



Arcati Research Bulletin

The rise and rise of the CSO

by Mark Lillycrop

Despite numerous industry initiatives, security management within the enterprise remains a complex and time-consuming activity. That is why the new breed of high-profile Chief Security Officers can be worth their weight in gold.

We live in insecure times. It's not just because of world events and the aftermath of 9/11 – it's also because of a growing feeling across the business world that we cannot fully guarantee the safety of the vast amounts of critical data tied up in networked IT systems.

Watchdogs such as CERT (www.cert.org) never tire of quantifying the problem: they remind us, for example, that the 132 security incidents logged in 1989 grew to a stunning 73,359 for the first three quarters of 2002. Meanwhile, Microsoft is sending out so much technical information about security exposures in its products that it has started to issue edited highlights for non-technical users of a nervous disposition. And, to cap it all, hackers are now devising viruses that fire off insults to the computer user while trashing the contents of their hard disk.

The terms 'security' and 'grudge spend' are used together a great deal of late. Security is now firmly established at the top of the agenda for companies of all sizes, but its prominence is pretty much resented by everyone except hackers and developers of security management products. Most companies know that they have no choice about the small fortune being poured into new tools, firewalls, patches and upgrades, just to keep the interlopers out and the systems up and running. But in the main, security offers no effective return on investment, and knowing where and how to invest the security bucks most efficiently is one of the biggest headaches for managers today.

The problem is that electronic methods of communicating and handling transactions rely so heavily on user confidence. Anyone providing Web services or supporting Internet-enabled applications needs to demonstrate their commitment to security – in much the same way that banks have long chosen to operate from solid, imposing-looking offices as a way of reassuring customers that their money is held in complete safety.

It was just such a confidence-building exercise that inspired Microsoft to launch its Trustworthy Computing initiative early last year. It started with a now-famous e-mail to employees from Bill Gates, which asserted,



Arcati Research Bulletin

among other things, *“all those great features [in Microsoft’s products] won’t matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security.”*

But even as Mr Gates uttered his rally cry, the pragmatists were wondering just how far the company could go in building confidence among its users. Microsoft, like many other vendors of course, has a long inventory of legacy systems littering the desktops of the world; and whatever measures are taken to tighten up security in future releases, networks will continue to be as vulnerable as the oldest product attached to them.

Cooperative ventures

All IT vendors, particularly those in the so-called Web Services market, face an uphill task in building confidence among users. But much is going on behind the scenes to develop reasonably consistent standards for future development. WS-Security, for example, an extension to the Microsoft SOAP standard, provides what its originators describe as *“quality of protection through message integrity, message confidentiality, and single message authentication.”* The specification, originally drawn up by IBM, Microsoft and VeriSign, now has some 60 participating vendors. As the basis of watertight security for Web-based applications, it is only a small step; but as an indicator that IT vendors know how closely they need to cooperate to build confidence in the e-business world, it is very significant.

Another current vendor-driven initiative is the Liberty Alliance Project, with hard-hitting users such as American Express, Vodafone, General Motors, and United Airlines complementing vendors led by HP and Sun. Liberty Alliance focuses on what it calls *federated network identity* – the goal of providing users with a single online identity and personal profile, access to which would be determined by the user herself. The ultimate aim is to build an extensive network identity account for each person, including entertainment preferences, educational history and financial information, as well as credit card details and of course passwords. But the first step is to achieve a single, multi-vendor Web-based sign-on - a very attractive objective, but one that has eluded most security specialists so far.

The interesting thing about Liberty Alliance is that it is concentrating on the positive aspects of security, using identity management not just as a way of simplifying arduous processes like multiple sign-ons and repetitive entry of personal information; but also as a way of sharing this information under carefully controlled conditions to create new business opportunities.



Arcati Research Bulletin

Enabler or inhibitor?

There is clearly a message here for the industry as a whole – IT security as a defensive operation (patching systems, upgrading firewalls, and imposing rules regarding the use of insecure technologies) is a necessary function, but the danger is that it can actually inhibit commercial activity and efficiency unless it is correctly managed within the organization. Often business managers will implement insecure technologies, such as wireless LANs, risking the wrath of senior management because they see security as an obstacle that is out of step with corporate business goals rather than as a strategy that reflects the needs of the enterprise. Most companies have a security policy of some sort, but few incorporate a single, consistent view of the flow of information around the organization, and few offer sufficient training or internal marketing to sell the security message to business management and staff.

