THE LIGHTHILL RISK NETWORK

If there is valuable data, you can guarantee threats to its security will not be far behind.

By Dickie Whitaker, Simon Cartwright and Thomas Maillart

Essential criteria for the creation of reliable cyber insurance

INFORMATION RISK CAN arise anywhere that information is held, which today means almost everywhere. The possibility of disaster is obvious. Compromised information can cause enormous damage to an organisation's operations and reputation. Information not appropriately protected can lead to serious compliance and legal failures.

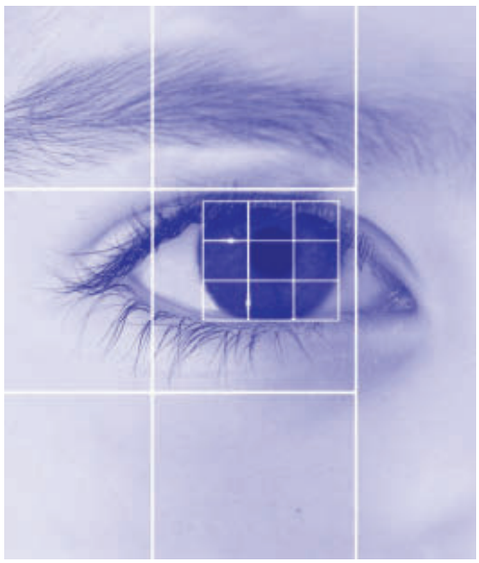
Cyber exposure and risk modelling for the re/insurance market were the subjects of the latest Lighthill Risk Network event in London in July.

Over the last few years, writers of malicious code have turned into seasoned pirates, exploiting the numerous weaknesses of information systems. The barriers to entry are low and they have almost no risk. Personal identities, credit card numbers and passwords are very fashionable targets and represent lucrative sources of profit.

Financial service institutions, unsurprisingly, are very popular with fraudsters, who cause havoc beyond the financial markets. Customers entrust them with their financial security, but high profile security breaches and alarming fraud statistics have led them, the media and regulators to question how safe customer identity data are.

But they are not the only target; government organisations and academic institutions are also concerned. Valuable information, wherever it is stored, may be subject to attacks, or at least loss of control. For example, in 2007, the UK Revenue and Customs lost control of 25 million taxpayers' very private financial information.

In the case of non-revocable identities, such as biometrics, catastrophic and disruptive events are a danger. For instance a successful attack on border police identification databases and more widely on police identification files of any country would have huge and permanent consequences by allowing replication of biometric IDs. Could we still trust fingerprints as reliable evidence of crime if 30 million or more had been stolen?



Cyber insurance

"Is IT security sufficient protection for company exposure, or should insurance play a key role in the management of such risk?" was a question posed by a participant at the event. The emphatic answer was that cyber insurance should be as ubiquitous a product as firewalls and antivirus software in terms of mitigating risk. Although insuring against IT risks is still relatively new, it will become more important as regulators interrogate directors about their corporate risk and internal controls.

Enough capital provision so that a more meaningful line size is possible should encourage the market to take this sector more seriously. Yet, it was very apparent that the insurance market finds that the complexity of cyber risk is such that quantifying it needs a more sophisticated approach. In the fast changing landscape of the internet, empirical evidence is clearly not sufficient. From awareness to the development of cyber insurance products, there is a gap that must be filled.

Reliable cyber insurance products will rely on extensive and precise knowledge of mechanics of information systems. For that, two major steps are required:

- Verified and validated models so we can understand why information systems fail
- Simulation, construction of future scenarios and predictions that can be used by industry, policy makers, and underwriters, etc.

Good risk management helps an organisation get the best out of its information and allows it to develop, confident that its risks are mitigated and under control. It is not simply about controlling data, nor is it purely a technical issue which can be left to IT staff alone.

It should go beyond compliance and the illusory search for 100% IT security. Reliable and quantitative figures of cyber risk must drive appropriate security policies at any organisational or regulatory level. Strong risk mitigation strategies and subsequent security will change the work ethics and culture of the organisation, enabling companies to refine fraud detection procedures, improve customer service and continuously improve their security operations.

WEBLINKS visit: **www.cat-risk.com**
▶ Roundtable: The key cyber risks

Dickie Whitaker is a director of the Lighthill Risk Network, Simon Cartwright is managing director of consultancy Sciemus Cyber and Thomas Maillart is a researcher at the Chair of Entrepreneurial Risks, Swiss Federal Institute of Technology (ETH) Zurich.

The Lighthill Risk Network has two more events planned in London this year: Modelling terrorism for the re/insurance industry on 29 September and Bayesian networks and their applications for the re/insurance industry on 22 October. See the web site for more details: www.lighthillrisknetwork.org natalie.compton@lighthillrisknetwork.org