Cyber - From Risks to Claims Including Business Interruption – Part 2

Tue 14 January 2020

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

Tick indicates covered in Part 1

London Office Timeline

1933

Founded as Johnson Atwater & Co in Chicago

1979

Became Matson, Driscoll & Damico with 4 U.S. Offices

1991

Founding partner Norm Matson opens London office at Guild House

2019

MDD London has 5 partners and 18 accounting staff who speak 13 languages

Practice Areas

Builders' Risk Claims & Soft Costs Claims

Business Disputes & Shareholder Disputes

Business Interruption

Business Valuations

Catastrophe Services

Class Actions

Contingency Claims & Entertainment Claims

Cyber Risk

Areas in RED are our core Practice Areas

Practice Areas

Disability & Workers Compensation Claims

Divorce & Marital Disputes

Environmental Damage Claims

Expropriation

Extra Expenses/ Increased Costs

Fidelity Claims

Franchise Litigation

Fraud & Investigations

Areas in RED are our core Practice Areas

Practice Areas

Intellectual Property

Litigation Support

Mining Claims/
Refining Claims

Personal Injury &
Wrongful Death

Liability Losses

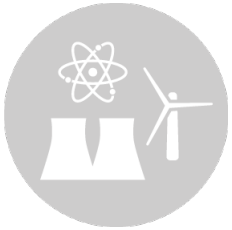
Lost Profits

Oil & Gas

Physical Damages

Areas in RED are our core Practice Areas

Practice Areas



Power Generation

Product Liability &
Product Recall

Reported Insurance
Values

Stock &
Contents Loss

Subrogation

Surety Bond & Funds
Control Services

Toxic Torts

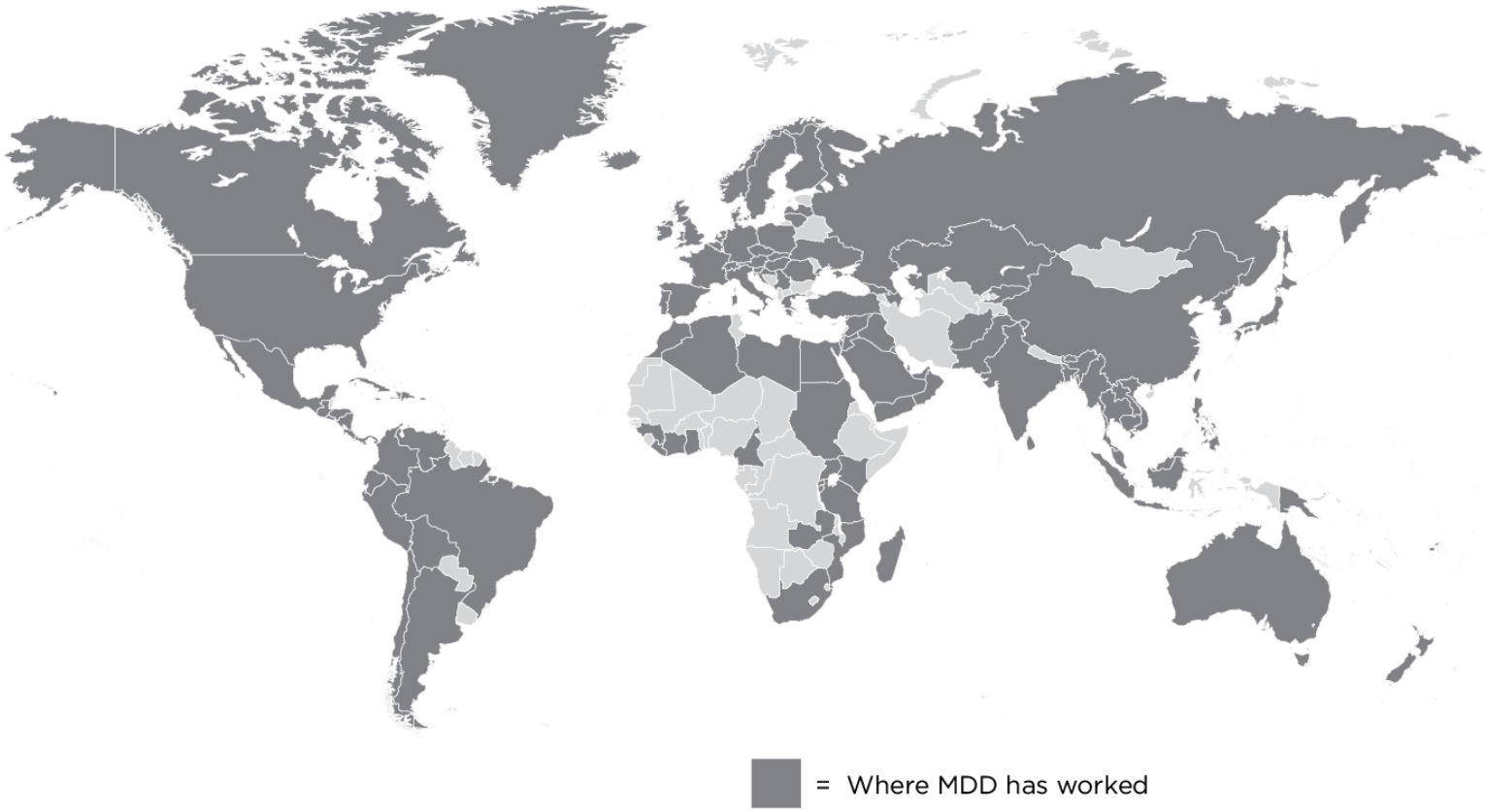
Valuable Papers

Areas in RED are our core Practice Areas

What Sets Us Apart

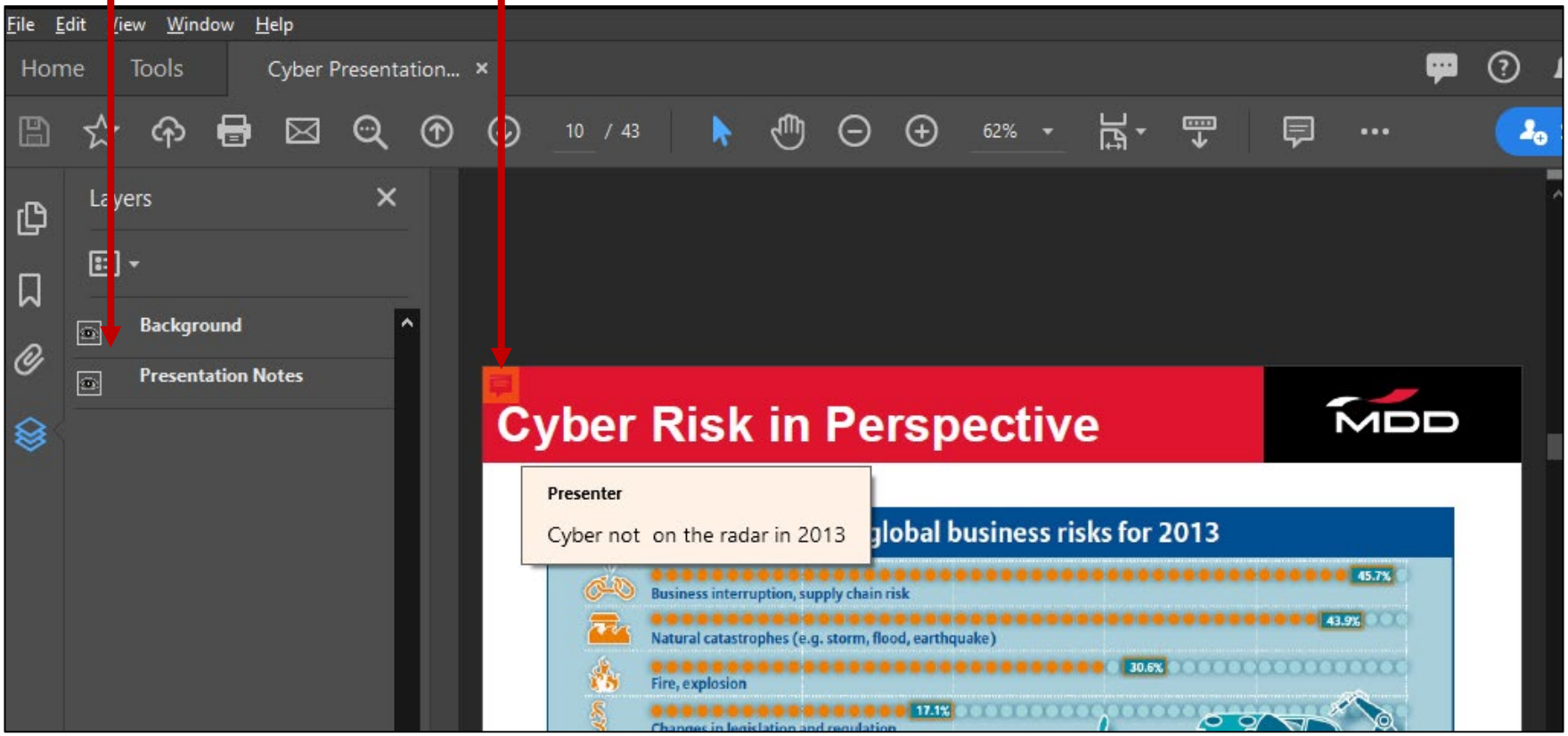
- Significant experience in 800 industries
- Strong litigation and expert testimony background
- Few, if any, conflicts
- Extensive Global Resources across 5 continents, all 100% MDD offices
- Ongoing internal training for accountants
- More than 10 language fluencies in London office alone

Where We Have Worked

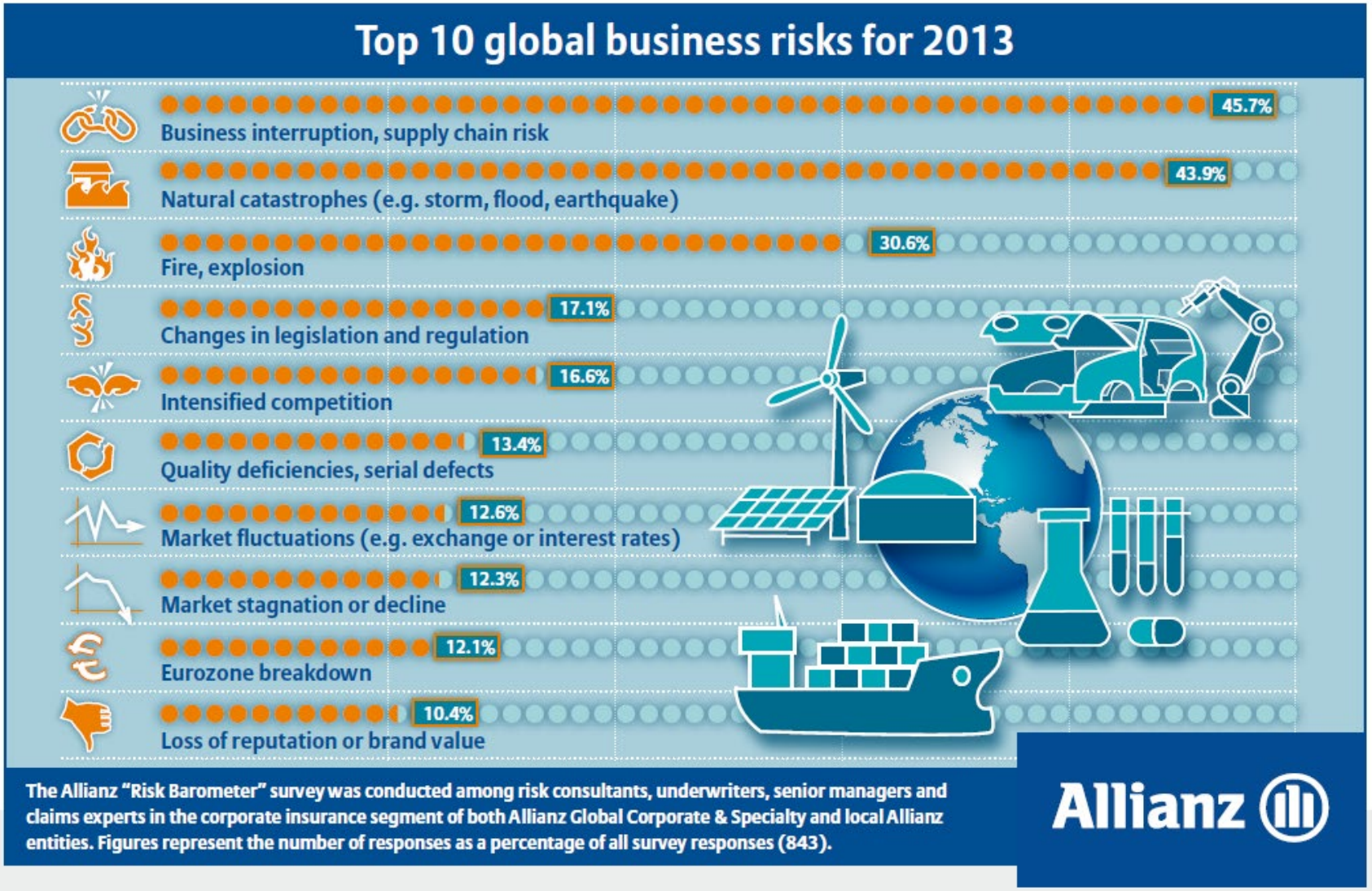


Notes

If you switch on the layers in Adobe Reader and then hover the cursor in the corner of a slide, you will obtain context on the slides



