Emerging Risks Scenarios for Risk Management

Cambridge Centre for Risk Studies Seminar 20 March 2014

Scenario 2 - A Cyber Catastrophe

The Sybil Logic Bomb

Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

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

Bloomberg Our Company | Professional | Anywhere

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE

Hackers in China Compromise U

Defense Department contractor QinetiQ was infiltrated by hac
The company makes defense systems such as spy satellites a

GRAPHIC: MICHAEL RILEY / BLOOMBERG NEWS, ALEX TRIBOU / BLO

A history of hacking at QinetiQ — Period of reported succes

2007 D — Dec. 4, 2007
2008 J
F
M
A

QinetiQ North America, QNA, is informed by Naval Criminal Inve resulting in the loss of a "large quantity of sensitive information." intelligence sources have linked to China's People's Liberation A

The Telegraph

Home News World Sport Finance Comment Blogs Culture Travel Life Women

Technology News | Technology Companies | Technology Reviews | Video Games | Technology

HOME » TECHNOLOGY » TECHNOLOGY NEWS

Barack Obama 'ordered Stuxnet cyber attack on Iran'

President Barack Obama ordered the Stuxnet attack on Iran as part of a wave of cyber sabotage and espionage against the would-be nuclear power, according to a new book citing senior Washington sources.

BBC Sign in | News | Sport | Weather | iPlayer | TV

NEWS US & CANADA

Home World UK England N. Ireland Scotland Wales Business Politics Health Education Sci/Envi

Africa Asia Europe Latin America Middle East US & Canada

10 May 2013 Last updated at 00:53

Cybercriminals 'drained ATMs' in $45m world bank heist

A gang of cybercriminals stole $45m (£29m) 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 stretched across 26 countries.

An eighth suspect is thought to have been murdered in April.

The network used fake cards to target banks in the United Arab Emirates and Oman, court documents said.

Anonymous Message To Greek Gov For Ert

0:23 / 2:01

Sign In | Help — Make Y! My Homepage

! NEWS — Search

ORLD BUSINESS ENTERTAINMENT SPORTS TECH POLITICS SCIEN

News Search — Videos Photos Just Explain It Katie's Take Weather The Up

fear cyber attack more than euro crisis: lane

euters – Wed, Jun 12, 2013

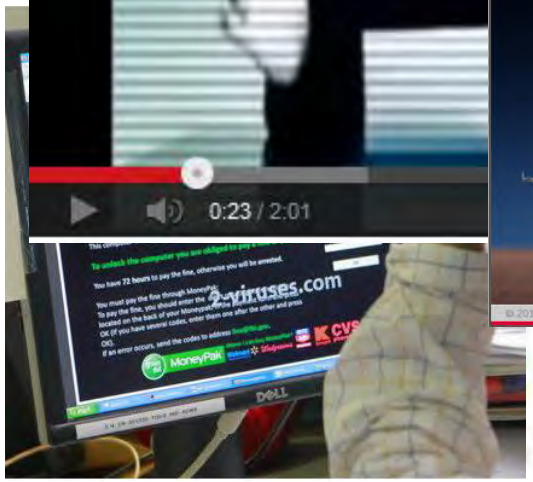
17 Tweet 64 Share 3 +1 0 Print

Reuters - A bus passes the Bank of England in the City of London February 23, 2013. REUTERS/Neil Hall

ON (Reuters) - Worries over hacking and other cyber attacks has pushed aside the euro zone s the top risk for Britain's banks and they must do more to protect themselves, a senior Bank and official said on Wednesday.

cyber crime in the financial sector has become a more pressing worry, underlined by a series s this year.

osecutors last month laid out details of a crime ring they say stole $45 million from two



House and Barack Obama is injured

Reply Retweet Favorite Buffer More

3,242 RETWEETS 153 FAVORITES

12:07 PM - 23 Apr 13

Macro-economic View of Cyber Catastrophe

Subject Matter Specialists

Cyber Catastrophe Risk

Éireann Leverett

Security Researcher, IOActive

Works in the Industrial Systems Security team at IOActive, Studied Advanced Computer Science in Cambridge's computer security group. Specialises in industrial system security incidents and cyber risk management in the corporate sector.

Dr. Rob Watson

Security Research Group, University of Cambridge Computer Laboratory

University Lecturer in Systems, Security, and Architecture in the Security Research Group at the University of Cambridge Computer Laboratory. Specialist in operating system security extensibility.

Dr. Richard Clayton

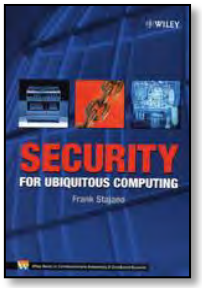
Security Research Group, University of Cambridge Computer Laboratory

Software developer who specialises in digital crime, with research into email spam, fake bank "phishing" websites, and other Internet wickedness. As an expert in these areas, he is a regular speaker and media commentator.

Dr. Frank Stajano

Senior Lecturer, University of Cambridge Computer Laboratory

Specialist in systems security with particular interest in the human aspects of systems security. Frank is the author of the book *Security for Ubiquitous Computing*.



Cyber Event Catalogue

		Theft	Disruption	Damage
ILOVEYOU	2000			■
MafiaBoy	2000			■
Code Red	2001			■
SQL Slammer	2003			■
MyDoom	2004		■	
Sasser	2004		■	
Titan Rain	2004	■		
TJX	2005	■		
APT1	2006	■		
Conficker	2007		■	
Zeus	2007	■		
Estonian Cyber attack	2007		■	
Heartland	2008	■		
RBS WorldPay	2008	■		
Stuxnet	2010			■
Operation Aurora	2010	■		
Epsilon	2011	■		
Sony Playstation	2011	■		
Citigroup	2011	■		
RSA	2011	■		
Operation Ababil	2012		■	
Shamoon	2012			■
Flame / Skywiper	2012	■		
The Unlimited Operation	2012	■		
CloudFlare	2013		■	
ObamaTwitter Scare	2013		■	

