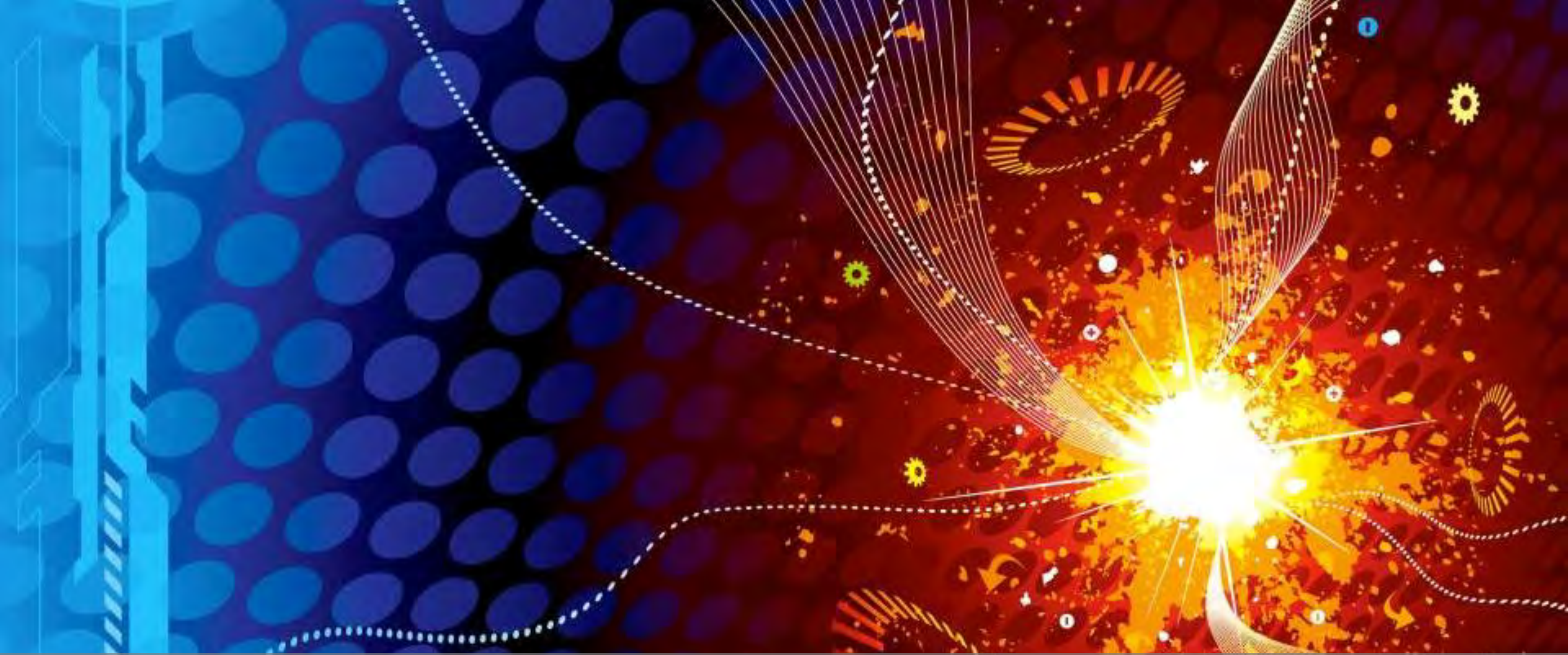


Cambridge Centre for Risk Studies

London Risk Briefings

Cyber Catastrophe

Defining a Risk Test Scenario for managing the business risks posed by cyber threats

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

@Risk_Cambridge
#cybercat

University of Cambridge Centre for Risk Studies

Research Application Partners

RMS™ LOCKHEED MARTIN E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL HSBC bp LLOYD'S

Deloitte. CATLIN Munich RE McKinsey&Company THE LIGHTHILL RISK NETWORK

Collaborators

Cytora COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK OXFORD ECONOMICS Axco A Wilmington Company FNA NANYANG TECHNOLOGICAL UNIVERSITY

Catastrophe Modelling in Complex Systems

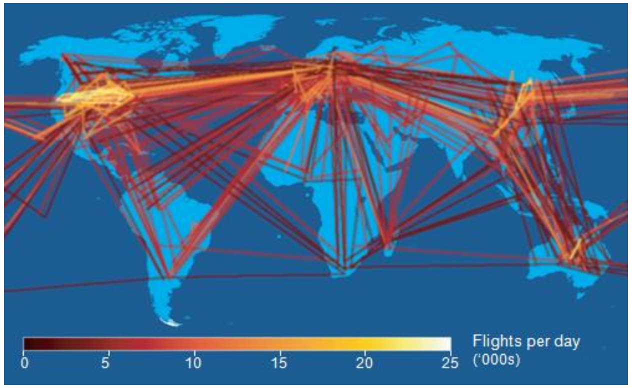
- The Centre for Risk Studies arises from shared interests by the participants in exploring areas of intersection between
  - Catastrophe modelling and extreme risk analytics
  - Complex systems and networks failures
- Advance the scientific understanding of how systems can be made more resilient to the threat of catastrophic failures

To answer questions such as:

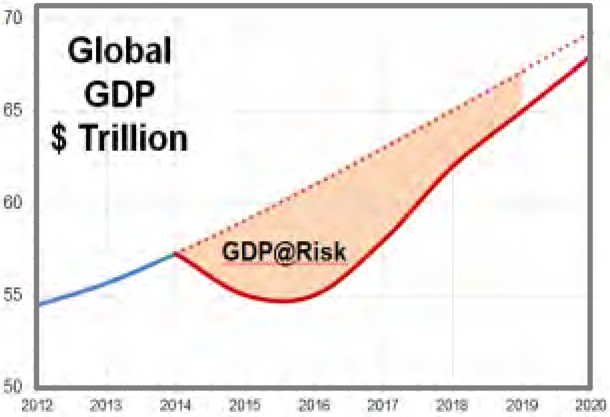
'What would be the impact of
a [War in China] on [Trade Networks] and how would this impact the [Global Economy]?

Regional Conflict

Air Travel Network



Global Economy



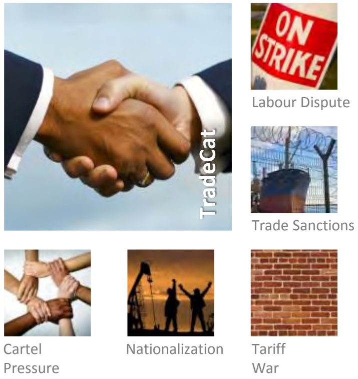
UNIVERSITY OF CAMBRIDGE
Judge Business School
Centre for Risk Studies

Cambridge Taxonomy of Threats

Financial Shock

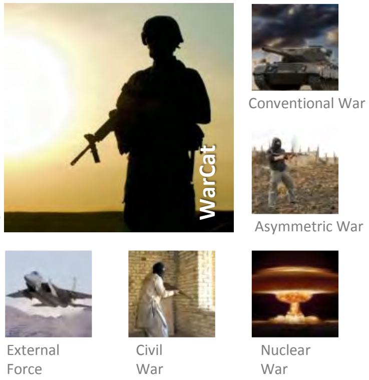
Asset Bubble, Financial Irregularity, Market Crash, Sovereign Default, Bank Run

Trade Dispute



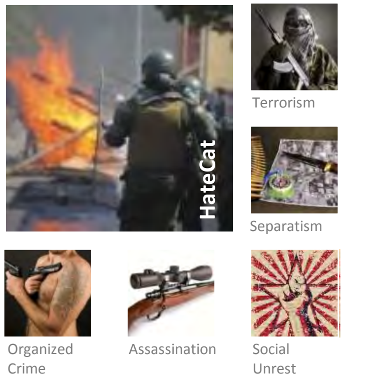
Labour Dispute, Trade Sanctions, Cartel Pressure, Nationalization, Tariff War

Geopolitical Conflict



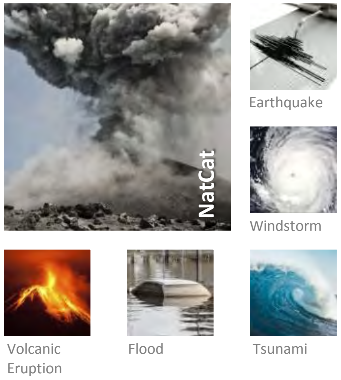
Conventional War, Asymmetric War, External Force, Civil War, Nuclear War

Political Violence



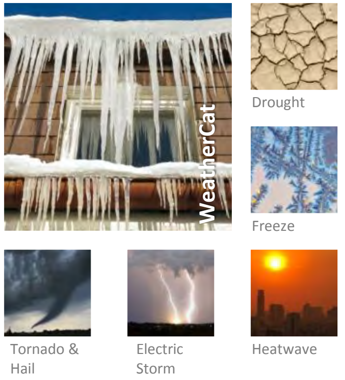
Terrorism, Separatism, Organized Crime, Assassination, Social Unrest

Natural Catastrophe



Earthquake, Windstorm, Volcanic Eruption, Flood, Tsunami

Climatic Catastrophe



Drought, Freeze, Tornado & Hail, Electric Storm, Heatwave

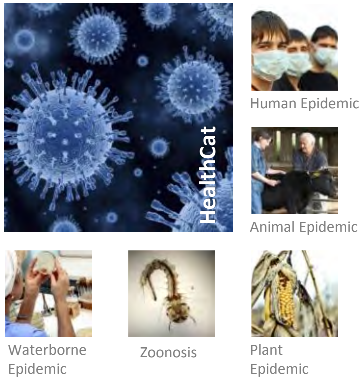
Environmental Catastrophe

Sea Level Rise, Ocean System Change, Wildfire, Pollution Event, Atmospheric System Change

Technological Catastrophe

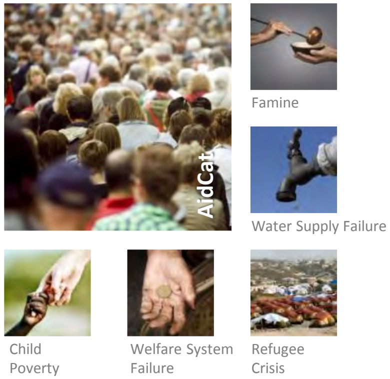
Nuclear Meltdown, Industrial Accident, Cyber Catastrophe, Technological Accident, Infrastructure Failure

Disease Outbreak



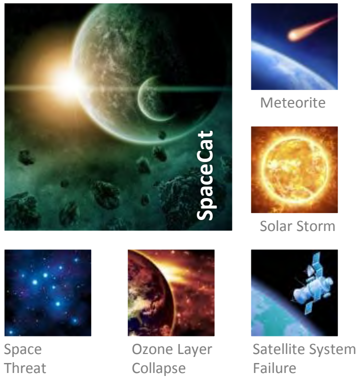
Human Epidemic, Animal Epidemic, Waterborne Epidemic, Zoonosis, Plant Epidemic

Humanitarian Crisis



Famine, Water Supply Failure, Child Poverty, Welfare System Failure, Refugee Crisis

Externality

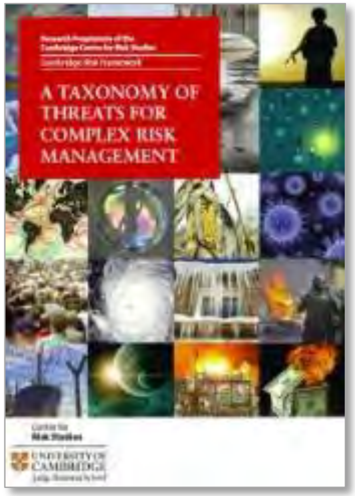


Meteorite, Solar Storm, Space Threat, Ozone Layer Collapse, Satellite System Failure

Other

UNIVERSITY OF CAMBRIDGE
Judge Business School | Centre for Risk Studies

Published Reports on Stress Test Scenarios



A TAXONOMY OF THREATS FOR COMPLEX RISK MANAGEMENT

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE Judge Business School

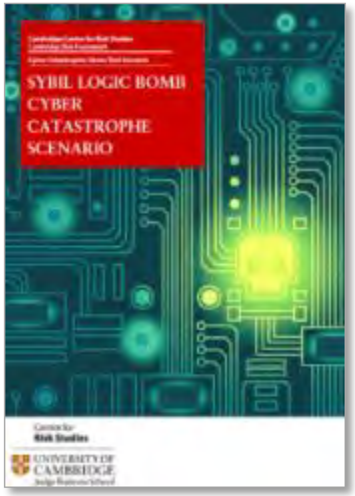
Taxonomy of Threats

MILLENNIAL UPRISING SOCIAL UNREST SCENARIO

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE Judge Business School

Social Unrest
Stress Test Scenario



SYBIL LOGIC BOMB CYBER CATASTROPHE SCENARIO

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE Judge Business School

Cyber Catastrophe
Stress Test Scenario

SÃO PAULO VIRUS PANDEMIC SCENARIO

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE Judge Business School

Pandemic
Stress Test Scenario

CHINA-JAPAN CONFLICT SCENARIO

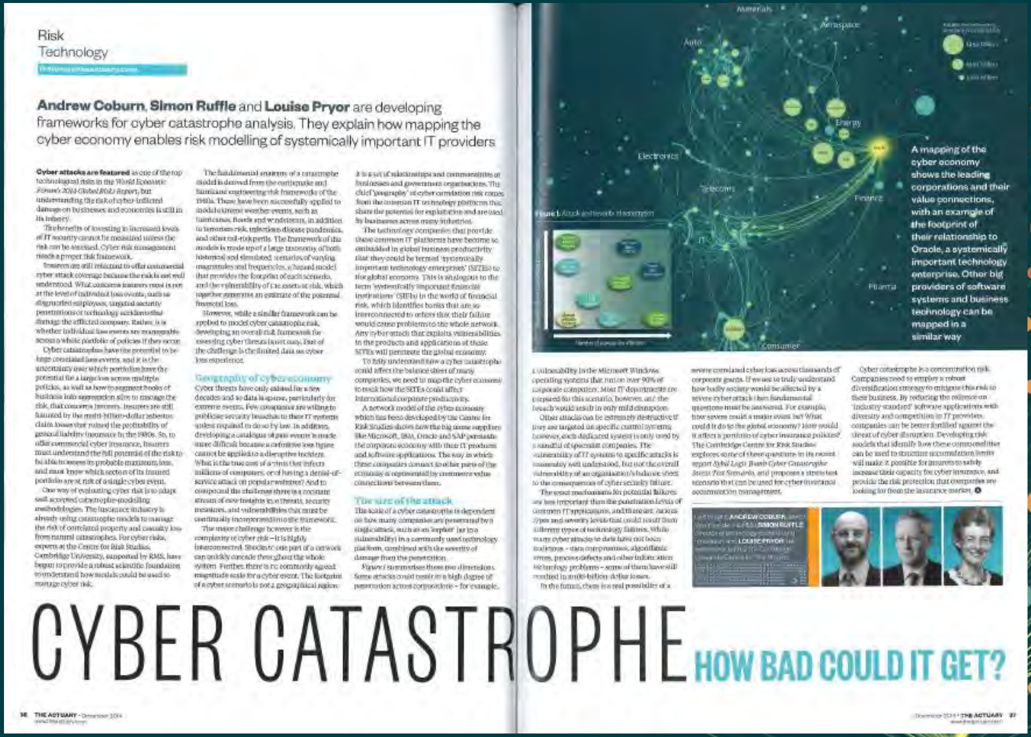
Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE Judge Business School

Geopolitical Conflict
Stress Test Scenario

Available for Download from Website:
CambridgeRiskFramework.com

Our Cyber Research in the Media



Andrew Coburn, Simon Ruffle and **Louise Pryor** are developing frameworks for cyber catastrophe analysis. They explain how mapping the cyber economy enables risk modelling of systemically important IT providers

Cyber attacks are featured as one of the top technological risks in the *World Economic Forum's 2014 Global Risks Report*, but understanding the risk of cyber-inflicted damage on businesses and economies is still in its infancy.

