

Increasing the Business Relevance of Security Resources

A Holistic Strategy Emphasizing Business Value

Author

Chuck Adams

Contributor

Joanne Bethlahmy

October 2009



Cisco Internet Business Solutions Group (IBSG)

Increasing the Business Relevance of Security Resources

A Holistic Strategy Emphasizing Business Value

When the economy declines, everyone tightens their belts. Budgets are slashed. Programs that don't contribute to the bottom line are eliminated. Managers must continually find new ways to do more with less.

Enterprises must be quick and agile in responding to the volatile economy. Every department and function must prove its worth. That is why, in times of boom or bust, it is important for security professionals to align with business objectives and clearly explain the critical role security—in all its guises—plays in driving corporate success.

The security organization in many enterprises today is viewed primarily as a defensive function. Senior leaders often consider it a “necessary evil” with little value beyond loss prevention.¹ When business leaders do not understand the potential value the security organization can bring, they may unintentionally initiate a “self-fulfilling prophecy” where security fails to add business value because no one expects it—or equips it—to do so. Unless current perceptions change, security resources will be at risk.

Today's security solutions—especially those employing modern video surveillance and analytics—can provide new opportunities for revenue generation and customer loyalty. This potential, however, typically goes unrecognized. Top-level executives seldom consult the security team about new market opportunities or insights on increasing enterprise efficiency—primarily because they don't know they should ask.

Security leaders must articulate their ability to support business strategies and add value beyond loss prevention. This will require a unified risk-management strategy, and a broader view of how to use security resources more fully. The possibilities are enormous, with the potential to extend throughout the value chain for every business, operation, and industry across the globe. This paper illustrates some of these possibilities.

Security Performance Has Been Fragmented, Ineffective

Most people claim to know very little about the security industry, yet these same people employ security mechanisms hundreds of times a day. Everything ranging from seat belts and airbags to bicycle helmets and business contracts are mechanisms that relieve some level of risk. Security technologies are simply those that offer the advantages of task and control automation for protecting physical or digital assets. In most enterprises, security is initially seen as supplemental to core functions. But as security practices become accepted, it is reasonable to expect they will be slowly integrated into core functions.

Cyber and physical security organizations, however, continue to be myopic in making security investment decisions. Buying decisions often are made in a disjointed manner, with little consideration for interoperability or alignment with overall enterprise objectives or risk-management strategies.

¹ Information World Review, Martin Courtney, IT Week, June 2007 (quoting Accenture survey).

The global physical security market was estimated at roughly US\$170 billion² in 2007, with services representing about 45 percent of the total. This means global spending on services such as assessments, patrol guards, viewing of video surveillance monitors, intelligence collection, integration, evidence analysis, and investigation support totaled about \$75 billion. Products and technologies accounted for the remaining \$95 billion. Global cyber security expenditures top US\$20 billion³ yearly.

This spending, however, has not solved the problem. Annual losses associated with cyber security attacks have exceeded US\$1 trillion.⁴ For an example of physical security ineffectiveness, simply look at the September 11 experiences. Although U.S. spending exceeded \$329 billion⁵ for national defense in 2001, the country remained vulnerable to an attack that resulted in thousands of casualties and untold economic losses.

These dynamics lead to the conclusion that we are doing something fundamentally wrong in security; our investments are not achieving the business value we need.

Evolving Security Within a Unified Risk-Management Vision

Business resiliency involves much more than just the creation and implementation of security policy. A comprehensive risk-management strategy is built around an integrated framework of people, processes, and technology (see Figure 1).

Figure 1. Key Elements of Resiliency



Source: Gartner, Principles of Organizational Resilience

For security to become more effective, influential, and relevant across the enterprise, it must become more integral and pervasive, acting within an all-encompassing vision. All traditional security functions—both physical and cyber—must evolve toward a consolidated, unified risk-management platform. When something unexpected happens

² 2007 Security Industry Annual, Lehman Brothers, November 2007.

³ Global estimate developed by gathering projections across major market segments of content and network hardware and software security, VPN, and services. Sources of information are InfoWorld, Infonetics, and Gartner articles published in 2007.