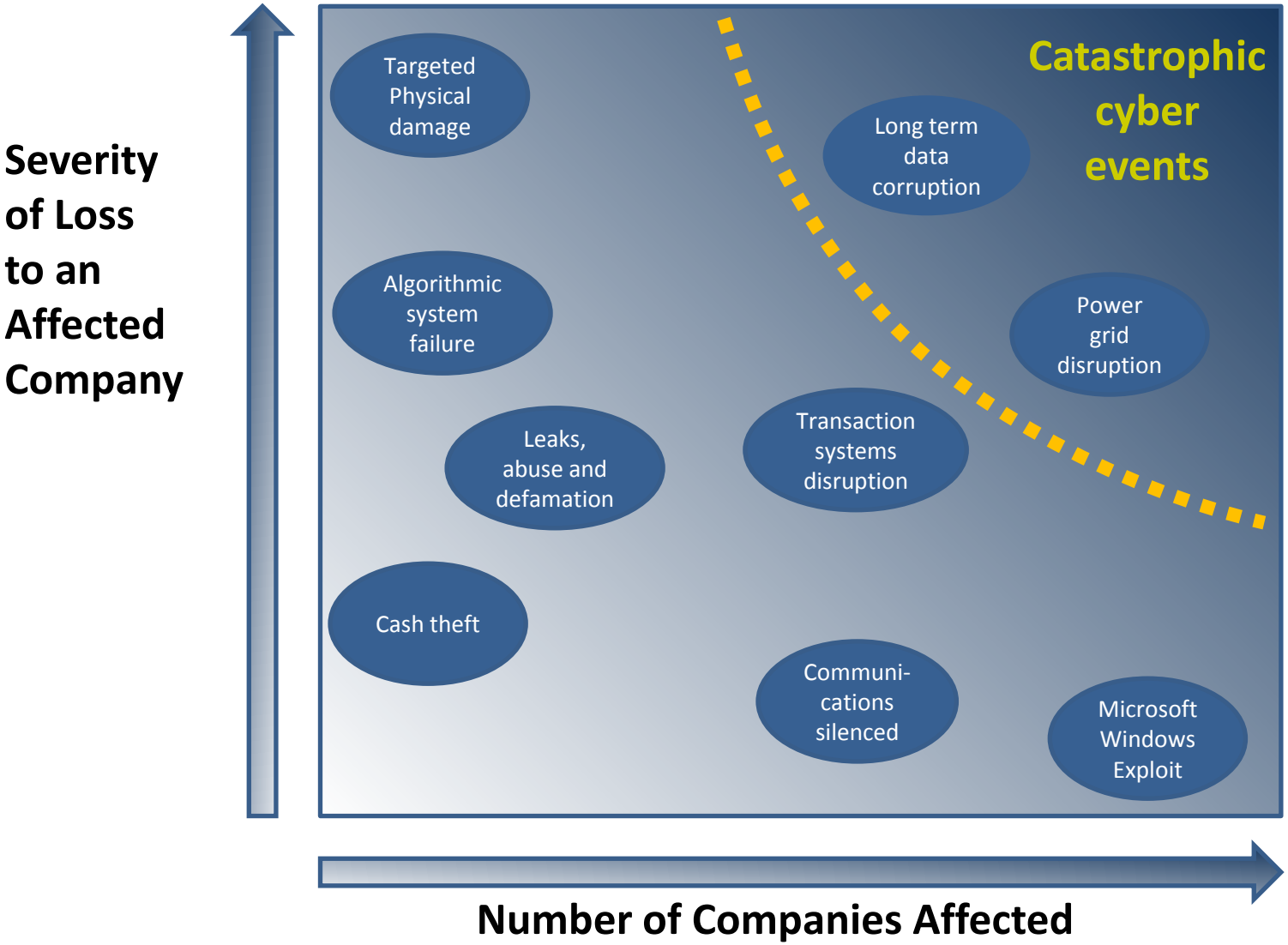
Taxonomy of Cyber Catastrophe Scenarios

*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



Cyber Catastrophe Risk

“The Sybil Logic Bomb”: Scenario Definition

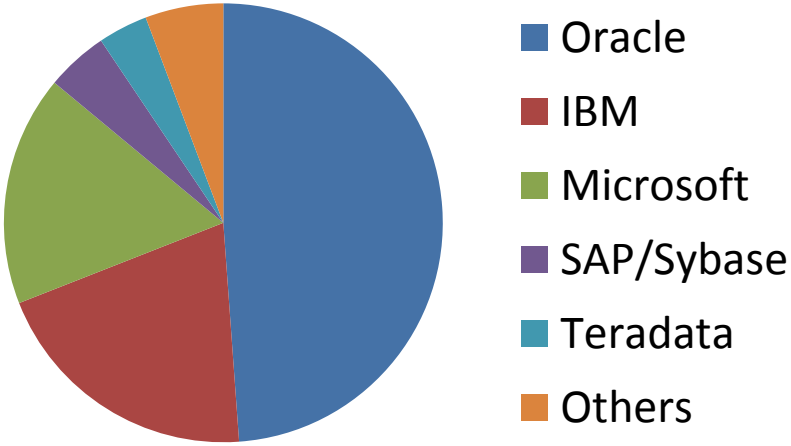
Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

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

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 based on Oracle. We use Oracle to characterise Sybil.

Key Features of Scenario

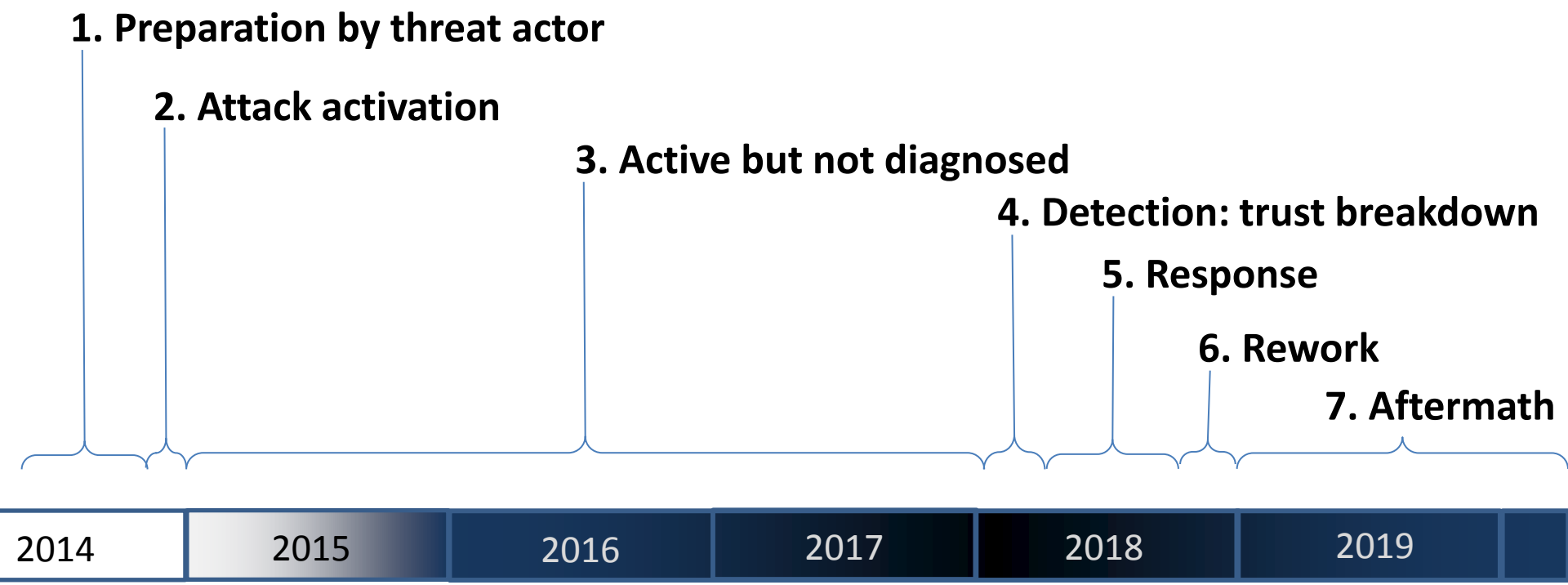
- Slow burn: over months, years
- Small errors difficult to spot
- Small errors can cause big problems
- Backups corrupted
- Difficult to replicate
- Affects algorithms not transactions

