Data Loss Prevention Implementation Initiatives|

THE HITACHI WAY

White Paper

By HitachiSoft America Security Solutions Group

September, 2009

HITACHI SOFTWARE ENGINEERING AMERICA, LTD.

Executive Summary

When implementing data loss prevention (DLP) solutions for your organization, you must address three key drivers regarding information security: compliance, risk management, and governance (control). Organizations cannot conduct business in their respective industries or countries without complying with laws, regulations, and standards. Organizations must protect their intellectual properties from being lost and/or leaked as organizations become more mobile. Organizations can approach DLP implementation as a part of an IT governance initiative which creates value to stakeholders. However, effective DLP implementation is not an easy task.

Following a Plan-Do-Check-Act cycle helps information security officers navigate through a maze of complex data security initiatives. Once security management policy is established, you will need solution to execute your plan. HitachiSoft's award-wining DLP solution provides a complete data protection, data control, and data management capabilities to support such initiatives.

In this white paper, we will discuss the three key information security requirements, recommend an approach that can guide you to a successful DLP implementation, and illustrate how HitachiSoft's DLP solution can support your initiative.

Three Key Drivers

Driver 1: Compliance

Organizations cannot conduct business in their respective industries or countries without complying with laws, regulations, and standards. The following are examples of key regulations and standards relating to information security.

The Sarbanes-Oxley Act (SOX) is the major compliance regulation with which all publicly traded companies must comply. Although the main purpose of SOX is to protect financial data against fraud, information security plays a significant role in securing the underlying IT infrastructure because financial records are almost always generated, updated, and saved on computers.

Protection of privacy is another regulatory compliance. California Senator Bill 1386 is an example of law regulating the privacy of personal information. Demand and concern for privacy protection is increasing; however, we see many identity theft incidents on media. Many incidents related to divulging personal information have accelerated an establishment of regulations related to privacy protection. In 2004, the Payment Card Industry Data Security Standard (PCI-DSS) was established by a consortium of major credit card companies to protect privacy for credit card users.

Driver 2: Risk Management

Organizations must protect their intellectual properties from being lost and/or leaked. As organizations become more mobile, this becomes a challenging task. Proliferations of mobile devices expose the organizations to data breaches and regulatory violations. Failing to protect data from leaking places business sustainability at a high risk. Organizations must protect data on all devices that are dispersed globally.

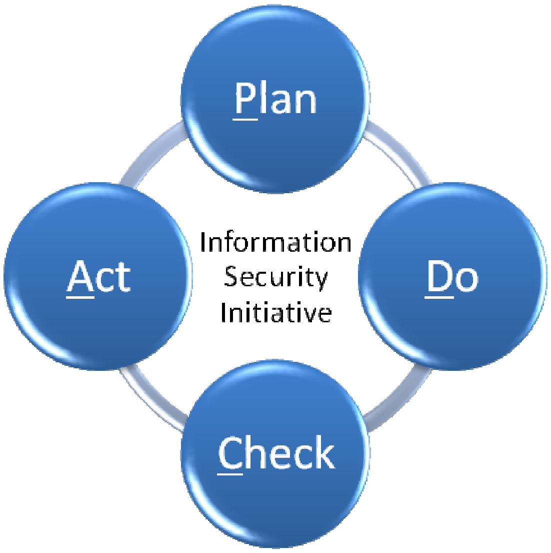
According to a CIS Computer Crime and Security Survey conducted in 2008, 50% of those surveyed had experienced theft of laptops or mobile devices. At the same time, 47% of organizations have already implemented encryption to counter this type of threat. In the meantime, 17% of organizations experienced theft of customer data, and 8% experienced theft of intellectual properties. Often, these thefts were committed by people within the organizations, including employees, contractors, and partners. As of 2008, 27% of organizations had implemented endpoint security to prevent this type of threat. Organizations have also implemented high security measures against hacking into corporate networks, as evidenced by the fact that over 94% and 97%of the organizations have implemented firewalls and antivirus software respectively. Organizations are looking for more effective way to protect data beyond firewalls and antivirus software in order to protect data against today's newer threats.

