


Your Grandfathers DLP 
Solution Can Not Protect
You In The Age Of Wikileaks

First - What (In My Opinion) Is DLP?

- + DLP (Data Leakage Prevention) by-and-of-itself is not a product or a technology..... it is a collection / series of infosec programs that when implemented properly can provide for the mitigation of some of the risk associated with data leakage.
- + These programs most often include (among others) :
 - + Risk Assessment
 - + Security Awareness Training
 - + Controls Management
 - + Removable Media Policies
 - + Monitoring & Auditing of Controls
 - + Incident Response Planning

Really - DLP Is Not A Product?

- + But Vendor XYZ claims to have a DLP Solution ?
 - + Any vendors DLP offering is really a collection of some (or all) of the technologies that can be used to accomplish the goals defined within the scope of the previously noted programs
 - + Risk Assessment
 - + Security Awareness Training
 - + Controls Management
 - + Removable Media Management / Controls
 - + Monitoring & Auditing of Controls
 - + Incident Response Planning
 - + Great care should be taken in evaluating any vendors DLP offering. Some are very comprehensive solutions and some are not - caveat emptor....

A Clarification To Set The Stage

- + I don't "dislike" DLP – I really don't
 - + However I "don't like" how many organizations implement DLP
 - + DLP without removable media controls will likely fail
 - + DLP without user awareness education / training will fail
 - + DLP that is limited to any specific group of protocols will fail
 - + i.e. are you checking your VoIP communications (RTP) for embedded data?
 - + See Stego RTP



Wikileaks – I Told You So.....

[Home](#) [Forensics](#) [Virtualization](#) [Blog](#) [Interviews](#) [Articles](#) [Events](#) [Links](#)



Wikileaks - New host for mass document
leaking and analysis

Friday, January 12, 2007

This is poised to get very ugly.....

Wikileaks



250,000 US Diplomatic Documents and
150,000 US State Department Documents

A personal opinion:

Sorry folks I have a hard time believing that
this was some glorious patriotic act...

Manning reportedly was upset over "Don't Ask
- Don't Tell" and the recent bitter breakup with
his boyfriend..... He copied the documents to
a recordable CD as he lip-synced Lady Gaga
tunes...



Wikileaks

10. CHARGE I: VIOLATION OF THE UCMJ, ARTICLE 92

SPECIFICATION 1: In that Private First Class Bradley E. Manning, U.S. Army, did, between on or about 19 November 2009 and on or about 27 May 2010, at or near Contingency Operating Station Hammer, Iraq, violate a lawful general regulation, to wit: Paragraph 4-6(k), Army Regulation 25-2, dated 24 October 2007, by wrongfully introducing a classified video of a military operation filmed at or near Baghdad, Iraq, on or about 12 July 2007, onto his personal computer, a non-secure information system.

SPECIFICATION 2: In that Private First Class Bradley E. Manning, U.S. Army, did, between on or about 19 November 2009 and on or about 27 May 2010, at or near Contingency Operating Station Hammer, Iraq, violate a lawful general regulation, to wit: Paragraph 4-6(k), Army Regulation 25-2, dated 24 October 2007, by wrongfully introducing more than 50 classified United States Department of State cables onto his personal computer, a non-secure information system.

SPECIFICATION 3: In that Private First Class Bradley E. Manning, U.S. Army, did, between on or about 19 November 2009 and on or about 27 May 2010, at or near Contingency Operating Station Hammer, Iraq, violate a lawful general regulation, to wit: Paragraph 4-6(k), Army Regulation 25-2, dated 24 October 2007, by wrongfully introducing a classified Microsoft Office PowerPoint presentation onto his personal computer, a non-secure information system.

(SEE CONTINUATION SHEET)

Wikileaks – A Wake Up Call

- + Simply because you have access to information does not necessarily give you the right to copy it to removable media..
- + This could have been prevented
 - + Typical Policies without Technical Enforcement
 - + Removable media on a classified network – DUH?
 - + However important to note that “Traditional DLP” probably would have missed it
 - + Traditional DLP (filtering) is great for things like credit card numbers but not much help when you want to control the spread of secrets

Wikileaks

+ What's next for Wikileaks?

