



Five Easy Tips for *Effectively Adopting Security*

By Claudiu Popa, CISSP, PMP, CISA
President, Informatica Corporation

Every year, our security consultants encounter a wide variety of companies, firms of different sizes that play distinct roles in their respective industries. Some are in a position to mitigate all sorts of risks to information assets, but they are in the minority. The vast majority of companies have adopted controls that are considered standard (firewall, anti-virus, locks on server room doors, etc), but there is a general consensus among the staff that the really valuable assets of the firm continue to be exposed to risk. Management knows this but is often afraid of spiraling security costs once the decision is made to at least look into the company's level of exposure, called the company's security posture.

I have compiled a list of no-nonsense recommendations to help anyone tackle that challenge, and mitigate the vast majority of the risk to their business. These are simple, require little effort and their corresponding investment can easily be contained. Here they are:

1. **Tackle the biggest risks first**

You know what's most valuable to you. Your financial data, private client information, trade secrets, intellectual property are all critical information assets and represent a small portion of the company's overall volume of data. You already know where they are stored, how they are used, transported and safeguarded. These represent at least 80% of all information asset risk and most of the value of the organization. Plan to protect them first and look for weaknesses in the security controls already in place.

2. **Think from the top down**

What does it take to have an overarching plan for security protection? Simply, management accountability. Once a strategic commitment is made to embrace security, everything flows naturally from it. Policies, procedures, communications, techniques and tools all fall into place within the larger set of business activities. Organizations are always surprised at the elegance and ease with which good security solutions fit within their business process.

3. **Good security is layered security**

Layered security applies to people, processes and technology. The organizational structure must support accountability and adequately delegate tasks with increasing granularity. Business processes and procedures need to follow policies and incorporate controls and monitoring that can be used by people and technology to close security gaps and provide on-going security throughout the organization. Overlapping security controls strengthen security, but redundancy weakens it. Eliminate or redirect unnecessary efforts that duplicate activities.

4. **The weakest and the strongest links are the same**

People continue to play a key role in the effectiveness of every organization's protective envelope. When adequately educated and empowered, accountable employees contribute to the application of policies, controls and monitoring to strengthen security and address gaps that technology simply cannot. Without proper guidance, communication and tools, employees cannot be expected to play an active security role. In such situations, people can accidentally cause security breaches through sheer apathy. In the absence of accountability, cases of malicious damage and internal security breaches can only rarely be punishable by law.

5. **Do not sacrifice productivity**

It is a common misconception that security and productivity are at odds with one another. All too often, companies force unrealistic controls upon employees that have for effect to essentially lower security when people create workarounds and otherwise reject complicated, ineffective tasks. While convenience can be sacrificed for the sake of security, compromising productivity is never a good idea. Understand the difference.