Singapore infocomm Technology Federation

SECURITY & GOVERNANCE CHAPTER

DATA LEAKAGE / LOSS PREVENTION

- summary & contentions

Anthony Lim

MBA CISSP CSSLP FCITIL

CSSLP Certified Secure Software Lifecycle Professional

* Advisor, Security & Governance

www.sitf.org.sg

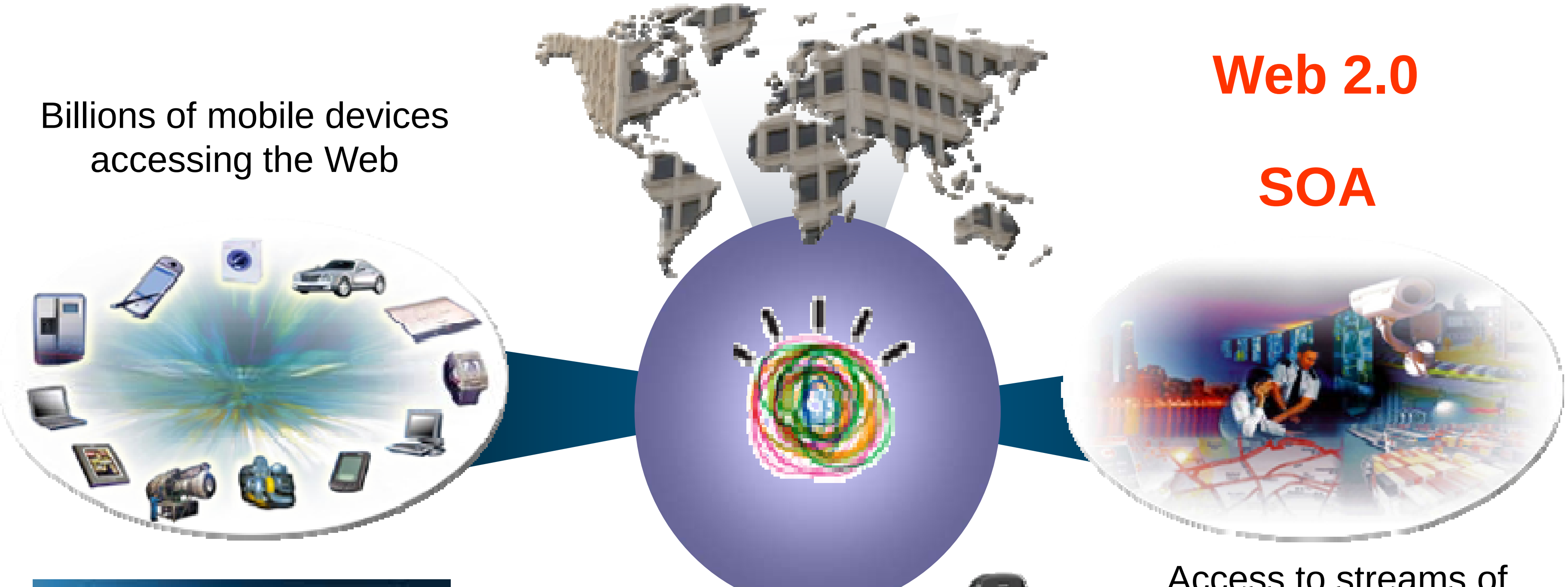
* Director Asia Pacific, Security, Rational Software, IBM

8/17/2009

MEDIABUZZ D.L.P. SOLUTION SEMINAR 13-8-09

Welcome to THE SMARTER PLANET

Globalization and Globally Available Resources



Billions of mobile devices accessing the Web

Web 2.0

SOA

Access to streams of information in the Real Time

New Forms of Collaboration

New **possibilities.**
New **complexities.**
New risks.

Regulation & Compliance SARBANES-OXLEY, HIPAA, BASEL II …

- It is part of doing business
- Business Continuity
- An environment of TRUST
  - □ For doing business
  - □ Ensure Orderliness in Internet world
  - □ Promote Economic growth

- More than just Confidentiality, Integrity and Availability
- **Privacy**

3rd Party Customer Data

SEND THE SALARY SPREADSHEET TO HUMAN RESOURCES.
scottadams@aol.com
www.dilbert.com
DON'T LET ANYONE ELSE SEE IT. THAT SORT OF INFORMATION COULD SOW THE SEEDS OF DISCONTENT.
9-11-04 © 2004 Scott Adams, Inc./Dist. by UFS, Inc.
WE'D HAVE MASSIVE DISLOYALTY, FIGHTS, VANDALISM, MAYBE EVEN RIOTS.

