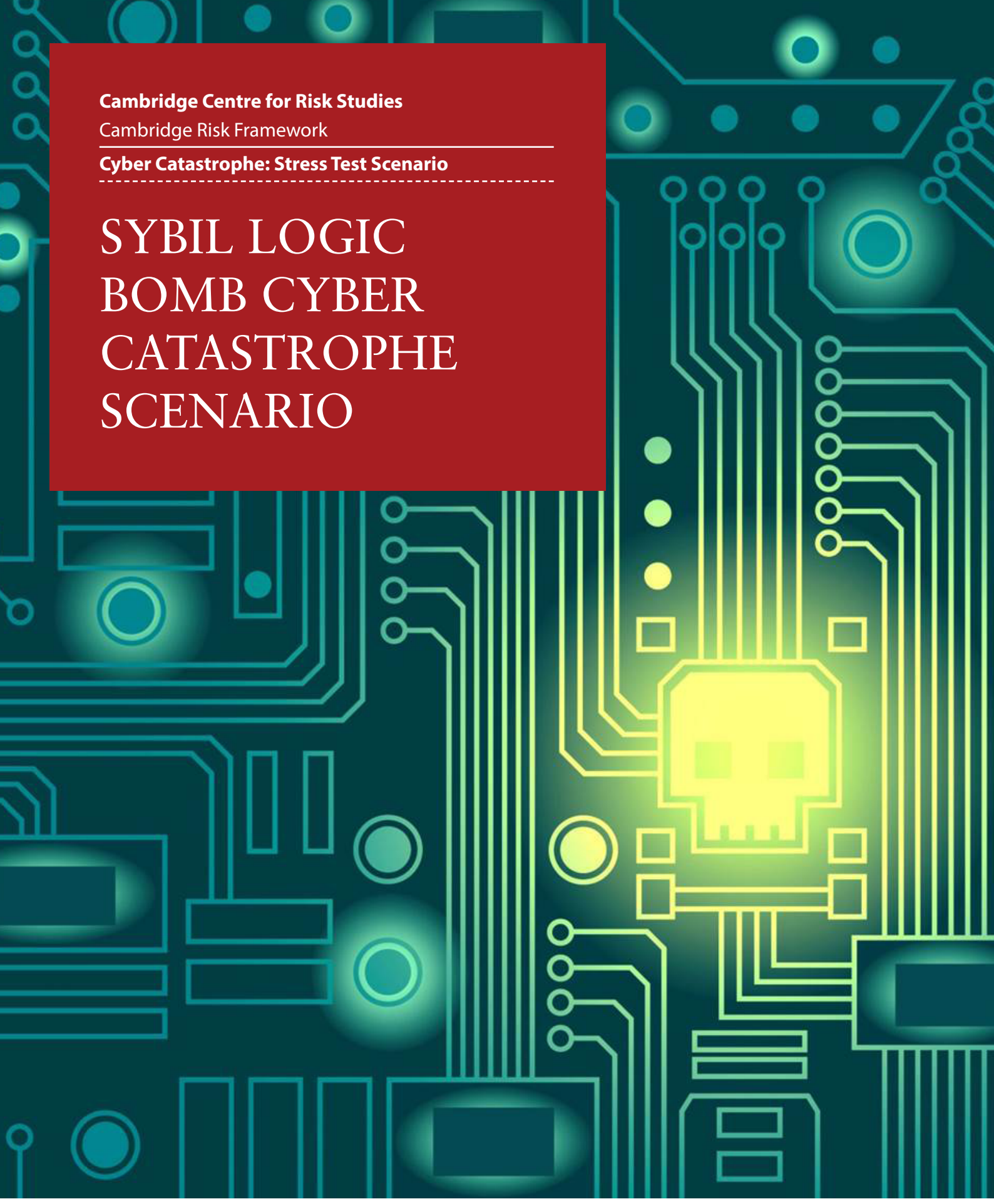


Cambridge Centre for Risk Studies

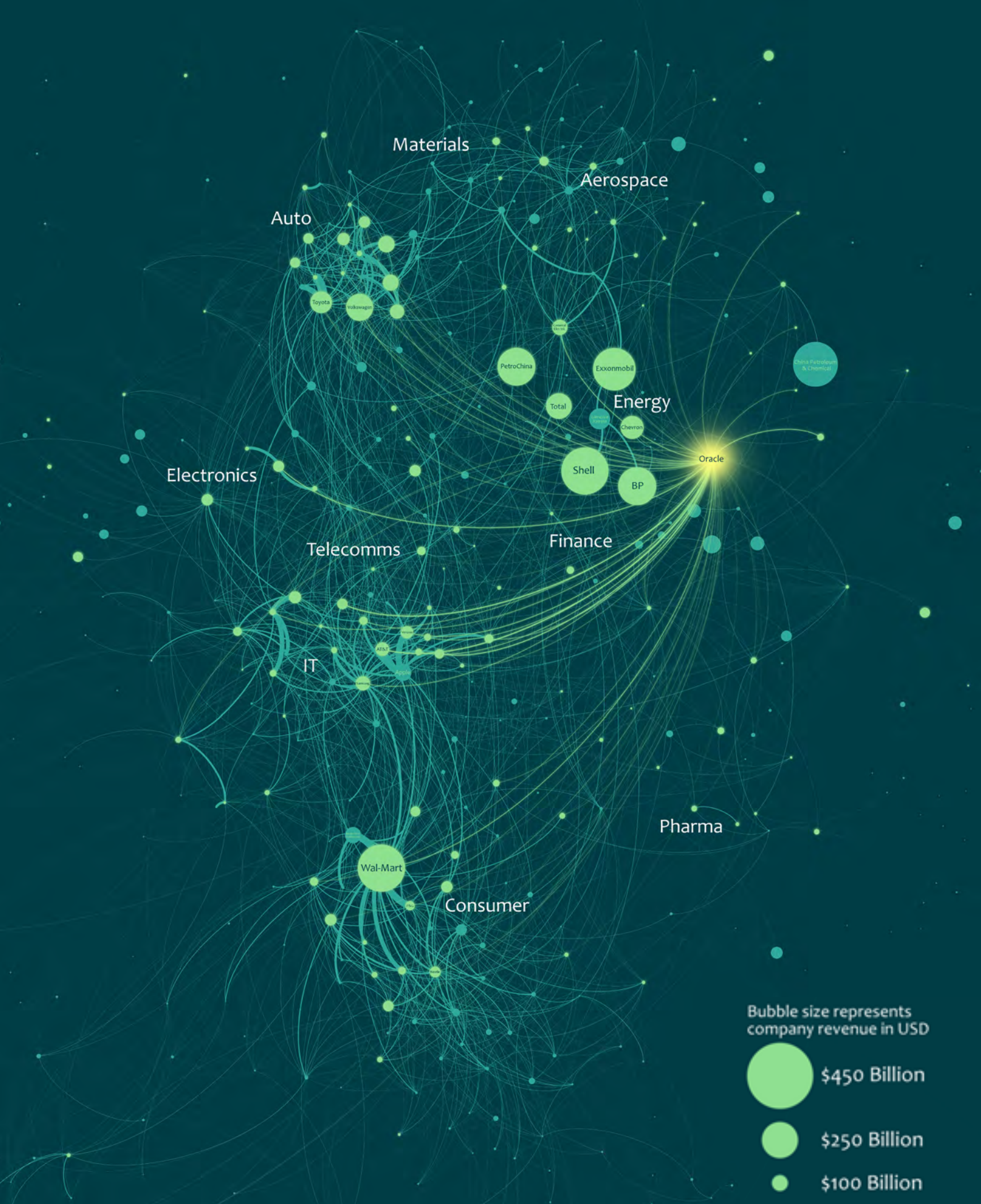
Cambridge Risk Framework

Cyber Catastrophe: Stress Test Scenario

SYBIL LOGIC BOMB CYBER CATASTROPHE SCENARIO

Centre for
Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School



Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Enterprise Network of the Global Economy: Systemic Cyber Threats

The world's largest commercial companies and their trading relationships, showing the systemic linkages through major software providers, using Oracle as an example.

Cambridge Centre for Risk Studies
University of Cambridge Judge Business School
Trumpington Street
Cambridge, CB2 1AG
United Kingdom
enquiries.risk@jbs.cam.ac.uk
http://www.risk.jbs.cam.ac.uk/

October 2014

The Cambridge Centre for Risk Studies acknowledges the generous support provided for this research by the following organisations:

Institute of Catastrophe Risk Management

The views contained in this report are entirely those of the research team of the Cambridge Centre for Risk Studies, and do not imply any endorsement of these views by the organisations supporting the research.

This report describes a hypothetical scenario developed as a stress test for risk management purposes. It does not constitute a prediction. The Cambridge Centre for Risk Studies develops hypothetical scenarios for use in improving business resilience to shocks. These are contingency scenarios used for 'what-if' studies and do not constitute forecasts of what is likely to happen.

Report citation:

Ruffle, S.J.; Bowman, G.; Caccioli, F.; Coburn, A.W.; Kelly, S.; Leslie, B.; Ralph, D.; 2014, ***Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe***; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.

Research Project Team

Cyber Catastrophe Project Lead

Simon Ruffle, *Director of Technology Research*

Cyber Catastrophe Subject Matter Editors

Éireann Leverett, *Senior Security Consultant, IO Active Ltd.*
Dr Rob Watson, *Cambridge Computer Labs, University of Cambridge*
Dr Richard Clayton, *Cambridge Computer Labs, University of Cambridge*
Dr Frank Stajano, *Cambridge Computer Labs, University of Cambridge*

Cambridge Centre for Risk Studies Research Team

Professor Daniel Ralph, *Academic Director*
Dr Michelle Tuveson, *Executive Director*
Dr Andrew Coburn, *Director of External Advisory Board*
Simon Ruffle, *Director of Technology Research*
Dr Gary Bowman, *Research Associate*
Dr Fabio Caccioli, *Research Associate*
Dr Scott Kelly, *Research Associate*
Dr Roxane Foulser-Piggott, *Research Associate*
Dr Louise Pryor, *Risk Researcher*
Andrew Skelton, *Risk Researcher*
Ben Leslie, *Risk Researcher*
Dr Duncan Needham, *Risk Associate*

Consultants and Collaborators

Oxford Economics Ltd., with particular thanks to Fabio Ortalani, Senior Economist
Financial Networks Analytics Ltd., with particular thanks to Dr Kimmo Soramaki, Founder and CEO; and Dr Samantha Cook, Chief Scientist
Cambridge Architectural Research Ltd., with particular thanks to Hannah Baker, Graduate Research Assistant
Axco Ltd., with particular thanks to Tim Yeates, Business Development Director
Dr Andrew Auty, *Re: Liability (Oxford) Ltd.*
Antonios Pomonis, *Independent Consultant*
Dr Gordon Woo, *RMS, Inc.*

Cambridge Centre for Risk Studies
Website and Research Platform
http://www.risk.jbs.cam.ac.uk/

Stress Test Scenario

Sybil Logic Bomb Cyber Catastrophe

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

Contents

Stress Test Scenario

Sybil Logic Bomb Cyber Catastrophe

1 Executive Summary

Cyber and technology risks

Cyber and technology risks are some of the foremost facing business and society today.

Whilst much of the current focus is on direct impacts to individual businesses and individuals, in the Centre for Risk Studies we want to understand better the risk of cyber inflicted harm on the global economy and financial markets.

What is worrying is the potential for a global system-wide IT failure occurring across many organizations – a "correlated loss" event that ultimately erodes value in a vast number of companies across multiple industries. As businesses become more globally interconnected, our research suggests this type of threat is increasing.

Systemically Important Technology Enterprises

This report shows how some technology companies have become so critical to business productivity that they are systemically important to the global economy. Like the "Systemically Important Financial Institutions" (SIFIs) – banks that are so interlinked their failure would cause major impact – we use the term "Systemically Important Technology Enterprises" (SITEs) that identify technology enterprises crucial to international corporate productivity [1].

Sybil Logic Bomb Scenario

In this scenario we take an imaginary SITE, which we call the Sybil Corporation, and investigate the impact on the global economy of an insider attack that introduces a compromise, or 'Logic Bomb' into their flagship database product used throughout the corporate world.

Impact of Sybil Logic Bomb Scenario

The resulting global macro-economic impact portends an economic downturn driven by a reduced trust in IT by business leaders, investors and consumers, which we call an 'information malaise'.

The damage caused by the more extreme variants of Sybil Logic Bomb is almost as severe as the Great Financial Crisis of 2007-2012.

We measure financial market impacts through a standardized high quality fixed income portfolio. The main effect is seen in cumulative returns which drop substantially in the post-scenario years due to the ongoing information malaise.

Building the Sybil Logic Bomb Scenario

Classifying cyber threats

No comprehensive framework for risk assessment of cyber catastrophes exists, so it has been necessary for us to innovate in this area. We have built a framework for classifying cyber threat and compiled a database of past real-life attacks that have resulted in significant impacts. In conjunction with our Subject Matter Experts, collaborators and stakeholders, and literature review, we have built a taxonomy of possible cyber catastrophe scenarios.

Scenario selection

The cyber scenario was selected though a process that began with a workshop held in Cambridge in July 2013 involving our Cyber Subject Matter Experts, Éireann Leverett, Security Researcher, IOActive, and Dr. Rob Watson, Dr. Richard Clayton and Dr. Frank Stajano of the University of Cambridge Computer Laboratory. The process continued with a literature review and consultation with our supporters. From this we chose the Sybil Logic Bomb as having significant systemic impact.

Building blocks of cyber threat methodology

To develop the Sybil Logic Bomb we drew upon several key insights:

- A paper by the Brookings Institution that assesses the impact of cyber threats on company performance and which guided us to a methodology for the production of a revenue at risk for companies [2].
- The Bloomberg Industry Leaderboard, a set of 600 large global companies, on which we perform risk analysis for the private sector [3].
- The UN System of National Accounts on which we perform risk analysis by function for the public sector [4].

- The Global Industry Classification Standard (GICS) to differentiate the impact of the cyber scenario in different industry groups [5].
- A selection of the market leading relational database vendors, to benchmark Sybil. We assume Sybil has about 50% market share worldwide, 300,000 business customers and their products are used by most of the companies in the corporate world.
- The concept of IT Business Process Criticality that assesses the importance of individual technologies to a business process as a whole.

Macroeconomic and financial market modelling

We use the Global Economic Model of Oxford Economics to measure global macro-economic impact in terms of losses to global GDP output over 5 years [6]. The key parameters used to shock the economic model are productivity, confidence and consumption. Altogether we look at 4 variants (S1, S2, S3 and, the most extreme, X1) based on different parameter settings.

The output of the Global Economic Model is then applied to our standard investment portfolio, predominately fixed assets.

This is a stress test, not a prediction

This report is not a prediction. It is one of a series of scenarios that have been developed by the Centre for Risk Studies to provide stress tests for managers and decision takers. Beyond understanding impacts and responses around a specific shock, a suite of scenarios is needed to understand aspects of fragility of an organization and global system in which it sits.

A '1-in-100' Event

The Sybil Logic Bomb is extremely unlikely to occur. We gauge that a scenario of this severity could only be expected to occur with a chance of 1-in-100 in any year. There is a 99% probability that a cyber catastrophe of this severity will not occur next year.

The unfolding scenario

Information malaise

The scenario envisions corruption of the software of a fictional market leading relational database vendor, Sybil Corporation, by a malicious insider. The key feature of the Sybil Logic Bomb Scenario is that it is slow burning. It introduces small errors over time; these anomalies are hard to spot and replicate. It corrupts data backups – data backups being one of IT departments' key weapons for protecting systems. It unfolds potentially over several years slowly damaging and undermining business systems around the globe, with resulting increasing mistrust of systems and digital data supporting both the public and private sector. This is the "information malaise" where people just don't trust computer systems any more.

Quickly goes global

The Logic Bomb corruption is placed into a routine upgrade of the Sybil database software product – and, with Sybil being a widely trusted supplier, we can expect the corruption to be active in companies around the globe within weeks.

Latency period

A long latency period between activation of the Logic Bomb and its discovery is crucial to the catastrophic nature of the scenario. In our standard scenario this period is 5 quarters or 15 months. During this time it slowly and unobtrusively introduces low-level errors into data stored in Sybil databases.

