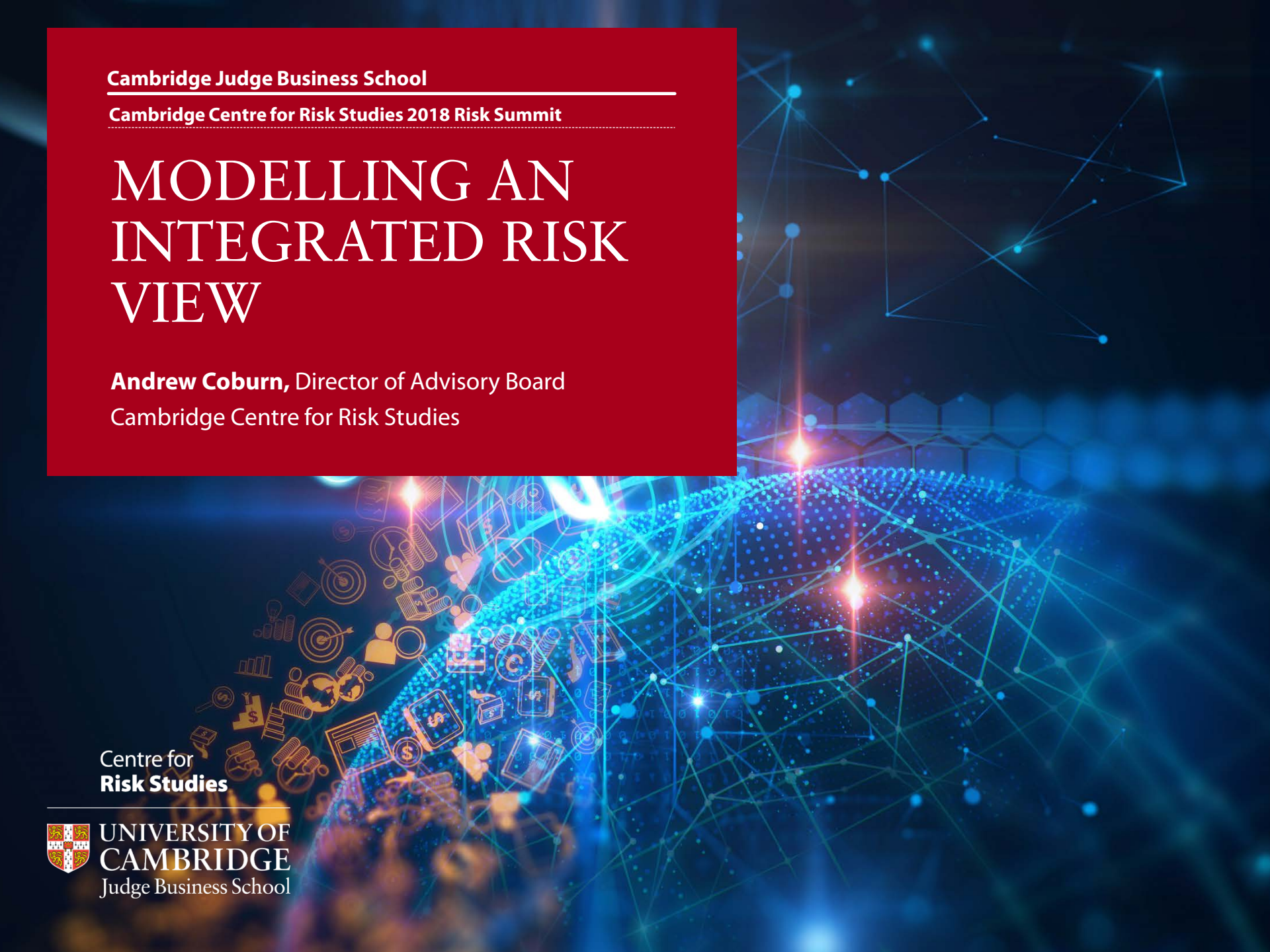
Cambridge Judge Business School

Cambridge Centre for Risk Studies 2018 Risk Summit

MODELLING AN INTEGRATED RISK VIEW

Andrew Coburn, Director of Advisory Board
Cambridge Centre for Risk Studies



Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Themes in Today's Risk Summit