© UFS, Inc.

SUMMARY : DATA LEAKAGE / LOSS

- "New" "Term" ("Jargon") introduced out of post-Enron regulatory-compliance Sarbanes-Oxley, Basel II, HIPAA, ISO-27001 (17799) etc
  - technically, the issue and concept is not new at all
  - term "popularized" in 2006

- **So, what happened to the data? Where did it go?**
  - Original Security mantra of C.I.A. still applies –

    ➢ Confidentiality of the data – STOLEN?
    (a copy of it was taken but the original left intact)

    ➢ Integrity of the data – DAMAGED?
    (corrupted /modified)

    ➢ Availability (Accessibility) of the data – GONE?
    (destroyed /erased)

D.L.P. – per Wikipedia

- A computer security term referring to **systems that:**
  - **- identify, monitor, and protect**
    - ➢ **data in use (e.g., endpoint actions),**
    - ➢ **data in motion (e.g., network actions), and**
    - ➢ **data at rest (e.g., data storage)**

- through deep content inspection and with a centralized management framework.
- The systems are designed to detect and prevent the unauthorized use and transmission of confidential information.

- Also referred to by various vendors as
  - ☺ Data Leak Prevention
  - ☺ Information Leak Detection and Prevention (ILDP),
  - ☺ Information Leak Prevention (ILP),
  - ☺ Content Monitoring and Filtering (CMF)
  - ☺ Extrusion Prevention System by analogy to IPS

D.L.P – per Vendor “S”

Comprehensive coverage of confidential data across endpoint, network, and storage systems - whether the users are on or off the corporate network. By measurably reducing risk, … gives organizations new confidence to demonstrate compliance while protecting their customers, brand, and intellectual property.

Discover	- Discover where confidential data is stored.
Monitor	- Monitor how confidential data is being used.
Protect	- Protect and prevent confidential data loss.
Manage	- Manage and enforce unified data security policies.

D.L.P. – per Vendor “C”

- helps organizations assess risk and prevent data loss over the highest points of risk

- safeguards proprietary information against security threats due to enhanced employee mobility, new communication channels, and diverse services

  - ➢ In-motion data leakage protection against loss over the web and through email, with policies that include content, context, and destination knowledge

  - ➢ Services to understand data loss risk and develop data leakage protection strategies that incorporate people, processes, and technology

  - ➢ Protecting at-rest data by encrypting backup tapes and other storage devices

  - ➢ Providing data leakage protection from other avenues of risk, such as unauthorized physical or network access, malware, and end-user actions

D.L.P. – A *D.R.M.* APPROACH per (Singapore Vendor “S”)

“DIGITAL RIGHTS MANAGEMENT”

DISALLOW

- PRINT SCREEN
- SAVE TO SEPARATE FILE /LOCATION /FILE-TYPE
- CUT /COPY –PASTE
- Access via DOS format /flat-file / ASCII text /Frame …

- TIME BOMB (AUTO EXPIRY /SELF-DESTRUCT) OF GIVEN DOCUMENT /DATA . FILE

- PASSWORD PROTECT FILE-OPENING (so what’s new?)

-DOCUMENT CAN BE OPEN BY PRE-DESIGNATED 'GOOD' / LICENSED SOFTWARE ONLY THAT’S PRE-INSTALLED ON AUTHORIZED PC

- **DOESN’T MATTER IF DESIGNATED DATA IS ON PORTABLE DEVICE E.G. THUMBDRIVE**
- **IT CAN'T BE READ BY UNAUTHORISED PC**
- **SPECIAL AUTHENTICATION E.G. IF WRONG 3 TIMES, PKI TOKEN LOCKS /SELF-DESTRUCTS**
- **REMOTE WIPE CAPABILITY IN CASE OF LOSSOR MISPLACEMENT OF MOBILE DEVICE**

D.L.P. – Other thoughts and issues

- THUMBDRIVE (MP3 PLAYERS?, CAMERA / CELL PHONE RAM SD CARD?)
  - MANY PCS TODAY HAVE SDCARD/MAGICSTICK READER SLOTS BUT YOU CAN'T PRACTICALLY KILL THESE AND/OR USB DRIVE - FLASH STORAGE DEVICES

- THUMBDRIVE ENCRYPTION SOLUTIONS AVAILBLE AND FREE - EASY AND PORTABLE EG SECUREAGE, TREK. SANDISK, BUT NOBODY CARES

- NETWORK PRINTER?

