Naked to the extreme

Emerging evidence suggests increasingly common computer-driven extreme events are a power law phenomenon. This should make them easier to avoid. But, asks Jonathan Rosenoer, is anyone learning this valuable lesson?

"We can't solve problems by using the same kind of thinking we used when we created them"
Albert Einstein

Computer technology is now embedded into the fabric of our economy. The benefits are undeniable, and many are due to inter-networking, which has flattened the world and put knowledge and business processes at our fingertips.

There is a downside, however, that accompanies this shift to an inter-networked world. The media has reported extensively on the exploits of criminals that leverage information technology to infect and take control of our computers, steal credit card numbers and provide the conduit for the distribution of malevolent information and imagery. Not as widely publicised is a much broader set of extreme events that have been driven by computer technology, and which seem to be happening with greater frequency and severity. For example:

- A computer coding error by a leading credit rating agency resulted in the erroneous award of its best (triple-A) rating to billions of dollars' worth of complex debt products. (The *Financial Times* notes, "While coding errors do occur there is no record of one being so significant.")
- A network component configuration error in Denmark halted operations at many of the country's major businesses, with results ranging from missed milk deliveries to disabled ATMs, debit and credit card services.
- Intracompany incompatibility of design and manufacturing software at Airbus led to at least a year's production delay in delivering the world's largest passenger aircraft and $2.5 billion in lost profit.
- A US broker entered a sell order for $4 billion in place of $4 million, causing not only a business loss but also a 2% drop in the Dow index.
- UK government workers lost two computer disks containing the personal information of approximately 25 million residents, including national insurance numbers and, in some cases, banking details.
- In their first overseas deployment, a group of six F-22 Raptors crossing the International Date Line experienced multiple computer crashes, losing navigation and communication functions.

When these events are reported, many times they are characterised as unexpected freak events or anomalies, which might be attributed to very bad luck or the work of a malevolent "computer genius" (the way Société Générale characterised a trader who made unauthorised trades of more than $77 billion over a two-year period and caused a $7 billion loss).

There is reason to believe the rise of extreme events is an expected result of the tremendous growth and systematic leveraging of computer technology. Partly, this can be explained by a unique aspect of computers. An error can suddenly emerge and trigger catastrophic failure. For example, a bug in the software of the Ariane 5 rocket, developed over a period of 10 years and at a cost of $7 billion, triggered a self-destruct mechanism, causing the rocket to explode after less than a minute into its maiden voyage. Similarly, rapid data entry speed triggered software errors in medical therapy machines used to create energy beams that destroy tumours, leading to a terrible series of radiation accidents, including several deaths. Further, as we use computer systems to connect across enterprise boundaries, errors and failures can cascade, amplify and cause a 'butterfly effect'. Just as the flapping of butterfly wings in one part of the world are said to be capable of changing the weather on the other side, a coding error in a debt rating system in New York or London can threaten the future of a public hospital in Australia.

In analysing extreme events, emerging evidence suggests they are a power law phenomenon. Such phenomena exhibit a classic 'signature': plotting the logarithm of one variable against the logarithm of the other renders a sloping, straight line. Examples of other power law phenomena include wealth distribution, cotton prices, movie profits and the structure of the World Wide Web, among many others.

That the incidence and severity of extreme computer-driven failures can be described by a mathematical function challenges notions that they are 'unexpected' big departures from the mean that only happen to others, so that the risk of disregarding them is negligible. To the contrary, the existence of a power law relationship indicates that extreme events are a feature of interdependence, interactivity and feedback dynamics. It also suggests a solution, founded on the Law of Requisite Variety, which calls for the structure and dynamics of an organisation to grow in order to meet the complexity of its operating environment. If the organisation is unable to do so, it may be ultimately destroyed. The global response to the 9/11 World Trade Center attack illustrates a surge of adaptation and change designed to quickly build up the structure needed to counter the threat of extreme events.

