

The SAVVIS Approach to Security Risk Management

This document reviews the emerging changes in the IT risk landscape, the increasingly important role IT plays in enterprise risk management, and how SAVVIS' infrastructure and security services can help address those risks cost effectively.

By: Chris Richter
Vice President, SAVVIS Security Products and Services



Table of Contents

- 3 What is at risk for enterprises?
- 4 What choices do companies have in addressing risks?
- 4 Costs Associated With Implementing Risk Management Controls

What is at risk for enterprises?

Much of what is driving enterprise risk is the increasing value of information, and the increasing number of methods available to access it. The internet, VPNs, mobile & home-based work forces and extranets have all contributed to the ever-growing number of access vectors to enterprises' data. Malicious access may be for the purpose of using the data illegally, destroying it, altering it and thus compromising its integrity, and denying its availability to legitimate users.

Many senior IT executives struggle with managing a multitude of risks.

The value of data, as a share of a typical enterprise's overall asset portfolio, has grown exponentially in just the last ten years. The risks related to data compromise are significant. Examples of risk to a company include:

- Income and revenue loss
- Lost reputation, brand damage
- Legal (compliance, contractual)
- Loss of assets (customer data, intellectual property)
- Liability of the Board of Directors and senior management
- Random expenses associated with risk

Publicly-held companies and board members are especially under pressure to establish best practices to protect data, and can be held liable for failing to establish guidelines for adhering to regulatory requirements.

What are the components of risk?

The generally accepted theoretical formula used by risk managers is: Risk = Threat x Vulnerability x Asset Value (or $R=T \times V \times AV$).

Typical examples of threats include:

- Accidents
- Malicious attacks
- Theft and fraud
- System failure
- Network and power outages
- Employee or service provider errors
- Force majeure

Examples of vulnerabilities to a company include:

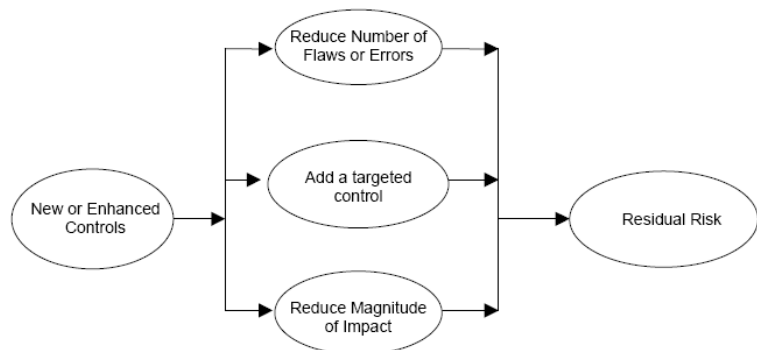
- Lack of compliance enforcement
- Lack of security policies and procedures
- Insufficient security controls
- Lack of a business continuity program
- Lack of redundancy
- Lack of maintenance and patch management process
- Poorly trained or inadequate staff
- Poorly-written software
- Configuration mistakes
- Poorly-designed architecture
- Poor password control

What choices do companies have in addressing risks?

Companies can never completely eliminate risk and still remain in business. The objective is to reduce risk to an acceptable level at an acceptable cost, through the application of a risk mitigation process. There are four primary methods for mitigating risk:

- Organizations can transfer the risk, such as financial risk, to a third-party – an insurance company, for example.
- They can cease the activity that causes the risk.
- They can accept the risk.
- Or, they can treat the risk with controls. A cost-effective way of doing that is by using a third-party to manage those controls. For example, an infrastructure services company like SAVVIS can manage the security and operational controls of an IT infrastructure.

The relationship between control implementation and residual risk is graphically represented as follows:



Companies must understand that there will always be residual risk, and that they cannot transfer all risk to a third-party. Managing risk can be a cooperative process even though businesses remain accountable for the security of their infrastructures and data, regardless of how much is outsourced.

Enterprises that use a risk management approach know how much of their infrastructure and controls they want managed by a third-party infrastructure services provider, such as SAVVIS, and how much they need to manage themselves.