- EMAIL OUT? ANTI-SPAM SCANNER SCANS OUTGOING EMAIL FOR APPROPRIATE LANGUAGE, WORDS AND ATTACHMENTS?

- EMAIL ACCESS USING NEW MOBILE 'SMARTPHONE' DEVICES

- SMARTCARD SDCARD CONTAINING SECURITY SOLUTIONS FOR MOBILE DEVICES (I.E. INSTEAD OF JUST FOR STORAGE)
- PKI /CA

- HARD DISK AND PORTABLE STORAGE DEVICE AUTHENTICATION AND ENCRYPTION E.G. POINTSEC - SO IF YOU LOSE YOUR PC, IPOD, PORT HARD DISK OR THUMBDRIVE OR SMARTPHONE, YOU DON'T HAVE TO FEAR THE DATA on it BEING COMPROMISED ...

- EMAIL ENCRYPTION AND AUTHENTICATION SOLUTIONS
  - e.g. if you send to wrong /unauthorized user no sweat because they can't read it
- CLOUD COMPUTING?!

-EAVESDROPPING, SESSION-HIJACKING, MAN-IN-THE-MIDDLE, ...

-keyboard logger and defense?

Phishing

- BLUETOOTH P.A.N. LOCAL DATA TRANSFER - bluejacking? accidental on-always bluetooth?

New D.L. issue - Software Imperfection

- Information Leakage and Improper Error Handling

- Unneeded (or restricted) information made available via application/code errors or other means.

- Implications?
  - □ Sensitive data exposed
  - □ Web App internals and logic exposed (source code, SQL syntax, exception call stacks, etc.)
  - □ Information aids in further hacks

SOMETHING ELSE IS OUT THERE ….

BBC NEWS

Watch One-Minute World News

Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
nce/Nature
Technology
tertainment
in the news

Last Updated: Tuesday, 21 August 2007, 10:01 GMT 11:01 UK

E-mail this to a friend   Printable version

Monster attack steals user data

US job website Monster.com has suffered an online attack with the personal data of hundreds of thousands of users stolen, says a security firm.

Monster is a leading online service

A computer program was used to access the employers' section of the website using stolen log-in credentials.

Symantec said the log-ins were used to harvest user names, e-mail addresses, home addresses and phone numbers, wh were uploaded to a remote web server.

$12k fine for accessing clients' data

A FORMER clerk who illegally accessed information on insurance policyholders was fined $12,000 on Monday.

Helen Foo Mei Hwa (right), 41, admitted to three charges of mining information on 156 policyholders from her workstation without clearance from The Asia Insurance Company, her then-employer in August 2005.

Two other similar charges were taken into consideration.

She passed on the details to an in-

ing its rule against misusing or divulging information. She is now a freelance insurance agent.

Her lawyer, Mr Suresh Damodara, said his client, who is separated and has two children, had not benefited from the offences. He added that the last three years had been traumatic for her, with the investigation hanging over her head.

She could have been fined up to $5,000 and/or jailed for up to two years on each charge.

THE STRAITS TIMES   THURSDAY MARCH 3, 200

Dating site's weakest link exposed

Security flaw on SDU website allows access to members' accounts and personal details

BY CHAN CHI-LOONG

OVER 30,000 members of the Social Development Unit (SDU) have been locked out of the matchmaker's website, after a computer security flaw was uncovered.

This flaw on SDU's website (lovebyte.org.sg), which has been up since 2001, allows members to access other members' accounts in addition to their own, and leaves their personal details open to exposure.

The member login portion of the site was taken down for maintenance on Tuesday night after The Straits Times alerted the Ministry of Community Development, Youth and Sports (MCYS), which oversees the SDU, to the problem.

If uncorrected, the flaw allows users to see other members' personal details like name, age, salary, telephone numbers and e-mail address.

