

Centre for Risk Studies

5th Risk Summit: Special Topics Seminar

Cyber Catastrophe: An Interlinked Systemic Risk

Simon Ruffle

Director of Technology Research and
Innovation

Centre for
Risk Studies



UNIVERSITY OF
CAMBRIDGE
Judge Business School

The Cyber Threat Landscape

Bloomberg Full Company Professional Anywhere Search News, Videos, Photos, Audio

Hackers in China Compromise U.S. Defense Secrets
Defense Department contractor Qinetic was infiltrated by hackers from China on several occasions. The company makes defense systems such as spy satellites and bomb disposal robots used by the U.S. military.

A history of hacking at Qinetic
Period of reported successful hacking Dates of hacking
Dec. 4, 2007 Qinetic North America, QNA, is informed by Naval Criminal Investigation Service that proprietary data is being stolen, resulting in the loss of a "large quantity of sensitive information." The hackers were identified as the Shanghai-based group known as the People's Liberation Army.
Jan. 7, 2008 NASA tells QNA of an attack on space agency's systems originating from a hacked QNA computer.
Feb. - Mar. 2008 The Communist Group attacks the company three times in February and March.
Feb. 10, 2009 - March 13, 2009

Anonymous Message To Greek Gov For Ert

2.4 Digital Disintegration WORLD ECONOMIC FORUM
Data fraud/loss, Cyber attacks, Critical information infrastructure breakdown, Terrorist attack, Organized crime and illicit trade, Global governance failure

Breaking: Two Explosions in the White House and Barack Obama is injured
3,242 RETWEETS 153 FAVORITES
12:07 PM - 23 Apr 13

BBC NEWS US & CANADA
Cybercriminals 'drained ATMs' in \$45m world bank heist
A gang of cybercriminals stole \$45m (£28m) by hacking into a database of prepaid debit cards and draining cash machines around the world, US prosecutors say.
Seven people have been charged in New York over the heist, which allegedly involved actors in 20 countries.
An eighth suspect is thought to have been murdered in April.
The network used state cards to target banks in the United Arab Emirates and Oman, court documents said.
Prosecutors said law enforcement agencies in Japan, Canada, the UK, Somalia and 12 other countries were involved in the investigation.
Arrests had been made in other countries, they said, although details were not released.
'Laptops not guns'

banks fear cyber attack more than euro crisis: Haldane
Reuters - Wed, Jun 10, 2013
Worries over hacking and other cyber attacks has pushed aside the euro zone risk for Britain's banks and they must do more to protect themselves, a senior Bank of England official said on Wednesday.
The financial sector has become a more pressing worry, underlined by a series of cyber attacks in the last month laid out details of a crime ring they say stole \$45 million from two

ViewpointMICHELLE 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



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

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.

