Business-driven security
White paper

Take a holistic approach to business-driven security.

March 2008

IBM Service Management
Visibility. Control. Automation.™

Contents

Overview

Today's corporate leaders face multiple challenges, including the need to innovate in extremely competitive business climates, address highly dynamic regulatory and compliance challenges, speed returns on investments to counter shrinking IT budgets and secure the enterprise against a wide barrage of new and evolving sophisticated threats. However, unlike other business challenges, organizations typically take a technology-driven approach to securing their infrastructure, when in reality, a business-driven approach is warranted.

A business-driven approach to security is unlike a technology-centric approach in that the business goals drive the requirements in securing the enterprise. Organizations often take a bottoms-up approach to security because security solution vendors typically promote this approach to their clients. To close identified security gaps, enterprises broaden and bolster their defenses by continually building on top of or adding to their existing security investments. This technology-centric methodology often creates an excessively complex and disjointed security infrastructure. It becomes difficult to manage and prone to unseen vulnerability gaps, needlessly escalates IT costs and eventually fosters unnecessary operational inefficiencies that inhibit business growth rather than enhance it.

Instead of trying to protect against every conceivable threat, organizations should understand and prioritize the security risk management activities that make the most sense for their organization. By understanding the level of risk tolerance within an organization, the IT team can more easily focus on mitigating risks that the organization can't afford to neglect. Overemphasizing certain risks leads to wasted resources and efforts, while underemphasizing others can have disastrous consequences.

Organizations can find it difficult to achieve a strategic, end-to-end security approach that supports business goals such as driving innovation and reducing organizational costs, as well as operational requirements to address

> "Every business continuously balances risk and reward to find a way to achieve the best returns at an acceptable level of risk. For IT security professionals, this is the most difficult part of the job: objectively analyzing risk in the context of the business goals and possible return on investment. It may seem counterintuitive, but the end-goal for the business as a whole is not to achieve zero risk — shutting down would be the best way to achieve that, just as the server least vulnerable to attack is the server that is not turned on. Rather, the business goal is to allow the maximum acceptable level of risk — to live at the limit of the organization's 'risk tolerance.' Every business decision is about risk — getting the maximum return for a given level of risk; IT decisions are no different."[1]

compliance measures and protect against internal and external threats. This paper introduces actions that organizations can take to drive security efforts from a business and operational perspective and discusses how security leadership from IBM can help enable their success.

Optimize and protect business processes

The common security model ingrained in today's corporate world involves implementing a broad set of capabilities to protect against the most publicized threats of the day. This security approach results in the deployment of an array of siloed security tools. Not only do these tools lack the means to work together to effectively protect against today's highly sophisticated and organized attacks, but they can hinder business operations, generate cost redundancies, create IT complexity, operate in isolation of business objectives and fail to provide appropriate metrics to allow today's business-minded security executives to determine their effectiveness.

Security should not be addressed in isolation from other business activities within the enterprise. Instead, it should be viewed from a business perspective – looking at security as a means to protect and enhance business processes. In most organizations, the 80/20 rule applies in this regard. Most organizations have just a handful of business processes that make up 80 percent or more of their risk, while they might have many other processes that account for less than 20 percent of their risk. To align security efforts with business concerns, organizations should focus on securing those few processes that make up the bulk of the risk. They must also prioritize risks and vulnerabilities based on their potential to disrupt the business' most critical processes.

This strategy involves a level of planning and assessment to identify risks across key business areas, including people, processes, data and technology throughout the entire business continuum. Such planning can facilitate the

A recent survey of consumers conducted by Cyber Security Industry Alliance found that:

- 44% of respondents feel their information is safe when engaging in e-commerce.
- 50% avoid making purchases online because they are afraid their financial information will be stolen.
- 94% say identity theft is a serious problem.
- Only 24% believe businesses are placing the right emphasis on protecting information systems and networks.[2]

design and building of a business-driven security blueprint and strategy that can act as an effective shield of defense for the entire organization – to meet business needs and optimize business results.

Secure business processes across all risk domains

IT decisions, like business decisions, are about getting the maximum return for a given level of risk. Five key security areas or domains need to be examined for their potential risk elements and impact. Within these domains, it is critical for the organization to define and manage the maximum level of acceptable risk. No organization can (or even should from a cost perspective) remove all risk, but organizations must objectively analyze risk in the context of the business goals.

- **People and identity** – Businesses need to make sure people across their organization and supply chain have access to the data and tools that they need, when they need it, while blocking those who do not need or should not have access. Key business challenges that must be addressed in this domain deal with the ability to effectively manage the on-boarding and off-boarding of dynamic work forces, as well as the need to improve secure collaboration among customers, suppliers and business partners. Additionally, IT compliance continues to be a concern within organizations and is a significant driver for implementation of comprehensive user provisioning processes. An appropriate set of security controls should be put in place to successfully manage user privileges across multiple technology systems and to ensure that end users have access to the right IT resources, according to predetermined policies.

- **Data and information** – Organizations need to support widespread electronic collaboration, while protecting their critical data – whether it's in transit or at rest. They need to understand where their critical data lives and have methodologies in place to manage all of the processes associated with classifying, prioritizing and protecting data. Effective information security starts with a risk management approach that balances risks and rewards against availability and confidentiality of data. This approach should be undertaken in a way that safeguards the value of all volumes of data that

Highlights

flow throughout the business from misuse and abuse. A key concern for many organizations is how to implement such a comprehensive data security solution with limited staff and expertise. Putting processes in place to achieve, measure and report on an organization's IT compliance posture is an example of a process relative to securing data. Identifying, prioritizing and protecting sensitive data, as well as demonstrating effective security controls, are critical elements to enabling and protecting the value of information to the business.