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 Language

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

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

Cybercrime on the Rise

Anonymity and Deep Web

Inability to trace crime back to bad actor

Ease of malware purchase

Liquidity

Speed or ease of converting data or information to money

Movement of Funds

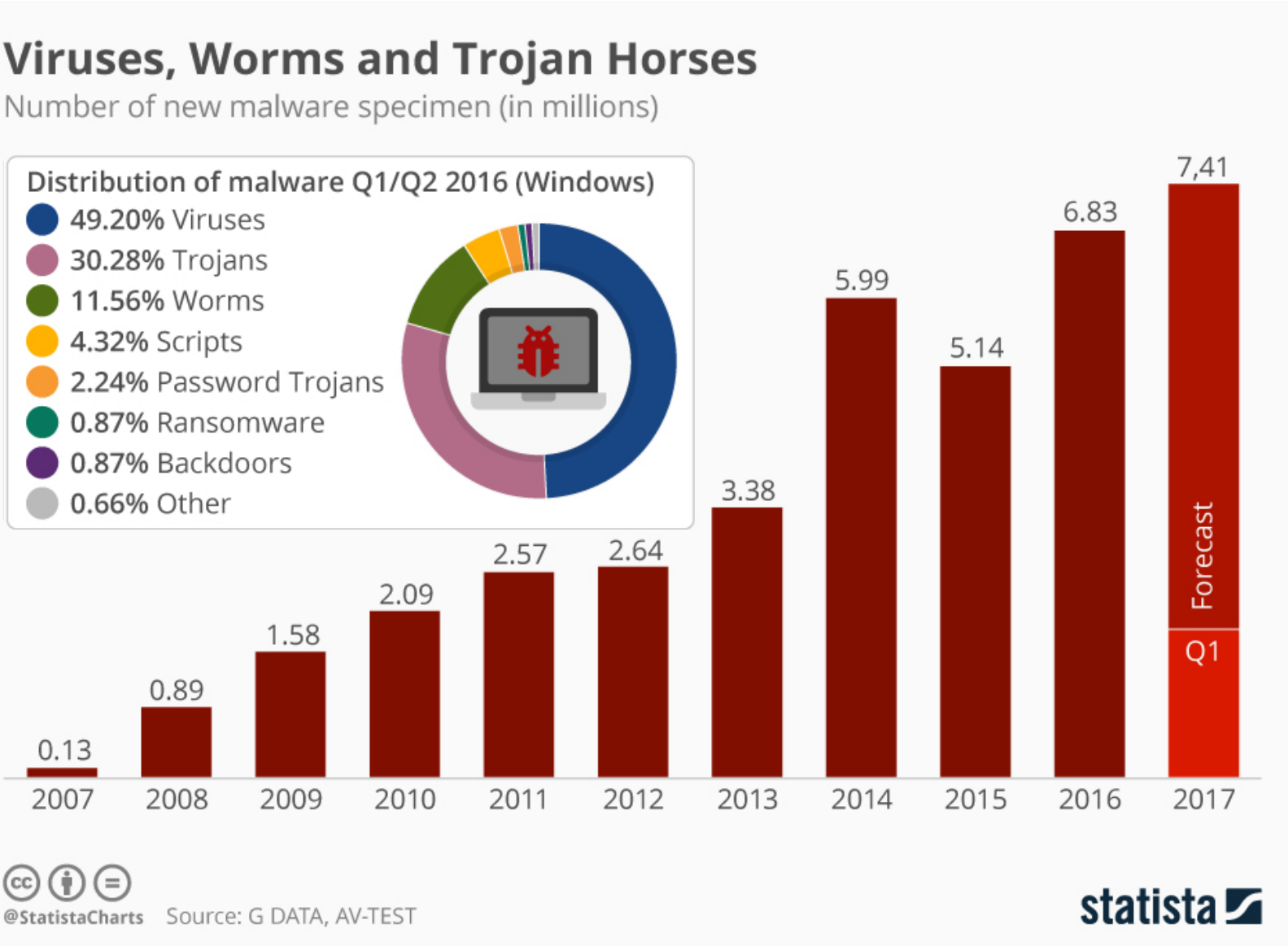
Further anonymity once monetised and ease of laundering

Internet of Things

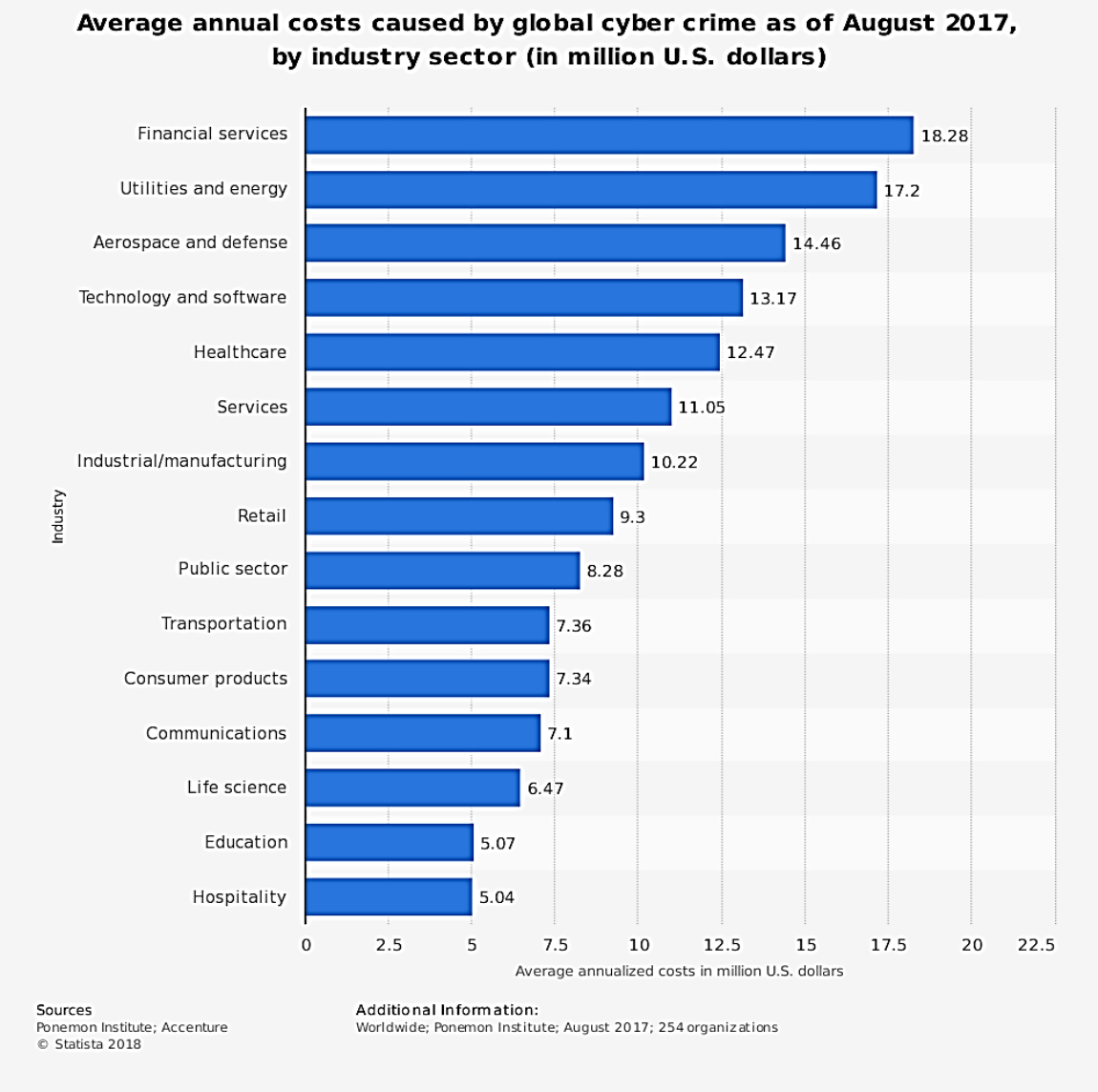
Increasing amount of devices or ‘doorways’

