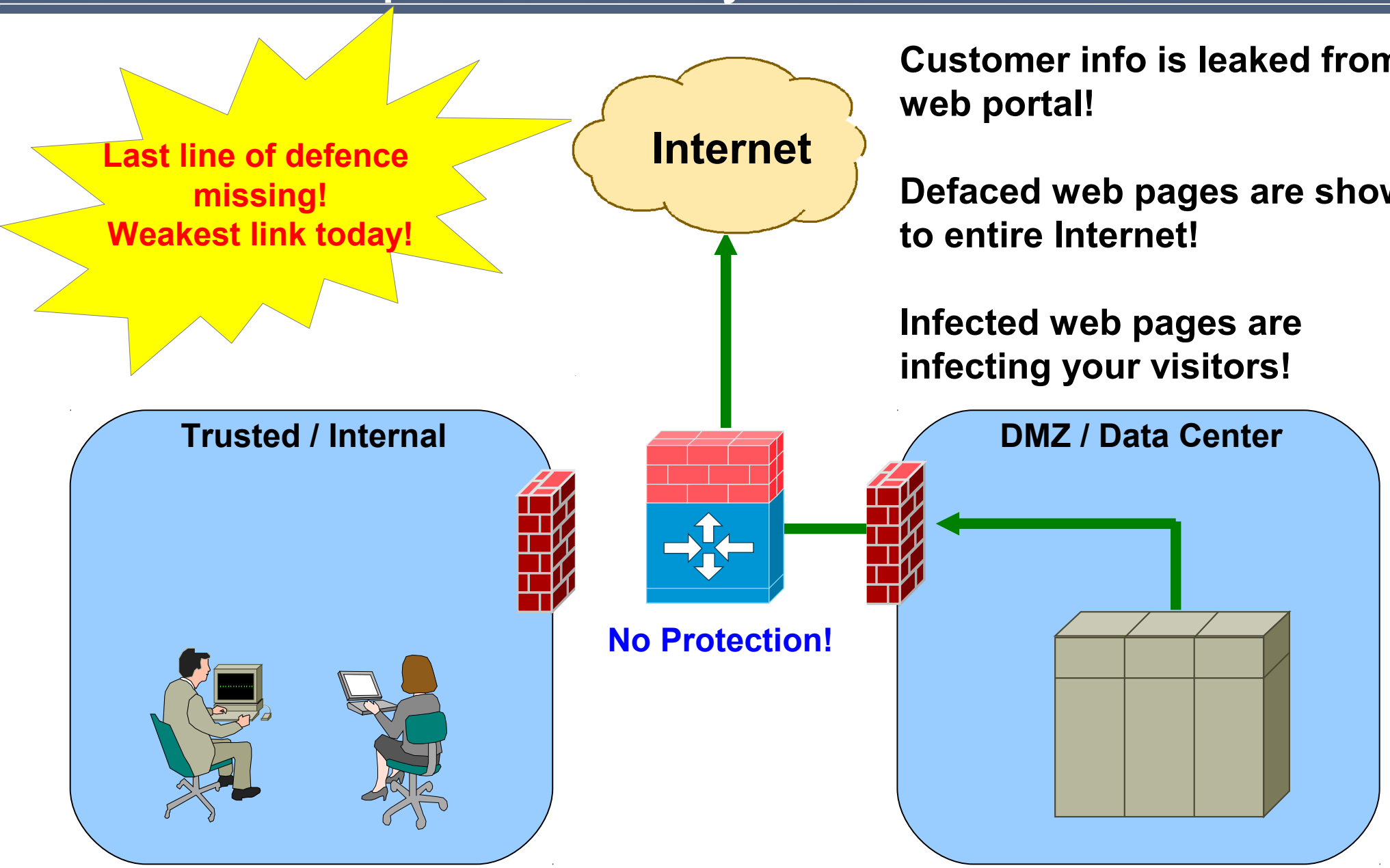
Outbound Security of Your Web and Cloud Services

Where is your last line of defence for information coming out from your web servers / cloud?

Is the “outbound information” from your web / cloud portals really safe?



Do You Know These Business Trivia?

1. You ***cannot hide*** when your website leaks information or is defaced, but you can hide when your PC leaks information or is infected.