Magnitude Scale Value
Magnitude **4** Cyber Hazard

~~*Transaction processing*~~
- ~~Payroll~~
- ~~Airline ticketing~~
- ~~Retail bank accounts~~
- ~~Credit card payments~~

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

Scenario Phases



Phase 1 – Preparation and Research

- Disgruntled employee of Sybil writes deliberate piece of malware code – a ‘logic bomb’.
- The logic bomb corrupts the ‘floating point computation’ (or similar) to produce a low number of errors, randomly, in ways that are difficult to replicate.

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
    OSStatus        err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

Phase 2 – Attack Activation

CASSANDRA.com

Sign up | Log in

Tech News | TV & Video | International | Business | Sport | Entertainment

Sybil Releases Database Upgrade

Version 11.6 release majors on Big Data

February 20th

REDWOOD SHORES, CA (Reuters) – Today Sybil Inc., (NASDAQ:SYBL) releases their much awaited release 11.6 of their flagship RDBMS with over 1000 new features including tools for Big Data.

Sybil forms the basis of many corporate IT systems including those involved in high speed algorithmic stock trading, industrial and utility control systems, corporate reporting and financial analysis.

Corporate customers have been waiting two years for this release which places Sybil well ahead of its nearest rivals

Installation of the new upgrade is expected to take place over the next 18 months.

Phase 3: Active but not Diagnosed (Latency Period)

CASSANDRA.com

Sign up | Log in

Tech News | TV & Video | International | Business | Sport | Entertainment

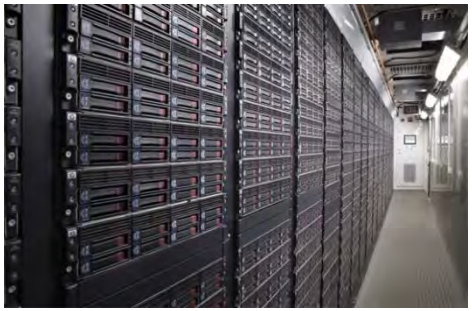
Are recent tech meltdowns due to faulty servers?

IT departments shun major manufacturer of enterprise hardware

September 20

A series of unexplained IT failures in the past year may be explained by faults in Elliott's range of Enterprise LocalCloud servers.

A survey of IT managers in Fortune 500 companies confirmed that they are steering clear of these servers after rumours they have been involved in a number of high profile IT meltdowns in the past year.



Could hardware be to blame for recent mystery stock market fluctuations?

A spokeswoman denied that their servers were at fault. Elliott's stock price was trading 15% lower today.

Fictional Algorithmic IT Failures Caused by Logic Bomb

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

Algorithmic Trading Losses

CASSANDRA.com

Sign up | Log in

Business Headline | TV & Video | International | Business | Sport | Entertainment

Trading glitch cost £440 Million

£10 million lost per minute

February 20th

The Standard 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.

Spokesperson Kara Fitzwilliams acknowledged that "a technology issue" occurred in its market-making unit that affected how shares for some 150 stocks were routed.

Technical commentators described the loss making trades as 'bizarre' saying that Standard Capital's high speed trading algorithm was one of the most respected in the market.

Shares of Standard Capital closed down 20 percent on Thursday.

Precedent: Knight Capital

Knight's bizarre trades rattle markets

CNNMoney

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

Recommend 66 Tweet 23 Share +1 2 Email Print

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

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

Environmental Damage Leads to Liability Claims and Fines

CASSANDRA.com

Sign up Log in

Tech News | TV & Video | International | Business | Sport | Entertainment

UK Utilities fined again for pollution

IT control system to blame

February 20th

UK Utilities Group faces another big fine after raw sewage leaked into local rivers.

A proposed order follows a recent string of nearly two dozen sewage spills that could cost customers £15,000. UK Utilities again blame faulty IT controls systems for opening valves that cause the spills

"The kids, the environment, that's what worries me the most," said Ashley McAllister who lives near Panther Creek.

Yet another environmental disaster for trouble-prone UK Utilities Group

Four leaks since last October have sent thousands of gallons of sewage into the same river. The latest one in April was upstream of several neighbourhoods and a playground.

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 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

Track
Like 17
Tweet 1
Share 0
Share
Submit
reddit this!

Simplify data access, analysis and reporting with Toad Data Point.
Download Trial
DELL Software

Typical SCADA controlled sewage system

Bad Data Leads to Write-down

CASSANDRA.com

Sign up Log in

Business Headline | TV & Video | International | Business | Sport | Entertainment

Bad data leads to write-down

Glitch caused $1.75 Billion write-down for UK bank

September 20th

London, UK (Bloomberg) – Today Albion Bank booked a write-down associated with a US-based lender totalling $1.75 billion.

A spokesman said a software glitch had caused bad underlying data to be fed to two computer models causing a difference between net and gross interest rate calculations which had gone unnoticed for two years.

Albion had acquired the US-based lender in 2009 and had integrated their IT systems.

For two years the difference between the net and gross interest rate calculations in two computer models went unnoticed.