The accounts are thus wide open to hacking and impersonation, but as of today, there has been no case reported.

An SDU spokesman said the "possible breach of security" was being investigated, and online ser-

PHOTO: WONG KWAI CHOW
CONCEPT: MIEL

SDU says sorr

WE ARE currently investigating a possibl of security at the SDU SDU's online services remain suspended unt notice.

In the meantime, S take all necessary step strengthen security at website and keep mem informed of the enhan procedure when servi resume. Members ma SDU if they have exp any problems with the so far.

We sincerely apolo the inconvenience cau this unfortunate incide will take all necessary prevent similar proble occurring in future.

Infocomm authority sa

ALL government web security measures in pl protect the integrity of information. The incid has happened is an isol says the Infocomm Development Authori Singapore.

MY PAPER TUESDAY MARCH 3, 2009

SINGAPORE   TUE MAR 03 09 MYPAPER

Glitch spills UBS clients' info

Wealthy customers saw details of others' online accounts, but bank says number affected is small

KENNY CHEE

A TECHNICAL glitch at Swiss bank UBS gave its wealthy customers in Singapore and Hong Kong a shock last week when they logged on to their online accounts.

The private-banking clients found confidential details of other clients' bank statements and account information instead of their own. Clients' online accounts, though, do not indicate their names.

Asked how many clients were affected, all she said was that "some limited account information concerning a small number of UBS wealth-management clients was accessible by a very limited number of other system users". She added that fewer than five accessed the information.

She told *my paper* the glitch occurred "as a result of an inadvertent technical error following an information-technology system upgrade over the weekend

ing to the incident and has implemented measures to prevent a similar occurrence in the future.

The bank also reported the incident to the banking authorities here and in Hong Kong: the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA).

Asked about what MAS would be doing, its spokesman said that "we are following up with the bank", but did not elaborate.

The HKMA said it is "following up with the bank on any impact... and the remedial measures that should be taken".

Its spokesman added: "We have requested the bank to sub-

Mr Tan Teik Guan, chief ecutive of Data Security Syste Solutions, said such acciden leaks of confidential inforn tion could lead to "embarrass situations for clients and repu tion risks for banks".

"Intentional leakages more serious as the dat (could be) used for more ma cious activities," he said.

