Outbound Security of Your Web and Cloud Services

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

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- My night jobs
  - Chapter Lead, OWASP Singapore
  - President, Cloud Security Alliance Singapore Chapter
  - Main Organizer, Singapore Security Meetup Group
  - Cloud Security WG Chair, Security and Privacy Standards Committee, IT Standards Committee, Singapore
  - Member, International Standardisation Council, CSA
  - CIS Community Contributor
  - Champion, Singapore Cyber Defender Programme, Ministry of Home Affairs
  - Feeding my 6-mth old baby girl at midnight

About Me

- My day jobs
  - CTO, Resolvo Systems
  - MD, Infotect Security www.infotectsecurity.com
  - CISSP, CISM, CISA, SABSA Chartered Architect and etc....

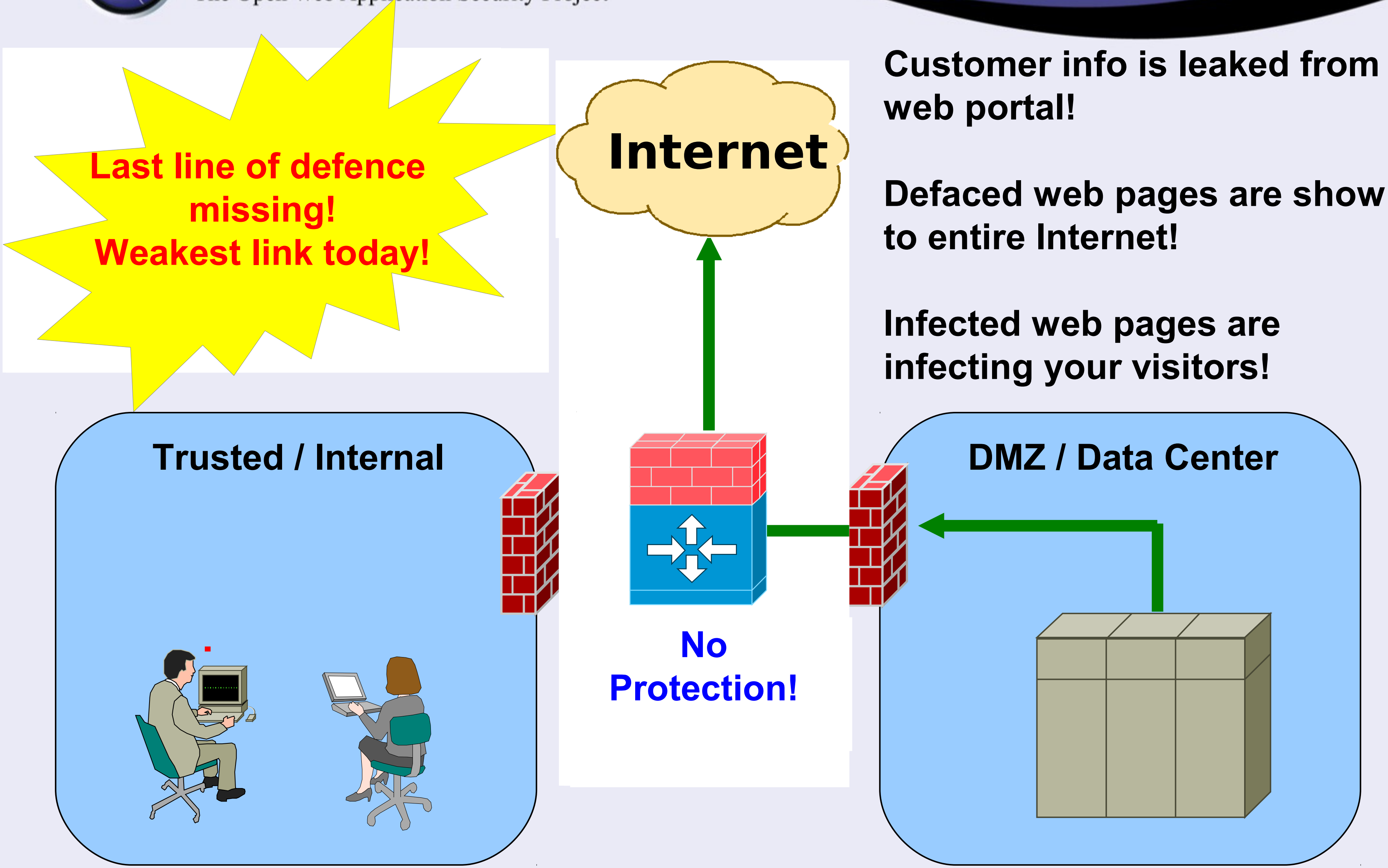
Is the “outbound information” from your web / cloud portals really safe?

OWASP
The Open Web Application Security Project

Customer info is leaked from web portal!

Defaced web pages are shown to entire Internet!

Infected web pages are infecting your visitors!



Last line of defence missing!
Weakest link today!

Internet

Trusted / Internal

DMZ / Data Center

No Protection!

OWASP
The Open Web Application Security Project

Do You Know These?

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.

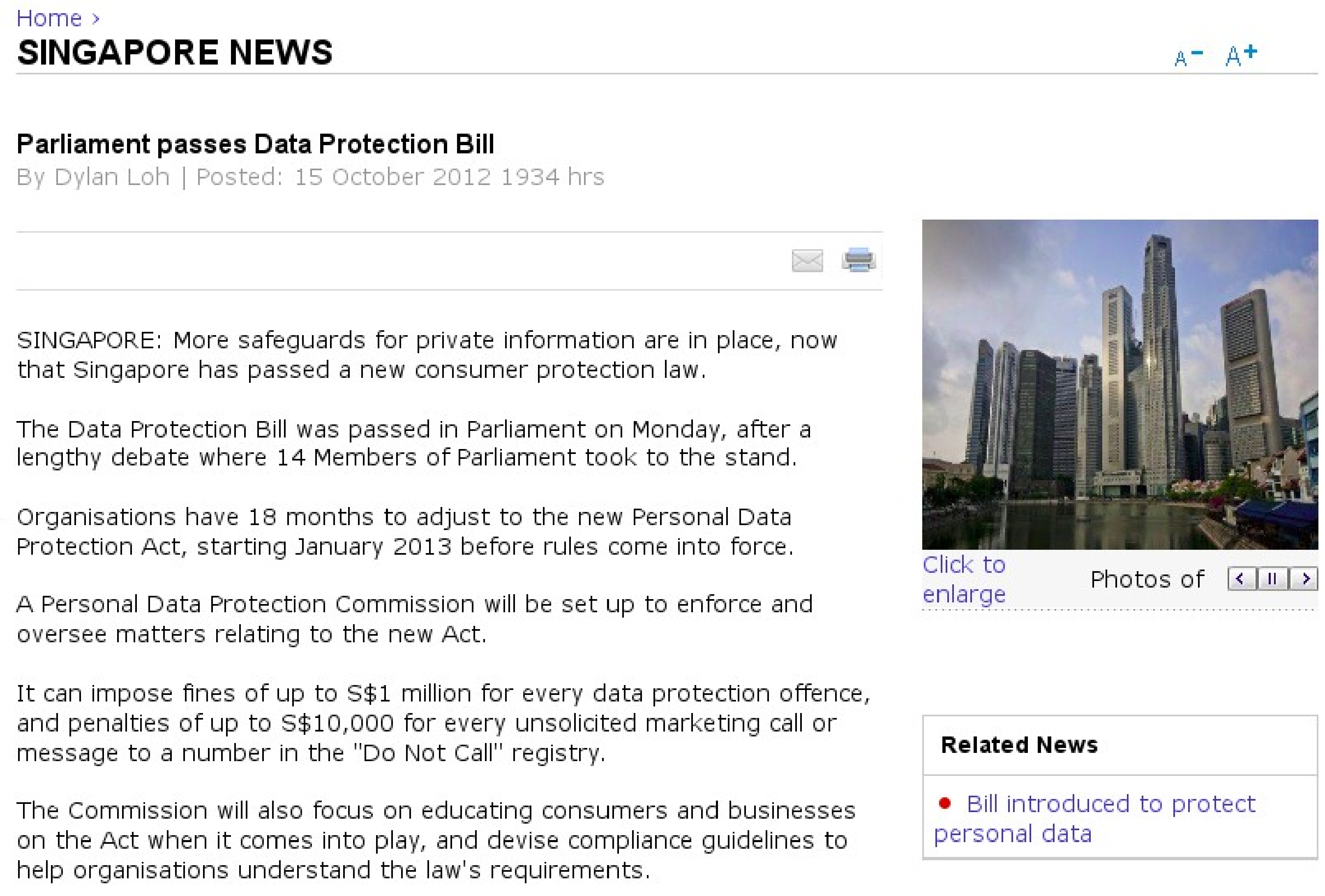
5 ***Data leakage from cloud***, not data leakage into cloud, is one of the ***Top 3 obstacles*** blocking widespread cloud adoption.