Shareholders are attempting to sue Albion in the United States for securities fraud

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

FACEBOOK
TWITTER
GOOGLE+
EMAIL
SHARE
PRINT
REPRINTS

THE GRAND BUDAPEST HOTEL

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

Calibration Points: Revenues at Risk

Company	Date	IT Failure	Total Loss US$ millions	Total Annual Revenue US$ millions	% RAR
Knight Capital	2012	Algorithmic trading loss	440	1,156	**38%**
Maroochy Shire County Council	2000	Environmental Damage Leads to Liability Claims and Fines	1.3	22	**6%**
National Australia Bank	2001	Bad Data Leads to Write-down	2,000	7,000	**29%**

Phase 4: Detection: Start of Trust Breakdown

CASSANDRA.com

Sign up Log in

Business Headline | TV & Video | International | Business | Sport | Entertainment

Was Sybil to blame for Toyota recalls?

Industry experts are blaming Sybil for the 20 million Toyota recalls in the past two years

February 20th

Torrance, Calif., (Reuters) – Toyota Motor Sales, U.S.A., Inc., denied it is investigating whether the Sybil Logic Bomb was the cause of software failures behind their recent product recall of 960,000 Prius, RAV4, Tacoma and Lexus Vehicles

Toyota's latest announcement puts the number of recalls over the past two years at nearly 20 million. That is far more than the number it called back in 2009 and 2010 - widely seen as the worst years for its reputation.

The recent fault caused the Vehicle Stability Control, Anti-lock Brake, and Traction Control functions to intermittently turn off

In rare circumstances, the hybrid system might shut down while the vehicle is being driven, resulting in the loss of power. A spokesman from Sybil Inc was unavailable for comment.

Phase 5: Response to Contain the Attack

CASSANDRA.com

Sign up | Log in

Tech News | TV & Video | International | Business | Sport | Entertainment

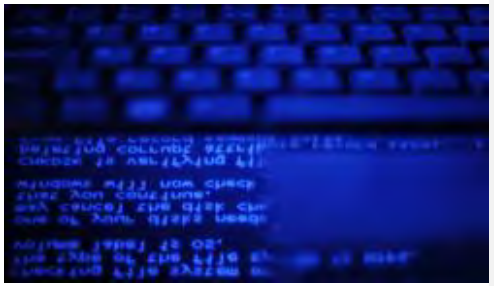
Sybil Releases software update to fix floating point vulnerability

Emergency software update repairs vulnerability that introduced random errors

February 20

REDWOOD HILLS, CA (Reuters) – Today Sybil Inc., (NASDAQ:SYBL). released an emergency software update today to fix a security vulnerability in its RDBMS software that was introducing random floating point errors.

A Sybil spokeswoman said only a small number of customers were affected by the vulnerability.



Could this vulnerability explain recent mystery stock market fluctuations?

Customers most likely affected are in the financial services and utilities sectors, she added. Sybil stock price has dropped 4%.

Phase 6: Rework

TOP CLASS ACTIONS
Connecting Consumers to Settlements, Lawsuits and Attorneys

The Volvo V40 R-Design
Fully maintained from £299 a month*
Find out more

Home | News | Class Action Settlements | Class Action Investigations | Attorneys | About | START A CLASS ACTION

AvMed Health Data Breach Class Action Lawsuit Settlement

By Saren Pierce
December 3, 2013

Add to Favorites | Tweet 1 | Like 3

AvMed Inc. has agreed to settle a class action lawsuit over allegations that it failed to adequately secure and protect customers' sensitive personal data. If you paid for or received health insurance from AvMed Inc. at any time through December 2009, you may be eligible for compensation. The AvMed health data breach settlement will resolve a class action lawsuit (Curry v. AvMed Inc.) that alleges unsecured laptops containing the sensitive personal information of AvMed customers were stolen while in AvMed's custody, putting the customers at risk of identity theft. AvMed denies all allegations but has agreed to a class action settlement, which was preliminarily approved on Oct. 25, 2013.

Who's Eligible

Class Members of the AvMed health data breach class action settlement include all current and former AvMed customers who, prior to December 2009, paid AvMed for Insurance and whose sensitive personal information was contained on the laptops that were stolen in December 2009.

Potential Award

Up to $30

Proof of Purchase

Serial number of device (or other identifying information)

Claim Form

CLICK HERE TO FILE A CLAIM »

POPULAR SETTLEMENTS

- Suave Keratin Infusion Smoothing Kit Class Action Settlement 16,967 views
- Emergen-C Class Action Lawsuit Settlement 14,961 views
- Popchips Snack Products Class Action Lawsuit Settlement 14,247 views
- Bank of America TCPA Class Action Settlement 13,989 views
- Duracell Ultra Batteries Class Action Lawsuit Settlement 10,850 views

START A CLASS ACTION LAWSUIT

Do you want to start a class action?

If you think you have a case for a possible class action lawsuit, get started today!

START A CLASS ACTION

ACTIVE INVESTIGATIONS

Liability Analysis: Standard Capital

- £440m in cash losses
- Blamed on faulty software code – developed internally by Standard Capital, based on Sybil database.
- Shareholders sue directors for 40% loss of share value due to poor QA procedures.
- Standard Capital's professional liability insurers take over claim
- They sue Sybil
- Sybil tries to hide behind limited warranty clause
- Political intervention allows claim to proceed
- Sybil seek cover under their own Product Liability insurance

Impact on Pomegranate

Pomegranate

- Pomegranate is a Sybil user
- Their competitor, Hewlett Packard (HP) announce they are certified Sybil-free
- Impacts heavily on Pomegranate as its customers jump ship to HP
- Pomegranate sees 20% stock price fall

CASSANDRA.com

Sign up | Log in

Tech News | TV & Video | International | Business | Sport | Entertainment

HP certifies Sybil-free

HP distances itself from logic bomb

February 20th

Palo Alto , CA – Hewlett Packard (NYSE: HPQ) today distanced itself from trouble prone Sybil Inc by announcing it had been certified as not using Sybil in any of its operations worldwide

"This will give comfort to our customers who can be confident that no Sybil Logic Bomb related issue has affected our company in the past and can continue to do business with us in the knowledge that Sybil products will not be used in the future"

Customers are likely to move to the safety of HP

This is not good news for HP's competitors, notably Pomegranate Inc who are known to make substantial use of Sybil database technology

Phase 7: Aftermath

CASSANDRA.com

Sign up Log in

Business Headline | TV & Video | International | Business | Sport | Entertainment

New laws for software standards after Sybil catastrophe

'This must never happen again' say lawmakers

December 20th

New York – A raft of new legislation was outlined in the business agenda for Congress in the wake of the Sybil logic bomb crisis.

A series of measures was put before lawmakers on Tuesday designed to ensure that the errors that allowed the Sybil logic bomb to occur will never occur again. Software companies will have to put into place exemplary standards of quality control and will no longer be able to waive liability rights

Fitness for purpose clauses in software licences will be removed under new proposed legislation

A software industry spokesman said that there was willingness to engage on these issues but that software developers shouldn't be made a scapegoat for the events that occurred.

