Leveraging Policies for Data Loss Prevention

Tobie Marais
Senior Technical Consultant

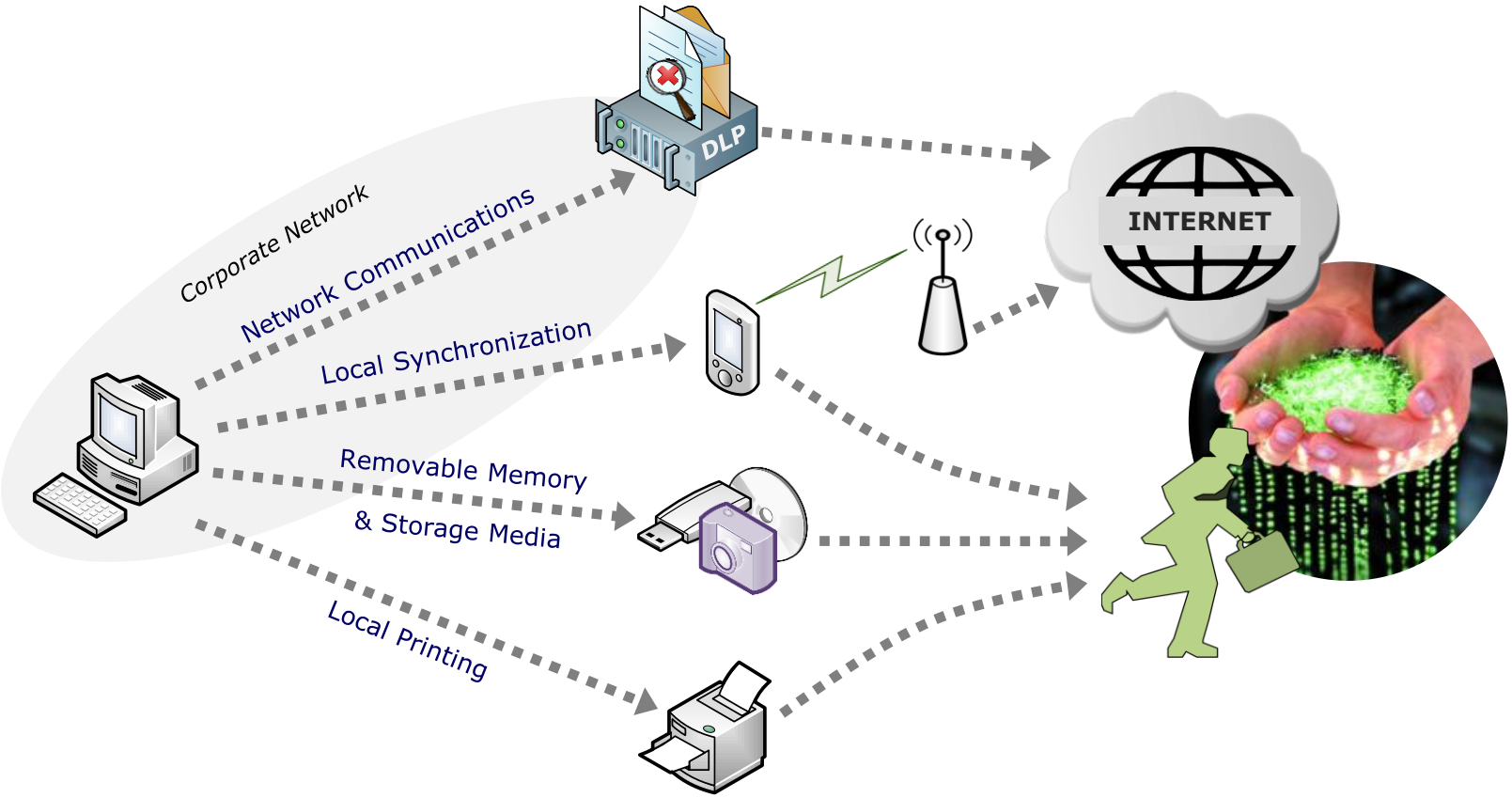
26 July 2011

chillisoft

Data Leakage – sounds familiar?