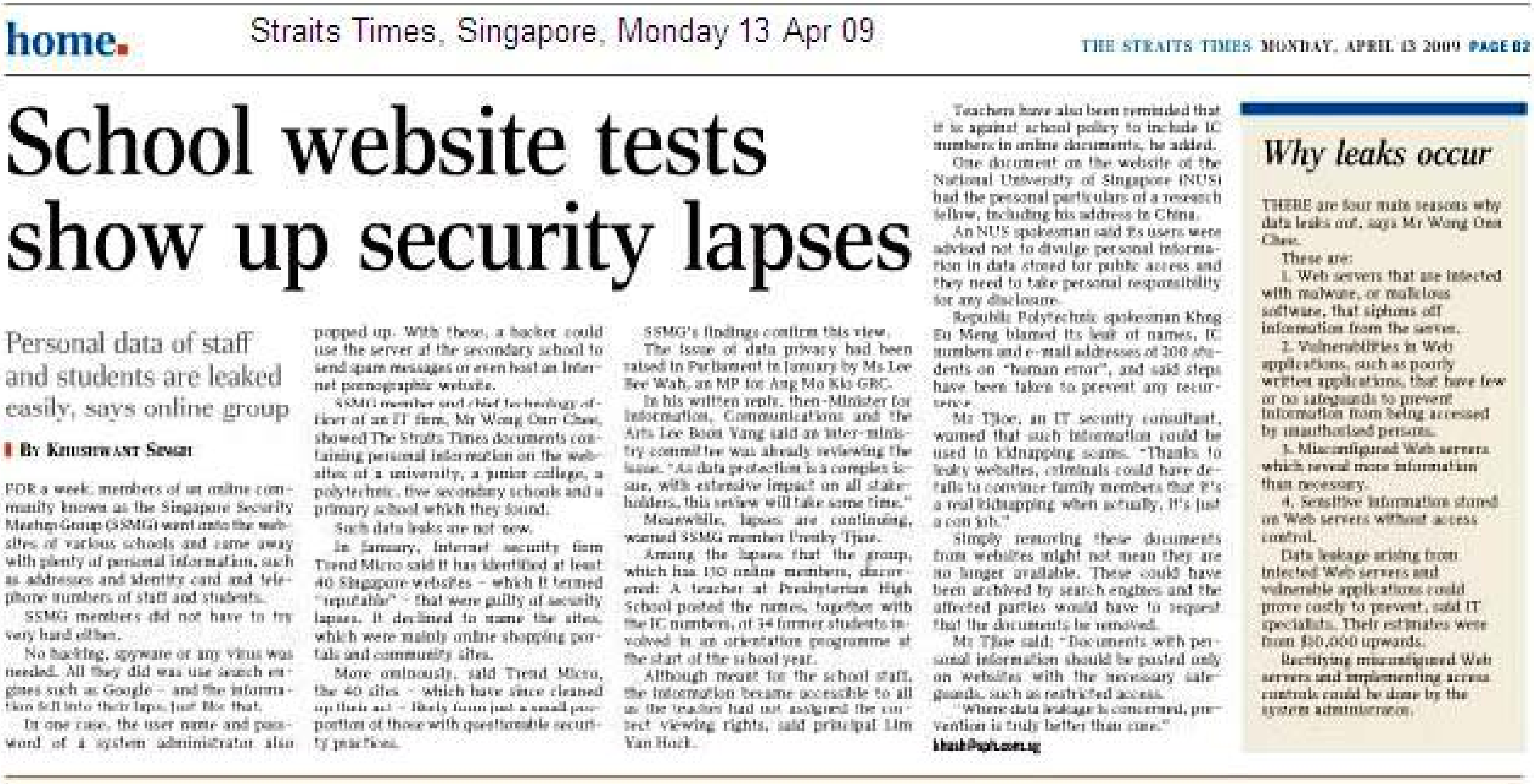
kennyc@sph.com.sg

HELPDESK 我的字典

Glitch: 小故障
xiǎo gù zhàng

Confidential:

Straits Times, Singapore, Monday 13 Apr 09



home.

THE STRAITS TIMES MONDAY, APRIL 13 2009 PAGE 02

School website tests show up security lapses

Personal data of staff and students are leaked easily, says online group

By Khushwant Singh

FOR a week, members of an online community known as the Singapore Security Meetup Group (SSMG) went onto the websites of various schools and came away with plenty of personal information, such as addresses and identity card and telephone numbers of staff and students.

SSMG members did not have to try very hard either.

No hacking, spyware or any virus was needed. All they did was use search engines such as Google – and the information fell into their laps, just like that.

In one case, the user name and password of a system administrator also popped up. With these, a hacker could use the server at the secondary school to send spam messages or even host an Internet pornographic website.

SSMG member and chief technology officer of an IT firm, Mr Wong Onn Chee, showed The Straits Times documents containing personal information on the websites of a university, a junior college, a polytechnic, five secondary schools and a primary school which they found.

Such data leaks are not new.

In January, Internet security firm Trend Micro said it has identified at least 40 Singapore websites – which it termed "reputable" – that were guilty of security lapses. It declined to name the sites, which were mainly online shopping portals and community sites.

More ominously, said Trend Micro, the 40 sites – which have since cleaned up their act – likely form just a small proportion of those with questionable security practices.

SSMG's findings confirm this view.

The issue of data privacy had been raised in Parliament in January by Ms Lee Bee Wah, an MP for Ang Mo Kio GRC.

In his written reply, then-Minister for Information, Communications and the Arts Lee Boon Yang said an inter-ministry committee was already reviewing the issue. "As data protection is a complex issue, with extensive impact on all stakeholders, this review will take some time."

Meanwhile, lapses are continuing, warned SSMG member Franky Tjioe.

Among the lapses that the group, which has 130 online members, discovered: A teacher at Presbyterian High School posted the names, together with the IC numbers, of 34 former students involved in an orientation programme at the start of the school year.

Although meant for the school staff, the information became accessible to all as the teacher had not assigned the correct viewing rights, said principal Lim Yan Hock.

Teachers have also been reminded that it is against school policy to include IC numbers in online documents, he added.

