Global Information Assurance Certification Paper

Electronic Data Security Awareness

By Phillip A. Grove

Introduction

The primary asset of many companies is data. In a growing number of companies this can be its only asset. These companies process, use, and sell this data as a primary income source. This is why data security is so important, and so often overlooked. This can also be something very tricky. You aren't just securing your network from hackers, internal or external. You are securing your data from thieves, internal and external.

There are many potential security holes, and many people who will work against you for convenience sake.

The primary purpose of this paper is to make you aware of some of the many different issues with the data security. The secondary purpose is to enlighten people to the fact that it isn't merely the systems that need to be secured. This seems to be a flawed approach to security that all too many people fall into. The systems security, while important to maintaining the integrity of that hardware, is secondary to the security of the data. Hardware is easy to replace.

Data Protection

Data, the primary asset

I work at an insurance company. In my company, data is **the** major asset. Without it, we would go out of business. We keep large volumes of data on many different things.

- Clients
- Claim information
- Premiums (income)
- Losses (expenses)
- Injury statistics
- Credit Information

All this data has a single purpose in the company. To help us make more money. This data is so important to us; in fact, the largest percentage of employees in the company spends all of their time entering this data into our systems. The next largest percentage of people spends all of their time analyzing and using this data.

This isn't unique to my company. There are many different types of organizations that use large amounts of proprietary or confidential data like this.

- Sales – Client Lists, Marketing Campaigns
- Technology – Patents, Blueprints, algorithms
- Securities – Stock trading information, customers
- Banks – Customers, account information, securities
- Publishers – Copyrights on books or magazines
- Consultants – Clients, customer project information
- Internet "Dotcoms" – Customers, Email addresses, credit cards, etc.
- Demographic Companies – Surveys, reports, statistics

In all of these company's, the loss of a significant amount of data can spell the end of that company. This is why data security can be such an important issue.

Some examples:

> **Ex-FAA engineer eyed for software theft**
>
> (CHICAGO) A former Federal Aviation Administration engineer has been charged with stealing the only copy of a computer code for software used by flight controllers to guide jetliners through O'Hare International Airport[1].
>
> **Why the DVD Hack Was a Cinch**
>
> The anonymous developers of the decryption program that removes DVD copy protection had an easy time doing it, thanks to a gaffe by a software developer and the surprising weakness of the encryption technology.
>
> Essentially, the two European hackers who developed the DeCSS utility that copies a DVD movie disc were able to break the code because one of the product's licensees inadvertently neglected to encrypt the decryption key. [2]
>
> **October 1996, The American Employment Law Council Conference**
>
> Borland International Inc. brought a lawsuit against one of its' former employees who had used the company's e-mail system to send confidential trade secrets to his new employee. The former employee and the recipient were both charged with trade secret theft. [3]

Data Thieves

Who is stealing all of this information? For our purposes we will call these people data thieves. Data thieves are white-collar criminals that come in two flavors, those that know they are stealing data, and those that do not.

Malicious

They are out to steal trade secrets. Most likely they already work for your company. Perhaps they used to work for your company? Perhaps they are planning to go to another company? Maybe a competitor?

These people are removing this data for personal gain. This data could be used for insider trading, client lists to competitors, personal information about customers or employees?

> "In the days where all your blueprints were bulky and on real paper, it was reasonably difficult for someone to walk off with them undetected. While we have all seen films with spies taking covert photographs of such things, you are more likely to find someone walking out with a tiny backup tape containing ALL of the company data, and not just the odd document. Something like a 4mm DAT tape, commonly used as a backup medium, can hold vast quantities of data (24 Gigabytes in one format). This is usually sufficient to take all or a sizeable chunk of vital business data and, if carefully executed, it is difficult (but not impossible) to detect that anything has been taken.
>
> "It is not readily apparent to many managers that in order for someone to be able to backup all users files, the operative must have high level access rights on say a network server in order to access everything. This is a lot of responsibility, and due the mundaneness of the job, the task of backing up is often left to low grade staff. If you have a high turnover of staff in this area you are leaving yourself wide open to potential fraud. Your competitors will pay handsomely for a copy of everything you have!"[4]

Accidental

These would be the innocents. These people are merely taking a document home to work on. They were working on their laptop in an airplane. They dialed in to the network and downloaded some records. What about if they emailed that spreadsheet to their home to finish? You may argue that they aren't really stealing, just borrowing this data. And in many cases that may be true.

The questions you must ask then are "How important is this data to the company?" and "How vital is this data to the company?" Can you really trust that user to not "lose" that data? Does this user really need to take this data off premises?

Most of the time, these are the ones that most of your security is for. Unfortunately, the ones who really want to steal it, will find a way.

Security Issues

When reviewing your security issues, there are several areas you need to look at.

Data Stores

First are the data stores. Where is this information and how is it secured?

Database

Databases are the ultimate data stores for some companies. My company keeps most of the really important business data in a huge database called a data warehouse. This data is used and analyzed for all sorts of very important business functions. Without it, we would not be able to function properly. If it were compromised, that data could be used by our competition to take over all of our business.

A security review of these very important corporate databases revealed that the default administrator's password was blank. Another database developer had given all of it's users administrator-level privilege on the data sets, because he couldn't figure out a problem where permissions were preventing access to certain users. Still another database developer had just given everyone the server administrator's username and password to use, instead of setting up individual accounts.

This stuff runs rampant. Either due to lack of time, skill, or motivation to make things work properly. These aren't even really high-level technical security issues. These are the easy ones everyone knows about.