Bank of America



Bank of Opportunity™

Data Leakage Business Drivers

Loss of Customer & Confidential Data

- Credit Card Records
- Social Security #s
- Financials

Breach of Corporate Governance

- | | |
|--------------------------------|------------|
| ▪ HIPAA | ▪ GLBA |
| ▪ EU Data Protection Directive | ▪ SB 1386 |
| ▪ SOX | ▪ Basel II |

Loss of Intellectual Property

- Patents
- Source Code
- Trade Secrets

Can't Forget About Red Flag Rules...

SEC. 2. SCOPE OF CERTAIN CREDITOR REQUIREMENTS.

(a) AMENDMENT TO FCRA.—Section 615(e) of the Fair Credit Reporting Act (15 U.S.C. 1681m(e)) is amended by adding at the end the following:

“(4) DEFINITIONS.—As used in this subsection, the term ‘creditor’—

“(A) means a creditor, as defined in section 702 of the Equal Credit Opportunity Act (15 U.S.C. 1691a), that regularly and in the ordinary course of business—

“(i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;

“(ii) furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or

“(iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person;

“(B) does not include a creditor described in subparagraph (A)(iii) that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person; and

“(C) includes any other type of creditor, as defined in that section 702, as the agency described in paragraph (1) having authority over that creditor may determine appropriate by rule promulgated by that agency, based on a determination that such creditor offers or maintains accounts that are subject to a reasonably foreseeable risk of identity theft.”.

Red Flag Rules... Are You Exempt?

Congress Exempts Physicians From Identity Theft 'Red Flags' Rule

By Sheri Porter

12/8/2010

Congress has voted to exempt physicians from the Federal Trade Commission's antifraud identity theft regulation known as the "Red Flags" Rule. The Senate passed S. 3987, the Red Flag Program Clarification Act of 2010 (at the THOMAS website, type "S. 3987" in the search field after selecting "Bill Number"), on Nov. 30, and the House gave the go-ahead by voice vote on Dec. 7.

President Obama is expected to sign the legislation before the Jan. 1 compliance deadline.

The Red Flags Rule, which was drafted in 2008 in connection with the implementation of the Fair and Accurate Credit Transactions Act of 2003, requires financial institutions and creditors, including -- until now -- physician practices, to address the risk of identity theft by implementing identity theft prevention programs.