Cyber Catastrophe Risk

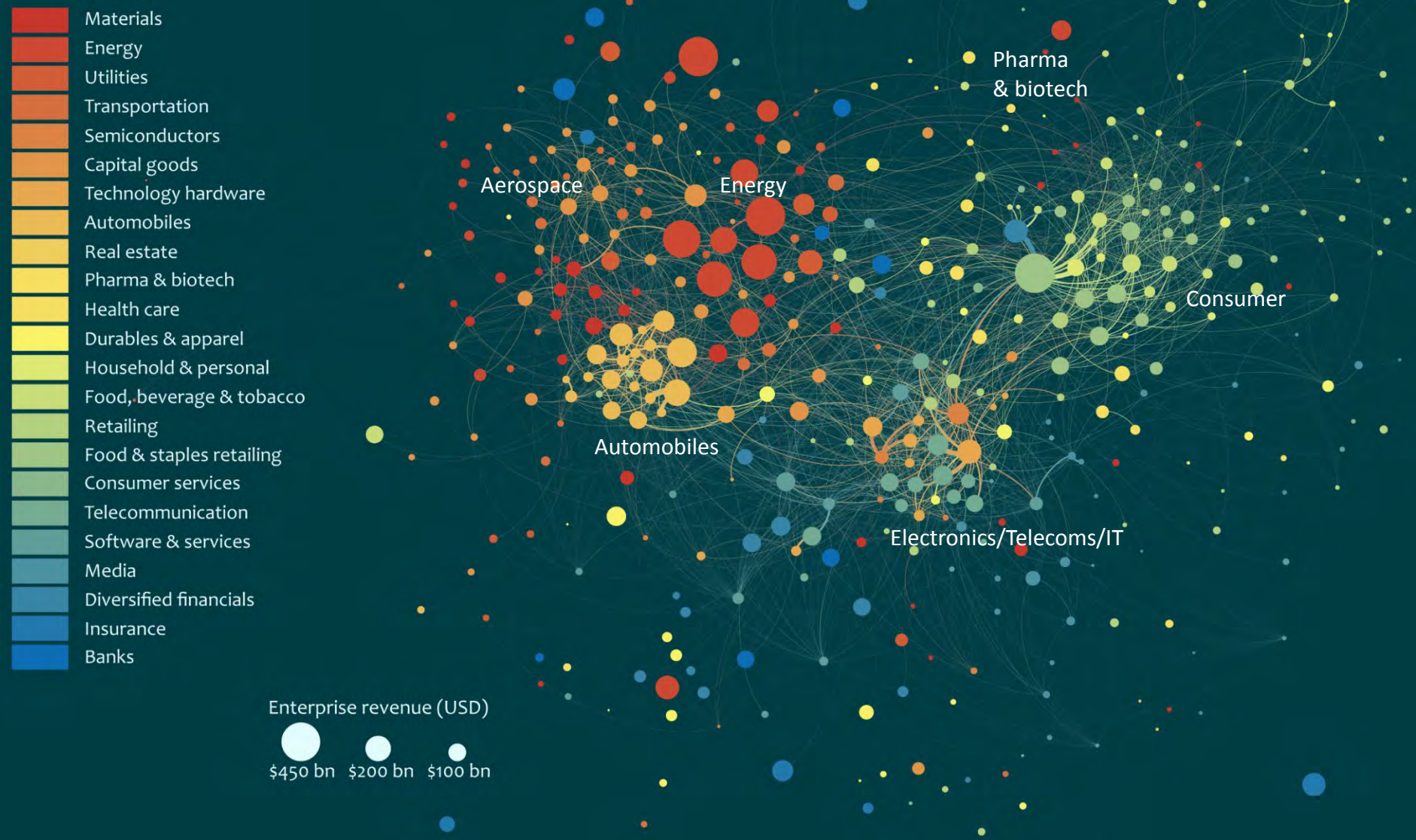
“The Sybil Logic Bomb”: Macro-economic Impact

Centre for
Risk Studies

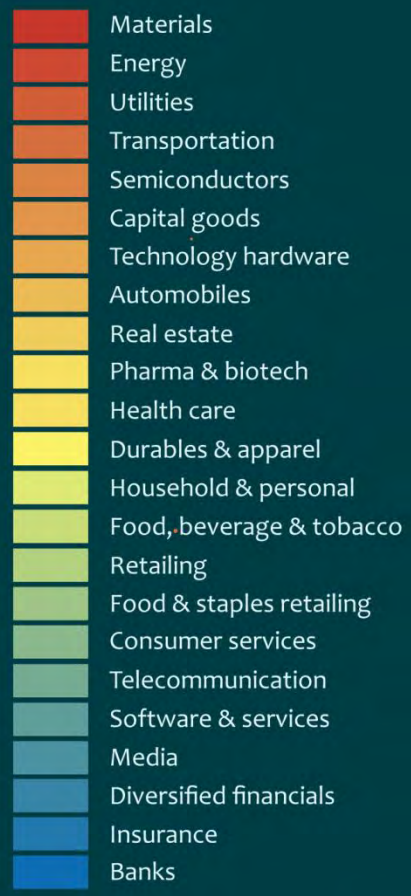
UNIVERSITY OF CAMBRIDGE
Judge Business School