The benefits of investing in increased levels of IT security cannot be measured unless the risk can be assessed. Cyber risk management needs a proper risk framework.

Insurers are still reluctant to offer commercial cyber attack coverage because the risk is not well understood. What concerns insurers most is not at the level of individual loss events, such as disgruntled employees, targeted security penetrations or technology accidents that damage the afflicted company. Rather, it is whether individual loss events are manageable across a whole portfolio of policies if they occur.

Cyber catastrophes have the potential to be large correlated loss events, and it is the uncertainty over which portfolios have the potential for a large loss across multiple policies, as well as how to segment books of business into aggregation silos to manage the risk, that concerns insurers. Insurers are still haunted by the multi-billion-dollar asbestos claim losses that ruined the profitability of general liability insurance in the 1980s. So, to offer commercial cyber insurance, insurers must understand the full potential of the risk to be able to assess its probable maximum loss, and must know which sectors of its insured portfolio are at risk of a single cyber event.

One way of evaluating cyber risk is to adapt well accepted catastrophe-modelling methodologies. The insurance industry is already using catastrophe models to manage the risk of correlated property and casualty loss from natural catastrophes. For cyber risks, experts at the Centre for Risk Studies, Cambridge University, supported by RMS, have begun to provide a robust scientific foundation to understand how models could be used to manage cyber risk.

The fundamental anatomy of a catastrophe model is derived from the earthquake and hurricane engineering risk frameworks of the 1980s. These have been successfully applied to model extreme weather events, such as hurricanes, floods and windstorms, in addition to terrorism risk, infectious disease pandemics, and other tail-risk perils. The framework of the models is made up of a large taxonomy of both historical and simulated scenarios of varying magnitudes and frequencies, a hazard model that provides the footprint of each scenario, and the vulnerability of the assets at risk, which together generate an estimate of the potential financial loss.

However, while a similar framework can be applied to model cyber catastrophe risk, developing an overall risk framework for assessing cyber threats is not easy. Part of the challenge is the limited data on cyber loss experience.

Geography of cyber economy

Cyber threats have only existed for a few decades and so data is sparse, particularly for extreme events. Few companies are willing to publicise security breaches to their IT systems unless required to do so by law. In addition, developing a catalogue of past events is made more difficult because a definitive loss figure cannot be applied to a disruptive incident. What is the true cost of a virus that infects millions of computers, or of having a denial-of-service attack on popular websites? And to compound the challenge there is a constant stream of new insights into threats, security measures, and vulnerabilities that must be continually incorporated into the framework.

The major challenge however is the complexity of cyber risk – it is highly interconnected. Shocks to one part of a network can quickly cascade throughout the whole system. Further, there is no commonly agreed magnitude scale for a cyber event. The footprint of a cyber scenario is not a geographical region: it is a set of relationships and commonalities of businesses and government organisations. The chief 'geography' of cyber correlation risk comes from the common IT technology platforms that share the potential for exploitation and are used by businesses across many industries.

The technology companies that provide these common IT platforms have become so embedded in global business productivity that they could be termed 'systemically important technology enterprises' (SITEs) to the global economy. This is analogous to the term 'systemically important financial institutions' (SIFIs) in the world of financial risk, which identifies banks that are so interconnected to others that their failure would cause problems to the whole network. Any cyber attack that exploits vulnerabilities in the products and applications of these SITEs will permeate the global economy.

To fully understand how a cyber catastrophe could affect the balance sheet of many companies, we need to map the cyber economy to track how the SITEs could affect international corporate productivity.

A network model of the cyber economy which has been developed by the Centre for Risk Studies shows how the big name suppliers like Microsoft, IBM, Oracle and SAP permeate the corporate economy with their IT products and software applications. The way in which these companies connect to other parts of the economy is represented by commerce value connections between them.

The size of the attack

The scale of a cyber catastrophe is dependent on how many companies are penetrated by a single attack, such as an 'exploit' (as in a vulnerability) in a commonly used technology platform, combined with the severity of damage from the penetration.

Figure 1 summarises these two dimensions. Some attacks could result in a high degree of penetration across corporations – for example, a vulnerability in the Microsoft Windows operating systems that run on over 90% of corporate computers. Most IT departments are prepared for this scenario, however, and the breach would result in only mild disruption.

Other attacks can be extremely destructive if they are targeted on specific control systems; however, each dedicated system is only used by a handful of specialist companies. The vulnerability of IT systems to specific attacks is reasonably well understood, but not the overall vulnerability of an organisation's balance sheet to the consequences of cyber security failure.

The exact mechanisms for potential failures are less important than the penetration levels of common IT applications, and there are various types and severity levels that could result from different types of technology failures. While many cyber attacks to date have not been malicious – data compromises, algorithmic errors, process defects and other information technology problems – some of them have still resulted in multi-billion dollar losses.

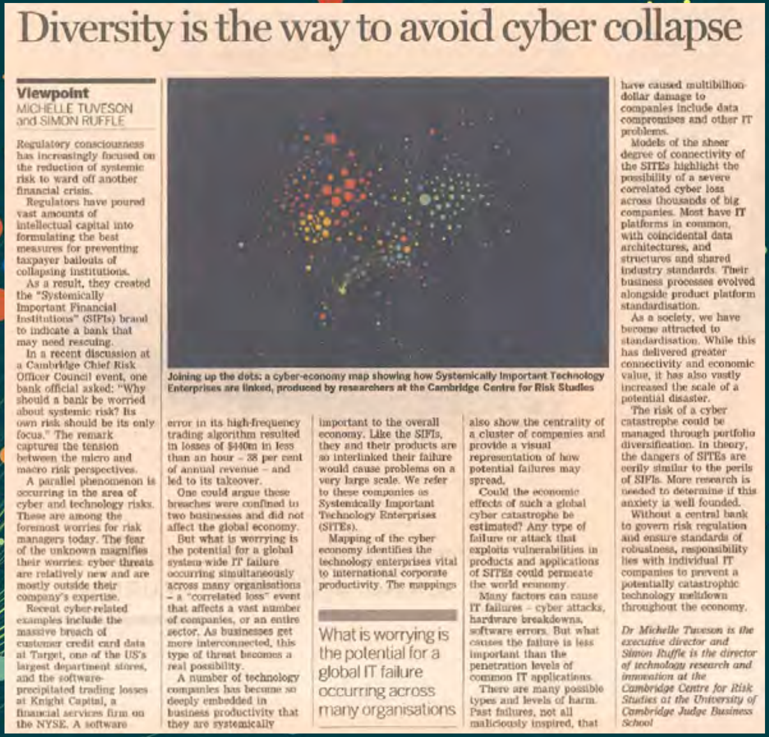
In the future, there is a real possibility of a severe correlated cyber loss across thousands of corporate giants. If we are to truly understand how badly society would be affected by a severe cyber attack then fundamental questions must be answered. For example, how severe could a major event be? What could it do to the global economy? How would it affect a portfolio of cyber insurance policies? The Cambridge Centre for Risk Studies explores some of these questions in its recent report *Sybil Logic Bomb Cyber Catastrophe Stress Test Scenario*, and proposes a stress test scenario that can be used for cyber insurance accumulation management.

Cyber catastrophe is a concentration risk. Companies need to employ a robust diversification strategy to mitigate this risk to their business. By reducing the reliance on 'industry standard' software applications with diversity and competition in IT providers, companies can be better fortified against the threat of cyber disruption. Developing risk models that identify how these commonalities can be used to structure accumulation limits will make it possible for insurers to safely increase their capacity for cyber insurance, and provide the risk protection that companies are looking for from the insurance market.

A mapping of the cyber economy shows the leading corporations and their value connections, with an example of the footprint of their relationship to Oracle, a systemically important technology enterprise. Other big providers of software systems and business technology can be mapped in a similar way

Left to right: **ANDREW COBURN**, [illegible] **SIMON RUFFLE**, director of technology research and innovation; and **LOUISE PRYOR** [illegible]

CYBER CATASTROPHE HOW BAD COULD IT GET?



Diversity is the way to avoid cyber collapse

Viewpoint
MICHELLE TUVESON and SIMON RUFFLE

Regulatory consciousness has increasingly focused on the reduction of systemic risk to ward off another financial crisis.

Regulators have poured vast amounts of intellectual capital into formulating the best measures for preventing taxpayer bailouts of collapsing institutions.

As a result, they created the "Systemically Important Financial Institutions" (SIFIs) brand to indicate a bank that may need rescuing.

In a recent discussion at a Cambridge Chief Risk Officer Council event, one bank official asked: "Why should a bank be worried about systemic risk? Its own risk should be its only focus." The remark captures the tension between the micro and macro risk perspectives.

A parallel phenomenon is occurring in the area of cyber and technology risks. These are among the foremost worries for risk managers today. The fear of the unknown magnifies their worries: cyber threats are relatively new and are mostly outside their company's expertise.

Recent cyber-related examples include the massive breach of customer credit card data at Target, one of the US's largest department stores, and the software-precipitated trading losses at Knight Capital, a financial services firm on the NYSE. A software error in its high-frequency trading algorithm resulted in losses of $440m in less than an hour – 38 per cent of annual revenue – and led to its takeover.

One could argue these breaches were confined to two businesses and did not affect the global economy.

But what is worrying is the potential for a global system-wide IT failure occurring simultaneously across many organisations – a "correlated loss" event that affects a vast number of companies, or an entire sector. As businesses get more interconnected, this type of threat becomes a real possibility.

A number of technology companies has become so deeply embedded in business productivity that they are systemically important to the overall economy. Like the SIFIs, they and their products are so interlinked their failure would cause problems on a very large scale. We refer to these companies as Systemically Important Technology Enterprises (SITEs).

Mapping of the cyber economy identifies the technology enterprises vital to international corporate productivity. The mappings also show the centrality of a cluster of companies and provide a visual representation of how potential failures may spread.

What is worrying is the potential for a global IT failure occurring across many organisations

Could the economic effects of such a global cyber catastrophe be estimated? Any type of failure or attack that exploits vulnerabilities in products and applications of SITEs could permeate the world economy.

Many factors can cause IT failures – cyber attacks, hardware breakdowns, software errors. But what causes the failure is less important than the penetration levels of common IT applications.

There are many possible types and levels of harm. Past failures, not all maliciously inspired, that have caused multibillion-dollar damage to companies include data compromises and other IT problems.

Models of the sheer degree of connectivity of the SITEs highlight the possibility of a severe correlated cyber loss across thousands of big companies. Most have IT platforms in common, with coincidental data architectures, and structures and shared industry standards. Their business processes evolved alongside product platform standardisation.

As a society, we have become attracted to standardisation. While this has delivered greater connectivity and economic value, it has also vastly increased the scale of a potential disaster.

The risk of a cyber catastrophe could be managed through portfolio diversification. In theory, the dangers of SITEs are eerily similar to the perils of SIFIs. More research is needed to determine if this anxiety is well founded.

Without a central bank to govern risk regulation and ensure standards of robustness, responsibility lies with individual IT companies to prevent a potentially catastrophic technology meltdown throughout the economy.

Dr Michelle Tuveson is the executive director and Simon Ruffle is the director of technology research and innovation at the Cambridge Centre for Risk Studies at the University of Cambridge Judge Business School

Joining up the dots: a cyber-economy map showing how Systemically Important Technology Enterprises are linked, produced by researchers at the Cambridge Centre for Risk Studies

Cyber Catastrophe Risk

Updating Our Thinking About Cyber Risk

Centre for
Risk Studies

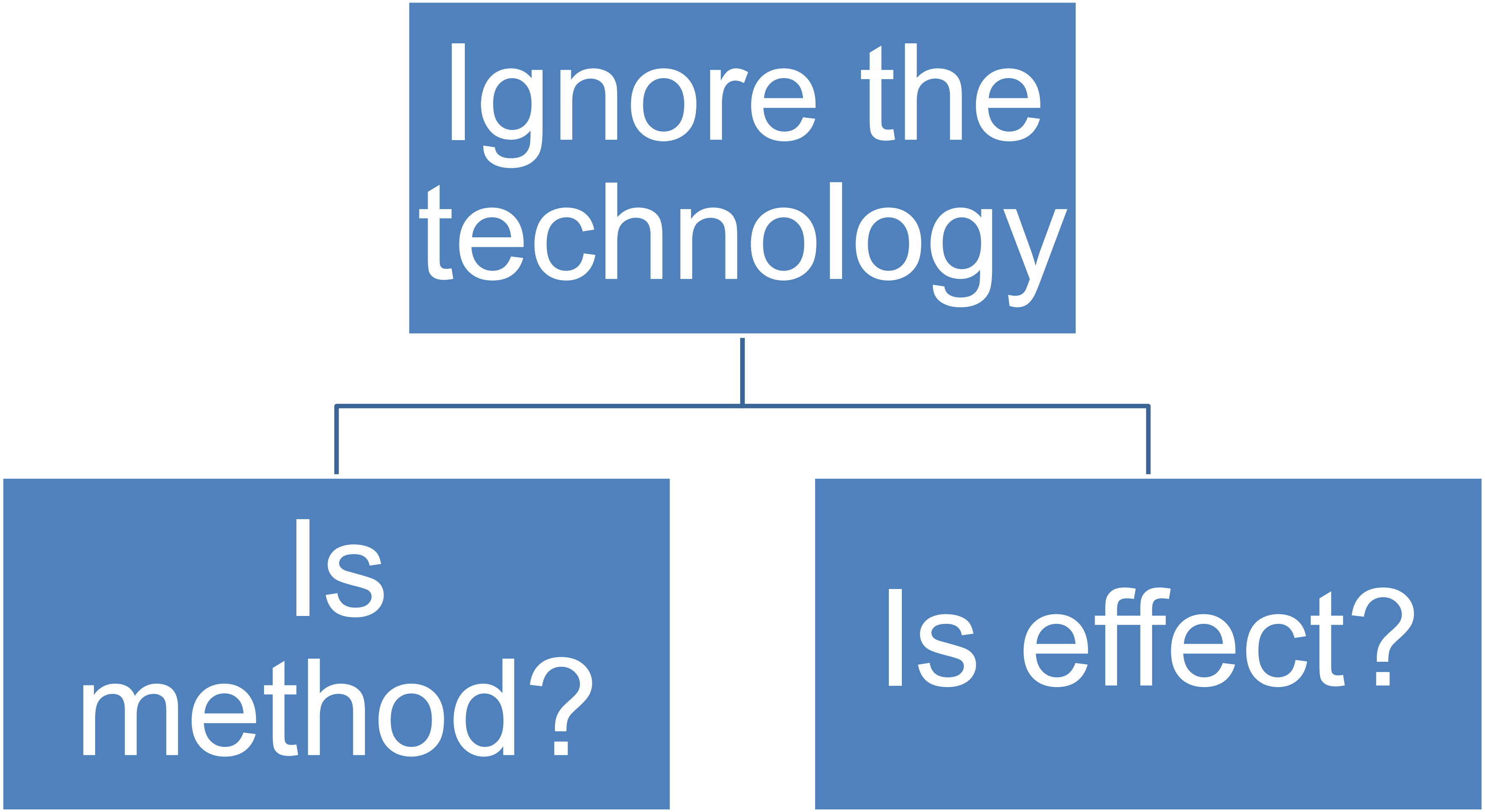
UNIVERSITY OF
CAMBRIDGE
Judge Business School