Many with weak or out-of-date security

Cybercrime on the Rise



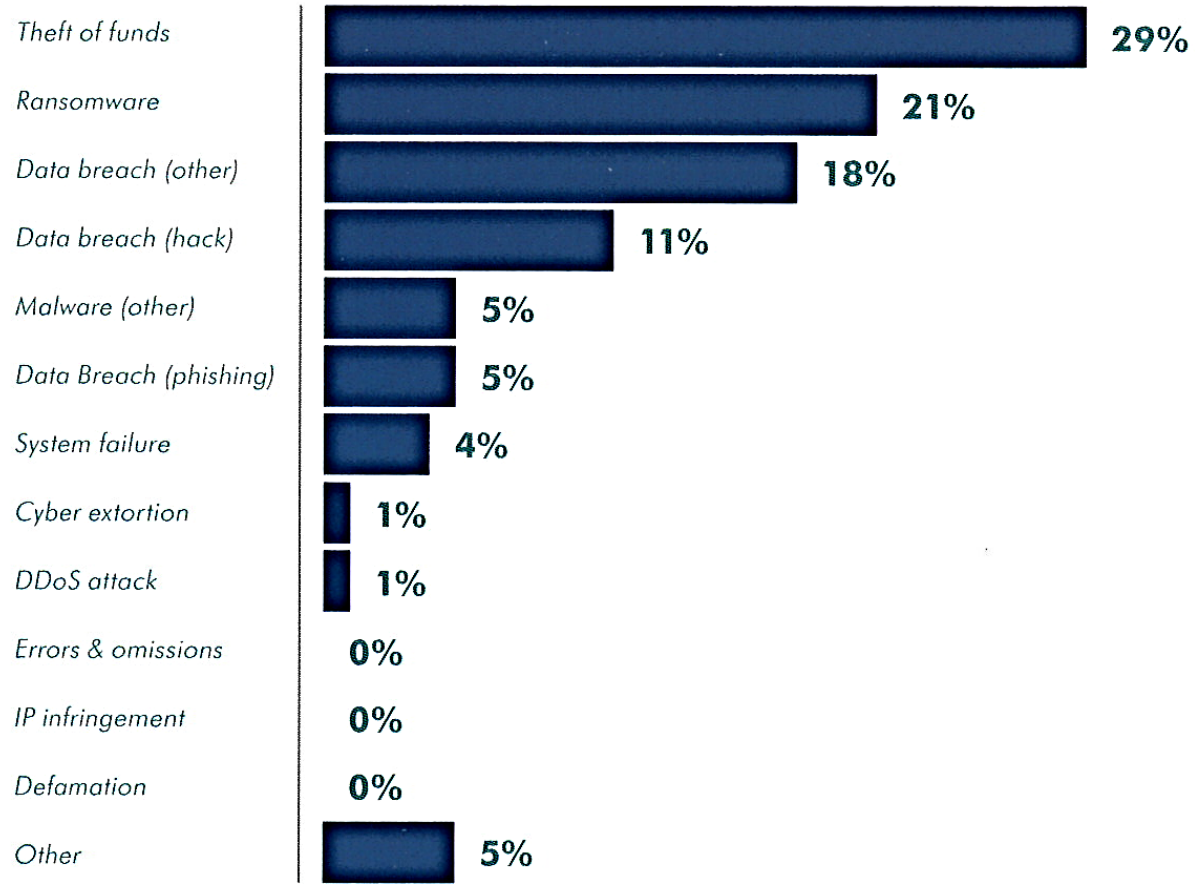
Cybercrime on the Rise



Who is getting hit the hardest?