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

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

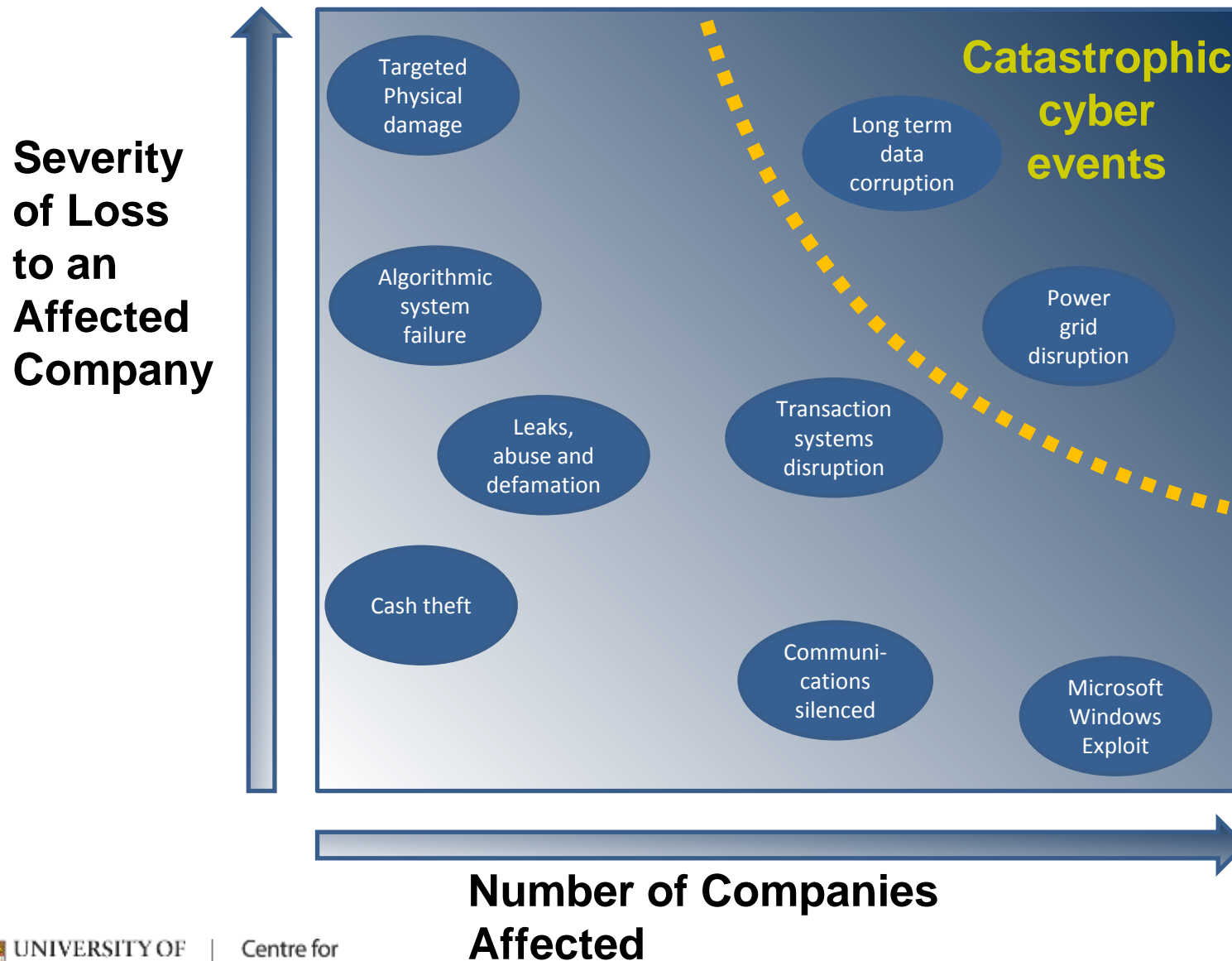
Taxonomy of Cyber Catastrophe Scenarios

*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	

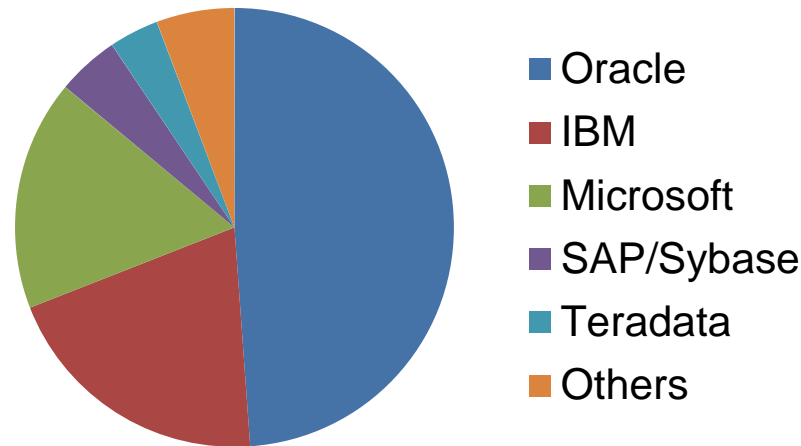
* = ranked worst case scenarios by subject matter expert team at Cyber Threat Workshop 17th July 2013

Scenario Definition



The Sybil Logic Bomb 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 Strategically Important Technology Enterprise (SITE)
- Sybil is based on Oracle. We use Oracle to characterise Sybil.

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

Year 1

Year 2

Year 3

Year 4

Year 5

3

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

CNN Money

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

Recommend 66 Tweet 23 Share 2 Email Print



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

Knight spokesperson Kara Fitzsimmons 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

1 2 3 4

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

Timeline: Trading Errors

Precedent: The Maroochy Shire Pollution Incident

The Register[®]

Data Centre Software Networks Security Policy Business Jobs Hardware Science Bootnotes Co
Operating Systems Applications Developer Verity Stob

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 Maroochydhore 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

Track

Like 17

Tweet 1

Share 0

Share

Submit

reddit this!

Simplify data access, analysis and reporting with Toad Data Point.