Éireann Leverett
Senior Risk Researcher
@blackswanburst

News of the Week

- Sony PlayStation
- Sony Pictures
  - Sub effects: gender pay gap debate
  - Personal privacy invaded
    - Will you pay out twice for these?
- Ransomware
  - Tennessee Sheriff’s Dept PAID $500
  - Autopsy reports, witness statements, crime photos
  - Infection rates increasing 700%

You Need a Framework

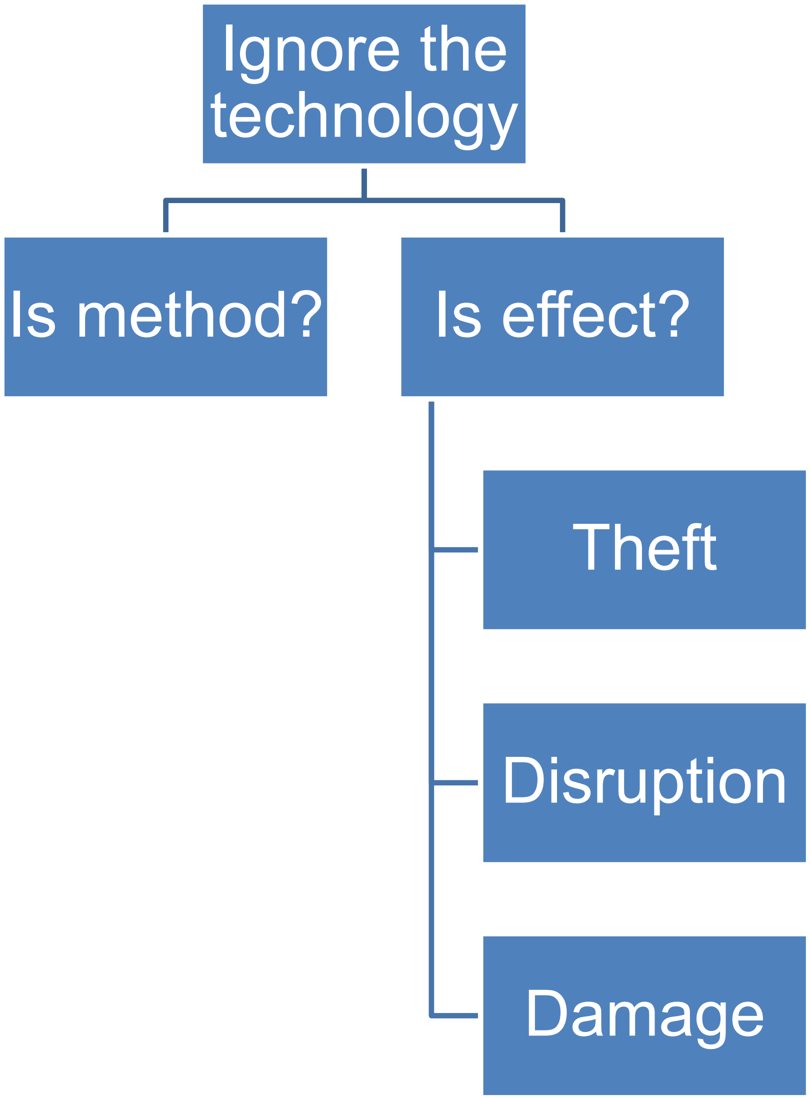


Ignore the technology

Is method?

Is effect?

You Need a Framework



Ignore the technology

Is method?

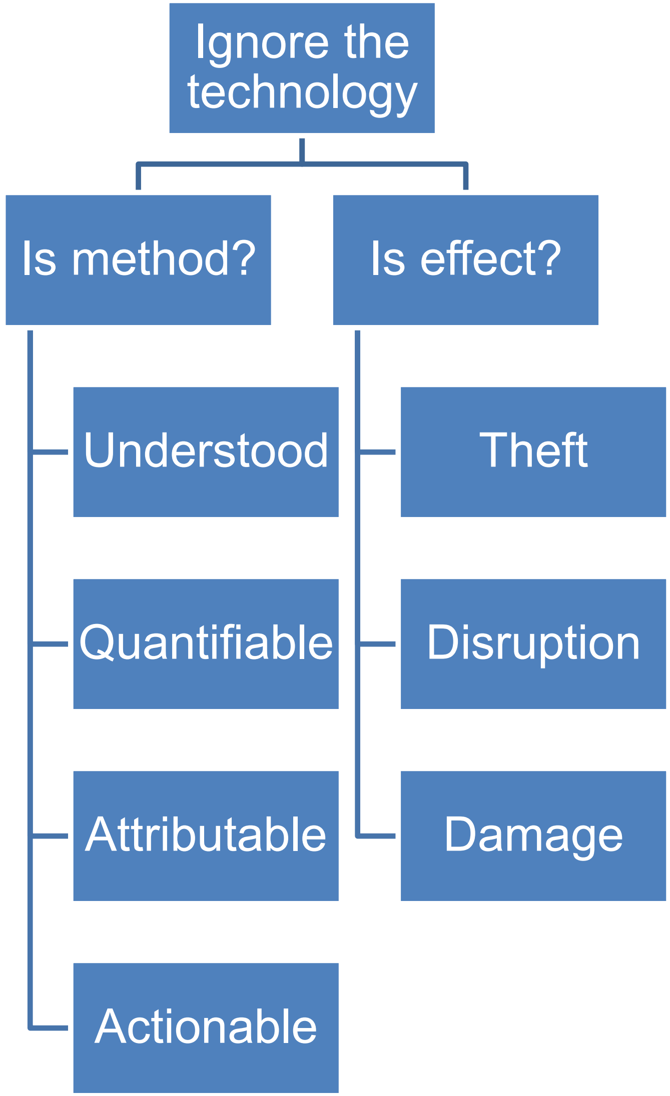
Is effect?

Theft

Disruption

Damage

You Need a Framework


Ignore the technology

Is method?

Is effect?

Understood

Quantifiable

Attributable

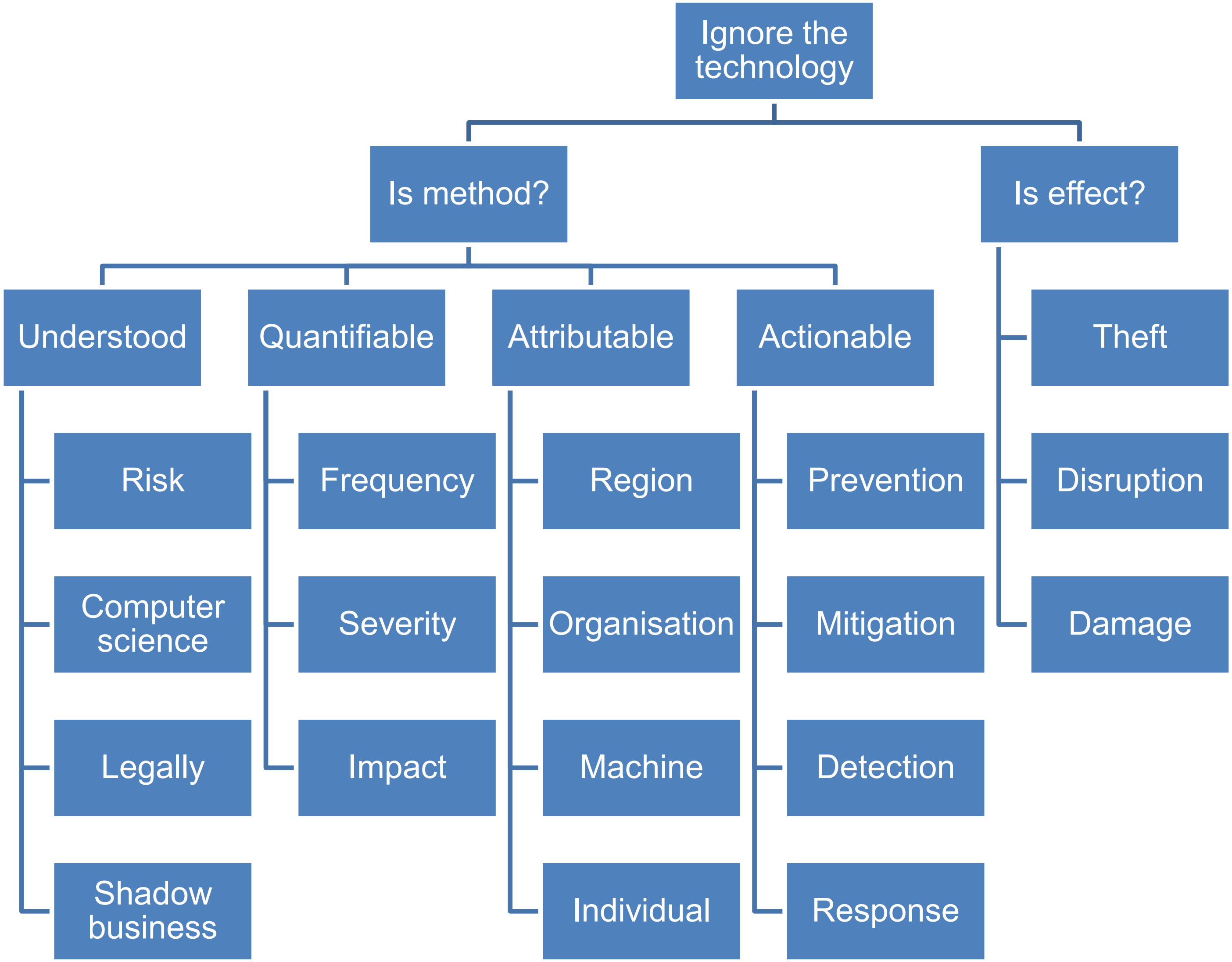
Actionable

Theft

Disruption

Damage

You Need a Framework


Ignore the technology

Is method?

Understood
- Risk
- Computer science
- Legally
- Shadow business

Quantifiable
- Frequency
- Severity
- Impact

Attributable
- Region
- Organisation
- Machine
- Individual

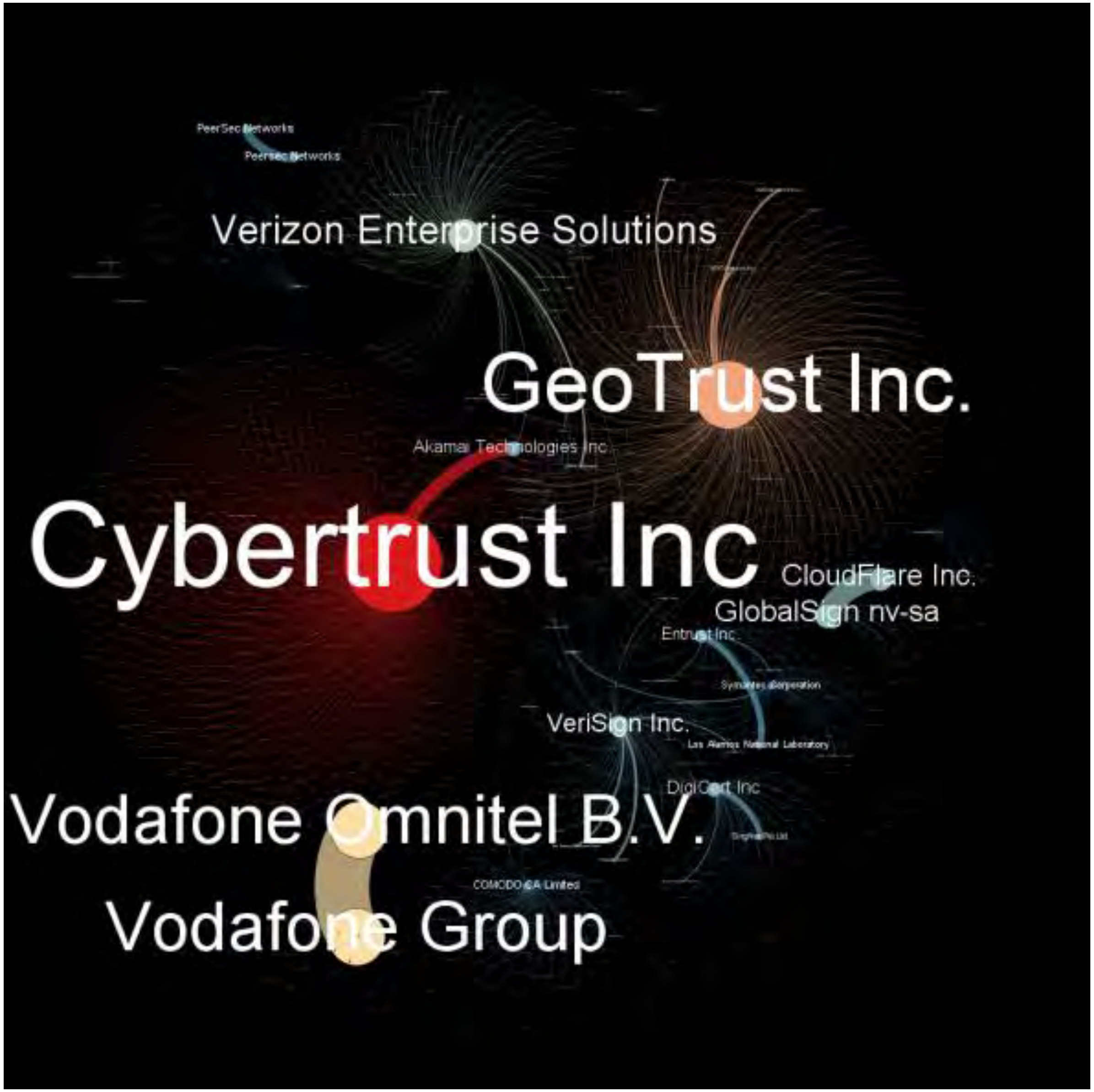
Actionable
- Prevention
- Mitigation
- Detection
- Response

Is effect?
- Theft
- Disruption
- Damage

10 Cold Truths of Cyber

- Man Made Peril
  - Don’t mistake whitehat research for blackhat research
  - Your clients are dealing with intelligent adversaries
  - So frequency and severity will change rapidly
- Complexity
  - There are no technological “silver bullets”
  - ALL your security infrastructure is a commons
  - Anti-business is a blackmarket
  - Information asymmetry
  - Paxson’s law
- Logic Adjustment
  - Damage isn’t virtual
  - Anything can be hacked, insecure until proven

Trust on the Web



# of Subjects	# of Issuers
3	Four
16	Three
104	Two
1797	One
222	Zero

Cyber Catastrophe Risk

Insurability of Cyber Risk

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Dr Andrew Coburn
Director of Advisory Board, Centre for Risk Studies
& Senior Vice President, RMS

