RISCAuthority at work

Dr Jim Glockling shares his views on the importance of making business continuity templates simple and easy for businesses to use

WHILE PIECING together a paper-based business continuity template for small business to augment RISCAuthority's ROBUST BCP software toolkit, I downloaded, examined, and borrowed bits from many other downloadable offerings. The need has been driven by an acceptance that, although ROBUST is aimed at SMEs, and can indeed be configured to simple form, the software format is just too off-putting for many smaller businesses to even warrant investigation.

I recall how at the launch of ROBUST, having demonstrated its wealth of capability and output, an insurer commented: 'That's great, but if all I manage is to get my customers to take their data home at night that would be a major success!' And she is right. The lesson has to be that something is better than nothing.

The London Prepared BCP reports some interesting statistics, which show that:

- 80% of businesses affected by a major incident close within 18 months
- 90% of businesses that lose data from a disaster are forced to shut down within two years
- 58% of UK organisations were disrupted by 9/11, one in eight seriously affected

Scary as these statistics are, I wonder whether the message could be rephrased to make those with ultimate responsibility for the company, the owner and managing director, take more notice? Since resilience is firmly embedded in the job specification of every managing director, a suggested reworking of the form is '80% of businesses affected by a major incident show themselves to have been incompetently managed within two years of the event!'. Harsh perhaps, but it's certainly an alternative viewpoint, not without merit.

In next month's issue there will be a review of the papers of the RISCAuthority Seminar that took place in London in March. While not wishing to give too much away, I would like to give insight into an extraordinary talk given by Benedict Hamilton from Kroll Solutions on cybercrime, since it has more than a passing relevance to business continuity planning. A welcome excursion from fire for the listeners, Benedict provided immensely interesting facts and figures supported by to-die-for anecdotes on current and emerging methods in electronic extortion. Key to his talk is the changing value of information to the criminal. Credit card details, including the security code on the back, might 'retail' at 10 cents a card – surprisingly little in my mind. An 'identity' however, in the form of a Facebook account log-in detail, might be worth $30 – and for good reason. We also learned:

- Benedict switches his phone Wi-Fi off when he leaves home – such is his experience of Wi-Fi security and what can be done
- standard business computer configurations, even with patches and virus protection, are still vulnerable
- criminals don't need to go to the lengths of creating complex computer viruses, as simple deception techniques will get company employees to click on download links that 'invite the wolf over the server doorstep'
- with log-in details and associated access to your company computer, a criminal may hold lengthy transaction conversations with your bank and others, entirely under your nose and without you ever knowing
- to re-issue a credit card to its legitimate owner by the bank, following criminal theft of details, costs around $30. Now imagine that in the context of the US Target data theft where over 100 million account details were stolen

On the subject of the last point, there is clearly a grey area in insurance. Do losses incurred from cybercrime come under business interruption insurance? Some companies do offer specific cyber insurance but, as RISCAuthority chairman Chris Hanks pointed out, how do you assess the potential scale of loss?

RISCAuthority, through the Security Working Group, will be working with Kroll to deliver an insurer guide to cybercrime, which should be available later in the year. The Business Continuity Working Group will be releasing a simple BCP Template file for small business in the summer ■

Dr Jim Glockling is technical director of the FPA and director of RISCAuthority