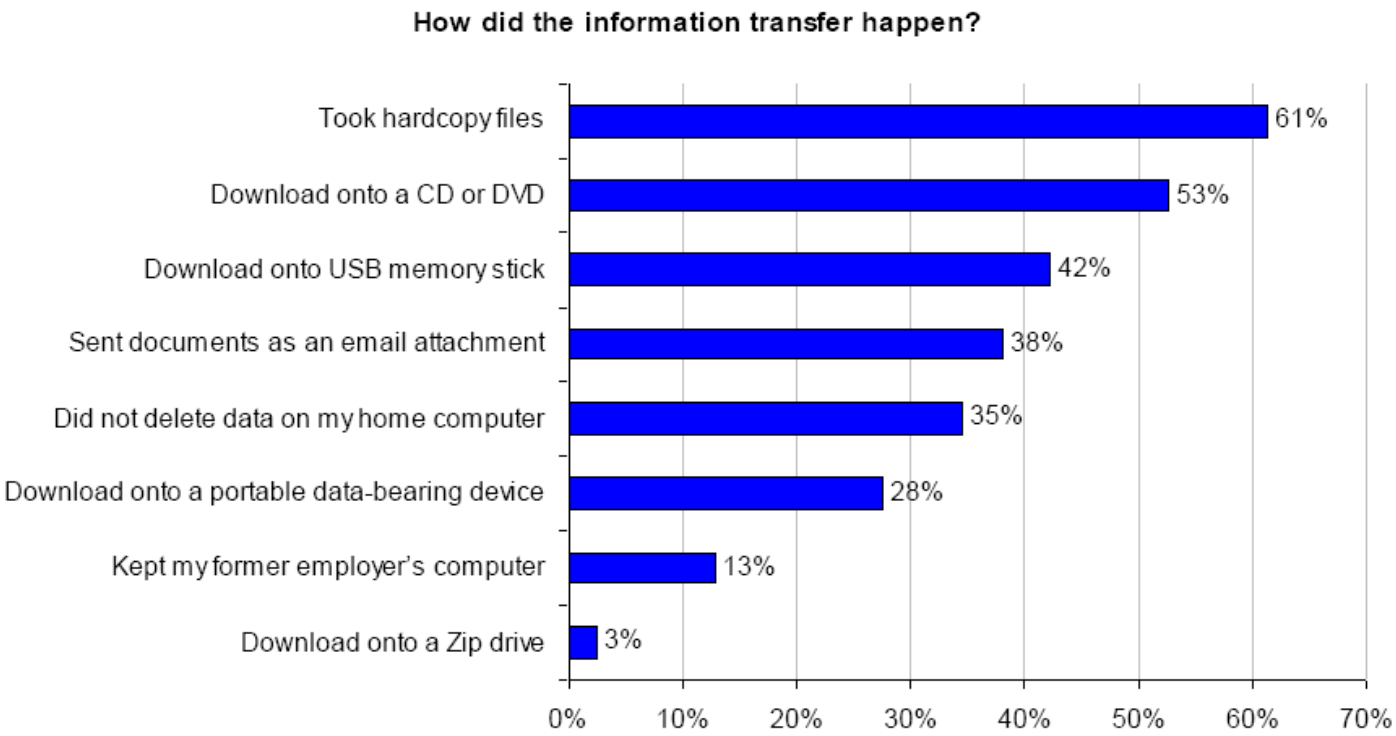
- **Unauthorized transmission of data**
  - Internally to external destination or recipient
- **Unintentional or malicious intent**

Endpoint Data Leak "Mechanics"



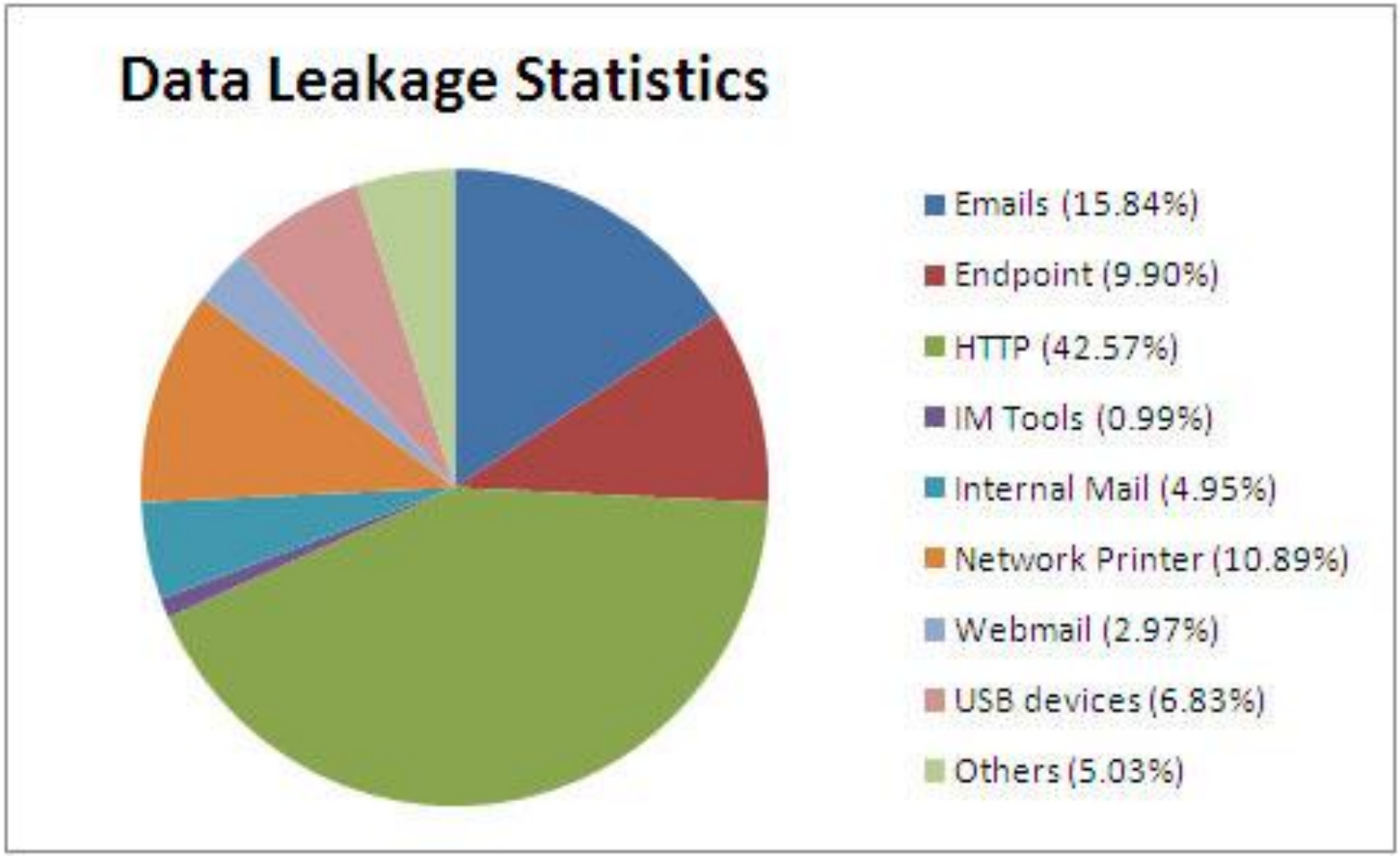
LOCAL LEAKS PREVAIL

Employees leaving an organisation most commonly steal corporate data by using local ports and devices attached to endpoint computers. This way far outweighs other methods.