One document on the website of the National University of Singapore (NUS) had the personal particulars of a research fellow, including his address in China.

An NUS spokesman said its users were advised not to divulge personal information in data stored for public access and they need to take personal responsibility for any disclosure.

Republic Polytechnic spokesman Khng Eu Meng blamed its leak of names, IC numbers and e-mail addresses of 300 students on "human error", and said steps have been taken to prevent any recurrence.

Mr Tjioe, an IT security consultant, warned that such information could be used in kidnapping scams. "Thanks to leaky websites, criminals could have details to convince family members that it's a real kidnapping when actually, it's just a con job."

Simply removing these documents from websites might not mean they are no longer available. These could have been archived by search engines and the affected parties would have to request that the documents be removed.

Mr Tjioe said: "Documents with personal information should be posted only on websites with the necessary safeguards, such as restricted access.

"Where data leakage is concerned, prevention is truly better than cure."

khush@sph.com.sg

Why leaks occur

THERE are four main reasons why data leaks out, says Mr Wong Onn Chee.

These are:

1. Web servers that are infected with malware, or malicious software, that siphons off information from the server.

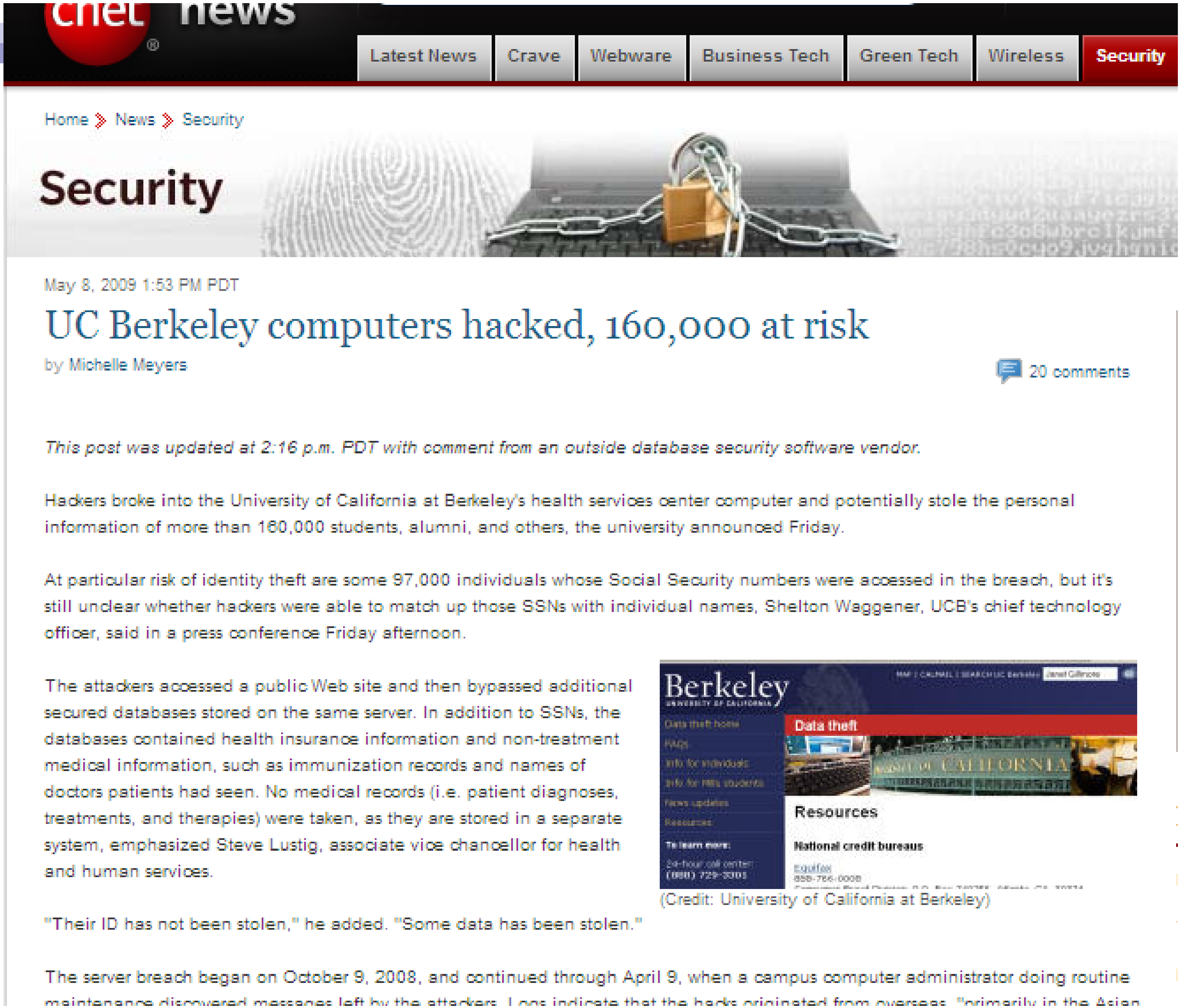
2. Vulnerabilities in Web applications, such as poorly written applications, that have few or no safeguards to prevent information from being accessed by unauthorised persons.