2. It is a ***public relations disaster*** when your website infects your visitors, while the public won't know even if all your PCs are infected.

3. IT staff are more likely to be ***fired for embarrassing business management*** because of defaced/infected/leaking websites, instead of infected or leaking endpoints.

4. ***Data privacy regulations*** also forbid you to leak your customer information from your website. You can be fined millions for leaking information from your website.

5. ***Data leakage from cloud***, not data leakage into cloud, is one of the ***Top 3 obstacles*** blocking widespread cloud adoption.

Do You Know These Tech Trivia?

1. Most, if not all, Web Application Firewalls (WAFs) and IPS cannot detect sensitive information leakage in ***binary documents***, e.g. Office docs, PDF files, zipped files.

2. Most, if not all, Web Application Firewalls (WAFs) and IPS cannot detect whether your web pages are ***defaced***.

3. Most, if not all, Web Application Firewalls (WAFs) and IPS cannot detect whether your web pages are ***infected with malicious content***.

4. ***No one*** has deployed endpoint-focused DLP solutions in front of their web and cloud portals.

5. Endpoint-focused DLP solutions can ***severely impact the performance*** of your web and cloud portals.

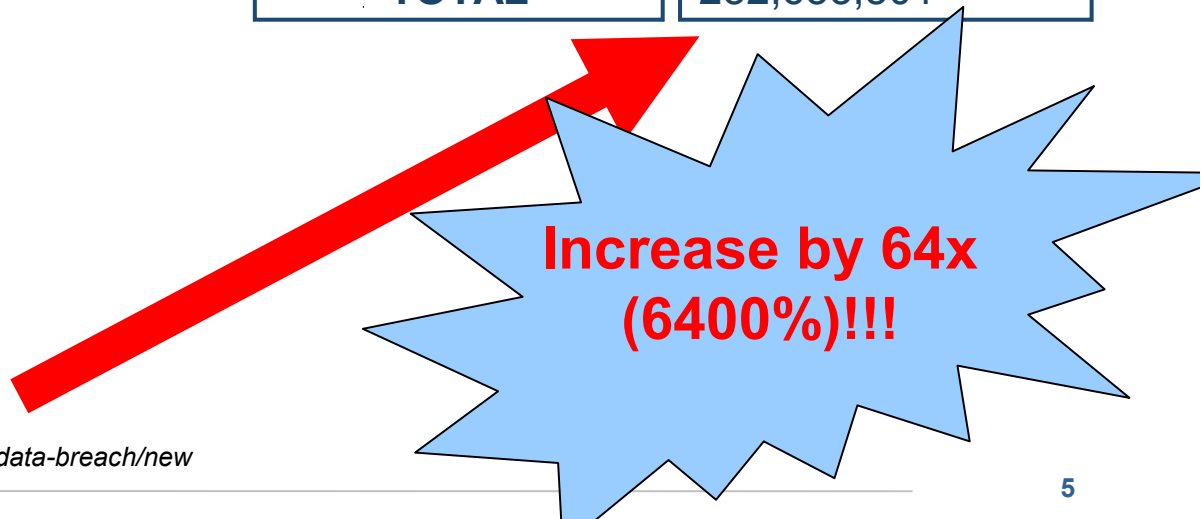
6. Endpoint-focused DLP solutions cannot detect ***defaced or infected web pages or insecure server configuration***.

7. Antivirus solutions cannot detect ***password-protected malicious PDFs***.

Web Leakages Had Been and Still is a Serious Risk!

Industry	# U.S. Records Lost from Web Servers (2005-2008)
Government	2,269,656
Education	588,846
Healthcare	529,034
Financial	114,745
Manufacturing	46,000
Retail	22,735
Real Estate	13,000
Security	5,878
Utilities	3,000
Internet	2,750
Legal	530
Logistics	465
TOTAL	3,596,639

Industry	# U.S. Records Lost from Web Servers (2009-2011)
Retail	140,176,987
Others	85,061,873
Government	3,968,541
Financial	2,313,412
Healthcare	690,765
Education	350,368
Non-profit	71,555
TOTAL	232,633,501



Source: https://www.privacyrights.org/data-breach/new

4 common causes of information leakages from web servers / cloud

1. **Compromised web servers**
   Infected web servers can cause information to be leaked out.

