Plugging the holes! Your data is leaking OUT!

Robert G Downey

Version 1.2e

Data is essential to the development and success of a company. It can also be the downfall of a company if it gets into the wrong hands. There are many improper uses of data obtained from a company. Data can be used to compromise trade secrets or potential transactions. Data can also be used to "profile" a company. Profiling may be the first step before an attempted infiltration of your network. It involves gathering data from any and all sources to complete an assessment of the structure and controls within the company and potential holes in the defense. Many times the data obtained for profiling is obtained through normal channels - take the instance when the US nuclear test plans and locations of pertinent officers were obtained from profiling government web sites. A major breach in security was accomplished without a "break-in". This emphasizes the need to understand the data available from all sources that references your company.

Data classification - labeling and handling

The first step is securing your network using the latest in security configurations and patches, and then an evaluation and monitoring of all the other holes in the network becomes essential. Beyond these normal controls for locking down access to a network, a security administrator should also look to see how information is used, transported and disposed.

A good security program must know the data flow, what information exists and develop methods of classifying it.[1] A general categorization of data to classified, restricted or general will provide a good basis for analyzing and assessing the risks and the impact that may occur if the data is compromised. This classification should be conducted in joint discussions with users of the data and the security administrators. They must work together to correctly assess the value of the data.

After the classification of the data, the administrator should look to the security of the containers of that data. Data can take many forms. As Security administrators we are usually looking at data in the electronic format. Electronic data can have many containers. Storage can be on server disks, user disks, CDs, tapes or floppies. All these represent a potential loss if compromised. Proper storage and disposal of electronic copies of data is needed to protect the company assets.

Portable media

Data can also leave the company through portable media. Virtually every PC and Laptop comes with a floppy drive. Fortunately, the space limitations of the floppy drive, 1.44 MB, limits the risks of data loss with the biggest threat being the importation of viruses from

[1] http://csrc.nist.gov/secpubs/rainbow/

the floppy. Issues do arise when users have access to newer technologies such as ZIP drives, Jazz drives and CD ROM writers. Establish a policy and procedures for a user to follow who is requesting one of these devices. All requests should be reviewed by security and a proper business justification required before their purchase. Use media that is appropriately labeled as “Property of Company X Internal Use Only” and establish procedures for the secure storage and destruction of the information. All data that is stored on this media should be given the same security considerations as a backup tape. They contain company information that should not be allowed outside of the company without appropriate permissions. Also, any tapes or CDs that are no longer being used must be properly disposed of to insure the confidentiality of the data. There are various methods of destruction. CDs can be rendered unusable by scoring their surface with sandpaper.[2] Tapes can be degaussed or crushed for disposal.[3]

Paper copy

Security administrators must also consider other potential vehicles that can contribute to losses. Data in hard copy can also have compromising information. And is frequently mishandled. When all the areas of data storage have been compiled whether electronic copy or hard copy, security risks need to be assessed and mitigating controls incorporated to protect the data.

Paper copies of information must be properly classified and appropriately labeled. Do you mark the documents as to their data classification? This is only valuable if the paper is handled properly. Confidential information must be stored in a secure location and properly labeled. If data is properly labeled, a review should be conducted of how users handle that data. A walk around at night by properly trained security personnel can be conducted with a quick review of desktop materials left on the desks. If confidential documents are observed in plain view, they should be confiscated and a form left informing the user of the confiscation and procedures for the document returns. Users training should be conducted on proper handling of confidential material when they request the documents to be returned.

How is paper disposed of in your organization? Disposal of confidential and restricted paperwork must be done in a secure manner. Recycling is a good for the environment but leaves the documents available to many individuals during the process. Using either an office shredder or one of the available shredding services will prevent the documents compromise. If a shredding service is used, choose one that shreds the documents on site to lessen the potential for exposure. Documents that are thrown into the dumpster can be retrieved by dumpster diving[4], a practice commonly used to profile a company.

