

Effective information security management

by: sbi-secureit.com

One of today's main concerns in the Information Technology field is the risk of losing confidential business data, a serious issue that might put business integrity, privacy and confidentiality at risk. If you are a business owner who is facing such a problem of losing confidential company data, or that clients' privacy would be at a risk of malicious actions by hackers and crackers. Also if you aren't sure of what information security system to use that would



best fit your company needs, or need a clear scope to calculate your needs and give the best information security solution that would work perfect according to your budget and business needs, then continue reading this article hoping it would be of a good help to future business plans.

It is indeed a very stressful job to manage Information Security in any organization. Even with huge budget it is very hard to know if the budget money is spent on the right technologies. Information Security Managers face many problems trying to maintain the **Confidentiality, Integrity and Availability** of the Information Systems. Budget justification, understanding the threats to the business, selecting the proper countermeasures, and managing the operations once the solution is implemented are some of these problems.

How to choose the best Information Security System for your business

Information security market has numerous technologies each solving some of the security problems with different degrees of efficiency. Choosing the most suitable set of technologies that best satisfy the business needs is a very confusing task and should always be referred to an information security expert. However, consulting and/or employing an expert is not enough anymore as the need to rely on up-to-date integrated information system to manage corporate information security is being realized as the next paradigm in security.

What is PheonixWall Information Security Manager - PISM

The need to effectively manage all information security aspects via a central system that is granular enough to calculate information risk, define countermeasures, implement and manage solutions lead to the development of *PheonixWall Information Security Manager* (PISM). PISM is a system specialized in Information Security Risk Management which can be used to provide Information Security consulting service or manage information security internally by an employee of the organization. PISM simply works by being a permanent part of the organization infrastructure. First it integrates with

The objectives of the PISM -in brief- are as follows:

- Identify how business works and what are the threats compromising the business.
- Help management develop information security policies and choose the solution that best fits the policy based on cost benefit analysis that takes business as well as technical factors into consideration.
- Make sure security budget is spent right where should be by tightly linking the Information security policy with the technical and administrative controls.
- Manage Service delivery and Service support of the solution.

The problem with information security is that new vulnerabilities are introduced everyday

and attack vary in forms and agents. It is a must to have a system capable of adapting with the changes, Integrating all security controls and facilitates intelligent decisions to be taken. This unfortunately is unachievable by merely installing a hardware or software systems. An integrated management system must be in place to manage any organization's information security.

The components of the PISM:

- A Bastion Host.**
- Multiple Security Softwares.**
- A Management System that hosts Configuration, Change, Incident and Problem Management operations as well as the Information Security Policy.**

How does PISM work

PISM works in a simple straight forward methodology.

Phase I: Gathering information and understanding business track:

Starting with the organization's information security managers – *internal resources or out sourced* – interview the business management to understand the business and collect data about the business services that bring money into the company, the value of trade secrets, and value organization's reputation to the business, etc.

The objective of this phase : is to have a very good understanding of what is important and what is not from the business point of view.

PISM role: This is very important as asset values in the PISM model depends on how much it provides to the business model and not just on its acquiring or development cost. A good example for this is a server that currently provides no significant value to the business but it is still operational, vulnerable to attack and has a significant recovery cost. In this case the existence of this server will increase the risk value and consequently the security solution budget. PISM avoids this situation by developing the risk assessment based on the business view rather than existing assets and technical view.

Phase II: Technical information analysis:

Secondly, the organization's information security manager interviews the technical *staff – information custodians and sometimes owners* - as they are aware of all the assets – including security assets - and have relatively clear view on how the business services depend on these assets.

The results of this interview are:

a- an assets registry where all the assets are collected, classified, and their recovery cost identified

b- a dependency web that connects assets and services they provide and with the services they need to operate.

Phase III: Defining dependency & risk calculation:

Defining the dependency web is a key to the third step which is risk calculation. The assets are compared against existing and estimated threats – sometimes with the help of an external penetration test tool to double check the integrity of results – and a risk value is calculated. The risk value is calculated based on how much vulnerabilities in the system (assets) can lead to business services disturbance and loss of money.

The previous Analysis phases are responsible for managing the following:

- Business Objective Analysis Management.
- Risk Analysis Management.
- Configuration Management.

Phase IV: Develop security policies:

The fourth step is to develop the security policies. The security policies should be developed to prevent system vulnerabilities to be exploited. References are available for information security standards to make it much easier and efficient to develop the policies. In one structure, all policies and procedures are maintained to make it easier to verify consistency and check for backdoors. The Policy structure is granular enough to maintain most information security policies. Each policy record demands the existence of specific security technology requirements (functional or assurance). Based on the relation between the policy and the security requirements a list of alternative solution is proposed by the system. Each can maintain the security policy with different degree of efficiency. The organization's information security manager must now choose the best fit alternative.

This Design phase is responsible for managing the following:

- Capacity Management.
- Financial Management
- Information Security Policy Management.

Phase VI & VII: System delivery & maintenance via ITIL guidelines:

The sixth and seventh steps are helping the organization's information security manager manage and follow up information security management activities according to ITIL guidelines, respectively service delivery and service support. Service delivery is maintained by an action plan, Analysis & Design reports, and Implementation Scripts. Service support is maintained by a logbook and Incident, Change, Problem, and Release Management reports, as well as security equipment control capabilities via the PISM interface.

This operations phase is responsible for managing the following:

- Change Management.
- Release Management.
- Security Incident Management.
- System Incident Management.
- Security Problem Management.
- System Problem Management.
- Firewall Management.
- VPN Management.
- NAT Management.
- Antivirus Management.
- Remote Access Management.
- Intrusion Detection System Management.
- Security Auditing Management.
- Security Forensic Investigation Management.
- Security Penetration Testing Management.
- Log Management.

PISM could be deployed in different ways:

- Standard deployment: as a stand alone box that maintains the security system and does most of the security requirements by itself.
- Control node deployment: as a stand alone security server that maintains the security system and controls other boxes provided by other vendors. The other boxes or solutions provide the security requirements.

- Scalable deployment: A cluster of PISM boxes is used to manage the security system and provide the security requirements.
- Infrastructure deployment: PISM becomes the network infrastructure. The bastion host acts as a layer 7 security switch. This solution availability depends on the available hardware.
- Hybrid deployment: A combination of the above solutions.

Conclusion:

PISM is the first information security management system with this scale of granularity, integration and flexibility to be introduced to the market. The aim of which is to help decision makers take faster, more accurate and lucrative decisions and be able to manage the solution they have chosen for their information security.

References:

imagery: <http://forum.crystalxp.net/index.php?showtopic=22291>

white paper URL: <http://www.sbi-secureit.com/whitepapers>