2. **Vulnerabilities in web applications**
   Poorly written applications can result in more information than necessary being shown.

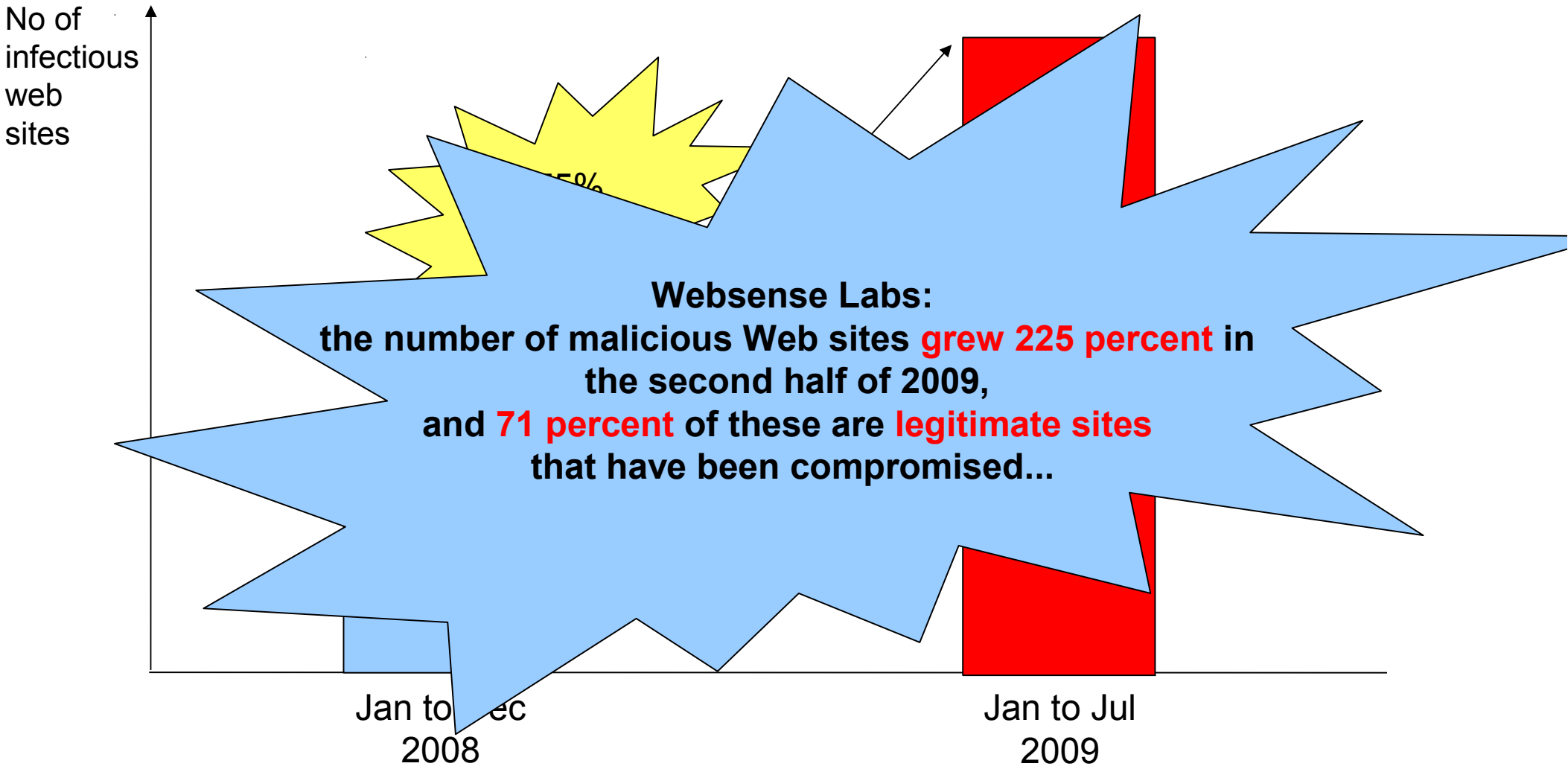
3. **Server errors**
   Malfunctioned or misconfigured web servers can display too much information.