- Integrated Risk Assessment
  - Tools for managing risk from multiple threats
- Risk and the Digital Economy
  - Understanding cyber threat
- Corporate Risk Profiling and Enterprise Risk Management
  - What threat risk means to an individual organization
- Trend Risk and Business Decisions
  - Forward business planning in a changing world

- **Equifax** is a consumer credit reporting agency
  - Equifax collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide
- 2017 Revenues: **$3.4 Bn**
- 9,000 employees, operating in 14 countries

- Headquarters: Atlanta Georgia, US
- Operating Income: $824 m
- Assets: $7.2 Bn
- Equity: $3.2 Bn

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

The Catastrophe

- A cyber attack on Equifax over the summer of 2017 exfiltrated **146 million** protected data records:
  - 130m individuals in US
  - 15m individuals in UK
  - 19,000 Canadians
- It was made public on 6 September
  - (A month after the data breach was discovered)

For the Technically Minded…

- The hackers got in using a flaw in Apache Struts 2
  - an open-source toolkit for developing Java EE web applications
- During an error message, a hacker can execute their own commands
  - This is a well known vulnerability, logged as CVE-2017-5638 in Common Vulnerabilities & Exposures, with a CVSS score of 10 (worst)
- A patch for the vulnerability was released March 7
  - Equifax had not installed this patch when attack occurred 2 months later
- Plus a poorly segmented network design, inadequate encryption of protected data, and ineffective breach detection mechanisms.

Apache » Struts : Security Vulnerabilities

Total number of vulnerabilities : **72**

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
10	CVE-2017-5638	20		Exec Code	2017-03-10	2018-03-03	**10.0**	None	Remote	Low	Not required	Complete	Complete	Complete

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

Direct Costs to Equifax

- Direct Costs of $439 million
  - Incident response costs
  - Notification costs
- Company's insurance had a limit of $125 million, and a deductible of $10.5m
- Equifax left to find $326 million from its own resources
- 40% of its operating income for a year

Share Price Drop

- Equifax shares dropped 37 percent, and recovered to a 24 percent loss
- Immediate ‘retirement’ of:
  - CEO and Chairman Richard Smith
  - Chief Information Officer David Webb
  - Chief Security Officer, Susan Mauldin

Other Financial Threats Resulting from the Attack

- Regulatory fines from the State Attorneys General are likely to reach very large sums – potentially up to **$3.2 Billion**
- Debt-to-Equity ratio impacted:
  - "substantial litigation and potential finds" coupled with an unknown cost to repair the damage will likely mean debt leverage will remain **"above 2x over the next two years."**
- Standard and Poor's revised its outlook on the company from stable to negative
  - Credit rating changes make it more costly to finance a company's debt
- Multiple lawsuits filed against Equifax as a result of the breach
- California law firm Geragos & Geragos filed for **$70 billion** in damages
  - The largest class-action suit in US history
  - The application for damages is 21 times the valuation of the company

What Effect Do Cyber Losses Have on Other Businesses?

- A third of companies that have a data breach report revenue loss
  - 12% report losses greater than 20% of their annual revenue
  - just over 1% lost more than 80% of their annual revenue
- Companies also report significant losses in business opportunities and customer desertion as a result of the breach
  - Typical churn rates of around 7% of a company's customers
  - 31% of consumers have discontinued a relationship with an organization that has suffered a data breach
- Large cyber attacks typically result in stock prices marked down.
  - Analysis suggests share prices are reduced by an average of 5% after a data breach attack.
- A few companies have declared bankruptcy following cyber attacks.
  - Nayana, an Internet Service Provider in South Korea, declared bankruptcy after being hit by Erebus ransomware that froze its operations in June 2017.
- Companies that have had their intellectual property stolen have found themselves out-competed in the market, leading to their long-term failure.
  - Nortel, a Canadian telco company filed for bankruptcy in January 2009. Analysts cite cyber theft of their IP among reasons for them being outcompeted in the market by Chinese competitors. Reference GW.