➢ Driver 3: Governance (Control)

Organizations can approach information security implementation as a part of an IT governance initiative. Often, an organization fails to create value if it looks at information security implementation as purely a cost. In such a case, the IT department is reluctant to implement an unwelcome security tool that limits users' operations. If an organization could position the information security implementation as an investment for the organization, the effort begins to make sense for all participants, including IT, business, and management. Recently, many organizations have assigned an information security officer to lead initiatives concerning information security and risk management. For instance, Hitachi has invested in a global security initiative regarding data security for 910 subsidiaries with 389,752 employees worldwide. Each subsidiary has retained an information security officer, or equivalent staff, to support the global security initiative. Planning occurs at the headquarters in Tokyo, and implementation occurs at each local subsidiary. High security computing matched with our corporate image of Hitachi adds value for our stakeholders, including customers, partners, suppliers, and stockholders.

Plan-Do-Check-Act Cycle

When organizations take on an information security implementation, we recommend a PDCA cycle for successful implementation of the initiative. A PDCA is the basis for implementing ISO27001 of the ISMS (Information Security Management System). Here are four steps in the PDCA cycle:



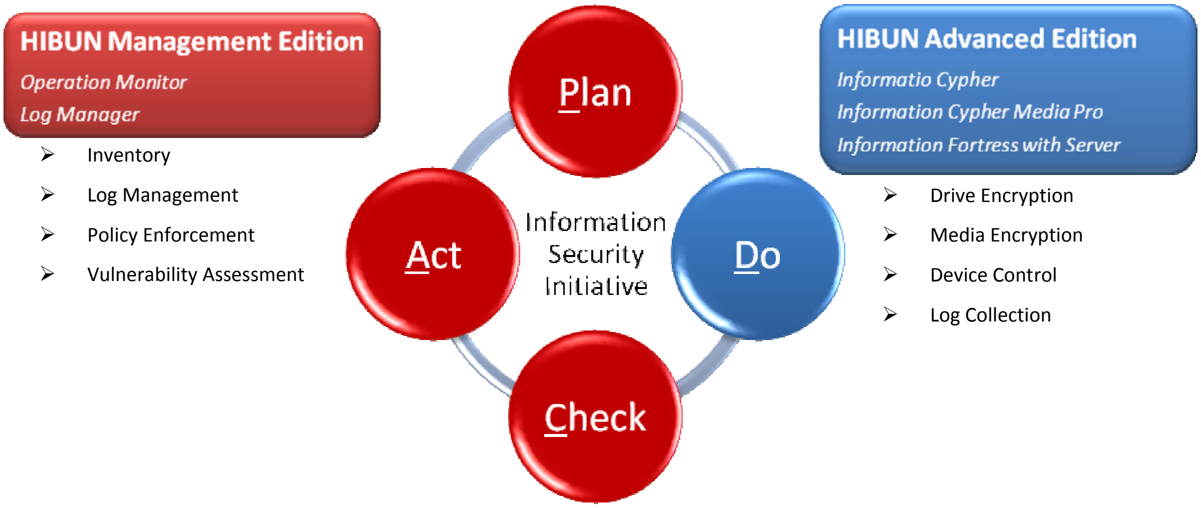
➢ Pitfalls

Many organizations put too much focus on the "DO" step when trying to mitigate data security threats. Because security threats put an organization in emergency mode, IT is pressured to find an immediate remedy to mitigate the risk. Under such pressure, IT often resorts to a first-aid approach without thorough planning. It is difficult to measure the long-term effectiveness of such a job. Moreover, when another requirement comes up later, IT often repeats the same approach. Such patched remedies often lack features for emerging requirements. If you implement the wrong tools, you end up having to replace them with new ones.