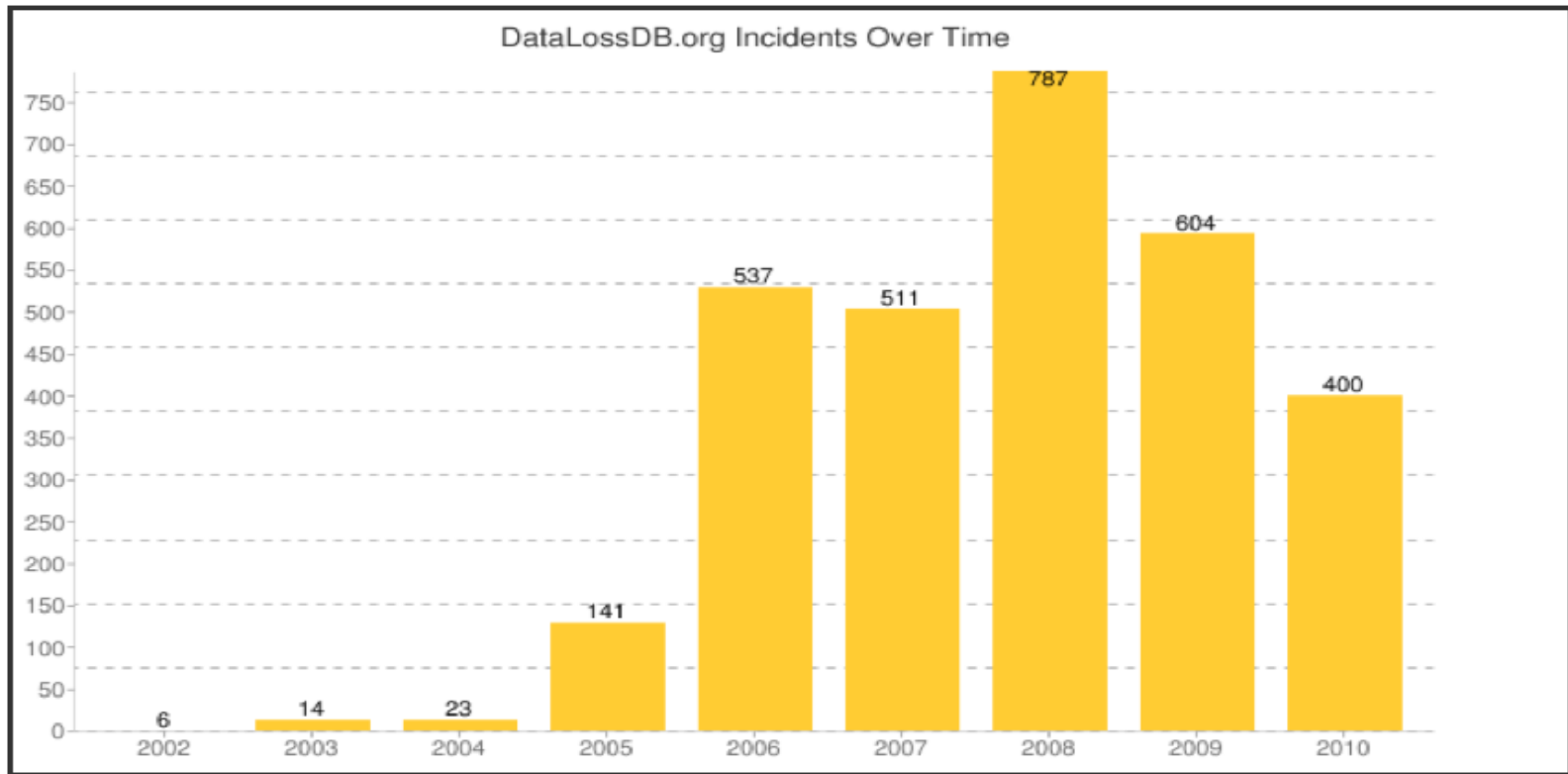
Breaking

NEWS

Largest Incidents To Date

RECORDS	DATE	ORGANIZATIONS
<u>130,000,000</u>	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
<u>94,000,000</u>	2007-01-17	TJX Companies Inc.
<u>90,000,000</u>	1984-06-01	TRW, Sears Roebuck
<u>76,000,000</u>	2009-10-05	National Archives and Records Administration
<u>40,000,000</u>	2005-06-19	CardSystems, Visa, MasterCard, American Express
<u>26,500,000</u>	2006-05-22	U.S. Department of Veterans Affairs
<u>25,000,000</u>	2007-11-20	HM Revenue and Customs, TNT
<u>17,000,000</u>	2008-10-06	T-Mobile, Deutsche Telekom
<u>16,000,000</u>	1986-11-01	Canada Revenue Agency
<u>12,500,000</u>	2008-03-26	LaSalle Bank, BNY Mellon Shareowner Services, Archive Systems Inc, The Walt Disney Company, SYNOVUS