Impacts of Cyber Threat on Company Valuations

- What is the risk premium for cyber on company valuations?
- How can we quantify probability of cyber loss?
- Which companies are most at risk?
- How can a company protect itself?

Chances of a Data Breach

Data Breach Severity Scale	Range (min to max number of personal data records)	Number of regulatory reported events by US organizations (2012-2017)	Odds of a large US company suffering in a year (1-in-…)
P3	1,000 to 10,000	2,022	34
P4	10,000 to 100,000	918	81
P5	100,000 to 1 million	324	206
P6	1 million to 10 million	162	472
P7	10 million to 100 million	50	1,449
P8	100 million to 1 billion	19	4,762
P9	More than 1 billion	2	50,000

Scenarios and Likelihoods of a $50 Million Cyber Loss

Loss Process	Magnitude	Vulnerability	Potential Cause	Odds per yr
Contagious Malware	Over 1% infection of key servers	Network traffic scanning	Ransomware	1-in-200
Data Exfiltration	Over 10M PII records	Network intrusion	Malicious External	1-in-250
Data Exfiltration	Over 1M PCI records	Payment process malware	Malicious External	1-in-500
Contagious Malware	Over 10% infection of general devices	Firewall and AV failure	Diskwiper	1-in-600
Counterparty Failure	Serious Bug in MM Platform software	Third party plug-ins	QA in supplier	1-in-750
Financial Theft	Multiple multi-million bank transfers	Bank transfer authentication	Insider or External	1-in-800
Data Exfiltration	Over 100K PHI records	Access control failure	Insider	1-in-900
Contagious Malware	Infection of Media Management Platform	Network traffic scanning	Targeted payload	1-in-1,000
Denial of Service	Ultra high intensity DDoS on Server, 7 days continuous	Web Application Firewall	Hacktivist external	1-in-4,000
Denial of Service	Very high intensity DDoS on Server, 20 days intermittent	Web Application Firewall	Hacktivist external	1-in-4,800
Counterparty Failure	4+ day cloud outage: Object storage; US	Cloud platform continuity	Human error	1-in-5,000

Not Just Cyber Threat

Threats to Business Output
(Supply shock)

A. Site-specific threats to key facilities & assets

B. Risks that affect the whole company
Idiosyncratic – i.e. unlikely to affect other businesses at the same time

C. Systemic risks for sectors or all businesses
Will this business be affected more than average for sector?

Threats to a Company's Market
(Demand shock)