Download Trial





Typical SCADA controlled sewage system

Precedent: National Australia Bank

The New York Times **Business Day**

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION

Search International DealBook Markets Economy Energy Media

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

FACEBOOK
TWITTER
GOOGLE+
EMAIL
SHARE
PRINT
REPRINTS

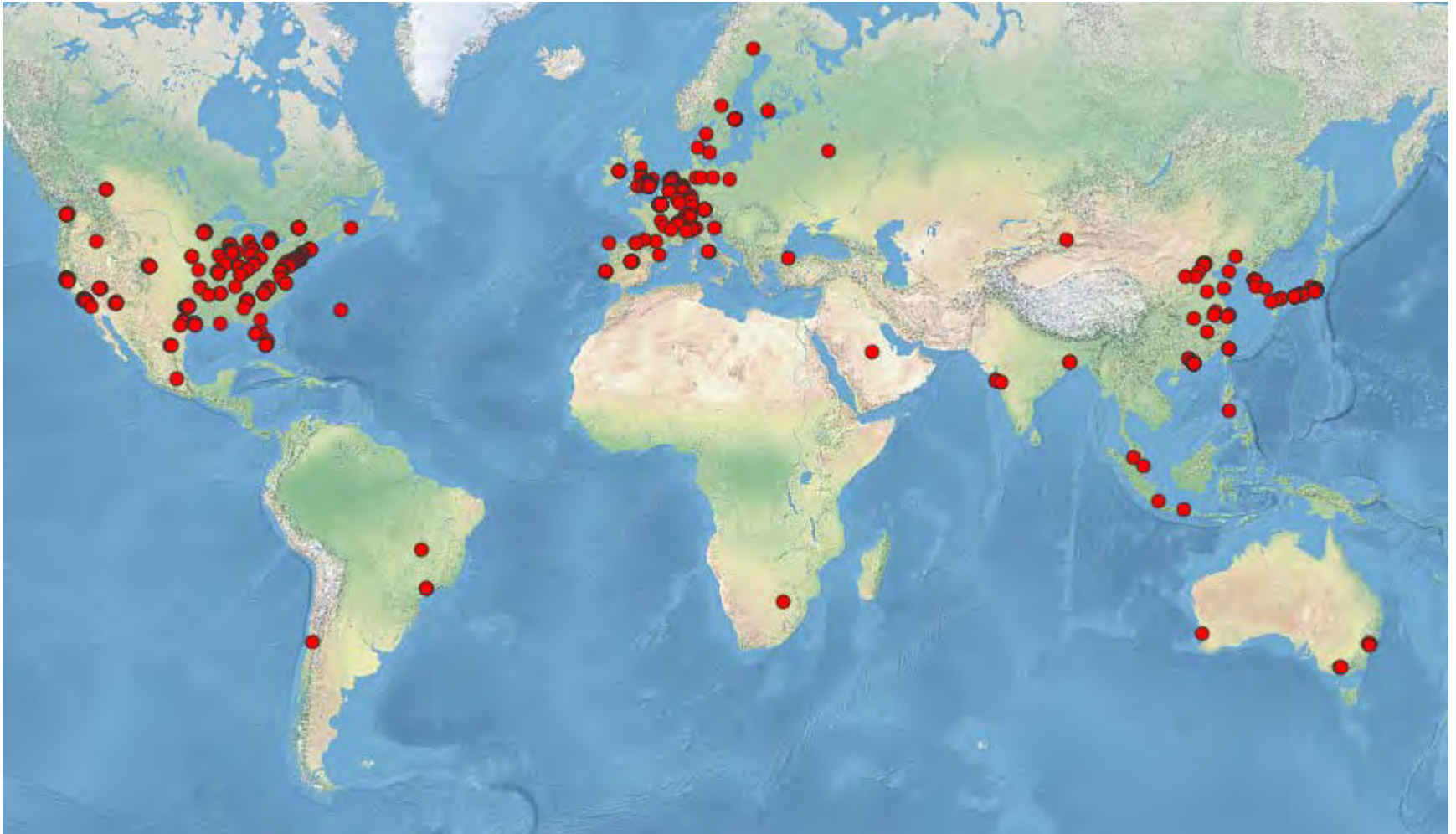
THE GRAND BUDAPEST HOTEL



Loss Mechanisms

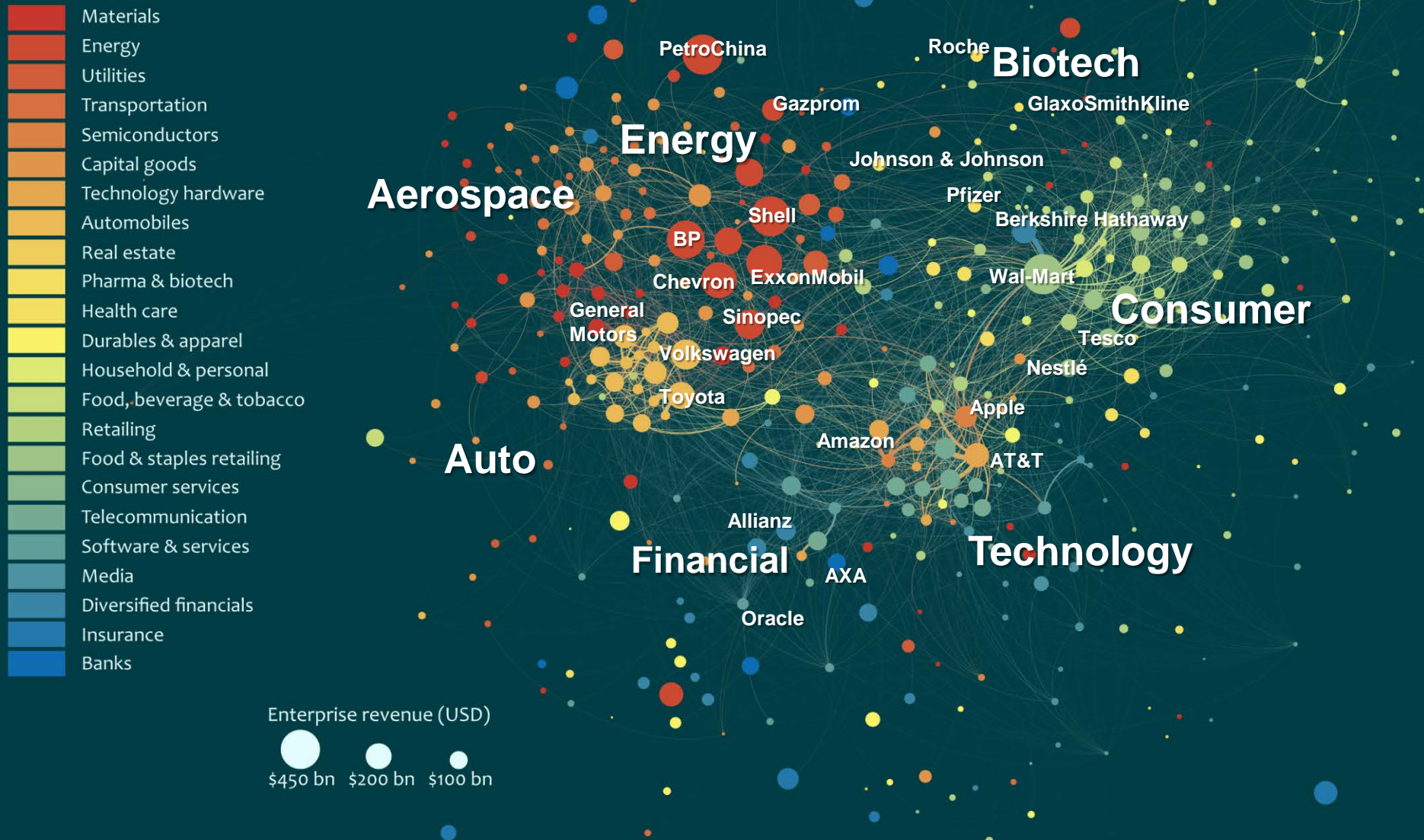
Business Interruption	
Loss of income	Business Interruption
Increased cost of operation	Extra Expense Insurance
Degradation in service	
3rd Party Liabilities and Penalties	
General liability	General liability (GL)
Directors and Officers	Directors and Officers
Workers' compensation	Workers' compensation
Liability for Loss / corruption of 3rd party assets - digital, physical	Liability
Privacy breach liability	Liability
Data misuse liability	Liability
Compensation to customers	Liability
Contractual compensation	Liability
Fines	Cyber Insurance
Property Losses	
Loss of assets	Cyber Insurance
Loss of digital assets	Cyber Insurance
Financial theft, of money or equipment	
Financial fraud/extortion	
IP Losses	
Patented, Copyright material	
Customer lists	
Commercially sensitive information	
Reputation Losses	
Goodwill	
Market Value	
Customer/Partner Confidence	
Operational costs	
Administrative and recovery	Extra Expense Insurance
Security activities	

