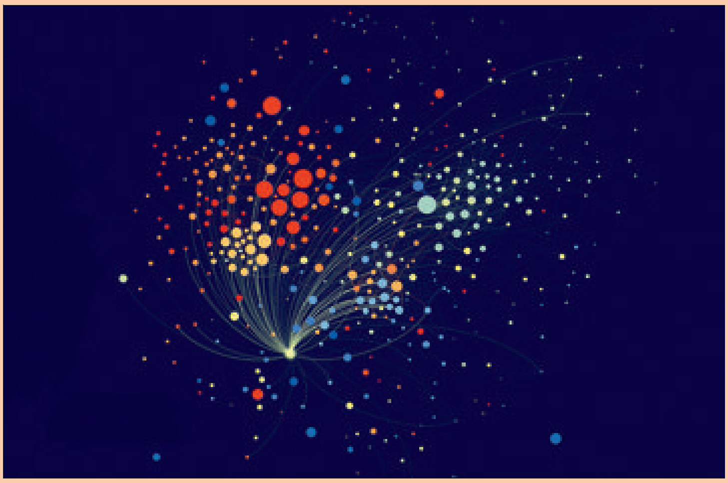
FINANCIAL TIMES

MONDAY APRIL 24 2014

Risk Management

Diversity is the way to avoid cyber collapse

Viewpoint
MICHELLE TUVESON and SIMON RUFFLE



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

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

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

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

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

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

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

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

One could argue these breaches were confined to two businesses and did not affect the global economy. But what is worrying is the potential for a global system-wide IT failure occurring simultaneously across many organisations – a "correlated loss" event that affects a vast number of companies, or an entire sector. As businesses get more interconnected, this type of threat becomes a real possibility.

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

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

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

Many factors can cause IT failures – cyber attacks, hardware breakdowns, software errors. But what causes the failure is less important than the penetration levels of common IT applications. There are many possible types and levels of harm. Past failures, not all maliciously inspired, that have caused multibilliondollar damage to companies include data compromises and other IT problems.

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

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

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

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

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

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School