HERMENEUT Case Study Approach

Alexander Szanto

Brandenburg Institute for Society and Security (BIGS)

Safe and Ethical Cyberspace, digital assets and risks:
How to assess the intangible impacts of a growing phenomenon?

The World Conference on Intellectual Capital for Communities

UNESCO, June 14&15 2018

iC 14
Intellectual Capital for Communities In the Knowledge Economy

Outline

I. Sector-Specific Case Studies

   i. Structure of the Case Studies

   ii. Examples for each Sector

   iii. Lessons learnt

iC 14
Intellectual Capital
for Communities
In the Knowledge
Economy

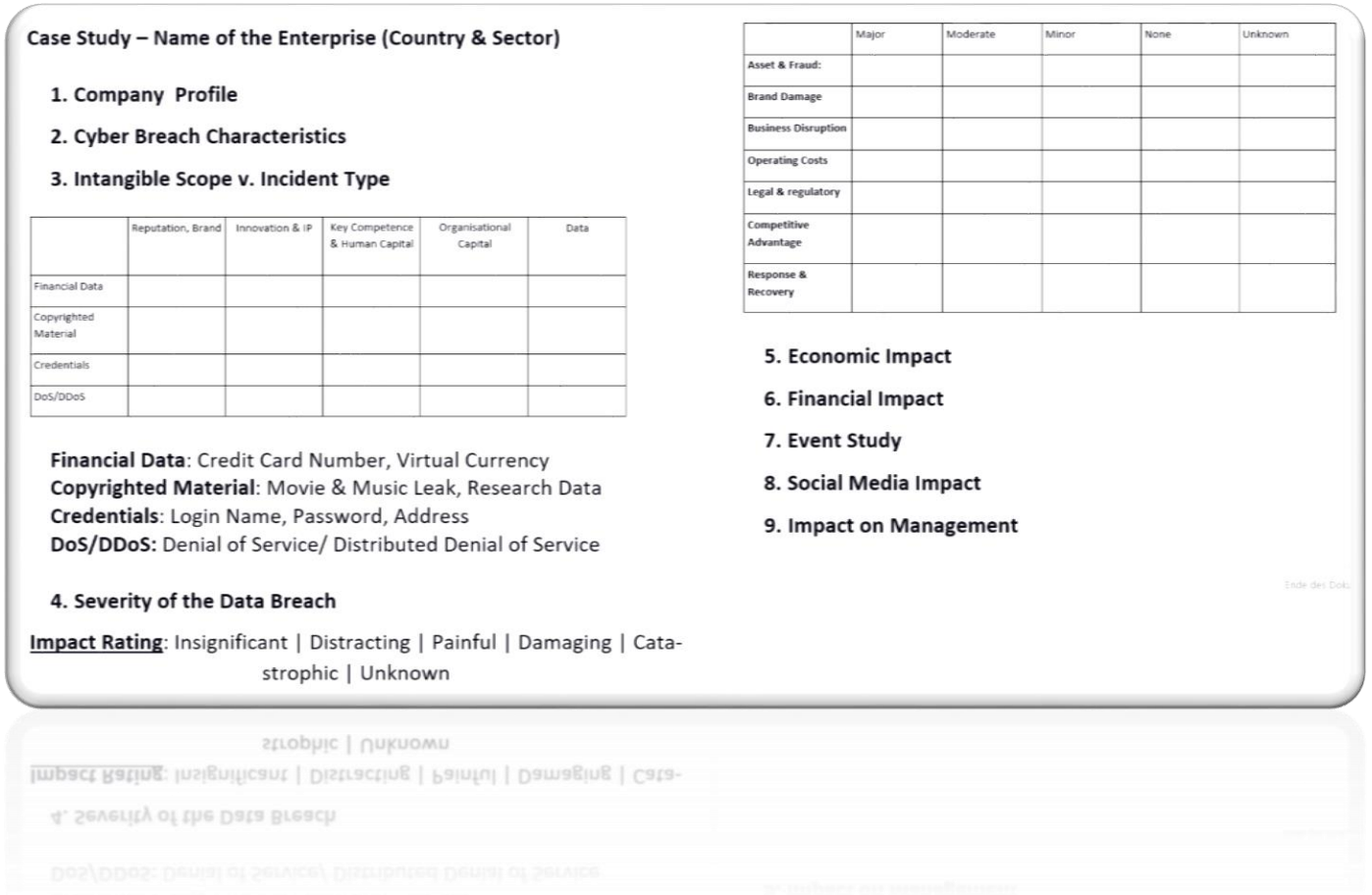
Sector-Specific Case Studies

Overview

Structure of the Case Studies

- Company Profile
- Cyber Breach Characteristics
- Intangible Scope v. Incident Type
- Severity of the Data Breach

- Economic Impact
- Financial Impact
- Event Study (UPSud)
- Social Media Impact (UPSud)
- Impact on Management



