

SECURITY CONVERGENCE

Maximizing Security ROI in Today's Business Enterprise



Presented by Steve Lasky,
Publisher/Editor-in-Chief
Security Technology & Design magazine

February 7, 2006

The Meaning of Convergence



This new paradigm captures a significant shift in emphasis from security as a purely functional activity within an enterprise, to security as a “value add” to the overall mission of business

The Business of Security



Security professionals have to reexamine the key operating levers available to them ---

- Roles & responsibilities
- Risk management
- Leadership

New Technologies, New Threats



- As new technologies emerge and threats become increasingly complex and unpredictable, senior security execs recognize the need to merge security function throughout the enterprise
- To be effective, a converged approach must reach across people, processes and technology
- The end result enabling enterprises to prevent, detect, respond to and recover from any type of security incident

Imperatives Driving Convergence



Security Convergence: A Trend Affecting Global Enterprises



- **Rapid Expansion of the Enterprise Ecosystem**
- **Value Migration from Physical to Information-based & Intangible Assets**
- **New Protective Technologies Blur Functional Boundaries**
- **New Compliance & Regulatory Regimes**
- **Continuing Pressure to Reduce Costs**

Rapid Expansion of the Enterprise Ecosystem



- In today's global economy, outsourcing & emerging technology are creating more interconnected environments, expanding the enterprise ecosystem into a much larger, complex system
- Organizations are increasingly relying on external partners as integral components in their daily business
- Enterprises now must consider the integrated security implications of outsourcing specific functions to other companies and manage alliances that will create a competitive edge

Rapid Expansion of the Enterprise Ecosystem



- The rapid expansion of the enterprise ecosystem also requires that the private sector establish strong relationships with the public sector
- Enterprise leaders should establish uniform security language in contracts using standards and guidelines
- Learn the business! Security professionals must continue to develop staff with knowledge that can interact with external stakeholders to serve as liaisons to the overall business

Value Migration from Physical to Information-based Assets



- Company assets are becoming more information-based & intangible
- Even most physical assets now rely on information and secured databases

Value Migration From Physical to Information-based Assets



- Because information and secured databases are increasingly a product of physical assets, there is an even greater need for the integration of physical and information security issues
- Security personnel who understand physical and information security can evaluate a wider view of risks and vulnerabilities
- Understanding what the business drivers are is crucial for security convergence to occur

New Protective Technologies Blur Functional Boundaries



New and emerging technologies designed to improve physical & information security are crossing over departmental silos, forcing security organizations to work together for the common goal of protecting the enterprise and realizing business goals

New Protective Technologies Blur Functional Boundaries



- **Assets, whether physical or information-based, have physical and information security related risk**
- **In order to facilitate security convergence triggered by this blurring of functional boundaries, enterprises are learning that interdepartmental cooperation can greatly leverage the budget process**
- **Companies must integrate risk agendas into shared business initiatives**
- **It is critical to develop relationships with people across functional boundaries to enhance security convergence**

New Compliance and Regulatory Regimes



With new threats and business procedures becoming more intricate, it follows that adherence to regulations and compliance guidelines will become even more complex

Legislation like Sarbanes-Oxley, HIPAA & Gramm-Leach-Bliley have escalated pressure on organizations to efficiently address enterprise security issues



“Mere compliance to stay out of jail is of no real use to the company or its employees.”

Continuing Pressure to Reduce Costs



- **Enterprises will constantly wrestle with balancing risk/reward tradeoffs**
- **Security convergence is forcing companies to look beyond functional restraints to include all parts of the security and business life-cycle, which creates a need for a unified security framework**
- **Security leaders must prioritize all enterprise risks so that the business can focus spending on critical risks to optimize investment**

Continuing Pressure to Reduce Costs



- **Enterprise Security Organizations should streamline and simplify budget requests, plus use a common language**
- **Communication between and among departments is critical during the budget process**
- **Organizations must define their ROI challenges with careful risk analysis and establish spending guidelines that will enhance security convergence**

Continuing Pressure to Reduce Costs



Facilitating Convergence

- Migrate from insurance focuses to enterprise-wide view
- Help develop active C-Level awareness and involvement
- Develop shared common processes focused on the business

Benefits of Convergence

- Ability to escalate projects
- Competitive advantages through enhanced productivity
- Improved capital allocation
- Cost reduction
- Collaboration & interoperability

State of Convergence



Last Words



The convergence of security within enterprises is rapidly emerging, so business leaders need to recognize this emergence and begin to adapt accordingly!

ROI & Security Convergence



**Security Technology & Design magazine can
be subscribed to at
www.securityinfowatch.com**

**Steve Lasky
Publisher/Editor-in-Chief
770-886-0800 ext. 221
steve.lasky@cygnuspub.com**