Information risk management solutions
White paper

Create a secure collaborative environment.

December 2007

IBM Governance and Risk Management
Business alignment, visibility and control

Contents

Introduction

Effective use of information helps drive innovation – and a recent study suggests that five times more value is created by organizations that use information effectively.[1] Often, the most effective use of information is sharing it with other entities, such as other lines of business, partners, distributors and customers. In fact, today's organizations need collaboration to thrive. For example, a distributed product development process enables companies to compete more effectively by specializing in the areas where they have competitive advantages. It also helps them accelerate the speed with which they deliver a product or service to market.

The problem with collaboration is that sharing information exposes organizations to increased risks, including theft, alteration, damage and destruction. If information is too available and accessible, it can fall into the wrong hands. Isolation inhibits collaboration and hence business innovation and growth. A delicate balance must be maintained – keeping information secure from prying eyes, but making it easily available to those who can use it to enhance business performance.

This paper describes best practices for maintaining information security – while enabling innovation through business collaboration. In addition, it describes the IBM portfolio of information risk management solutions – including software, hardware and services – that help organizations create secure collaborative environments.

Highlights

A properly balanced information risk management security strategy helps the business enable collaboration, protect the IT infrastructure and support compliance initiatives

Apply a risk management approach to information security

Risk management is often thought of as *removal* of risk. But properly applying a risk management approach actually means *balancing* risks associated with an activity against the activity's rewards for the business.

When creating a collaborative work environment, risk management requires a balance between the availability and confidentiality of information. This challenge is difficult but rewarding, because a properly balanced information risk management security strategy helps the business:

- *Enable collaboration* — by facilitating access to information by authorized parties.
- *Protect the IT infrastructure* — to help protect the continuity of systems and processes that support the flow of information within and outside the enterprise.
- *Support compliance initiatives* — through the implementation and monitoring of controls that protect the confidentiality, integrity and availability of information.

Engage in a four-stage process to achieve information security success

Sophisticated information security programs are designed to achieve this delicate risk balance. These programs leverage best practices around risk management and IT operations principles and implement integrated, phased approaches like below:

1. ***Assessment,*** in which IT and information security priorities, vulnerability and risks are evaluated
2. ***Planning,*** in which information security processes, then policies, are analyzed and defined
3. ***Implementation,*** in which information security controls are designed and deployed
4. ***Management,*** in which the security infrastructure is monitored and controlled

Highlights

Enterprises must keep current with ever-evolving threats and vulnerabilities to continuously prioritize their security initiatives

Assess information security priorities, vulnerability and risks

The first step in assessing an organization's information security posture in the context of collaboration is to determine where its sensitive information resides. That way, the information can be classified and the vulnerabilities that surround the information can be identified and prioritized. Subsequently, the organization can identify and prioritize gaps in current security systems.

This is not a one-time activity, but an ongoing process. Enterprises must keep current with ever-evolving threats and vulnerabilities to continuously prioritize their security initiatives. Ongoing assessments enable the security team to verify that an enterprise's information security program retains its effectiveness over time, as threats, vulnerabilities and the enterprise itself evolve. The following are all part of a well-conceived assessment program to:

- Understand where sensitive information resides.
- Classify that information for future reference.
- Identify and prioritize vulnerabilities.
- Locate gaps in information security systems.
- Continually assess the threat profile.

IBM services such as IBM Information Security Assessment can play a key role in the initial assessment phase, by providing a realistic view of an enterprise's current information security setup. Invaluable for ongoing assessment are IBM Rational® quality and vulnerability software solutions such as IBM Rational AppScan, which performs scans of customized Web application environments for known vulnerabilities. It also offers strong remediation capabilities to help organizations properly protect their information resources.

Analyze and develop security processes, then create security policies

The planning phase begins by analyzing current security processes and enhancing these processes or developing new ones to improve program quality and efficiency. Following this, security policies can be developed around enterprise information and the assets that support it. A key element is developing an acceptable use policy for how and when such information may be accessed, and by whom. This planning process follows this outline:

- Define a security roadmap for the enterprise.
- Develop processes, policies and procedures.
- Create an enterprise security architecture.
- Define and maintain an acceptable use policy.

IBM can help enterprises put these policies in place through definition and architecture services, as well as process development. The IBM Security Process Development service helps enterprises define and document the processes based on an organization's predefined information security standards or a standards-based code of practice. The IBM service creates a custom security policy that helps organizations implement controls and measure their effectiveness.

Implement proper information security controls

During the implementation phase, information security controls are designed and deployed that preemptively help protect against internal and external

Highlights

The IBM approach to information security management helps organizations maintain a view of the entire security landscape, identify potential capability gaps and prioritize initiatives for improvement

threats, while simultaneously ensuring that critical information is accessible to those who need it. The key goals for the implementation phase are to:

- Implement security architecture and encryption to protect critical data.
- Determine access rights around sensitive information.
- Deploy application-level security.
- Design a security incident management plan.
- Perform ongoing risk assessments.

Manage IT infrastructure effectively

The management phase consists primarily of monitoring an enterprise's security infrastructure over time. By addressing key security themes across the enterprise, the IBM approach to information security management helps organizations maintain a view of the entire security landscape, identify potential capability gaps as they occur and prioritize initiatives for improvement. The primary goals of the management process are to:

- Perform 24x7 security infrastructure and user activity monitoring.
- Maintain an audit-ready posture.
- Preemptively detect, analyze and react to threats.
- Monitor trends for emerging threats.