Reported Incidents Are Declining



But Cost Per Lost Record Is Increasing

Per capita cost for five industries

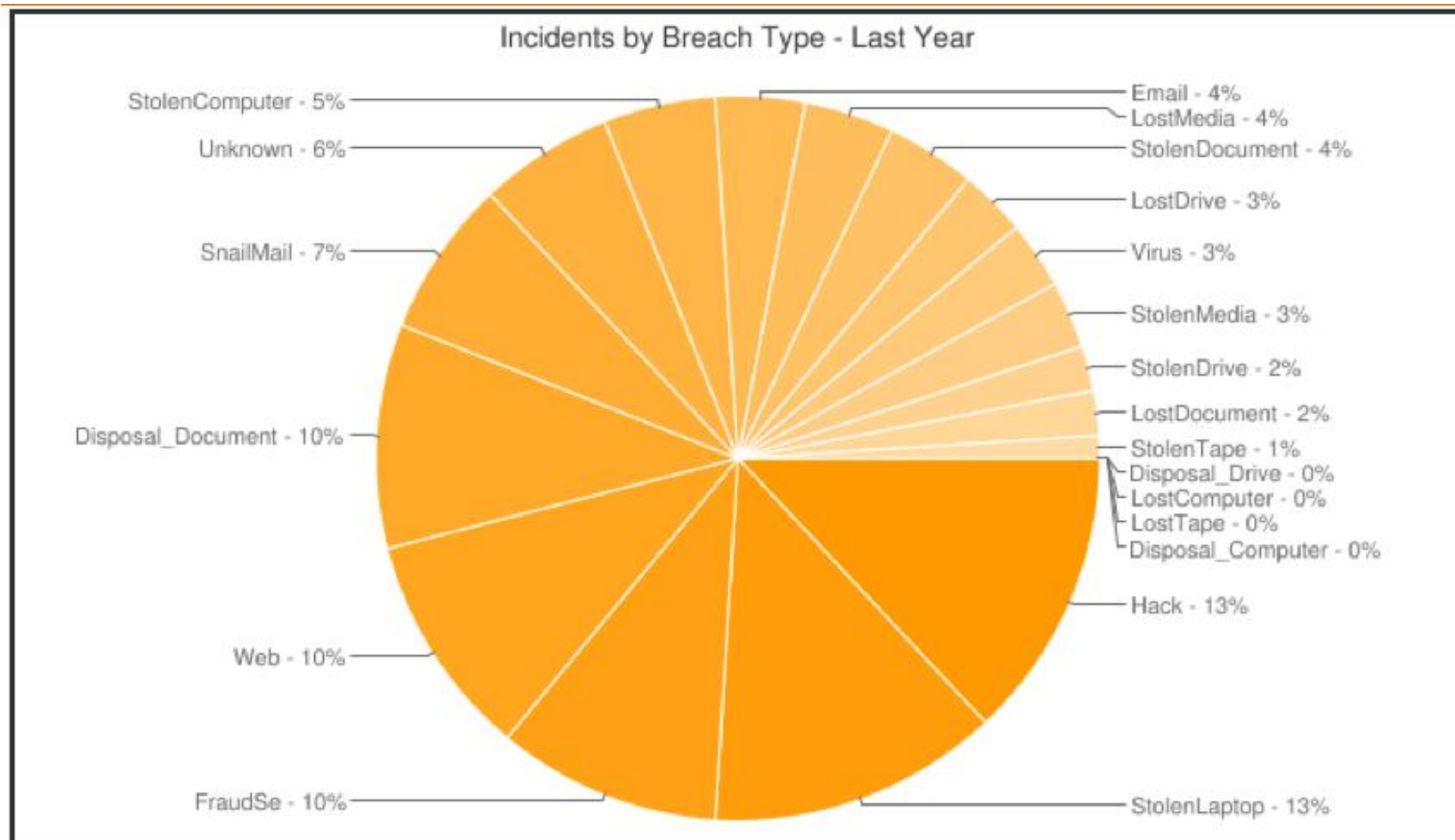
Converted into \$US dollars



Please note that these five industries are fully represented in all 2010 country studies.



Incident By Type - 2010



Staggering Statistic

Nearly 12 Million In U.S. Were Victims Of Identity Theft, Report Says

2010-12-16 - [Los Angeles Times](#)

...12 million people, about 5% of the U.S. population ages 16 and older, were victims of identity theft in a recent two-year period, the Department of Justice reported Thursday. The most common type of theft was the unauthorized use of an existing credit-card...

Via [DayLife](#)

This One Got Me...

Guidance Software Announces Breach

This is big news about a small breach. The self proclaimed "leader in computer forensics and incident response solutions" discovered a security breach on December 7th, 2005.

SecurityFocus **reported** today that financial information including CVV was lost:

The breach, which took place in November, resulted in the loss of customer names, credit-card numbers and the three-digit card verification values (CVVs), which merchants are not supposed to retain, according to reports.