Consequential analysis

Global macroeconomic losses

The overall effects of the Sybil Logic Bomb are measured in losses to global GDP output over 5 years ('GPD@Risk'). The 5 year GDP@Risk for the standard or base scenario, S1, is in the order of $4.5 trillion. The most extreme scenario variant, X1, shows a GDP@Risk of $15 trillion.

Financial market impact

In the short term the impact on our standardized portfolio is relatively small. In the longer term, effectively after the software problem has been rectified in Sybil's database packages, the effect is a 4% loss in cumulative returns due to the information malaise affecting the global economy.

Risk management strategies

The Sybil Logic Bomb Scenario illustrates the threat posed by systemically important technology enterprises, SITEs, to global trade. It is just one indicative example of a wide range of scenarios that could occur.

This scenario suggests that organisations, whether at the firm or government level, should consider redundancy in their database software systems in addition to redundancy in holding several copies of critical data.

This scenario is presented to help organizations develop operational risk management processes, contingency plans, and strategies for improving their ability to manage a crisis of this kind and survive the financial and counterparty challenge. It is presented as a capital stress test for insurers to consider their ability to manage underwriting losses while also suffering market impacts on their investment portfolios.

Summary of Effects of the Sybil Logic Bomb Scenario and Variants				
Scenario Variant	**S1**	**S2**	**S3**	**X1**
Impact factor	1	1.5	1.75	1.75
Latency period	15 months	15 months	15 months	24 months
Global recession severity (peak negative growth rate global GDP)	-2.5%	-2.7%	-2.9%	7.9%
Global recession duration	6 months	9 months	9 months	12 months
GDP@Risk $Tr (5 year loss of global output)	$4.5 Trillion	$7.4 Trillion	$8.8 Trillion	$15 Trillion
GDP@Risk % as % of Year 0's GDP	8%	13%	15%	26%
Standardized Investment Portfolio: Long term outlook (with baseline expected return of 4% return without cyber scenario):	-3%	-3.5%	-4.5%	-8%
US Equities (Dow Jones) Short Term Maximum Impact at Yr1Q4	-3.0 pts	-3.1 pts	-3.2 pts	-3.2 pts
US Equities (Dow Jones) Long Term Maximum Impact at Yr4Q4	-27.0 pts	-35.3 pts	-39.1 pts	-51.5 pts
UK Equities (FTSE 100) Short Term Maximum Impact at Yr1Q4	-1.4 pts	-1.7 pts	-1.8 pts	-1.8 pts
UK Equities (FTSE 100) Long Term Maximum Impact at Yr4Q4	-17.8 pts	-24.7 pts	-28.0 pts	-36.0 pts
US Consumer Price Index Short Term Maximum Impact at Yr1Q4	-1.7%	-2.6%	-3.0%	-3.0%
US Consumer Price Index LongTerm Maximum Impact at Yr4Q4	-15.5%	-22.8%	-26.3%	-33.4%
UK Consumer Price Index Short Term Maximum Impact at Yr1Q4	-1.7%	-2.7%	-3.2%	-3.2%
UK Consumer Price Index Long Term Maximum Impact at Yr4Q4	-8.0%	-12.4%	-14.7%	-21.5%

Table 1: Summary impacts of the Sybil Logic Bomb Scenario

2 Stress Test Scenarios

This report describes a plausible extreme future scenario and explores the effects that it would have. It is not a prediction. It is a 'what-if?' exercise, designed to provide a stress test for risk management exercises by companies who want to assess how their business systems would hold up under extreme circumstances.

This report is one of a series of stress test scenarios that have been developed by the Centre for Risk Studies to explore the management processes of dealing with an extreme shock event. Each individual scenario may reveal some aspects of potential vulnerabilities for an organization, but they are intended to be explored as a suite, to identify ways of improving overall resilience to surprise shocks that are complex and have many faceted impacts.

The scenarios have been designed in a number of ways. Firstly they are selected as plausible, but not probable, extreme events that would disrupt normal life and business activity. They are illustrative of the type of disruption that would occur with a particular category of 'threat' or 'peril' – i.e. a cause of disruption. In this example we explore the consequences of a cyber catastrophe, as a representation of the threat of infectious disease outbreaks disrupting daily life. Other threats considered in our suite of stress test scenarios include geopolitical conflicts, extreme weather events, pandemics and financial crises.

Complex risks and macroeconomic impacts

These threats are of interest because they are complex risks – they impact the networks of activities that underpin the global economy, disrupting the interrelationships that drive business, and causing losses in unexpected ways and places. They have multiple consequences, in causing severe direct losses, but also operational challenges to business continuity, cascades of effects on counterparties and the macroeconomy in general, and on the capital markets and investment portfolios.

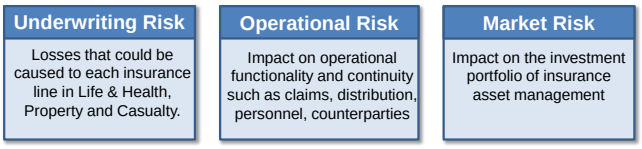
In these scenarios we explore how these effects might occur and try to trace the flow of consequences from initial losses to macroeconomic impact, and to market effects in the change of returns that would occur in a standardized investment portfolio.

The stress test is aimed at providing an illustration of the effects of an extreme event, to help a general audience understand the potential for events of this type to cause disruption and economic loss. It is aimed at informing the risk management decisions of a number of different communities.

Use of this scenario by insurance companies

The insurance industry uses scenarios as stress tests for their risk capital assessments, with explicit return periods of capital adequacy required by internal management, or for regulatory or reporting purposes such as AM Best, Solvency II, Lloyd's Realistic Disaster Scenarios, or other requirements. We offer this stress test scenario as a potential addition to the suite of scenarios that insurers may choose to use for their own internal purposes.

The particular contribution of this work is the assessment of the correlation of potential underwriting losses with an investment portfolio loss, while also considering the operational risks that could be challenging the business at the same time.



For insurers, the scenario provides an indication of potential losses across different silos of risk

The scenario attempts to assess indicatively where losses might occur across a range of different lines of insurance underwriting. Where we have access to data on total insurance industry exposure we have attempted some indicative quantification of the potential order of magnitude of losses. Insurers interested in assessing the impact to their own portfolios can apply these loss ratios to their own exposure in these lines of business.

We have also estimated how the event would impact investment asset values, using a standardized high quality, fixed income oriented portfolio to show the effect on indicative aggregate returns. Investment managers could apply these asset values changes to their own portfolio structures to see how the scenario would potentially affect their holdings.

Risk capital models make assumptions about correlations between underwriting loss and market risk. This report explores how this correlation occurs and provides a detailed example for one scenario.

It does not provide a probabilistic view of this correlation, but it does provide additional variants to the scenario that act as sensitivity tests and indicative additional data points around the primary narrative.

The scenario is deterministic and is not designed to provide exceedance probability data points.

It is very approximately selected on the basis of expert elicitation, to be in the range of the 1-in-100 annual probability of occurrence worldwide, but not rigorously determined.

Use of this scenario by investment managers

The scenario provides a timeline and an estimation of the change of fundamental value in assets in an investment portfolio. These are segmented into broad asset classes and geographical markets to provide indicative directional movements.

The scenario enables investment managers to optimize portfolio strategies against shocks of this type

These provide insights for investment managers into likely market movements that would occur if an event of this type started to play out. In real events, market movements are chaotic and difficult to analyze. This analysis suggests how the underlying fundamentals are likely to change over time, due to the macroeconomic influences. Investment managers can expect this to be overlaid with a lot of noise and chaotic market activity.

The asset class differences and geographical distributions enable investors to consider how different portfolio structures would perform under these conditions and to develop strategies for portfolio management that will minimize the losses that might occur. Where there are obvious winners and losers by economic sector, these have been highlighted to provide inputs into optimal hedging strategies and portfolio diversification structures.

This report provides performance projections for a standardized high-quality, fixed income portfolio, under passive management. This is to enable comparisons over time and between scenarios. We also estimate returns for individual asset classes to help investment managers consider how this scenario might impact their particular portfolio and to consider the intervention strategies over time that would mitigate the impact.

Use of this scenario by organizations

Many companies and organizations in the public and private sectors use 'what-if' scenarios for understanding and managing risk.

This scenario is designed to help organizations improve their operational risk management, and to identify improvements in business practices that will increase their resilience to shocks of this type in the future.

Stress test scenarios to improve risk preparedness have been well studied in management science. Scenarios that are most useful for improving operational risk management are those that are disruptive and challenging, and that force participants to confront a changed reality. Such scenarios should challenge management assumptions about the status quo. For a scenario to be useful, it also has to be plausible (but not probable), and 'coherent' – i.e. everything in the scenario is consistent and interlinked.

Acceptance of a scenario can be a problem in implementing stress tests. It is natural for managers to challenge the assumptions of the scenario and to question how feasible it is. The actual details and severity metrics for the scenario are less important than the exercise of working through management actions, however this report includes a section explaining how the scenario was selected and the justification for the parameters of the scenario.

The scenario is selected to illustrate the severity of shock that can be expected from this particular threat type (cyber catastrophe) with around a 1-in-100 (1%) chance in any given year, so it is extreme but plausible.

Our other scenarios are also selected at the same level of (im)probability. It is worth noting that the Centre for Risk Studies taxonomy of shock threats identifies over 50 potential causes of future shocks.

Each threat type is capable of providing some level of challenging shock to parts of the world's economy at around a 1-in-100 chance each year, so a global organization could expect to experience, and have to manage through, one of these shocks on average every few years.

This scenario is presented as a narrative, with specific metrics of loss, impact, and disruption estimated as indicators of the levels of management challenge that would be faced. We try to make the narrative as realistic as possible, to help managers identify themselves and their organizations in the fiction for the purpose of exploring their decisions in this hypothetical situation.

Improving an organization's resilience to a crisis requires a number of management elements, for which scenarios can be useful components. A major challenge is improving awareness of the potential for shocks and the expectation of disruption. Many companies face the challenge of developing a risk management culture in their organization, where expectations of continuity of the status quo are properly challenged, and contingency planning is an evolving process.

The scenario is designed for use by organizations to improve operational risk management

Operational risk management involves a wide range of activities, including procedures and response planning under a wide range of potential conditions, and broader cultural issues such as measures to sustain institutional learning about risk, consideration of succession planning, shared value systems, incentives, reporting, governance, and management monitoring.

This scenario provides inputs into the contingency planning around a situation of eroding confidence in IT infrastructure, disruption to the economy, failures of business counterparties, and disruption to global supply chains. It is intended to help companies improve their resilience to future crises.

Use of this scenario by policy-makers

International agencies, national governments and local authorities consider scenarios for global and national security, public safety and welfare of the population. Studies of potential catastrophes are produced by agencies such as World Bank, World Health Organization, United Nations, World Economic Forum, OECD, and others to improve the awareness and decision-making ability of policy-makers. This scenario is proposed as an addition to that literature.

National governments create risk analysis frameworks and preparedness scenarios for civil emergencies. Examples include the United Kingdom National Risk Register for Civil Emergencies, and the Australian Government National Risk Assessment Framework.

These frameworks commonly include example scenarios as guidance for local authorities in preparedness planning for deployment of emergency services and extreme response needs. In some cases, performance reviews against classified versions of these scenarios are mandatory requirements for regional authorities.

This scenario is a contribution to the design of future versions of these policy-maker scenarios. It offers a view of the economic environment and broader business and social disruption that will be the context for the challenges of ensuring public safety and continuity of public services. It provides inputs into the decision making and resource planning of these authorities, and is offered as context for policy-makers concerned with disaster mitigation in general.

It is worth remembering in policy formulation in the public realm that there is considerable crossover between policy making and overall business and societal impact.

Some SITEs are in the organizations that are making policy and there is reliance in the public sector on outsourcing to the private sector. Organizations must ensure they do not become misaligned with policy in the cyber area.

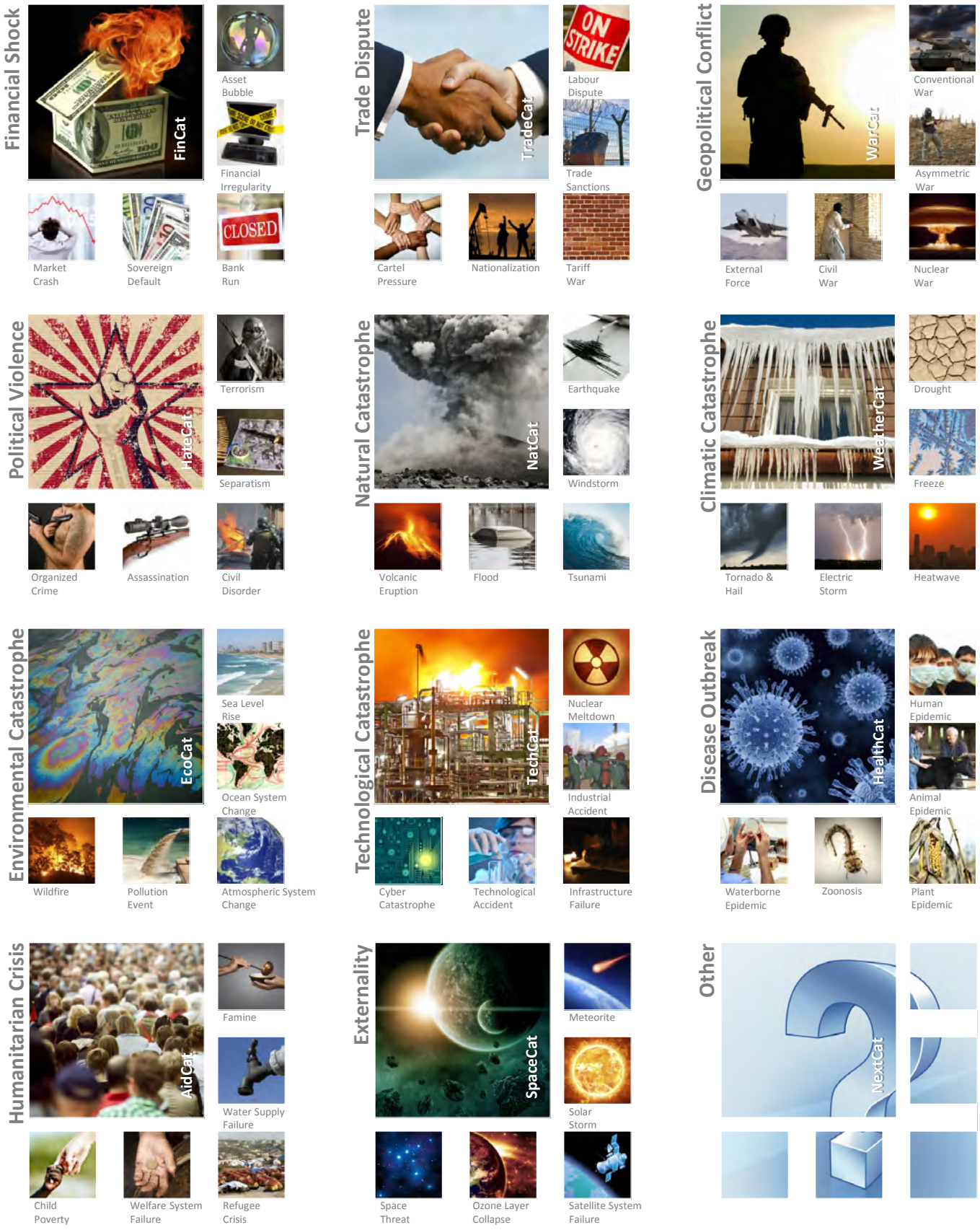
Understanding threats

This scenario explores the consequences of a key emerging threat type – cyber risk – by examining the 1-in-100 severity of an IT catastrophe with a selected example of how that shock could come about.

For a process that truly assesses resilience, we would need to consider how other types of shocks might occur. It would include different severities and characteristics of other types of cyber threats. It would also include an appraisal of other types of threat that could cause shocks.

The Cambridge Risk Framework includes an attempt to categorize the potential threats of social and economic catastrophes, to provide a checklist of different potential causes of future shocks.

This has involved a process of reviewing chronological histories for over a thousand years to identify all the different causes of disruptive events, collating other disaster catalogues and categorization structures, and researching scientific conjecture and counter-factual hypotheses, combined with a peer-review process.



