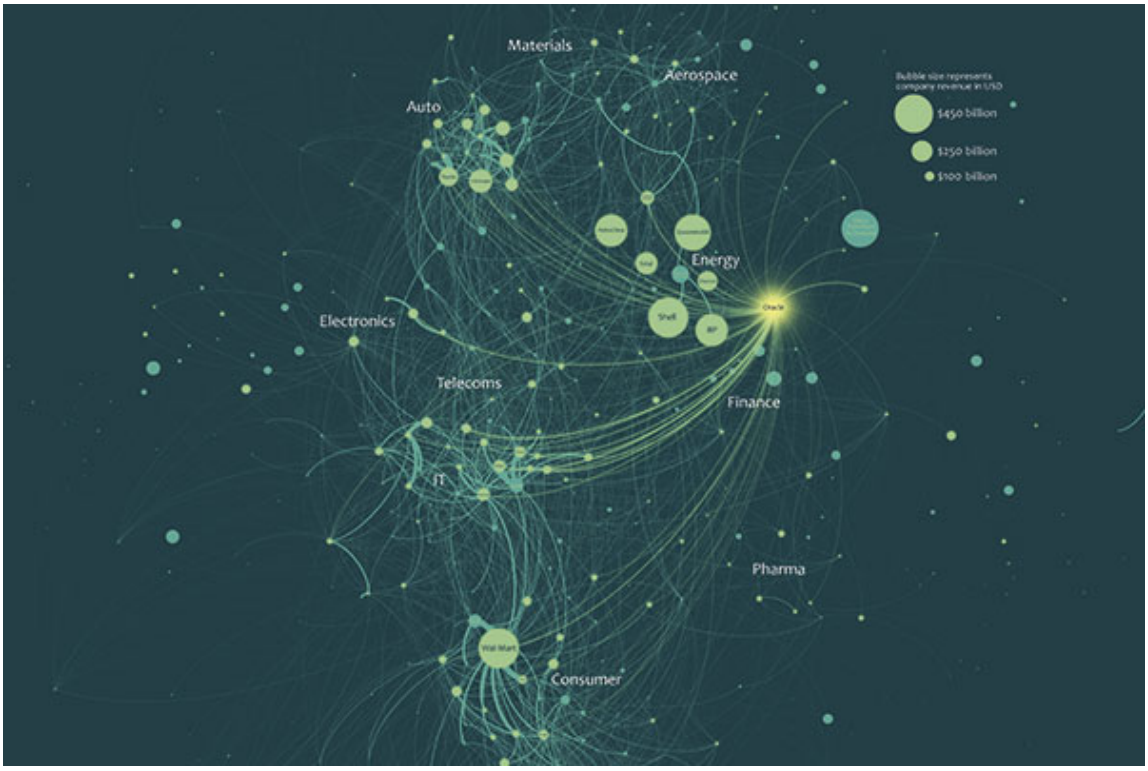
Cyber Catastrophe

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

04 DECEMBER 2014 | ANDREW COBURN, SIMON RUFFLE AND LOUISE PRYOR



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

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

Insurers are still reluctant to offer commercial

Mapping the cyber

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

economy enables risk modelling of systemically important IT providers

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

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

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

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

Geography of cyber economy

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

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

The technology companies that provide these common IT platforms have become so

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

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

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

The size of the attack

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

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

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

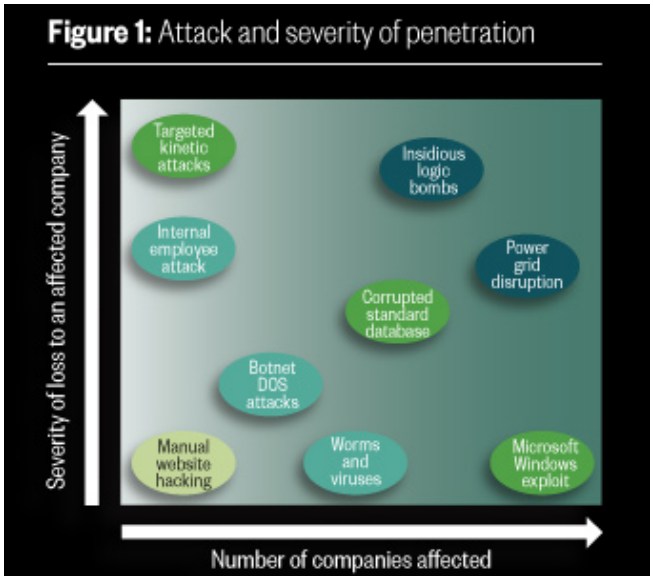
The exact mechanisms for potential failures are less important than the penetration levels of common IT applications, and there are various types and severity levels that could result from different types of technology failures. While many cyber attacks to date have not been malicious – data compromises,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

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

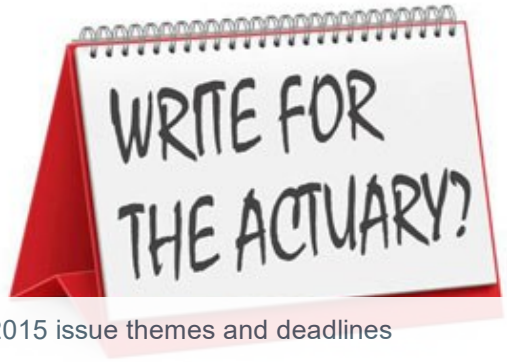
Cyber catastrophe is a concentration risk. Companies need to employ a robust diversification strategy to mitigate this risk to their business. By reducing the reliance on 'industry standard' software applications with diversity and competition in IT providers, companies can be better fortified against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

Andrew Coburn is senior vice-president at RMS.

Simon Ruffle is director of technology research and innovation, and Louise Pryor is a risk researcher, both at the Cambridge University Centre for Risk Studies



EDITOR'S CHOICE



2015 issue themes and deadlines

FEATURES

Carbon Risk: how do we measure and manage it?

COMMENT

PRINT THIS PAGE

RELATED LINKS

Just say yes

On a wing and a prayer?

Back to bonds

Present and correct

ABOUT

Contact

Editorial
Advertising
Institute and Faculty of Actuaries
Editorial team
SIAS

Quick Links

Contribute
Advertise
Site map
Terms & conditions
Cookies

EMAIL NEWSLETTER

The Actuary Weekly - our regular e-newsletter containing the latest actuarial news, features and opinion - is delivered direct to your inbox. Subscriptions to The Actuary Weekly are free

Sign Up

TOPICS

General Insurance
Health
Investment
Life
Pensions
Regulation
Risk Management
Soft Skills
Technology

MAGAZINE

THE ACTUARY JOBS

Sign up for job alerts

Pensions jobs
General insurance jobs

Health jobs
Reinsurance jobs
Risk jobs
Solvency II jobs

Actuarial job search