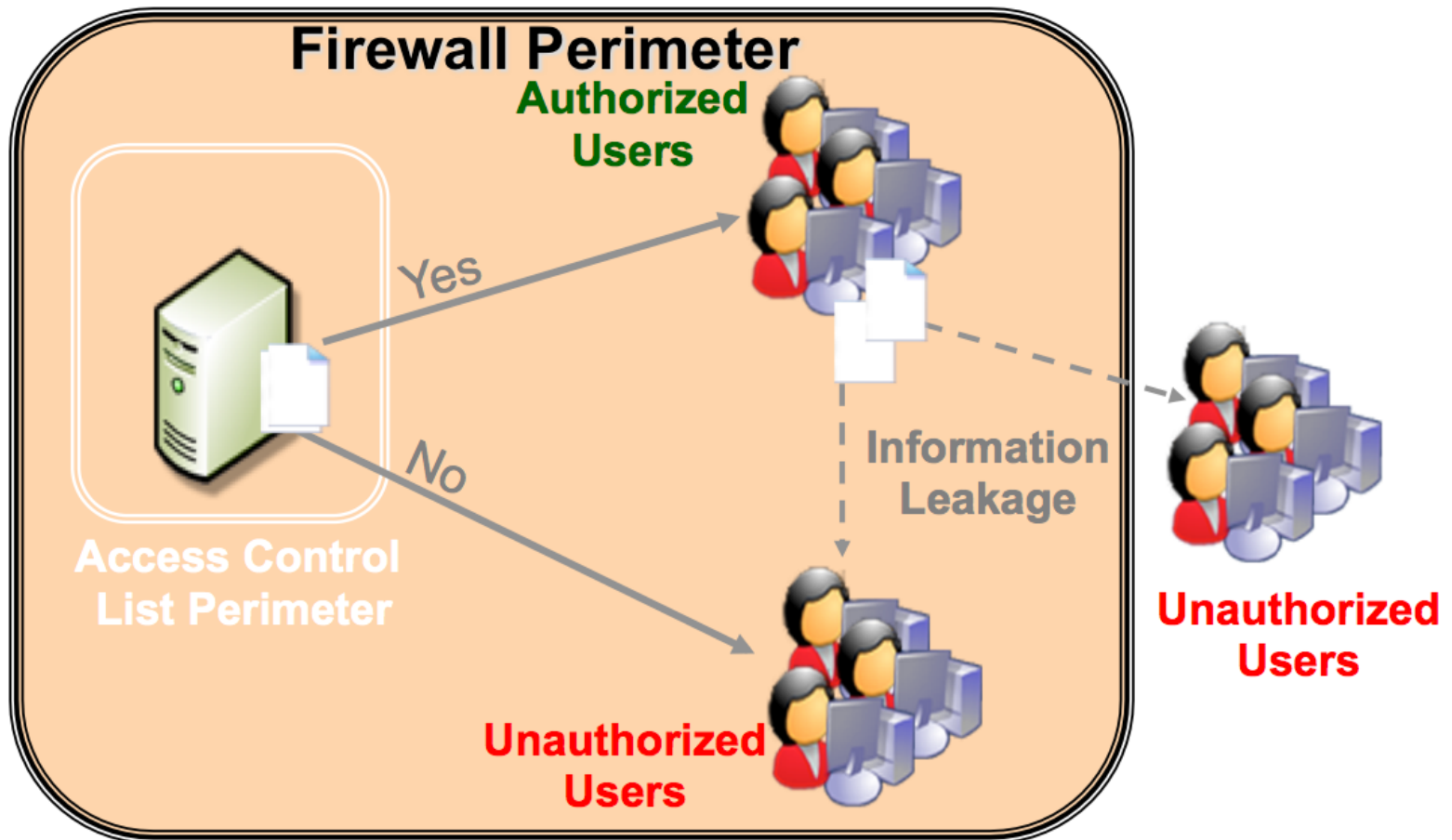
This is also reported on [news.com.com](#) (strange domain name, eh?):

The attack occurred in November, but wasn't discovered until Dec. 7, John Colbert, chief executive officer of Guidance, said in an interview Monday. The attack exposed data on thousands of the company's customers, including 3,800 whose names, addresses and credit card details were exposed, he said.