A related principle of scaling, the Square-Cube Law, shows that in creating the needed structure, more attention is needed internally than externally. The Square-Cube Law states that while the surface of an object is measured as a square of its dimensions, its volume varies as a cube of its dimensions.

[1] *See, Moody's error gave top ratings to debt products, Financial Times, May 20, 2008, at http://us.ft.com/ftgateway/superpage.ft?news_id=fto052020081848170760.*
[2] *See, P Andriani and B McKelvey, Beyond Gaussian averages, Journal of International Business Studies, 2007.*
[3] *See, eg, E Stephan, The Time Division of Territory in Society, Ch. 9, at http://www.ac.wwu.edu/~stephan/Book/chap9/9.html*

In the case of buildings, this means you cannot blindly scale up a 10-story building from a one-story building. If suitable supports are not used in the taller building, it will collapse because it generates many times more stress. The Square-Cube Law has been shown to apply to organisations, ranging from businesses to villages.

In practice, this means an enterprise must evolve its internal management processes, procedures and operating structure to match the complexity and the risk of extreme events shaped by features of its extended operating environment, eg, the scope and velocity of the economic 'surface' transactions in which it is engaged. Not only should a firm ensure extreme events are managed as a normal part of its business, but it should also ask whether it needs to invest and reallocate resources across a number of key vectors:

- *Governance*: does the current organisational model and reporting structure enable suitable risk direction, control and line of sight (transparency)?
- *Sensing*: is there timely and effective situational awareness of incidents as they occur throughout the organisation and its extended operating environment?
- *Reasoning*: are executive and line of business management, as well as operations managers, given knowledge and understanding of what is happening across the operating environment and the associated (or potential) business impact? Are automated decision-support and dynamic, self-healing capabilities in place?
- *Communication*: do the appropriate managers and systems receive the alerts and information needed to support effective and timely decision-making, and reporting?
- *Threat modelling and prioritisation*: does the business understand the true nature of the threats it faces, so that informed decisions can be made on the scope and extent of investments needed to manage and constrain risk to the right level? Is risk priced into the products and services the business offers?
- *Risk control*: does the business execute a standardised methodology and framework for identifying, managing and reporting on risk? Has it developed and implemented appropriate control strategies and leading risk indicators?
- *Testing*: has the business not only examined whether the 'correct' processes, such as policies, procedures and controls, are in place to control risk, but conducted direct testing and undertaken other direct means of effectiveness and assurance? Investigation: Is there a process in place to capture and maintain event information across time, including audit trails, incident logs and analysis?
- *Human capital*: does the business identify, acquire, retain and develop persons with appropriate levels of skill and experience?
- *Learning*: has it created the inputs and organisational alignments needed for continuous improvement?

To effectively manage risk across these dimensions, an organisation may need to flatten its operating model, as it is highly unlikely that the threat of extreme events can be effectively managed within discrete business or operational silos. It will also be necessary to couple executives with the technology managers whose systems underpin their business processes, so that there is better understanding of the relationships and trade-offs between risk and business value.

Owing to rapid changes in the way companies across the economy leverage information technology and, indeed, in the technology base itself, past event analysis will not provide guidance on when the next extreme event will materialise or how it is likely to unfold. But the evidence strongly suggests extreme events are a by-product of the way information technology powers the economy. To manage the risk, much work needs to be done to change management thinking, organisation and supporting capabilities. If not, the structure is liable to collapse under its own weight.

Jonathan Rosenoer is a partner in KPMG Global Advisory's Financial Services practice, and an adjunct professor of risk management at Carnegie Mellon University. Prior to joining KPMG Advisory Support S.a.r.l, he was global risk officer for IBM's Financial Services Sector, where he also served as global banking risk and compliance solutions executive, and global head of operational resilience and risk solutions. Jonathan is the author of CyberLaw: the law of the internet (Springer Verlag 1996) and The Clickable Corporation: successful strategies for capturing the internet advantage (Free Press 1999).
Email: jrosenoer@kpmg.com