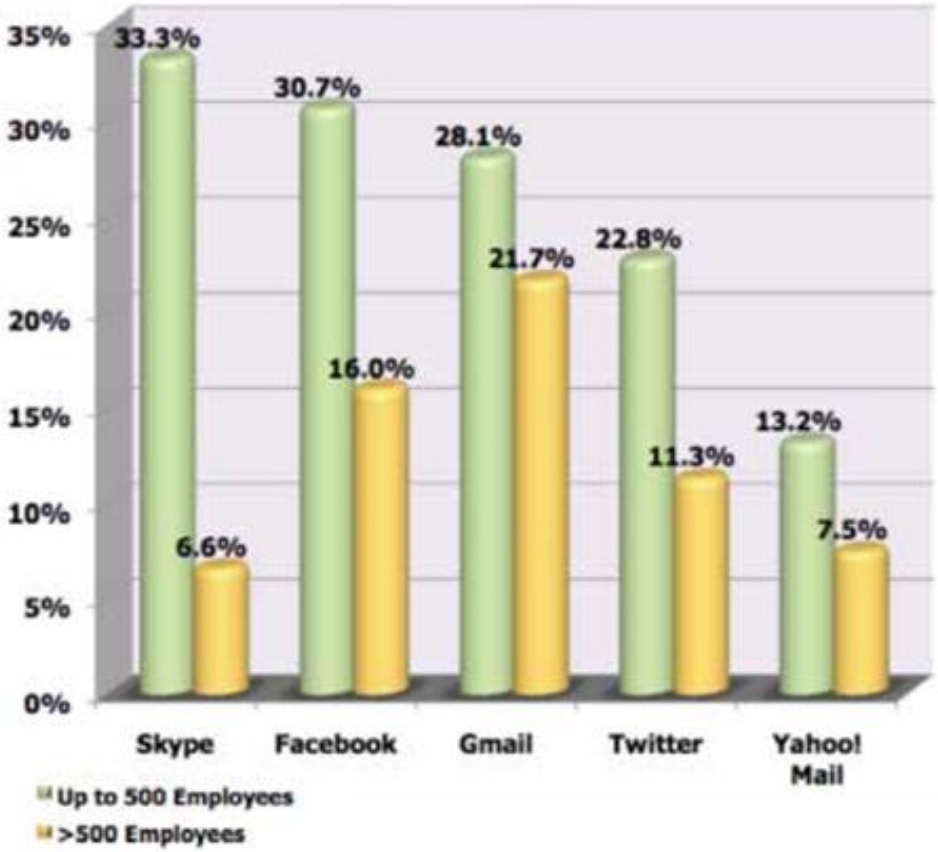
Source: "Data Loss Risks During Downsizing", Ponemon Institute, February 2009

General Data Leak Vectors



USE OF VARIOUS WEB 2.0 TOOLS

- In April 2010, 110 billion minutes were spent on blogs and social networking pages
- In April 2010, Blog and Social media sites attracted 24% more visitors than a year earlier
- There are currently 190m Twitter users, 519m Facebook, 65m LinkedIn and 115m on Friendster



Source: The Benefits and Risks of Web 2.0', Osterman Research, 2010

What about External Threats?

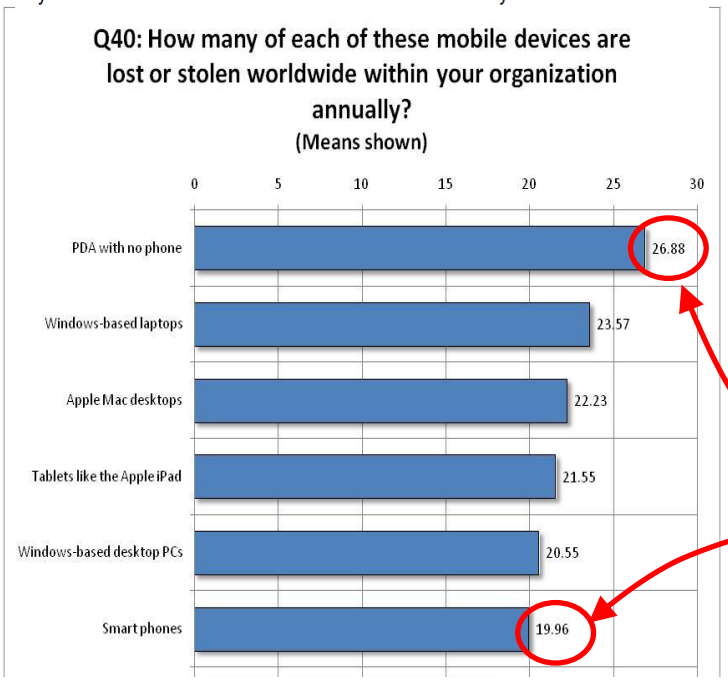
- **Phishing attacks**
  - Acquire sensitive information

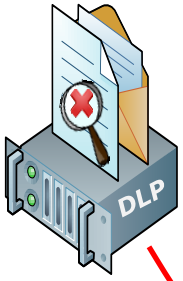
- **Social Engineering**
  - Trick or manipulate people
  - Sensitive information gathering
  - Attacker never comes face-to-face

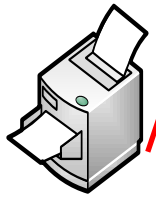
- **Physical Theft**

ARE ALL DATA CHANNELS REALLY DANGEROUS?