Cambridge Taxonomy of Threats provides a checklist for complex risks of concern to organizations

The figure on the previous page shows the resulting Cambridge taxonomy of macro-catastrophe threats that have the potential to cause damage and disruption to social and economic systems in the modern globalized world. The threat taxonomy is hierarchical and categorized by causal similarity. The report Cambridge System Shock Risk Framework: A taxonomy of threats for macro-catastrophe risk management provides a full description of the methodology and taxonomy content.

The taxonomy provides a company with a check-list of potential causes of future shocks. It also provides a framework for collating information about these threats and populating it with more detailed studies of each threat. Threat types of particular interest are profiled with a stress test scenario like the one described in this report.

The taxonomy is being used to map the global landscape of complex risks, and to provide a suite of potential stress test scenarios that inform an organization's ability to withstand the wide range of shocks that it could potentially encounter. It is an aid to improving the resilience of an organization.

Developing a coherent scenario

It is a challenge to develop a scenario that is useful for this wide range of risk management applications. Fully understanding the consequences of a scenario of this type is difficult because of the complexity of the interactions and systems that it will affect. The economic, financial and business systems that we are trying to understand in this process are likely to behave in non-intuitive ways, and to exhibit surprising characteristics. We are trying to obtain insights into this interlinkage through using an extreme scenario.

Systemic instabilities constantly challenge our intuition, with many examples such as crowd behavior, traffic congestion, financial crashes, power grid failures and others. These are examples of strongly coupled, complex systems that exhibit have unexpected behavior. In these systems we see patterns such as feedback loops; non-linear amplifications; control interactions; cascade effects; avalanche phenomena; threshold effects and regime shifts; emergent patterns of behavior; temporary stabilities; and equilibrium states. It is important to identify the potential for these scenarios to trigger these types of cascading consequences which are the main causes of catastrophic loss.

These effects are what we mean when we call them complex risks. For stress tests to be useful, they need to be 'coherent' i.e. the described effects are all consistent with each other, follow causal mechanisms and logical consequence, and the correlation patterns of multiple impacts are represented comprehensively. The development of a coherent scenario requires structural modeling – i.e. scientific consideration of the cause and consequence sequence along the chain of cause and effect.

A structural modelling methodology

To develop a coherent stress test we have developed a methodology for understanding the consequences of a a scenario, as summarized in Figure 1.

This involves sequential processing of the scenario through several stages and sub-modeling exercises, with iteration processes to align and correct assumptions.

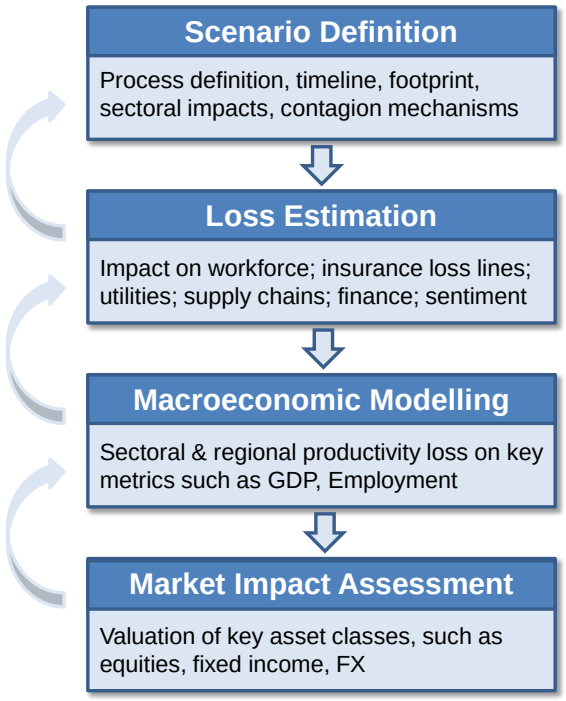


Figure 1: Structural modeling methodology to develop a coherent stress test scenario

The construction of a scenario using structural modeling techniques presents a number of challenges to fulfill the requirements for a coherent stress test.

- The first challenge is can we construct an extreme fictional scenario that has never occurred before and make it plausible? We have attempted to do this through using evidence-based precedents, and detailed analysis of how similar events of the past would play out today, under current conditions.
- Our second challenge is can these scenarios meet the criteria of being useable by businesses and ultimately adopted for use in risk management? To achieve this we have worked with key users to try to make these scenarios meet their

management needs for stress test scenarios, and are actively seeking ways to get the scenario tested further and more broadly adopted.

- Other challenges include can we estimate the losses that would result from extreme events that have not occurred in today's world, such as the Sybil Logic Bomb? We have addressed this through using historical precedents and extrapolation from similar but less severe occurrences to provide an evidence-based approach to estimation.

We believe it is important to create a robust and transparent estimation process, and have tried to achieve this through detailed process of recorded assumptions made, and sensitivity tests about the relative importance of one input into another.

In the macroeconomic stages of the modeling, we are conscious that we are attempting to push macroeconomic models, calibrated from normal economic behavior, outside their comfort zone, and to use them in modeling extreme events. We have worked closely with the macroeconomic modelers to understand the useful limits of these models and to identify the boundaries of the models functionality.

A further test comes when we try to model the impact of hypothetical economic extreme conditions on investment asset classes and portfolios. We need to understand the limits of usefulness of assumptions such as asset value 'fundamentals' in investment performance estimation.

Uncertainty and precision

Overall the scenario consequence estimation process is steeped in uncertainty. The process entails making a number of assumptions, which feeds into a set of models to assess loss and direct impact. These are then used as inputs into a macroeconomic modeling exercise, with additional assumptions and the introduction of considerable uncertainties and variation. The outputs of this then feed the assessment of portfolio performance, with additional assumptions and uncertainties. Linking all the components into a coherent scenario is difficult to achieve and the process described in this report is one approach that has attempted to do this. It is flawed in that the process is imprecise and one of compounded uncertainty from one stage to the next and the credibility of multiple aspects of any particular scenario can be attacked.

The point, however, of producing the scenario is to understand the consequences in terms of their holistic effects, their relative severities and the patterns of outcome that occur.

The scenario production process, limited as it is, does provide interesting insights, and many of the applications of the scenario are achieved through this imperfect approach. The scenario is offered as a stress test, to challenge assumptions of continuing status quo and to enable companies to benchmark their risk management procedures.

3 Cyber Threat as an Emerging Risk

Cyber threat covers a wide range of malicious activity that can occur through cyberspace.

There are numerous recent examples demonstrating the breadth and complexity of the cyber threat landscape: individual computers are attacked in people's homes with viruses that attempt to extort money; 'hacktivists' attack government websites; nation states are accused of sustained cyber espionage; malicious software damages physical infrastructure; organized crime employs hackers to enable them to steal millions in cash; stock markets react to hoax information posted on news feeds by state sponsored "electronic armies".

The constant reports of companies being hacked contribute to a growing sense that cybercrime is out of control [7].

The threat of a major cyber attack features as one of the top technological risks in the 2014 Global Risks Report of the World Economic Forum [8].

There is a tendency with cyber threat to think about attacks on individual organizations. In the Centre for Risk Studies we want to understand better the risk of cyber inflicted harm on groups of firms, industry, and the global economy and financial markets. We are interested in a systemic cyber catastrophe.

Cyber risk is a fast growing emerging threat. Different constituencies have an interest in – and often a self interest in – this topic.

- IT / Security: Concerned mainly with day to day defence against cyber attack on companies and particularly interested in the technology of the threat.
- Military science: Concerned with understanding the battle going on in cyber space, attack and defence postures and the resources and covertness of attackers.
- Criminology: Concerned with understanding what crimes have been committed, the modus operandi of criminals and criminal organisations, methods of prosecution and sentencing policy.
- Regulation / Standards: Looking to improve cyber security through regulations and standards.
- Policy: Governments, industry bodies and institutions such as the EU looking to improve resilience to the cyber threat through policy decisions.

Date	Name	Primary Harm
2013	Target	Theft
2013	Obama Twitter Scare	Disruption
2013	Cloudflare Attack	Disruption
2012	The Unlimited Operation	Theft
2012	Flame/Skywiper	Theft
2012	Shamoon (Aramco)	Damage
2012	Operation Ababil	Disruption
2011	RSA	Theft
2011	Citigroup	Theft
2011	Sony Playstation	Theft
2011	Epsilon	Theft
2010	Operation Aurora	Theft
2010	BlackShades	Theft
2010	Stuxnet	Damage
2008	RBS Worldpay	Theft
2008	Heartland	Theft
2007	Estonia	Disruption
2007	Zeus / Gameover	Theft
2007	Conficker	Disruption
2006	APT1	Theft
2005	TJX	Theft
2004	Titan Rain	Theft
2004	Sasser	Disruption
2004	MyDoom	Disruption
2003	SQL Slammer	Damage
2001	Code Red	Damage
2000	Mafia Boy	Damage
2000	ILOVEYOU	Damage

Table 2: Catalogue of major cyber events from 2000 to 2013 with their primary consequence or harm

The threat to companies

A 2011 report by the Cabinet Office and Detica Limited [9] estimated a total cost to the UK economy of £27bn annually, and published a distribution amongst different crimes. Attempts to estimate an annual US total cost have resulted in figures ranging from $250bn to $1tn. However these estimates are controversial.

The Detica report was greeted with widespread skepticism and its estimates of substantial losses due to IP theft and espionage have been criticized as lacking in evidence [10]. Reliable data on individual company losses from cyber attacks is difficult to obtain. Companies are often concerned about reputation damage if they go public with losses due to a cyber attack.

Even within companies, IT departments may want to shield senior management from details of breaches in security. This may change with a trend for regulators to start demanding disclosure of cyber breaches as is happening in the US with the Securities Exchange Commission [11] and forthcoming in the EU according to ENISA [12].

The average direct cost varies widely but according to the annual Ponemon Cost of Cyber Crime study [13], which surveyed 199 companies in five countries, it averaged $9m per company per year in the US in 2012 (see Figure 2). To these costs should be added the indirect costs – lost business opportunities, staff morale and company reputation that although difficult to estimate, can be greater than the direct costs suffered.

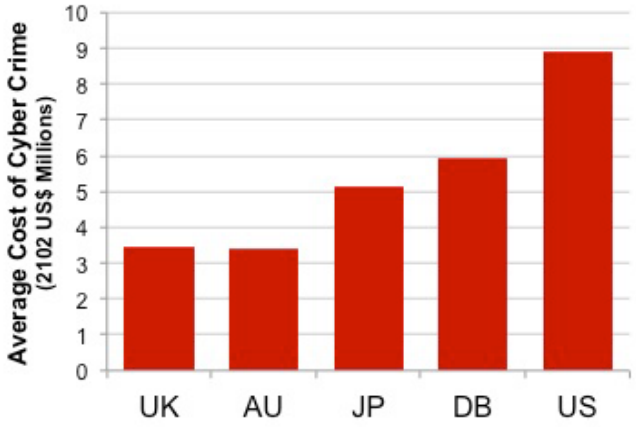


Figure 2: 2012 total average cost of cyber crime in five countries (USD, n=199 companies)

A report by the Center for Strategic and International Studies [7] estimates the likely annual cost to the global economy from cybercrime as more than $400 billion.

Theft

Actions that extract data items that are of *value* to *the perpetrator* and breach the *confidentiality and duty of care* of the data holder.

- Espionage of industrial secrets, intellectual property, corporate know-how
- Theft of money; transfer of funds; appropriation of assets, investments, stocks and bonds
- Obtaining customer records; Databases of personal information; trading records; confidential business transaction data
- Obtaining identity information; passwords; credit card details; consumer data

Disruption

Actions that *interrupt business functionality* for a period of time, or *degrade productivity* of commercial operations, transactions, or communications

- Denial of service for internet-based businesses
- Blocking or degrading communications, emails, transaction orders
- Downtime of public facing websites, internal servers, cloud resources and individual workstations

Damage

Actions that corrupt data, or damage software, systems, or physical equipment, and require resources to repair or restore, and incur costs, liabilities and reputational damage

- Hacks that corrupt or delete data or software
- Attacks that disable servers, hard drives, individual computers
- Subverting control systems to trigger damage to physical equipment or systems
- Losses due to malfunctioning trading algorithms

Historical Case Study
Stuxnet (2009)

Stuxnet was a game changer – although losses were not large, it made headlines because malicious code was seen deliberately targeting physical critical infrastructure. Stuxnet targeted industrial systems under control of the Siemens PCS7 SCADA (Supervisory Control and Data Acquisition) system. The specific target appears to be the Natanz Nuclear Facility in Iran where it spun 1000 nuclear centrifuges past their operating limits and destroyed them. It also caused damage to other industrial systems under control of the Siemens system; the oil industry seems to have been particularly affected. The perpetrators are generally considered to be the US and Israel.

Secondary characteristics of cyber threat

The motivation behind cyber attacks can be political, military, financial, revenge, or just curiosity or notoriety. As cyber attacks become more sophisticated the resources behind a particular attack become an important measure, as are the degree of covertness and the duration of the attack before discovery. Perpetrators can be divided into groups as follows:

Intelligence services / electronic armies: Many states now operate cyber intelligence specialists (GCHQ in the UK; NSA in the US) which are actively involved in cyber offence and defense.

- Terrorists
- Industrial Spies and Whistleblowers
- Organized crime: Organized crime has moved into cyber space.
- Insiders: Often cited as the biggest risk to companies is the disgruntled employee who has access to passwords and sensitive systems.
- Hacktivists: Groups with an activist or anarchist agenda now have many channels for expounding their views and launching attacks.
- Individual Hackers: Of less concern as cyber attacks become more sophisticated and require increasing resources, but the individual hacker still has potential.

These threat groups often exchange information amongst themselves; a well developed market exists for the trading of information such as stolen credit card details. Ironically information about cyber threats flows more fluidly around the attackers than it does amongst companies and law enforcers, and the hacking community is becoming increasingly well organized and associated with organized crime. [13].

We bring together the secondary characteristics in our cyber magnitude scale, see Table 3.

History

We are constructing a database of significant cyber attacks since 2000, see Table 1.

There is no consistent naming convention for cyber events - events often are given more than one name.

There is a shortage of robust loss data from past cyber events. There is little agreement on the overall costs – although some cost estimates have been published they are highly controversial and estimates for the same event from different commentators vary by orders of magnitude. For this reason we do not attempt to estimate cost.

Historical Case Study

APT1 (2006)

Chinese 'Comment Crew' hackers emptied QinetiQ of top-secret military data

US firm complacent about serious breaches, Bloomberg alleges

APT1 ('Advanced Personal Threat' 1) is a large scale economic espionage attack by China on western nations that allegedly has taken place over many years from 2006 onwards. Companies in industry sectors that match the strategic industries identified in the Chinese Five Year Plan were particularly targeted. The preferred mode of attack was 'spear phishing' where individuals are targeted in organizations. The key document that has identified this attack is by the Mandiant Corporation [15] – it identifies the perpetrators as Unit 61398 of the Chinese People's Liberation Army (PLA). In May 2014 the US published a "Wanted" poster [16] of five PLA officers indicting them on charges of computer hacking, economic espionage and other offenses.

Magnitude and vulnerability scales

We have developed a simple cyber magnitude scale of our own to use for classifying our historical catalogue of cyber events, see Table 3.

There are various measures of the vulnerability of an organization to cyber threat, including the Security Effectiveness Score (SES) [17].

The Ponemon 2012 Cost of Cyber Crime: United States [13] ranks losses in companies by their SES. Their study shows that companies with a better SES, i.e. which are less vulnerable to cyber threat, tend towards lower losses (see Figure 3).

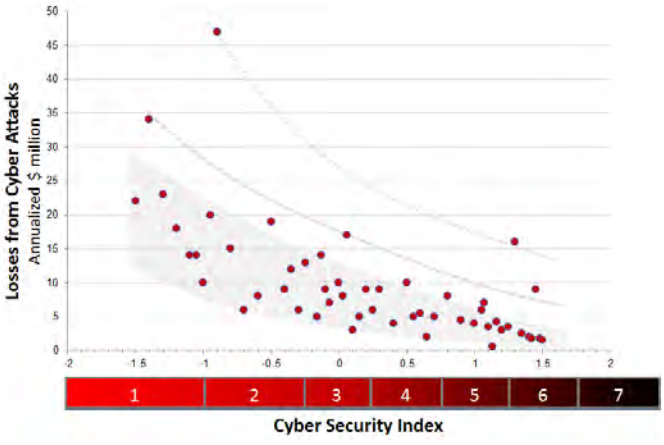


Figure 3: Level of cyber security (SES Index) reducing the cost of cyber events (Ponemon 2012).