Cyber Risk as an Insurable Peril

- Insurers see demand from corporate clients for cyber insurance cover
  - Today they provide specific and constrained covers for particular cyber insurance applications
  - They are wary about large scale exposure to cyber risk
- Insurers may already have significant cyber risk exposure
  - Commercial General Liability and other coverages can be ‘silent’ on cyber losses
  - Strong preference for insurers to move customers to ‘affirmative’ cyber coverage products
- For insurers to allocate a significant amount of capital to insuring cyber risk requires
  - A comprehensive framework for understanding and quantifying the risk
  - An assessment of the potential for severe catastrophe loss across a portfolio of insureds (‘Probable Maximum Loss’)
  - Accumulation control structures that will limit the potential for correlated large losses

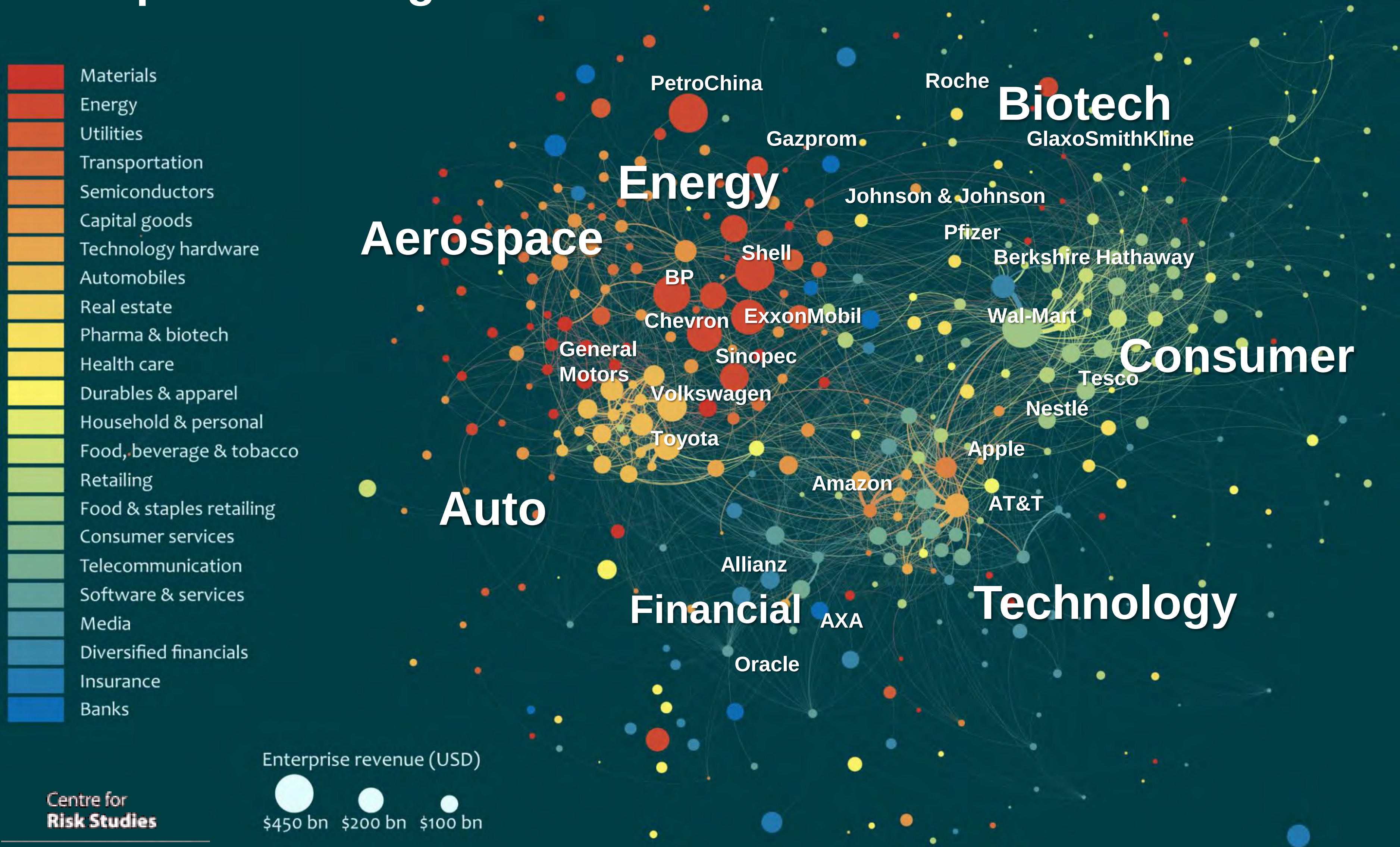
Understanding the Cyber Economy

- To understand loss potential, we first need to understand how Information Technology creates economic output
  - A Model of the Cyber Economy
- We need to understand mechanisms of harm and loss processes in the cyber economy
  - A comprehensive framework for loss assessment
- We need to understand the correlation between companies that would give rise to a cyber catastrophe
  - A mapping of the systemic risk of cyber vulnerabilities

A framework for cyber risk modelling

The Cyber Economy

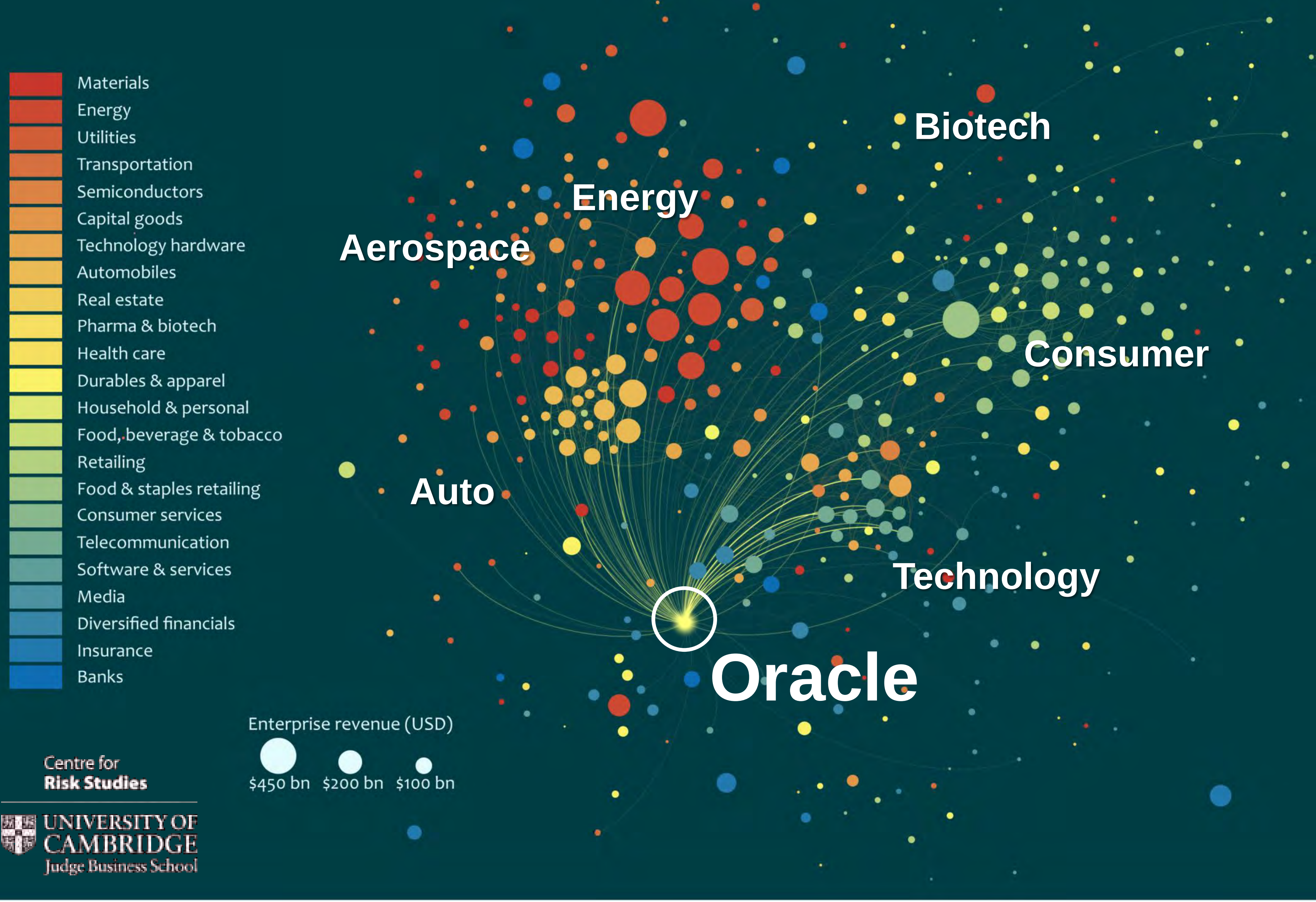
Enterprise Trading Network



Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

SITEs and the Cyber Economy



Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

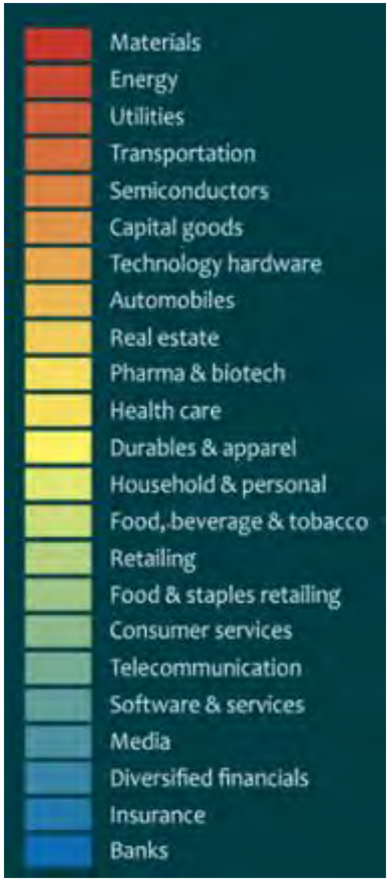
Systemically Important Technology Enterprises

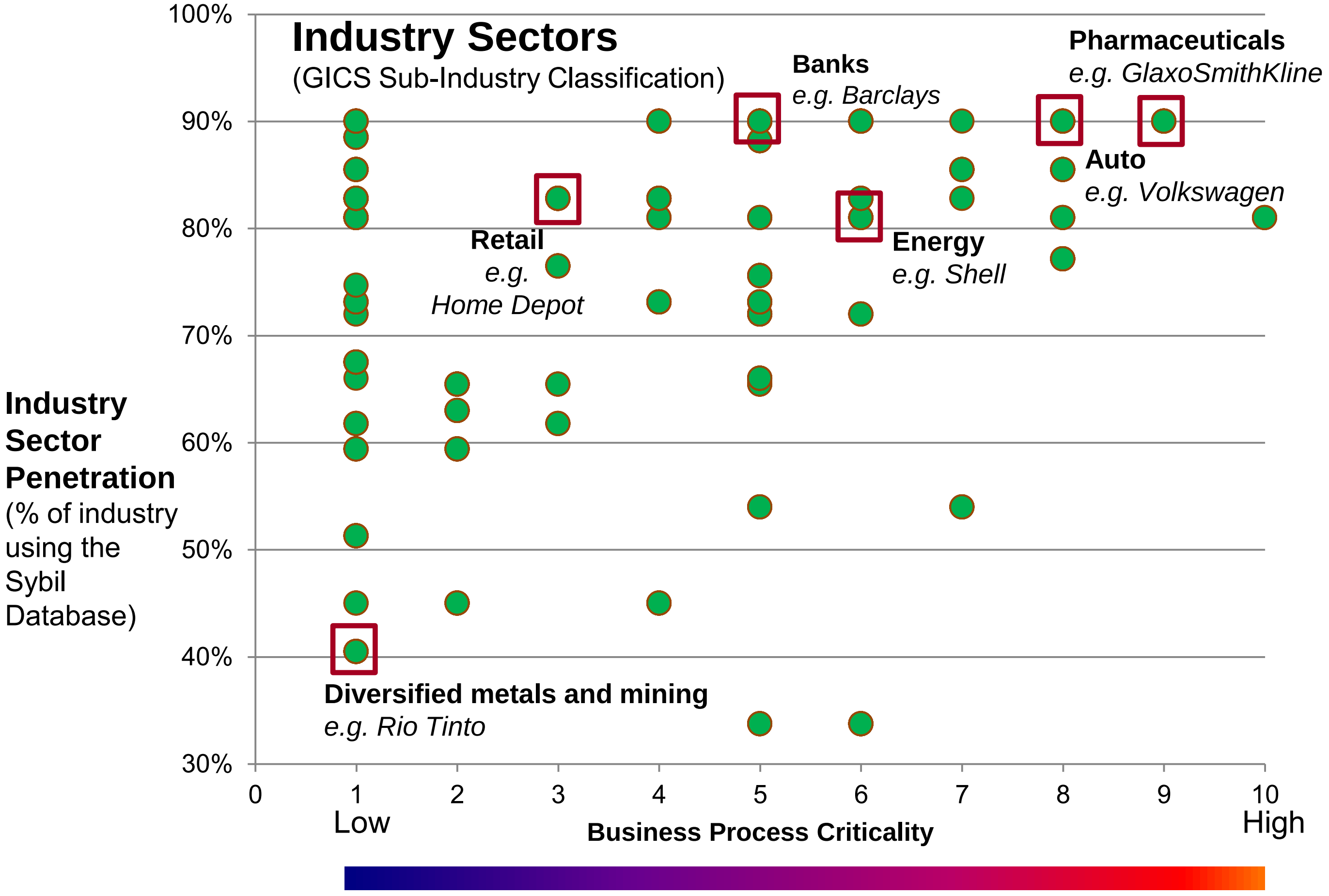
- Some software systems of individual technology companies underpin a large proportion of the cyber economy
  - These represent vulnerabilities to cyber threat
- We term these ‘Systemically Important Technology Exploits’ (SITEs)
- These are analogous to Systemically Important Financial Institutions (SIFIs) currently being identified and regulated by financial supervisory authorities

Systemic Cyber - Scenario Candidates

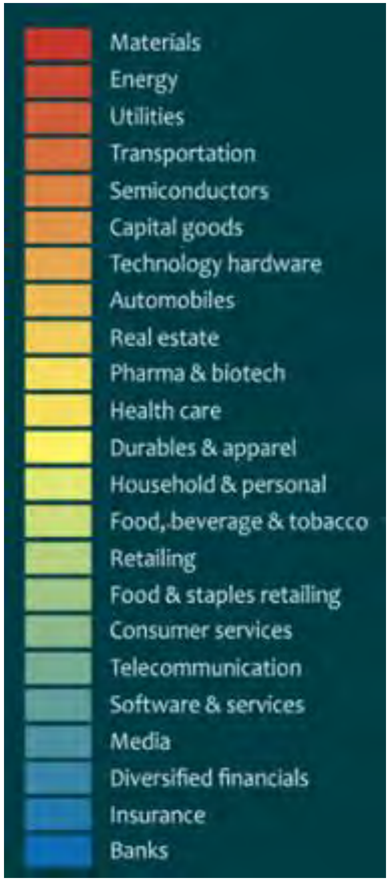
- **Algorithm Corruption** – 'Sybil Logic Bomb' corruption of Industry Standard Relational Database for algorithmic parameters.
- **Power Outage** – Attack on Supervisory Control and Data Acquisition (SCADA) Systems to disrupt electrical power distribution networks in US and Europe
- **Leakomania** – Systematic release of confidential customer records from many corporate enterprises
- **Cloud Compromise** – Failures of SAAS applications through attacks on cloud hosting service providers
- **Financial Transaction Interference** – major theft or disruption of financial transaction system through a common exploit across multiple enterprises that carry out financial transactions
- '**Internet of Things**' – fires and physical damage triggered to appliances and machines that are remotely operated
- **Hackspionage** – systematic and widespread theft of intellectual property and commercial secrets by coordinated teams of agents
- **Extortion Spree** – large number of companies held to ransom by hackers disabling IT functionality to obtain payoffs
- **Mass D-DOS** – Denial of service attacks across thousands of companies, using bot-nets; reflectors, and amplifiers
- **Kinetic attacks on key classes of insurance**
  - **Satellite Hacks** - Satellite or GPS disruption through hacker attack
  - **Aviation** –attacks on aircraft through remote interference with control systems
  - **Property** – Building and contents loss through remotely activated sprinkler systems
  - **Marine** – loss of hull and cargo through attacks on navigation and operating systems