Symantec 2010 SMB Information Protection Survey - Global: June 2010







P2P networks a treasure trove of leaked health care data, study finds

Eight months after passage of HITECH Act, data leaks still a problem in health care industry

Jaikumar Vijayan

May 17, 2010 (Computerworld)

Nearly eight months after new rules were enacted requiring stronger protection of health care information, organizations are still leaking such data on file-sharing networks, a study by Dartmouth College's Tuck School of Business has found.

In a research paper to be presented at an IEEE security symposium Tuesday, a Dartmouth College professor Eric Johnson will describe how university researchers discovered thousands of documents containing sensitive patient information on popular peer-to-peer (P2P) networks.

One of the more than 3,000 files discovered by the researchers was a spreadsheet containing insurance details, personally identifying information, physician names and diagnosis codes on more than 28,000 individuals. Another document contained similar data on more than 7,000 individuals. Many of the documents contained sensitive patient communications, treatment data, medical diagnoses and psychiatric evaluations. At least five files contained enough information to be classified as a major breach under current health-care breach notification rules.

Who Is Pvt. Bradley Manning?

Suspicions Mount That He's Behind the Leak of Classified Reports on Afghanistan War

BY DAVID MUIR AND JESSICA HOPPER
July 26, 2010

abc NEWS

In his Army dress greens, Pvt. Bradley Manning looks like most of his fellow soldiers; but beneath the uniform, many suspect, is a man who may be responsible for the leaking of over 90,000 secret military reports to the whistleblower website WikiLeaks.

Manning was stationed at a base 40 miles east of Baghdad, at Forward Operating Base Hammer. Manning, who enlisted in the Army in 2007, was working as an Army intelligence analyst, pouring through classified information. What he saw with his clearance level, it is believed, left him disillusioned with U.S. foreign policy.

The twenty-two year old Manning went online

Home > Forms, Laws & Publications > Laws > Privacy > **ADHC Security Breach**

DHCS Reports Security Incident Involving ADHC Mailing

The California Department of Health Care Services (DHCS) reported on February 8, 2010, that a mailing sent to 49,352 Adult Day Health Care (ADHC) services inadvertently included their Social Security Numbers (SSN).

The incident occurred on February 1, when DHCS sent a notice to ADHC beneficiaries, entitled, "Notice of Change in Medical Necessity and Eligibility Criteria for Authorization of ADHC Services." In preparing and formatting a mailing list, beneficiaries' SSNs were mistakenly included. The SSNs did not have spaces or dashes so they may have appeared to be a random nine-digit number to people other than the recipients. On February 4, DHCS was notified of the error and took swift action to notify beneficiaries. In addition, DHCS further strengthened its procedures to protect the privacy of beneficiaries.

Headline NEWS

DATA LEAKS THAT MADE THE HEADLINES…

Sony shares slide as worries mount over data leak

Recommend 36 people recommend this.

TOKYO | Wed Apr 27, 2011 9:40pm EDT

(Reuters) - Shares of Sony Corp (6758.T) extended losses to trade down as much as 5.2 percent, hitting a one-month low on Thursday as investors worried over the widening impact of a massive leak of personal information of users of its PlayStation network.

Sony said on Tuesday that hackers had breached the network a week earlier, compromising confidential information including the names, addresses and possibly credit card data of 77 million users.

Experts say Sony could face legal action across the globe due to the incident.

The stock is now down more than 8 percent this week with investors nervous about the fall out of the data leak episode that plagued the company.

There is concern that loyal PlayStation gamers could ditch Sony in the wake of the data theft. The theft could cost the company more than $1.5 billion, or an average of $20 for each of the 77 million customers whose

Tweet 23

Share 10

Share this

+1 0

Email

Print

Related News

Sony gamers threaten to leave after hack
Wed, Apr 27 2011

Apple denies tracking iPhone customers
Wed, Apr 27 2011

Sony may face global legal scrutiny over breach
Wed, Apr 27 2011

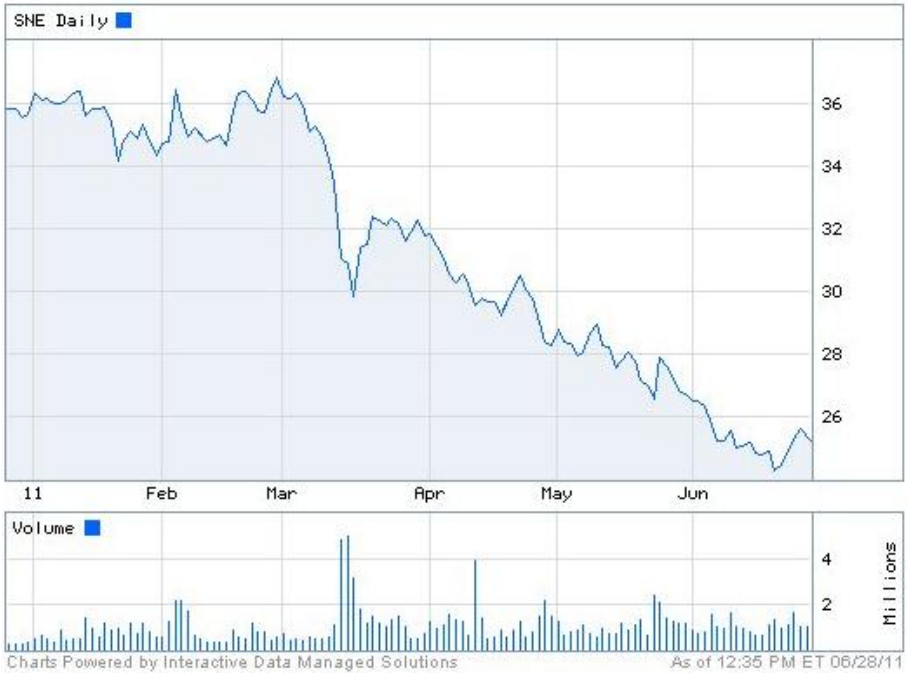
Furor at Sony after hackers steal

Sony – The Happy Days…

Sony (SNE) Stock On NYSE At Highest Levels Since September 2008 – WOW!!!

