Stick-on Security - management practices that thwart your efforts

Michael Barwise

Despite ongoing and creditable advances in information security technologies, corporate information systems are still constantly proving their vulnerability. We all hear of disasters like Melissa and Code Red, and a substantial amount of corporate data loss and corruption also occurs from day to day without such dramatic causes. So we have to ask what is going wrong.

I believe the fundamental problem is what I call "stick-on security": considering information security only as an afterthought instead of building it into the enterprise as an intrinsic component of all business activities. I would like to propose five specific management practices that stand out as primary symptoms of stick-on security. If any of these look like they might apply to your organisation, maybe it's time to rethink the way you manage your information security.

Fragmented Structure

The cubicles in which many of us work are a symbol of fragmented structure. There are almost always similar virtual cubicles between work groups with different specific responsibilities. They are barriers to communication, and prevent concerted action. Your IT staffing will include desktop support staff who install and maintain the users' computers and applications, server room staff who keep the servers running and do the backups, and security staff to configure the firewall. But I bet these groups don't talk to each other.

Desktop configuration is inseparable from network security if you don't what hundreds of back doors into your business, and to prevent accidental data loss by controlling what users can do. Backups are potentially one of the weakest links both in business continuity and information leakage. The firewall is only a small part of a larger programme of defence. And no single technical group alone can develop the security policies, as each only addresses part of the overall problem.

Do you have a formal mechanism whereby these groups can share information or work in concert? Are they managed coherently by someone with overall control and both the technical and the business knowledge to apply that control in an appropriate manner? Such mechanisms and management are essential, but you won't find many businesses enabling them. If you believe, as most of your competitors do, that each of these groups provides a stand-alone service, your security will fail.

Fragmentation of technical responsibilities is bad enough, but we must also look beyond, to the level of interaction between technical staff, business leaders and those at the "coal face".

Poor Communications

Once a business reaches the size where it needs internal ID badges, individuals may no longer retain the freedom to communicate directly up and down the hierarchy, but must use "channels". And the channels are generally pretty restrictive of who can communicate what to whom. A cynic might get the impression they were primarily designed to give the upper echelons a quiet life. In such a culture, information from the wrong source is disregarded, however valid it might be. As a result, the quality of information suffers. Even those who are supposed to know the true position with respect to inventory and risk can find they are ill informed when the crunch comes. You might think that auditing could assist here, by formalising the gathering of information, but that entirely depends how it's done.

Perfunctory Controls

I was delivering a security management course to a group from the financial sector. Having wrapped up risk assessment, we got to the final questions and answers section a little ahead of time, so I said to one of the delegates "OK, John, I've explained the theory for two days. You manage this all week. Tell us what your people do in practice".

His reply was "well, once a year they have an audit".

That was it: the sum total of their security controls. Once a year, they had an audit, updated their inventory documents and revised their policies. Then they cast the lot in stone for the following eleven months, regardless of what happened in the meantime. And yet significant new threats emerge, business needs change, staff join and leave, equipment and software are deployed and upgraded.

Controls are conducted like this because everyone involved sees the task as a burden, the impact of which has to be minimised. But although it may seem the quickest and cheapest way to "get the job done", a once-a-year slog is not the way to go about it, as it's not really doing the job at all. Out-of-date inventory, policies and risk assessments are more dangerous than none: you'll finish up trusting something unreliable, rather than staying alert in the knowledge that you can't trust anything.

The fundamental error is viewing security controls as exercises. You can't afford them to be. If they are to work, they must become processes. Only if you've never done it before should you be faced with a blitz on the whole inventory or the whole risk assessment or policy definition. Once the process is rolling, individual threats, business changes and technical modifications are assessed as they emerge. This must become part of day-to-day business management. And even if you currently have change control systems in place, take a long hard look to see whether they are functional and contribute to your security. All too often, they are merely redundant paperwork. I have participated in change control where the requester of the change was left to define the risk without any independent assessment process.

Technological Dominance

One of the greatest security hazards is the dominance of technological solutions. Security is generally left to the IT people, who are all technical and are rarely if ever given business briefings. They tend to think in terms of "attacks" and "defences" rather than confidentiality, integrity and availability of data. Business IT requirements are met by negotiating requests for services or facilities into the extant technical framework as well as possible, and the framework is defined on technical grounds alone. This can lead to two extremes, depending on who wins the negotiation.

At one end of the scale, security can be left wide open in order to facilitate some department's activities. For example, several people in Marketing may want individual direct update access to the public web server so they can post press releases. They may well get it, without any training or warnings as to risk.

At the other end, security may seriously impact on productivity. Not so long ago ,the senior IT man in a national-scale company told me with pride that he had tightened the corporate e-mail policy so much that huge numbers of e-mails get quarantined (i.e. not delivered) because of "questionable" choice of wording.

The really shocking thing is that you often find both these approaches operating side by side. While one technical arm locks the business to the ground, another exposes it to unacceptable risk. The problem here is failure to appreciate that information security is a business issue with technical facets, rather than a purely technical issue. All aspects of the business must be considered when implementing security, and the impact and cost to the business of security measures must be factored into risk assessments. This implies that certain risks will have to be accepted, and sometimes things may go wrong, simply because it is excessively expensive to protect against some threats.

Shooting the Messenger

Which brings us to the last, and possibly the most telling symptom of "stick-on security": shooting the messenger.

At the ISSE conference this year a leading security professional stated from the podium "If a new technology is released, of course you will buy it, because if you don't and something subsequently goes wrong, your job's at stake".

In a recent presentation, a representative of a leading data recovery company said "When I get back to the person who supplied a disk or tape for recovery, I often find they're no longer on the staff".

Similar statements have been made by at least one person at nearly every security conference and meeting I have attended this year. I find, when talking to senior IT staff, that they are generally scared stiff of the slightest suggestion they are not doing everything perfectly. Nobody wants an objective audit. Nobody wants to admit that their systems or procedures may need revising. Everyone is just hoping and praying that nothing will happen to draw attention to them. And I suspect the fear they experience is justified, particularly in the current economic climate.

But, given that information security is about minimising a risk that can never be eliminated entirely, where does this leave us? Frankly, wide open to a security breach. If the people who are supposed to

secure your business are constantly distracted by worry about whether they get the sack if something is seen to go wrong, there is a serious conflict of interest. This will inevitably lead to inefficiency, and at worst, to cover-ups.

It may feel very satisfying to crucify a culprit, but in my experience it never really solves your problem. It doesn't recover your losses. It doesn't prevent the breach occurring again. The appropriate solution is a rigorous and impartial debriefing, leading first to changes which protect the enterprise, and only second to penalties if they are proved to be merited. If you are strictly impartial, you'll probably find out the breach happened because your information security is under-resourced and insufficiently co-ordinated. The average US spend on information security is about two percent of gross, whereas security experts consider that eight percent would be a realistic minimum under current conditions. So the penalty will usually be spending more money and effort to bring your provisions up to standard.

The bottom line is that "stick-on security" does not work. However much you have spent on security hardware and software, business practices like those described here will thwart your efforts. The best you will achieve is a false sense of security that will not hold up under stress. Security that sticks, that will protect you as far as possible, requires sound business practices that maximise the currency of your information and the co-operation and effectiveness of all your staff in what is, after all, a common purpose: securing your corporate data against loss or corruption.

Originally appeared in Computer Weekly, November 2001