Sectoral Differentiation of Scenarios





A Sectoral Approach to Accumulation Control



- Segmentation of insured corporates by their prevalence or dependency on the SITE
  - For example using metrics such as ‘Revenue@Risk’
- Identify harm processes and loss mechanisms that trigger insurance claims
  - Guided by insurance coverages
- Estimation of severity of losses and limitations and constraints on loss development
  - Components of loss, metrics, benchmarks and precedents
- Estimation of loss ratios or loss severity relativities
  - Including multiple lines of insurance
- Mapping of segmentation of insured corporates by their severity of loss from scenario
  - Identification of scenario loss ‘footprint’ by e.g. NAICS sectors or company characteristics
- Loss ratio matrix across exposure segmentation for use in accumulation controls
  - The loss ratio matrices from the scenarios will be a deliverable to development partners

Exposure Data Model for Cyber Insurance

- Collaborative initiative with RMS and other industry partners
- We are exploring the development of a data schema for the capture and monitoring of cyber insurance exposure
- To be a published and open data standard
- EDM will capture coverages, policy structures, company details, accumulation characteristics, of cyber exposure
- Schema aims to capture most of the cyber coverages currently being offered and managed in the market
- Conducting a survey of products and coverages in the market
- Please let us know if you would be willing to participate
- Key objective is to identify major needs and practical usefulness of EDM

Cyber Catastrophe Risk

Sybil Logic Bomb Cyber Catastrophe Scenario

Risk Test Scenario for managing business risks posed by cyber threats

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Simon Ruffle
Director of Technology Research and Innovation
Centre for Risk Studies

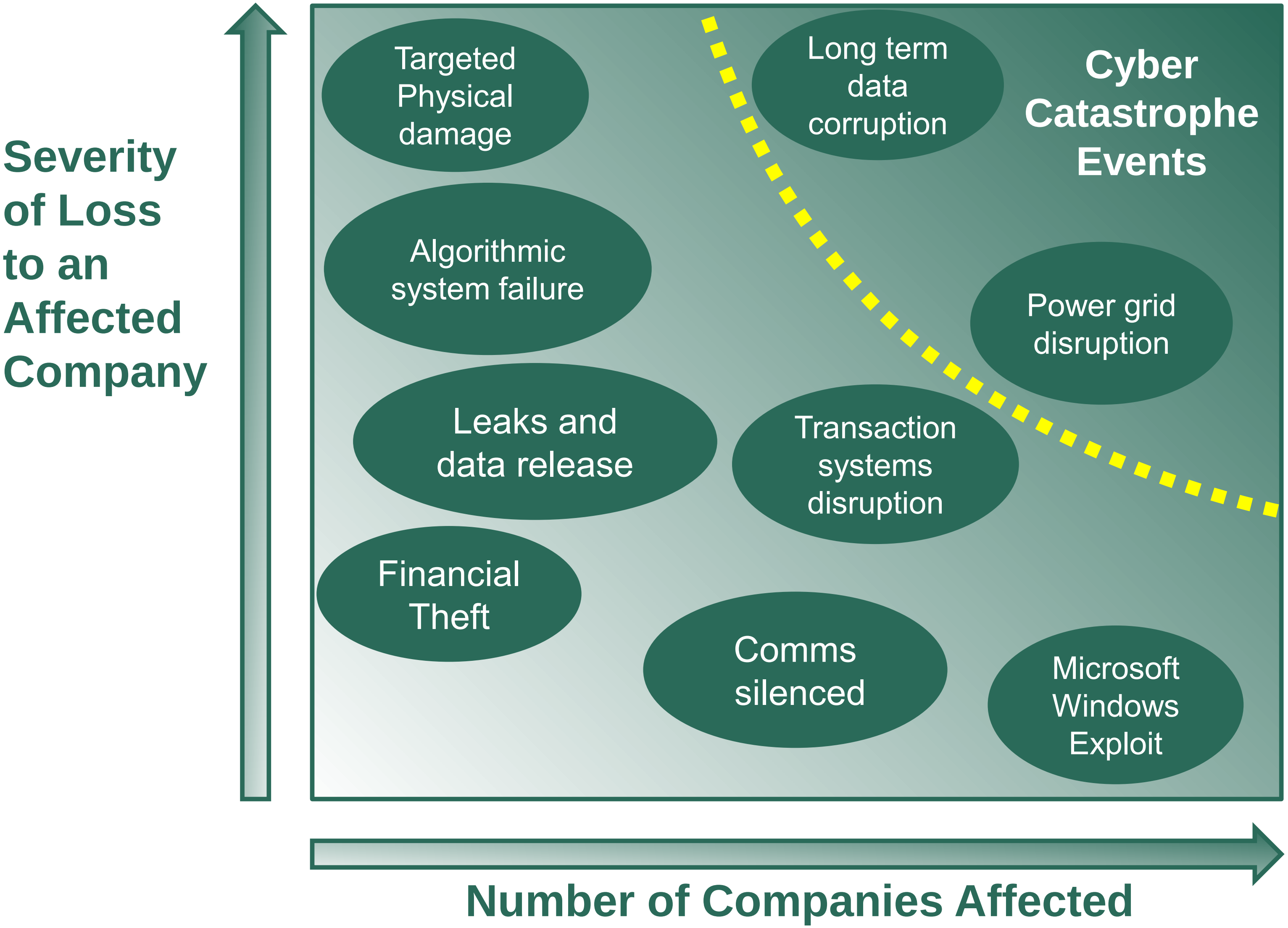
The Harm Caused by a Cyber Catastrophe

three types of ***harm***

Theft	Disruption	Damage
Mass theft of credentials*	Power grid disruption*	Long term data corruption*
Data Espionage	Microsoft Windows exploit	Leaks, abuse of data and defamation
Financial fraud	Transaction systems disruption	Data centres, internal IT and cloud servers damaged
Cash theft	Communications silenced	Targeted physical damage
	GPS Failure	Algorithmic systems failures
	Tactical data espionage	
	Degrading of internet and denial of service	

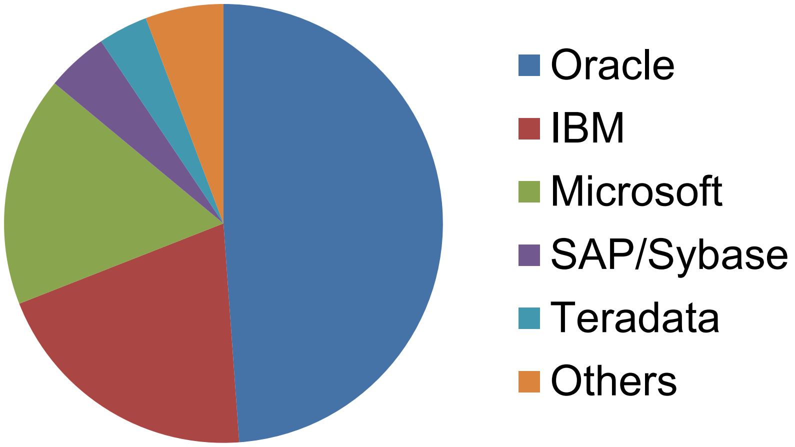
* = ranked worst case scenarios by subject matter expert team at Cyber Threat Workshop 17th July 2013

Choosing a Scenario


Severity of Loss to an Affected Company
Targeted Physical damage
Long term data corruption
Cyber Catastrophe Events
Algorithmic system failure
Power grid disruption
Leaks and data release
Transaction systems disruption
Financial Theft
Comms silenced
Microsoft Windows Exploit
Number of Companies Affected

The Sybil Logic Bomb Stress Test Scenario

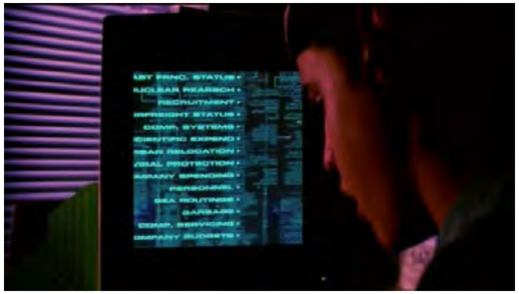
- Unobtrusive corruption of an industry-standard relational database in common use by many major corporations
- Real-world examples of relational databases include



- Sybil is a Systemically Important Technology Enterprise (SITE)

Key Features of Sybil Logic Bomb Scenario

- Insider attack
- Slow burn: over months, years
- Small errors difficult to spot
- Small errors can cause big problems
- Backups corrupted
- Difficult to replicate
- Affects algorithms not transactions



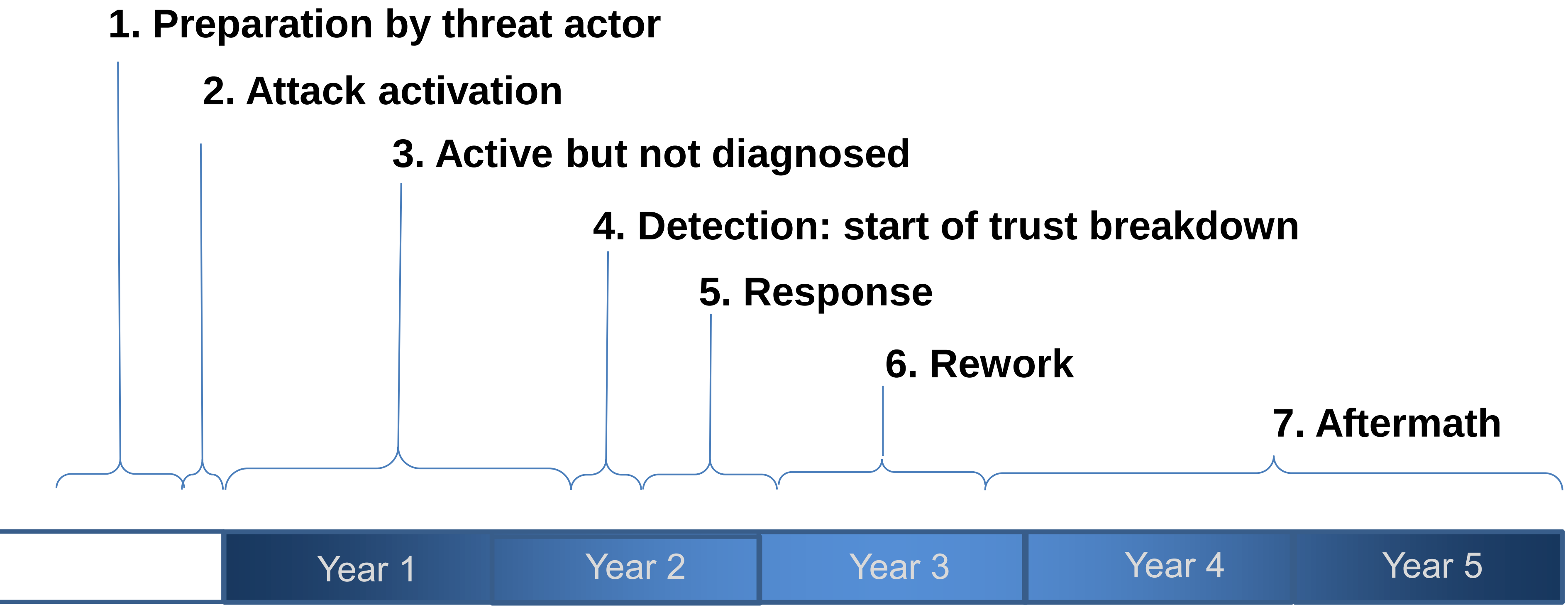
~~Transaction processing~~

- ~~Payroll~~
- ~~Airline ticketing~~
- ~~Retail bank accounts~~
- ~~Credit card payments~~

Algorithmic processing

- Forecasting
- Modelling
- Trading
- Design
- Analysis
- Process Control

Sybil Logic Bomb Scenario Phases


1. Preparation by threat actor

2. Attack activation

3. Active but not diagnosed

4. Detection: start of trust breakdown

5. Response

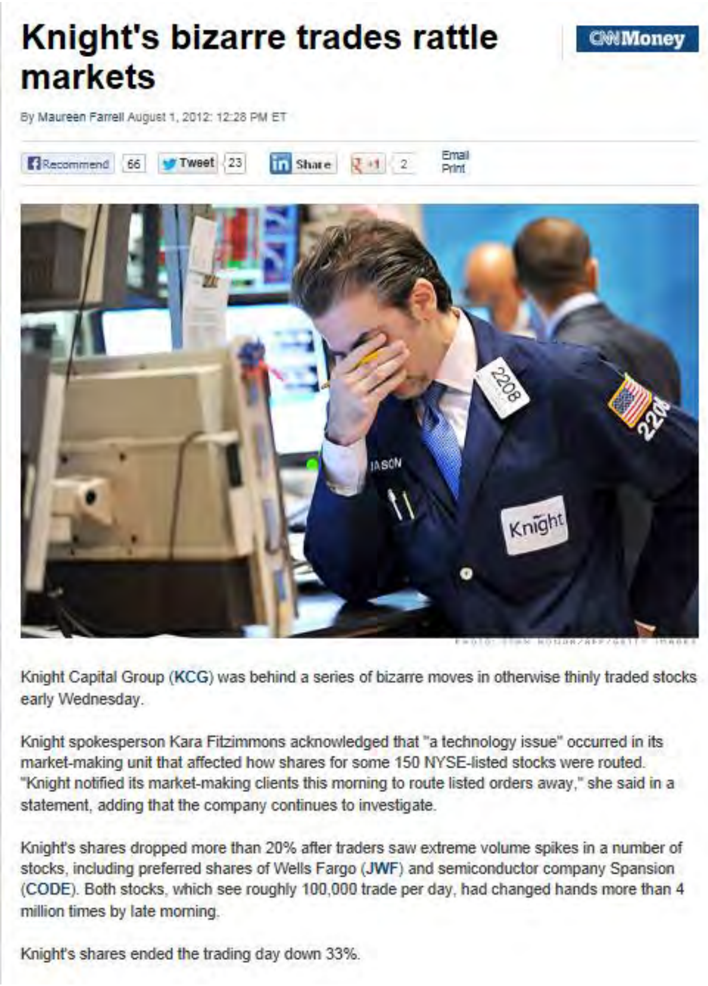
6. Rework

7. Aftermath

Fictional Algorithmic IT Failures Caused by Logic Bomb

GICS Industry group	Type of failure	Real life precedents
Automobiles & Components	**Robotic manufacturing failure causes loss of production**	"Ping Sweep": Robotic arm out of control
Banks	**Bad data leads to write-down**	National Australia Bank, 2001:HomeSide write-downs, $2.2Bn loss
Insurance	**Corruption of scanned paper based customer records**	Xerox WorkCentre Document Scanning Flaw
Diversified financials	**Algorithmic trading losses**	Flash Crash, Knight Capital $450m loss, AXA Rosenberg $250m loss
Semiconductors	**Losses to high value items in production**	Semiconductor fabrication production line failure: $50,000 damage
Pharmaceuticals & Biotechnology	**Financial forecasts and reports wrong**	AstraZenica spread sheet error sends wrong data to sell side analyst community, 2012.
Media	**Event overbooking, loss of consumer confidence**	Locog spread sheet error causes Olympic ticket overselling, 2011
Energy	**Unable to send gas through pipeline**	Penetration test locks up SCADA system of gas utility for 4 hours.
Utilities	**Contractual errors lead to losses**	Transalta: $25m charge due to wrong transmission hedging contracts
Utilities	**Environmental Damage lead to liability claims and fines.**	Maroochy Shire Incident, 2000: 800,000L raw sewage spill in 47 separate incidents

