

Client: IT Governance Limited
Source: Accounting & Business (Main)
Date: 01 January 2006
Page: 56
Circulation: 101354
Area(cm²): 174

80:20 PR

book

A Business Guide to Information Security
by Alan Calder
Kogan Page, £18.99

■ **When we leave home for work, we check that the front door is locked. When we park the car that reassuring bleep of the central locking device lets us walk away from the vehicle with at least some sense of security. But when we run a business, which may depend crucially on the protection of confidentiality and the secure marshalling of intellectual assets, how careful are we to make sure that our systems are secure? Answer: not careful enough.**

A 2001 survey by the UK's DTI found that lapses in security policy had cost firms between 6% and 7% of annual revenue in the preceding year. That figure may represent the difference between making a profit or a loss. European businesses alone lost more than £4.3bn in 2001 due to internet-related crime. And PwC's 2004 "Information Security Breaches Survey" found that corporate behaviour was still leaving many vulnerable to hackers and cyber-criminals.

For example, one third of large businesses and two thirds of all companies still had no information security policy. Only half of all wireless networks had security controls in place. And the average UK business was experiencing one security incident a month, while large businesses had one a week.

Complacency in the face of these kinds of threats is not merely unwise, it is almost literally criminal. No wonder that Alan Calder, the author of this new book (and CEO of consultants IT Governance), writes: "Information security in business is now too important to be left to the IT department. Information security is, in fact, now a boardroom issue." And he adds: "Information security can no longer be the Bermuda Triangle of the executive role."

But there are all your staff, busy out in the field every day, with their PDAs, mobile phones and their laptops, beavering away for the next contract or the next sale. Can't they be left to get on with their work in peace? Aren't security policies just going to get in the way of doing business? Calder says not. And in this clearly argued and thorough guide, he takes the busy

reader through a powerful checklist of simple but necessary steps that will help protect your business.

It turns out that good security procedures are in many cases simply an extension of good management practice. Employees need to understand their responsibilities as far as information and security are concerned. Training and the communication of good practice must be undertaken. Firewalls, anti-virus software and other technical precautions must be kept up to date. The crooks are thinking up new ways and methods of defrauding businesses all the time, from ever more exotic locations. Business has to try and keep up with them.

Of course, this wouldn't be an IT book without an amazing array of TLAs—Three Letter Acronyms. But, thankfully, there is a very full and detailed glossary which helps to provide enlightenment and clarification. In any case, Calder writes clearly and keeps jargon to a minimum. This book should not give you nightmares, but it will give any senior executive pause—a serious new year's wake-up call. It is time to get serious about IT security. ■

Review by Stefan Stern, a regular contributor to the specialist press and writer on work, management and industrial issues.