4. **Sensitive Information left on web servers**
   Backup copies of source codes, SQL files, CSV files containing customer records can be left on web servers.

Infected web sites is becoming the more popular way to spread malware

3x more web sites in China were being hacked and used to infect visitors.

Source: Knownsec.com database of defaced Chinese sites



3 reasons to hack a website

1. **Commercial**
   Steal sensitive information to resell or to blackmail

2. **Political (e.g. defacement)**
   Send a message to the whole world.

3. **Transmission to visitors**
   Infects visitors to high-traffic web sites.

Outbound protection blocks these hacker's goals, regardless of the means used by hackers!

Scenario 1: Compromised Web Servers

Adidas

Adidas pulls down sites hit in 'sophisticated' hack

Gymwear biz given a right shoeing

By **John Leyden** · **Get more from this author**

Posted in Enterprise Security, 7th November 2011 15:44 GMT

Adidas has taken some of its websites offline as a precaution following the discovery of a "sophisticated, criminal cyber-att

The s

**...taken down affected sites,
including adidas.com, reebok.com, miCoach.com,
adidas-group.com and various local eCommerce shops,
in order to protect visitors to our sites...
hackers might have
planted malicious scripts on the targeted website...**

**sop
attack. Our p
investigatio
evidence th
data is imp
continue
review, we have taken down
affected sites, including
adidas.com, reebok.com,**

Scenario 1: Compromised Web Servers

Apple

Apple.com hit in latest mass hack attack

Cupertino succumbs to Jedi server trick

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Enterprise Security, 17th August 2010 22:52 GMT

A hack attack that can expose users to malware [illegible] million webpages, at least two of which bel[illegible]

The SQL injection attack[illegible] commands that atten[illegible] sites that fell prey a[illegible] pages Apple uses [illegible] links appear to hav[illegible]

In all, at least 538,000 [illegible] similar fingerprints but poin[illegible] claimed close to 500,000 more.

"These attacks have been ongoi[illegible] changing pretty often," said Mary Landesman, a senior researcher with ScanSafe, a Cisco-owned service that provides customers with real-time intelligence about malicious sites. "Interestingly, many of the sites compromised have been involved in repeated compromises over the past few months. It's not clear whether these are the work of the same attackers or are competing attacks."

SQL injection attacks succeed because web applications don't properly filter search queries

"A hack attack that can expose users to malware exploits has infected more than 1 million webpages, at least two of which belong to Apple....
The attacks that hit Apple used highly encoded text strings to sneak past web-application filters.

Scenario 1: Compromised Web Servers

5 major Japanese companies

At least 73,000 visitors may be infected

Gumblar virus inf
websites

THE ASAHI SHIMBUN

2010/1/6

The dreaded Gumblar virus m
70,000 visitors to the websites o
that were confirmed altered via the m

The websites of East Japan Railway
gano-based Shin-etsu Broadcasting Co., Kobe-based Radio Kansai and Kobe confectionary Morozoff Ltd., were also altered by hackers using the virus.

The virus sends visitors to the corporate sites to an alternative site that contains further malware that allows the virus to propagate in the visitors' computers.