Precedent: Knight Capital



Knight's bizarre trades rattle markets

By Maureen Farrell August 1, 2012: 12:28 PM ET

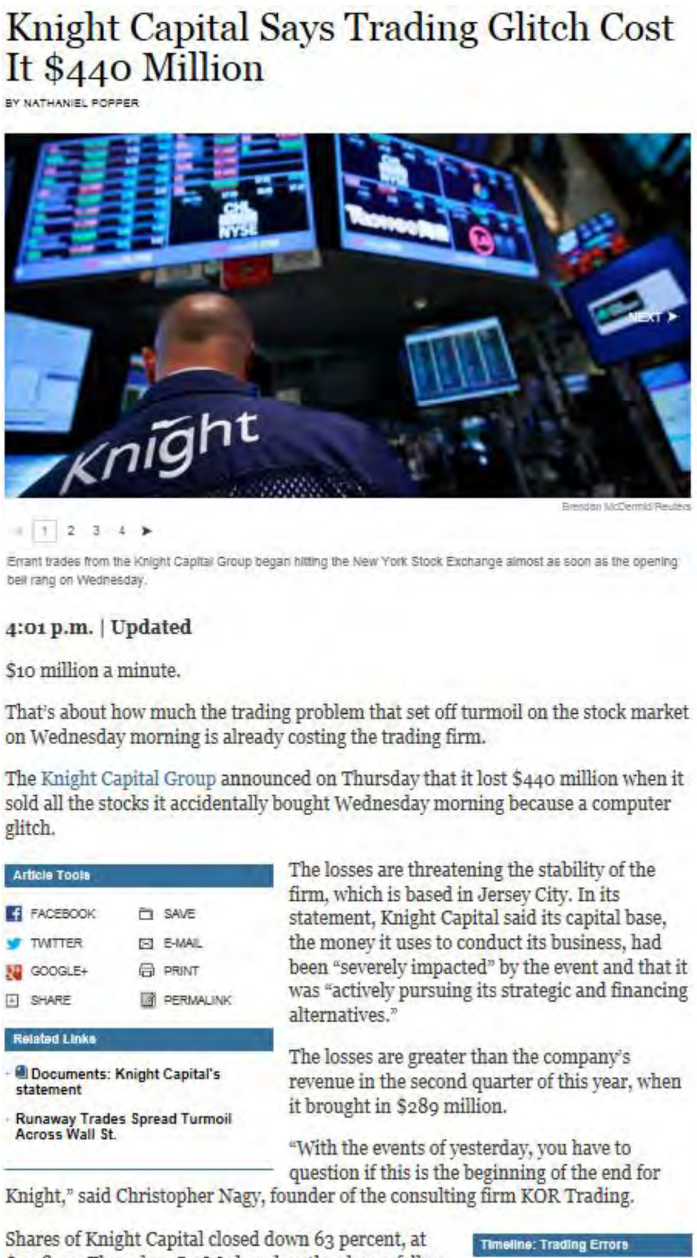
PHOTO: STAN HONDA/AFP/GETTY IMAGES

Knight Capital Group (KCG) was behind a series of bizarre moves in otherwise thinly traded stocks early Wednesday.

Knight spokesperson Kara Fitzimmons acknowledged that "a technology issue" occurred in its market-making unit that affected how shares for some 150 NYSE-listed stocks were routed. "Knight notified its market-making clients this morning to route listed orders away," she said in a statement, adding that the company continues to investigate.

Knight's shares dropped more than 20% after traders saw extreme volume spikes in a number of stocks, including preferred shares of Wells Fargo (JWF) and semiconductor company Spansion (CODE). Both stocks, which see roughly 100,000 trade per day, had changed hands more than 4 million times by late morning.

Knight's shares ended the trading day down 33%.



Knight Capital Says Trading Glitch Cost It $440 Million

BY NATHANIEL POPPER

Brendan McDermid/Reuters

Errant trades from the Knight Capital Group began hitting the New York Stock Exchange almost as soon as the opening bell rang on Wednesday.

4:01 p.m. | Updated

$10 million a minute.

That's about how much the trading problem that set off turmoil on the stock market on Wednesday morning is already costing the trading firm.

The Knight Capital Group announced on Thursday that it lost $440 million when it sold all the stocks it accidentally bought Wednesday morning because a computer glitch.

Article Tools
FACEBOOK
SAVE
TWITTER
E-MAIL
GOOGLE+
PRINT
SHARE
PERMALINK
Related Links
Documents: Knight Capital's statement
Runaway Trades Spread Turmoil Across Wall St.

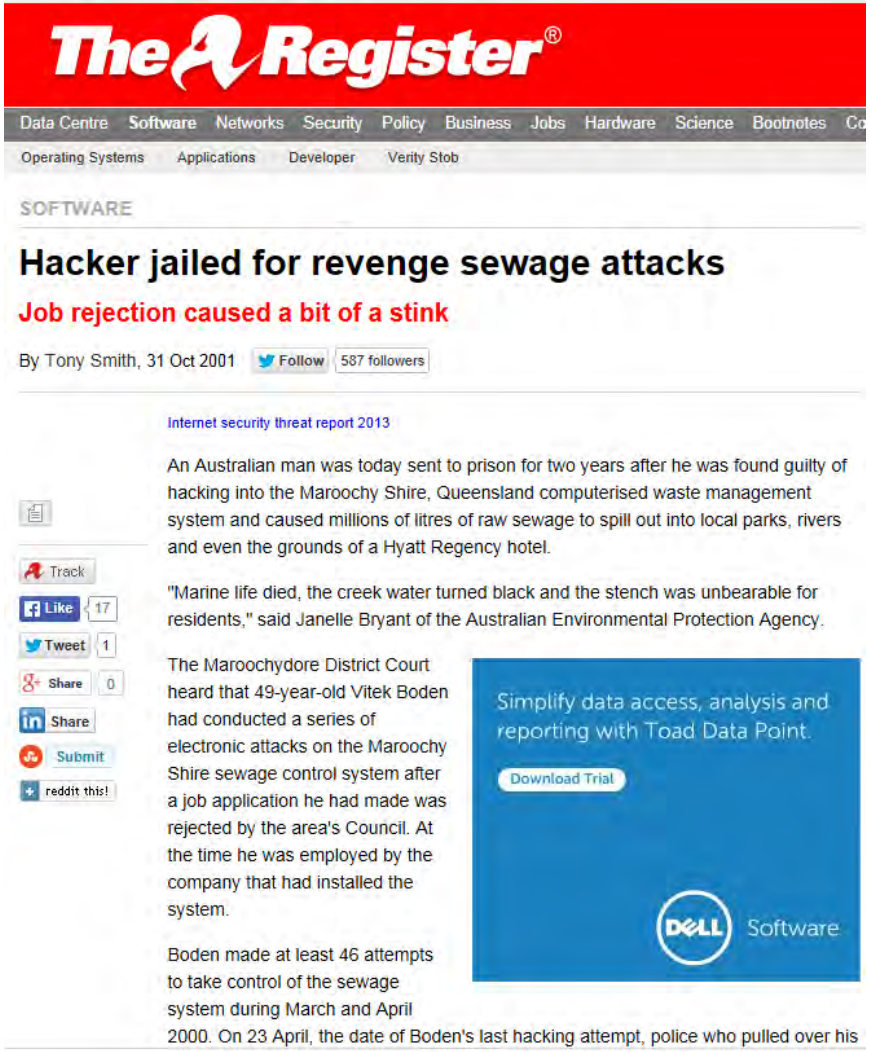
The losses are threatening the stability of the firm, which is based in Jersey City. In its statement, Knight Capital said its capital base, the money it uses to conduct its business, had been "severely impacted" by the event and that it was "actively pursuing its strategic and financing alternatives."

The losses are greater than the company's revenue in the second quarter of this year, when it brought in $289 million.

"With the events of yesterday, you have to question if this is the beginning of the end for Knight," said Christopher Nagy, founder of the consulting firm KOR Trading.

Shares of Knight Capital closed down 63 percent, at

Precedent: The Maroochy Shire Pollution Incident



SOFTWARE

Hacker jailed for revenge sewage attacks

Job rejection caused a bit of a stink

By Tony Smith, 31 Oct 2001 Follow 587 followers

Internet security threat report 2013

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency.

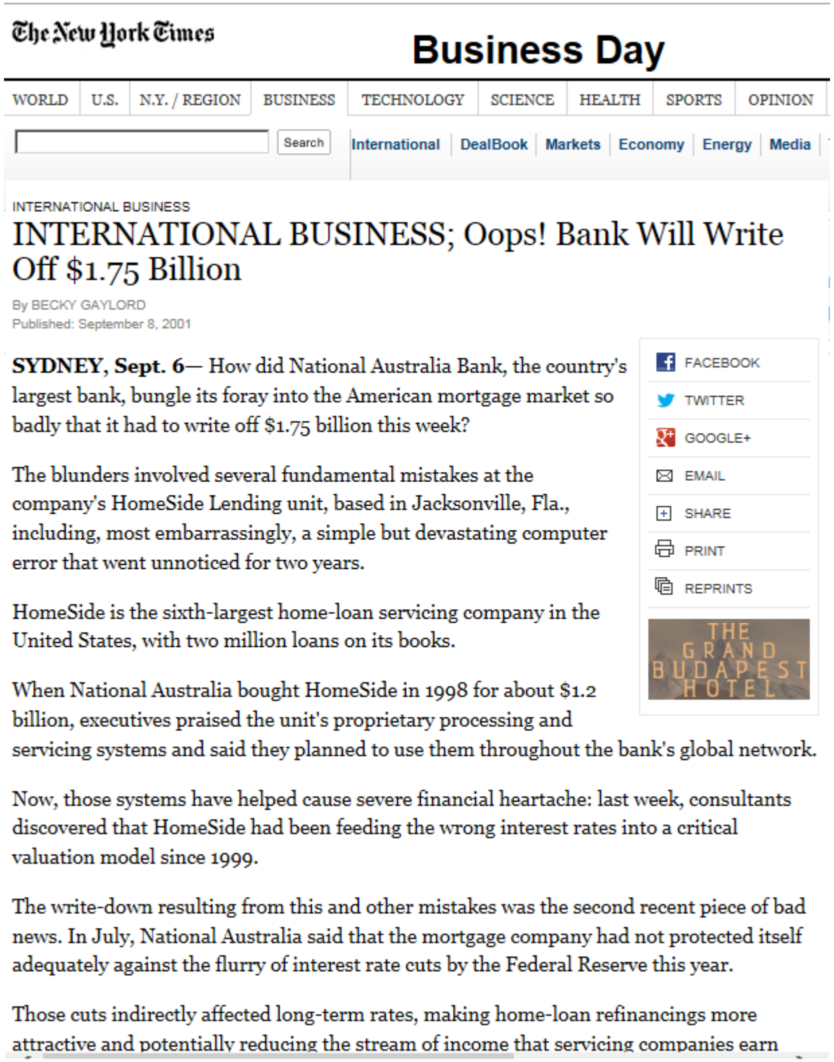
The Maroochydore District Court heard that 49-year-old Vitek Boden had conducted a series of electronic attacks on the Maroochy Shire sewage control system after a job application he had made was rejected by the area's Council. At the time he was employed by the company that had installed the system.

Boden made at least 46 attempts to take control of the sewage system during March and April 2000. On 23 April, the date of Boden's last hacking attempt, police who pulled over his

Typical SCADA controlled sewage system

UNIVERSITY OF CAMBRIDGE
Judge Business School
Centre for **Risk Studies**

Precedent: National Australia Bank



INTERNATIONAL BUSINESS

INTERNATIONAL BUSINESS; Oops! Bank Will Write Off $1.75 Billion

By BECKY GAYLORD
Published: September 8, 2001

SYDNEY, Sept. 6— How did National Australia Bank, the country's largest bank, bungle its foray into the American mortgage market so badly that it had to write off $1.75 billion this week?

The blunders involved several fundamental mistakes at the company's HomeSide Lending unit, based in Jacksonville, Fla., including, most embarrassingly, a simple but devastating computer error that went unnoticed for two years.

HomeSide is the sixth-largest home-loan servicing company in the United States, with two million loans on its books.

When National Australia bought HomeSide in 1998 for about $1.2 billion, executives praised the unit's proprietary processing and servicing systems and said they planned to use them throughout the bank's global network.

Now, those systems have helped cause severe financial heartache: last week, consultants discovered that HomeSide had been feeding the wrong interest rates into a critical valuation model since 1999.