Increased privacy legislations will drive the need to monitor your websites for leakages

Websites **MUST** comply with information leakage protection and data privacy requirements in the following regulations:

1. EU Data Protection Directive – Security Safeguards Principle 11
2. Sarbanes-Oxley Act (2002), HIPAA, GLBA - U.S.
3. Data Protection Act – UK
4. Personal Information Protection Act – Japan, Korea
5. Personal Data Protection Act – Malaysia, China, Taiwan, Singapore
6. Information Technology Act – India
7. Privacy Act – Australia, New Zealand
8. Personal Data Ordinance – Hong Kong

Singapore Personal Data Protection Act passed on 15 Oct 2012



SINGAPORE NEWS

Parliament passes Data Protection Bill

By Dylan Loh | Posted: 15 October 2012 1934 hrs

SINGAPORE: More safeguards for private information are in place, now that Singapore has passed a new consumer protection law.

The Data Protection Bill was passed in Parliament on Monday, after a lengthy debate where 14 Members of Parliament took to the stand.

Organisations have 18 months to adjust to the new Personal Data Protection Act, starting January 2013 before rules come into force.

A Personal Data Protection Commission will be set up to enforce and oversee matters relating to the new Act.

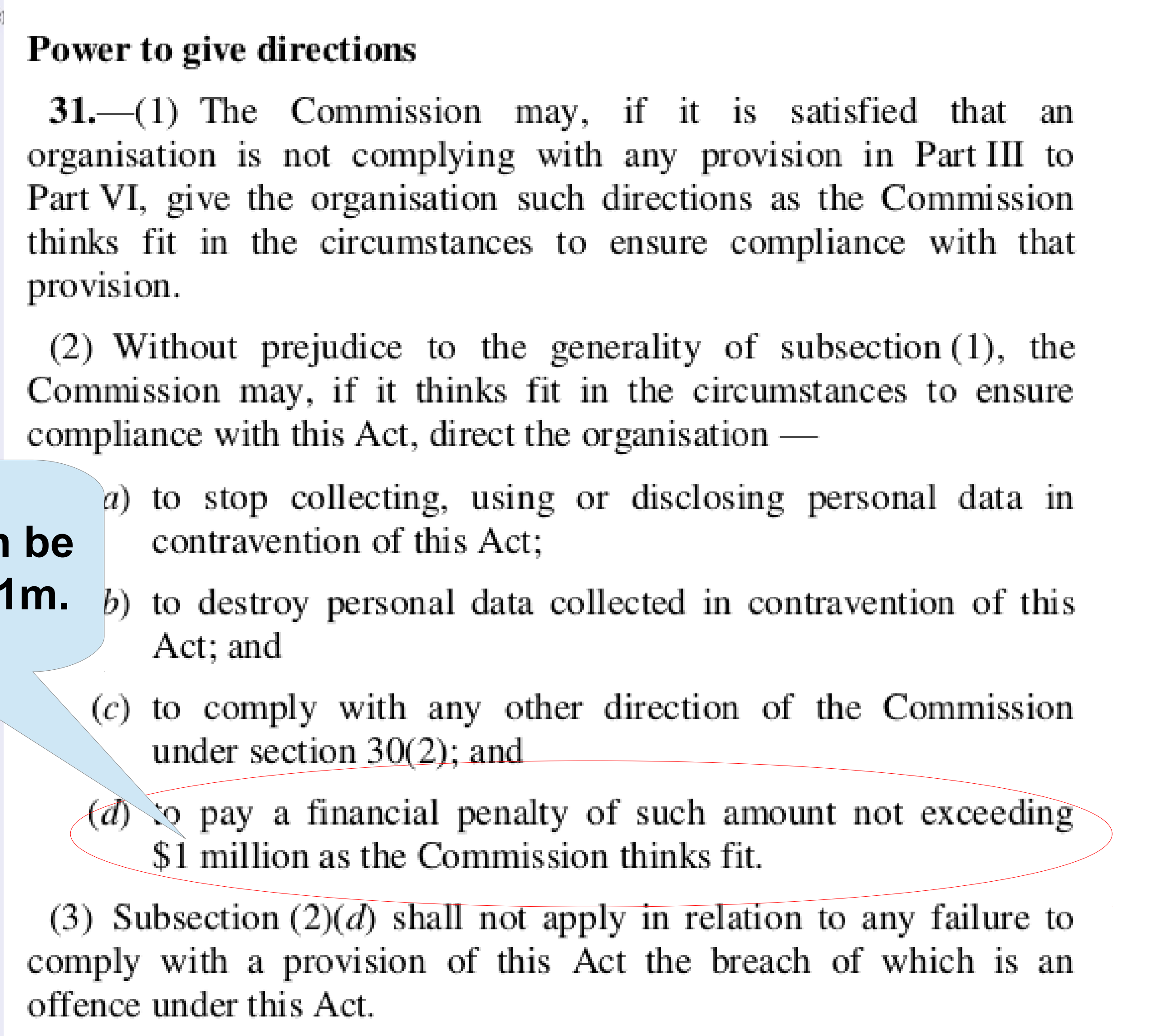
It can impose fines of up to S$1 million for every data protection offence, and penalties of up to S$10,000 for every unsolicited marketing call or message to a number in the "Do Not Call" registry.

The Commission will also focus on educating consumers and businesses on the Act when it comes into play, and devise compliance guidelines to help organisations understand the law's requirements.

Related News

- Bill introduced to protect personal data

For companies, up to S$1m financial penalty for breaching the Singapore PDPA



Power to give directions

31.—(1) The Commission may, if it is satisfied that an organisation is not complying with any provision in Part III to Part VI, give the organisation such directions as the Commission thinks fit in the circumstances to ensure compliance with that provision.

(2) Without prejudice to the generality of subsection (1), the Commission may, if it thinks fit in the circumstances to ensure compliance with this Act, direct the organisation —

(*a*) to stop collecting, using or disclosing personal data in contravention of this Act;

(*b*) to destroy personal data collected in contravention of this Act; and

(*c*) to comply with any other direction of the Commission under section 30(2); and

(*d*) to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

(3) Subsection (2)(*d*) shall not apply in relation to any failure to comply with a provision of this Act the breach of which is an offence under this Act.

Companies can be fined up to S$1m.