- **Applications** – Enterprises need to preemptively and proactively protect their business-critical applications and processes from external and internal threats throughout their entire life cycle – from design to implementation and production. This typically requires a combination of capabilities such as centralized authentication, access and audit policy management, Web application vulnerability scanning and intrusion prevention. Whether the application is internally focused such as a customer relationship management (CRM) system delivered through a service oriented architecture (SOA) or an externally facing application such as a new customer portal, clearly defined security policies and processes are critical to ensure the new application is enabling the business rather than introducing additional risk.

- **Network, server and end point** – Proactive threat and vulnerability monitoring and management of an organization's network, server and end points are critical to staying ahead of emerging threats that can adversely affect system components and the people and business processes they support. The need to identify and protect against emerging threats has dramatically increased with the rise in organized and financially motivated network infiltrations. For example, enterprises leverage virtual technology to support their goals of delivering services in less time and with greater agility. By building a structure of security controls within this environment, organizations can reap the goals of virtualization – such as improved physical resource utilization, improved hardware efficiency and reduction of power costs – while gaining peace of mind that the virtual systems are secured with the same rigor as the physical systems.

The need to identify and protect against emerging threats has dramatically increased with the rise in organized and financially motivated network infiltrations

- **Physical infrastructure** – Protecting an organization's infrastructure means ensuring that its physical assets are also protected from security threats. Effective physical security requires a centralized management system that allows the monitoring of property, employees, customers and the general public. For example, securing the perimeter of the data center with cameras and centralized monitoring devices is critical to ensure access to an organization's IT assets is managed. Therefore, organizations concerned about theft and fraud, such as banks, retail stores or public agencies, should define and implement an integrated physical security surveillance strategy that includes monitoring, analytics and centralized control. This approach enables organizations to extract intelligent data from multiple sources, respond to threats sooner than manually monitored environments, and reduce cost and risk of loss.

Every organization should understand and manage risk in all five of these domains. Unfortunately, most security vendors tend to only focus on one or two domains, or worse, they only focus on securing a single technology within a domain. This results in point solutions that fail to provide protection across the business processes within the organization. It also leads to the creation of security silos that increase complexity, introduce redundancy, leave vulnerability gaps and ultimately fail to meet the organization's overall business needs.

Elevate IT security to a business-driven approach

Today's executives are expected to manage risk in their areas of responsibility in the same way that CFOs manage risks in their domains. Security risks and the potential impact on IT need to be communicated to executive peers in business terms. Additionally, they need to align IT security controls with their business processes, monitor and quantify IT risk in business terms, and dynamically drive business-level insight at the executive level. They need to manage risk and orchestrate security operations in a way that enforces compliance and optimizes business results.

Highlights

IBM provides the full breadth and depth of solutions and services that enable organizations to take a business-driven, holistic approach to security in alignment with an IT governance framework

As an organization secures its business processes, a business-driven approach needs to become the guiding influence for ensuring that all the different security domains work together in a holistic and synergistic manner, in alignment with the overarching business objectives. Otherwise, the organization's risk stance becomes vulnerable due to misalignment of priorities between IT and the business strategy.

Aligning IT security with a business-driven approach can also put organizations in a position to have their unique business objectives drive their compliance goals, rather than having compliance drive their business. Too many organizations invest significant time and money to ensure that they can comply with industry and government regulations, only to find out too late that their key business processes were still vulnerable to attack. Leveraging security management from a business-driven perspective enables them to successfully secure those business processes in a manner that inherently provides the necessary evidence to demonstrate compliance.

Maximize business success with IBM

Ranked as a top security provider by industry analysts, IBM provides the full breadth and depth of solutions and services that enable organizations to take a business-driven, holistic approach to security in alignment with an IT governance framework. IBM capabilities can empower organizations to dynamically monitor and quantify security risks, to better understand threats and vulnerabilities in terms of business impact, to better respond to security events with security controls that optimize business results, and to better quantify and prioritize their security investments. IBM helps organizations simplify and automate their business controls for significant cost savings, while enabling the business to make more informed decisions about allocating funds and resources for managing security risks and supporting greater business value for the enterprise.

IBM offers an unparalleled capacity to focus on driving business innovation and securing operational processes across all risk domains. Its comprehensive solutions and services encompass identity and access management, information and data security, application security, threat and vulnerability management, and physical security to enable organizations to reduce the complexity of security within their enterprise and implement a holistic security management strategy that optimizes business results.

For more information

To learn more about how IBM security services and solutions help organizations holistically orchestrate and implement security across the enterprise for maximum business success, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/itsolutions/security

About IBM Service Management

IBM Service Management helps organizations deliver quality service that is effectively managed, continuous and secure for users, customers and partners. Organizations of every size can leverage IBM services, software and hardware to plan, execute and manage initiatives for service and asset management, security and business resilience. Flexible, modular offerings span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards–based technology. IBM acts as a strategic partner to help customers implement the right solutions to achieve rapid business results and accelerate business growth.

IBM Corporation
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
March 2008

[1]"Information Risk Management in the Enterprise," John Burke, Principal Research Analyst, Nemertes Research, 2008.

[2]Cyber Security Industry Alliance survey of consumers (2007).

GMW14008-USEN-00