On the other hand, security-sensitive organizations often invest heavily in security initiatives and solutions with the most features, even though those features are overkill for their current requirements. It is important to implement only what is necessary and select solutions that can expand as your requirements increase. You, as an information security officer, need to know what is most relevant to protect your organization’s intellectual properties to sustain your business.

HitachiSoft's DLP Solution

HitachiSoft's DLP solution provides protection, control, and management capabilities to protect your intellectual properties. Our solution helps implement DLP by following the PDCA cycle recommended previously.



HIBUN Management Edition

Operation Monitor
Log Manager

- Inventory
- Log Management
- Policy Enforcement
- Vulnerability Assessment

HIBUN Advanced Edition

Informatio Cypher
Information Cypher Media Pro
Information Fortress with Server

- Drive Encryption
- Media Encryption
- Device Control
- Log Collection

PLAN

- HitachiSoft's DLP solution helps identify current security vulnerabilities related to endpoints. Based on collected information, you can establish objectives to mitigate current and future security threats.

DO

- HitachiSoft's DLP solution protects data by strong encryption algorithms. The solution flexibly supports all types of hard drives and removable media that are commercially available. Once implemented, users can exchange data freely via encrypted removable media or share data securely via encrypted files and/or folders.
- HitachiSoft's DLP solution also controls data outflows from endpoints. For instance, you can prohibit users from copying data onto USB memories. Users are allowed to

copy data onto approved devices only if the policy admits them access to such devices.

CHECK

- HitachiSoft's DLP solution collects users' operation logs from endpoints and stores them centrally. Collected logs are encrypted so that they cannot be manipulated. This increases the reliability of logs during audit tracking.
- Additionally, HitachiSoft's DLP solution proactively monitors security vulnerabilities of endpoints. The solution alerts users about improper data usage and allows security administrators the ability to trace improper data usage as needed.

ACT

- Finally, HitachiSoft's DLP solution helps security administrators summarize collected logs for trend analyses to enhance the security level for their organization.

For more information about our solutions and products, please visit us at:

http://www.hitachi-soft.com/security/products/

Conclusion

With a correct implementation approach, you can establish robust security measures against endpoint security threats without overinvesting in IT assets. The PDCA cycle helps organizations implement information security measures effectively. HitachiSoft's solution helps implement DLP to support the initiative and is easy to deploy and manage for the security administrator, with minimum user impact. With a flexible choice of settings, users can exchange data freely and securely. HitachiSoft's DLP solution also assists the security administrator in identifying the gap between ideal corporate security and automotive reporting processes and provides hints for improving organizational security for better compliance and governance.

HITACHI
Inspire the Next

About HitachiSoft America Security Solutions Group

Security Solutions Group is dedicated to providing reliable data loss prevention solutions to help today's organizations address challenges regarding information losses and thefts. Data loss incidents are rising, and a majority of these incidents are caused by insiders who have legitimate access to sensitive data on their personal computers. Anti-malware and network-based anti-theft solutions cannot prevent the loss of data in an organization when employees transfer data using removable media or accidentally lose their personal computers.

For twenty years, Security Solutions Group has implemented a variety of technologies to improve information security for many organizations. We understand the challenging tug-of-war between security and convenience. Our goal is to increase your organization's security without compromising the efficiency of your existing technologies. By leveraging our world-class endpoint data loss prevention solutions, we minimize the risk of information loss and theft for your organization. Currently, we have more than five million worldwide install-bases of HitachiSoft's DLP solutions, providing more than 5,300 satisfied customers with advanced information security technology.

Hitachi Software Engineering America, Ltd.
Corporate Headquarters
601 Gateway Blvd. Suite 100, South San Francisco, CA 94080 |650.615.7600
New York Office
90 Park Avenue, Suite 200, New York, NY 10016 | 212.827.1771

For Product Information: www.hitachi-soft.com | 866.554.4286 | info@hitachi-soft.com