Global Information Assurance Certification Paper

Secure Data
Is there such a thing?

GSEC Practical Assignment
Version 1.4b

Sheetal Sood
August 5, 2004

Table of Contents

Abstract:

Information security is the buzzword today in the IT field. Everyone is talking about it, many are implementing it and few are implementing it correctly in a planned fashion.

When you talk of securing a company's network today, we talk of firewalls, network perimeter security, and anti-virus procedures.
We talk about securing servers by keeping up to speed with the numerous operating system patches, up-to-date anti-virus signatures and making sure that no malicious code exists on the servers.
When it comes to database security, we talk about preventing SQL injection, database worms etc.

And of course we talk about physical security of the company premises and social engineering issues.

The one thing that gets neglected in the whole process of implementing security is the security of the actual data on the network.

This paper investigates the growing problem of organizations securing their networks in the tightest possible fashion but leaving their data wide open and available on a platter.
Despite the growing debate and increased legislation, it will be highlighted as to why companies are failing to recognize that this risk is big and very real and is prevalent in every aspect of their business processes.

Introduction:

Most companies have done a reasonable job implementing DMZ environments and other protected perimeters to secure their networks using firewalls, intrusion detection systems, VPNs, and significant personnel resources.

Sadly, intellectual property continues to leak outside.

Why? Data has no easily defined frontiers. Despite all these security measures, data will continue to leak outside traditional company boundaries-requiring enterprises to do something different to protect vital information throughout its entire lifecycle, no matter where it resides, the applications it touches, or where it travels to.

Companies need to start assuming that confidential data will find its way out-and they need a new way to easily enforce security at the data level, no matter where data resides or travels.

The famous Robert Hanssen case is a prefect example:

Hanssen spent much of his 25-year career with the FBI in counterintelligence, giving him access to highly sensitive cases and documents. In 1995, he began working as the bureau's liaison to the State Department Office of Foreign Missions and the State's Bureau of Intelligence and Research.

Since 1985, FBI agent Robert Philip Hanssen was a mole inside the FBI, accused of spying for the former Soviet Union and then for Russia in exchange for cash and diamonds. Hanssen pled guilty on July 6, 2001, to 15 counts of espionage and conspiracy charges

(http://www.cicentre.com/Documents/DOC_Hanssen_1.htm
http://www.cnn.com/SPECIALS/2001/hanssen/)

To summarize, the power that Robert Hanssen possessed was just having plain old ‘access’ to his company data.

According to a recent PWC/ASIS study, in 2001 most companies experienced two major IP losses that together totaled nearly a million dollars in damage. Intellectual property losses to US companies totaled $53 billion to $59 billion, with the greatest loss areas being strategic plans, R & D, customer lists and financial data.

http://www.asisonline.org/newsroom/surveys/spi2.pdf

Recent findings that insiders constitute the primary threat to enterprise security are being challenged by experts who insist the greater threat to security remains external.

Only 38% of respondents to the latest computer crime survey sponsored by the FBI and the San Francisco-based Computer Security Institute said they detected insider attacks during the preceding 12 months. That's down from 49% reported a year ago, and 71% reported in 2000.

http://www.computerworld.com/securitytopics/security/story/0,10801,70112,00.html

The Real Problem:

1. Is your company doing anything to protect confidential information from deliberate or inadvertent electronic dissemination?
2. What happens to confidential documents once they are no longer necessary? Is there an appropriate destruction of documents procedure in place?
3. Are there any policies that employees know regarding data security?

These questions make perfect sense but are often not asked.

Let us take a moment to think about the various possible sources of data leaks.

The information leaks within an organization can happen with unsophisticated external attacks like amateur hackers snooping around for security holes.

They could happen with extremely sophisticated external attacks like a hacker doing it for his reasons or being hired to target the specific organization.

And then there are the internal attacks more popularly called the ‘insider threats’ that are employees – trusted employees, within a company indulging in industrial espionage.

And this is where the real problem lies.

Who are the insider threats?

According to the recent PWC/ASIS study, former employees, foreign competitors, on-site contractors, and domestic competitors form the most common insider threats.

But finally, we must not forget the most dangerous insider threat of all – the blissfully ignorant employee that has the power of access to data.