⁴ "Unsecured Economies: Protecting Vital Information," McAfee, January 2009.

⁵ Report published by Homeland Security Market Research, February 2006.

that negatively impacts the enterprise, security leaders must take responsibility and work to improve the processes. Enterprises must learn to hold security accountable for awareness and continuous improvement. Conversely, they must also seek insights from the security team to learn how security tools and expertise can contribute to the company's larger business goals.

Once a consolidated strategy is defined, every dollar spent must be scrutinized and maximized, with a focus on interoperability and analysis methods that turn data streams into accurate, actionable information. This will result in a more rational, unified, risk-based decision-making process. To realize this vision, all security mechanisms must be designed and implemented in a manner that is consistent, follows industry standards, and is conducive to cross-technology analysis methods. They must also generate alerts when issues occur, regardless of the device that detects the event. Additionally, processes designed to control behaviors and/or respond to issues must be synchronized to enforce common policies, whether they are physical or digital.

Security leaders should also begin to educate the enterprise on the vision and significance of unified risk management. They must start to redefine expectations to prepare for the transition to broader information collection and analysis.

Security Opportunity: Data Collection and Analysis

When security is compromised, businesses lose productivity, resource availability, and, ultimately, brand value. A security breach—physical or digital—has the potential to detrimentally affect the people, equipment, and systems on which an enterprise relies to achieve its objectives. Therefore, business leaders need to evaluate all risks in a way that aligns the level of resilience with the enterprise's business objectives.

A security failure is not necessarily due to lack of information; most technology-enabled enterprises have a wealth of relevant data. The problem is that this information is not typically produced and accessed in a way that enables effective decision making. This is especially true in the emotionally charged atmosphere of a security crisis, where high-stakes decisions must be made quickly based on the best available information. The challenge and opportunity for security leaders is to show that their teams have the skills needed to harvest accurate, actionable, and timely information from the cyber realm.

Mature, effective security organizations have a comprehensive risk-management strategy and an integrated set of security technologies and tools that align with the enterprise's business objectives. They thrive when challenged to find the proverbial "needle in a haystack." Their data collection and analysis methods can deliver significant value when applied to problems of any nature being considered by business leaders.

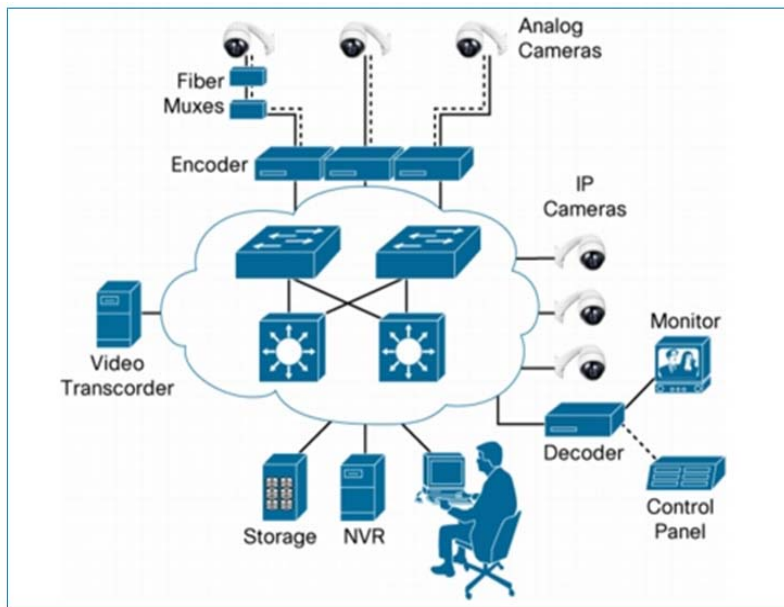
They can be particularly effective when their physical and cyber security resources are consolidated and integrated. For example, with the advent of IP video, physical security can benefit from traditional cyber security analysis methods, and vice versa. These security functions must work closely together, share models, and integrate their processes to complete the overall risk-management picture. When they are part of an integrated approach to information gathering, the digitization and networked capabilities of next-generation video surveillance technologies can produce a wealth of high-quality information for analysis.