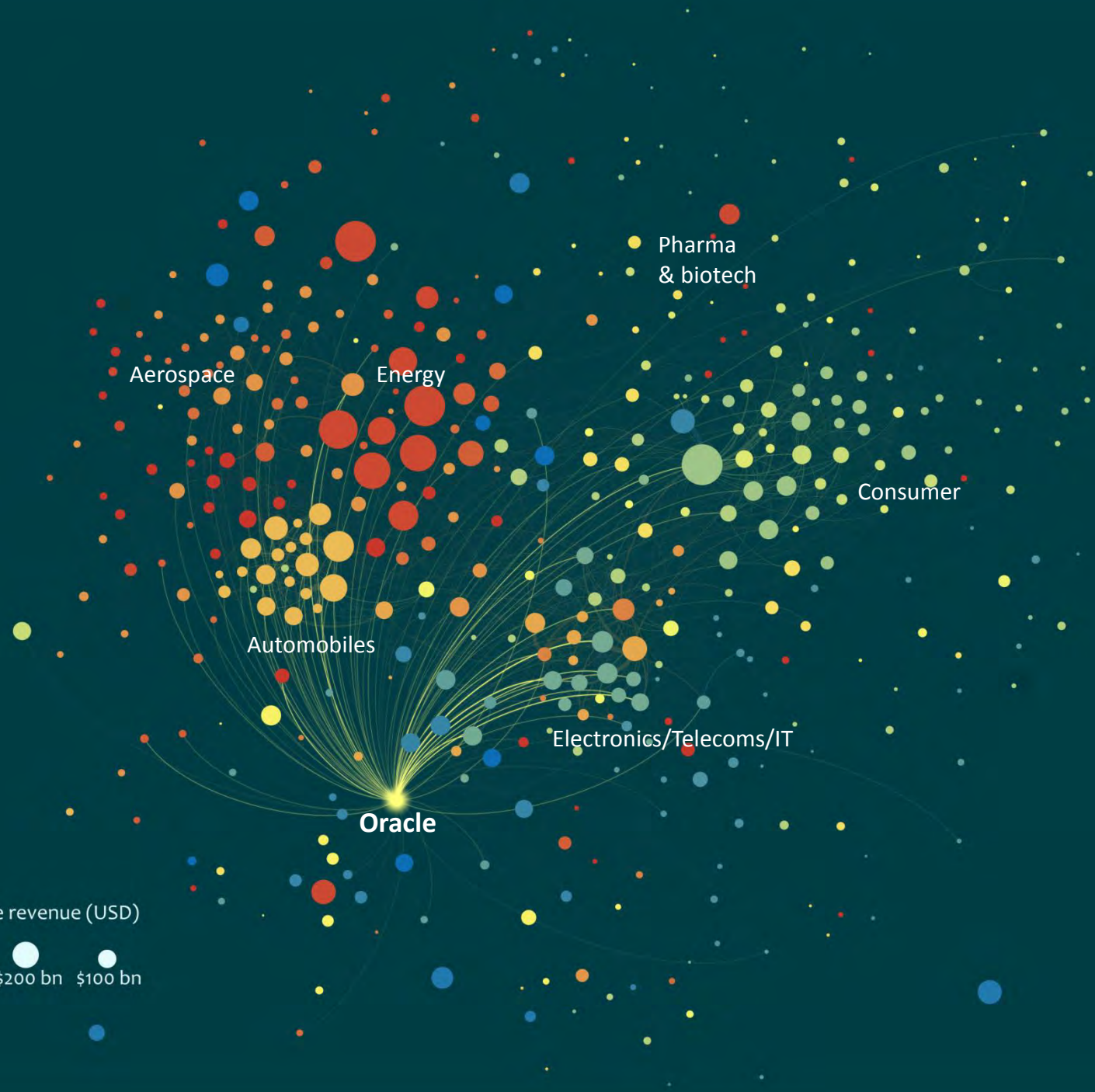
Simon Ruffle
Director of Technology Research and Innovation
Cambridge Centre for Risk Studies