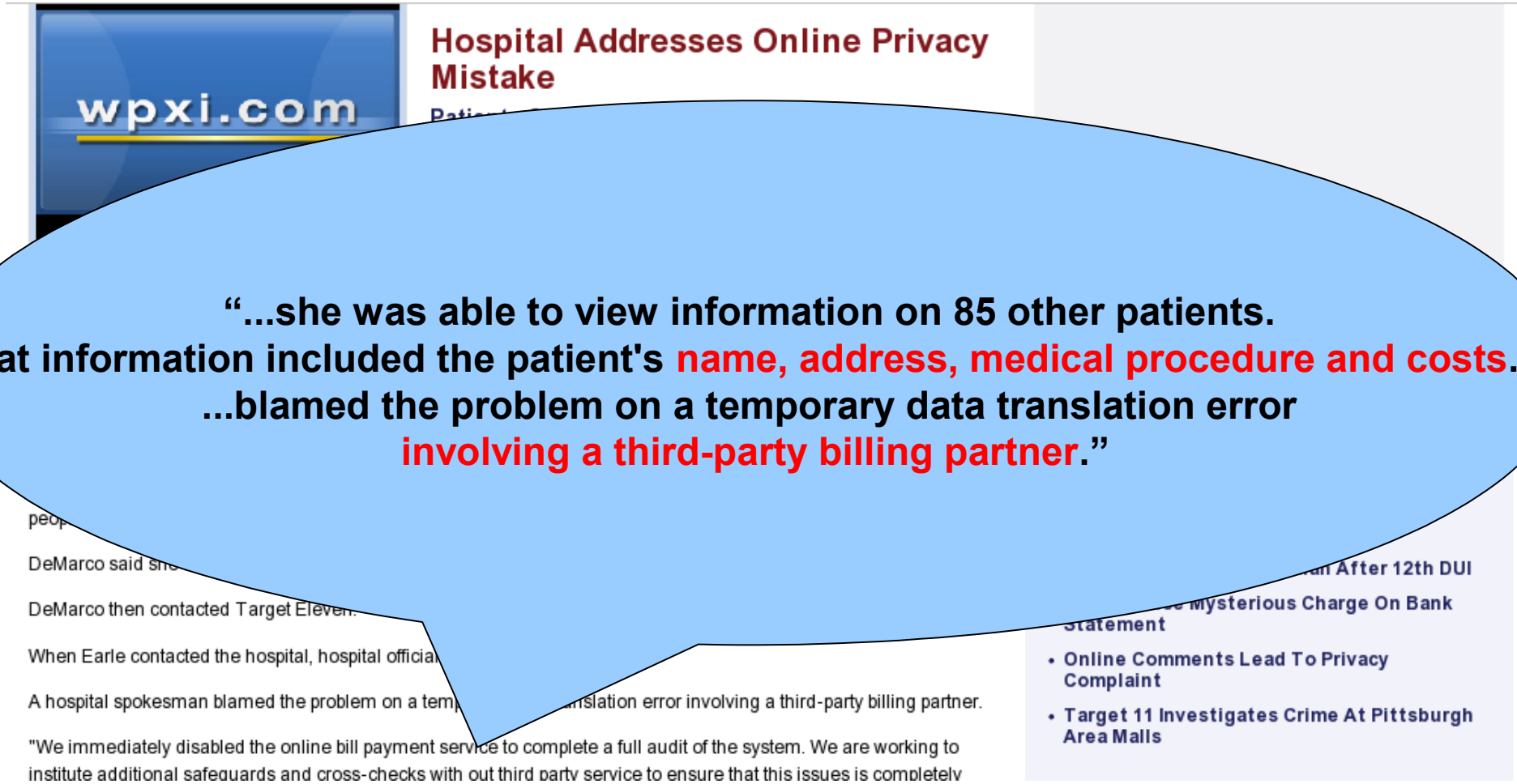
Experts warn that the virus could cause further damage and allow hackers to steal passwords of other sites managed by infected computers and alter the programs.

"...websites of five companies, including Honda Motor Corp.... The virus sends visitors to the corporate sites to an alternative site that contains further malware that allows the virus to propagate in the visitors' computers... "

Scenario 2: Vulnerabilities in Web Applications

West Penn Hospital

85 other patient records were shown in online bill payment portal.



**"...she was able to view information on 85 other patients.
That information included the patient's name, address, medical procedure and costs....
...blamed the problem on a temporary data translation error
involving a third-party billing partner."**

Scenario 3: Server Errors

Microsoft BPOS Cloud Service

Microsoft BPOS cloud service hit with data breach

A 'small number' of Offline Address Book users had some of their data accessed

By Andreas Udo de Haes, Webwereld Netherlands

December 22, 2010 11:39 AM ET Comments (3) Recommended (14)

...due to a configuration issue,
Offline Address Book information for Business Productivity Online Suite (BPOS) Standard customers could be inadvertently downloaded by other customers of the service, in a very specific circumstance,"...
Microsoft has notified all Business Productivity Online Suite-Standard partners and customers about the issue.