Global Enterprise Network

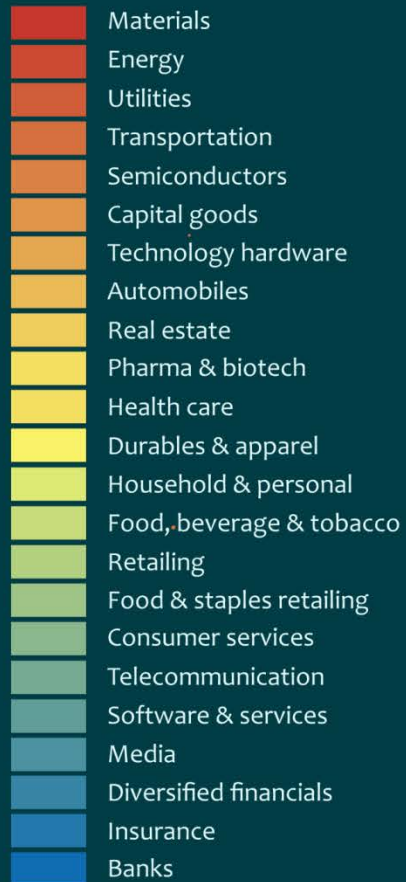


The 600 enterprises with the location of their corporate HQs mapped

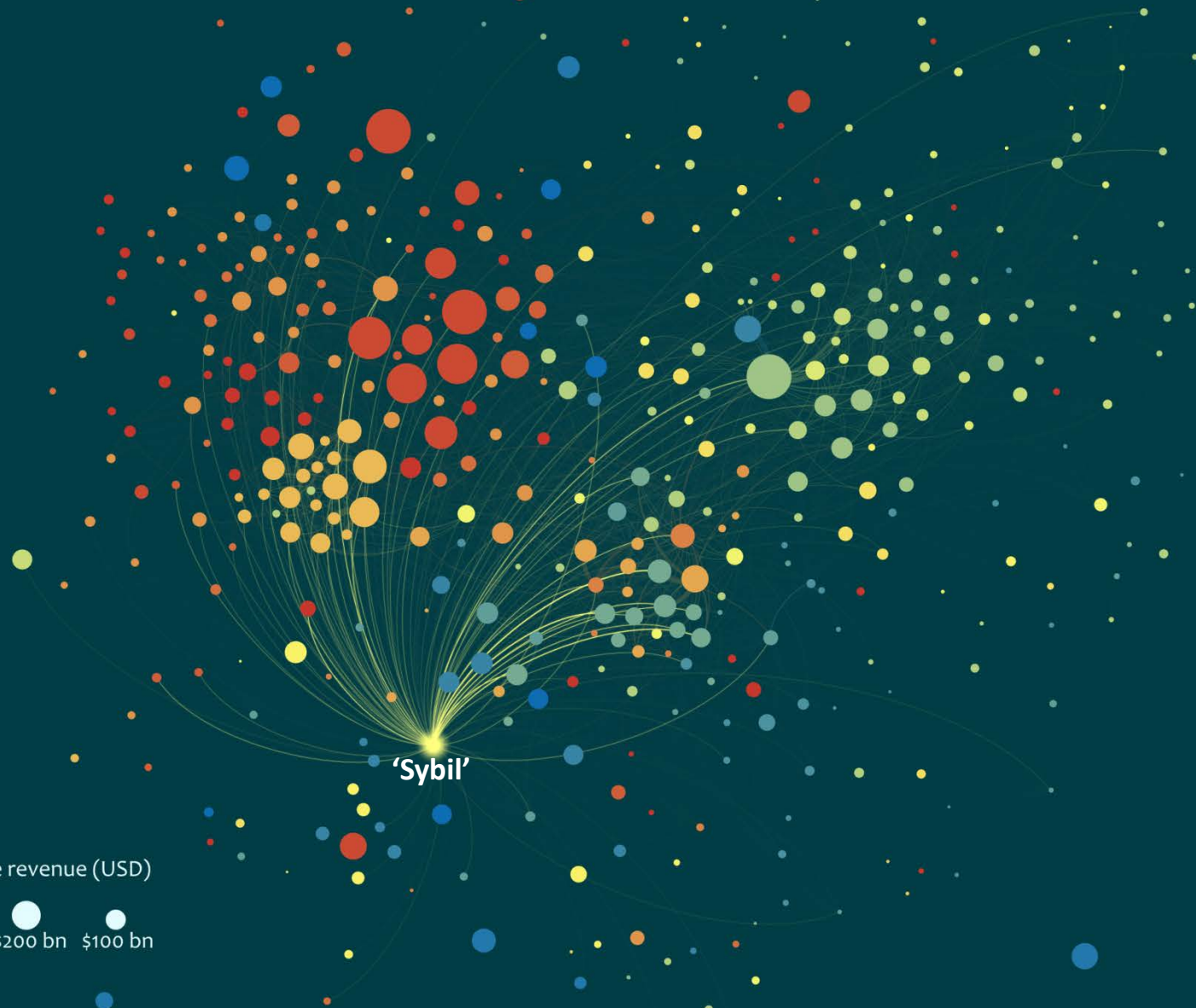
Global Enterprise Network




Sybil Market Penetration



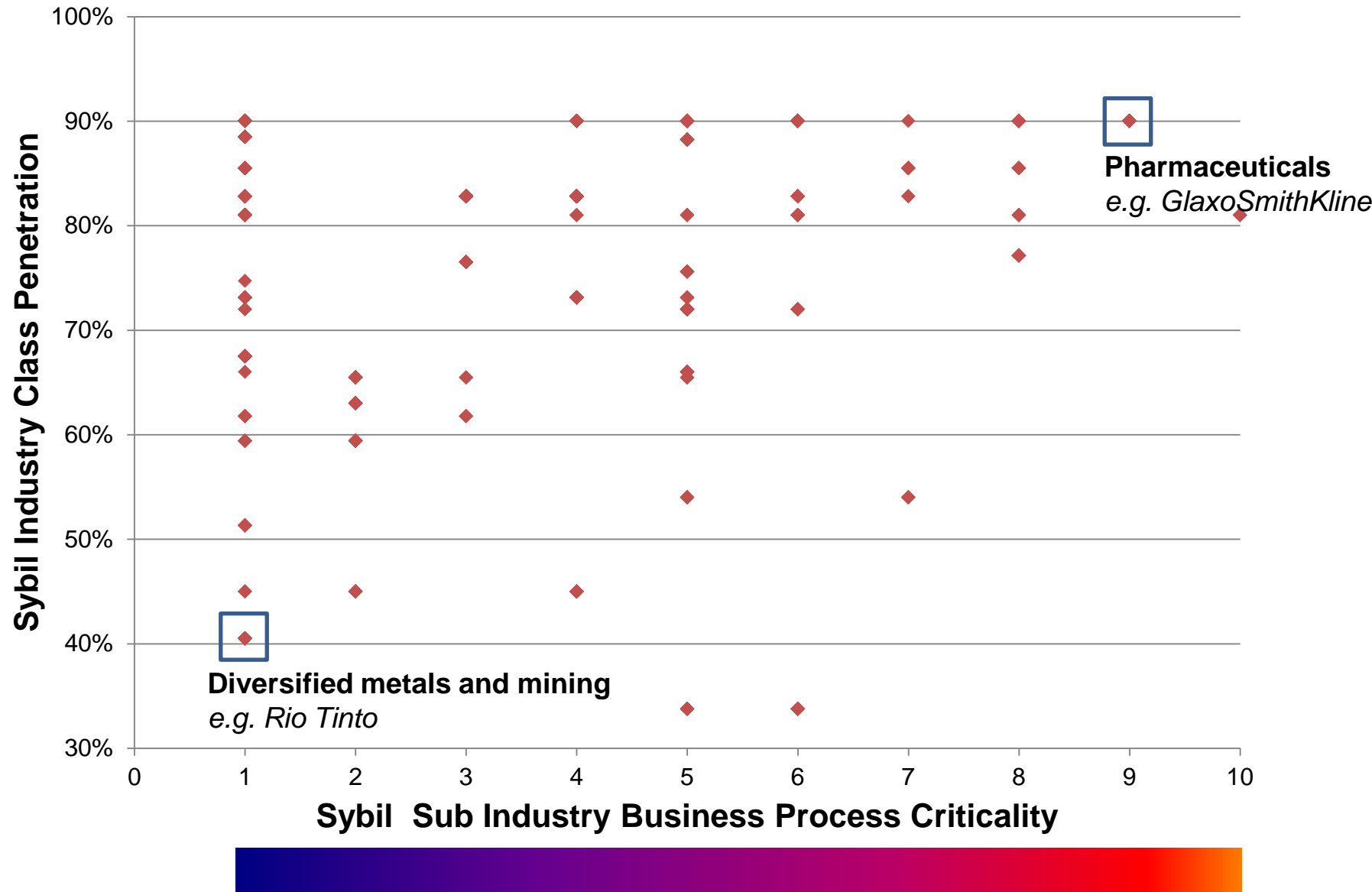
Enterprise revenue (USD)



