



Arcati Research Bulletin

Security strategy - a view from the outside!

by Mark Lillycrop

Chief Security Officers (CSOs) frequently need to call on impartial external advice to help build an effective and workable security policy for the enterprise as a whole, and to help gain the backing of senior management. Unisys' new Zero Gap initiative looks set to provide a new level of support for the CSO, offering a complete, integrated picture of the customer's security requirements.

In many organizations, security policy is the issue that keeps the CEO awake at night. In almost all enterprises of any size, the subject figures among the top three priorities for IT planning, and things are not getting any easier. According to industry watchdog CERT, the number of security incidents and reported vulnerabilities in products is still growing at a near-exponential rate, with 73,359 security incidents logged for the first three quarters of 2002 alone. Any company that neglects security management, either externally or internally, risks placing its whole reputation and commercial future on the line.

Yet security remains a 'grudge spend'. Rarely, if ever, does it offer a tangible return on investment - except, perhaps, as a way of building user confidence in a product or brand - and companies often find themselves pouring vast resources into a diverse collection of encryption and certification tools, firewalls and related hardware, password and authentication products, without any real conviction that the money is being spent in the right places and with the desired effect. Responding to security violations now absorbs billions of dollars a year worldwide; protecting information resources from unspecified future attacks accounts for billions more.

An integrated approach

The problem is that security is all about finding the seams in apparently seamless systems, identifying flaws in end-to-end solutions. Most mature IT infrastructures, and indeed the business processes that they support, have grown up piecemeal, with different



Arcati Research Bulletin

managers, departments, or divisions putting different parts of the architecture in place. Every time a new process or technology is 'bolted on', new opportunities arise for security to be compromised or neglected. Few companies have the time or expertise available to take a look at the 'big picture', and draw up a strategy for re-deploying their security investment in the most efficient and logical way.

The answer, we believe, is two-fold. Companies need a single, high-level manager to take on company-wide responsibility for security strategy and deployment - the Chief Security Officer, as the post is now widely described. They also need a single, consistent top-down security policy, which is understood across the board and implemented with a firm hand.

Empowering the CSO

The CSO is a highly skilled and diverse job with enormous responsibility attached. Opinions vary as to what should be included in the job spec, but in most cases the candidate will not only require a broad understanding of the technical infrastructure for information and physical security, but also possess the ability to communicate the company's vision for security to all levels of management. He will also need to instil confidence, both inside and outside the organization, and wield sufficient power to make changes happen.

The hardest part of the job is creating awareness of security issues at the highest levels of management, and attaining board-level buy-in to help drive through potentially unpopular security management decisions. This is where external support can be particularly valuable. Many IT consultancies and service providers now offer company-wide security audits, and can aid the CSO in building a policy that encompasses the various areas of company activity. Many external advisors, however, do not offer real breadth of expertise, and rarely achieve a full examination of all business processes and associated vulnerability to security exposure.

Zero Gap

One service which, we believe, will take security guidance to a new level of sophistication is the Zero Gap Security Planning initiative, recently announced by Unisys. Unisys' extensive service organization - including 700 certified security consultants - benefits strongly from the company's background in large-scale data center



Arcati Research Bulletin

systems, and its long-standing association with the financial services industry. Unisys is leveraging its experience in dealing with top-level business management to raise awareness of security in all its forms.

Zero Gap covers a broad range of security services, from assessment to planning and implementation, and is promoted as a 'holistic' approach to security management, enhancing business integration by helping users to establish best practices across the enterprise. Its main areas of focus are defined as:

- *physical* – protecting buildings and other physical areas
- *operational* - identifying areas of vulnerability in day-to-day operational practices
- *cyber* - protecting on-line information resources against attack, internally and externally
- *financial* - mitigating risk against financial theft etc.

As such, Zero Gap embraces areas of strategy that are often neglected in security reviews, closely relating the financial aspects of security management with protection of both IT and physical resources. This approach mirrors the far-reaching responsibilities now bestowed upon many new-breed CSOs, and the service is well positioned to support security managers within the organization.

One particular benefit of the Unisys approach is that it helps users to assign priority to the most pressing, financially precarious areas of security, something that can be extremely difficult with a more fragmented approach to security assessment. Since security is such an open-ended responsibility in most enterprises, identifying priorities in this way is paramount to long-term success.

We anticipate that more services of this kind - aligning security needs more closely with business processes - will emerge in the months ahead, probably with a number of significant partnerships between more specialized security advisors. Meanwhile, Unisys will be able to capitalize on its pioneering position in this field, and is bound to attract some major customers.

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.