Case Study – Name of the Enterprise (Country & Sector)

1. Company Profile

2. Cyber Breach Characteristics

3. Intangible Scope v. Incident Type

	Reputation, Brand	Innovation & IP	Key Competence & Human Capital	Organisational Capital	Data
Financial Data					
Copyrighted Material					
Credentials					
DoS/DDoS					

Financial Data: Credit Card Number, Virtual Currency
Copyrighted Material: Movie & Music Leak, Research Data
Credentials: Login Name, Password, Address
DoS/DDoS: Denial of Service/ Distributed Denial of Service

4. Severity of the Data Breach

Impact Rating: Insignificant | Distracting | Painful | Damaging | Catastrophic | Unknown

	Major	Moderate	Minor	None	Unknown
Asset & Fraud:					
Brand Damage					
Business Disruption					
Operating Costs					
Legal & regulatory					
Competitive Advantage					
Response & Recovery					

5. Economic Impact

6. Financial Impact

7. Event Study

8. Social Media Impact

9. Impact on Management

Example I – IP-Intensive Industry (1)

Codan Limited (Australia)

- **Why is this case a good example?**
  - One of world's best hand held metal detection technology companies.
  - Half of the companies revenue was generated from sales of metal detectors, worth A$35.2m (2012).
- **What happened?**
  - 12 separate companies manufacturing fake Codan gold detectors of varying quality were discovered.
  - Counterfeit products have been sold in increasing numbers across north-eastern Africa > experienced a gold rush prior to 2012 – with millions of gold prospectors making a living prospecting for gold.
  - Hackers managed to hack into a Codan employee's laptop when he logged on using hotel Wi-Fi during business trip to China.
  - Codan carried out its own private investigation. The counterfeit products were more than A$10m worth.

Example I – IP-Intensive Industry (2)

Codan Limited (Australia)

- China meted out jail terms of up to two years for the principals of three first-tier manufacturing companies in the supply chain, while Dubai fined several players around A$5,000 ($3,859.50).
- Codan introduced encrypted products and employed several people on preventing hacking-led counterfeiting.
- Consequently, Codan sought a solution in the form of Fujifilm's ForgeGuard anti-counterfeiting labels.
- The company's net profit fell to A$9.2 million in the year to June 30, 2014, from A$45 million a year earlier as a result.

Example II – Financial Service (1)

Equifax Inc. (U.S.)

- **Why is this case a good example?**
  - Equifax is one of the world's three-largest consumer credit reporting bureaus and holds data of more than 820 million consumers and more than 91 million business worldwide.
  - The recent data breach affects almost every second American. The consequences for the financial market are not predictable, but can be devastating.

- **What happened?**
  - PI of 143m Americans (including some Australian & British customers) were stolen. The exposed data include names, birth dates, SSNs, addresses and some driver's license numbers.
  - Three executives sold shares worth approximately $1.8m days after the data breach has been discovered.
  - Equifax's South America operations was also affected by the data breach (Brian Krebs).
  - Equifax learned about the breach almost five months before the date it has publicly disclosed (March).

iC 14 Intellectual Capital for Communities In the Knowledge Economy

Example II – Financial Service (2)

Equifax Inc. (U.S.)

- **Consequences**
  - The data theft could cause financial grief for years for home buyers & mortgage applicants.
  - The theft of driver's licenses is especially worrisome > could help cyber thieves create a more credible fake ID.
  - Equifax customers have been offered one year's free access to Equifax's own Trusted ID service.
  - The share price collapsed as an immediate reaction to the publication. The securities lost about one-seventh of their value.
  - Standard & Poor's has revised its outlook on Equifax's BBB-plus rated bonds from stable to negative.
  - Within days, at least 100 suits had been filed.
  - The company faces scrutiny from Congress, which is to hold two hearings, and several state attorneys general, including New York's.
  - The CEO, Richard F. Smith, was forced to retire from his position.

iC 14 Intellectual Capital for Communities In the Knowledge Economy

Example III – Digital Platforms (Retail) (1)

Target Corporation (U.S.)

- **Why is this case a good example?**
  - Target Corporation is the second largest retailer in the U.S. and a component of the S&P 500 index.
  - The company reached one of the largest data breach multistate settlements in recent history.
- **What happened?**
  - Hackers managed to steal credit and debit card records from more than 40m Target customers, as well as personal information from some 60-70m people.
  - An investigation by the states found that in November 2013, scammers got access to Target's server through credentials stolen from a third-party vendor.
  - The data breach was the first in a series of scams that hit other retailers and forced the retail industry, banks and card companies to increase security and sped the adoption of microchips into U.S. credit and debit cards.
  - The company has been subject to a number of lawsuits initiated by credit card companies ($106m), customers ($10m) and state governments. ($18,5m)

Example III – Digital Platforms (Retail) (2)

Target Corporation (U.S.)