Global Enterprise Network

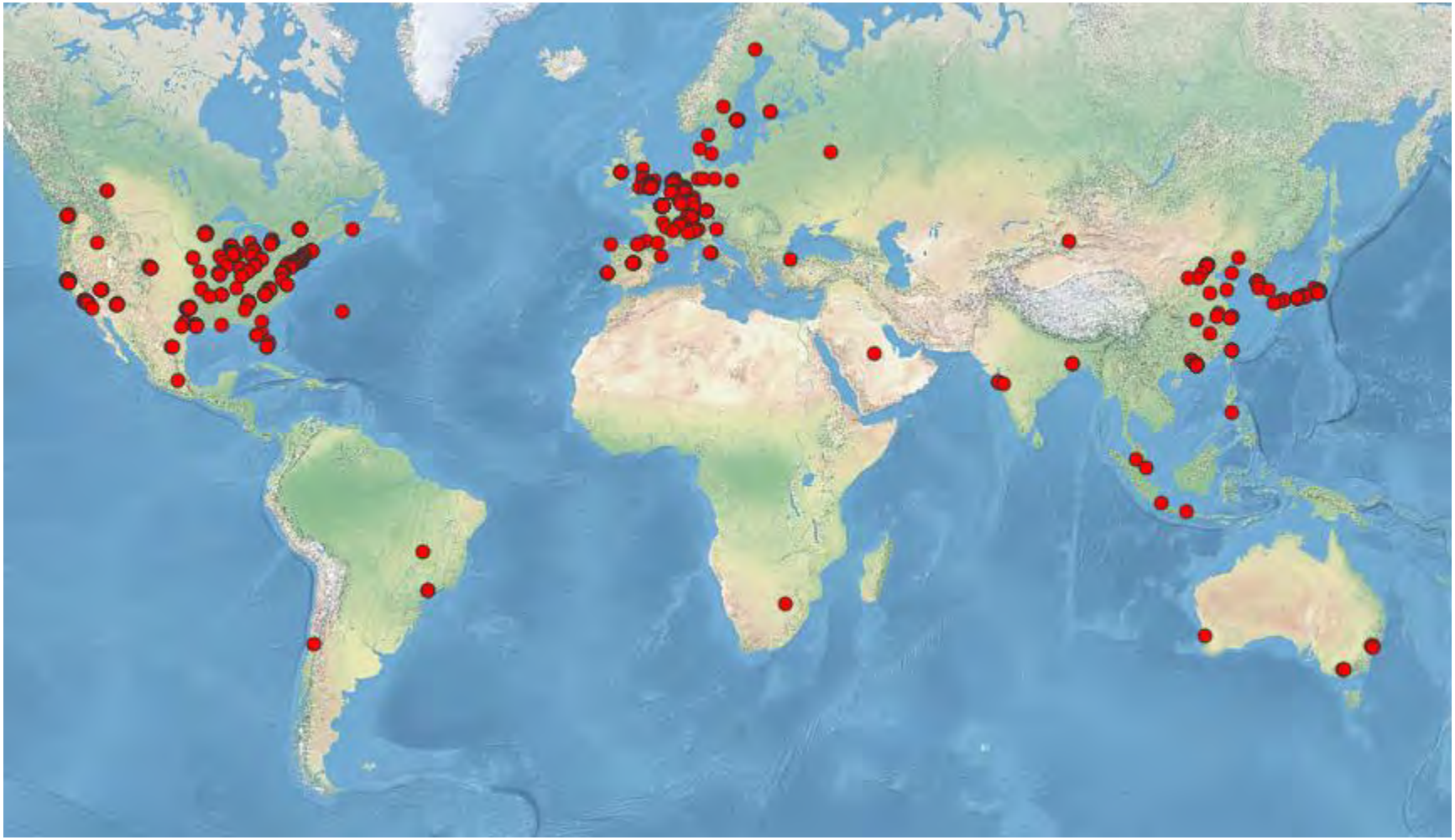


Oracle Market Share = Penetration %





Global Enterprise Network



The 600 enterprises with the location of their corporate HQs mapped

Business Process Criticality

Finance

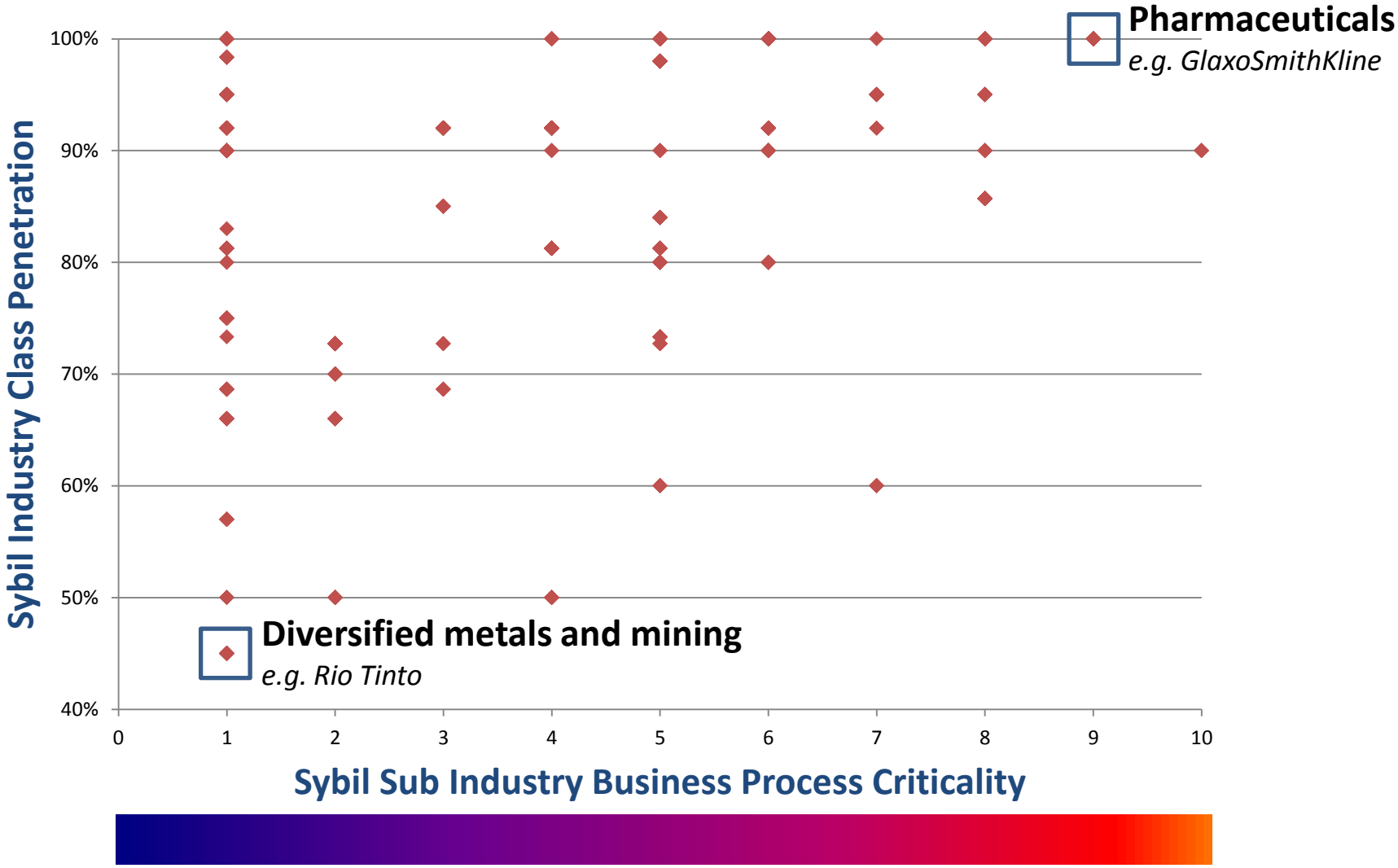
Sales & Marketing & Customer Relations

Admin and Management

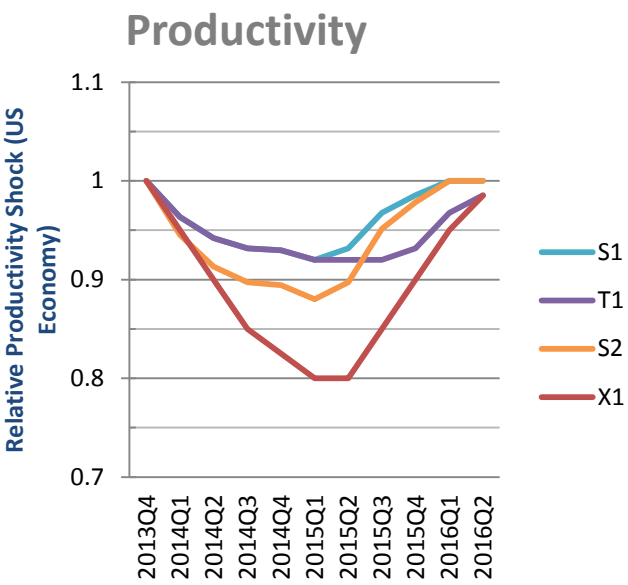
Operations

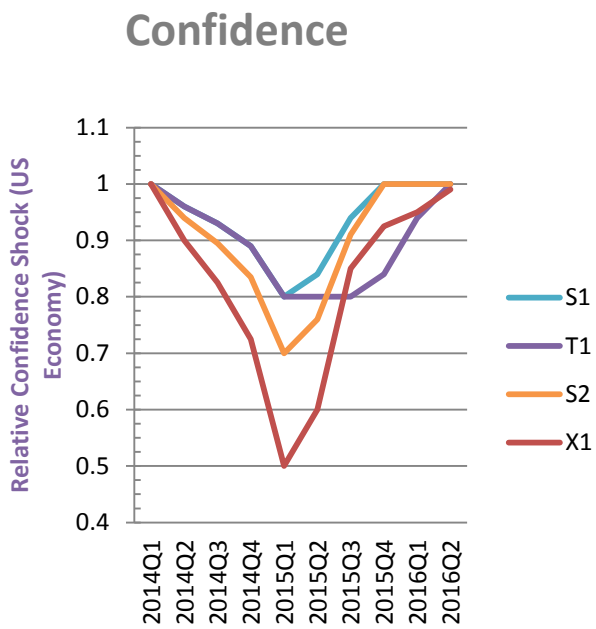
Score	Definition
1	Minor use
2	Used for minor administrative tasks
3	Used for many administrative tasks
4	Used for all main company administration & finance
5	Used for admin, finance and some customer relations
6	Central to customer relations: sales, marketing and billing
7	Used in one but not all core 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