Magnitude Scale Value	Threat profile	Typical perpetrator profile	Motivation	Time scale	Covert-ness	Resources/ Logistics	Historic precedents
Magnitude **1** Cyber Hazard	Undirected attack using a single cyber attack technique	Lone bedroom hacker; "script kiddie"	Curiosity; notoriety	Short	Low	Low	SQL Slammer; Mafia Boy
Magnitude **2** Cyber Hazard	Directed attack on defined targets using single cyber attack technique	Group of hackers; online buddies; hacktivists	Notoriety; activism; political	Short	Medium	Low	Sony Playstation, Conficker
Magnitude **3** Cyber Hazard	Directed attack using mix of cyber attack techniques, kinetics and social engineering	Malicious insider; organised crime; "hacker-backer-casher"	Revenge; political; financial	Medium	Medium	Medium	Unlimited Operation
Magnitude **4** Cyber Hazard	As 3 but with addition of more development resources, testing facilities, increased covertness and kinetics.	Security agency in peacetime mode; Mafia grade criminal organisation	Financial; political	Long	High	High	APT1, Stuxnext
Magnitude **5** Cyber Hazard	As 4 but with military grade resources and intensity of attack.	Electronic army; nation state	Political; military	Long	High	High	

Table 3: Cyber Magnitude Scale

Historical Case Study

The Unlimited Operation (2012) [17]

This was an organized crime of the type known as a 'backer – hacker – casher' attack. Hackers were paid to compromise two banks in the Middle East — the National Bank of Ras Al-Khaimah PSC in the United Arab Emirates and the Bank of Muscat in Oman — where prepaid debit card accounts were breached and the withdrawal limits normally placed on debit card accounts were removed.

Then teams of operatives on the ground (the cashers) were provided with corresponding compromised debit cards which were used to extract cash from ATMs in various places around the world. A map of their extractions from ATMs in Manhattan is shown here. There were two attacks – the first in December 2012 lasted 3 hours and netted $5m. A second attack in April 2013 netted $40m in 9 hours. Some cashers were later arrested.

4 Defining the Scenario

Defining a cyber catastrophe

We define a cyber catastrophe as a systemic event that can impact many organizations at the same time, causing many of them to suffer significant levels of loss. This focus on the systemic aspects of cyber risk means that we are not as concerned with attacks on individual companies or single targets, even though these can be severe in themselves. Figure 4 illustrates example scenarios and those we might consider as systemic cyber catastrophes.

Severity

To benchmark this stress test scenario to others in the Centre for Risk Studies suite of emerging risk scenarios, we need to assess the severity of a cyber event that would occur with about a 1% probability of exceedance somewhere in the world in a given year – a '1-in-100' annual likelihood. With cyber threat this is a particularly difficult assessment, as the historical records only span a few decades and is a rapidly evolving threat, so a historical statistical perspective is of little value. Instead we have reviewed the magnitudes and typologies of cyber threat, and proposed that a magnitude 4 event would provide approximate comparability with the 1-in-100 benchmarking of other threat scenarios.

Selection process

To select the scenario we worked within our three primary areas of harm – theft, disruption and damage. During a process which began at a workshop held in summer 2013, involving our Subject Matter Specialists, and continued for nine months with our research partners and stakeholders, and including an extensive literature review, we identified a set of candidate abstract cyber scenarios, seen in Table 4. They are based to some extent on past cyber events, and also hypothetical possibilities that our experts have identified. We have had to extrapolate from the limited range of past events and our knowledge of the science to design our scenario.

Scenarios can be plotted on a two dimensional graph with number of companies affected along the bottom and severity of loss up the side. For example an exploit of Microsoft Windows would affect a large number of companies – but we don't think it would cause much loss. Most modern IT departments are well equipped to deal with an attack of this type. Similarly a big budget highly targeted physical attack – like Stuxnet – may do a lot of damage but is very unlikely to act simultaneously across a wide range of victims.

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	

Table 4: Candidate Cyber Catastrophe Scenarios

We have chosen long term data corruption as the basis for our Sybil Logic Bomb cyber scenario.

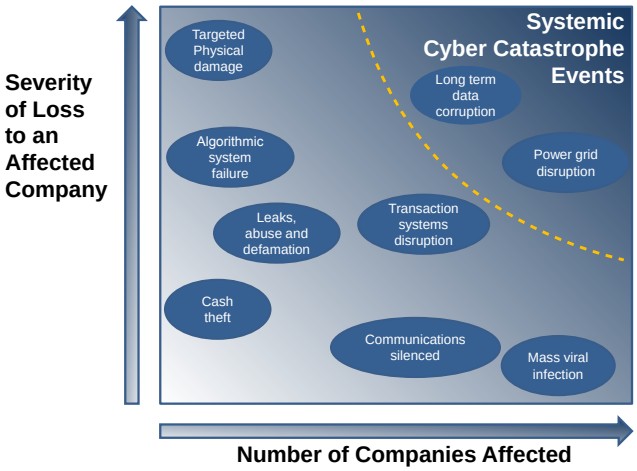


Figure 4: Cyber event scenarios and those that constitute systemic cyber catastrophes

A '1-in-100' Event

The scenario we describe is unlikely to occur. In fact we have chosen a severity of scenario that could only be expected to occur with a chance of 1-in-100 in any year. So there is a 99% probability that a scenario of this severity will not occur next year. We stress that for a counterfactual event that has never occurred, estimating how its severity corresponds to its return period is problematic.

We have combined a historical review of IT events, accidental and malicious, with a workshop to seek expert opinion, to gauge the scale of a 1-in-100 likelihood year cyber catastrophe.

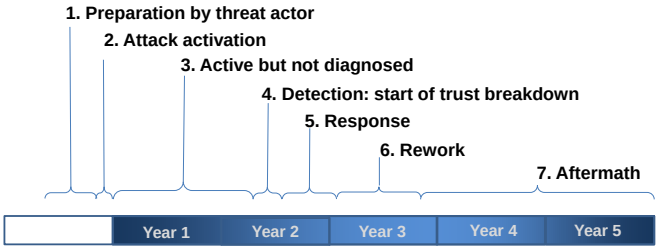


Figure 5: Timeline of scenario showing phases

Cassandra

We use an imaginary website called cassandra.com to illustrate the narrative of the scenario.

Scenario Variants

We have produced variants of the Sybil Logic Bomb scenario S1, S2 and S3 with increasing impacts of 1, 1.5 and 1.75 respectively. The amount of time that Sybil remains undiscovered – in its "Activated but not Diagnosed" latency phase – is a further variation. The first three variants have a latency time of 5 quarters and the additional X1 variant is S3 with 2 years latency time.

Other variants that we have not considered in any detail include varying the industry groups targeted by the logic bomb; and varying the profile of the company or companies that Sybil is based on, because the different real life vendors operate in different markets.

The variants are discussed in the macroeconomic modeling chapter.

5 The Scenario

Background

The Sybil Corporation is a software vendor that produces the market leading relational database. Established in the late 1970's, Sybil's databases run on all common operating systems and are employed in most sectors of the global economy with a particularly strong uptake in the corporate world. Sybil databases tend to sit on servers at the heart of corporate IT systems storing data from all aspects of the business. Many third party vendors offer systems and services that are built upon the Sybil database.

Working in Sybil's software development division in Redwood Shores, CA, USA, is a thirty year old mathematician employee responsible for the computational and arithmetical software code. She is becoming increasing antagonistic to global capitalism and has recently become interested in and sympathetic to the activities of the "Anonymous" hacktivist collective. She decides to covertly and maliciously modify some of the source code of the Sybil database to which she has access, knowing that the next routine upgrade which will be issued to all users of the product, will include her modified code.

Phase 1 Preparation and Research

The employee decides to modify the floating point computation of the Sybil database to produce errors in results that are in the range -10% to +10% away from the correct value. The error is only to occur if any of the input variables match the last three numbers of the host computer's manufacturer's serial number.

This will cause errors in the many critical business systems based on the Sybil database. By targeting floating point, the errors will appear in algorithmic systems rather than in transaction processing. Transaction processing includes many traditional uses of computers – such as payroll, stock control, invoicing and reservations; algorithmic systems are those involved more in design, decision support, trading and modeling and are increasing in their importance and influence in business processes. "Algorithms are what computers use to decide stuff" [19].

By design the compromise will be hard to detect. Routine financial computations found in transaction processing will be largely unaffected – because errors in this type of calculation would be quickly spotted by the daily checks and balances of accountants and bookkeepers. Small errors in the ±10% region in algorithmic systems are harder to detect.

The additional filter of the input matching the machine serial number means that a specific problem cannot be replicated on a different machine but will be consistent on the host machine. This undermines attempts to replicate the issue, which will be the first thing support staff will try when attempting to diagnose the problem.

The employee then covers her tracks by altering the date on the source file, and the meta data in the code repository back to their original conditions before the modification was made, making it difficult for her managers to spot the change. The employee uses her knowledge of the Quality Assurance procedure in Sybil – specifically what tests are run on the floating point algorithm – to further optimize the compromise so it will not be detected by QA procedures.

Phase 2 Attack Activation

The compromised software is released as part of a routine upgrade for all Sybil customers. An upgrade from a well-respected company like Sybil will be trusted. Good corporate cyber security practice which is on the lookout for worms, phishing and insider attacks will not spot a compromised upgrade.


CASSANDRA.com

Sign up | Log in

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

Sybil releases latest database upgrade

Version 11.6 release majors on Big data

Wednesday, February 20th

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

Sybil's software suite 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 eighteen months.

Customers vary widely as to when they actually apply the upgrade. Many run the upgrade through their own QA testing before they apply it but it is unlikely to include rigorous testing of the floating point algorithm. Some have been waiting for it and are keen to apply it because it contains a bug fix or new feature they need. Some wait to see if other companies experience problems with it, but as there appear to be none they install it.

Application of software updates varies by industry sector. On average the financial sector will install upgrades in 6 months, and the industrial sector 18 months.

Phase 3 Active but not Diagnosed (Latency Period)

With the compromised upgrade released, and companies beginning to apply it, the scenario moves into the pre-detection or 'latency' period where the compromise is activated but not yet detected.

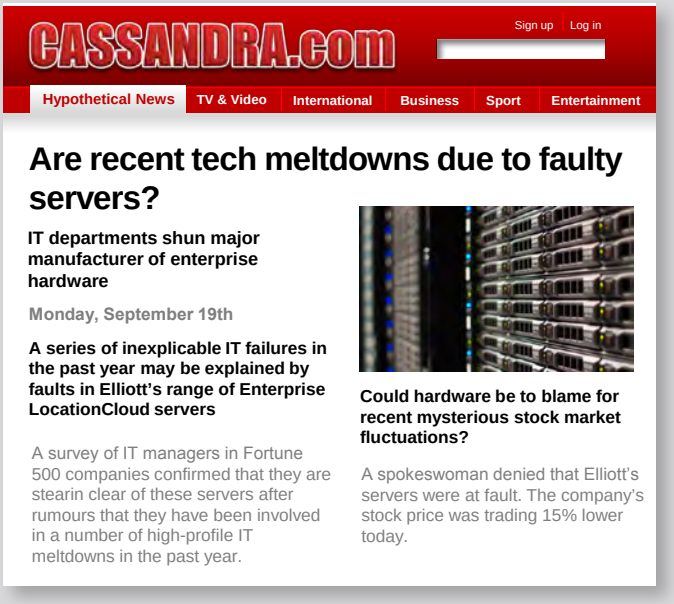
Once a company has installed the compromised upgrade, all their algorithmic systems based on the Sybil database start to accumulate errors but these go unnoticed for a while as they largely affect design, modeling, decision support and reporting activities in small ways. Some users are never exposed to the errors – their data does not contain a value that matches the last three digits of the server's serial number.

Over time some users spot errors. Then begins the procedure of escalating the issue. Initially the user thinks there is an error in their own calculation. Once this is discounted they report it to their IT support desk. IT attempt to replicate the problem on a test machine – which having a different serial number does not produce the error. The issue is reported to Sybil's support team but they also are unable to replicate it. This leads to periods of frustration for users as their problems are not being taken seriously by support teams. Eventually many companies draw the conclusion that this is a hardware fault, so they replace the server. Unless the new machine's last three serial numbers happen to match the old machine, this appears to fix the issue.

Some companies call in security consultants, but they draw a blank as the issue does not show any of the traces of a normal cyber attack – no unauthorized access, no detectable malware, and no known exploits of Sybil.

As it emerges in the IT world that servers running Sybil seem to be experiencing unexplained hardware issues, a certain brand of server is erroneously suspected, resulting in pre-emptive replacement of that brand and avoidance of purchasing that brand in the future by IT departments. This impacts the profitability, brand value and stock price of this server manufacturer.

As time passes the key disruptive consequences of this cyber attack become evident though still no one is making the connection to the upgrade or even to an issue within Sybil. These key consequences will be characterized as impacts on quality, for example:


CASSANDRA.com

Sign up Log in

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

Are recent tech meltdowns due to faulty servers?

IT departments shun major manufacturer of enterprise hardware

Monday, September 19th

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

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

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

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

- Design systems (such as Aeronautical CAD systems) based on Sybil have started to introduce small random changes in manufactured parts which begin to fail or give degraded performance.
- Modeling and Decision Support Systems (such as a Commodity Trading or Oil Pricing Model) start to give random erroneous results resulting in loss making trades and price setting that results in loss of profitability.
- Reporting systems (such as MIS and CRM systems) start feeding erroneous data back to managers and boards who make incorrect decisions. Company regulatory filing and annual reports appear with errors in them.
- Process Control Systems (such as can be found in manufacturing and industrial control systems) start producing erroneous threshold values resulting in degradation in quality and, in the worst cases, equipment malfunctions [20].
- Logistics systems start causing shortages of parts to industry and products to consumers resulting in a fall in quality of service in these sectors.

Waves of unease are appearing through various sectors of the world economy. The rate of corruption is slow and difficult to detect but over time more and more data is being corrupted, but the extent is not easily verifiable. Meanwhile as normal routine backup procedures have been running, erroneous data within Sybil, and other company systems to which erroneous data has propagated, is progressively corrupting backups.

News stories start circulating about regular inexplicable costly events taking place in the corporate world. Investment analysts start to notice and mark down stocks.

Almost daily events are being reported like the following examples in the table. These are imaginary but are based on real events caused by erroneous data in corporate modeling, decision support and forecasting systems.

This table also begins to show how we will assess the impact of the scenario.

The overall harm caused by the Sybil Logic Bomb is damage to organizations through 'long term data corruption' as discussed in Chapter 4. In the following table we start to classify the mechanism by which loss is incurred by the companies. Loss mechanisms are explored in more detail in Chapter 6.