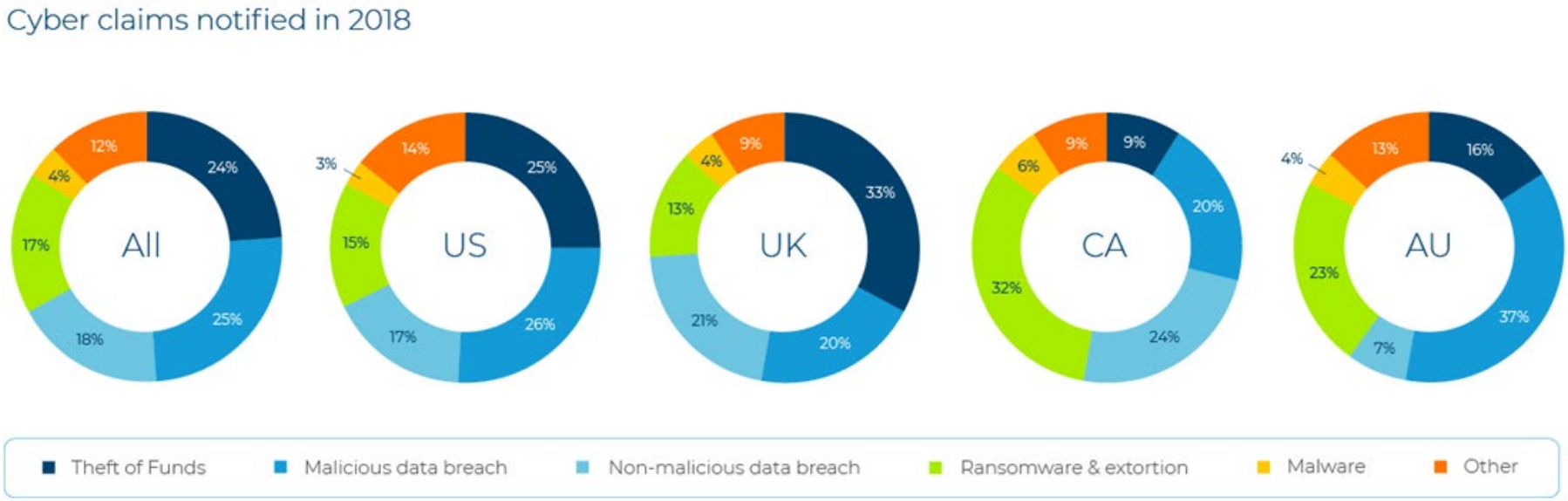
Cybercrime on the Rise

KEY 2017 CYBER STATISTICS



CFC Underwriting cyber claims statistics, 2017

Cybercrime on the Rise



Source: CFC Underwriting

Cybercrime on the Rise

Current News

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

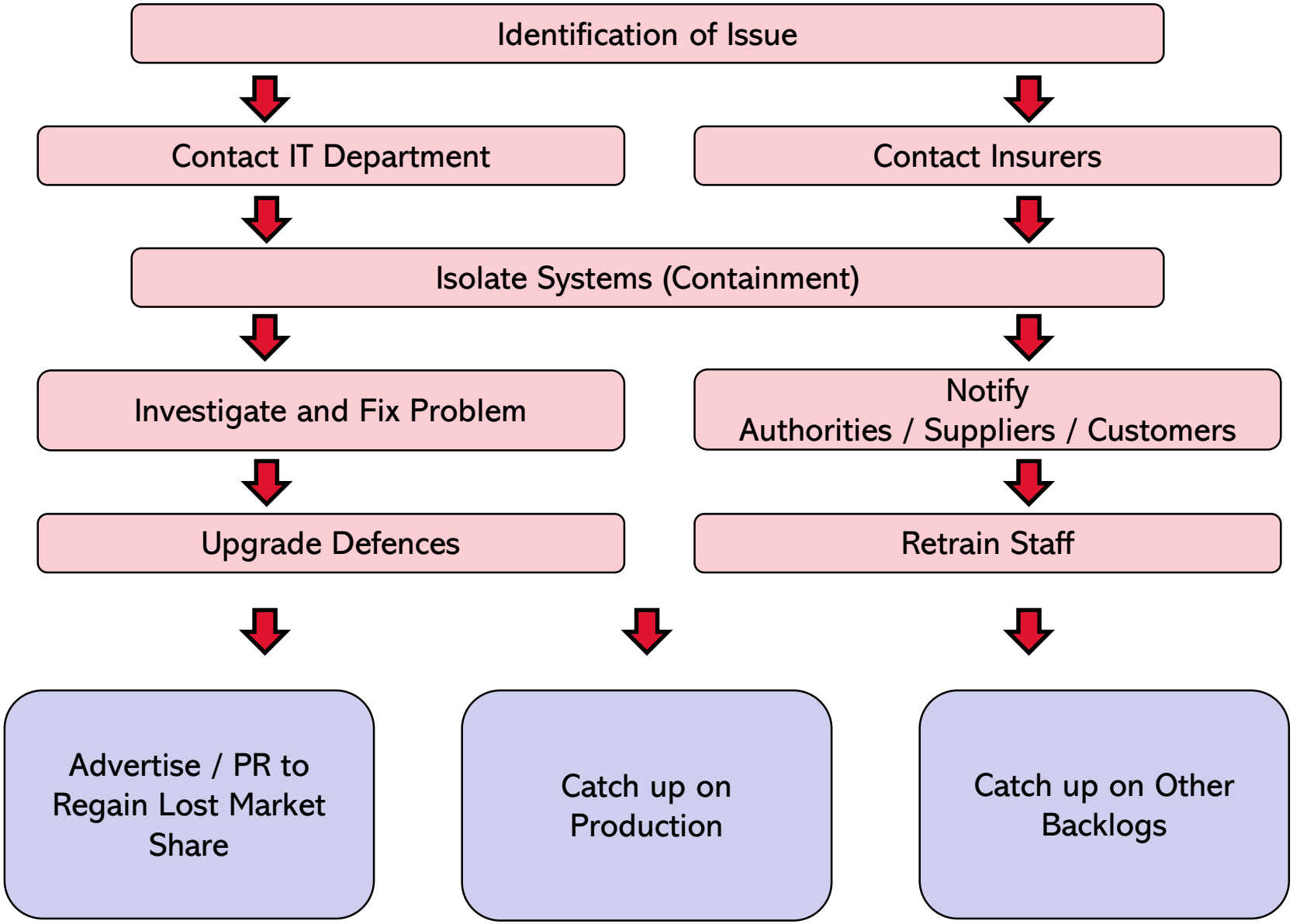
Lower IT security and protections
(prevention and detection)

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

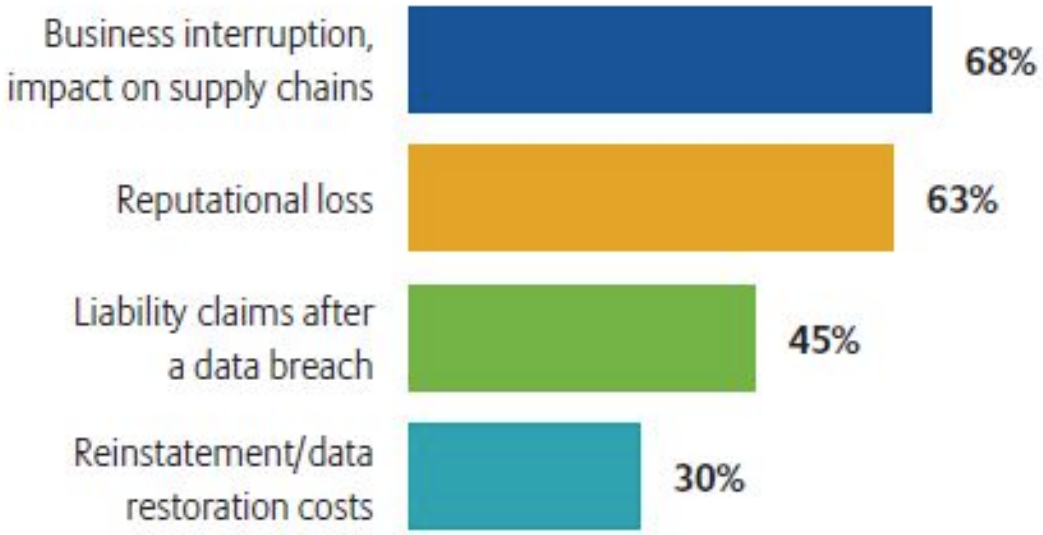
Road to Recovery



Services Provided

Cause

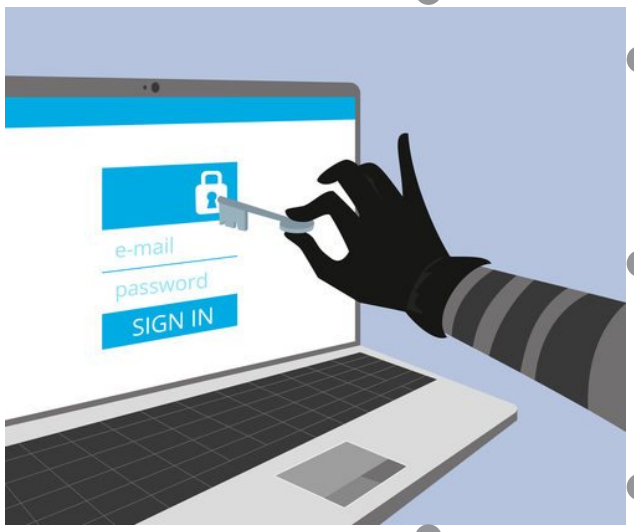
What are the main causes of economic loss after a cyber incident?