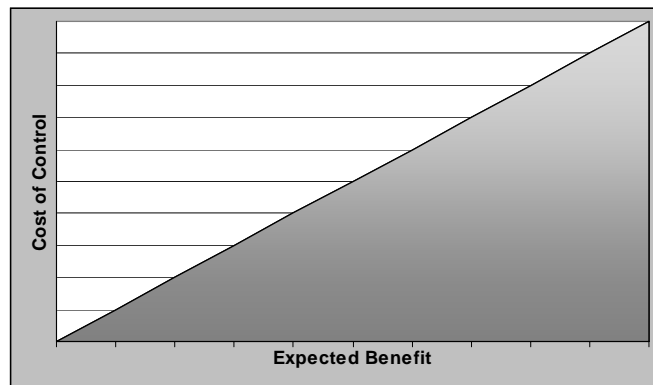
Costs Associated With Implementing Risk Management Controls

The changing value of information and the resulting demand for controls designed to protect that information has dramatically increased the importance of the IT function within the enterprise. And this influence is not just security-related, but also cost-related.

Controls, which include policies, procedures, and technologies, along with the individuals who are trained to implement these controls, can be extremely expensive to implement.

SAVVIS commonly encounters companies that have to trim back on IT expenditures due to the costs of implementing these controls. That's unfortunate,

because controls should never negatively impact the bottom line. If implemented properly, security controls should improve the bottom line by making companies more secure, more efficient, and less likely to incur a loss of high-value data assets.



But some controls can still be very capital-intensive. Creating extensive sub-nets to isolate sensitive information assets from lower-value assets, or elaborate data encryption, archiving and key management infrastructure, can involve a great deal of capital and management resources, especially if architected poorly. Companies too often resort to throwing money at the problems they face.

It's well documented that implementing too many controls will actually make a company less secure, less efficient, and ultimately more prone to a data breach.

Gartner recently published a study indicating that companies who have a formal risk management program in place were able to reduce the number of regulatory-compliance related controls they had to implement by up to 70%. And again, reducing the number of controls reduces cost.

The Right Approach

The first step is to develop a formal risk-management program that begins with a comprehensive risk assessment. It is believed that a solid risk-management program can improve a company's business efficiency, reduce its risk exposure, and thus improve its performance and bottom line. The key benefit of a risk assessment is that it can actually help enterprises *reduce* the number of controls they are required to implement. It does this by identifying those IT assets that need to have strong controls (which are often very expensive), and those assets which, based on their risk ratings, require less stringent controls.

Since controls are required by several government, trade, and industry compliance regulations, they are a fact of life. Furthermore, these controls must often be audited by third-parties for the purpose of validating their existence and effectiveness. Again, the key is to reduce the cost of these controls.

SAVVIS can reduce the cost of implementing and maintaining controls:

- We've built an efficient Infrastructure-as-a-Service portfolio that consists of data centers, managed systems, network, storage, backup and security services.
- Our professional services team's risk-management practice can assess risks, and work with clients to develop a formal risk management program.
- SAVVIS can help customers tailor a security management plan that balances the necessary expenditure with the value of the information to be protected.
- We use best-in-class technology as the basis of our cloud-based, and premise-based, security, network, and infrastructure services.

Note regarding PCI compliance:
Not all companies have performed a risk assessment (PCI/DSS now requires that all companies that handle card-holder data must have a security policy established and conduct annual risk assessments). More companies are expected to implement risk management as ISO 17799 becomes more widely adopted.

- To support these services, SAVVIS provides full, 24x7 management, which can free-up our customers' internal resources to devote more time to other activities.
- SAVVIS has audited its services against a framework of industry-standard controls to make it easier for our customers to work with third-party audits of the infrastructure that we host and manage.
- Building controls that are documented, and ready for an auditor's scrutiny, can be a grueling task. SAVVIS can greatly assist this process through the design of our controls-oriented managed services.

SAVVIS' services provide solid solutions for customers seeking to manage risks to an acceptable level at an acceptable cost. It's very important to choose a service provider that understands the language of risk management and IT audit controls. SAVVIS understands these requirements and designs its services with the requirements in mind.

Corporate Headquarters

SAVVIS Inc.
1 SAVVIS Parkway
St. Louis, MO 63017
1-800-SAVVIS-1
www.savvis.net

ASIA

SAVVIS
50 Raffles Place
Singapore Land Tower
#13-01/04 Singapore,
Singapore 048623
65 6768 8000
www.savvis.jp

EMEA

SAVVIS UK Limited
Eskdale Road
Winnersh Triangle
Workingham
Berkshire RG41 5TS
United Kingdom
+44 (0)118 322 6000
www.savvis.co.uk