Network Shares

Network shares should also be reviewed. In Windows NT there are two sets of permissions on user files on a network share. The share permissions and the NTFS drive permissions. Make sure you look at them.

Email Systems

Most people keep all kinds of information in their email software. They will often categorize this data so they can find it. They leave passwords, important statistical data, project proposals, etc. There are several things to consider in securing email systems. One, try and minimize the use of email as a means of communicating confidential information. Two, try and eliminate the excess of that information by implementing an automatic purging process. Our company automatically purges all email every 90 days. This also has legal implications that I will not go into here.

Tape Backups

Most companies back up pretty much all their data. These tapes are often the repositories of all corporate data. Secure them well.

Data Egress

Data can be removed from your company in many ways. These are some of the more common data egress points.

Removable Media

Tape backups generally contain data that is important enough to back it up. It is unfortunate that most companies usually delegate this task to the low grade, high turnaround workers. The new guy is the one that gets "stuck" with performing this arduous task. In reality, this should be a task for someone you can trust with access to this data. The system admin, the office manager, the boss, or anybody who has a stake in ensuring this data is secure. Anyone can walk out with a tape.

What about floppy drives, ZIP drives, removable hard drives. These can hold lots of important data and fit neatly in someone's pocket.

Laptops

The only thing we can say about laptops is to use them wisely. Do your best to minimize the number of laptops in your company. Educate the laptop users about there unique responsibilities. There are also many tools that will allow you to secure them

Email

It may seem fairly innocuous, but email is one of the biggest data security holes in any corporation. Unfortunately, there is often no good way to prevent this. Any one, in any company, can email any file they have access to. And there isn't much you can do about it. There are things you can do after the fact, but if the data is already been sent, you are never going to get it back.

Remote Access

Dial in and VPN users can often access your network at any time from anywhere. Make sure you educate these users about their data security responsibilities. Other possibilities include limiting the systems a dial in user can access.

Remote User Issues

Remote users open up a whole new slough of security issues. Some of them we touched on previously.

Home PC Security

When a user connects his home PC to your network you have to worry about many

things. You no longer are worrying about security from workstations, or even laptops that you have some modicum of control over. Now you have to worry about Joe's home computer, that his youngest kid plays games on, and his older boy likes to download the latest software of the Internet. These systems can become portals into your network. They can also be used to spread all sorts of malicious software around on your network including any number of virus, Trojan horse programs, security scanning tools, and hacking tools. You have no control over these PCs and what the many users of it may do.

Physical theft of laptops

Laptop users tend to synchronize data to their laptop for working offline. They also may retrieve data when dialed in. For the most part when laptops are stolen, it is specifically for the value of the laptop itself. This is also a loss that can be written off. Look at different solutions for securing the data on these laptops should they be stolen.

Solutions

There are many different solutions that you will need to evaluate for all of these various security issues. These methods and best practices are also fairly widely known and will not be covered here.

An outline of some things you may wish to cover in developing these security practices are as follows:

- Company Policies
    - Strict Dial In/VPN
    - Email Policies
    - Termination Policy
    - Industry Users
    - Accounts Disabled
    - Equipment Returned
    - Password Policies
    - Pre-Hire Background Checks
- User Education
    - Social Engineering
    - "Common Sense" Security Issues
    - Virus Issues
    - Home machines
        - Security
        - Virii
- Workstation Lockdowns
- Laptop Lockdowns
    - Hard Drive Passwords
    - BIOS Passwords
    - Tracking Devices
    - Locking Cases

    - Cable Locks
- Security Tools
- Toolkit for remote users
    - Documentation
    - Virus Scan
    - Personal Firewall Software
    - Inexpensive Firewall Device
    - VPN Clients

Conclusion

"The sad truth is that most computer crime is committed by ordinary employees who have the opportunity in their place of work. In most instances it is not ultra high-tech hacking and phreaking techniques that cost an organisation money, but poor operating practice, improper supervision, poor staff morale and lack of correct checking procedures."[5]

The primary asset of many companies is data. In a growing number of companies this can be its only asset. This is why data security is so important.

When developing security plans you must be aware of where the data is. Too many people spend a good portion of their security planning on securing servers, routers, etc. You must be aware of issues of securing the data. The server doesn't have to be compromised if everyone has administrative rights to the database.

Server security is important from the standpoint of availability. However, data security is what needs to be the primary focus of security analysis.

References

[1] Author Unknown, "Ex-FAA engineer eyed for software theft" Associated Press. 10/21/1999. http://www.usatoday.com/life/cyber/tech/ctg484.htm. 11/20/2000

[2] Andy Patrizio. "Why the DVD Hack Was a Cinch". Wired News. 11/2/1999. http://www.wired.com/news/technology/0,1282,32263,00.html

[3] Author Unknown. "Content Security Issues – Theft of Data." 1999. http://www.mimesweeper.com/products/cs/datatheft.asp, 11/20/2000

[4] Author Unknown. "Are You at Risk?" Forensic Bulletin Issue 2. 5/1999. http://www.vogon-computer-evidence.co.uk/forensic_bulletin-02/forensic_bulletin_2_4.htm, 11/20/2000

[5] Author Unknown. "Where is the enemy?" Forensic Bulletin Issue 4. 8/1999. http://www.vogon-computer-evidence.co.uk/forensic_bulletin-02/forensic_bulletin_4_4.htm, 11/20/2000