3. Misconfigured Web servers which reveal more information than necessary.

4. Sensitive information stored on Web servers without access control.

Data leakage arising from infected Web servers and vulnerable applications could prove costly to prevent, said IT specialists. Their estimates were from $80,000 upwards.

Rectifying misconfigured Web servers and implementing access controls could be done by the system administrator.



May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

This post was updated at 2:16 p.m. PDT with comment from an outside database security software vendor.

Hackers broke into the University of California at Berkeley's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced Friday.

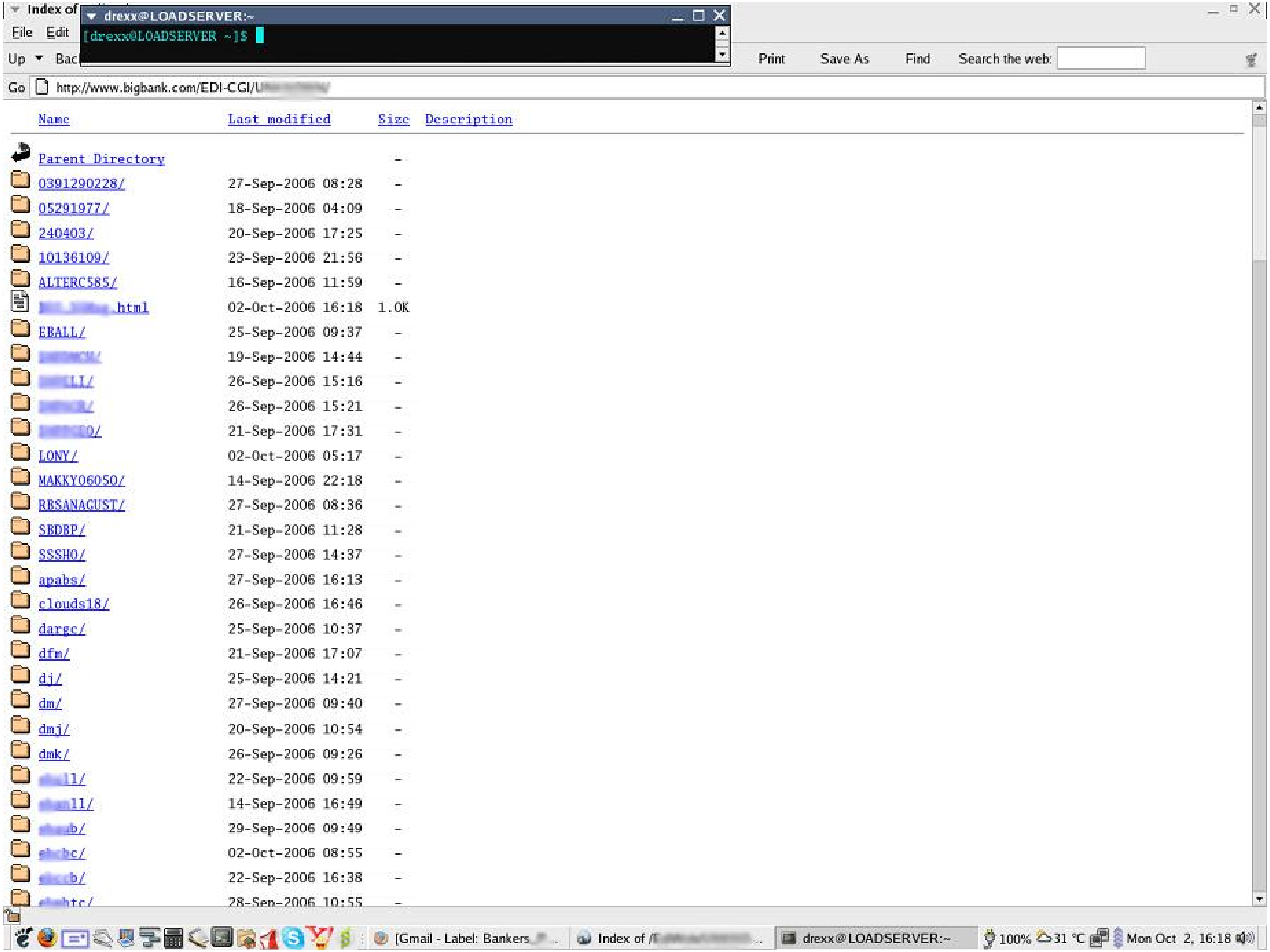
At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waggener, UCB's chief technology officer, said in a press conference Friday afternoon.