GICS Industry Group	Fictional Company	Fictional Failure	Real life precedents	Loss Mechanisms
Automobiles and Components	UK Auto Group	In UK Auto Group, an automobile manufacturing facility, a 9-foot robotic swings around 180 degrees despite the controller for the arm being in standby mode. 3 workers are killed. The SCADA system controlling the facility was being fed operating parameters from a compromised Sybil database.	"Ping Sweep": Robotic arm out of control (Duggan, Berg, Dillinger, & Stamp, 2005) [21]	Workers' compensation.
Banks	Albion Bank	For two years at UK based Albion Bank they failed to notice an error in interest rate calculations caused by erroneous data from their compromised Sybil database. They are forced to write off $1.75 billion. Company directors are sued by the shareholders for loss of share value.	National Australia Bank, 2001:HomeSide write-downs, $2.2Bn loss. (The Cost of Bad Data, 2013) [22]	Loss of assets; Loss in market value; Directors and Officers liability
Insurance	Eviva	A UK insurance company, Eviva, admits it has lost all record of thousands of customer policies. A system based on a Sybil Database that is used to scan and archive paper documents in bulk is discovered to be altering numbers randomly	Xerox WorkCentre Document Scanning Flaw (Kriesel, 2013) [23]	Loss of digital assets, loss in customer confidence, recovery costs
Diversified financials	Standard Capital	Standard Capital trading in US Equities suffers a trading error that costs £440 million due to a 'technology breakdown' in its high frequency trading algorithms, which unknown to them was caused by erroneous data from a compromised Sybil database. 75% of the company's equity value was erased forcing its eventual sale.	Knight Capital $450m loss (Popper, Flood of Errant Trades Is a Black Eye for Wall Street, 2012) (Popper, Knight Capital Says Trading Glitch Cost It $440 Million, 2012) [24, 25]	Loss of assets
Semiconductors & Semiconductor Equipment	Acorn Holdings	In Acorn Holdings, an integrated circuits fabrication plant a system controlling the creation of integrated circuits in the fabrication plant hangs. The outcome is the destruction of $50m worth of wafers. The SCADA system controlling the facility was being fed operating parameters from a compromised Sybil database.	Semiconductor fabrication production line failure: $50,000 damage (Duggan, Berg, Dillinger, & Stamp, 2005) [21]	Loss of assets, loss of income, contractual compensation

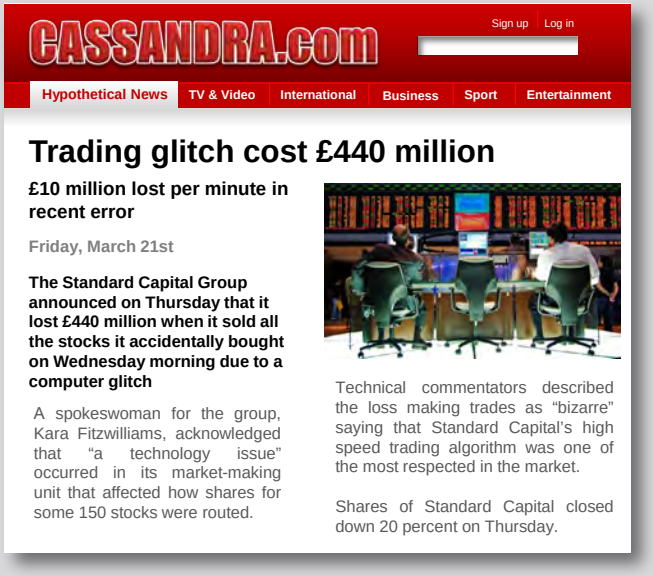
Continued.

Pharmaceuticals & Biotechnology	UK Pharma	UK Pharma, a struggling pharmaceutical company is forced to reiterate its yearly and midterm financial forecasts after admitting it contained "out of date planning information" which had resulted from data from a compromised Sybil database entered into a forecasting spread sheet. Its stock price falls as a result and shareholders sue the Directors.	AstraZenica spreadsheet error sends wrong data to sell side analyst community, 2012. AstraZenica (Reuters, 2012) [26]	Loss in market value; Directors and officers liability
Pharmaceuticals & Biotechnology	US Pharma	US Pharma has to recall its latest flagship drug after side effects are revealed. It turns out that errors at the Clinical Trials stage lead to incorrect formulation of the drug. The Clinical Trials system runs on a compromised Sybil database.	Target Health Inc. report (Mitchel & al, 2011) [27]	Liability; Loss of income; loss in market value
Media	SatMedia	SatMedia, a major live event organizer has several occasions when their events are massively overbooked causing disruption as large numbers of people arrive at venues and cannot gain entry. This is being caused by the compromised Sybil database the runs their booking systems. Audiences at live events fall and the company's stock price crashes.	Locog spread sheet error causes Olympic ticket overselling, 2011 Locog / Ticketmaster "Spreadsheets behind Olympic data misentry" (Kelso, 2012) [28]	Loss in market value; loss in customer confidence
Energy	Anglo Dutch Oil	Anglo Dutch Oil is not able to send gas through its pipelines to its customers for 24 hours due to its Process Control System being fed incorrect operating parameters from a compromised Sybil database.	Penetration test locks up SCADA system of gas utility for 4 hours. (Duggan, Berg, Dillinger, & Stamp, 2005) [21]	Loss of income; degradation of service; contractual compensation; customer compensation
Utilities	UK Power	A large publicly traded power generator and marketer of electricity and renewable energy called UK Power takes a $25m charge after it lands more power transmission hedging contracts than it bargained for at higher prices than it wanted to pay. The error came from ranking bids based on a compromised Sybil database.	Transalta: $25m charge due to wrong transmission hedging contracts (EuSpRIG, 2012) [29]	Loss of assets

Table 5: Fictional IT failures with real life precedents

Fund manager loses £440 million

For example, a fictional fund manager we call Standard Capital suffers a huge trading loss – £440 million is lost in just 45 minutes of trading. The cause of this is their high speed trading algorithm taking operational parameters from its compromised Sybil database. The database is passing values 10% too high into the highly sensitive workings of the trading algorithm. This is fiction, yet is based on the real example of Knight Capital where a mistake in their trading algorithm resulted in $440m of trading losses in 45 minutes and the ultimate demise of the company.



CASSANDRA.com

Sign up | Log in

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

Trading glitch cost £440 million

£10 million lost per minute in recent error

Friday, March 21st

The Standard Capital Group announced on Thursday that it lost £440 million when it sold all the stocks it accidentally bought on Wednesday morning due to a computer glitch

A spokeswoman for the group, 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.

Utilities company liable for spillage

In another example, a fictional utilities company UK Utilities Group suffers a series of pollution incidents where a sewage treatment system repeatedly opens valves and spills out raw sewage in many locations resulting in big clean up bills, fines and liability claims. The cause is their process control system is taking parameters from a compromised Sybil database. This is fiction, yet is based on the real example of Maroochy Shire County in Australia where a disgruntled employee caused 47 sewage spill incidents over 6 months by hacking into the sewage pumping control systems.

CASSANDRA.com

Sign up | Log in

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

UK Utilities fined again for pollution

IT control system to blame

Tuesday, June 30

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 against blames faulty IT control systems for opening valves that caused 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 the 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.

Bank accounting errors

In another example a fictional UK bank we call Albion Bank suffers a $1.75 billion write-down. A mortgage servicing rights valuation model for an acquired US home mortgage lender is 2% in error over a period of two years. The cause of this is their model taking data from a compromised Sybil database. This is fiction, yet is based on the real example of National Australia Bank in 2001 where an error in a financial model that went unnoticed for two years caused just such a write-down and resulting legal action in the US for securities fraud.

CASSANDRA.com

Sign up | Log in

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

Bad data leads to write-down

Glitch caused $1.75 billion write-down for UK bank

Friday, November 21

LONDON, UK (Bloomberg) – Today, Albion Bank booked a write-down associated with a US-based lender totalling $1.75 billion (£1 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 following a contract

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

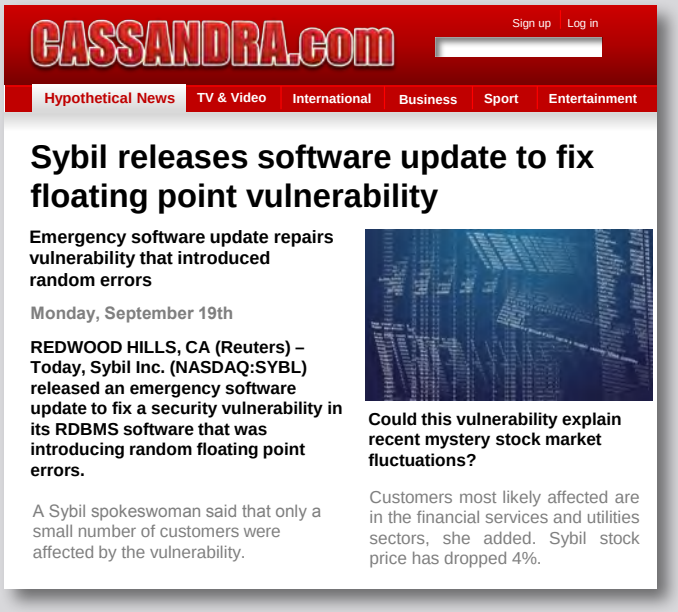
Shareholders are already attempting to sue Albion in the United States for security fraud.

Phase 4 Detection

A certain time after the release of the compromised upgrade Sybil finally recognizes the problem as being theirs and quickly releases an urgent security upgrade that removes the compromised code. Sybil apologizes for the defect but announces it only affects a minority of its user base and points to its limited warranty clause in its software license.

The time period known as the latency period when the Logic Bomb is active but not diagnosed in our standard scenario is 5 quarters or 15 months. We also have a more severe variant where the latency period is 8 quarters or 24 months.

In their security bulletin Sybil describe the timeline of the compromise thus companies can identify the period over which they were infected based on the date they installed the upgrade. Companies vary in the length of time it takes them to install an upgrade, and there is evidence that the average time for doing this varies by industrial sector.


CASSANDRA.com

Sign up | Log in

Hypothetical 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

Monday, September 19th

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

A Sybil spokeswoman said that 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 5 Response to contain the attack

Awareness of the impact of the Sybil compromise dawns on the corporate sector. An investigative journalist writes an article 'The Sybil Logic Bomb' explaining how the previously assumed unrelated and unconnected events can all be traced back to the Sybil compromise and how there is now corrupted data all over the corporate sector that has impacted decisions and quality and is now embedded deeply into backup systems.

He points out that the rectification of the defect by Sybil will have no effect on the data already corrupted and the problems will continue.

There is a collapse in trust. Events continue to occur – now, no one knows if are connected to corrupted data caused by the Sybil Logic Bomb or not.

Panic begins to spread around companies. No one knows which data is compromised and which is not. Because Sybil acts as a basis for so much business activity there is no guarantee that compromise is limited to the Sybil database – corruption could be any part of the business.

- Some companies wipe hard drives and go back to the last clean backup, but consequently lose many months of work. Most companies do not even have this option.
- Most companies decide to carry on fixing issues as they arise, but if they suffer problems it is difficult to tell whether or not they are related to the Sybil Logic Bomb. This creates uncertainty and loss of confidence in management teams.
- Consumers and industry becomes mistrustful of supplies and products. Some companies decide to recall all products manufactured since the installation of the upgrade, and refund customers.
- Trust in the corporate sector is damaged and stock prices fall.
- The resulting "information malaise" in the world economy caused by fear and uncertainty has an impact on productivity, confidence and consumption.

Phase 6 Rework

Each individual company carries out internal audits to establish what parts of their computer systems have been affected by the Logic Bomb. Many call in consultants to detect and analyze the problem. Data restitution is the priority. In extreme cases, some companies have to poll customers to rebuild data from scratch. Internal staff time is absorbed throughout the organization as IT departments scramble and senior managers attempt to minimize the impact on customers and business operations. Many companies re-install software and data systems, reconfigure firewalls and instigate new quality assurance measures at considerable expense. Legal counsel is brought in and consultants and staff spend time preparing a potential case for legal action against the perpetrator.

Losses occur from:

- Paying compensation to customers who have suffered a loss as a result of a data error in company records
- Legal proceedings from counterpart companies

- Class action law suits from customers
- Shareholder and analyst reactions in devaluing stock of affected companies

In Section 6 we discuss these losses in more detail.

Phase 7 Aftermath

Companies absorb most of the costs themselves. Although more than a third of major corporations have insurance policies that incorporate some protection against cyber crime losses, the number of medium and smaller companies that have insurance is less than 2%. Several individual companies affected face losses of over $100 million from lost revenues, shortfalls in assets, consultancy costs and extra expenses incurred for restitution and repair. The insurance recovery is less than 1% of the overall direct costs that result from the attack. Businesses hit by the virus take a long time to recover from the scale of the unexpected costs and the loss of revenues.

If the Sybil Corporation is seen to have handled the situation well they may suffer no more than reduced market share. If they didn't they will be the target of class actions.

New regulations are enacted aimed at improving quality control in software. Software companies are prohibited from hiding behind limited warranty clauses and this raises the cost of software by 20%.

In summary the algorithms that increasingly underpin modern decision support, trading, design and modelling systems will be undermined. Complicated problems will linger in global systems for years costing companies to sort out. Going forward, no one will be sure that the infection has been entirely eradicated, and it may never be declared to be formally fixed.

'Information Malaise'

We are calling this result of the scenario an "information malaise", where there is a reduced trust in IT by business leaders, investors and consumers. For example, people fall out of love with the internet as it is increasingly seen as unreliable and lawless; control of physical systems by SCADA is seen as too risky and the replacement of human business to business and business to consumer interaction by digital is seen as lacking necessary resilience. This is an opinion being arrived at by several thought leaders in the cyber arena – as the 2014 WEF report puts it, a future scenario of 'insecure growth' and 'digital disintegration'. [8]

6 Loss and Direct Impacts

The Costs to Companies of a Cyber Attack

Broadly the ways losses can be incurred by a company as a result of a cyber attack can be classified as

- Tangible Losses (Business Interruption, 3rd Party Liabilities and Penalties, Property Losses and Intellectual Property losses)
- Intangible Losses (Reputation losses)
- Operational costs (recovery, enhanced security)

In some cases losses may be insured by specialist cyber cover, in other cases by normal insurance cover.

Contingent business interruption

'Business Interruption' (BI) is traditionally linked with insurance policies for building damage – the insured property has to be damaged (by fire, flood etc.) for compensation to be paid. However companies are increasingly getting insurance coverage for loss of earnings due to failures in their communications, utilities or essential services even if their own property isn't damaged (known as 'Contingent BI'). Network issues are probably dominating their thinking in this context. In addition, insurers are beginning to offer more specific insurance products to cover network failures and virus infection. Some insurers see this as a major growth area however a recent BBC report stated how power companies are being refused insurance cover for cyber-attacks because their defenses are perceived as weak ('Energy firm cyber-defence is 'too weak', insurers say' [31]).

Loss Mechanisms

In this table we identify the range of possible loss mechanisms for the cyber threat and map each mechanism to an insurance coverage if one exists.

In Table 7 we take the lines of business of a typical insurance company and estimate impact on frequency of claims on each line of business as a result of the Sybil Logic Bomb scenario. Positive numbers indicate an increase in frequency of claims.

Type of Loss	Insurance Coverage
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 infomation	
Reputation Losses	
Goodwill	
Market Value	
Customer/Partner Confidence	
Operational costs	
Administrative and recovery	Extra Expense Insurance
Security activities	

Table 6: Loss mechanisms [32]

Class	Line of Business	
Property		
	Personal Lines/Homeowner	1
	Personal Contents	1
	Commercial Combined	0
	Construction & Engineering	0
	Commercial Facultative	2
	Binding Authorities	2
Casualty		
	Workers Compensation	1
	Directors & Officers	5
	Financial Lines	4
	General Liability	5
	Healthcare Liability	3
	Professional Lines	3
	Professional Liability	4
Auto		
	Personal Lines	0
	Commercial & Fleet	0
Marine & Specie		
	Cargo	0
	Marine Hull	0
	Marine Liability	0
	Specie	0
Aerospace		
	Airline	0
	Airport	2
	Aviation Products	2
	General Aviation	1
	Space	0
Energy		
	Downstream	2
	Energy Liability	2
	Onshore Energy & Power	2
	Upstream	0
Specialty		
	Accident & Health	0
	Aquaculture insurance	0
	Contingency - film & event	1
	Equine insurance	0
	Excess & Surplus	1
	Life Insurance	0
	Livestock	0

Class	Line of Business	
Life & Health		
	Life Insurance	0
	Health Insurance	0
	Income Protection	2
	Death & Disability	0
	Hospital Cover	0
Pension and Annuities		
	Standard Annuities	2
	Variable Annuities	0
	Enhanced Annuities	0
	Life Settlements	0
War & Political Risk		
	Kidnap & Ransom	0
	Political Risk	1
	Political Violence & Terrorism	0
	Product Recall	5
	Trade Credit	5
Agriculture		
	Multi-peril crop	0
	Crop hail	0
	Livestock	0
	Forestry	0
	Agriculture	0

Key to change in insurance claims	
Major decrease in claims	-5
	-4
	-3
	-2
	-1
No change in claims	0
	1
	2
	3
	4
Major increase in claims	5

Table 7: Exposures & Claim Impacts

Liability analysis

As an example of the way a liability claim might play out in the scenario we have considered the fictional case of a fictional fund manager, described earlier, that we call Standard Capital who suffers a huge trading loss where £440 million is lost in just 45 minutes of trading. The cause of this is their high speed trading algorithm taking operational parameters from its compromised Sybil database. The database is passing values 10% too high into the highly sensitive workings of the trading algorithm.