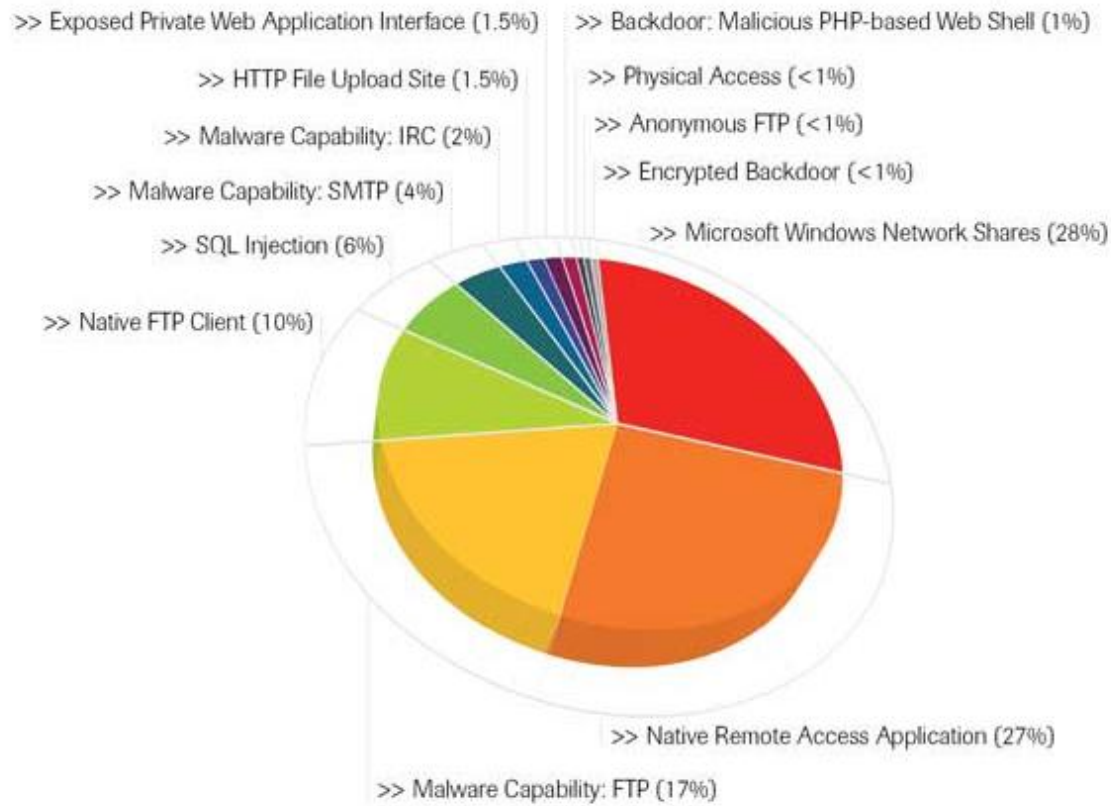
However, the official Guidance letter clearly states in the first paragraph "**Fortunately, the database that was compromised did not contain any of your financial information that could put you at risk of identity theft.**"

Of course most of the people (computer forensics and incident response professionals) who recieved this letter must have immediately suspected something was fishy. After all, why would Guidance send out the notice if there was no breach of sensitive data? And then there were those who are already **reporting** that they are victims of the breach...

Defining The Problem...



Where Are Your Data Leakage Sources?