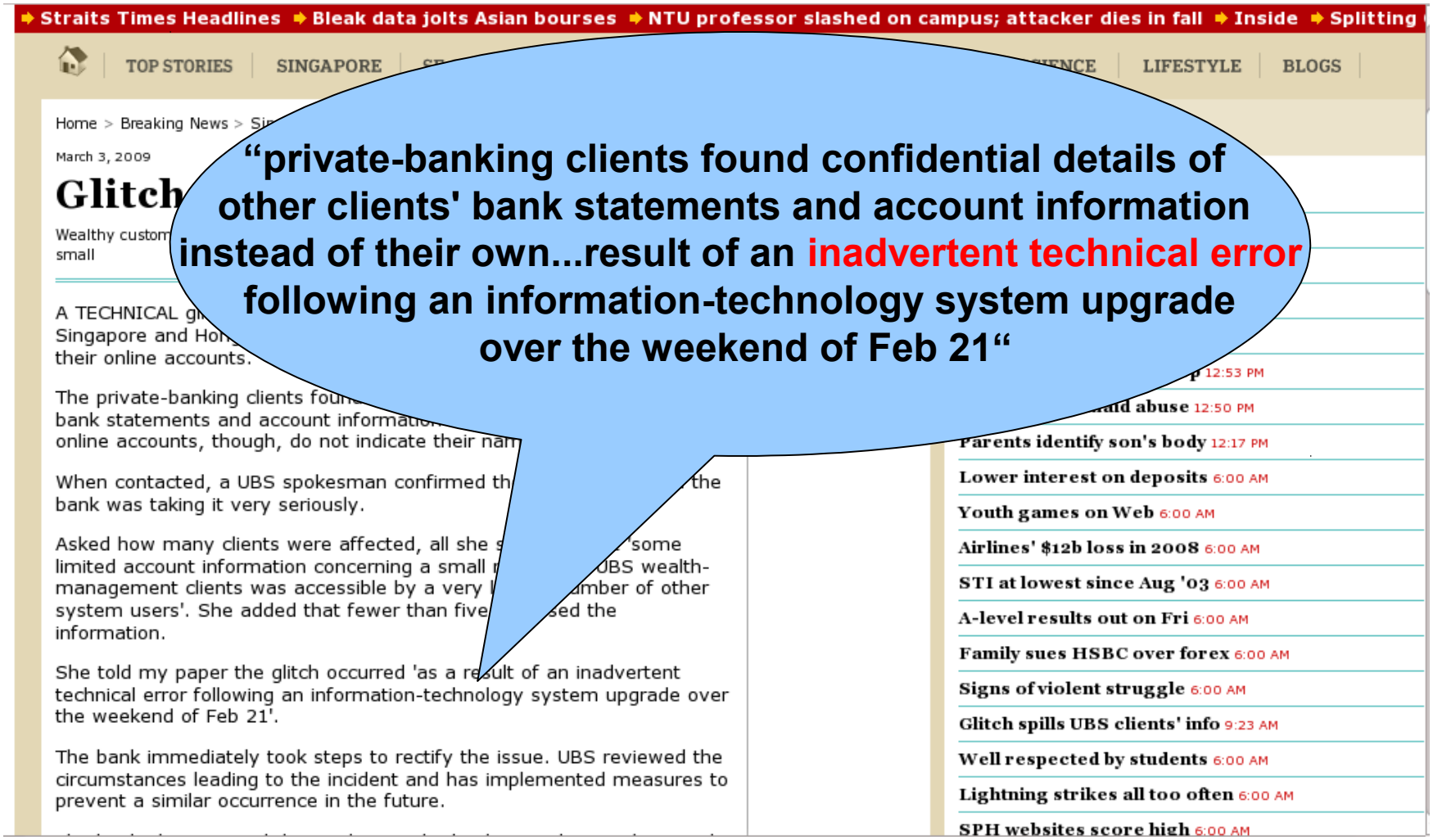
service ... director of
BPOS ... rosoft.