The sequence of events in the liability claim might be as follows:

- £440m incurred 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 seeks cover under their own Product Liability insurance

7 Macroeconomic Consequences

Methodology

- Our methodology for estimating the macro-economic impact of the Sybil Logic Bomb is founded on several key concepts:
- We use a selection of the market leading relational database vendors, to benchmark Sybil. We assume Sybil has about 50% market share worldwide, 300,000 business customers and their products are used by most of the companies in the corporate world.
- We use the Bloomberg Industry Leaderboard, a sample of 600 large companies chosen from a wide range of different industries. We estimate the impact of the Sybil Logic Bomb on these companies, and use them as representatives of the world of business.
- We employ the Global Industry Classification Standard (GICS) as a way to differentiate scenario impacts on different sectors of the world economy.
- We use expert judgment applied to each GICS sub-industry to attain an IT Business Process Criticality (BPC) score.
- We combine the BPC score with market penetration data to derive a Sybil Risk Score for the private sector.
- We model impact to the public sector by looking at government spending broken down by function.
- We use a General Equilibrium Model [6] to project quantitative macroeconomic impacts. A weighted average of Sybil Risk Scores gives national-level scores for major economies. These national scores dictate the relative severity of the shocks to the model's inputs.

Data collection

Our approach involves using the 600 Bloomberg Industry Leaderboard companies to represent "the world of business". We call this list of companies a Global Enterprise Network, and have determined that it represents about 25% of world GDP.

A range of additional data is collected about each of the companies, from Bloomberg Data Service [33], including revenue, locations of company headquarters and GICS classification.

Whereas traditional catastrophe modeling is based on the geographic footprint of the disaster, a cyber-catastrophe such as the Sybil Logic Bomb does not have a footprint defined by geography. Given that the attack is introduced through a trusted avenue as opposed to some weakness of network security, the presence of the logic bomb is defined by the presence or absence of Sybil software.

In order to establish the Sybil footprint, marketing data from leading relational database vendors is collected. This data allows us to create a realistic breakdown, by industry, of Sybil's market penetration [34]. The industries are then correlated with the GICS in order to give a market penetration percentage to each of the sub industries in the classification system. Thanks to the tree-like structure of the GICS, missing data for the sub-industries can be inferred from the higher classes.

The GICS market penetration data is uniformly scaled to form the Sybil Industry Penetration. The Sybil Industry Penetration gives the probability, as a percentage, of a company in a particular sub industry using Sybil software. This average-case probability, as opposed to a binary yes/no for each company, is sufficient for the subsequent steps in the modeling process.

The Sybil Industry Penetration forms one half of the Sybil Risk Score, and represents the likelihood of a company being affected by the Sybil Logic Bomb. To properly quantify the risk posed by a Sybil-type scenario, we also need to assess the magnitude of the impact to a company.

We have developed a scoring system called IT Business Process Criticality (BPC) in which a business or an industry group is scored according to the estimated business impact of the Sybil logic bomb. The BPC score ranges from 1 to 10. A BPC score of 1 means that Sybil technology is used in minor non-critical activities or in those activities where the logic bomb has no impact, i.e. transactional processes, for example payroll. The BPC score increases with the strategic importance of Sybil, with a score of 10 meaning it is used in every aspect of the core business processes, see Table 8.

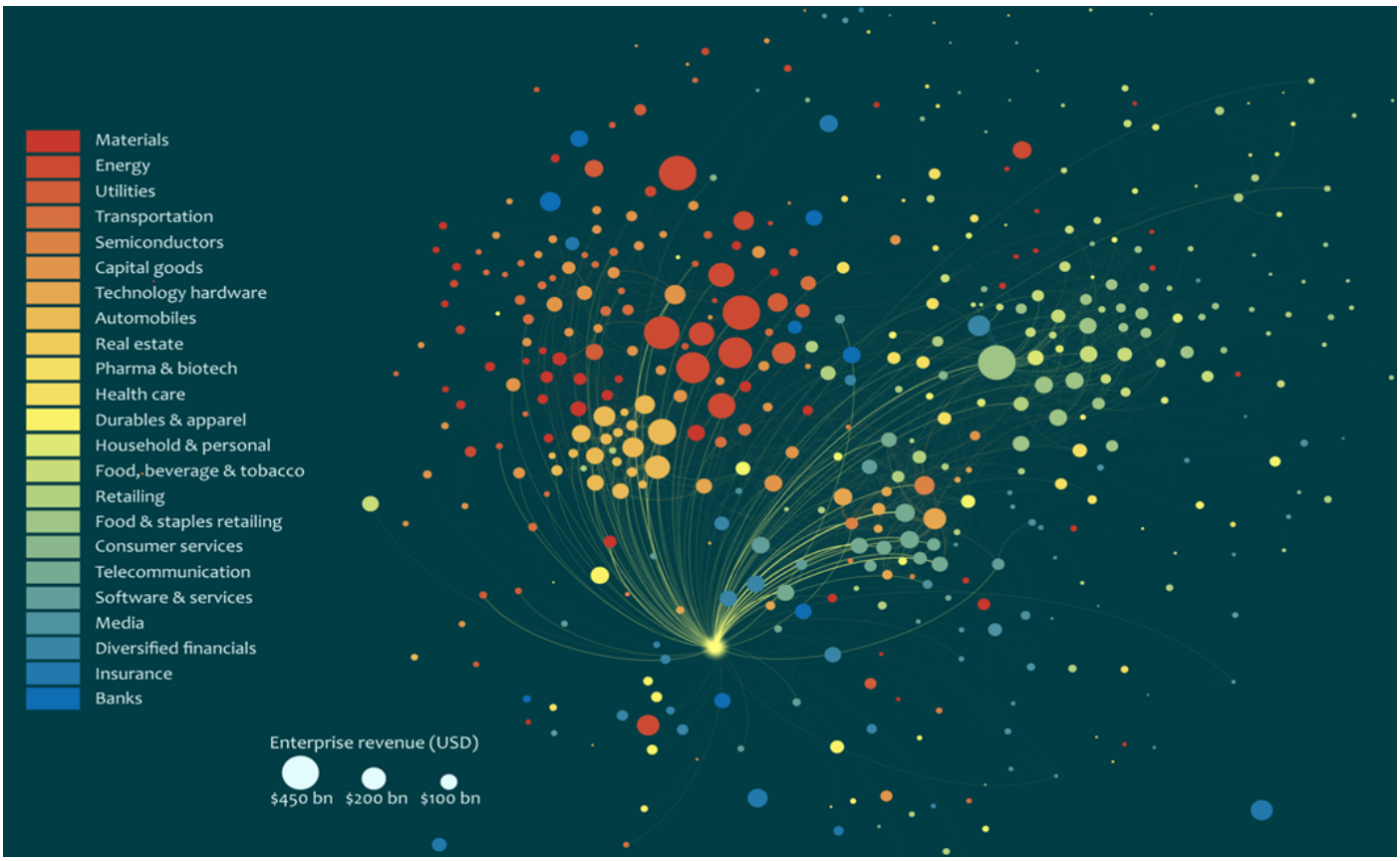


Figure 6: Mapping the Cyber Economic: 600 companies by GICS industry group

Score	Definition
1	Minor use
2	Used for minor administrative tasks
3	Used for many administrative tasks
4	Used for all main company administration and 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

Table 8: Sybil Business Process Criticality (BPC)

We developed this metric by individual analysis of the 150 GICS sub industries, using expert judgment to create the score.

We also studied government functions, as defined by the UN System of National Accounts [4] and gave each of these functions a BPC score.

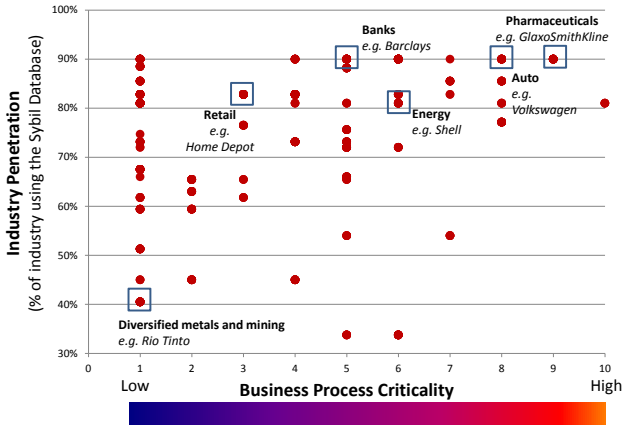


Figure 7: Industry sector scoring (GCIS Sub-industry classification) of penetration and criticality

Quantification of risk

The scatter plot in Figure 7 shows the industry penetration on the vertical access against Business Process Criticality on the horizontal. Each point in this plot is a GICS sub industry.

We combine the Sybil Industry Penetration with the Business Process Criticality to give us a Sybil Risk Score for each industry, which is assigned to each of the companies in said industry. Thus we arrive at a score for each of the 600 companies in our Global Enterprise Network.

Consider, for example the "Diversified Metals and Mining" sub industry. Companies in this sub industry are unlikely to use Sybil in their core business activity e.g. a database failure is unlikely to seriously affect a company like Rio Tinto's ability to mine titanium in Australia. Consequently, this sub industry has a BPC score of 1. This sub industry also happens to have the lowest market penetration, so the impact predicted for the companies within this sub industry is low.

In the case of a pharmaceutical company, like for example GlaxoSmithKline – where there is a long tradition of using relational databases in clinical trials – a long running corruption of GSK's systems could be very damaging for the business as a whole: a problematic drug going on the market would create large losses in terms of product recall, liability claims and reputation damage. Because databases are so core to their business processes, pharmaceutical companies get a BPC of 9. A high penetration figure for the sub industry combined with the BPC of 9 will result in a high impact on pharmaceutical companies.

The Sybil Risk Score is multiplied by the company's revenue to give a 'Revenue at Risk' figure. The Revenue at Risk is a measure of the potential negative impact to the economy of the Sybil catastrophe, as contributed by each company in the Global Enterprise Network.

General Equilibrium Global Economic Model

We use a computable general equilibrium (CGE) global economic model [6]. It contains a detailed database with the historical values of many economic variables and equations describing the interactions between them. CGE models are suited to analyzing the impact of future policy changes or, as in the case of catastrophe modeling, shocks to the economy from an exogenous source.

Aggregation to country level

The global economic model uses variables defined at national level – it would not be tractable to try to model companies individually. Shocks to the economy therefore need to be defined at the resolution of nations, and so the Revenue at Risk figures must undergo an aggregation process.

A national score is produced by taking the sum of the Revenue at Risk figures for companies headquartered in a country, and then dividing that figure by the total revenue of those companies. The average of all the national scores is calculated, and then each country is given a scaling factor, defined as the ratio of the country's score to the average. This averaging process, combined with that detailed below for the public sector, allows us to design shocks to the CGE model for a theoretical "average economy" and modify them according to the characteristics of each nation's economy.

Public sector

The GICS classification does not include the public sector, but we use the same methodology to produce a simple estimate of impacts to the public sector. A score is compiled by looking at the breakdown of public spending by function. Categories are taken from the UN SNA93 [4]. Those governments whose spending (as a proportion of GDP) is more concentrated in functions with a high BPC are given a higher score.

We assume a constant penetration of Sybil technology across all governments and apply a Business Process Criticality to each of the government functions, as in the case of the GICS sub industries. In place of company revenue, we use government spending as a proportion of GDP. As the public accounts are represented at national level already, there is no aggregation process. Data is collected from a variety of sources, including the OECD [35], the U.S. GPO [36], the U.S. Census Bureau [37] and Statistics Canada [38]

In a manner parallel to that used for the private sector, scores are once again calculated as a ratio to the mean.

We now combine the private and public sector data. The scaling factor from the Revenue at Risk calculations is combined with the government spending score to produce a Harm Scaling Factor (HSF) for each country. The HSF defines the relative harm experienced by the countries modeled.

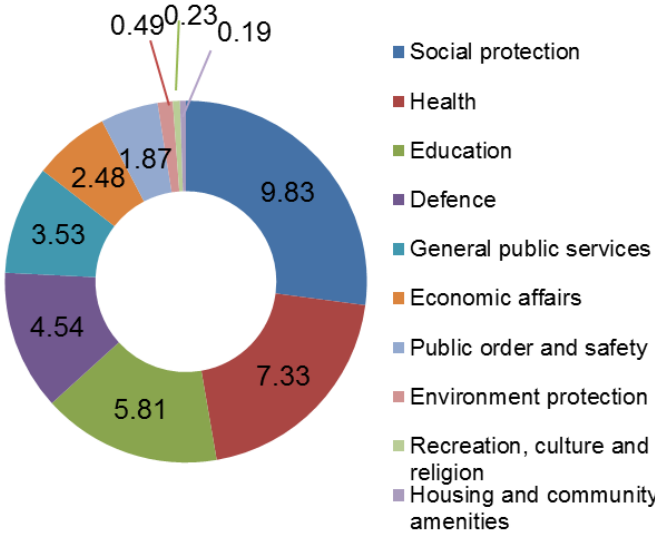


Figure 8: U.S. government spending breakdown

Shocking the model

We shock the global economic model through three key inputs: productivity, confidence (represented by the share price index) and consumption. When the Sybil Logic Bomb is in its latency stage, companies' data are being subtly corrupted without their knowledge. This is likely to impact their productivity – it has been shown that IT is strongly linked to productivity [39] and a lessening of its efficacy would slow this trend. The errors introduced by the Sybil Logic Bomb would lead to a variety of tangible effects on companies. These effects include increased recall of items, customer refunds and associated reputation recovery. These consequences, endemic to such a large number of companies, will in turn lead to reduced investor confidence and a decrease in share prices. Finally, upon discovery of the bug, consumer confidence will be hit, leading to a decrease in consumption.

The following graphs (Figure 9, Figure 10 and Figure 11) show the generic profile of the shocks to the three variables, with the different scenario variants visible in different colors. S1, S2 and S3 are simple variants in which the magnitude of all shocks is scaled by factors of 1, 1.5 and 1.75 respectively.

Scenario X1 is a more extreme variant which uses the same shocks as S3 but includes a longer latency period in which the bug goes undetected. These generic shock profiles are then modified by each country's Harm Scaling Factor before being input to the model.

Model outputs

The global economic model is run with the inputs specified by the scenario, modified according to each country's Harm Scaling Factor. The output from the model is a 5-year forecast for the world economy. This process is repeated for each of the four scenarios.

The primary figure produced is the world gross domestic product at risk, or GDP@Risk. The GDP@Risk is the total difference in GDP between the baseline projections and the scenario-adjusted projections. The figure is calculated over a 5-year window, beginning in the quarter during which the first shock is applied. The results can be seen in Table 9, where the S1 scenario produces a 5 year GDP@Risk of $4.5 trillion.