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

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

Example Wordings

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.

Example Wordings

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.

Example Wordings

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.

Example Wordings

Business Interruption:

We will pay your:

i. loss of income;

ii. increased costs of working; and

iii. additional increased costs of working …

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

Example Wordings

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:*

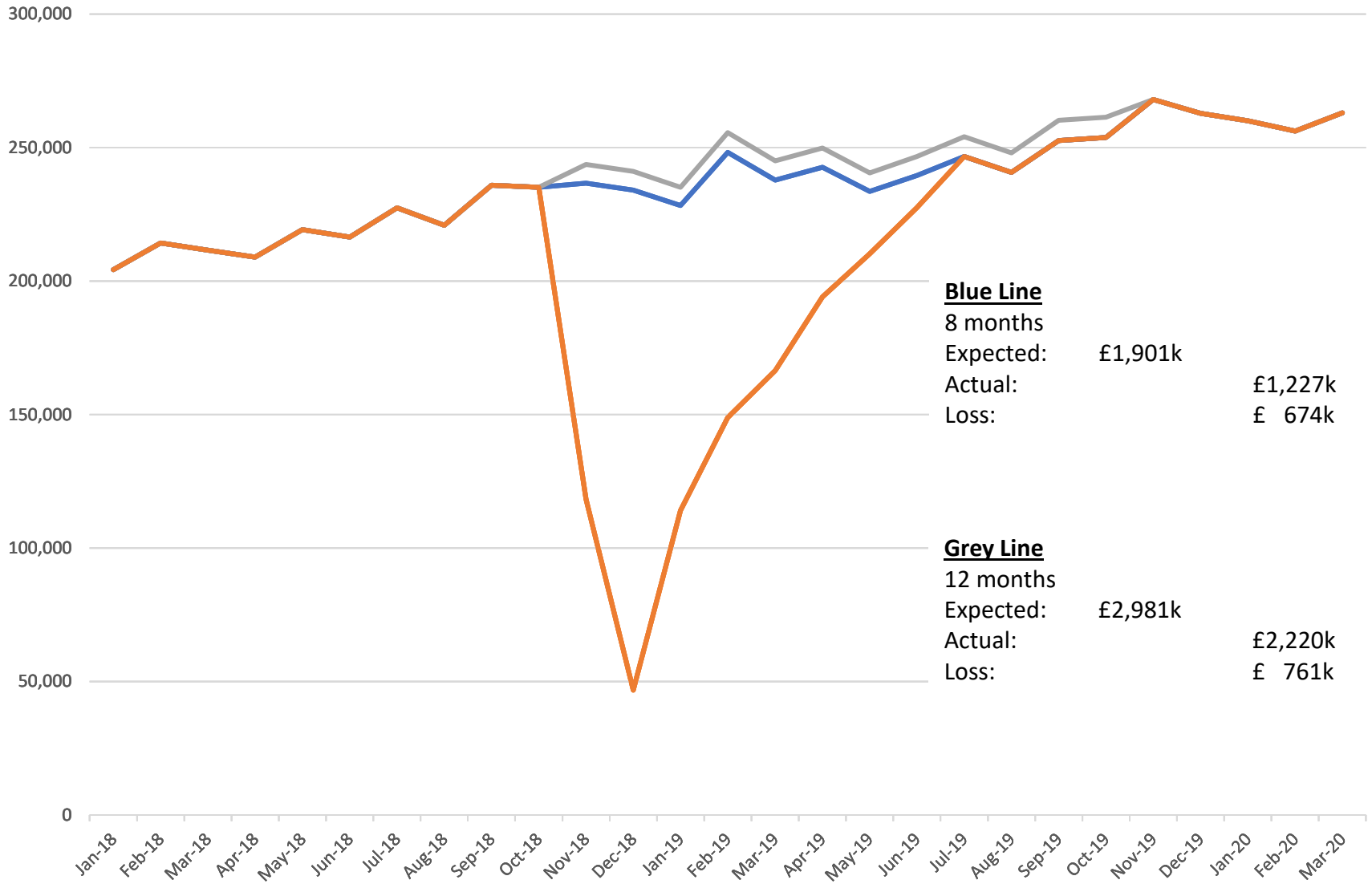
1. the date when the business operations have been restored substantially to the level of operation that existed prior to the interruption; or

2. three hundred and sixty five (365) days after the business operations have first been interrupted.