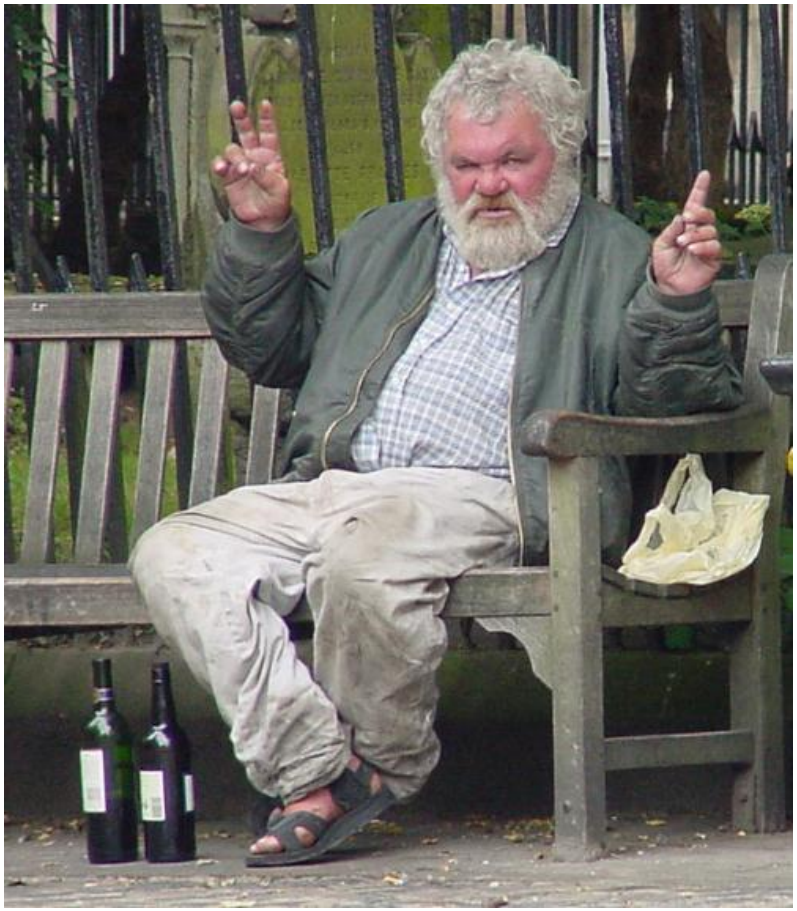
Happy IT Manager

SONY AFTER THE LEAK…WHAT !!!???



Current Sony (SNE) Stock On NYSE

Not so happy IT Manager



Headline NEWS

DATA LEAKS THAT MADE THE HEADLINES…

Sony shares slide as worries mount over data

State of Texas exposes data on 3.5 mil people

Epsilon … megaleak h … to spamme … tigating

Number of records leaked	Country	Brief description
76 min	USA	In National Archives and Records Administration (NARA), a hard drive storing part of a database of 76 million veterans' personal information had been sent back to a contractor for repair without having its information wiped
62 min	UK	Nine employees of Department for Work and Pensions (DWP) attempted non-authorized access to the department database with personal data of 62 million citizens – the total majority of UK population – including 12 million minors
32.6 min	USA	More than 32 min personal accounts were compromised (via SQL Injection) as a result of a hacking attack upon RockYou.com, a website offering services to such social networks as Facebook and MySpace
7.5 min	Germany	A vulnerability was found in the social network StayFriends GmbH (www.stayfriends.de), which allowed unauthorized access to personal data of all network members
6 min	UK	A range of companies (including Castrol) based their ad campaigns on personal data of car owners illegally obtained from the governmental car database
2.5 min	UK	Malicious users gained access to the database of National Health Service (NHS) with personal data of all patients
1.5 min	Japan	An unauthorized employee retrieved personal data of company clients from the corporate database and sold some of them
807 th.	USA	Archive tapes were lost that contained 12 years of personal data on police suspects, including social security numbers

Pentagon hit by massive cyber attack

7:18 AM Friday Jul 15, 2011

Share Tweet 0 Email Print

The Pentagon has revealed that in the spring it suffered one of its largest losses ever of sensitive data in a cyberattack by a foreign government.

It is a dramatic example of why the military is pursuing a new strategy emphasizing deeper defences of its computer networks, collaboration with private industry and new steps to stop "malicious insiders."

William Lynn, the Deputy Secretary of Defence, said in a speech outlining the strategy that 24,000 files containing Pentagon data were stolen from a defence industry computer network in a single intrusion in March.

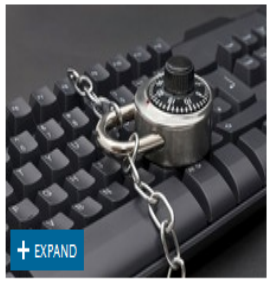


Photo / Thinkstock

FBI raided LulzSec hacking rampage suspect: report

Hackers claim US Senate breach

Related Tags

Technology

your news

- BP employee loses laptop containing data on 13,000 oil spill claimants
- Hard drive with private information of nearly 90,000 students missing
- British local council gets fined for mishandling of data

Closer to Home

WikiLeaks docs may embarrass NZ - Key

4 comments | Post Comment Email Print Text Size: aA aA aA

MON, 29 NOV 2010 6:17P.M.

