

Exclusive feature for Computer Fraud & Security

## Holistic Security: Why Doing More Can Cost You Less *and* Lower Your Risk

By Tom Patterson

*Tom Patterson leads the Deloitte & Touche Security Services Group in Europe, Middle East, and Africa from Frankfurt, Germany. He is part of the firm's global security services leadership team and is responsible for coordination and delivery of information security solutions to clients in more than 30 countries. Patterson is responsible for developing new business and delivery methodologies in response to evolving client needs, and is a trusted security and business advisor to executives around the globe.*

### Introduction:

The search continues for a magic bullet to cure the ills of corporate security. With the increase in potential threats from worms, viruses, and hackers, and the demand for an open system architecture to support e-business, security professionals often feel as though they are trying to plug an ever-growing number of leaks in the IT dike. What most security professionals understand is there is no magic bullet; that no one technology or methodology will address all the security needs of any organization. Effectively safeguarding data and assets requires a holistic approach that embraces all aspects of security, including systems architecture, policies and procedures, and user education. Holistic security isn't so much a matter of deploying the right solution as much as it is getting the entire organization to embrace a security state of mind.

Implementing a holistic security strategy means moving your organization from a technology-centric to a business-centric security process to assess risk and manage potential threats. Executive management needs to drive security as an organization-wide priority, so everyone understands his or her level of responsibility, accountability, and authority. That's one reason the Chief Security Officer (CSO) and Chief Information Security Officer (CISO) is emerging as the newest key member of the executive team.

A recent survey conducted by Deloitte & Touche Tohmatsu revealed that among 35 percent of the world's top 500 financial institutions surveyed, 39 percent had their IT systems compromised in the last year, and only a fraction of those attacks were mounted from within the organization (counter to popular belief). The survey also revealed that only five percent of companies were "extremely confident" that they were safe from an internal cyber-attack, and 13 percent were extremely confident they were secure from external threats. In response to the growing concern over cyber-security, more than 61 percent reported having a CSO or CISO as part of the executive staff, and 14 percent reported having more than one C-level executive responsible for security.

To keep their data secure, these companies are adopting a holistic security strategy that embraces the whole organization and infrastructure. Holistic security means balancing technology, procedures, and people. It also means balancing the factors of mitigating risk, enhancing productivity, reducing cost, and streamlining application development and integration.

### **Nurturing Access with Accountability**

In today's world of Internet-driven business, too much security can be as disastrous to operations as too little security. You want to keep your systems sufficiently "open" to promote employee productivity, online customer support, and third-party Internet collaboration. Promoting global access to support B2B and B2C business models means you need to support more access points and Internet portals while managing more user access requirements. This also means a new approach to security: access with accountability. Rather than making security the moat around an impregnable IT system, security becomes the conduit for safe access and open information exchange.

Your first step is to audit your infrastructure to assess potential threats in light of other factors, such as productivity and the cost to secure your systems, and setting holistic risk management objectives. Take stock of all the company's assets, including the building, equipment, finances, products, services, personal, information, and even reputation, as well as the IT infrastructure, taking into account possible threats and exposure from employees, contractors, suppliers, and others. In assessing these assets, ask yourself three key questions: What can go wrong? What will most likely go wrong? What are the consequences if something does go wrong?

The key to effective risk assessment starts with good communications among all departments. In order to take inventory of potential risks, assess their probability, and prioritize those risks based on their potential impact on the organization, you need input from all the stakeholders, which may require regular department meetings and an efficient reporting structure. If you understand that eliminating risk is not achievable and that your overarching objective should be to promote secure connectivity, it will help you prioritize your risk and balance productivity, cost, and integration.

### **Using Technology to Enforce Policy Management**

Policies and procedures to manage provisioning and system access are also critical and should emerge from your internal research. This means creating a common set of procedures, documenting them, distributing them, and abiding by them to the letter. As part of your holistic security strategy, you need to get all departments working together through a central provisioning system. In the past, allowing accounting, IT, customer support, and other stakeholders in the organization to manage their own systems was the norm. Today, you need to consolidate security management, which not only centralizes control but also lets you bring security issues back into the boardroom. It's easier to manage corporate assets from the top down, than taking inventory and managing the process from disparate departments.

Technology can help. For example, an identity management system can consolidate access management to mitigate risk. Where in the past, there were different systems and passwords for e-mail, purchase orders, timekeepers, accounting, and other applications, using sophisticated identity management software, you can consolidate administration through a single database that keeps track of users, their access rights, and can turn applications on and off from a single access point.

Companies are not, however, putting all their security eggs in a single database basket. Consolidating user security has the advantage of centralizing administration so access through all departmental applications is consolidated at a single point. Today's companies recognize that they can't manage what they can't see. While they need to keep operations distributed, but within a common security framework that supports a cost effective security management system. If you think about security as you are deploying the database, operating systems, IT applications, and related technology, it will promote affordable holistic security.

### **Promoting User Security Through Education**

While a central identity management system can help address security problems from within the employee ranks, you still need to be wary of external intruders. Educating the system users should be your first line of defense.

A recent survey conducted at Infosecurity Europe 2003 revealed that 90 percent of workers approached at Waterloo station were readily willing to surrender their corporate passwords in exchange for a cheap pen. Hackers rely on the gullibility of system users to gain access to secure networks. Security officers should educate users about the need for security and help them understand the importance of keeping sensitive company information, like user passwords, safe and confidential.

Finally, you will have to contend with the legislative challenges of system security. Particularly in North America, emerging regulatory standards such as HIPAA and Sarbanes-Oxley are imposing new fiduciary responsibilities on corporate executives to protect company assets, including company and customer data, with responsibility for liability down the line. In Europe, emerging standards such as BS7799 and ISO 17799 are imposing similar security mandates, such as the creation of a common risk language. These legislative efforts can work in your favor, imposing a structure on your organization that promotes communication, drives consensus about security policies, and leads to access with accountability.

Your ongoing challenge is to change corporate thinking and establish sustainable, cost-effective business standards that encompass a common risk language across all departments. This will help engrain security into the organizational consciousness and create blueprint for security, manage process enhancement and change, deploy new business applications within the parameters of the risk profile, and monitor performance. This top-down approach using information provided from the bottom up forms the

foundation of a holistic approach to enterprise security that will stand you and your organization in good stead, no matter what may come.

Sidebar:

### **The Core Elements of Holistic Security**

- Executive leadership drives security so everyone in the organization understands his or her level of responsibility, accountability and authority
- Executive management support provides sufficient resources
- Company offers a well-developed security awareness and training program
- Security policies and standards are well documented and follow business governance and operations architectures, and are supplied to everyone in the organization
- Key performance indicators that measure the efficiency, effectiveness, value and continuous performance improvement of each individual security process
- Cost effective technical security architectures meet the objectives of reliability, availability, manageability, scalability, performance, flexibility and security
- Security approached from an operational versus technology perspective
- Security as core business processes, appropriate for your company's culture, that align policy, technology, roles, responsibilities & structures, operating procedures and key performance indicators
- Well-defined, comprehensive security philosophy with a constant vigilance approach.