The data ... curred in Microsoft data centers in North America, Europe and Asia. ... issue was resolved within two hours of being discovered, Microsoft said in a statement. However, during this time "a very small number" of illegitimate downloads occurred. "We are working with those few

Scenario 3: Server Errors

UBS

Bank customer records were leaked during system upgrade



Scenario 4: Sensitive Information Left on Web Server

Princeton Review

108,000 student records were leaked

Student Private Information Leaked on Preparatory Firm Website

Princeton Review published confidential data by accident

By **Denisa Ilascu**, Internet / SEO News Editor
19th of August 2008, 12:28 GMT

Adjust text size: A- A+

Princeton Review, an
responsible for
seven week
Review, h
address.

The organiz
Florida. The file
ethnicities and their gr
students' skills in mathematics, reading, science and
other sensitive information regarding learning disabilities, or whethe
language or not.

The schools in Sarasota were not the only ones affected by the fa
nity system of Princeton Review. The names and birthdays of approximately 74,000 students from the public s
x County, Virginia, were revealed in the same way.

"Some of the information is said to have been accessible th
earch engines like Google. You have to wonder - if companies are making it this easy to discover information ab
ndividuals, why do identity thieves go to all that effort of writing spyware?" **commented** Senior Technology Consultant
the security company Sophos, Graham Cluley.

The most intriguing thing about the incident was that it was discovered by another preparatory firm, as it was performing a survey to see how competition was doing. When finding that all the data, which were not supposed to ever be made public, were available on the Princeton Review website, the institution, on the condition of being allowed anonymity, broke the story to the Washington Post.

"The most intriguing thing about the incident was that it was discovered by another preparatory firm, as it was performing a survey to see how competition was doing.... broke the story to the Washington Post"

Scenario 4: Sensitive Information Left on Web Server

Government Agency, Malaysia

150 officers' private information was leaked while CEO was lecturing the public to have safe IT practices.

Bil	Nama	No. K/P	Alamat	Penempatan
1	Mohd Ghuzaimi B	14-5881	Bandar Tun ras, Kuala	aian Malaysia
2	Norazura Binti An	10-5622	la, 42000 Selangor	aian Malaysia
3	Amerul Hazriq Bi	43-5141	jah, 47000 elangor.	aian Malaysia
4	Mohd Nur Azimm	03-5139	Wakaf tan	n Cheras
5	Mohamad Ridwa Ali	14-6255	ri, 52100 umpur.	n Cheras
6	Norshazrina Binti	14-5176	, Kampung Rawang,	Jalan Duta
7	Mohd Khairul Azu	11-5325	Off Port Klang,	Jalan Duta
8	Norhamiza Binti A	08-6358	Taman m Kedah	Jalan Duta
9	Muhamad Al Hafi	56-5129	pung Limau, 59200 Kuala	Jalan Duta
			a, Kampung	

Scenario 4: Sensitive Information Left on Web Server

Elections Department, Singapore

Private information of election candidates was leaked

Elections Department boo boo

May 8, 2011 - 10:56pm

By: Tay Shi'an

... included the NRIC number of Health Minister Khaw Boon Wan, and the NRIC and handphone numbers of Aljunied candidate.... from the People's Action Party (PAP). The handphone numbers of opposition candidates .... were also made public.

TNP PHOTO: Kua Chee S

On April 29, The Ne ed the Elections Department that it had upload scanned forms containing th information of several candidates contesting in this year's elections.

At about 3pm on t same day, the website with all the forms was taken down.

The forms includ the NRIC number of Health Minister Khaw Boon Wan, and the NRIC and handphone numbers of Aljunied candidate Ong Ye Kung from the People's Action

Scenario 4: Sensitive Information Left on Web Server

Telco A, Singapore

National ID of 100 lucky draw winners were left undetected on telco web site for 5 years.

[redacted] **Mobile Valentine's Day Messaging Contest 2004**

Congratulations to all winners!
All winners will be notified by post and prizes must be collected by 21 April 2004.
Please email us if you do not hear from us by 31 Mar 04 5pm.