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

Table 9: GDP@Risk for the four Sybil Logic Bomb Scenario Variants

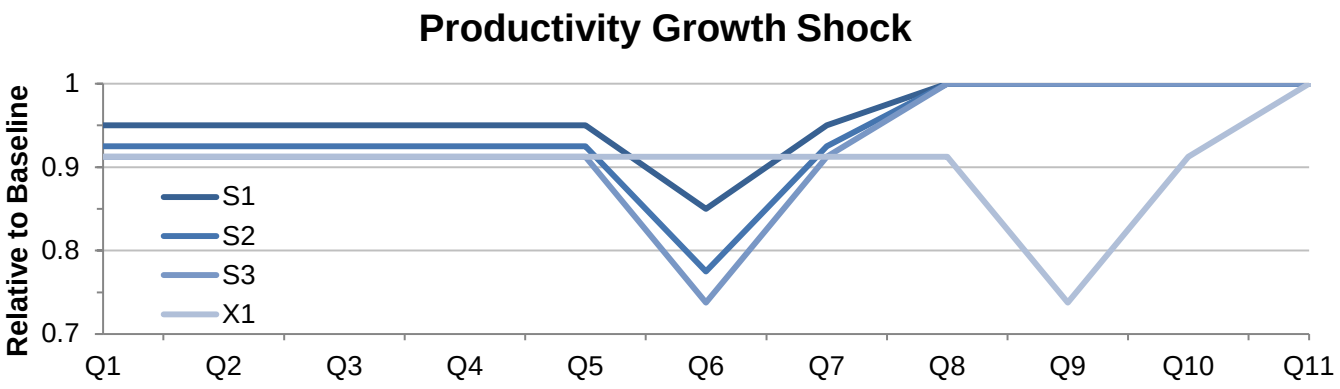


Figure 9: Productivity Growth Input Shock

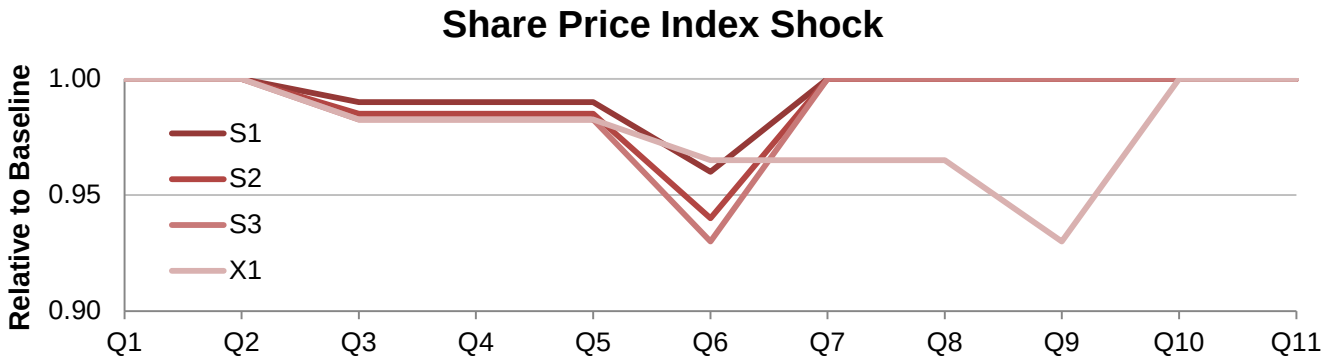


Figure 10: Share Price Index Input Shock

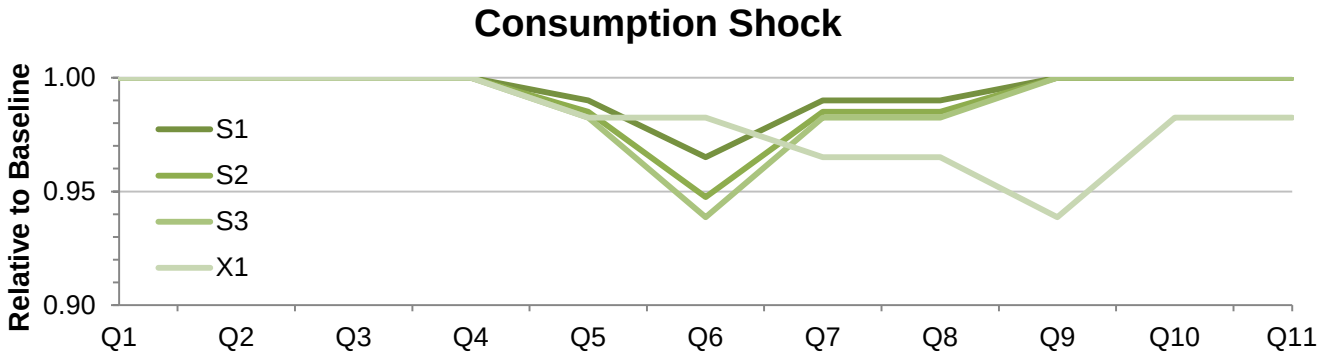


Figure 11: Consumption Input Shock

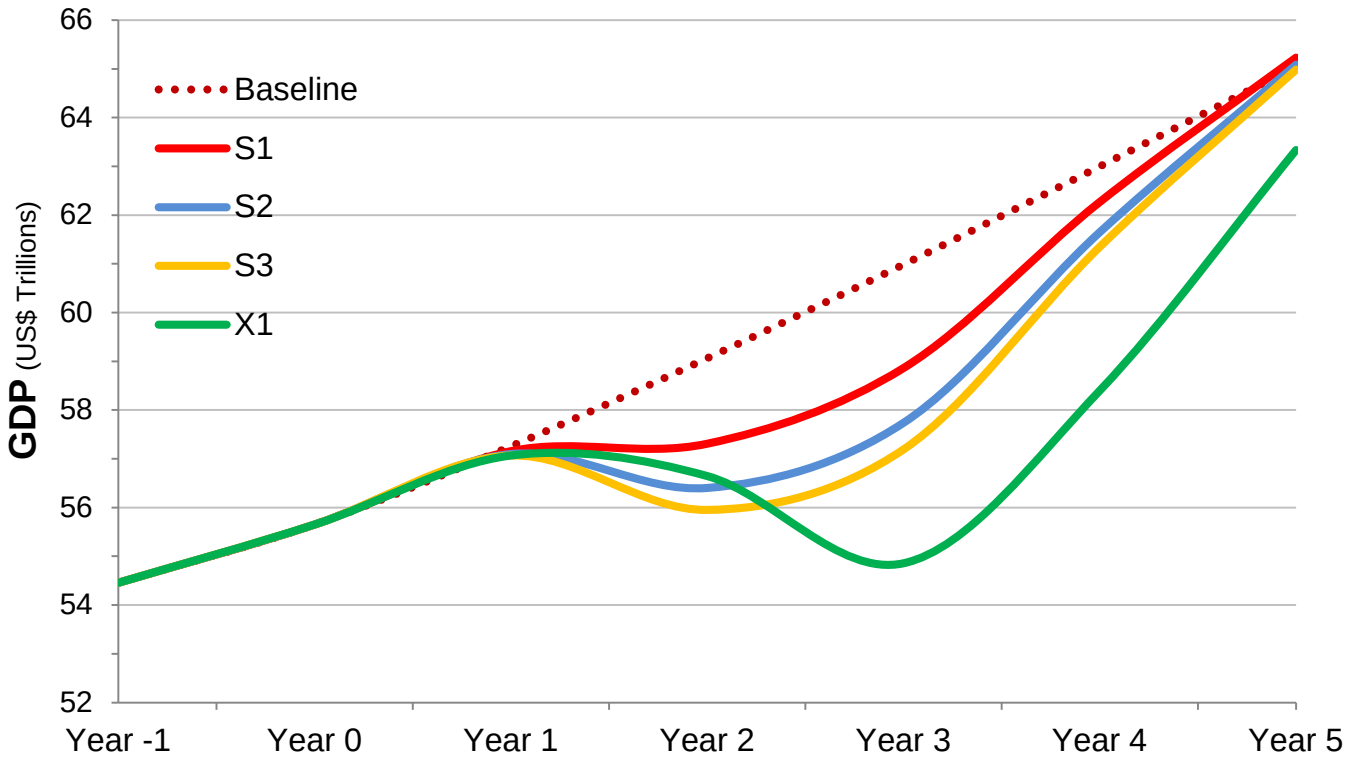


Figure 12: Estimated loss in global output as a result of the Sybil Logic Bomb scenario: World 'GDP@Risk'

8 Impact on Investment Portfolios

We assess the performance of a typical high quality investment portfolio under the Sybil Logic Bomb scenario. We build a fictional representative portfolio that mimics some features observed in the investment strategies of insurance companies – a high-quality fixed-income portfolio with about 85% of investments in sovereigns and corporate bonds most of which rated A or higher. Investments are spread across countries like the US, UK, Eurozone and Japan. Equities compose about 10% of the investment portfolio. In the following we will assume for simplicity that equity investments correspond to investments in stock indexes. We 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 are shown in Table 10.

	USD	GBP	Euro	Yen	Other	Total
Government medium/short	6%	5%	4%	2%	3%	20%
Government long	8%	7%	5%	2%	2%	24%
Cash	2%	1%	1%	0%	1%	5%
AAA medium/short	2%	2%	2%	1%	1%	8%
AAA long	4%	3%	1%	1%	1%	10%
AA medium/short	1%	1%	1%	0%	0%	3%
AA long	2%	1%	1%	0%	2%	6%
A long	2%	2%	2%	2%	0%	8%
BBB and lower	2%	2%	1%	0%	1%	6%
Equities	2%	2%	2%	0%	4%	10%
Total	**31%**	**26%**	**20%**	**8%**	**15%**	**100%**

Table 10: Composition of the representative portfolio

The capital gain is computed from bond yields as

$$g_b(t) = -D_b\,[y_b(t) - y_b(t-1)]$$

where $-D_b$ is the bond duration, for which we assumed the following values: D_b=7 for ten years bonds, D_b =1.8 for two years bonds and D_b=0.4 for bonds with maturity of three months. In our analysis we assume no default on sovereign bonds, while defaults on corporate bonds are accounted for through the introduction of a discount factor that calibrated to obtain in the baseline scenario the default probabilities shown in Table 11.

For the stressed scenarios we arbitrarily assumed default probabilities to increase by a factor 3 (the qualitative pattern of the results here discussed are robust with respect to changes of this parameter).

For the stressed scenarios we arbitrarily assumed default probabilities to increase by a factor 3 (the qualitative pattern of the results here discussed are robust with respect to changes of this parameter).

	Credit spread (bp)	Default probability
AAA medium/short	16	0.52%
AAA long	68	0.52%
AA medium/short	37	0.52%
AA long	80	0.52%
A long	51	0.29%
BBB and lower	95	2%

Table 11: Credit spreads and default probabilities for corporate bonds

Stock returns are computed as

$$r_s(t) = y_S(t) + g_s(t)$$

Where $y_S(t)$ is the dividend yield of stock s and $g_s(t)$ its capital gain.

The latter is computed from the stock price $p_s(t)$ as

$$g_s(t) = \frac{p_s(t) - p_s(t-1)}{p_s(t-1)}$$

The macro-economic model produces a forecast for dividend yields of UK stocks, that we assume to be similar to those of US and Eurozone stocks.

The return on the whole portfolio is then computed taking a weighted sum over the returns of all assets.

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 which to compare the performance of dynamical strategies.

Understanding what drives the behavior of the fixed portfolio at different times gives useful insight towards the design of an optimal investment strategy.

Results

Results of our analysis are presented in Figure 13, Figure 14, Figure 15 and Figure 16. In Figure 13 we plot, for the different variants of the scenario, the percentage change of portfolio returns with respect to the baseline. In all cases we observe significant departures from the baseline. The investment portfolio under the Sybil Logic Bomb scenario overall underperforms with respect to the baseline, with negative peaks as large as -1.8% per quarter. Interestingly, we observe that under the most extreme variant of the scenario the investment portfolio even registers higher returns with respect to the baseline in year 5.

A better estimation of the overall performance of the investment portfolio is represented in Figure 14, where we plot as a function of time the percentage change with respect to the baseline of cumulative returns. The cumulative return at time t is simply computed as the sum of returns up to that time.

The last part of our analysis is devoted to understanding the impact of the scenario on different asset classes. The aim is to show how performance varies across different groups of assets.

The summary of this analysis performed for the S1 (less extreme) variant of the scenario can be found in Figure 15 and Figure 16. In Figure 15, we present a breakdown of investments by geographical areas. From the figure we see that investments in the UK and Eurozone are characterized by larger deviations in profit and losses with respect to the baseline.

Figure 16 represents a breakdown with respect to the fixed-income and equities. In particular, from the plot we can see that profit and losses on equities relative to baseline are much higher than those for fixed-income investments.

Similar conclusions concerning the importance of different groups of assets can be drawn for the other variants scenario.

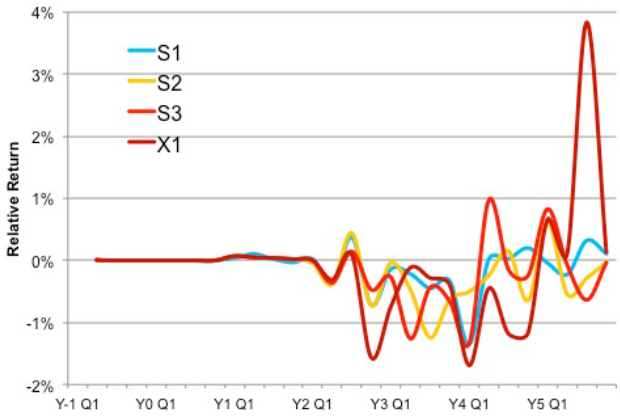


Figure 13: Percentage change with respect to baseline of portfolio returns under different scenarios.

In all cases the investment portfolio is underperforming the benchmark in the short term. Increasing the severity of the macro-economic shock increases the amplitude of the deviation from the baseline.

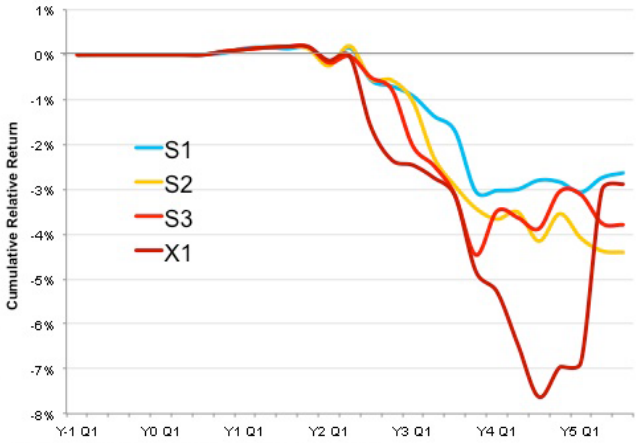


Figure 14: Relative change of cumulative returns with respect to baseline.

In all variants, investment portfolios display losses with respect to the baseline. Even in the less extreme scenario, cumulative losses with respect to baseline amount to 15% at the end of the simulation.

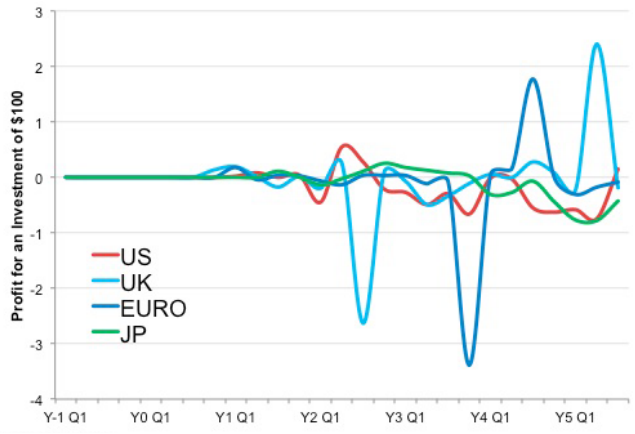


Figure 15: Relative return of a $100 investment in different geographical areas.

Figure 16: Relative return of a $100 investment in fixed income and equities.

Equities register bigger losses both in the short and long term.

Summary of investment portfolio analysis

In this part of the scenario analysis we have taken the output from the macro-economic model and used it as an input to assess the performance of a representative investment portfolio of an insurance company. We have estimated the performance of the portfolio under the different variants of the Sybil Logic Bomb scenario and compared it with the business as usual performance.

Under all variants of the scenario here considered, the investment portfolio registered losses with respect to the baseline benchmark. In the short term (12-18 months), cumulative losses are small. More significant losses are registered in the longer, where cumulative losses can be of 8% for the most extreme variant of the scenario see Table 12.

An important issue that we have not addressed in our analysis is that of systematically testing the stability of the results with respect to the parameter settings used in the earlier stages of the scenario development. This is to a certain degree taken into account in the fact that we considered different variants of the scenario, but a more systematic analysis will be needed in this respect.

Scenario	Cumulative loss from baseline: short-term	Cumulative loss from baseline: long-term	Short-term maximal loss from baseline
S1	0.5%	3%	1%
S2	0.5%	3.5%	1%
S3	0.5%	4.5%	1.2%
X1	2%	8%	1.5%

Table 12: Summary of results on estimate of losses with respect to baseline

Table 13 summarises some of the macro-economic indicators output by the Global Economic Model, which can be useful inputs to investment modeling systems.