Do You Know These Too?

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

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 (2009-2012)
Retail	168,280,885
Others	92,523,918
Government	13,611,652
Financial	3,406,956
Healthcare	807,076
Education	2,099,219
Non-profit	109,314
TOTAL	280,839,020

Increase by 78x (7800%)!!!

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

4 common causes of information leakages from web servers / cloud

OWASP
The Open Web Application Security Project

All OWASP Top 10 risks can result in loss of sensitive information from your web app!

1 Compromised web servers

Infected web se rs can cause aked out.

2 Vulner

an necessary being shown.

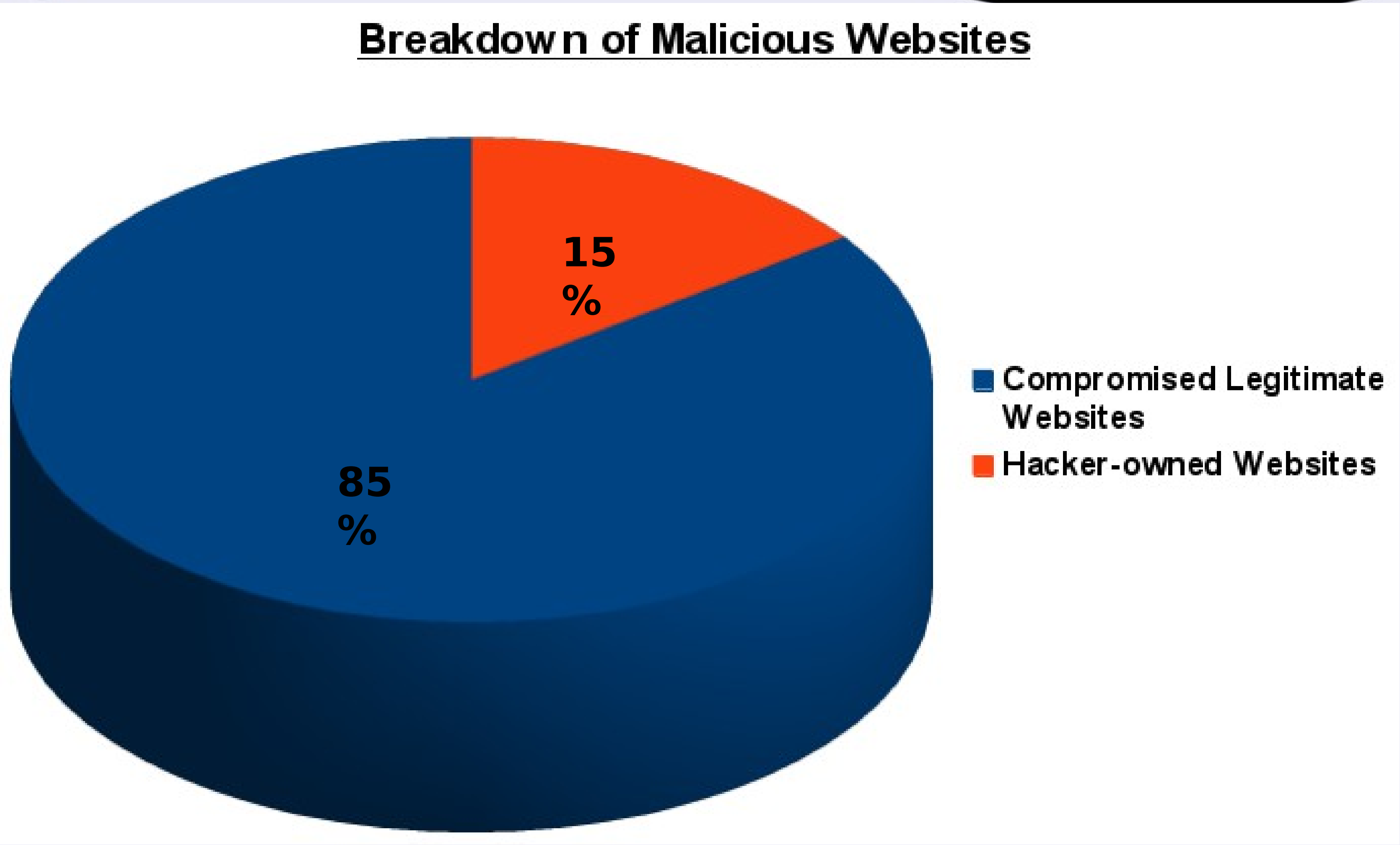
3 Configurat

Malfunctioned or misconfigured web servers can display too much information.

4 Sensitive Information left on web servers

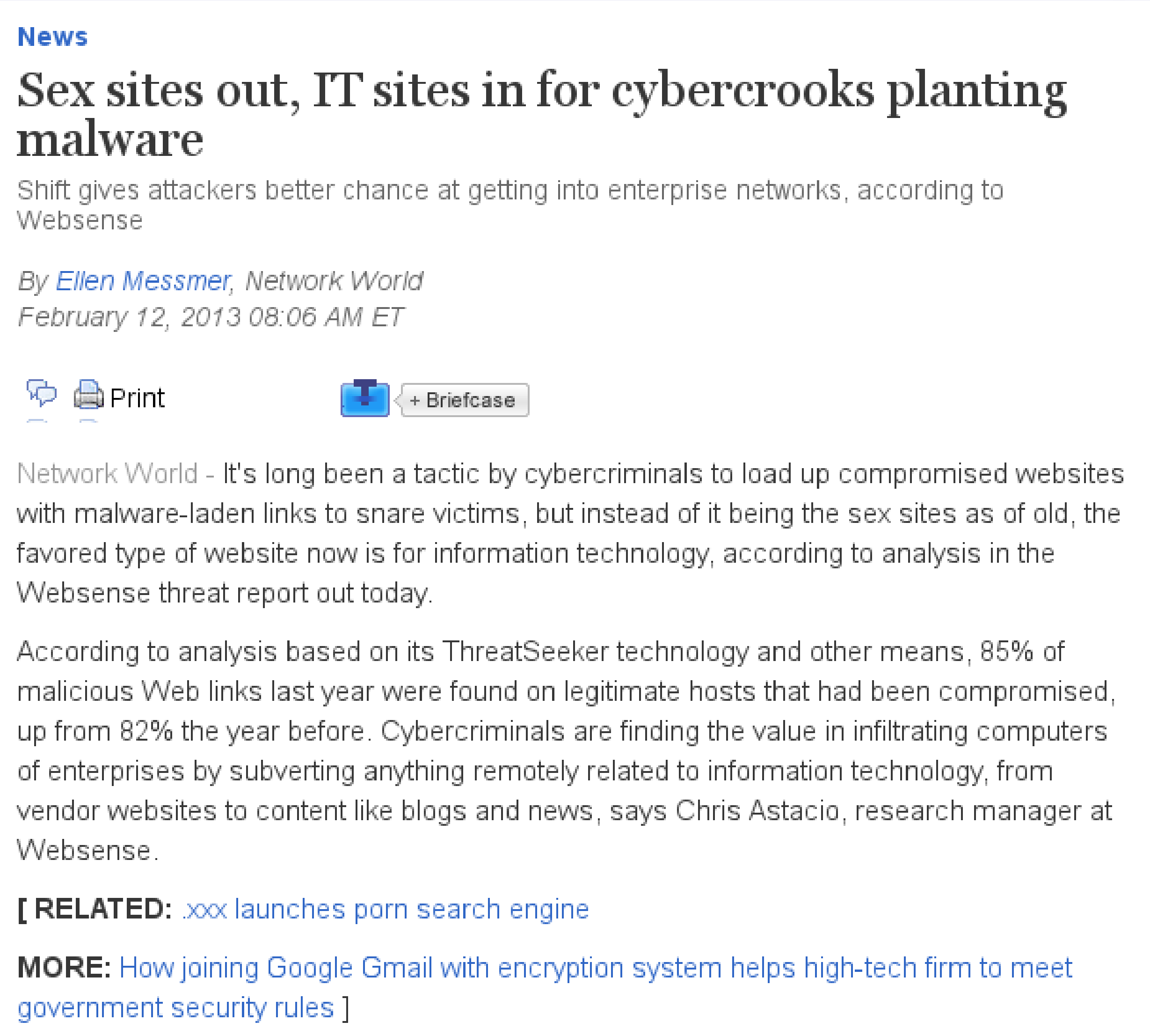
Backup copies of source codes, SQL files, CSV files containing customer records can be left on web servers.