D. Threats to demand in a national market

E. Threats to demand in regional or global markets

F. Trend risks that affect the company business model

Translating Risks to Global Economy to Risks to Corporates

Creating a business use case for corporates

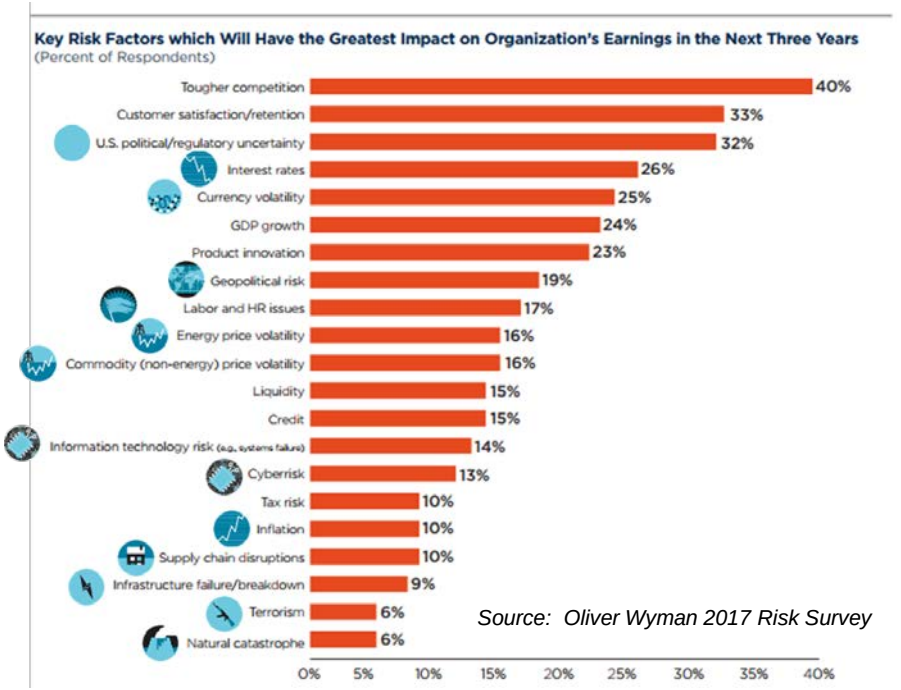
Corporates face a risk modelling gap

Lacking consistent and comprehensive approach across the enterprise that consider:

- External threats and emerging risk
- Geography
- Methods and Metrics

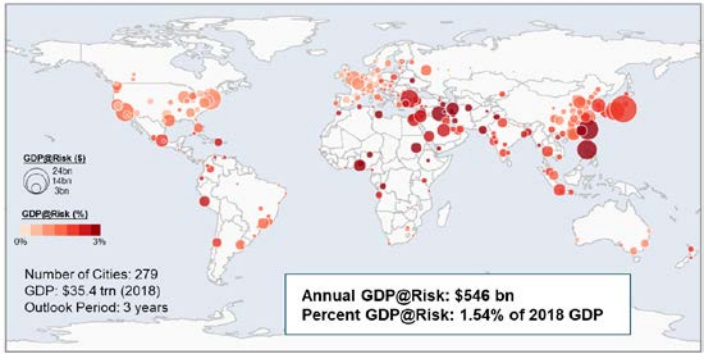
Increasing focus on risk modelling for:

- Stress Testing
- Reporting



Source: Oliver Wyman 2017 Risk Survey

Map of Risks to Global Economy



Map of Corporate Exposures

Themes in Today's Risk Summit

- Cambridge Centre for Risk Studies is making progress towards Integrated Risk Assessment
- CCRS is providing world-leading research into Risk and the Digital Economy
- Developing frameworks for Corporate Risk Profiling and Enterprise Risk Management
- And working with industry partners to understand how to make Business Decisions faced with Risky Futures

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Credit Rating on Watch

- Debt-to-Equity ratio impacted:
  - "substantial litigation and potential finds" coupled with an unknown cost to repair the damage will likely mean debt leverage will remain **"above 2x over the next two years."**
- "BBB+" rating on Equifax's corporate debt
- Standard and Poor's revised its outlook on the company from stable to negative
- Moody's Investors Service said that the criminal hack will hurt the company's earnings growth for the next three to four quarters, as well as its reputation.
- Credit rating changes make it more costly to finance a company's debt

Regulatory Fines

- Fines from the State Attorneys General are likely to reach very large sums
- In April, a state judge ruled that Massachusetts Attorney General can move forward with a potentially gigantic data breach case against Equifax
  - Asking for $25 per violation
  - This could potentially cost Equifax **$3.2 Billion** US-wide
- Equifax defense argument that the AGs need to demonstrate and quantify 'harm' was overruled
  - This is a landmark finding, moving on from previous data breach regulatory fines
- If the latest proposed senate law were enacted – the Data Breach Prevention and Compensation Act (Elizabeth Warren and Mark Warner Jan 2018) – it would result in Equifax being fined an additional **$1.5 Billion** by the Federal Trade Commission.

Private Law Suits

- Multiple lawsuits filed against Equifax as a result of the breach
- California law firm Geragos & Geragos filed for **$70 billion** in damages
  - The largest class-action suit in US history
  - The application for damages is 21 times the valuation of the company