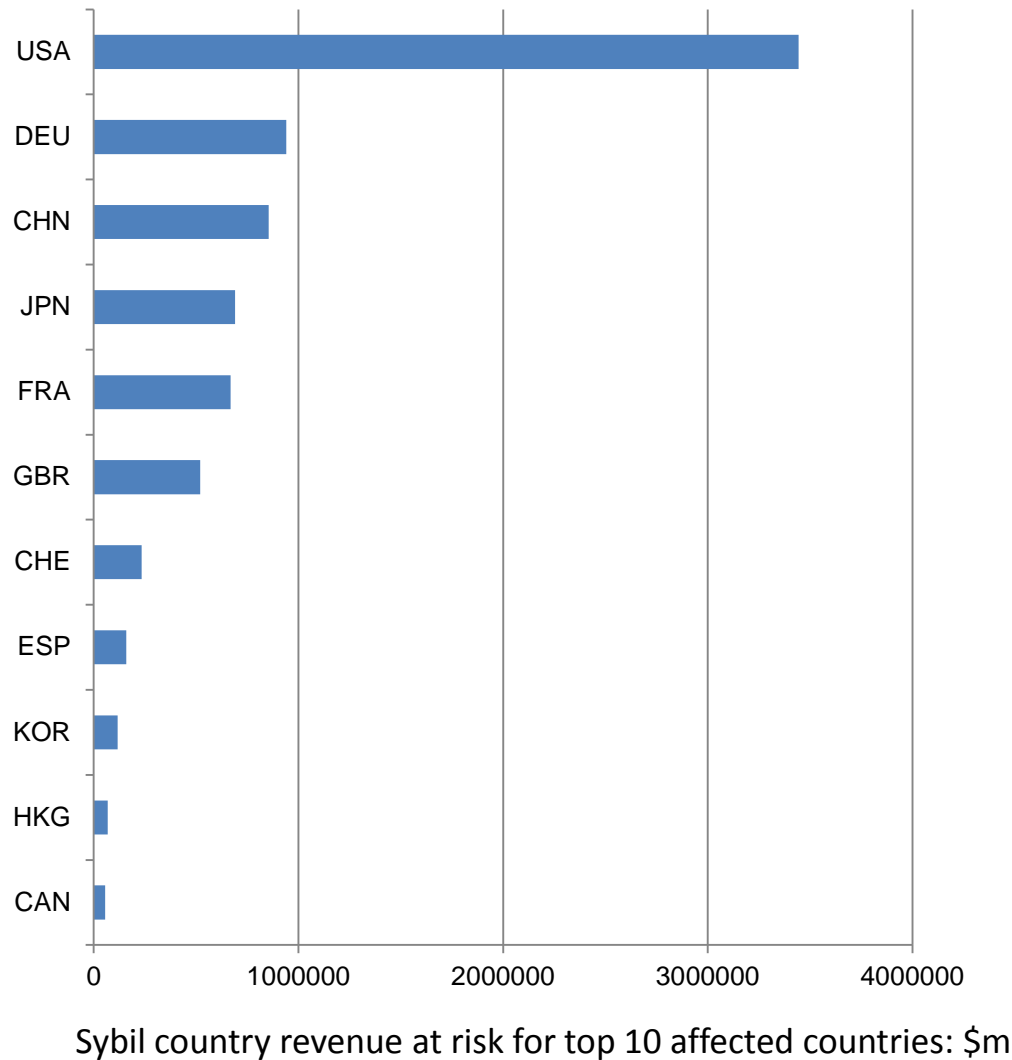
Business Process Criticality

		Score	Definition
<div>Finance</div> <div>Sales & Marketing & Customer Relations</div> <div>Admin and Management</div> <div>Operations</div>		1	Minor use
		2	Used for minor administrative tasks
		3	Used for many administrative tasks
		4	Used for all main company administration & finance
		5	Used for admin, finance and some customer relations
		6	Central to customer relations: sales, marketing and billing
		7	Used in one but not all core business processes, but not admin
		8	Used in some business processes and admin, finance and some customer relations
		9	Used in many business processes and central to customer relations: sales, marketing and billing
		10	Central to all main business processes, administration, finance and customer relations