Compromised websites is the most popular way to spread malware



Source: Websense 2013 Threat Report

Compromised websites is the most popular way to spread malware



News

Sex sites out, IT sites in for cybercrooks planting malware

Shift gives attackers better chance at getting into enterprise networks, according to Websense

By Ellen Messmer, Network World
February 12, 2013 08:06 AM ET

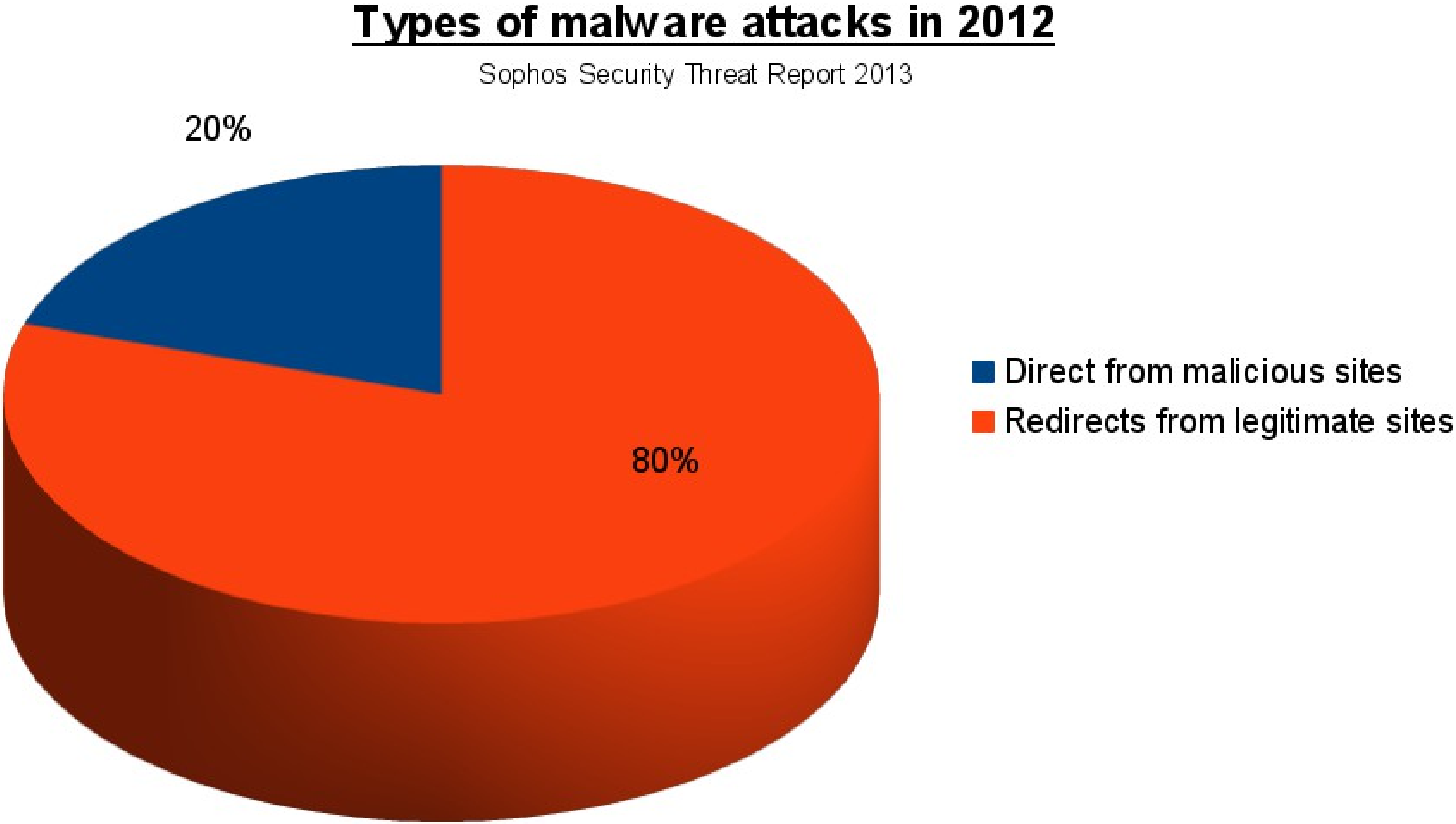
Network World - It's long been a tactic by cybercriminals to load up compromised websites with malware-laden links to snare victims, but instead of it being the sex sites as of old, the favored type of website now is for information technology, according to analysis in the Websense threat report out today.

According to analysis based on its ThreatSeeker technology and other means, 85% of malicious Web links last year were found on legitimate hosts that had been compromised, up from 82% the year before. Cybercriminals are finding the value in infiltrating computers of enterprises by subverting anything remotely related to information technology, from vendor websites to content like blogs and news, says Chris Astacio, research manager at Websense.

[RELATED: .xxx launches porn search engine

MORE: How joining Google Gmail with encryption system helps high-tech firm to meet government security rules]