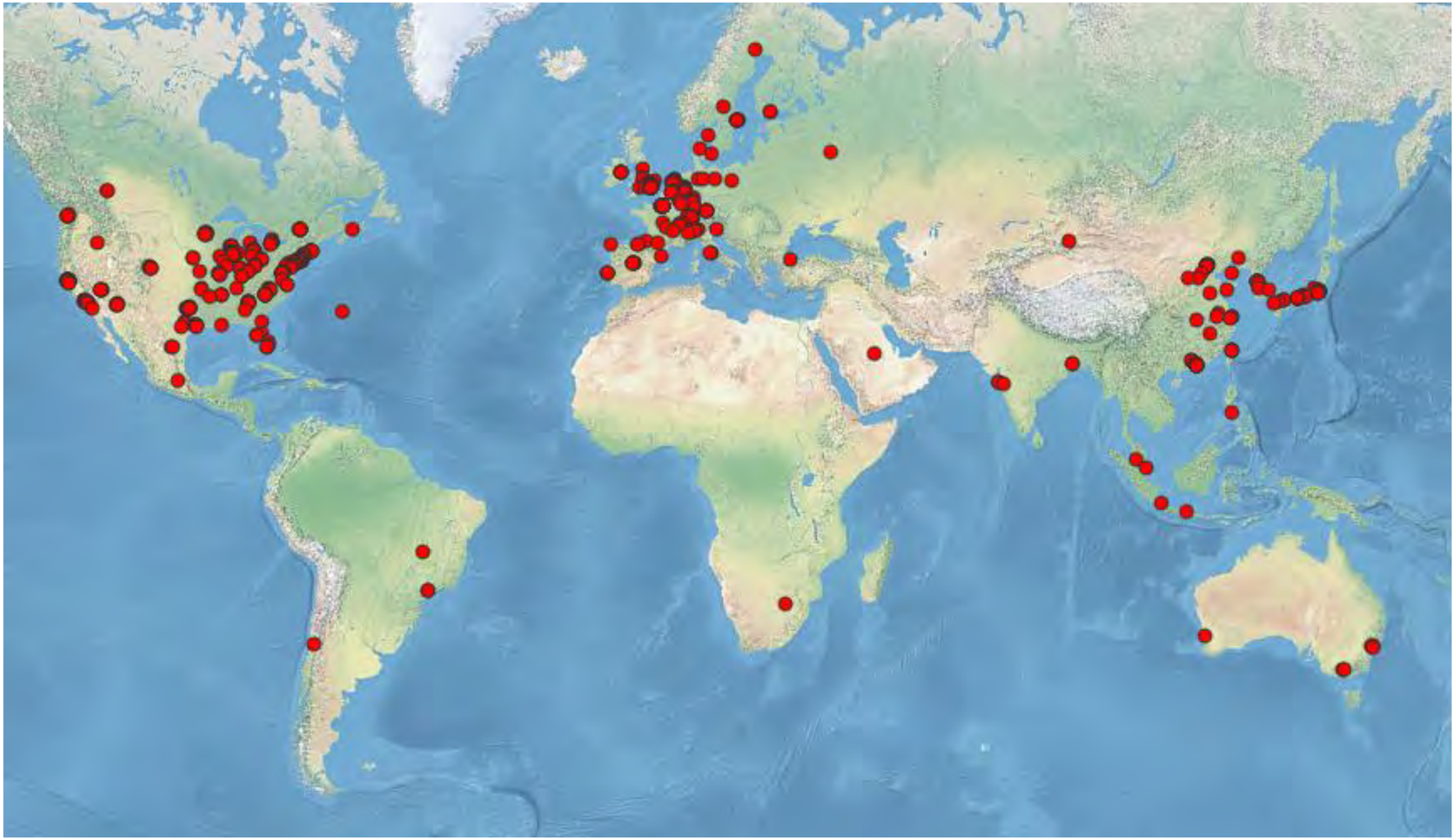
The write-down resulting from this and other mistakes was the second recent piece of bad news. In July, National Australia said that the mortgage company had not protected itself adequately against the flurry of interest rate cuts by the Federal Reserve this year.

Those cuts indirectly affected long-term rates, making home-loan refinancings more attractive and potentially reducing the stream of income that servicing companies earn

nab

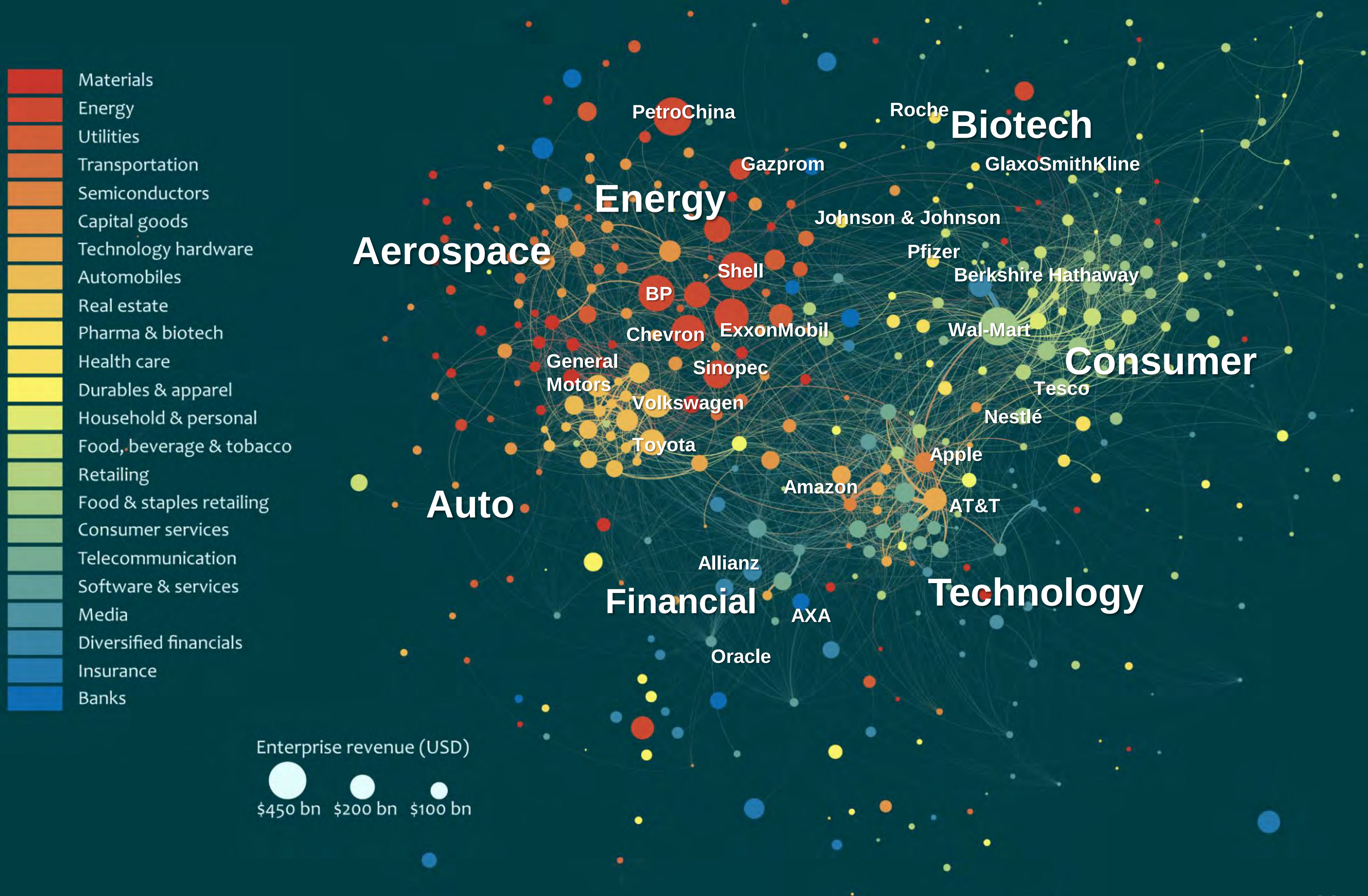
homeside
powered by nab

Global Enterprise Network

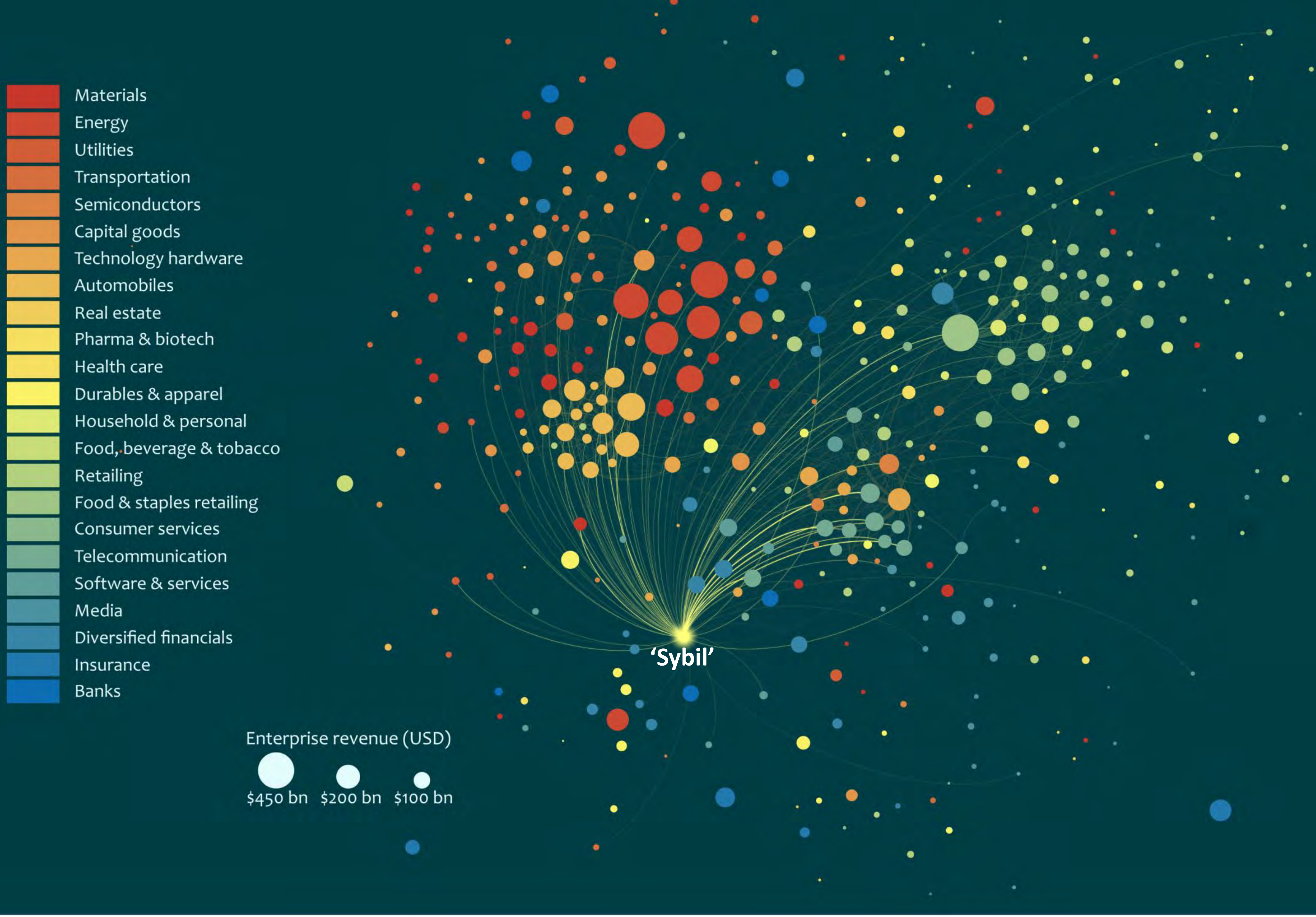


The 600 enterprises with the location of their corporate HQs mapped

Global Enterprise Network



Sybil Market Penetration

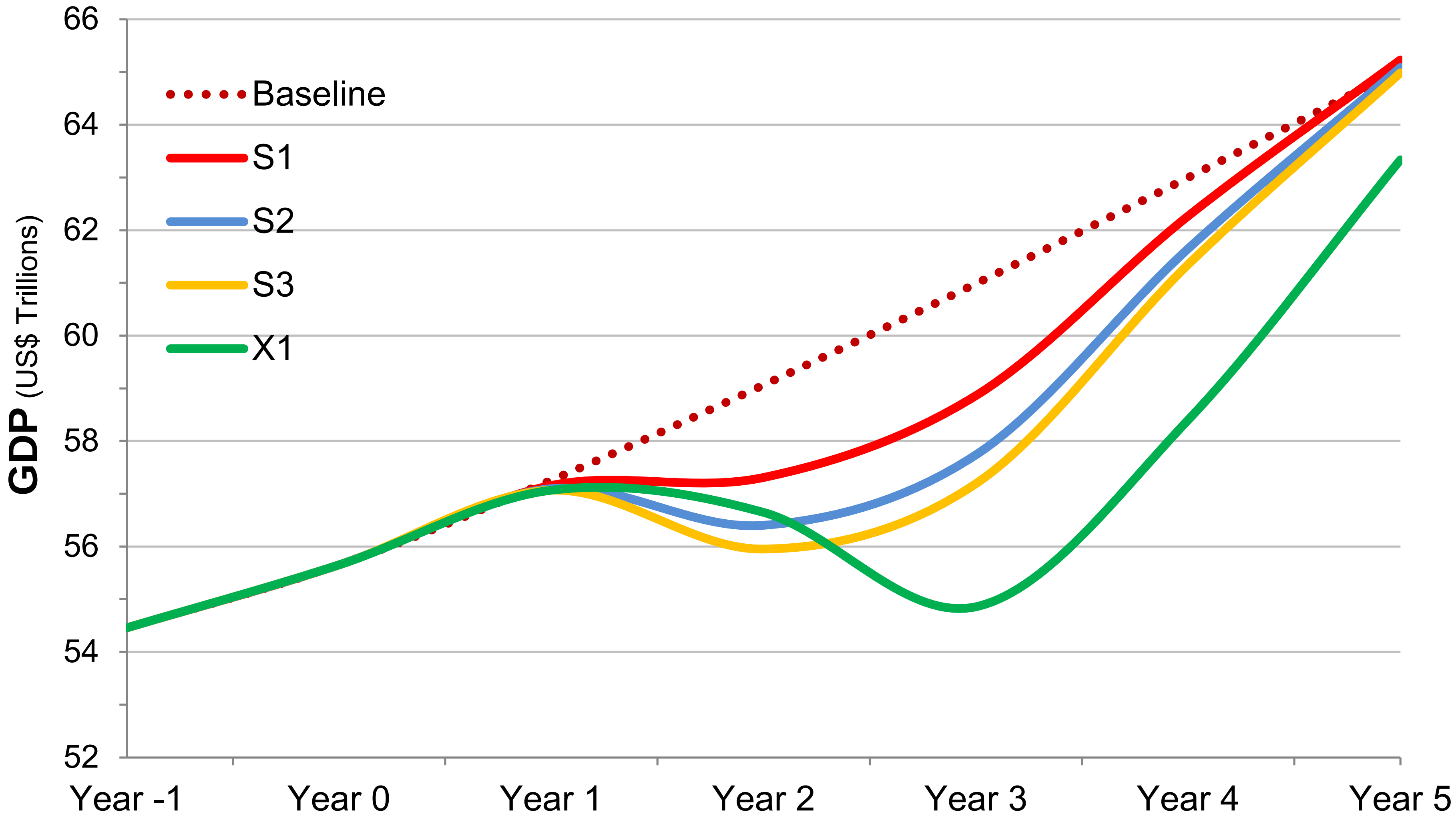


Impact of the Cyber Scenario and Variants

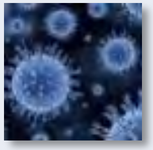
Scenario Variant	Latency period (quarters)	Global 5 year GDP@Risk
S1: Standard Scenario	5	$**4.5** Trillion
S2: Increased Impact Scenario x 1.5	5	$**7.4** Trillion
S3: Greatly Increased Impact x 1.75	5	$**8.8** Trillion
X1: Greatly Increased Impact x 1.75 & Long Latency Scenario	8	$**15.0** Trillion

