Getting Rid of your Old Computer?
How to Ensure you are Protected from Identity Theft

Presented by Joe Mount and Kevin Enders

Tabernus

October 22nd, 2008
Agenda for Presentation

1. Short introduction
2. Why you need to eliminate your personal data
3. Myths about data elimination
4. Data elimination methods available
5. Recommendations for Individuals
6. Business/State Agency Information
7. Recommendations for Businesses/State Agencies
Short Introduction
Presenters from Tabernus Management Team

Joe Mount – Director of Business Development
Engineering from Georgia Institute of Technology
Background:
- Dell
- Applied Materials
- US Army

Kevin Enders – Director of Marketing
Engineering from University of Texas
Background:
- Applied Materials
- ISDG Marketing
- Digital Light Innovations
Why Erasing your Personal Information is Important
What are Criminals Trying to Get from You

Criminals (particularly identity thieves) are working to get the following pieces of personal information from you:

- Credit card numbers (sixteen digits)
- PIN numbers (four digits)
- CW numbers (three digits)
- Social security numbers (ten digits)
- Bank routing numbers (nine digits)
- Bank account numbers (ten digits)
Security Extends beyond Your Possession of the Computer

Data Lifecycle

- Replace/sell/donate
- In your control
- Out of your control
- Well Protected
- Unprotected

Important Notes:

- Attempts are made to gather your personal information along the entire lifecycle of your data
- You are responsible for protecting yourself against this threat throughout entire lifecycle
- This includes what you do with old data or data storage devices

Tabernus
Leaders in Electronic Data Elimination
Technology Based Information Theft Techniques

• Phishing
• Pharming
• Spyware and Malware
• Hacking into Secure Networks
• Compromised computer equipment

* Obtaining sensitive information from legally purchased computers and storage devices is considered the **mother lode** for those planning illegal activities with the information. The amount of information that can be gathered from one hard drive, and the relative ease with which it can be obtained, makes this very appealing when compared to the others.
Protecting Your Personal Data Includes End of Life

Most individuals do a good job of protecting their personal information from threats while they own the computer. Attention must be paid to eliminating the data before getting rid of the computer.

- Phishing
- Pharming
- Spyware and Malware
- Hacking into Secure Networks

Have Software

Ensuring that data is removed from old computers/hard drives before they leave your control

Often Marginalized

Tabernus
Leaders in Electronic Data Elimination
Cost Burden Associated with Identity Theft

• Consumers are being held less responsible
• Companies are accepting larger risks
• Companies have large lobbies to create legislation…
Myths Regarding Elimination of Data
What Really Happens when you Hit Delete

Delete the File  Empty Recycle Bin

Data on a hard drive is not “gone” until it is overwritten by other data. Deleting a file simply partitions the deleted information in a manner that allows for it to be overwritten when this space on the hard drive is needed at a later time.

It is not gone.
Why Reformatting Leaves you in Jeopardy

Misconception:
Reformatting removes all data from a hard drive.

Reality:
Only 1% of a drive is overwritten.

Formatting only does the following:
• Manipulates the base root directory, file allocation tables, boot sectors
• Reads entire hard drive to find damaged sectors that should not be used for data storage in the future.

It does not overwrite the data on the drive.
This data can still be captured using readily available software programs.
Enough Bad News – Here’s the Good News

• Successful elimination of your personal data is not hard.
• Techniques to do it are readily available
• A technique is available for nearly every situation
Methods Available for Successfully Eliminating Data from the Hard Drive on Your Computer
Hard Drive Data Elimination Methods

- **Physical destruction of hard drive**
  Drive are crushed or drive/platters are damaged

- **Degaussing of hard drive**
  Magnetic media on the drive is destroyed with magnetic field

- **Overwriting of data contained on hard drive**
  Each bit on drive is replaced with “white” information

There are circumstances that would require the use of each of these three options. Each has strengths and weaknesses.
Physical Destruction of Hard Drive

Situations when destruction should be used:
- Drives are damaged and/or can not be communicated with
- Data can not be overwritten

Advantages:
- Fast
- Supposedly 100% foolproof*

Disadvantages:
- Waste generation – not a green solution
- Expensive (no reuse of hard drives)
- Difficult to document what has been done
- *Data is in someone else’s hands during process
Degaussing of Hard Drive

Situations when degaussing should be used:
• Drives are damaged and/or can not be communicated with
• Data needs to eliminated very quickly

Advantages:
• Very fast – drives can be degaussed in seconds
• Suited very well for tape and floppy disks

Disadvantages:
• Waste generation – not a green solution
• Degaussing tools are very expensive and heavy
• Most degaussing tools do not record asset information
• You’ve still got them, and they don’t work anymore
Overwriting Data Contained on Hard Drive

Situations when overwriting should be used:
• Drives need to be salvaged and reused
• Drives are part of lease agreement

Advantages:
• Not a destructive process – allows for reuse of drive
• Ease of reporting and documentation
• Easily and cost effectively performed inside your walls
• Drives do not need to removed from system to overwrite them

Disadvantages:
• Time intensive compared to other methods
Recommendations for Individuals
Recommendations

• Eliminate the personal data from your computer before you hand it off to anyone else.