Compromised websites is the most popular way to spread malware



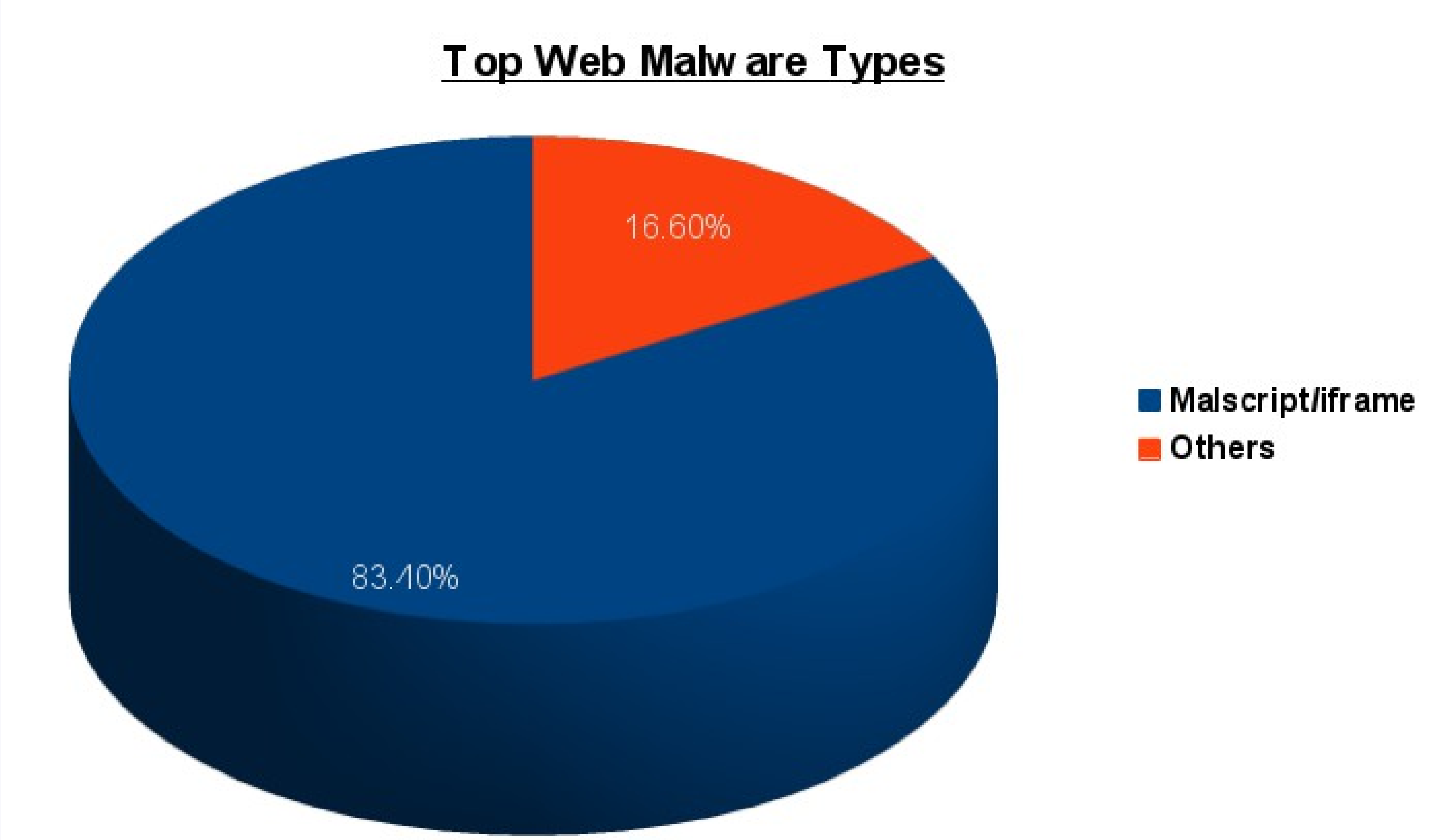
Types of malware attacks in 2012

Sophos Security Threat Report 2013

OWASP
The Open Web Application Security Project

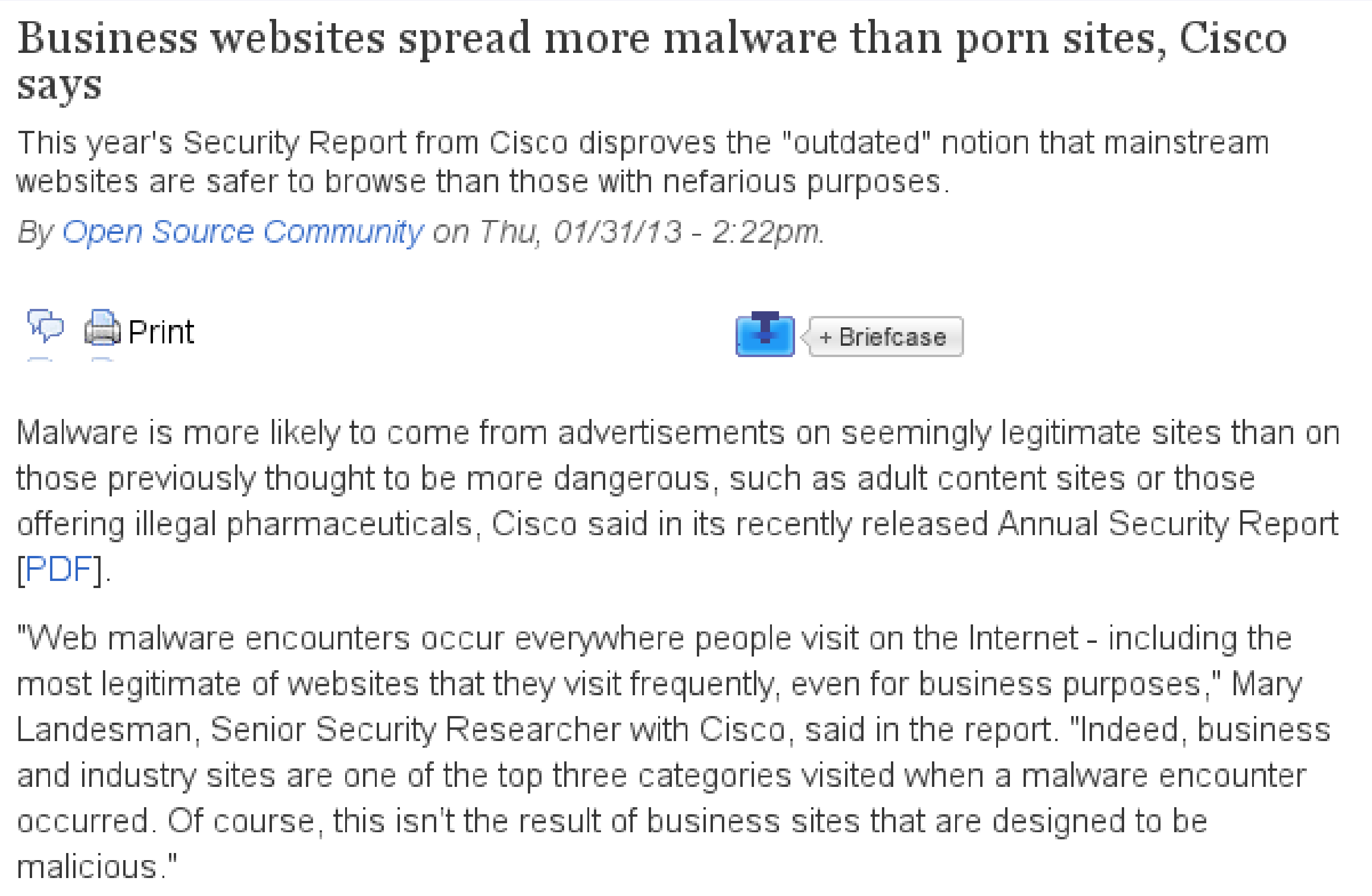
Compromised websites is the most popular way to spread malware

Cisco Annual Security Report 2013



Compromised websites is the most popular way to spread malware

Cisco Annual Security Report 2013



Business websites spread more malware than porn sites, Cisco says

This year's Security Report from Cisco disproves the "outdated" notion that mainstream websites are safer to browse than those with nefarious purposes.

By Open Source Community on Thu, 01/31/13 - 2:22pm.

Malware is more likely to come from advertisements on seemingly legitimate sites than on those previously thought to be more dangerous, such as adult content sites or those offering illegal pharmaceuticals, Cisco said in its recently released Annual Security Report [PDF].

"Web malware encounters occur everywhere people visit on the Internet - including the most legitimate of websites that they visit frequently, even for business purposes," Mary Landesman, Senior Security Researcher with Cisco, said in the report. "Indeed, business and industry sites are one of the top three categories visited when a malware encounter occurred. Of course, this isn't the result of business sites that are designed to be malicious."

Do You Know These?

Fact1

No one, among the audience, knows what new hacker attack techniques, behaviour, pattern will come to light by this evening.

Since we do not know what new hacker tricks will be, why focus our efforts on the unknown?

Fact2

For decades, we had been chasing after hackers by focusing on on their attack methods, but to date, we are still not winning the war with this reactive approach.

A definition of Insanity: Expecting different results by repeating the same things over and over again.

A better and smarter approach – DATA-CENTRIC SECURITY

Fact3

A good example is the use of encryption. In encryption, we focus on protecting valuable data, instead of worrying about hacker attack signature, behaviour, pattern, reputation and so on.