Great Financial Crisis 2007/08 at 2014	$20 Trillion

Global GDP@Risk Impact of Scenario and Variants



Comparison with other Risk Centre Scenarios

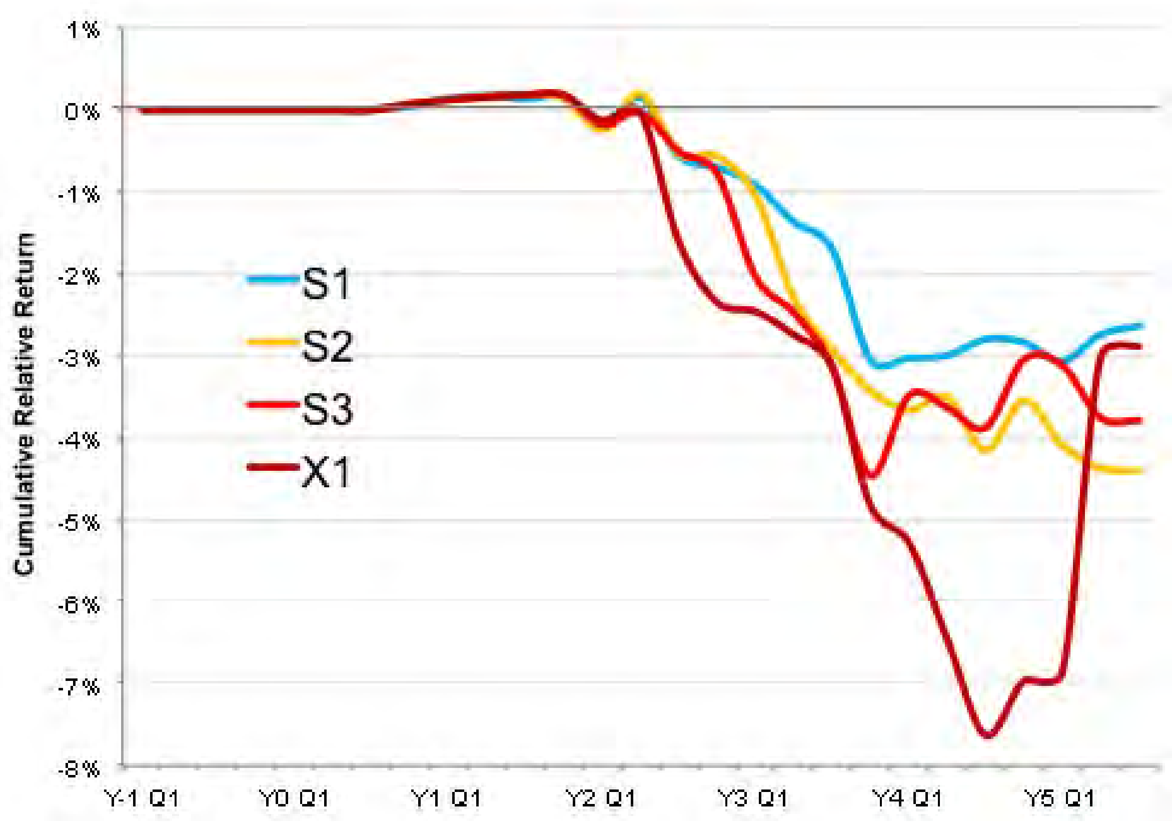
Scenario	S1	S2	X1
Geopolitical Conflict	**17**	**27**	**34**
	9 month conflict	2 year conflict	5 year conflict
 **Pandemic**	**7**	**10**	**23**
	43% infection	Poor response	Poor response + Vaccine failure
Social Unrest	**4**	*	*
	Europe & US Only	Europe, US + BRICS	Europe, US, BRICS + ME
Cyber Catastrophe	**4.5**	**7.4**	**15**
	Standard scenario	More damage + liability	Longer latency period
2007-2012 Great Financial Crisis	18		
Great Financial Crisis at 2014	20		

US$ Trillion 5 Year GDP@Risk

Impact on representative portfolio assets

				Base Levels	Short Term Impact (△Max)				Long Term Impact (△Max)			
				Yr0Q4	Yr1Q4				Yr3Q3			
				B0	S1	S2	S3	X1	S1	S2	S3	X1
US												
Bonds Short	TSY 2Y	Interest rate, 2-year T-notes (levels)	△	0.3	-0.06	-0.07	-0.07	-0.07	-0.07	-0.47	-0.71	-4.1
Bonds Long	TSY 10Y	Interest rate, 10 year government bonds (levels)	△	2.7	-0.09	-0.11	-0.12	-0.12	0.005	-0.4	-0.7	-4.3
Equities	S&P	Share price index (% change)	%	100	-3.0	-3.1	-3.2	-3.2	-27.0	-35.3	-39.1	-51.6
Credit	YSA CSPA	Credit spreads, period average (levels)	△	0.3	0.032	0.035	0.037	0.037	0.01	-0.02	-0.05	-0.04
Inflation	USA CPI	Consumer price index (% change)	%	100	-1.7	-2.6	-3.0	-3.0	-15.5	-22.8	-26.4	-33.4
UK												
Bonds Short	GBP 2Y	Interest rate, 2-year T-notes	△	0.5	-0.33	-0.35	-0.35	-0.35	-0.2	-0.4	-0.46	-1.6
Bonds Long	GBP 10Y	Interest rate, 10 year government bonds	△	2.8	-0.28	-0.31	-0.32	-0.32	-0.1	-0.4	-0.5	-1.9
Equities	FTSE	Share price index	%	100	-1.4	-1.7	-1.8	-1.8	-17.8	-24.7	-28.0	-36.0
Credit	GBP CSPA	Credit spreads, period average	△	0	0	0	0	0	0	0	0	0
Inflation	GBP CPI	Consumer price index	%	100	-1.8	-2.7	-3.2	-3.2	-8.0	-12.4	-14.7	-21.4
Foreign Exchange	USD/GBP	Exchange Rate (US$ £GBP)	%	1.6	-1.13	-1.09	-1.07	-1.07	2.98	3.28	3.52	0.145
Germany												
Bonds Short	DEM 2Y	Interest rate, 2-year German gov bond yields	△	0.2	-0.08	-0.06	-0.06	-0.06	-0.6	-1.2	-1.5	-2.8
Bonds Long	DEM 10Y	Interest rate, 10 year German gov bond yields	△	1.8	-0.08	-0.07	-0.06	-0.06	-0.4	-0.97	-1.2	-2.9
Equities	DAX	Share price index, Deutscher Aktien Index	%	100	-1.5	-2.7	-3.3	-3.3	-28.4	-39.3	-44.2	-55.0
Credit	DEM CSPA	Credit spreads, Period Average	△	1.8	0.03	0.05	0.06	0.06	0.13	0.17	0.19	0.23
Inflation	DEM CPI	Consumer Price Index, Germany	%	100	-2.9	-4.4	-5.2	-5.2	-19.1	-27.9	-32.0	-41.6
Foreign Exchange	USD/EUR	Exchange Rate (US$ per Euro)	%	1.3	-0.7	-0.7	-0.7	-0.7	1.21	1.15	1.12	1.07
Japan												
Bonds Short	JPY 2Y	Interest rate, 2-year Japan gov bond yields	△	0.1	-0.04	-0.03	-0.025	-0.029	0.08	-0.09	-0.17	-2.0
Bonds Long	JPY 10Y	Interest rate, 10 year Japan gov bond yields	△	0.6	-0.058	-0.047	-0.041	-0.041	0.12	-0.09	-0.19	-2.1
Equities	NIKKEI	Share price index, Nikkei 225	%	100	-1.1	-1.8	-2.3	-2.3	-10.6	-14.1	-15.7	-17.1
Credit	JPY CSPA	Credit spreads, Period Average	△	0.2	0	0	0	0	0	0	0	0
Inflation	JPY CPI	Consumer Price Index, Japan	%	100	-1.2	-1.9	-2.2	-2.2	-7.6	-11.3	-13.0	-19.8
Foreign Exchange	USD/JPY	Exchange Rate (US$ per JPY)	%	0.013	0.144	0.148	0.150	0.150	-0.27	-0.32	-0.35	-0.32

Relative change of cumulative returns



Conclusion: Diversify IT Platforms

Outcomes of Scenario

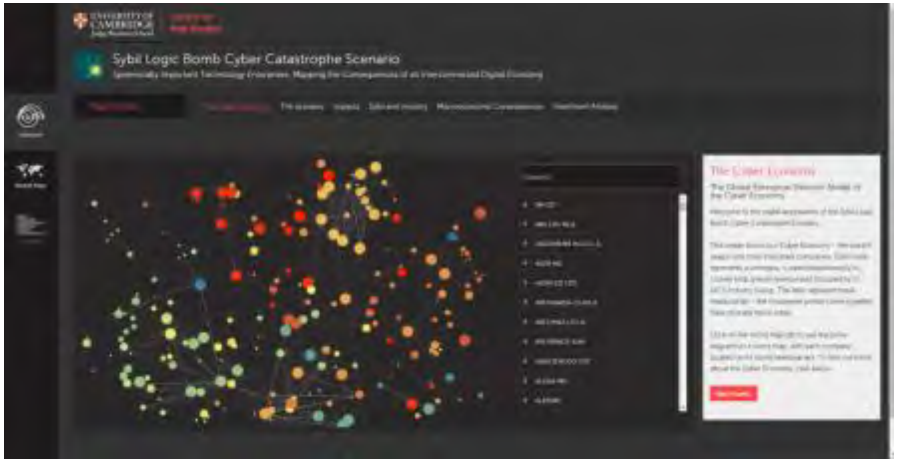
- Compromise of a Systemically Important Technology Enterprise (SITE)
- ‘Information Malaise’: Loss of trust in IT by business leaders, investors and consumers
- World 5 Year GDP@Risk: $4.5Tr

Implications for Risk Management

- Efficiency drive towards standardisation in corporate IT platforms contrary to good risk management
- Portfolio diversification by companies in their choice of technology platforms

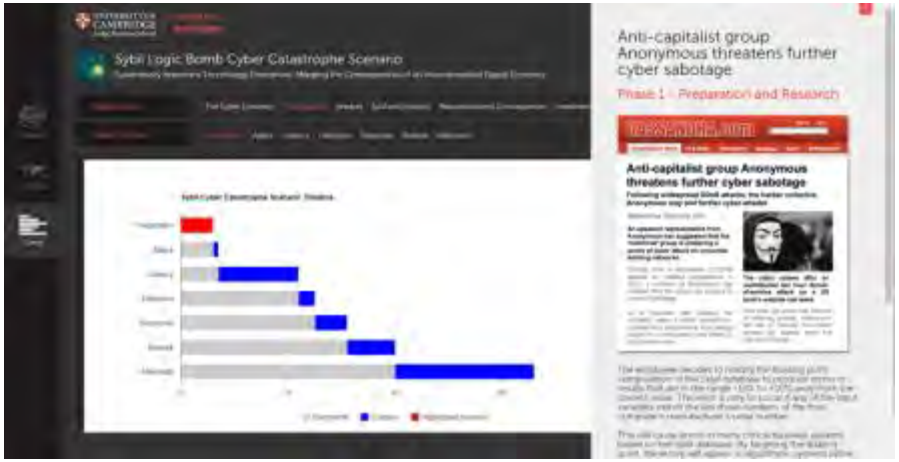
Online Digital Exploration

sybil.cambridgeriskframework.com



Sybil Logic Bomb Cyber Catastrophe Scenario

The Cyber Economy



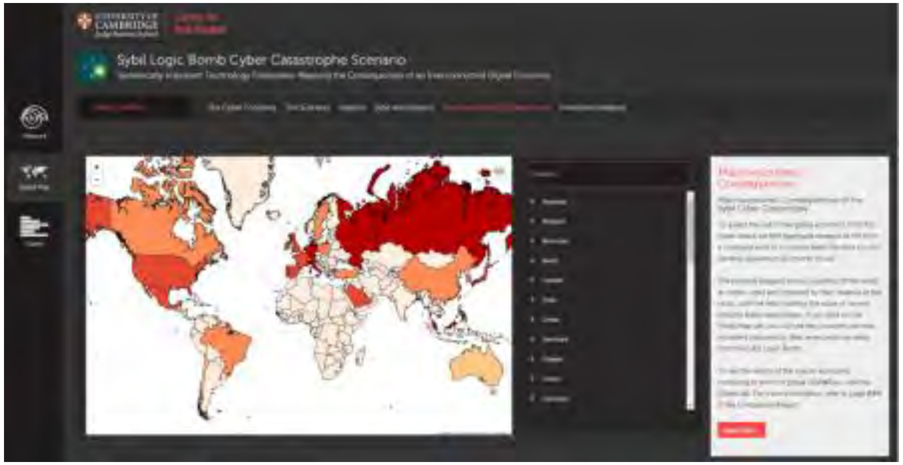
Sybil Logic Bomb Cyber Catastrophe Scenario

Sybil Cyber Catastrophe Scenario Timeline

Anti-capitalist group Anonymous threatens further cyber sabotage

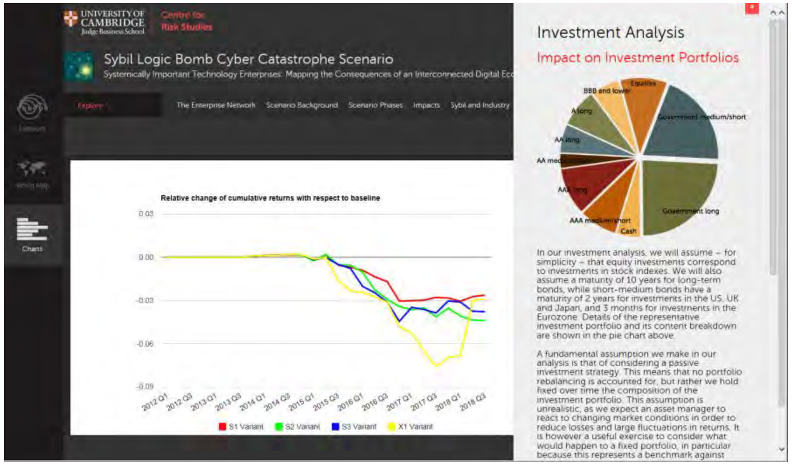
Phase 1 – Preparation and Research

Anti-capitalist group Anonymous threatens further cyber sabotage



Sybil Logic Bomb Cyber Catastrophe Scenario

Macroeconomic Consequences



Sybil Logic Bomb Cyber Catastrophe Scenario

Systemically Important Technology Enterprises: Mapping the Consequences of an Interconnected Digital Ec

Relative change of cumulative returns with respect to baseline

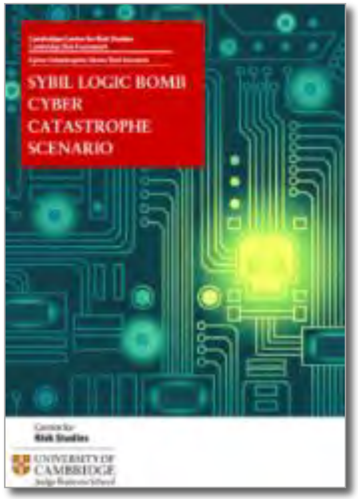
Investment Analysis

Impact on Investment Portfolios

In our investment analysis, we will assume – for simplicity – that equity investments correspond to investments in stock indexes. We will also assume a maturity of 10 years for long-term bonds, while short-medium bonds have a maturity of 2 years for investments in the US, UK and Japan, and 3 months for investments in the Eurozone. Details of the representative investment portfolio and its content breakdown are shown in the pie chart above.

A fundamental assumption we make in our analysis is that of considering a passive investment strategy. This means that no portfolio rebalancing is accounted for, but rather we hold fixed over time the composition of the investment portfolio. This assumption is unrealistic, as we expect an asset manager to react to changing market conditions in order to reduce losses and large fluctuations in returns. It is however a useful exercise to consider what would happen to a fixed portfolio, in particular because this represents a benchmark against

Sybil Logic Bomb Scenario Report



SYBIL LOGIC BOMB
CYBER
CATASTROPHE
SCENARIO

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Cyber Catastrophe
Stress Test Scenario

Available for Download from Website:
CambridgeRiskFramework.com

Thurs 22 January – **Social Unrest Risk**

Registration at

http://www.risk.jbs.cam.ac.uk/

Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School