LLOYD'S

Cyber and Business Continuity Management

23rd August 2017

LLOYD'S

Case studies

Target

At a glance:
The theft and sale of more than 40m credit card details from Target's point-of-sale terminals cost the large retailer almost $100m in litigation, with a similar amount spent upgrading the company's retail systems.

Type of attack: Malware

Total immediate cost: $60m

Total slow-burn cost: more than $219m

Total gross cost: more than $279m

What happened?
Between 27 November and 15 December, 2013 more than 40m credit card details and 70m pieces of personal information were stolen from Target, a major US retailer. An organised crime cyber-attack on its point-of-sale terminals resulted in stolen card details being sold on the black market, with prices varying from a median of $18-$35.70 per card. Similar attacks followed on a number of other major US retailers[12].

TalkTalk

At a glance:
The theft of more than 150,000 customer details resulted in one-off costs in excess of $52m and a 10% share price decline for one of the UK's largest telcos.

Type of attack: DDoS, followed by SQL injection

Total immediate cost: $52m

Total slow-burn cost: more than $44m (including estimate for lost revenue)

Total gross cost: more than $96m

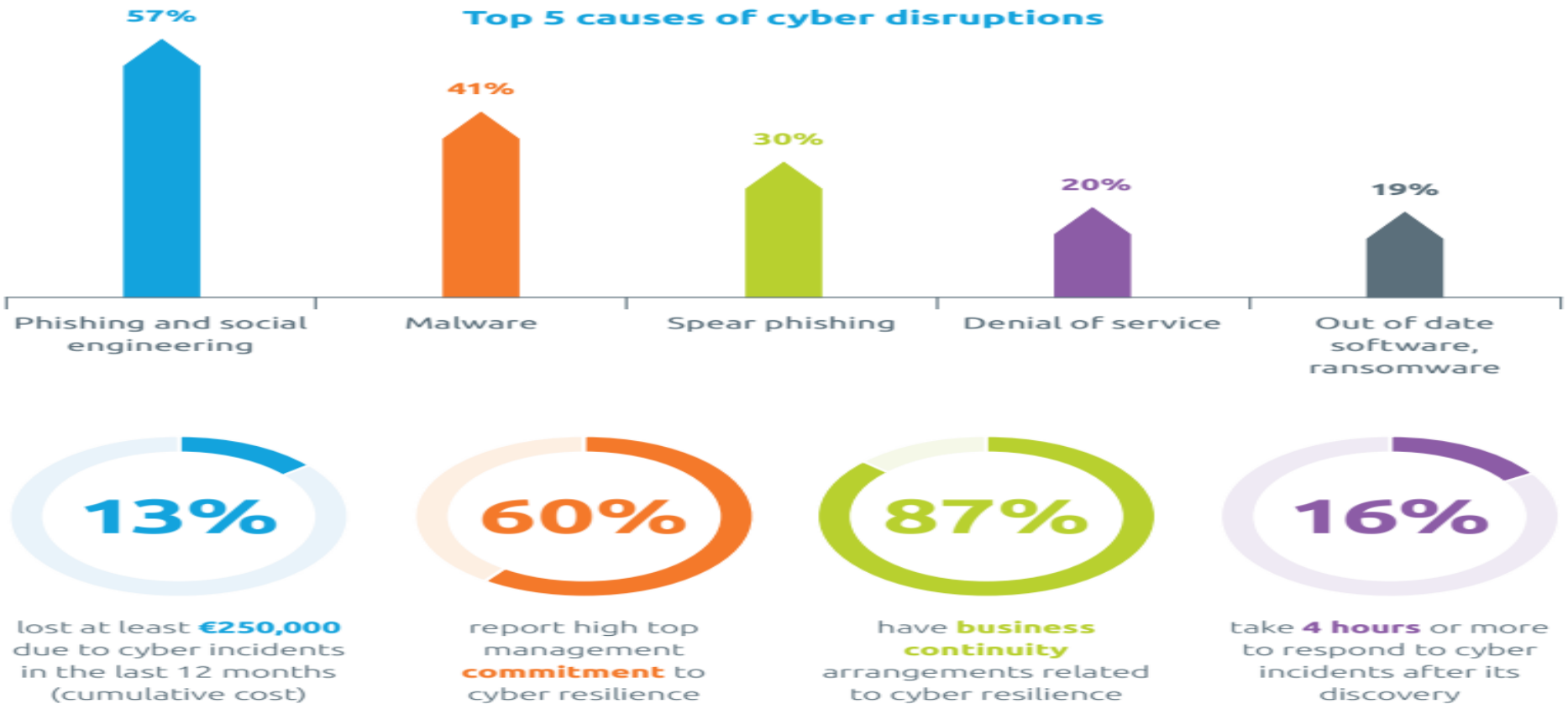
What happened?
In October 2015, TalkTalk was the victim of a major cyber breach, leading to the theft of 156,959 customers' personal details, 15,656 bank account numbers and sort codes, and some 28,000 credit and debit cards that were obscured[21]. The police arrested two teenage suspects shortly after the attack[22], and one 17-year-old subsequently admitted hacking offences linked to the TalkTalk data breach[23].