Best Messages - $2000 travel voucher:

I/C	Names
S[redacted]11H	Mr CHAN KOK KEONG
S[redacted]18I	MR JEREMY SEKSAN VORANATH
S[redacted]90C	MS TANG WEI HONG

Early Bird / DJ's Best Selections – A pair of GV movie vouchers :

I/C	Names
F[redacted]72N	MR HUANG CHI CHANG
G[redacted]93Q	MR HUNGERFORD RICHARD
G[redacted]23W	MR ASHOK GOPAL
G[redacted]02P	MR TAN KAK QUI
S[redacted]43G	MR TOH YEW WING
S[redacted]29J	MRS CHOO HWEE CHENG
S[redacted]03D	SAINI BIN SALLEH
S[redacted]12J	MR ROKIAH BINTE SITAM

Scenario 4: Sensitive Information Left on Web Server

Ministry of Defence, UK

Military secrets were leaked from an online PDF

TOP SECRET MOD LEAKS MADE AGAIN ON WEBSITE

An online internal report contained black-out -passages that could still be read by the enemy...
...made the same mistake just six months ago,
when they failed to secure a report into nuclear submarines...
..."To make such a blunder once is unfortunate, to do it twice is careless in the extreme."

ABOVE: Our story from April

In both gaffes, secret passages could be read by copying them into a new document.

In the latest clanger the report told how wind farms affect nearby radar stations and how any interference can be overcome.

> **To make such a blunder once is unfortunate, to do it twice is careless in the extreme**
>
> Graham Cluley, a computer security expert at the web safety firm Sophos

The 22-page "Air Defence And Air Traffic Systems Radar Transportation Study – Part 2" was posted on Parliament's website.

Graham Cluley, a computer security expert at the web safety firm Sophos, said: "Once again it's another schoolboy error. You have to wonder how many times they are going to keep making basic data security mistakes.

Scenario 4: Sensitive Information Left on Web Server

Southeast Asian Army

Sensitive military inventory was leaked

Resources

HEADQUARTERS

[redacted] ARMY

MONTHLY STATUS OF ENGINEER EQUIPMENT

(For the Month of November 2007)

NR	NOMENCLATURE	MAKE	MODEL	USN	ESN	YR ACQ	STAT	USING UNIT	LOCATION	REMARKS
1	BACKHOE EXCAVATOR	CASE	M1085L		46018864	1991	G	BCOY, 543ECB	[redacted]	
2	BACKHOE, LOADER	CASE	580SK	D130029	45049327	1991	G	BCOY, 542ECB		
3	BACKHOE, LOADER	CASE	580L	556022985	45323764	1991	R	EEMCO, 543ECB		FOR REPAIR
4	BACKHOE, LOADER (MINI)	YANMAR	3TN78L-DBS		01615	2006	G	BCOY, 552ECB		
5	ROAD ROLLER	DRESSER	VOS2-66B	SX320002U470268	44275750	1989	G	ACOY, 542ECB		
6	ROAD ROLLER	DRESSER	BOMAG	1984B	109937	1989	G	EEMCO, 542ECB		
7	ROAD ROLLER	DRESSER	VOS-266B	V320002U470272	44294767	1989	G	CCOY, 543ECB		
8	ROAD ROLLER PORTABLE	8RDP			1977506		G	EEMCO 546ECB		
9	ROAD ROLLER	DRESSER	VOS2-66B		44291750	1990	R	EEMCO, 546ECB		FOR REPAIR
10	ROAD ROLLER	DYNAPAC	C5508W	45179728	585278CD	1991	Y	EECO, ESB		
11	ROAD ROLLER VIBRATORY	DRESSER			44280114	1989	R	B COY 552ECB		FOR REPAIR
12	ROLLER, SF 2 DRUM	BROS	M5-1/2	TR-388		1968	G	EEMCO, 552ECB		
13	ROAD, GRADER	DRESSER	A450E	G75005U100619	44325830	1989	G	BCOY, 542ECB		
14	ROAD, GRADER	DRESSER	A450E	G750005U101045	44410174	1990	G	BCOY,542ECB		
15	ROAD, GRADER	DRESSER	A400E	G710002U100419	466DC2U521963	1988	G	ACOY, 543ECB		
16	ROAD, GRADER	CAT	E120G	87V06163	A4095Y	1982	R	EEMCO, 543ECB		FOR REPAIR
17	ROAD, GRADER	DRESSER	A450E	G75000U100621	44324459	1989	G	BCOY 543ECB		
18	ROAD, GRADER	DRESSER	A450E		44324460	1989	R	EEMCO, 546ECB		

Thank You

Wong Onn Chee

onnchee@infotectsecurity.com