Placing Strategic Security on the Front Burner Starts with Policy

by Adam Lipson

Given a choice between spending money on ERP (Enterprise Resource Planning) or information security, organizations typically choose the former. Information security does not generate revenue, reduce cost or drive innovation. Nonetheless, most organizations acknowledge that ignoring the issue may result in business stoppage, lost dollars, internal clients who lose confidence in their IT departments and diminished brand value to the outside world.

Unfortunately, most companies spend their precious IT security dollars on the tactical rather than the strategic application of security. All too often, time is spent investigating a breach rather than architecting secure solutions, scanning a firewall rather designing a flexible and secure perimeter, reacting to a termination with cause rather than developing an effective employee termination procedure.

Strategic security, like all other areas in IT, must be far-reaching and holistic. To achieve this goal, organizations must start with an over-arching policy framework upon which all other areas rely for guidance. To be effective, all components of a strategic security program cleave to the framework. Without it there is no program – only tactical response!

The absence of a policy, and ultimately a strategic security program, leaves an organization courting danger – in "react mode" rather than in "respond mode." The following components of a strategic security program* play a critical role in assuring business operations:

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management

- Compliance

These components all hinge on the existence of the first – a simple, clear and far-reaching policy.

At the highest level, information security policy dictates what is permitted, what is prohibited and what is required. It informs topics such as policy authority, governance, information classification, roles and responsibilities, physical access control, logical access control, network and communication management, secure system configuration, operational procedures, compliance monitoring and disaster recovery.

While most organizations view policy development as simple, an informal survey of corporate entities suggest otherwise. Most organizations report they have "pieces of policy" while few have comprehensive, enterprise-wide policy serving as the basis of their strategic programs.

Great policy is static. It is flexible. Most importantly, it has a layered and atomic nature that withstands the test of time.

Perhaps the best example of policy that touches all of our lives is the Constitution of the United States. It serves as the basis for all government, and by extension, all of our society. This strategic policy has existed for more than 225 years with few amendments. It states in simple and concise terms what is permitted and what is prohibited. It is not a law, but is the basis for all laws. It is the reason that the United States, one of the youngest countries on the globe, is the sole remaining super power.

Imagine the United States without the Constitution. Imagine designing an ERP solution without a strategy. Then imagine designing a security program without a policy.

Policy is the starting point and the foundation upon which a credible security program is based. Without it there is no program – only tactical response. This is your starting point.

Adam Lipson is president and CEO at Network & Security Technologies (www.netsectech.com), a leading provider of digital security consulting solutions.

[*] The International Organization for Standardization (ISO) has published this standard to provide organizations a common basis for measuring the completeness of their security program.