The reason why I call them the most dangerous is because data loss caused by this insider threat is not even recognized as data loss.
To better explain, let me cite an example:

A system administrator who has a fancy USB drive on his key-chain, and at the same time has all access to all company systems.
He loses the USB drive, no big deal, he buys another one.
Normally this incident is in fact no big deal except for the fact that the USM drive had 2 documents – one listing the IP addresses of all servers in the organization and the other listing all the server administration passwords.

Will this loss be reported to the management?
Probably not, maybe because the system administrator is indeed blissfully ignorant and thinks noone can really use those passwords and IP addresses unless they are within the organization.
Or he is afraid if he reports this, he will somehow be blamed if any incident occurs.

The second classic example is that of a high ranking officer within a company trying to get the company's quarterly financial report together. The report has seriously confidential data.
It's late and he decides to complete it on his way home in the train.
His laptop gets stolen and needless the say, the seriously confidential data with it.

My best example is of the CEO who needs two huge documents both containing classified information for the big company stake-holders' meeting tomorrow.
She is reading them on her computer and she decides to print them.
She accidentally prints to the network printer that she has access to, instead of her local printer. What she did was just release perhaps the most classified information in the company for the world to see and, in print form!

Regardless of how it happens, loss of intellectual property (IP) costs companies billions of dollars.

The most common data that is at risk is the organization's proprietary data which includes research and development data, customer and sales data and finally financial data.

Clearly, organizations have to realize that secure perimeters and secure networks are no longer sufficient to ward of the risk of information and intellectual property loss.
As technology gets better and we become more and more efficient by using snazzy devices, we need to keep in mind that the risk may have just gotten bigger!

With email, wireless devices and cellular phones, the company data can be anywhere you want in a flash.

While that is great, what's happening at the same time? The same data that you are securing with millions of dollars investment is outside your network and not protected anymore.

Most organizations have security policies, procedures and practices these days. These documents although comprehensive most often do not talk about specific data security.

In the PWC-ASIS survey, although most respondents (about three-fourths) indicated that information associated with new products and services was vital to the company's success, only 55% said that management was concerned about information loss and was taking necessary precautions.

• Based on a ranking of best practices by respondents, it appears that proper labeling and handling of classified information is not the norm among companies, although high-tech companies are more likely to correctly mark intellectual property to protect it and large companies (over $15 billion) are most likely to correctly destroy sensitive information when it is no longer needed.

• The ranking of best practices also suggests that employees are not typically trained to safeguard proprietary information in the office or when on travel.

• Although most companies indicated that the Internet represents a new threat, most do not require that information sent over the Internet be encrypted.

• Many responding companies do attempt to reduce the risk of proprietary information and intellectual property loss by employing 'need to know' policies; using screen savers and/or server passwords; and maintaining nondisclosure agreements.

• Attitudes about intellectual property loss and "best practice" strategies varied among companies that had and had not experienced incidents of loss. Information security was given a lower priority at companies where loss incidents occurred. Companies that made IP protection a higher priority were also those that indicated no loss incidents.

• Many companies, especially in the service sector, do not assign a value to their intellectual property until they are in litigation.

In addition to steep financial damage, companies also face the pressure of compliance with new federal regulations requiring new levels of data protection, including Sarbanes-Oxley, California SB 1386 and NASD 2711.

What is the Solution? Is there one?

The foremost thing that companies have to do is to recognize that their data is not secure just because they have all the firewalls and intrusion detection systems in place.

Instead of building more layers of perimeter security around data, organizations need to turn security "inside out"- enforcing security right down to the data level and transparently incorporating that security into existing business processes.

And they must do so in a way that is simple to administer and makes it easy for users to continue to use familiar applications and businesses processes- otherwise enterprises and their users will simply reject it.

The second most important thing that companies have to do is identify what needs to be protected.

Today, in the cutthroat competitive market, the only niche that a company has over the other is its intellectual property.

The company's data is the lifeline of the company.

Companies can start by assigning an independent task force dedicated to the task of identifying information and intellectual property within the company and then classifying it with different security levels.
The security practices required in each situation are dictated in part by the business you are in and the risks you face.
And it requires education, right from the top management to the lowest employee in the organization. Once employees understand the organization's products, research and intellectual knowledge base, and a pattern of communication is established with other departments, then you've formed the base on which to begin to build an IP protection plan.

Education of the employees must include awareness of the access they possess over company resources and how it can be harmful if care is not taken.
It can also include training them on what to say and what not to say for outsiders looking for company information.