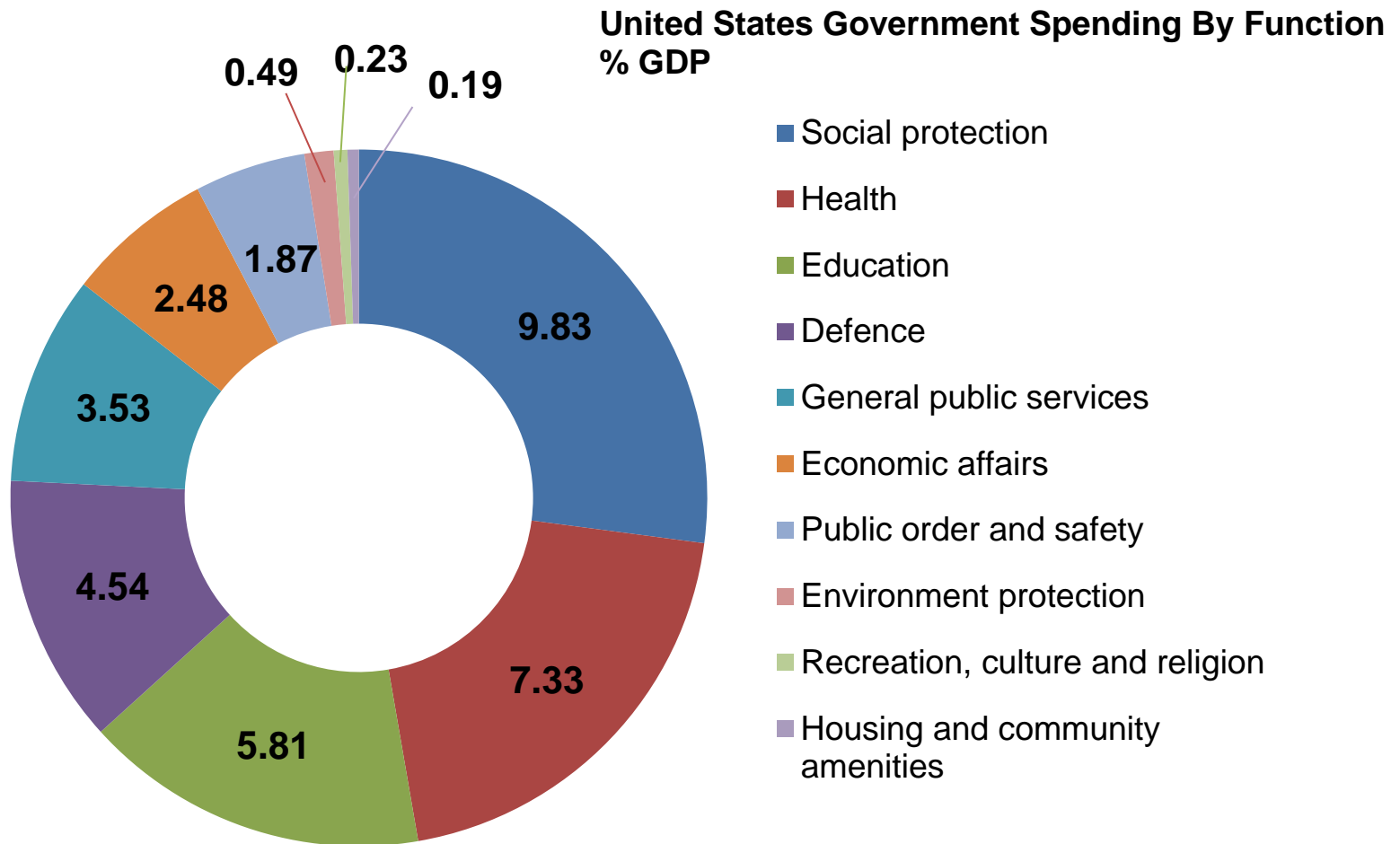
Sybil Risk Score



Country Revenue at Risk, Public & Private Sectors

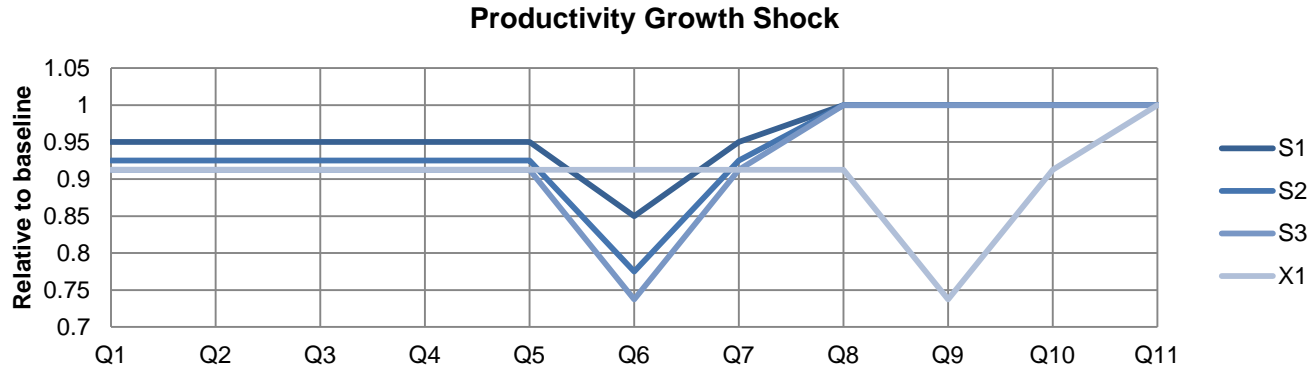


Public Sector: US Gov. Spending By Function

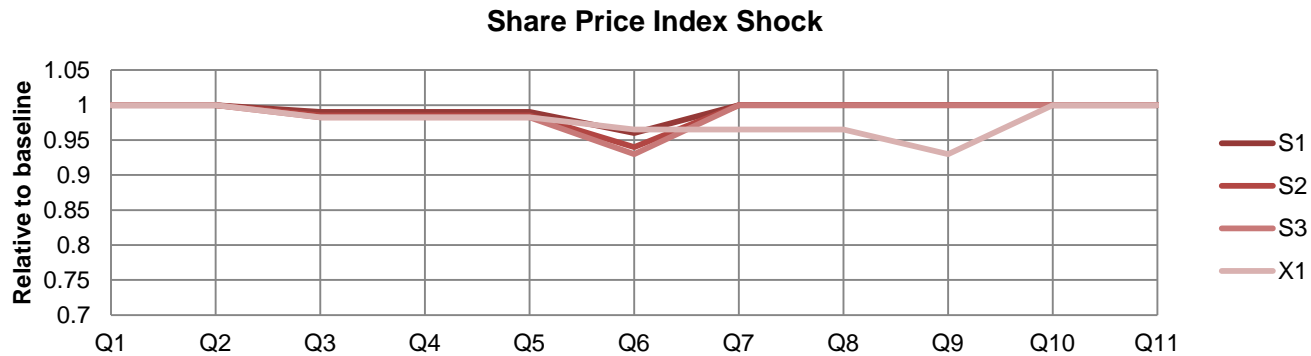