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	

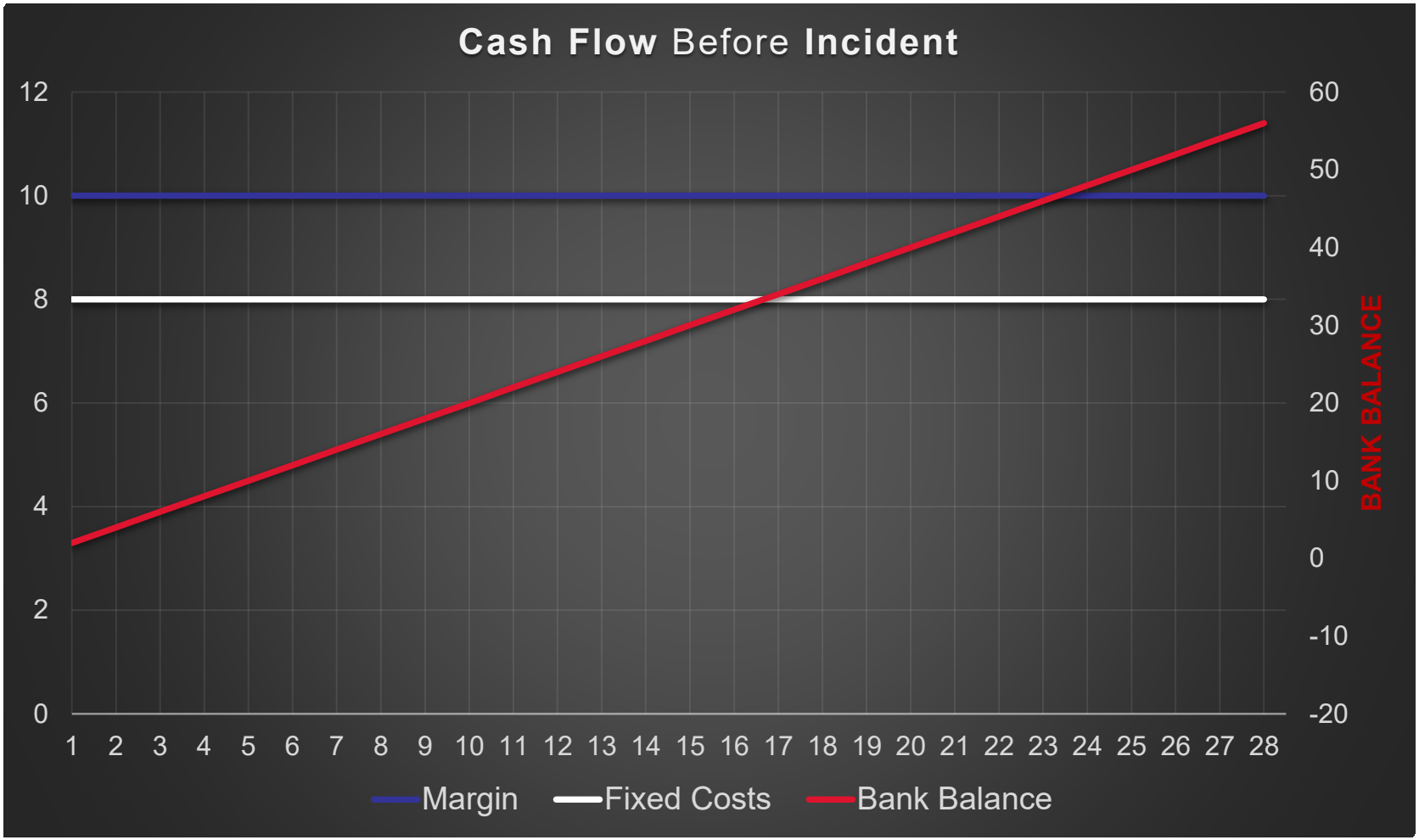
Example Subjectivity



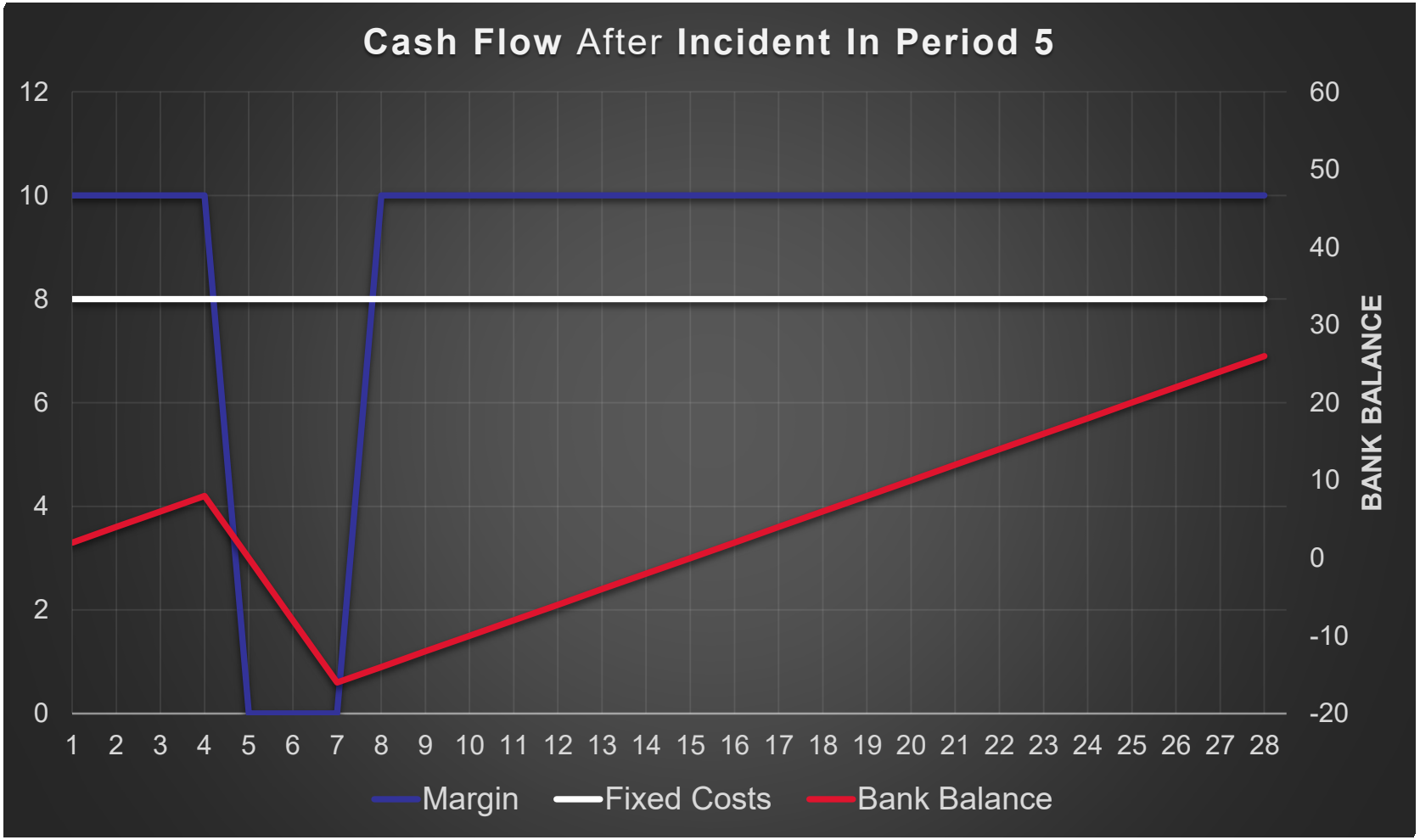
Supporting Subjectivities

- 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 With Existing
- Daily (Sales etc) Data If Short Impact Cyber
- 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



Case Study 1

UK Legal Firm Operating From Several Offices in UK

- Incident
  - Hit by ransomware. Database with client information encrypted.
  - Attacker exfiltrated data prior to encryption and posted samples on deep web and demanded ransom to stop posting further.
- Effect
  - Systems down, including emails. Management and staff contact via WhatsApp.
  - No chargeable time during outage.
  - Lost turnover from inability to conduct conflict checks on new work.
  - Possible loss of reputation may manifest in future turnover reduction.
  - Significant ICO report costs as very sensitive client information exfiltrated.
  - Servers quarantined for inspection and therefore required to purchase replacements.
- Considerations
  - Policy required BI losses to cease when business operations had been restored substantially to the level of operation that existed prior to the interruption. This could have been debatable
  - Granular loss of profit calculation based on chargeable hours (with varying rates and seasonality) instead of high level monthly turnover normally used in PD claims