Fact4

Alas! Encryption is not effective when it comes to web applications or cloud services. Ask yourself: Do you see a encrypted bank statement from your Internet banking portal even though the data is stored encrypted?

**A new and
more effective
way to
defeat the hackers!**

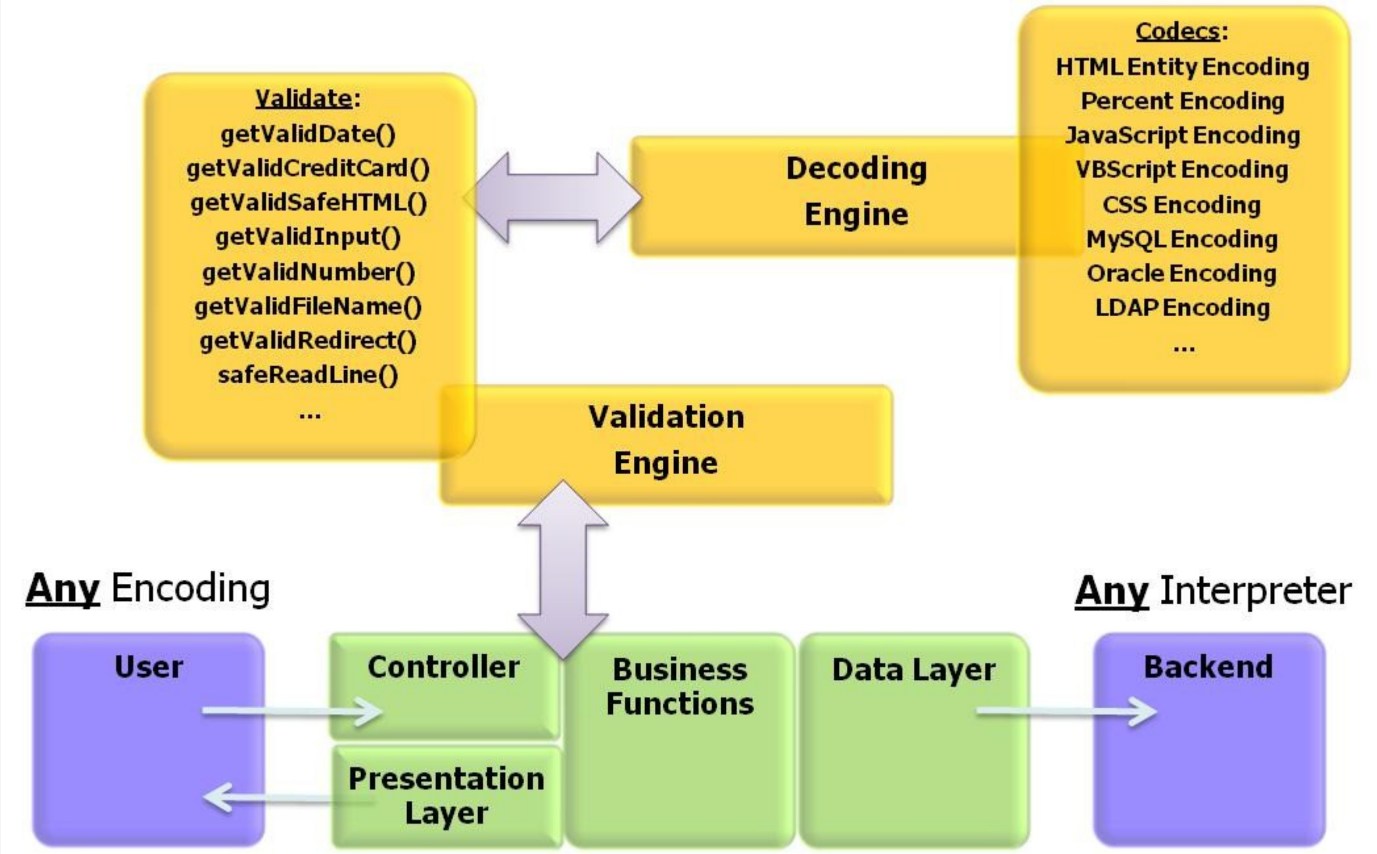
Top 10 steps to address outbound risks.

OWASP
The Open Web Application Security Project

1

Output Encoding

- Effective against XSS.
- Available from OWASP ESAPI: ESAPI.encoder().encodeforXXX()



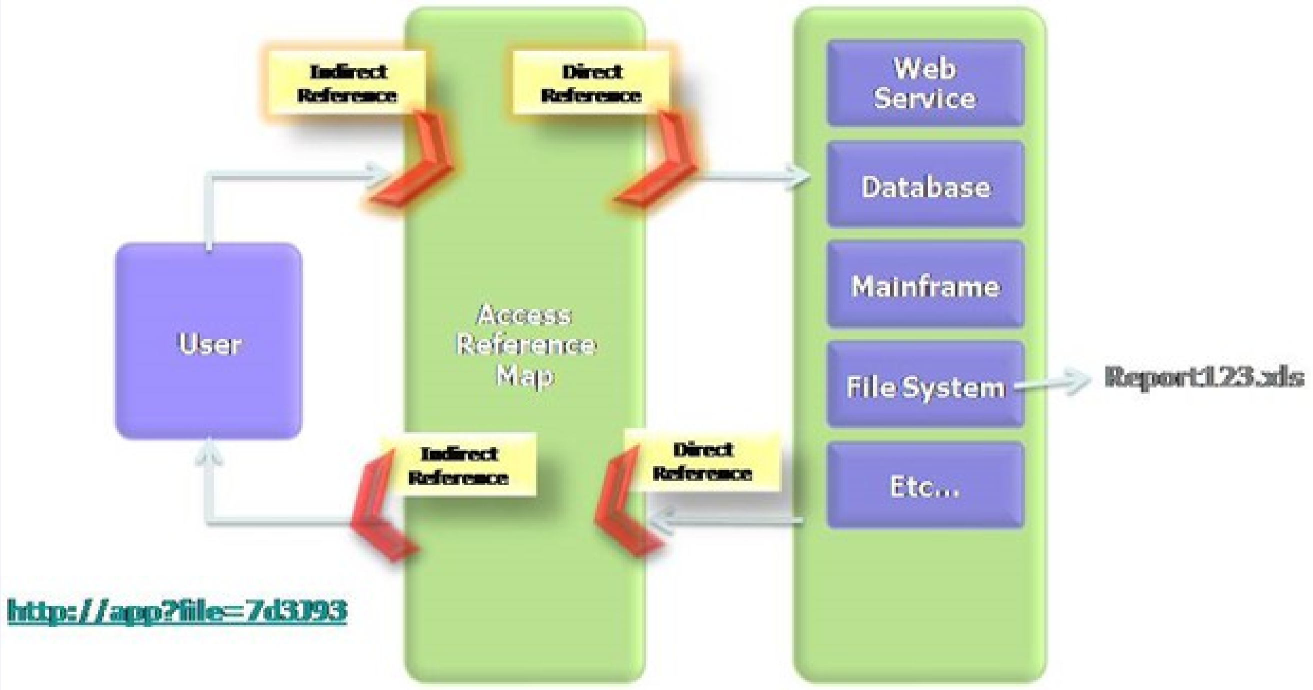
Top 10 steps to address outbound risks.

2 **Strong Authentication & Proper Session Management**

- 2FA. *Have you enabled 2FA for your Gmail?*
- OWASP ESAPI: Authenticator interface

3 **Secure, Indirect Object References**

- OWASP ESAPI: RandomAccessReferenceMap interface



Top 10 steps to address outbound risks.