Inputs to Macroeconomic Model

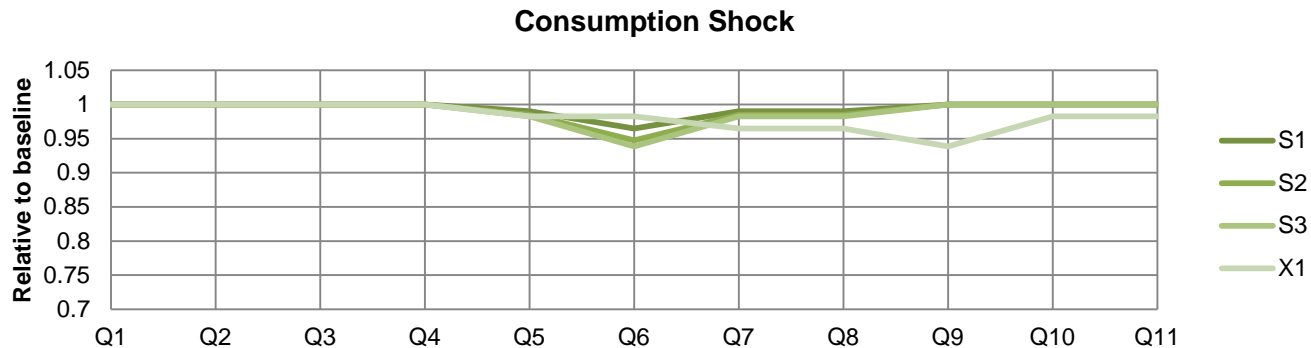
Productivity



Confidence



Consumption



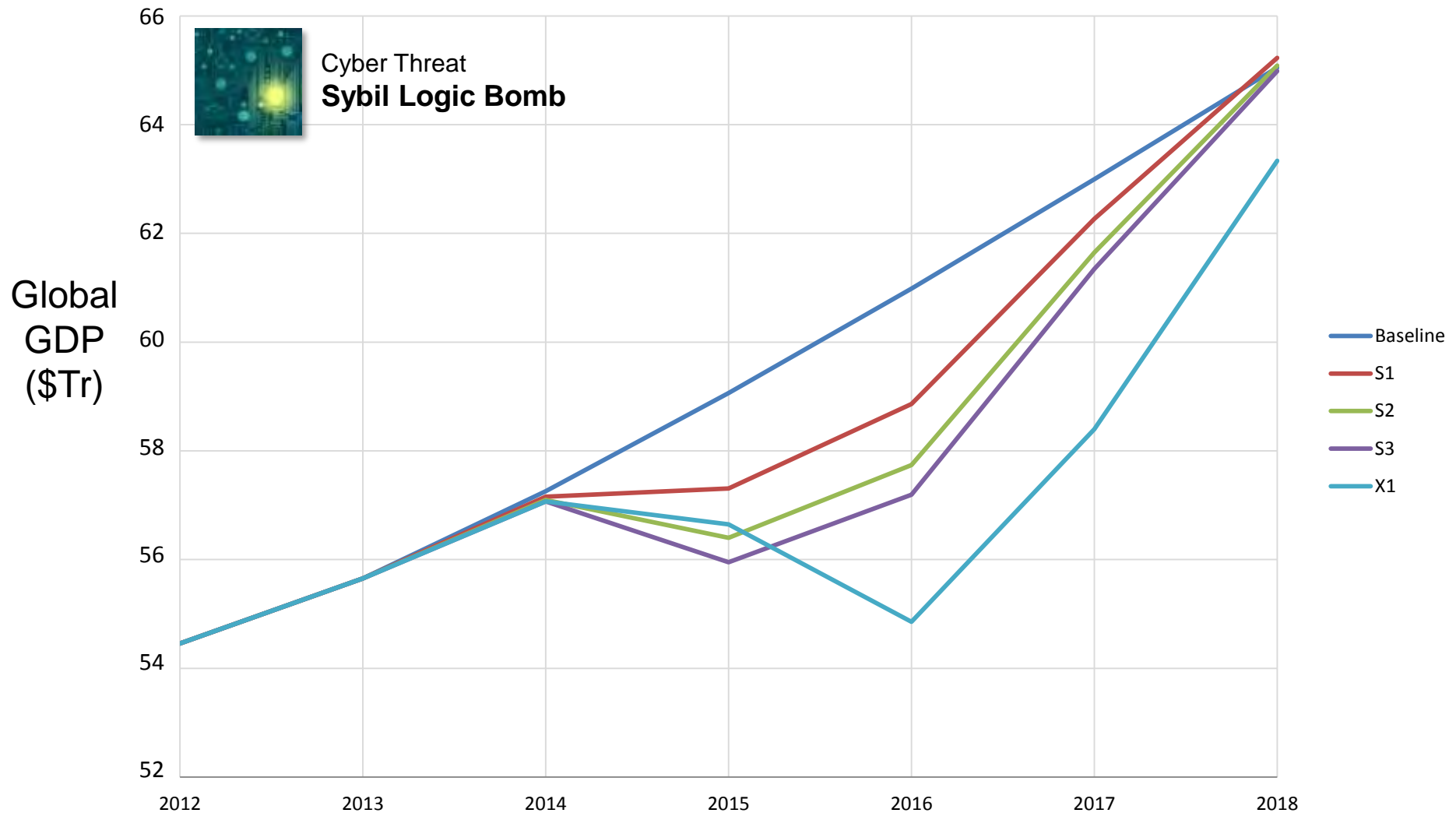
Impact of the Cyber Scenario and Variants