The task force must do a risk and cost-benefit analysis, logging which digital assets are considered the most precious and also determine what information, if lost, would hurt the company the most.
Once this is done, the next thing to do is to identify the data that is the most vulnerable.

Non-disclosure agreements should be made mandatory for employees especially for contract and part-time labor.

Policies and procedures should be rewritten highlighting how security on each type of data category is to be maintained.
Once the policies go into effect, the security on the organization data may have to be redone so that employees see only what they 'need to see'.

Vendors like Microsoft have introduced rights management in their new operating system Windows server 2003.
Microsoft Windows Rights Management Services (RMS) for Windows Server 2003 is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use. Windows RMS enables protection of sensitive information, such as Web content, documents, and e-mail, through the creation and enforcement of persistent policies that live with the information—no matter where it goes
Information workers can choose from a variety of usage rights to define exactly how the recipient can use the information and for how long. They can define who can open, modify, print, forward and/or take other actions with the information. Organizations can create custom usage policy templates such as "Confidential - Read Only" that can be applied directly to the information. (http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx)

Other Vendors like Authentica and Liquid Machines have really innovative products that organizations can consider embracing.

For example,
Liquid Machines transforms any application into a secure application. It prevents data leakage, and protects and tracks intellectual property regardless of where or to whom it might circulate. Authorized users work collaboratively with protected data the same way they do today. Access rights are dynamically applied and enforced in a way that is completely unobtrusive to these users. With the Liquid Machines solution, businesses can extend protection for remote and custom users with the ability to change or revoke rights even after broad distribution. With the click of a button, the business can revoke data access to reassigned or terminated employees, external consultants, contractors, business partners, lawyers, accountants and bankers regardless of where the data resides. (www.liquidmachines.com)

Authentica's document security solutions leverage our unique Active Rights Management technology to provide dynamic control over documents even after they're in recipients' hands. For example, you can change a recipient's document permissions in real time and automatically expire a document. All copies are deleted, wherever they're located (user desktops, servers, or back-up media). A continuous audit trail lets you monitor the activity on each document so you know when someone reads, edits, or prints it, and you have proof as to when and where the activity occurred.

Authentica also has a similar product for email that you can specify security on, and delete all copies at once.
An audit trail is maintained for the entire lifecycle of the email.
(http://www.authentica.com)

The beauty of these new products is that is becoming easier to enforce the kind of security that you would like to see on your data which was not available some years back.
Example, disabling printing of confidential documents etc.

Companies should also understand the need to protect mobile devices like laptops. There are numerous technologies available today to protect them from theft or to protect the data on them if they get stolen.

Security cables, laptop safe, laptop theft alarms are all ways to protect laptops from being stolen.

In case, a laptop does get stolen, there are many technologies like hardware or software passwords, file system encryption and even biometrics that can prevent the thief from actually accessing the data even if he has the laptop.

Some of the other steps that companies should take are:

- Organize a compliance committee to ensure adherence to new levels of data protection, including Sarbanes-Oxley, California SB 1386 and NASD 2711.
- Removing removable media drives or restricting them to absolute necessity
- Controlling modem usage
- Scanning for malicious data activity on the network
- Audit, audit and then audit some more!

Conclusion

Today, chief security officers know what to do when it comes to network security.

They know how to handle intrusion detection and external penetration attacks.

What is a big challenge is protecting what you don't know.

Most security officers today are still struggling with implementing end-to-end data security only because what needs to be protected and how, is not easily defined.

Expensive methods have to be adopted to purchase new technology, implement awareness courses, external audit processes and basically stay on top of the game.

But when your company's life and future depend on it, it is worth every bit of the struggle and every cent well-spent.

References:

Robert Hansen case: CNN coverage

http://www.cnn.com/SPECIALS/2001/hanssen

Robert Hanssen Espionage Case

http://www.cicentre.com/Documents/DOC_Hanssen_1.htm

Microsoft Windows Rights Management Services

http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx

PWC/ASIS study: Trends in Proprietary Information Loss

http://www.asisonline.org/newsroom/surveys/spi2.pdf

Insider threat to security may be harder to detect, experts say

http://www.computerworld.com/securitytopics/security/story/0,10801,70112,00.html

Authentica

(http://www.authentica.com)

Liquid Machines

www.liquidmachines.com

CSO: The Resource for Security Executives

www.csoonline.com