4 **Configuration Hardening**
- Use of CIS hardening benchmark guides for OS and web application platform

5 **Encryption**
- Useful for database storage and as part of multi-layered defence.

6 **Restrict URL access**
- OWASP ESAPI: isAuthorizedXXXX and assertAuthorizedXXXX methods

7 **Validate Redirects / Forwards**
- OWASP ESAPI: HTTPUtils.sendRedirect method

OWASP
The Open Web Application Security Project

Top 10 steps to address outbound risks.

8 **Content Security Policy**

- Whitelist authorized sources of images, scripts, videos and etc...

9 **Validate inputs**

- To minimize risks from injections.

10 **Inspect outbound traffic**

- Useful as the last safety net, especially when hackers change their attack means.
- Helps to identify sensitive data leakage, display of defaced pages and transmission of compromised infectious pages

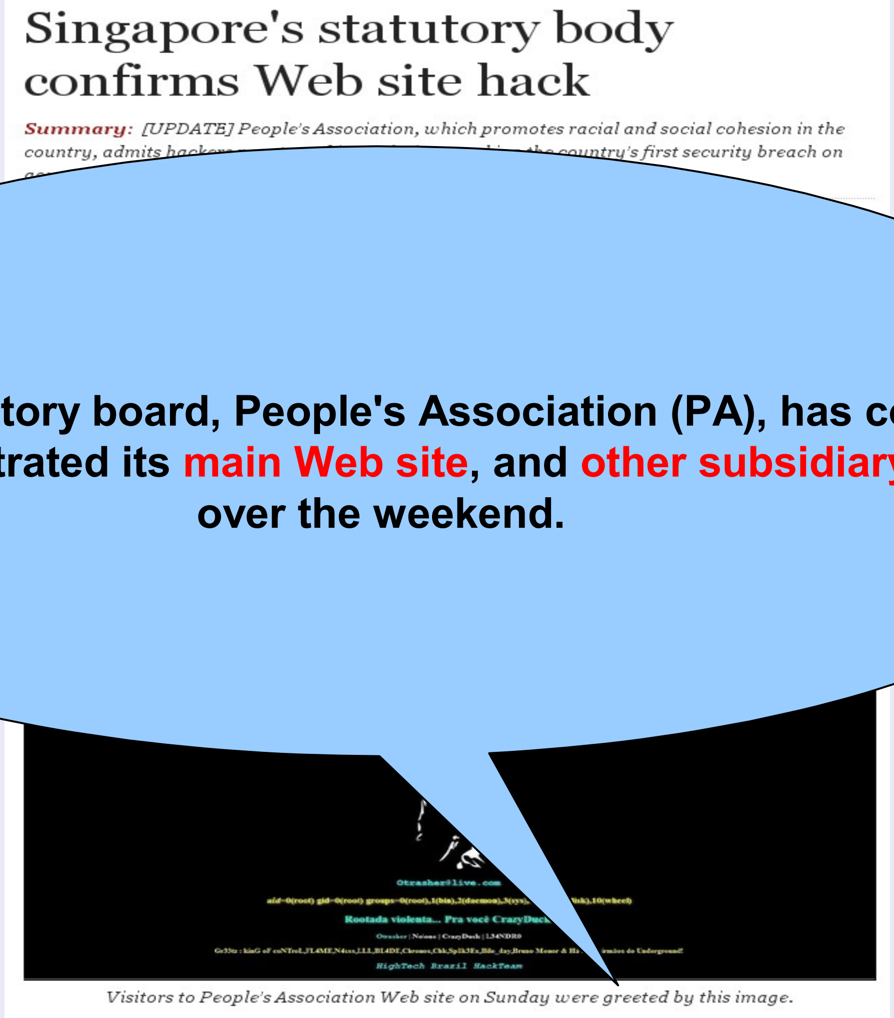
WARNING!

The following slides contain graphic examples which may cause sleepless nights to IT management

OWASP
The Open Web Application Security Project

Scenario 1: Compromised Web Servers

17 websites of People Association, Singapore



Singapore's statutory body confirms Web site hack

Summary: *[UPDATE] People's Association, which promotes racial and social cohesion in the country, admits hacker*

the country's first security breach on

0trasher@live.com
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),
isk),10(wheel)
Rootada violenta... Pra você CrazyDuck
0trasher | Noione | CrazyDuck | L34NDR0
Ge33tz : kinG oF coNTroL,FL4ME,N4sss,LLL,BL4DE,Chronos,Chk,Sp1k3Ex,Bile_day,Bruno Menor & Ha
irmãos do Underground!
HighTech Brazil HackTeam

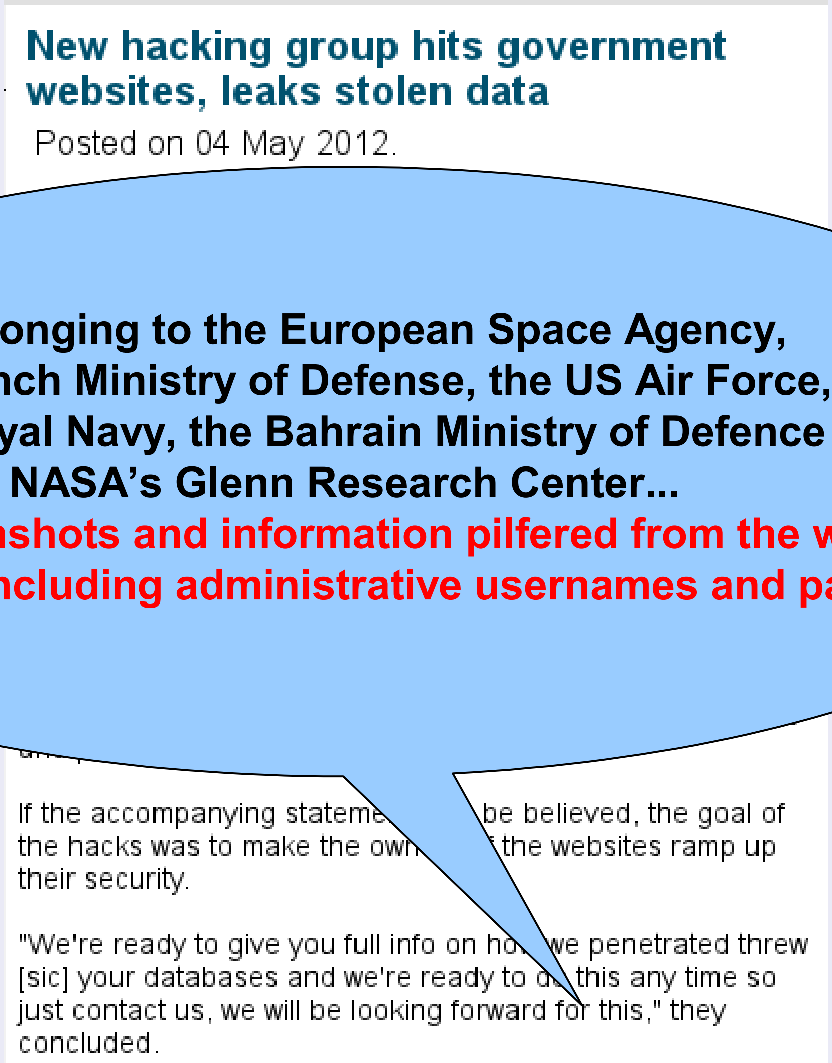
Visitors to People's Association Web site on Sunday were greeted by this image.

Singapore statutory board, People's Association (PA), has confirmed hackers penetrated its main Web site, and other subsidiary sites, over the weekend.