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

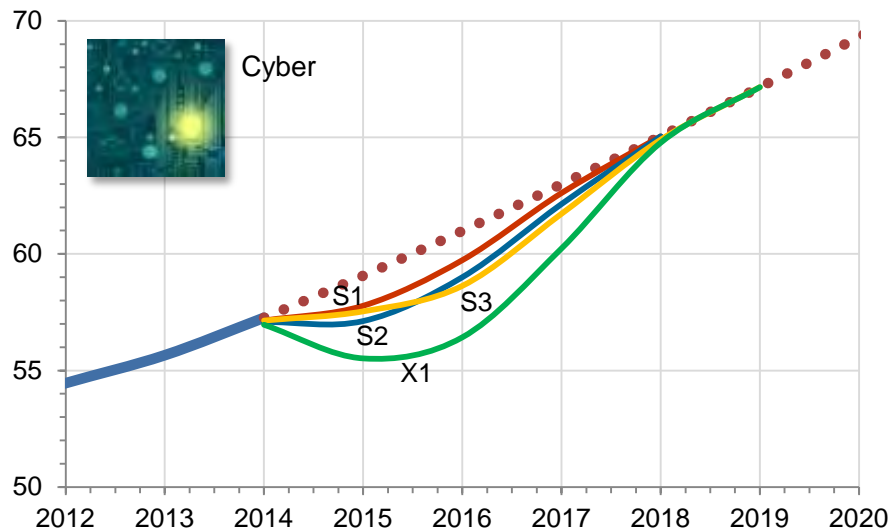
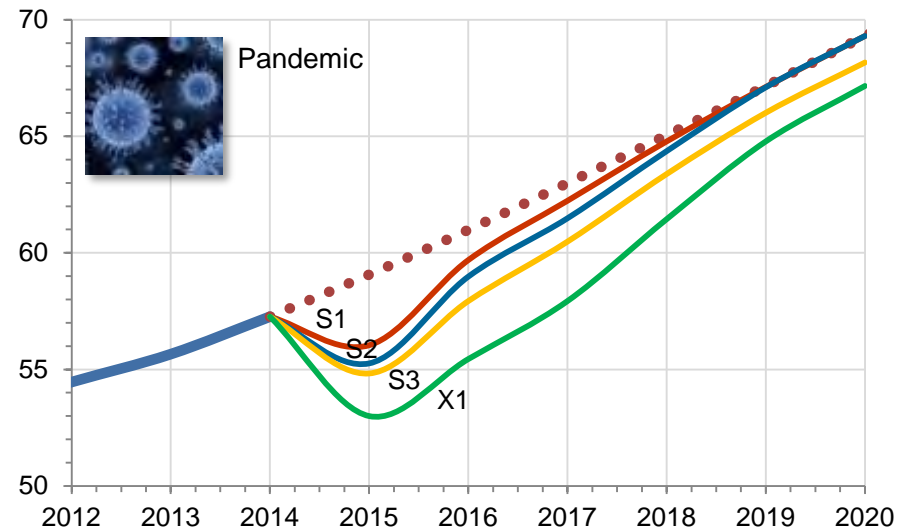
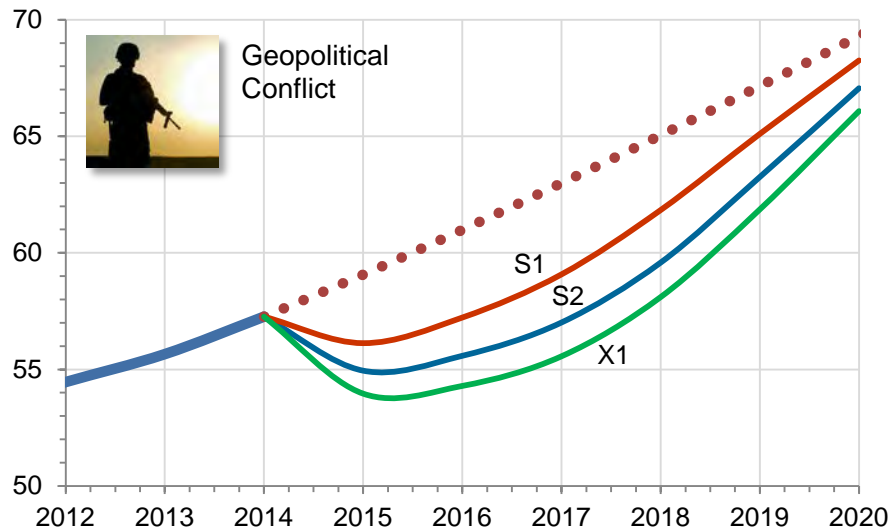


Comparison with other Risk Centre Scenarios

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

Comparison with other Risk Centre Scenarios



Future Stress Test Standards?

					Short Term Maximum Impact at Yr1Q4				Long Term Maximum Impact at Yr4Q4			
					S1	S2	S3	X1	S1	S2	S3	X1
US												
	Bonds Short	TSY 2Y	US Treasury 2 year	%	-0.06	-0.07	-0.07	-0.07	-0.07	-0.47	-0.71	-4.1
	Bonds Long	TSY 10Y	US Treasury 10 year	%	-0.09	-0.1	-0.1	-0.1	0.005	-0.4	-0.7	-4.3
	Equities	DJIA	Dow Jones	1970=830.3	-3.0	-3.1	-3.2	-3.2	-27.0	-35.3	-39.1	-51.6
	Credit	USA CSPA	Credit spreads, period average	%	0.03	0.03	0.04	0.04	0.01	-0.02	-0.05	-0.04
	Inflation	USA CPI	Consumer Price Index, US	1982/84=100	-1.7	-2.6	-3.0	-3.0	-15.5	-22.8	-26.4	-33.4
UK												
	Bonds Short	GBP 2Y	2 year UK govt	%	-0.33	-0.35	-0.35	-0.35	-0.2	-0.4	-0.46	-1.6
	Bonds Long	GBP 10Y	10 year UK govt	%	-0.28	-0.31	-0.32	-0.32	-0.1	-0.4	-0.5	-1.9
	Equities	FTSE100	FTSE 100	1962=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
	Inflation	GBP CPI	Consumer Price Index, UK	2005=100	-1.8	-2.7	-3.2	-3.2	-8.0	-12.4	-14.7	-21.4
	Foreign Exchange	USD/GBP	Exchange rate (US\$ per GBP)	Level values	-1.13	-1.09	-1.07	-1.07	-4.7	-6.5	-7.0	3.0
EU (Germany)												
	Bonds Short	DEM 2Y	2 year German govt	%	-0.08	-0.06	-0.06	-0.06	-0.6	-1.2	-1.5	-2.8
	Bonds Long	DEM10Y	10 year German govt	%	-0.08	-0.07	-0.06	-0.06	-0.4	-0.97	-1.2	-2.9
	Equities	DAX	Share Price index DAX	1987=1000	-1.5	-2.7	-3.3	-3.3	-28.4	-39.3	-44.2	-55.0
	Credit	DEM CSPA	Credit spreads, period average	%	0.03	0.05	0.06	0.06	0.13	0.17	0.19	0.23
	Inflation	DEM CPI	Consumer Price Index, Germany	2010=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)	Level values	-0.7	-0.7	-0.7	-0.7	-2.2	-3.2	-3.5	1.7
Japan												
	Bonds Short	JPY 2Y	2 year Japan govt	%	-0.04	-0.03	-0.02	-0.02	0.08	-0.09	-0.17	-2.0
	Bonds Long	JPY 10Y	10 year Japan govt	%	-0.06	-0.05	-0.04	-0.04	0.12	-0.09	-0.19	-2.1
	Equities	NIKKEI	Share Price Index Nikkei	1968=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	0	0	0	0	0	0	0
	Inflation	JPY CPI	Consumer Price Index, Japan	2010=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)	Level values	0.14	0.15	0.15	0.15	-1.0	-1.3	-1.3	0.2

Conclusion: Diversify IT Platforms

Outcomes of Scenario

- Compromise of a Strategically 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

Centre for **Risk Studies**



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Simon Ruffle

Director of Technology Research and Innovation

s.ruffle@jbs.cam.ac.uk