REAL USD PERCENTAGE VALUES				Baseline	Short-Term Impact (Δ Max)					Long-Term Impact (Δ 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)	Δ	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)	Δ	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)	Δ	0.3	0.032	0.035	0.037	0.037		0.01	-0.02	-0.05	-0.04
Inflation	USA CPI	Consumer price index	%	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	Δ	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	Δ	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	Δ	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
EU (Germany)													
Bonds Short	DEM 2Y	Interest rate, 2-year German gov bond yields	Δ	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	Δ	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	Δ	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	Δ	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	Δ	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	Δ	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

Table 13: Short term and long term impact on representative portfolio assets from all cyber scenario variants

9 Consequences and Mitigations

What are the consequences to companies and broader society likely to be from the particular catastrophe exemplified by the Sybil Logic Bomb?

Global economic recession

There would be a global recession, but not as bad as the recent credit crunch. The Sybil Logic Bomb scenario shows a modeled impact for the S1 variant on the global economy of about $5 trillion on our scale of 5 year GDP@Risk. By comparison, the Great Financial Crisis of 2007-2008 at 2014 prices measures $20 trillion.

Shift in investment portfolio holdings

Our analysis of our representative investment portfolio shows that during the Sybil catastrophe UK and Europe investments are riskier compared to the US.

Regulation of SITEs

In the aftermath of Sybil it is likely that Systemically Important Technology Companies would be regulated. This would have significant impact to the way those companies operate. Software limited warranties would be ruled out. Regulation would increase the cost of their products and services with resulting impact on the costs in business processes based on their technology.

Regulation would likely fundamentally change the Open Source movement. The Heartbleed Bug revealed that a systemically important technology, OpenSSL, used by half the web sites in the world, was developed and maintained by a small band of underfunded volunteers [40]. This kind of arrangement would be ruled out by regulation, and inevitably the 'free' would be taken out of Open Source.

Cloud vendors, and maybe even data held in the cloud, would be similarly regulated.

The end of society's love affair with technology

In the years after Sybil, society may never return to the unquestioning love of technology it had before the "information malaise". The internet would be seen as unreliable and lawless; control of physical systems by SCADA would be seen as too risky; and the replacement of human business to business and business to consumer interaction by digital lacking necessary resilience. This vision of the future has been arrived at by several thought leaders in the cyber area – a scenario of "digital disintegration", as the 2014 WEF report puts it [7].

Impact on the public sector

Our analysis shows that the Sybil Logic Bomb scenario has a low direct impact on the public sector compared to the private sector. Although government spending in many countries accounts for a significant proportion of GDP the effect of the scenario is low in the GDP@Risk analysis. However the line of distinction between public and private sector is blurred as in many cases public sector functions and critical infrastructures are outsourced to private companies.

Growth in liability risk

Claims for liability will be the key mechanism by which losses will be recovered by individuals and organizations who have suffered from the Sybil catastrophe. Shareholders would sue Director and Officers for loss of share value due to poor quality assurance procedures and failing to spot problems being caused by Sybil. The fact that Sybil may have been active in an organization for many months without being discovered will be key to this. Increased claims can be expected under Directors and Officers (D&O) insurance cover.

Mitigation

What could companies and broader society have done to mitigate the particular risk exemplified by the Sybil Logic Bomb?

IT Departments and Corporate IT Policy are always going to be the first line of defense against Cyber threat. The threat from Sybil would have been reduced by:

- Not being too quick to upgrade
- Reporting near misses: Not letting unexplained errors go unresolved.
- Dual-source technologies: For example two databases from different vendors mirroring each other; if this is not possible, mirroring two different versions of the same database.
- Plug swappable technologies: Be able to quickly swap one software module for another. This is commonplace with hardware, not so much with software.
- Not being over-seduced by standardization initiatives
- Techniques to provide better defense against insider attack

At a corporate level, reputation management would be crucial to dealing with Sybil. The way a company deals with perceived failings in its products and services, or those of a supplier, due to Sybil, or even not due to Sybil, will be vital. There are plenty of examples in the recent past of organizations who have survived major failings – for example Toyota has recalled 20 million vehicles in the past two years [41] – however manage their reputation well and even turn it to competitive advantage.

Good supply chain management would help to mitigate problems occurring due to Sybil in suppliers and partners, and good practice in disaster recovery would also help companies in the aftermath.

Rethinking business processes

How might companies rethink their business processes in light of the experience of the Sybil Logic Bomb catastrophe?

- Dual Sourcing Technology: Dual sourcing is already an established good practice in physical supply chains – this thinking could be extended to IT systems where alternative software and hardware technologies can be easily swapped in and out in the same way an underperforming supplier can be changed for another.
- Resilience against "digital disintegration": Consider supplementing digital with the physical. Organizations that can fall back in moments of crisis on alternatives to technology are going to be more resilient.

10 Bibliography

Recommended Further Reading

Clarke, Richard, A. and Knake, Robert; 2012; Cyber War: The Next Threat to National Security and What to Do about It, Ecco; ISBN-10: 9780061962240.

Healey, Jason; 2013; A Fierce Domain: Conflict in Cyberspace 1986 to 2012; Cyber Conflict Studies Association; ISBN-10: 098932740X

Mandrila, Eugen; 2013; Cyber Crimes in a Globalized World: Country Profiles, Rankings, Patterns & Risks, BNR ISBN; ISBN-10: 9730145806

Rid, Thomas; 2013; Cyber War Will Not Take Place; C Hurst & Co Publishers Ltd; ISBN-10: 1849042802

Sommer, Peter; and Brown, Ian; 2011; Reducing Systemic Cybersecurity Risk , OECD/IFP Project on "Future Global Shocks"; IFP/WKP/FGS(2011)3

US GAO; 2012; Cybersecurity: Threats Impacting the Nation; United States Government Accountability Office; Statement of Gregory C. Wilshusen, Director Information Security Issues, GAO-12-666T

World Bank; 2014; Database of indicators; http://data.worldbank.org/indicator/FI.RES.TOTL.CD

Other Related Reading

Data Loss DB; DataLossDB is a research project aimed at documenting known and reported data loss incidents world-wide.

DBIS; 2012; 10 Steps to Cyber Security – Executive Companion; Department for Business, Innovation & Skills, Cabinet Office, UK Government.

DBIS; 2012; Cyber risk management: a board level responsibility; Department for Business, Innovation & Skills, Cabinet Office, UK Government.

DBIS; 2012; Cyber security guidance for business; Department for Business, Innovation & Skills, Cabinet Office, UK Government.

Duggan, David P.; Thomas, Sherry R.; Veitch, Cynthia K. K.; and Woodard, Laura; 2007; Categorizing Threat: Building and Using a Generic Threat Matrix; Sandia Report; SAND2007-5791

Greisiger, Mark; 2013; Cyber Liability and Data Breach Insurance Claims: A Study of Actual Claim Payouts; NetDiligence.

Hu, Yu-Wei; 2010; Management of Chinas Foreign Exchange Reserves: A Case Study on the State Administration of Foreign Exchange (SAFE), European Commission Economic Papers 421.

Kirilenko, Andrei; Samadi, Mehrdad; Kyle, Albert S.; Tuzun, Tugkan;2011; 'The Flash Crash: The Impact of High Frequency Trading on an Electronic Market'; ('Flash Crash of 2:45' Unexplained 9% drop, US Stock Market 6th May 2010);

Lloyd's, 2010; Managing Digital Risk: Trends, issues and implications for business; Lloyd's 360 Risk Insight.

Mateski, Mark; Trevino, Cassandra, M.; Veitch, Cynthia, K.; Michalski, John; Harris, J. Mark; Maruoka, Scott; Frye, Jason; 2012; Cyber Threat Metrics; Sandia National Laboratories Report SAND2012-2427

Sommer, Peter; and Brown, Ian; 2011; Reducing Systemic Cybersecurity Risk , OECD/IFP Project on "Future Global Shocks"; IFP/WKP/FGS(2011)3

US GAO; 2012; Cybersecurity: Threats Impacting the Nation; United States Government Accountability Office; Statement of Gregory C. Wilshusen, Director Information Security Issues, GAO-12-666T

World Bank; 2014; Database of indicators; http://data.worldbank.org/indicator/FI.RES.TOTL.CD

Works Cited

[1] M. Tuveson and S. Ruffle, "Diversity is the way to avoid cyber collapse," Financial Times, 28 April 2014.

[2] A. A. Friedman, A. Mack-Crane and R. A. Hammond, "Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences," Brookings Institution, 2013.

[3] Bloomberg, "Bloomberg Industry Leaderboard," [Online]. Available: http://www.bloomberg.com/visual-data/industries/q/market-leaders. [Accessed January 2014].

[4] United Nations, "System of National Accounts '93," 1993. [Online]. Available: https://unstats.un.org/unsd/nationalaccount/sna1993.asp. [Accessed May 2014].

[5] MSCI, "Global Industry Classification Standard (GICS®)," [Online]. Available: http://www.msci.com/products/indexes/sector/gics/. [Accessed May 2014].

[6] Oxford Economics, "Global Economic Model Overview," Oxford Economics, 2014. [Online]. Available: http://www.oxfordeconomics.com/forecasts-and-models/countries/scenario-analysis-and-modeling/global-economic-model/overview. [Accessed 08 May 2014].

[7] Center for Strategic and international Studies, "Net Losses: Estimating the Global Cost of Cybercrime," Intel Security, Santa Clara, CA. USA, 2014.

[8] World Economic Forum, "Global Risks Report," [Online]. Available: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf. [Accessed 8 May 2014].

[9] Detica / Cabinet Office, "The Cost of Cybercrime," [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf. [Accessed 8 May 2014].

[10] Anderson, Barton, Bohne, Clayton, v. Eeten, Levi, Moore and Savage, "Measuring the Cost of Cybercrime," 2012. [Online]. Available: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf. [Accessed 08 May 2014].

[11] US Securities and Exchange Commission, "CF Disclosure Guidance," [Online]. Available: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. [Accessed 8 May 2014].

[12] ENISA, "Incentives and barriers of the cyber insurance market in Europe," June 2012. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport. [Accessed 08 May 2014].

[13] Ponemon Institute, "2012 Cost of Cyber Crime Study: United States," [Online]. Available: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6 .pdf. [Accessed 08 May 2014].

[14] L. Ablon, M. C. Libicki and A. A. Golay, "Markets for Cybercrime Tools and Stolen Data," 2014. [Online]. Available: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf. [Accessed 08 May 2014].

[15] Mandiant Corporation, "APT1: Exposing One of China's Cyber Espionage Units," [Online]. Available: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. [Accessed 08 May 2014].

[16] BBC, "China denounces US cyber-theft charges," 20 May 2014. [Online]. Available: http://www.bbc.co.uk/news/world-us-canada-27477601. [Accessed 20 May 2014].

[17] HP Information Security, Checkpoint, Ponemon Institute, "Security Effectiveness Framework Study," [Online]. Available: http://h71028.www7.hp.com/enterprise/downloads/software/Security Effectiveness Framework Study.pdf. [Accessed 08 May 2014].

[18] U.S. Attorneys' Office for the Eastern District of New York, "Putting a Face On It," [Online]. Available: http://s3.documentcloud.org/documents/698765/from-the-u-s-attorneys-office-putting-a-face-on.pdf. [Accessed May 2014].

[19] K. Slavin, "How Algorithms Shape Our World," [Online]. Available: http://www.ted.com/talks/kevin_slavin_how_algorithms_shape_our_world. [Accessed 08 May 2014].

[20] É. P. Leverett, "Quantitatively Assessing and Visualising Industrial System Attack Vectors," June 2011. [Online]. Available: http://www.cl.cam.ac.uk/~fms27/papers/2011-Leverett-industrial.pdf. [Accessed December 2013].

[21] Duggan, Berg, Dillinger and Stamp, "Penetration Testing of Industrial Control Systems," Sandia National Laboratories, 2005.

[22] "The Cost of Bad Data," 06 March 2013. [Online]. Available: http://c3integrity.com/blog/posts/the-cost-of-bad-data. [Accessed January 2014].

[23] D. Kriesel, "Xerox scanners/photocopiers randomly alter numbers in scanned documents," 2013. [Online]. Available: http://www.dkriesel.com/en/blog/2013/0802_xerox-workcentres_are_switching_written_numbers_when_scanning?. [Accessed January 2014].

[24] N. Popper, "Flood of Errant Trades Is a Black Eye for Wall Street," New York Times, 1 August 2012. [Online]. Available: http://www.nytimes.com/2012/08/02/business/unusual-volume-roils-early-trading-in-some-stocks.html. [Accessed January 2014].

[25] N. Popper, "Knight Capital Says Trading Glitch Cost It $440 Million," New York Times, 02 August 2012. [Online]. Available: http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/. [Accessed January 2014].

[26] Reuters, "AstraZeneca reaffirms outlook after mistaken release," 9 January 2012. [Online]. Available: http://uk.reuters.com/article/2012/01/09/uk-astrazeneca-idUKTRE8080BX20120109. [Accessed May 2014].

[27] J. Mitchel and e. al, "Evaluation of Data Entry Errors and Data Changes to an Electronic Data Capture Clinical Trial Database," 2011. [Online]. Available: http://www.targethealth.com/PDF/Home/01_DIJ_45(4)_2612_421-430_2011.pdf. [Accessed May 2014].

[28] P. Kelso, "London 2012 Olympics: lucky few to get 100m final tickets after synchronised swimming was overbooked by 10,000," The Telegraph, Jan 2012. [Online]. Available: http://www.telegraph.co.uk/sport/olympics/8992490/London-2012-Olympics-lucky-few-to-get-100m-final-tickets-after-synchronised-swimming-was-overbooked-by-10000.html. [Accessed May 2014].

[29] EuSpRIG, "EuSpRIG Original Horror Stories," 2012. [Online]. Available: http://www.eusprig.org/stories.htm#spreadsheetoperatorerror. [Accessed May 2014].

[30] M. Abrams and J. Weiss, "Malicious Control System Cyber Security Attack Case Study–," 2008. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf. [Accessed May 2014].

[31] BBC, "Energy firm cyber-defence is 'too weak', insurers say," BBC, 27 February 2014. [Online]. Available: http://www.bbc.co.uk/news/technology-26358042. [Accessed 08 May 2014].

[32] Airmic, "Airmic Review of Recent Developments in the Cyber Insurance Market," Airmic, 2012.

[33] Bloomberg Data Service, Bloomberg, 2014.

[34] Oracle, "Consumer Goods Overview," Oracle, 2014. [Online]. Available: http://www.oracle.com/us/industries/consumer/overview/index.html. [Accessed February 2014].

[35] OECD, "National Accounts at a Glance 2013," 2013. [Online]. Available: http://www.oecd-ilibrary.org/economics/national-accounts-at-a-glance-2013/general-government-expenditure-by-function_na_glance-2013-19-en;jsessionid=1g8mvziavigos.x-oecd-live-03 [Accessed May 2014].

[36] U.S. Government Printing Office, "BUDGET OF THE UNITED STATES GOVERNMENT," 2014. [Online]. Available: http://www.gpo.gov/fdsys/browse/collection.action?collectionCode=BUDGET. [Accessed 2014].

[37] U.S. Census Bureau, "State and Local Government Finances," 2013. [Online]. Available: http://www.census.gov/govs/local/. [Accessed April 2014].

[38] Government of Canada, "Consolidated government revenues and expenditures," 2009. [Online]. Available: http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/govt48b-eng.htm. [Accessed April 2014].

[39] E. Brynjolfsson and L. M. Hitt, "Computing Productivity: Firm-Level Evidence," MIT Sloan Working Paper No. 4210-01, 2003.

[40] S. Marquess, "Speeds and Feeds: Of Money, Responsibility, and Pride," 2014. [Online]. Available: http://veridicalsystems.com/blog/of-money-responsibility-and-pride/. [Accessed 14 May 2014].

[41] E. Haslett, "Toyota recalls hit 20 million after latest round," Management Today, 18 October 2013. [Online]. Available: http://www.managementtoday.co.uk/news/1217011/toyota-recalls-hit-20-million-latest-round/. [Accessed 15 May 2014].