The attackers accessed a public Web site and then bypassed additional secured databases stored on the same server. In addition to SSNs, the databases contained health insurance information and non-treatment medical information, such as immunization records and names of doctors patients had seen. No medical records (i.e. patient diagnoses, treatments, and therapies) were taken, as they are stored in a separate system, emphasized Steve Lustig, associate vice chancellor for health and human services.

(Credit: University of California at Berkeley)

"Their ID has not been stolen," he added. "Some data has been stolen."

The server breach began on October 9, 2008, and continued through April 9, when a campus computer administrator doing routine maintenance discovered messages left by the attackers. Logs indicate that the hacks originated from overseas, "primarily in the Asian



Index of
File Edit
Up Bac
Print Save As Find Search the web:
Go
drexx@LOADSERVER:~
[Gmail - Label: Bankers [redacted]
Index of /[redacted]
drexx@LOADSERVER:~
100% 31 °C Mon Oct 2, 16:18

```
[drexx@LOADSERVER ~]$
```

http://www.bigbank.com/EDI-CGI/U[redacted]/

```
Name                 Last modified        Size  Description

Parent Directory                           -
0391290228/          27-Sep-2006 08:28    -
05291977/            18-Sep-2006 04:09    -
240403/              20-Sep-2006 17:25    -
10136109/            23-Sep-2006 21:56    -
ALTERC585/           16-Sep-2006 11:59    -
[redacted].html      02-Oct-2006 16:18  1.0K
EBALL/               25-Sep-2006 09:37    -
[redacted]/          19-Sep-2006 14:44    -
[redacted]LI/        26-Sep-2006 15:16    -
[redacted]/          26-Sep-2006 15:21    -
[redacted]DO/        21-Sep-2006 17:31    -
LONY/                02-Oct-2006 05:17    -
MAKKY06050/          14-Sep-2006 22:18    -
RBSANAGUST/          27-Sep-2006 08:36    -
SBDBP/               21-Sep-2006 11:28    -
SSSHO/               27-Sep-2006 14:37    -
apabs/               27-Sep-2006 16:13    -
clouds18/            26-Sep-2006 16:46    -
dargc/               25-Sep-2006 10:37    -
dfm/                 21-Sep-2006 17:07    -
dj/                  25-Sep-2006 14:21    -
dm/                  27-Sep-2006 09:40    -
dmj/                 20-Sep-2006 10:54    -
dmk/                 26-Sep-2006 09:26    -
[redacted]ll/        22-Sep-2006 09:59    -
[redacted]ll/        14-Sep-2006 16:49    -
[redacted]b/         29-Sep-2006 09:49    -
[redacted]/          02-Oct-2006 08:55    -
[redacted]b/         22-Sep-2006 16:38    -
[redacted]tc/        28-Sep-2006 10:55    -
```

Singapore infocomm Technology Federation

SECURITY & GOVERNANCE CHAPTER

THANK YOU

CSSLP
Certified Secure Software Lifecycle Professional

Anthony Lim
MBA CISSP CSSLP FCITIL
* Advisor, Security & Governance
www.sitf.org.sg
* Director Asia Pacific, Security,
Rational Software, IBM