Source: Closing The Gap Report 2017, Lloyd's

Costs of an incident

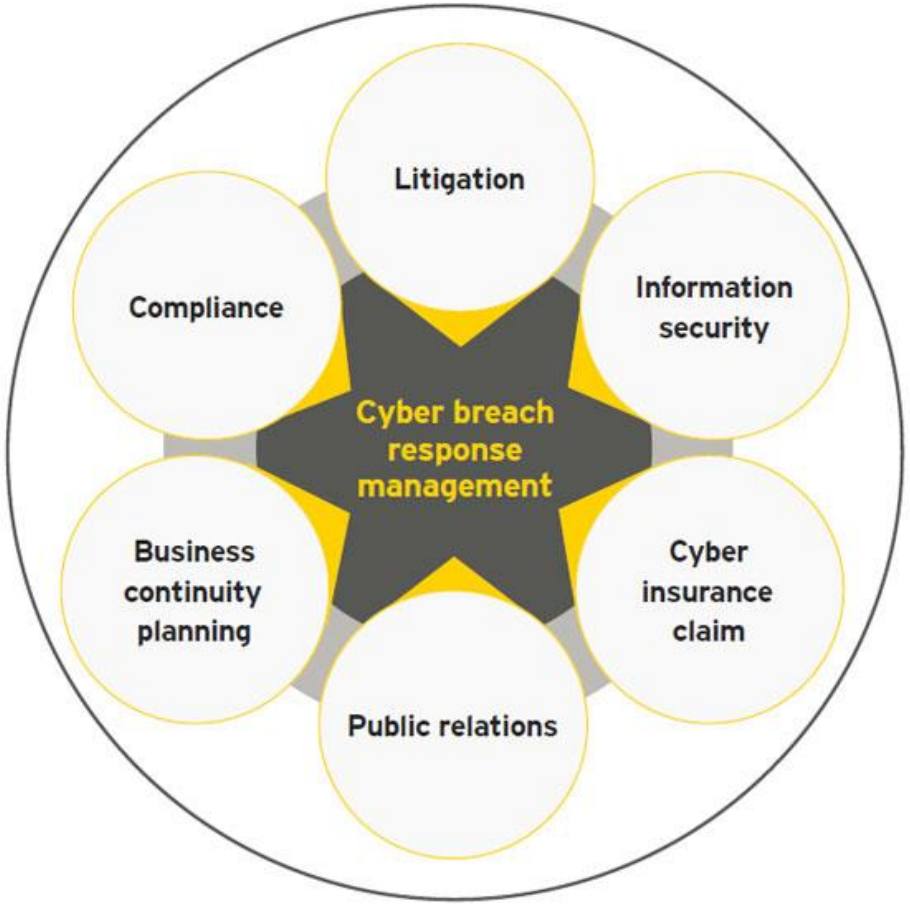
Source: Closing The Gap Report 2017, Lloyd's

BCI Resilience Report 2017



Source: BCI Cyber Resilience Report 2017

E&Y proposed framework



Source: EY Cyber breach response management report, 2015

BCM for cyber…….

Make sure everyone is aware of the threats and what they can do to help

Exercise and test – validate your approach and plans

Implement the appropriate technical and business strategies

Risk Assessment – what are the risks / likelihood / probability?
Part of Risk Mgmt framework
What would be the impact - BIA?

Design your response – how will you be able to recover, who needs to be involved?