Much of this comes down to the fact that security requirements, and the solutions to them, have grown up piecemeal within companies, with little high-level coordination, particularly between IT and non-technical areas of security. With every restructuring move, merger, or acquisition, the security message has become a little less consistent. Reporting lines, too, vary significantly, and some companies place far greater responsibility on the shoulders of the security manager than others. This is illustrated by a recent survey from AFCOM, an international association of data centre managers. Nearly half of respondents said that the security spend had increased within their organization, in the light of recent events and the raised awareness of security issues. Yet, in 62% of cases, there was no high-level Chief Security Officer who could implement a company-wide policy. Moreover, in enterprises without a CSO, there was a wide disparity in the level at which security professionals reported in.

CSO required - only Superman need apply

A growing number of companies, though, both inside and outside the IT industry, are biting the bullet and appointing high-profile, high-salaried CSOs, reporting straight to the Board. While these individuals have considerably more responsibility and influence than their predecessors, there is still no real consensus of opinion on the qualities and experience they should possess. Neither the upwardly mobile firewall administrator nor the nightclub doorman with an enthusiasm for hands-on intruder management is likely to be ideal for the role, but the CSO may well share qualities with both. Generally, the job seems to demand the following:

- *Renaissance man*. The ideal CSO is likely to need a very broad range of skills, encompassing both IT and physical security experience. He will need to be happy communicating with managers at all levels.



Arcati Research Bulletin

- *Spin doctor.* The good CSO will also need more than a passing enthusiasm for PR and marketing. After all, as suggested earlier, this role is all to do with instilling confidence, both within and outside the organization. The CSO is in many ways the custodian of the corporate 'brand': he needs not only a finger on the pulse and excellent channels of communication around the enterprise, but also a highly developed sense of perspective and instinct for damage limitation. In the Age of Spin, the way security incidents and alerts are reported is just as important as the way they are fixed. More than just providing a calm voice and smiling face for the outside world, the CSO also needs to convey the whole security strategy to the enterprise. He needs the enthusiasm to motivate the workforce, while being prepared to crack down on offenders as necessary. Above all, he needs to be aware of the need to use confidence in security measures as a way of building competitive advantage, rather than letting security be perceived as an obstacle to progress.
- *Training manager.* CERT suggests that 95% of recorded attacks could have been avoided by applying known fixes to vulnerabilities in software. Likewise, many pundits have noted that security is useless unless those who implement it understand the risks they are dealing with and the need to be vigilant and rigorous in applying policies. Many hacking cases can be put down to copy-cat mischief-makers, seeking out sloppy network configurations and weak default settings. The majority of products are easy enough to equip with basic protection, if those who support them are aware that they need to change defaults and simply close the doors that are left open on delivery. A growing number of training providers, and organizations like the International Information Systems Security Certification Consortium (which, you'll be pleased to know, abbreviates to (ISC)²), run certified courses in information protection and the technical aspects of security management, as well as topics such as ethical hacking to give managers an understanding of the intruder's perspective. Making sure the right people get the right training comes down to the CSO, and this needs to be a key part of the role.
- *Techie.* Even if the CSO has a remit that extends well beyond IT, he still needs a close familiarity with the technology underpinning the corporate strategy. He needs to work closely with system and network administrators and developers, to make sure that firewalls and physical security devices, as well as multi-level authentication and encryption within applications, are used consistently across the enterprise.
- *Lawyer.* Finally, the CSO will be involved, to a greater or lesser extent, with the legal aspects of data management, particularly securing personal data. In some companies, compliancy officers



Arcati Research Bulletin

will continue to look after data protection issues, but in others the roles of Chief Security Officer and Chief Privacy Officer are likely to be combined. Either way, they are now very closely connected disciplines, particularly in view of the legal implications of exposing sensitive data through lax security.

The demands placed on the top-level CSO are very great indeed, and the role is beginning to attract a salary to match. There are reports of CSOs in the financial services sector in the USA bringing in around \$400,000 a year, but the remuneration range is understandably very wide. As more and more companies understand the need to make security strategy an enterprise-wide affair, the demand for the right people to manage the activity is likely to soar.

Bottom line

In the end, there is only so much one top-level manager or vendor initiative can achieve. Business perceptions of security in general need to change: data is the most precious commodity held within most companies today, and the need to guard it and preserve its integrity must be understood at all levels. But companies also need to find ways of turning excellent security and strong user confidence to their advantage, to make security a business enabler rather than an inhibitor – and this might well be where the great CSO rises above the good one.

Mark Lillycrop is Chief Analyst of Arcati Ltd and an Associate of Valley View Ventures, Inc. For further information on this paper or Arcati services, visit www.arcati.com or e-mail mark@arcati.com.