Case Study 2

- **UK Car Manufacturing Plant**
  - Incident
    - Hit by ransomware. Infection via social engineering (email attachment click, vpn connection).
    - Malware flooded through admin network to production floor network.
    - Ethernet cables unplugged. Wi-Fi switched off. All internet connectivity intentionally cut-off to stop propagation.
  - Effect
    - No admin or production computers operational.
    - Management and staff contact via WhatsApp.
    - Sales are on a ‘pull’ basis and orders delayed. – Loss of orders where cancelled.
    - JIT production: Increased costs of inbound deliveries and temporary storage as piecemeal. Airfreight costs replaced shipping for expedited parts.
    - Stock loss of hybrid battery packs due to machines stopping midway through production and potentially unsafe to consumers if produced in two rounds.
    - Machinery repair costs on dried paint on spray heads.
  - Considerations
    - Replacement/upgrade to legacy software did not immediately communicate with machines. Machines needed to be reprogrammed and this was not foreseen.

Case Study 3

Beauty Products Distributor

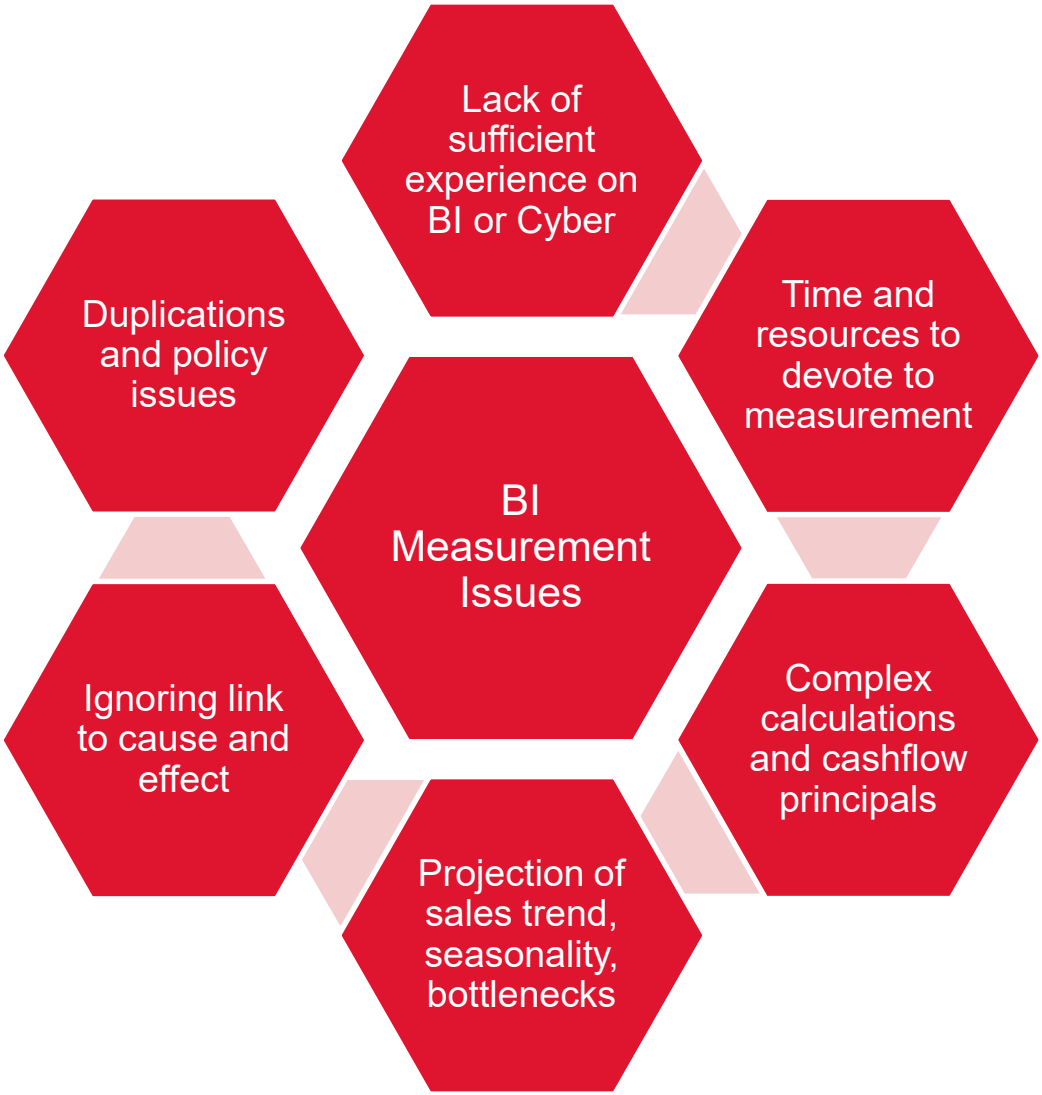
- Incident
  - Hit by ransomware. Inventory system encrypted. Some personnel information encrypted.
  - Backups failed. Server rebuilt over 11 days using snippets of configuration from ad-hoc and scattered backups.
- Effect
  - Loss of visibility of inventory. No outbound or inbound orders possible.
  - Customers and suppliers made aware as initially no idea how long to restore.
  - Loss of turnover due to KPI's not met for a large retailer and product delisted.
  - Potential compromise of personal data. Call centre set up and credit monitoring facility offered to potential victims.
  - Staff overtime costs to recount stock and repopulate inventory management system.
  - No inbound or outbound deliveries during initial No admin or production computers.
- Considerations
  - Loss of turnover to delisted product lasts longer than 12 month indemnity period.
  - Daily sales used for basis of loss estimate with differing margins for different product lines (only one delisted, others generally affected), rather than monthly overall sales and margin. This in-depth analysis produces a more accurate loss measure.

Case Study 4

Hotel Booking Agent For Specific Chain

- Incident
  - Temporary and intentional website repointing to sister website while planned website maintenance took place.
  - After maintenance IT contractors had difficulty re-pointing DNS back to original website.
  - Maintenance was planned to take four days. Additional three days for successful repointing.
- Effect
  - Loss of turnover due to repointed customers uncomfortable with ‘unfamiliar’ website (in different currency’ to make booking.
  - 2,100 bookings lost at Insured’s website over three days, with 800 offset by sister website. Loss of 1,300 bookings @ £85.
- Considerations
  - Possible offset of bookings to agents such as bookings.com
  - Subjective to project “but for” after the planned maintenance as there would have been a recovery curve over initial loss period.
  - Bookings analysed by webdomain on a per-booking basis to identify (a) financial loss, (b) end of restoration period to nearest hour and (c) 12 hour deductible.

Cyber BI Claim Issues



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

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.