Power companies get connected

Energy firms' concerns about exposure to cyber risks reflect a wider unease about the potential impact on physical assets, supply chain, brand and much more, says **Suki Basi**

Most business leaders and risk management professionals would accept the premise that the world has become a much more complicated, interconnected place.

The insurance industry in the UK, for example, has, for understandable reasons, been largely preoccupied in 2014 by the damage caused to lives and livelihoods by flooding.

While flood news has dominated, however, a chilling and timely news story appeared on the BBC recently, which demonstrated how important it is for underwriters to remain focused on their connected specialty insurance exposures. The story, which was picked up after a note was released by Lloyd's of London underwriter Kiln, outlined how energy bosses are getting increasingly worried about the risks posed by cyber-attack.

According to the BBC story on 27 February ("Energy firm cyber-defence is 'too weak', insurers say"), power companies are being refused insurance cover for cyber-attacks because their defences are perceived as vulnerable. Underwriters at Lloyd's explained they had seen a "huge increase" in demand for cover from energy firms, but surveyor assessments of the cyber-defences in place concluded that protections were inadequate.

Laila Khudari, an underwriter at the Kiln syndicate, which offers cover via Lloyd's, explained in the article: "In the last year or so we have seen a huge increase in demand from energy and utility companies. I think what's behind it is the increase in threats and the fact that a lot of these systems were never previously connected to the outside world."

The key word here is "connected". The news about the energy companies reflects a wider concern about cyber exposures more generally and the impact on business interruption.

As power generators and distributors struggle with the complexity and size of the networks they manage, they find it hard to locate and recruit staff with the specialist skills to defend these systems.

In the article, Nathan McNeill, chief strategy officer at remote management firm Bomgar, said that financial pressures and the ability to manage systems remotely are inadvertently giving attackers a loophole they can slip through.

"Trying to cut costs by linking up plant and machinery to a control centre so they could be managed remotely meant those systems were effectively exposed to the net. If something has basic connectivity then it will become internet connectivity through some channel."

To mitigate their exposures to cyber liabilities, some power companies are using supervisory control and data acquisition (Scada), which is a category of software application programme for process control – the gathering of data in real time from remote locations in order to control equipment and conditions.

Scada is used in power plants as well as in oil and gas refining,

> "Malware is being written to get at particular vulnerable elements in the infrastructure run by many utilities and manufacturers"

Continued on page 41

Power companies get connected continued from page 41

telecommunications, transportation, and water and waste control. Scada systems include hardware and software components. The hardware gathers and feeds data into a computer that has Scada software installed. The computer then processes this data and presents it in a timely manner. Scada also records and logs all events in a file stored on a hard disk or sends them to a printer. Scada warns when conditions become hazardous by sounding alarms.

Scada software, however, has come under increasing scrutiny by security researchers who have exposed many flaws in it. It can very difficult to update the core code in many Scada systems to close loopholes that attackers have slipped through, and it does appear that the number of attacks on Scada and other control systems is escalating.

Malware is being written to get at particular vulnerable elements in the infrastructure run by many utilities and manufacturers. Some attackers may just be curious, but others are thought to be carrying out reconnaissance in service of some future event.

It is becoming increasingly clear that to get around this problem individuals, businesses, entire industries even (including insurance), need to get better at sharing information to mitigate their risk exposures.

US power companies, for example, have begun sharing information about attacks so everyone knows about the threats to them, but the basic infrastructure remains very hackable. Search engines, meanwhile, are revealing public interfaces to huge numbers of domestic, business and industrial systems.

According to the latest report from BAE Systems Applied Intelligence, "Business and the Cyber Threat: The Rise of Digital Criminality", more than half of businesses list threats from cyber-attacks in their risk category. Companies have long feared physical risks like a major fire or an earthquake, but today's risk managers and their boards are just as likely to worry about potential threats to their reputation or brand, the loss of intellectual property or severe disruption to their supply chain or computer network from a data breach.

> "US power companies have begun sharing information about cyber-attacks so everyone knows about the threats to them, but the basic infrastructure remains very hackable"

What is clear is that critical infrastructure and industrial plant control systems are coming under more scrutiny from both attackers and defenders.

From the power insurance industry's point of view, underwriters firstly need to ascertain those parts of the client's business that are critically reliant on IT. The threats posed need to be evaluated and the internal processes and controls being used to mitigate the risks need to be reviewed.

Secondly, a consultancy approach needs to be adopted that helps clients to understand their risk profile and embed controls within the operation to mitigate such risk.

Thirdly, underwriters need to capture better data on the relationship between vendor technology and client risk profiles, so that potential threats can be evaluated and adequately priced for.

It can't be emphasised enough that the world has become a much more complicated, interconnected place and there are two ways of approaching this – either by saying this is someone else's problem or by facing up to the challenge and sharing knowledge and data.

Russell Group is evaluating the risks posed by the emerging cyber-risk market, especially because this particular risk can be picked up by many different policies in different coverage configurations, which makes it very difficult to aggregate. A cyber liability can pop up under a crime policy, a professional indemnity policy, a general liability policy or a standalone cyber policy.

In addition, a cyber-risk is not just a cyber-risk. There are huge business interruption elements, which are very important to companies that hosts clients' data.

At Russell Group even, we need to fully understand the exposure ourselves, which is why we are voluntarily implementing ISO 27001, which is an internationally recognised quality standard focused on data security and business continuity.

To obtain that accreditation, firms have to be able to identify and manage all the threats to their data records and storage.

Ultimately, however, the message to firms large and small – and their partners in the insurance sphere – is that we all need increasingly to harmonise big data across our businesses. What that means for the insurance world – where to date, lines of business in the market have tended to be silo-based – is that underwriters need a better risk profile of their own portfolio and their clients' business: a cross-silo approach.

Suki Basi is managing director of Russell Group