Revisiting USB Device - Our Achilles Heal



USB Solution - Start With A Policy

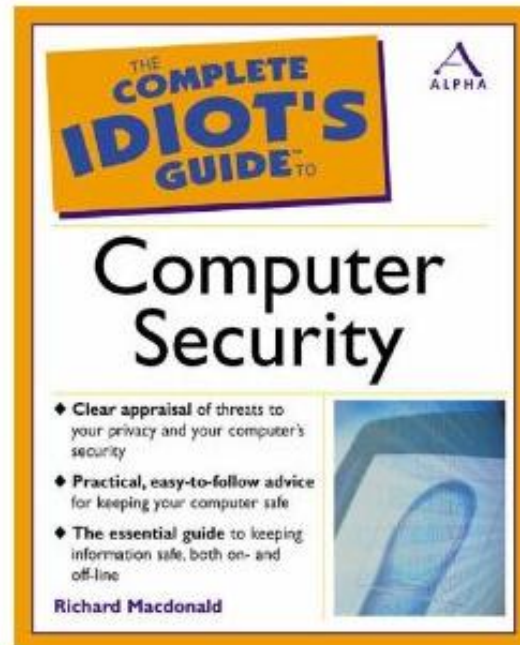
- + **Establish an Acceptable Use Policy concerning the use of USB devices within their networks for employees, vendors, contractors, and visitors.**
 - Should cover all USB devices
 - Mandate that all users who require USB devices obtain some form of authorization prior to using a device within the network
 - Policy should establish audit requirements (used to identify unauthorized USB devices)
 - Guidelines should be established to govern removal of these devices from the premises.
 - To counter the potential of loss of sensitive information, the policy should dictate a minimum level of encryption to protect the data.
 - All USB flash drives should be required to contain a file with contact phone number and Mailing Address to use if the device is found. A legal disclaimer should be included that indicates “information on the drive is company proprietary or confidential and protected by law”

USB Solution - Start With A Policy

- All removable drives should be scanned for viruses when used with a corporate computer
- When no longer needed, the removable drive should be “wiped” using an approved application
- User awareness programs should include an overview about the risks associated with USB storage media.
- Physical security personnel should receive training about the potential threat to the organization that unrestricted use of USB storage devices represents. They should also be taught how to recognize them.
- IT personnel should receive training about effective measures to control the use of this technology.

Enforce Policies With Technology

+ But wait a minute.... I can do this myself...



Do It Yourself - Prevention Approach 1

Restrict access to all USB devices through BIOS settings

- + Drawback - would prevent the use of USB keyboards, mice, printers, etc
- + Would require using a BIOS password to prevent users from changing the setting

Do It Yourself - Prevention Approach 2

Manually set registry key prevent users from formatting and ejecting of USB devices

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\AllocateDASD

+ Data type	Range	Default value
REG_SZ	0 1 2	0

Description

+ Determines which users can format and eject removable hard disks.

+ Value Meaning

- + 0 Only administrators of the computer
- + 1 Only administrators and power users
- + 2 Only administrators and the local current user

Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall your operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk

Do It Yourself - Prevention Approach 3

- + Prevent the user from installing the Windows built-in driver
 1. Remove all installed USB drives
 2. Uninstall the USB Mass Storage driver
 3. Deny all access to the driver usbstor.sys for each user individually
 - + or in a group (such as DenyUSBAccess)
 4. Set the same security permissions on the files usbstor.inf & usbstor.pnf
 - + Located in the \winnt\inf or \windows\inf directory.
 5. Remove the Administrator Group, Power User Groups and
 - + System Account from the security permission

Do It Yourself - Prevention Approach 5

- + Deny all access to the registry key *HKLM\SYSTEM\Microsoft\CurrentControlSet\Enum\Usbstor* for each user individually or in a group (such as DenyUSBAccess)
- + Remove the Administrators, Power Users, & Users groups and the System Account
 - + To all authorized users to install the devices on systems you can add the users individually or create a group (AllowUSBAccess) then set the permissions of this group to allow access.

Do It Yourself - Prevention Approach 6

+ MOVE THE DRIVER.CAB FILE

- + This approach requires moving the Driver.cab file found in the Winnt\Driver Cache\i386 directory to a location that users can't access. Using the administrator profile logon and logoff policy, you can copy and delete this directory to make sure it's available when you install new devices or deploy OS updates.
- + Moving the Driver.cab file is a network-centric approach that leaves the system state ready, and it puts the file in a location that's accessible only to the people with the authority to install new system devices.
 - + Affects all devices, not just USB Storage Devices

Or.... Invest In Technology

- + Who can write what and where
 - + All removable media
 - + USB control
 - + CD/DVD
 - + Firewire
- + Enforced encryption
 - + Nothing written to removable media without encryption
 - + Can only be read on authorized device with proper certificate
- + Enterprise scalable...