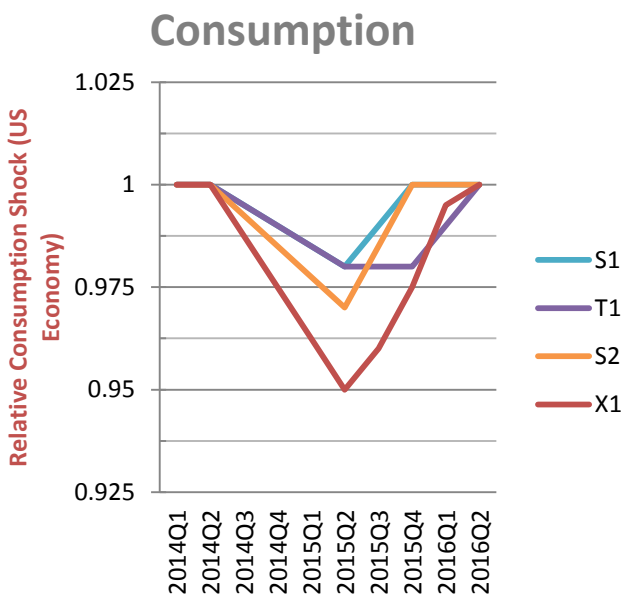
Sybil Risk Score



Inputs to Macro-economic Model







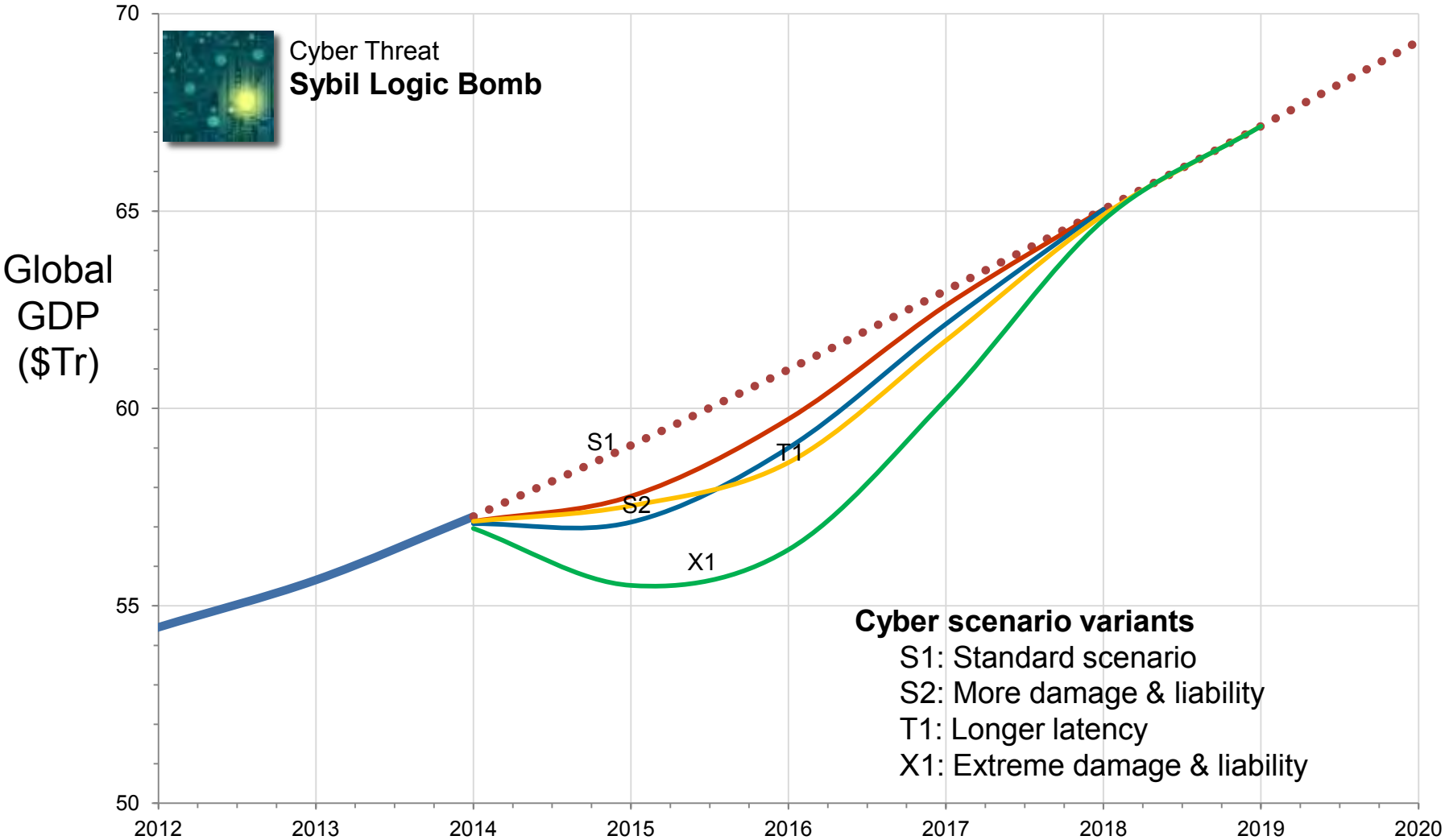
Variant	S1	T1	S2	X1
Harm Scaling Factor	5%	5%	10%	20%
Latency period	5Q	8Q	5Q	5Q

Impact of the Cyber Scenario and Variants

Scenario Variant	Latency period (quarters)	Harm scaling factor	Global 5 year GDP@Risk
S1: Standard Scenario	5	5%	$**3** Trillion
S2: Sybil more damage & liability	5	10%	$**4.5** Trillion
T1: S1 with longer latency	8	5%	$**5** Trillion
X1: Sybil extreme damage & liability	8	20%	$**11** Trillion

Great Financial Crisis at 2014	$20 Trillion

Global GDP Impact of Scenario and Variants



Conclusion: 'Information Malaise'

Outcomes of Scenario

- Compromise of a Strategically Important Technology Enterprise
- Loss of quality and trust
- World Annual 1% GDP@Risk between $3Tr and $11Tr

Implications for Risk Management

- Efficiency drive towards standardisation in corporate IT platforms - contrary to good risk management?
- Revenue at risk can be used for estimating cyber risk
- Have a backup cloud vendor
- Choose your counterparties wisely
- 100% dependency on SITEs is a risk