[2] http://selectug.mslicense.com/handlinganddisposal.asp

[3] http://www.usmc.mil/directiv.nsf/bf7ed869c4398a1685256517005818da/5b90a70b0c5184b985256977004c7af7?OpenDocument

[4] http://www.jargon.net/jargonfile/d/dumpsterdiving.html

Electronic Copy

Frequently the backup copies of servers are mishandled and controls are not established documenting all tapes and locations of those tapes. Most people are aware of the various backup cycling processes. Some companies are using off site storage for some if not all of their backup tapes. All this is good business practice, but without the proper handling, storage and disposal of the tapes the business is at risk. A backup tape contains either a partial or complete backup of a server. This can be critical information that should be guarded as closely as the original copies on the server. Tapes should be stored in secured and locked containers. Frequently, tapes are left on top of tape cartridges or on server tops waiting to be recycled. Anyone that has access to that area can pick up the tape and with the proper machine and software they can obtain a copy of the servers information. At risk are not only the company information but also potentially the password files from the server. Proper procedures must be in place to prevent the loss of a tape. These include:

1. Limited access to any area that has backup machines.
2. Total inventory of all tapes once they become part of the backup cycle.
3. A secure and locked storage compartment for all in cycle tapes. (It may be locked but can it be carried away?)
4. A valid offsite storage location – a commercial vault that has adequate protection
5. A pickup procedure that does not leave tapes in the open waiting for the driver.
6. A procedure to allow only authorized individuals to request return of tapes from archives.
7. A documented procedure for disposal of old or damaged tapes that provides the complete destruction of the magnetic media.

Laptops

Laptops have provided a large boost in production for companies but without proper controls they represent a large risk to the company for potential data loss and possible network compromise. Simple steps can be taken to insure a degree of security with laptops. All laptops should be supplied with security locks. There are many types of locks available. Ease of use insures that they are used. If necessary, supply 2 locks such as the Kensington type of security cable. One can be permanently set for the desktop while the other is stored in the carrying case for remote and offsite use. There are also new alarms being developed that can be used to guard a laptop. Some of these use motion sensors and others use proximity detectors. All decrease the potential for thief of the laptop.

Laptop protection – Encryption

Protection of the data on a laptop should continue even after it is stolen. A boot up password provides a limited amount of protection that can deter the casual thief. Most systems can be reset or an OEM password can override the user-defined password. IBM ThinkPad's at one time required the replacement of the motherboard to change the BIOS password protecting a stolen laptop but creating a problem if the password was lost. File encryption either on the whole drive or on a subset of sensitive files will protect sensitive information. The US State Department is still investigating the disappearance of a laptop containing sensitive information on nuclear weapons[5] with a $25,000 reward. What would have been the loss if the contents had been encrypted? There are many products that can be used to encrypt either files or complete systems.

PGP, a standard in the industry for years, can be used to encrypt sensitive files and directories. A PGP volume can be created that will store the data encrypted until ready for use. There are other software systems that will encrypt the hard drive of the laptop and require a password before access to the system. If the laptop is using Windows 2000 there is a native program that can be used to encrypt the system – Windows 2000 EFS.

Lost laptops and remote access

Laptops are frequently used as a means to gain remote access into a company. Users commonly use DUN (Microsoft Dial Up Networking) to dial into the company either from home or on the road. If configured improperly, the laptop can access the network by having the UID and password stored in the phone book entry. Configuring systems to prompt for this information is essential. A better level of security is to use a token system such as RSA SecurID.[6] A token can be either a card or a FOB but must be stored separate from the laptop i.e. a FOB as the user's key chain. The user will also have to know a PIN as well as the current token code generated from the FOB. Using such a method will prevent the thief from accessing your network and doing more harm.

Decommissioned Assets

Old and broken PCs and laptops usually contain sensitive data and need to be cleaned before disposal. Many companies recycle old PCs to their employees either free or at a low cost. This presents not only concerns on the licensing agreements but on the information that they may contain. All PCs should be wiped of all information before allowing an employee to take one home or before they are being disposed. PCs are now considered hazardous waste and must be properly disposed or recycled.[7] PCs contain lead, cadmium, mercury and chromium as well as plastics and other products can be readily recycled.[8] Many companies that specialize in the disposal of these assets can also provide a service to assure that either the hard drives are wiped clean or that they are properly destroyed. Get the assurance in writing on their methods of disposal and review it for assurance that the hard drives are to either be wiped or destroyed.

