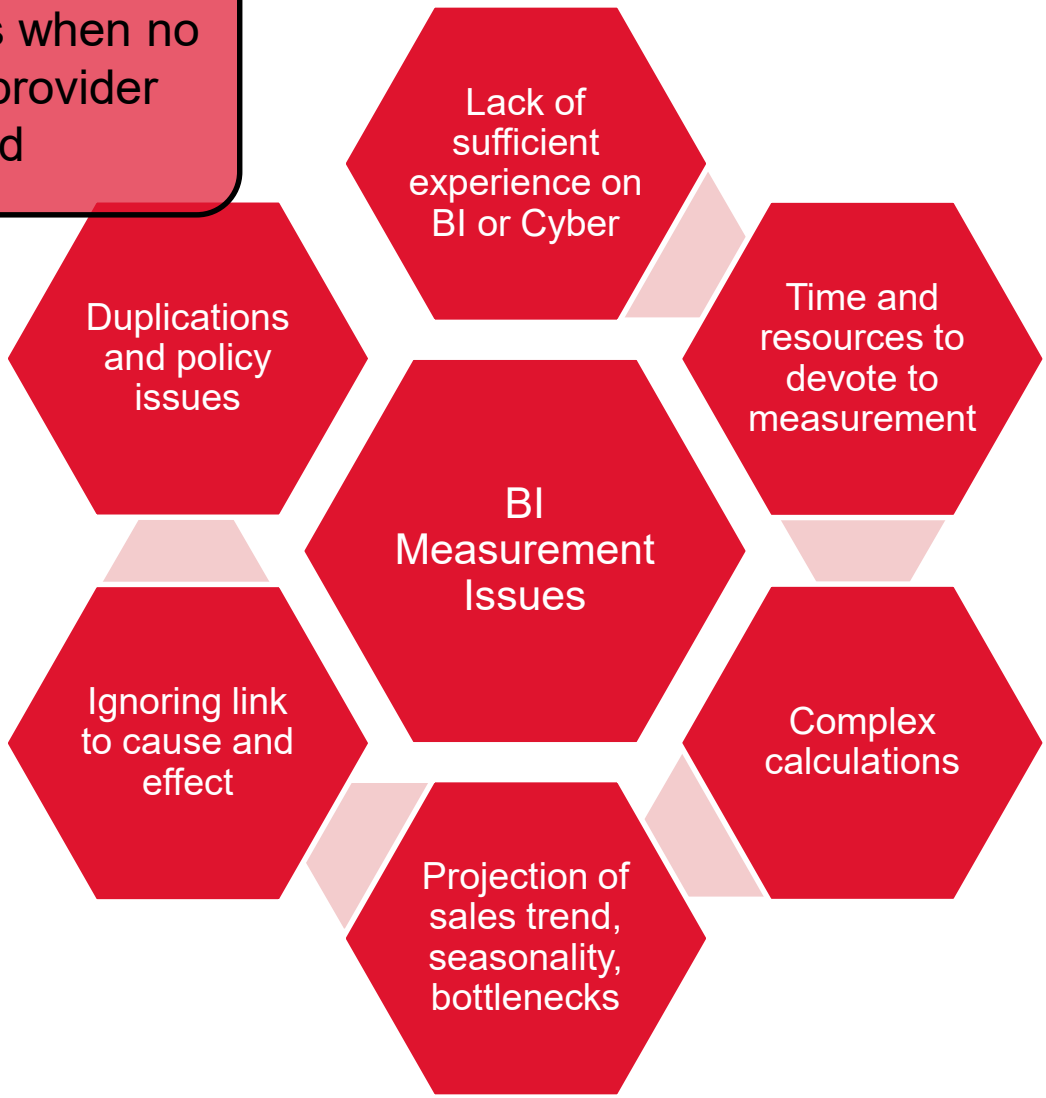


Importance of Cash Flow



Cyber BI Claim Issues

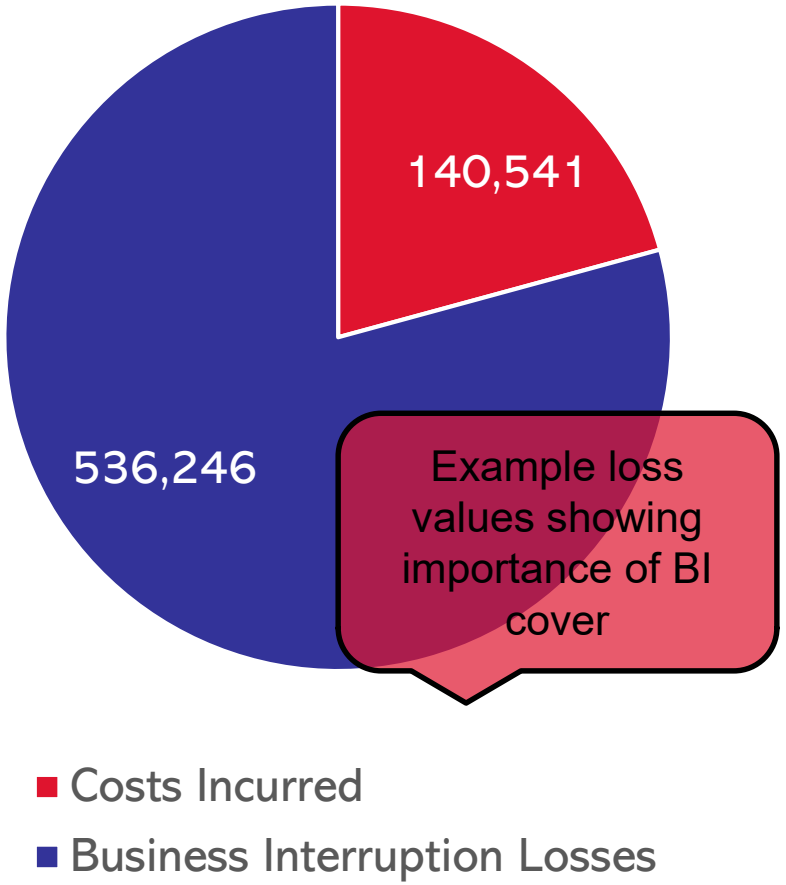
Possible issues when no specialist BI provider involved



How Important Is BI?

Temporary IT equipment	49,103
Assistance on server rebuild and data storage	19,100
System restoration	12,975
Legal handling of matters	12,584
Customer support (salaries)	9,736
Injunction costs	8,264
Ongoing IT assistance	6,350
Scanning network for malware	5,927
Recover old mailboxes. Configure mail server	3,525
Investigation	3,140
Initial IT assistance	2,945
Install and configure new mail servers	2,650
IT Engineer call out charges	1,719
Configure mail servers	1,025
Notification costs	896
Data recovery	603
TOTAL	**140,541**

Mid-Mar 2018	Breach via attachment on phishing email (approx. 2am)
09-May-18	Final server (mail server) configuration completed



Learning Objectives

By attending this event you will gain a further understanding of:

- the growing prominence of cybercrime as a risk to businesses;
- the effects on a business from a cyber breach;
- appreciation of the possible magnitude of economic damage from a cyber attack;
- interpretation of cyber risk policies;
- Business Interruption losses flowing from cyber damage

Thank You

Rajen Rajput
rrajput@mdd.com

www.linkedin.com/in/**rajenr**

MDD

FORENSIC ACCOUNTANTS

Marlow House
1a Lloyds Avenue
London
EC3N 3AA

(T) +44 203 384 5499
(F) +44 203 384 5489
www.mdd.com

London's Partners Contact Details

Flemming Jensen
M +44 7711 416 462
fjensen@mdd.com

Markus Heiss
M +44 7730 985 822
mheiss@mdd.com

Lee Swain
M +44 7714 262 850
lswain@mdd.com

Paul Isaac
M +44 7725 509 918
pisaac@mdd.com

Mark Mangan
M +44 7760 424 660
mmangan@mdd.com

MDD Forensic Accountants **@mdd1933** **MDD Forensic Accountants**

Proprietary & Confidential

Proprietary and Confidential – This presentation contains information that is confidential and proprietary to MDD Forensic Accountants and may contain trade secrets. It is intended to be strictly confidential and is to be used solely for discussion purposes. No part of this presentation may be disclosed to any third party or reproduced by any means without the prior written consent of MDD Forensic Accountants. This presentation does not constitute work product, opinion or a deliverable.

This presentation contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. MDD Forensic Accountants does not accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this presentation. On any specific matter, reference should be made to the appropriate advisor.

MDD Forensic Accountants refers to one or more of MDD International Limited, a UK private company limited by guarantee ("MDD-International"), its network of member firms, and their related entities. MDD International and each of its member firms are legally separate and independent entities. MDD International does not itself engage in the provision of services to clients.