By 3 News staff

Whistle-blowing website Wikileaks has published thousands more classified US documents.

Once again, they're both embarrassing and, in some cases, highly damaging.

The documents range from cables sent from the US Embassy in Wellington about New Zealand, to the revelation that the King of Saudi Arabia urged the US to bomb Iran's nuclear programme.

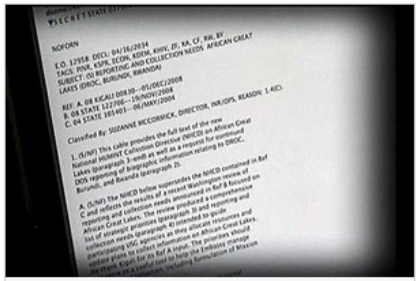
A list of the documents which will be available was released today, with at least 1610 documents tagged as relating to New Zealand. About 1400 of those came from the embassy in Wellington.

The earliest involving New Zealand is from the US embassy in Rome in October 1993 and also refers to Turkey. That is likely to be about New Zealand's new embassy in Turkey which opened that year.

In December 1997 a cable about New Zealand was likely to be about Jenny Shipley taking over the National Party leadership from Jim Bolger -- she became Prime Minister on December 8 that year.

The next cables date between 2004 and 2010.

Some cables refer to North Korea and likely are about a New



At least 1610 documents relate to New Zealand

VIEW VIDEO ▶ Facebook Twitter +1 0

Like Be the first of your friends to like this.

Data Leakage is Costly

Major Financial Impact

Costs of Data Breaches Are Rising

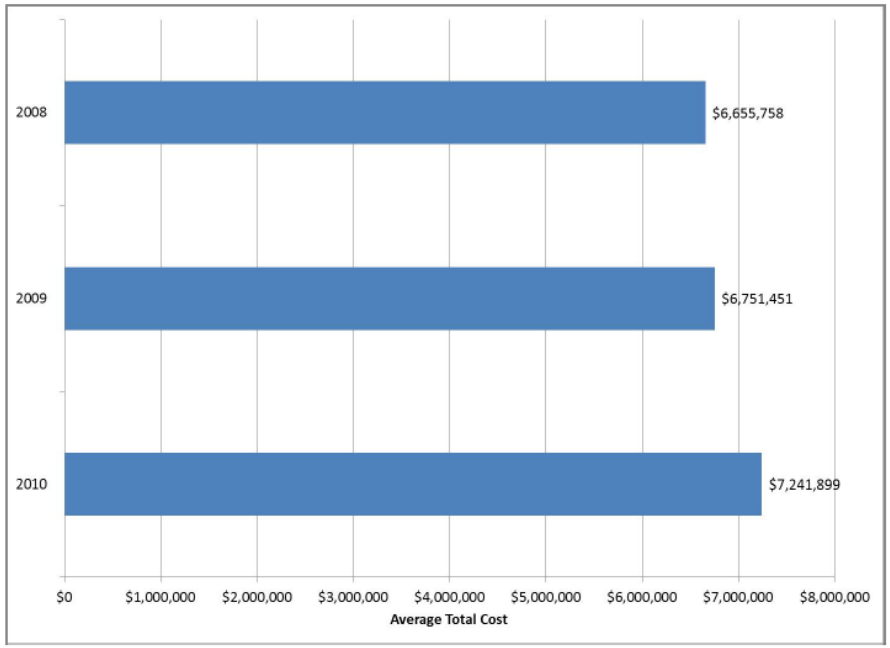


Figure 1: Average organizational cost of a data breach, 2008-10

Average total cost of a data breach for a U.S. organization has reached more than *$7.2M*

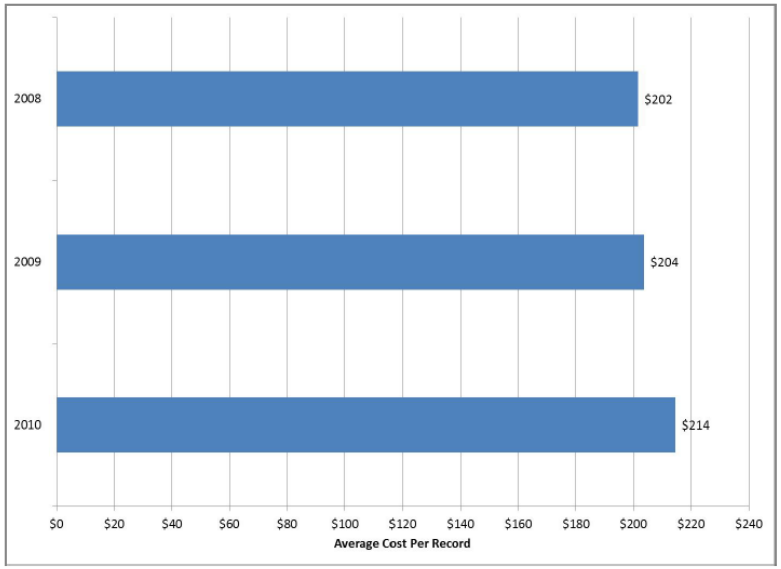


Figure 2: Average cost per record of a data breach, 2008-10

Average per-record cost of a data breach in the U.S. raised up to *$214*

Source: "2010 Annual Study: U.S. Cost of a Data Breach", Ponemon Institute, March 2011