5 Simplified Steps In DLP

1. Automated Data Classification (...on going)
2. Asset Discovery
3. Protecting the Asset
 - a. Preventive Controls
 - b. Detective Controls
 - c. Corrective Controls
4. Implementation Strategies
 - a. Deployment
 - b. Process
 - c. Ongoing Operations
5. Audit trail of all access activity in real time
 - a. Anomalous behavior alerts

Know Required Areas of Protection

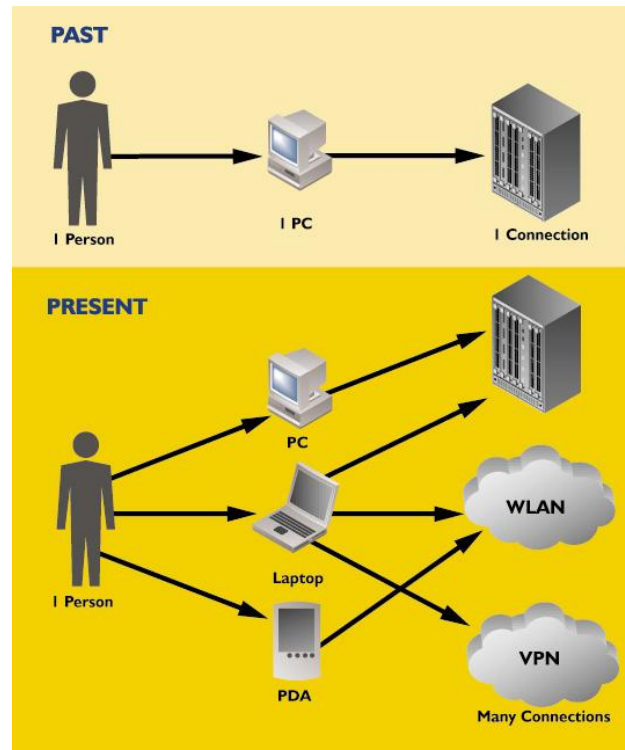
Data Loss Channels	Areas of protection		
	Corporate Network	Public Internet	Disconnected
Email	✓	✓	✓
IM	✓	✓	✓
HTTP	✓	✓	✓
Copy and Paste	✓	✓	✓
Local/Screen capture	✓	✓	✓
External (USB)	✓	✓	✓
Web Mail	✓	✓	✓
Agent-less Devices	✓		
Mobile Phone	✓		

2011 Is Looking Good For DLP

- + Data Classification has been fully automated
- + Active Detection is no longer vaporware
- + All Removable Media can now be centrally managed
 - + Including off line media/devices
- + Thin Client (like) technology is a Game Changer for DLP

A Few Closing Thoughts...

- + Complexity of our network environment is increasing



The “iProblem”....

- + “A survey revealed that while 65 % of IT decision makers recognized that unauthorized users could access valuable company data through the iPhone, 64 % said they had not taken any steps to secure company data against this threat.” <http://www.net-security.org/secworld.php?id=7749>



Virtualization Brings Additional Risks

- + All data in a vMotion is in the clear
 - + What ever was in memory can potentially be exposed
- + All data written to storage is in the clear
 - + Fiber Channel
 - + iSCSI
 - + NAS/SAN



When You Thought You Had Seen It All...



Almost there.....

I can't leave without sharing the
latest additions to my
Hacked Road Sign Collection..

A Few Hacked Road Signs



A Few Hacked Road Signs



A Few Hacked Road Signs



A Few Hacked Road Signs



A Few Hacked Road Signs



A Few Hacked Road Signs



A Few Hacked Road Signs



Questions?

Thanks for coming!

Contact:

paul.henry@bsius.com

phenry@sans.org