Address security considerations while creating a collaborative environment

A fundamental concern in creating a collaborative environment is determining who has access to information. Organizations must provision access rights to employees and then continuously monitor and enforce those rights.

IBM Tivoli® Identity Manager and IBM Tivoli Access Manager software serve as critical solutions that enable automation of these time-consuming and complex tasks. These products also help reduce human errors in the identity and access management processes that often lead to vulnerability and exposure.

Once an organization puts an identity and access management solution in place, it can address other information security challenges, such as:

- Secure collaboration across the supply chain.
- Mitigation of insider risk.
- Threat and vulnerability management.

Secure collaboration across the supply chain

While partnerships are often critical to efforts to innovate, the potential benefits of any new product or service that an organization develops could be overshadowed if the security of its intellectual property were compromised. In addition to properly administering access, an organization must be able to rapidly close down access rights as quickly as the business changes. The partner that needs access to a particular piece of information one day may change its relationship with the organization – or cease to be a partner entirely – the next.

In short, an organization's ability to engage and disengage with partners must be as fluid as the market within which it operates. Integration with partners must be inexpensive and efficient. Federation allows an organization and its partners to freely share data and applications as needed, while restricting

Highlights

access to things they don't want to share. When done properly, federation can be an economic and highly efficient method of integrating businesses.

IBM Tivoli Federated Identity Manager enables an organization and its partners to manage user identities and handle access rights consistently – across the various information stores and applications they rely on.

Mitigation of insider risk

Privileged users within an enterprise – whether employees or business partners – routinely use the enterprise's IT systems, applications and data to perform their jobs. Whether they perform actions maliciously or simply by accident, privileged users are the biggest threat to that organization's information integrity and data privacy. In fact, studies suggest that about 80 percent of security breaches originate from internal sources.[2]

Privileged users are the biggest threat to an organization's information integrity and data privacy

With IBM Tivoli Compliance Insight Manager, enterprises can create policies to automatically monitor user behavior and shed insight into potential problems. As user behavior is monitored, reported on and investigated, the enterprise can address accidental and malicious actions that violate policies or regulations – without putting unnecessary restraints on users.

IBM Optim data privacy solutions enable an organization to mask sensitive information – such as U.S. Social Security numbers and credit card numbers – from employees who do not need to access them, including application developers and testers.

For customers who choose IBM managed security services to address concerns around insider risk, IBM offers a suite of service solutions to help identify vulnerabilities within an organization and mitigate risks associated with potential insider threats.

Threat and vulnerability management

An organization's desire to allow access to information to allow for collaboration intensifies its need for a robust threat and vulnerability management solution set. Because the universe of threats to the IT and physical infrastructure is vast, an organization must pursue a model characterized as "defense in depth." This model emphasizes the need for preemptive, real-time and reactive tools to mitigate threats at all levels of the IT stack.

To help organizations stay ahead of potential threats, IBM offers application security solutions that include advanced encryption and protection against sophisticated attacks. IBM threat and vulnerability management products such as IBM Proventia® Network Enterprise Scanner and IBM Proventia Network Anomaly Detection System help protect against external attacks and malware. And IBM services help eliminate end-point data leakage.

Additionally, IBM Tivoli Security Operations Manager automates the collection and analysis of security event data across the heterogeneous environment. As a result, it helps streamline the incident management process.

Highlights

IBM encryption solutions help enterprises protect sensitive data stored on end points and removable media, and transmitted with e-mail communication channels

Rational AppScan is an automated Web application security testing solution that finds both known and unknown security vulnerabilities that hackers could exploit. It also provides advanced remediation and recommends fixes to development teams.

IBM encryption solutions help enterprises protect sensitive data stored on end points and removable media, and transmitted with e-mail communication channels. Encryption solutions can also protect the complete contents of a lost or stolen laptop or PC. Increasingly, companies are choosing to encrypt tape data and are turning to systems such as IBM System Storage™ TS1120 Tape Drive technology and IBM Linear Tape-Open (LTO) Ultrium 4 Tape Drives. Tape encryption is done with very little performance impact on the tape drive itself. Organizations can exchange encrypted tapes with business partners or data centers that have the encryption keys to unlock the tape drives on their end.

Conclusion

In today's extended enterprise, collaboration is crucial but can create complexity. Information in motion and at rest must be protected across its entire life cycle.

Using a four-phase process that encompasses assessment, planning, implementation and management, IBM helps forward-looking enterprises prove that "secure collaboration" is not an oxymoron. IBM information security solutions help enterprises successfully link their extended business partner and customer ecosystems, keeping information secure while at the same time making it available to the people who can use it to enhance that enterprise.

For more information

To learn more about how IBM solutions for information security can help your organization create a secure collaborative environment – or to find the IBM security solutions entry point that is right for your organization – contact your IBM representative or IBM Business Partner, or visit **ibm.com**/itsolutions/security

About IBM solutions for enabling IT governance and risk management

IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations, and draw on extensive customer experience, best practices and open standards–based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit **ibm.com**/itsolutions/governance

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

Produced in the United States of America
December 2007

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

[1]IBM CFO study, 2006

[2]*CIO* magazine survey, 2007

GMW14004-USEN-00