Cost of a Data Breach – Global Statistics

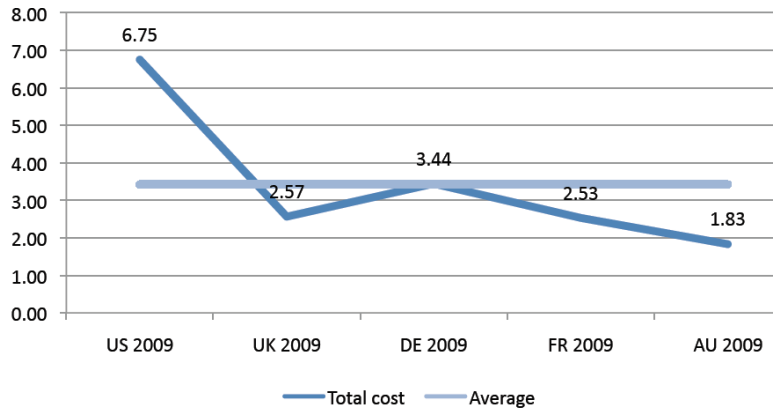


Figure 1: Average total cost of a data breach by country, 2009

On a global scale, the average total cost of a data breach is estimated as *$3.43M*

Global average per-record cost of a data breach is *$142*

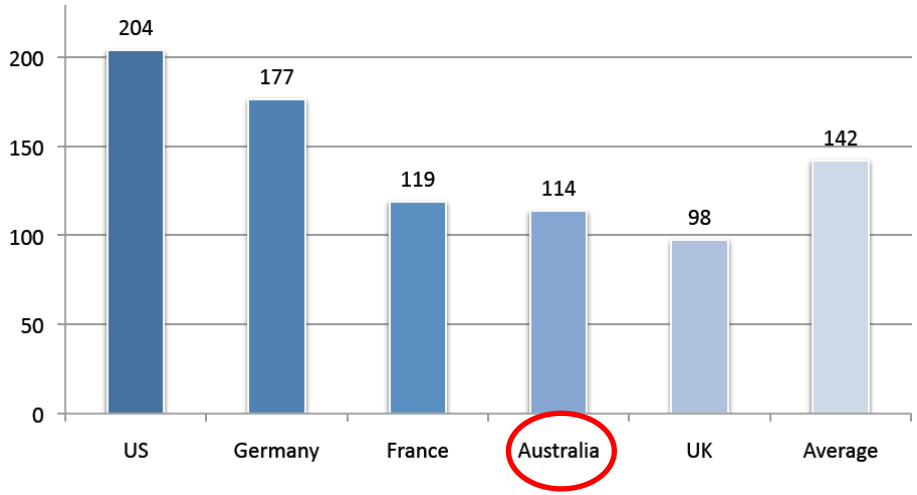


Figure 2: Average cost per record by country, 2009

Source: "2009 Annual Study: Global Cost of a Data Breach", Ponemon Institute, April 2010