File transfers

[5] Information Security Laptop Security February 2001

[6] http://www.rsa.com/products/securid/index.html

[7] http://news.cnet.com/news/0-1006-200-5983000.html
http://www.thegreenpc.com/epa_regulations.htm

[8] http://www.retrosystems.com/waste1.htm

Much information is sent over the Internet in emails or by FTP. If this information is sensitive to the company someone will be able to collect and use it. Email systems can be used for a transfer of information but should use some method of encryption to prevent the retrieval and use of the information by an unauthorized third party. PGP is one product that can incorporate into an email program and encrypt data either by using a password or through the use of Public/Private keys.[9] FTP file transfers can also be encrypted through automated processes using a public key and sent to a FTP server. PGP has developed a server-based solution for automatic encryption and decryption of files – E-business server. Using the E-business server inside the firewall protects the keys and the files either before encryption or after decryption. . If the FTP server, which resides in a DMZ, is compromised the data will be useless without the private key to decrypt the file.

Offsite Web and Server Storage

If you are limiting your connections to a dialup solution, your users are probably complaining about the speed of their connections. Some users may resort to using the relatively new storage options available through the Internet on Web servers. One listing of free storage solutions contains over forty sites. [10] A user can copy a document or a project to one of these servers and then access the information from their high-speed connection at home. This could be to continue working on a project after hours or to provide someone else access. Once that data is outside the bounds of the corporate network, it is open to the public. Not only will it be vulnerable in transit but while in storage on the web server.

Employees using off site email either with their home mail account or a web based email account can also be a problem. Some users will forward their mail to their home or web address. This creates a problem in both transit and storage. Mail frequently travels on the Internet but a large volume of the corporate mail is internal to a company. Once this mail is send outside of the company, it becomes vulnerable to collection. Email that may contain information that must remain within the bounds of the corporation can now be accessible not only in transit but while stored on the user's email server. The use of forwarding can be controlled by imposing controls limiting a user's option on using a forwarding agent and by limiting access through the firewall to other email servers. Web mail will still be available and email can also be manually forwarded to the address. Monitoring of web traffic (port 80) to email sites can be effective but with a large amount of web traffic from the user community it may become burdensome and limited to support staff availability. Web monitoring solutions such as Elron Internet Filtering software[11]can be used to block sites that provide web mail. This may create issues since a large number of the search sites that would be legitimately accessed by the users also host web mail and could be blocked. A policy may be more corporate friendly but less enforceable.

[9] http://www.baltimore.com/library/pki/
[10] http://www.webwizards.net/useful/wbfs.htm
[11] http://www.elronsoftware.com/index.shtml

Conclusion:

There are other areas that are of concern for data loss and continue to represent threats (as well as benefits) to a company. Remote access through portable devices and palms being lost outside of the company with sensitive databases are evolving threats. Wireless technologies provide added flexibility in connections but are susceptible to sniffing. As these new technologies develop each has to be assessed and mitigating controls placed to protect the company while still allowing the users to do the daily tasks of the business.

We have covered some of the obvious areas where data can leave the company. A good security officer must be curious and constantly asking questions and looking at what the users are doing. The security officer's job is to protect the company and to do that they must know how everything works.

Links:

Vendors:

RSA Security
http://www.rsasecurity.com/news/pr/981013-2.html

EFS Security
http://www.win2000mag.com/Articles/Print.cfm?ArticleID=5006

PGP Software
http://www.pgp.com/products/corporate-desktop/default.asp

Laptop motion security
http://www.trackitcorp.com

Laptop security locks
http://www.kensington.com/

Further Information:

Public Key Infrastructure
http://www.ietf.org/html.charters/pkix-charter.html

Protection Against Inadvertent Release of Restricted Data and Formerly Restricted Data
http://www.fas.org/sgp/othergov/inadvertent.html

Security of Confidential Information, Official Documents, Tax Data, and Government and Personal Property
http://www.irs.ustreas.gov/prod/bus_info/tax_pro/irm-part/part30/29712.html

A Checklist of Responsible Information-Handling Practices
http://www.privacyrights.org/fs/fs12-ih2.htm

Rainbow Series
http://csrc.nist.gov/secpubs/rainbow/

FBI finds what might be former nuclear scientist's tapes
http://detnews.com/2000/nation/0012/09/nation-159687.htm

Disposal of Vacuum Tubes and Circuit Boards
https://denix.cecer.army.mil/denix/Public/Library/HazWaste/Disposal-Guide/hwdg5.html#Vacuum%20Tubes%20and%20Circuit%20Boards

Energy Computers For Reuse Contained Important Data
http://www.fose.com/ind-news/010405112548.html

HP recycling program
http://206.144.247.60/state/

HP launches product-recycling program
http://news.cnet.com/news/0-1006-200-5983000.html