- **Consequences**
  - Fourth quarter and full-year 2013 net expense related to the data breach were $17m , reflecting $61m of gross expense partially covered by the recognition of a $44m insurance receivable.
  - In 2014, the company incurred breach-related expenses of $145m, which reflected $191m of gross expense partially covered by the recognition of a $46m insurance receivable.
  - CEO, chairman and president Gregg Steinhafel, resigned in May 2014.
  - In May 2017, a $18.5m settlement was reached, involving 47 states and the District of Columbia > this is the largest multistate data breach settlement to date.
  - The total costs for the breach had been more than $200m.
  - The agreement sets new industry standards for companies that process payment cards and maintain confidential information about their customers.

Example IV – Health Care (1)

Anthem Inc. (U.S.)

- **Why is this case a good example?**
  - With over 73m people served by its affiliated companies, including approx. 40m within its family health plans, Anthem is one of the leading health benefits companies in the US.
  - One of the largest data breach related settlements in history.

- **What happened?**
  - Approx. 80m Americans have had their personal information exposed to hackers.
  - Anthem failed to encrypt its files, indicating laxity in dealing with the security of personal information.
  - The breach affected a wide range of Anthem branches, including: Anthem Blue Cross, Anthem Blue Cross & Blue Shield, Blue Cross & Blue Shield Georgia, Empire Blue Cross and Blue Shield, UniCare, HealthLink, Amerigroup, Caremore, HealthKeepers, Golden West.

Example IV – Health Care (2)

Anthem Inc. (U.S.)

- **Consequences**
  - $230m in legal and consultant fees. Most of the costs were covered by its cyber insurance policy.
  - In 2017, Anthem agreed to pay a record $115m to settle a class action lawsuit.
  - Victims will receive protection services such as at least two years of credit monitoring and reimbursement for breach-related expenses.
  - By the end of August 2017, U.S. District Judge Lucy Koh granted preliminary approval of the $115m settlement between health insurance and the 80m affected customers.
  - Despite the fact that at least 100 class action lawsuits were filed against the company, in 2015, a survey issued by financial services firm Wedbush Securities indicated that Anthem's brand did not take a major hit after the breach. The impact was blunted by positive perceptions of the way the company handled the breach.

Lessons learnt (1)

There are two types of attacks

- **Targeted**
  - Considerable time, effort, expertise and recourses is invested in carrying out an targeted attack. This includes spying on the victim's infrastructure, as well as the collection of all available technical and operational details of the targeted object.
  - Various goals can be pursued, from stealing company data, through customer data, to blackmailing and disrupting operations.
  - The perpetrators are often concerned with not being recognized and moving around the system as freely and undetected as possible. > "dwell time" in 2017 was 146 days globally and 469 days in the EU (FireEye).
- **Distributed**
  - Try to affect a wide range of domains and users by phishing mails and other malware as well as DoS and DDoS attacks.

Lessons learnt (2)

Attack Strategies

- Approx. 97% of successful attacks involve some degree of social engineering.
- The human factor plays a significant role, either by human error, malicious intent or incompetence.
- The sharp rise in cyber-attacks on businesses illustrates that many companies are neither financially nor organizationally prepared for such scenarios.
- The most significant impacts on enterprises was a result of targeted attacks, although in most cases the attack-related costs were greater than the value of the lost asset.
- Increasing threat through digital services that are outsourced.
- Recent cyber-attacks show that collateral damage can cause also considerable damage.

Lessons learnt (3)

Attack Related Costs

- Companies with a strong reputation before crises have a higher degree of immunity and therefore suffer fewer reputational losses than companies with a lower reputation.
- Social media spread such news quickly and can have a far-reaching influence on reputation.
- Data breaches always present a reputational risk, however the extent to which enterprises suffer a reputational damage is dependent upon the severity, the origin and the duration of a breach.
- Becoming a case study contributes to the longevity of reputational damage.

Lessons learnt (4)

Factors Influencing the Impact on Reputation

- Speed of response of the affected company is crucial for the degree of the reputational damage.
- Discovering a cyber-intrusion enables enterprises to take immediate countermeasures. In addition, there is some time to remove the intruder from the system without causing even greater damage.
- A strategic battle plan will help to reduce chaos and uncoordinated attempts to manage the situation and foster a positive public image.
- Data management is important to reduce the risk of data contamination.
- A good communication strategy and public relations work generates a positive public image and conveys the image that the company is in control of the situation and deals conscientiously with the incident.
- However, that's not sufficient if technical and structural decisions are not taken in the aftermaths, which on the one hand ward off the cyber-attack, reduce the damage and secure data, and on the other hand ensure that such a cyber-attack is not repeated.

iC 14
Intellectual Capital
for Communities
In the Knowledge
Economy

Thanks!
Questions and Comments!?

Alexander Szanto