Funding the Strategy

The Cisco® Internet Business Solutions Group (IBSG) believes that the efficiency and value gained from consolidating physical and cyber security functions, and from deploying advanced video and analytics capabilities, can make these improvements virtually self-funding. Let's take a look at how this might happen.

The most interesting and relevant technology trend is the migration from analog to digital for video surveillance. When this is combined with innovations in video analytics and the ability to store and retain digital video on a standard, open communications platform, you have the ingredients for transformation. Digitization of video surveillance cameras and advances in encoding and compression enable the distribution and storage of video on a data network. In turn, this unlocks the potential to develop codified, automated analysis that emulates tasks that have, until now, been left to humans (see Figure 2).

Figure 2. IP Network-Centric Video Stream Management; Hybrid and IP Monitoring and Recording



Source: Cisco, 2008

At a glance, the efficiencies of digital video and automated analytics are extremely attractive, as is the potential for consolidating resources across physical and cyber security functions. This would be true if everything else stayed the same and enterprises simply automated video analysis. But something different is required to keep pace with the industry and effectively combat new and evolving threats. Today, we have an ideal opportunity to redefine the way security dollars are spent, to enhance risk-management effectiveness, and to boost the value of security to the rest of the enterprise.

As mentioned earlier, estimated annual global spending for physical security services is about US\$75 billion. Enterprises currently employing video surveillance as a detection and prevention mechanism can essentially exchange traditional service budgets for more comprehensive and effective video surveillance technology. This must be executed carefully, as any alterations to existing capabilities will directly affect the current risk profile. As part of a unified risk-management strategy, however, using service budgets to offset the

costs of new video and analytics technology can assure a significantly more resilient risk posture without increasing overall security spending.

Moving Beyond Security To Deliver Broader Business Value

Digital video camera surveillance and embedded analytics represent a major investment that may be difficult to justify based purely on “prevention.”

The potential uses for video analytics, however, go far beyond traditional security. Investments in digital surveillance technology can now be translated into revenue and profit. Major retailers, hotel chains, transportation companies, and other consumer service organizations are starting to employ video analytics to track customer traffic patterns in order to improve operational efficiencies, increase promotional effectiveness, and deliver better customer service.

Among other applications, video analytics can monitor queues at cash registers; determine how long customers are waiting to be served; watch how customers move around a store, a casino, or an airport to help improve product or display placement; monitor out-of-stock products on shelves; or measure the effectiveness of digital display advertising. Alerts can be sent to address issues in real time; analytics can calculate the ROI of promotions or staffing changes; and employees can be observed and trained.

Security executives should become familiar with the many uses of video analytics and present these opportunities to operations, merchandising, or marketing leaders. By demonstrating value and relevance to the core of the enterprise, the security organization can increase its influence and improve the business case for a proposed digital camera investment.

Getting Started

Every risk decision maker and security manager should begin to evaluate the overall risk-management model and prepare to transform his or her role and organization. Begin by taking the following steps:

- Design a comprehensive and holistic strategy for security, and advocate the value of execution to leadership and peers
- Consolidate physical and cyber security resources
- Reallocate service budgets to fund unified risk-management consolidation programs
- Transform risk-management procurement processes and purchasing criteria to focus on interoperability and alignment with unified risk-management strategy
- Evaluate the benefits and advantages of networked, digital video surveillance to enhance detection and enable digital, automated analytics
- Become familiar with uses of digital video surveillance analytics beyond security to enhance core company operations and gain additional financial justification for investment

Knowledge is power. By consolidating traditional security functions under a unified risk-management vision, security leaders can create a single information-harvesting and analysis center uniquely positioned to become an executive intelligence powerhouse.

For more information on how you can structure your security approach to deliver the greatest value, contact Chuck Adams, Cisco IBSG Innovations Practice, at cjadams@cisco.com.

More Information

The Cisco Internet Business Solutions Group (IBSG), the global strategic consulting arm of Cisco, helps CXOs and public sector leaders transform their organizations—first by designing innovative business processes, and then by integrating advanced technologies into visionary roadmaps that address key CXO concerns.

For further information about IBSG, visit <http://www.cisco.com/go/ibsg>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)