Source: BCI Good Practice Guidelines

LLOYD'S

What do businesses do

Source: BCI Cyber Resilience Report 2017

Preparation

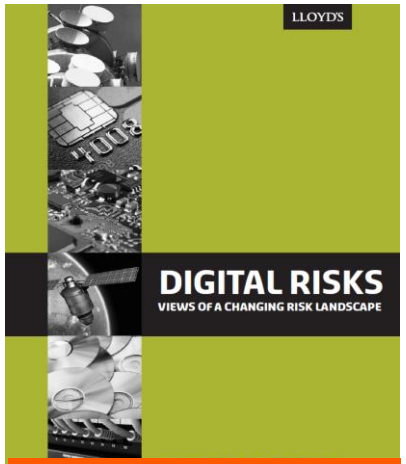
- Include cyber as one of the risks reported through your risk management framework, including defined appetite and metrics
- Understand how systems interact and share data
- Assess what the impact on business would be for the different types of cyber-event
- Define how your organisation would respond – specific cyber plan or adapt crisis plans already in place?
- Identify any additional people required to assist response – e.g. legal
- Train your responders and exercise your plans
- Run staff awareness campaigns – everyone has a role to play
- Understand how your supply chain may be impacted because of cyber events
- Investigate how insurance cover may help your response

Response

- IT escalate the issue before it gets out of hand
- Communications/media/PR – be honest and succinct
- Use legal and compliance people as part of the response
- Use forensics and government / law agencies
- Implement pre-defined workarounds
- Address the impact of corrupted back-ups
- Lloyd's minimum standard

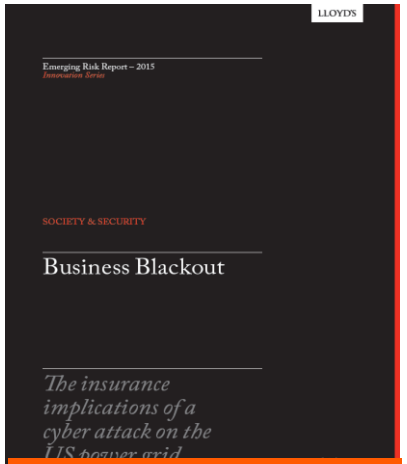
Our digital world

Lloyd's thought leadership catalogue

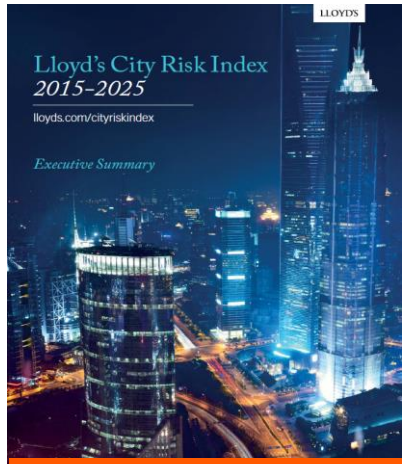


2009

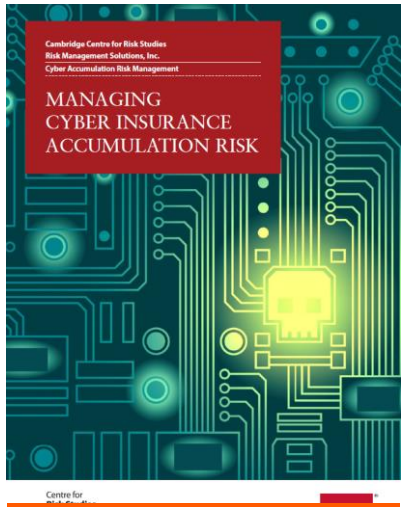
2010



2015

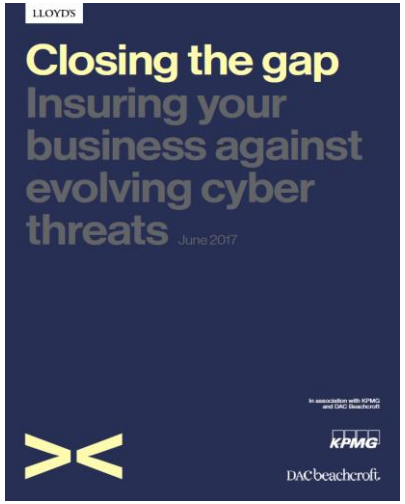


2015

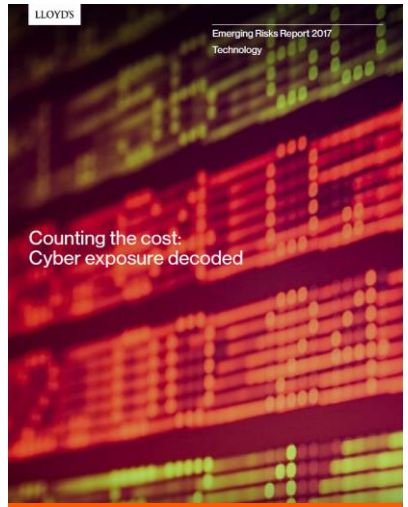


2016

2016



2017



July 2017