Implications of Data Leakage

Major Financial Impact

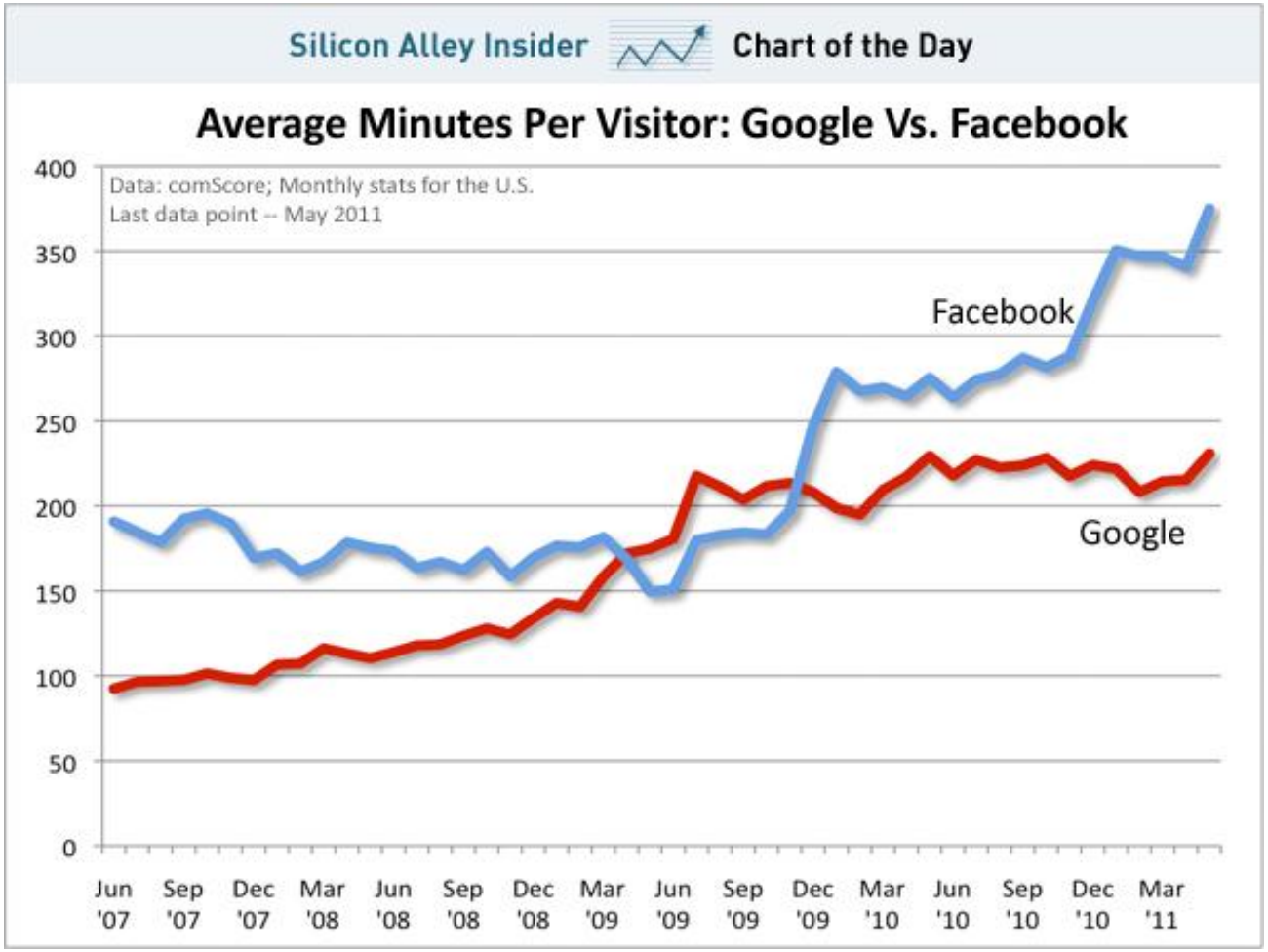
Business Reputation

Lost Productivity

SO, CAN YOU HAVE TOO MUCH SECURITY?

Not when it comes to your critical information!

FACEBOOK VS. GOOGLE

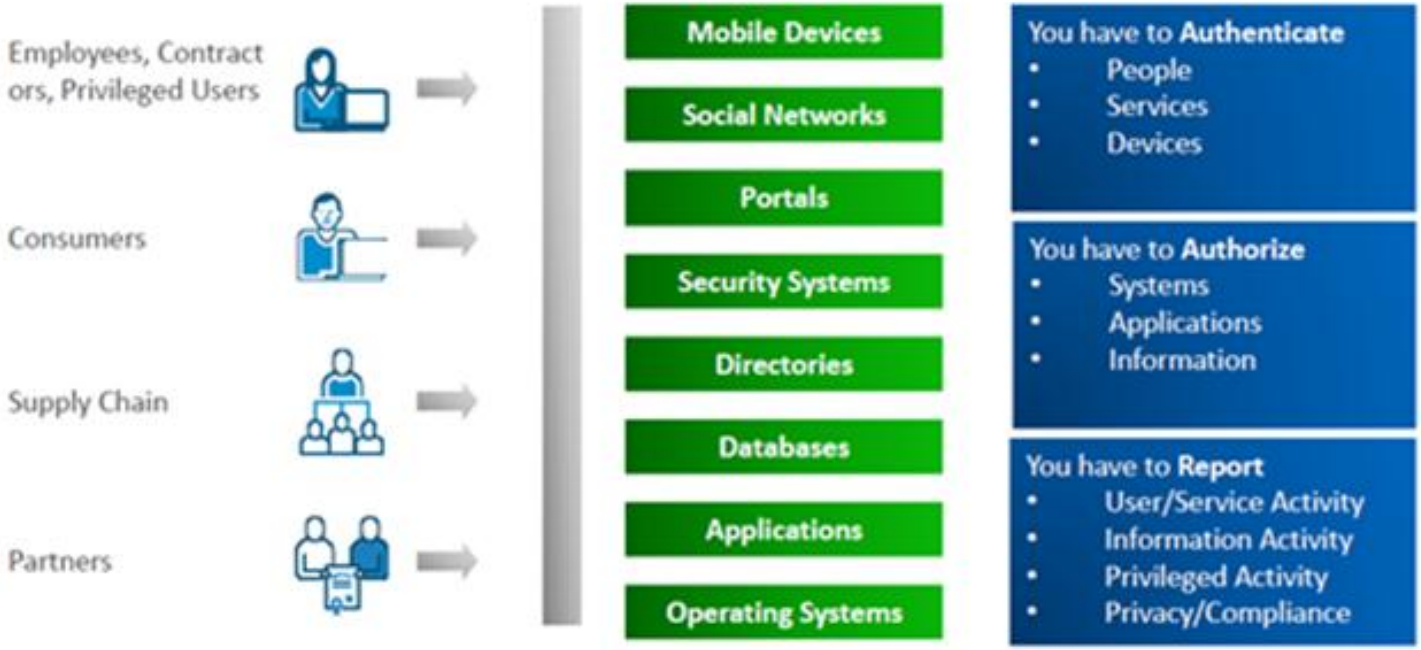


STATE OF CURRENT POLICY CONTROLS

Source: The Benefits and Risks of Web 2.0', Osterman Research, 2010

THE DYNAMIC CHALLENGE IN SECURITY

Ensure the right people have the right access to the right information at the right time



FACTS

- More than **6,000** USB flash drives left in pockets of clothes at drycleaners
- More than **12,500** devices such as laptops, iPads, iPhones and other storage devices found in taxi cabs

So what can we do?

- **Encryption**
  - Use encrypted USB flash drives
- **Indicate access hours**
- **Monitoring and enforcement**
  - Inform staff what's acceptable and not
  - Clearly state in policy
- **Disable outside software**
- **Get an internal data leakage prevention solution**
  - Control, Audit and Shadowing of transferred data
  - Content- Aware Rules and Device Whitelisting

So what can we do?

- **Disable USB and Firewire ports**
- **Restrict mail size and / or block all attachments**
- **Restrict the use of Social Networking Sites**
- **Define a tight policy on acceptable devices and their usage**
  - iPods, MP3 players, Bluetooth Devices, iPads etc.
- **Ensure that managers as well as users understand the security plans and policies**

CLOSING…

THANK YOU!

QUESTIONS?

Tobie Marais
Senior Technical Consultant

tobie.marais@chillisoft.net

For up-to-date data breaches
datalossdb.org

DATALOSS db
open security foundation

chillisoft