• If you plan to simply get rid of your computer (trash it), then work with an established recycling agency.

• Be very aware that you have many devices other than your computer that also have personal information on them.
Data Elimination for Businesses and State Agencies
Your Business/Agency is Responsible for Protecting Sensitive Data During the Entire Data Lifecycle

A lot of companies and organizations have strict policies for protecting themselves from data hacking, but lack disciplined approaches to eliminating data from storage devices prior to disposal.

- Phishing
- Pharming
- Spyware and Malware
- Hacking into Secure Networks

Ensuring that data is removed from old computers/hard drives

Policies in Place

Often Marginalized

Tabernus
Leaders in Electronic Data Elimination
Data Elimination is No Longer a One Step Process

In the past, data elimination was typically considered a one step process.

Simply erase the data.

Problems with this approach:

• Manual control over what has been erased/not erased
• No backup documentation to show what has been erased
• No process to follow for exceptions/anomalies
• Unnecessary destruction of drives
Data Elimination is a Multi Step Process

With new legislation in place, data elimination must be taken seriously. It needs to be viewed as a multi-step process.

1. Develop Process for Elimination
2. Control Asset Information
3. Eliminate Data from Hard Drive
4. Maintain Accurate Documents

Companies must develop disciplined processes, know exactly what they need to erase, and maintain accurate documentation showing what has been erased.
Problems Associated with Loss of Sensitive Information

**Legal Repercussions**
- Sarbanes Oxley
- HIPAA
- Graham-Leach-Bliley

**Civil Repercussions**
- Class action lawsuits

**Business Repercussions**
- Mandatory public disclosure – loss of public trust
- Loss or dramatic increase in insurance coverage
- Financial problems
Cost Burden Associated with Identity Theft

- Consumers are being held less responsible
- Companies are accepting larger risks
- Companies have large lobbies to create legislation…
In Process Legislation to Protect Consumers

As of early 2008, many new pieces of legislation are in process that will increase penalties associated with loss of personal/sensitive information

• S. 239: Notification of Risk to Personal Data Act of 2007
• S. 495: Personal Data Privacy and Security Act of 2007
• S. 1202: Personal Data Protection Act of 2007
• S. 699: Social Security Number Fraud and Identity Theft Prevention Act
• S. 1260: Data Security Act of 2007
Repercussions of Loss of Sensitive Data

• Aside from potential criminal and civil penalties, business related penalties can be just as damaging.

• Almost all legislation mandates that companies must disclose publicly any data losses or breaches.

• Loss of customer faith is difficult to measure, but can be extremely damaging to companies that are not careful and thorough.
Summary

• Any data in your control is your responsibility during entire lifecycle
• New legislation is putting more emphasis on consumer protection
• New legislation is putting higher penalties on violators
• Data elimination cannot be marginalized
Recommendations for Successful End of Lifecycle Data Control and Elimination

- Develop an agency policy
- Educate your staff
- Assess what you need to erase every time
- Document what you do
Recommendations for Successful End of Lifecycle Data Control and Elimination

Develop a Policy

Develop, document and disseminate a thorough set of policies and practices for eliminating end of lifecycle data in your possession, including any type of electronic storage devices.
Recommendations for Successful End of Lifecycle Data Control and Elimination

**Educate your Staff**

Educate staff on the importance of data control and the policies determined by your company for retiring any equipment that contains electronic storage capability.

Examples include:

- Hard drives
- Tape drives
- Jump drives
- Printers

*Tabernus*

*Leaders in Electronic Data Elimination*
Recommendations for Successful End of Lifecycle Data Control and Elimination

Assess the Situation Every Time

When the time comes to perform data elimination, assess what needs to be erased and ensure that your current policy covers what you need to do.
Recommendations for Successful End of Lifecycle
Data Control and Elimination

Document what You Do

Generate and accurately control documentation on all pieces of
storage media that are decommissioned or replaced.

• Equipment type
• Serial numbers
• Asset information
• Date of erasure
Recommendations for Successful End of Lifecycle Data Control and Elimination

- Develop a company policy
- Educate your company
- Assess what you need to erase every time
- Document what you do
Question and Answer