OWASP
The Open Web Application Security Project

Scenario 1: Compromised Web Servers

Military Websites



New hacking group hits government websites, leaks stolen data

Posted on 04 May 2012.

If the accompanying stateme be believed, the goal of the hacks was to make the own the websites ramp up their security.

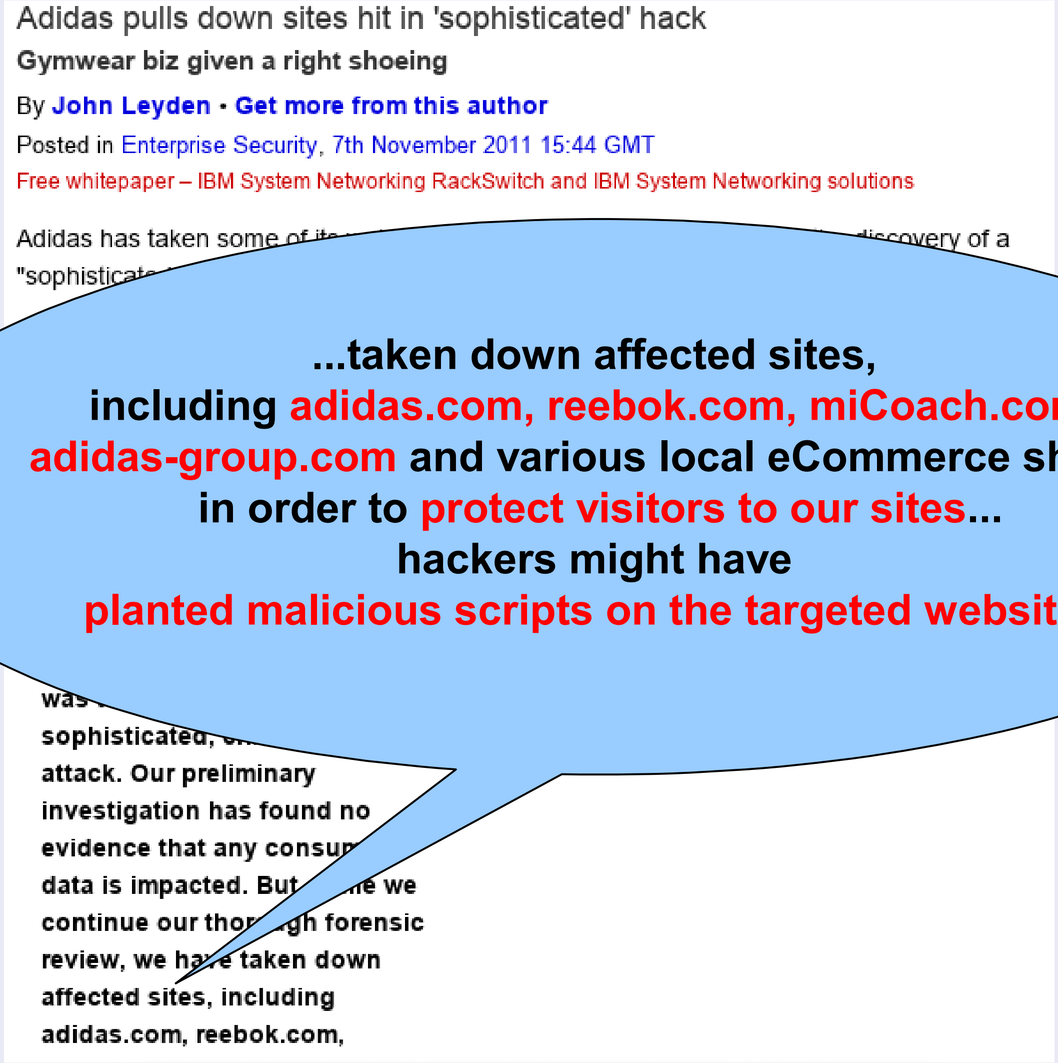
"We're ready to give you full info on ho we penetrated threw [sic] your databases and we're ready to d this any time so just contact us, we will be looking forward for this," they concluded.

....belonging to the European Space Agency, the French Ministry of Defense, the US Air Force, the Thai Royal Navy, the Bahrain Ministry of Defence and NASA's Glenn Research Center...
...posted screenshots and information pilfered from the websites and databases, including administrative usernames and passwords.

Scenario 1: Compromised Web Servers

OWASP
The Open Web Application Security Project

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

Free whitepaper – IBM System Networking RackSwitch and IBM System Networking solutions

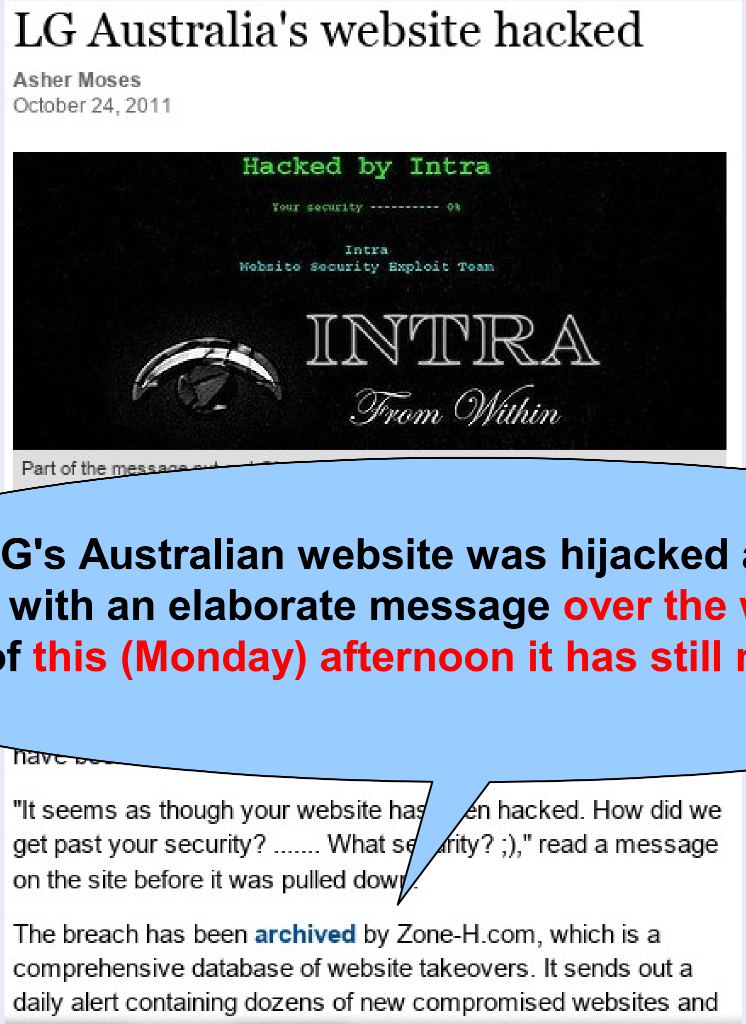
Adidas has taken some of its … discovery of a "sophisticat…

was … sophisticated, … attack. Our preliminary investigation has found no evidence that any consum… data is impacted. But … we continue our thor…gh forensic review, we ha…e taken down affected sites, including adidas.com, reebok.com,

...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...

Scenario 1: Compromised Web Servers

LG Australia



LG Australia's website hacked

Asher Moses
October 24, 2011

Hacked by Intra

Your security --------- 0%

Intra
Website Security Exploit Team

INTRA

From Within

Part of the messa

have bee

"It seems as though your website has en hacked. How did we get past your security? .... What se rity? ;)," read a message on the site before it was pulled dow

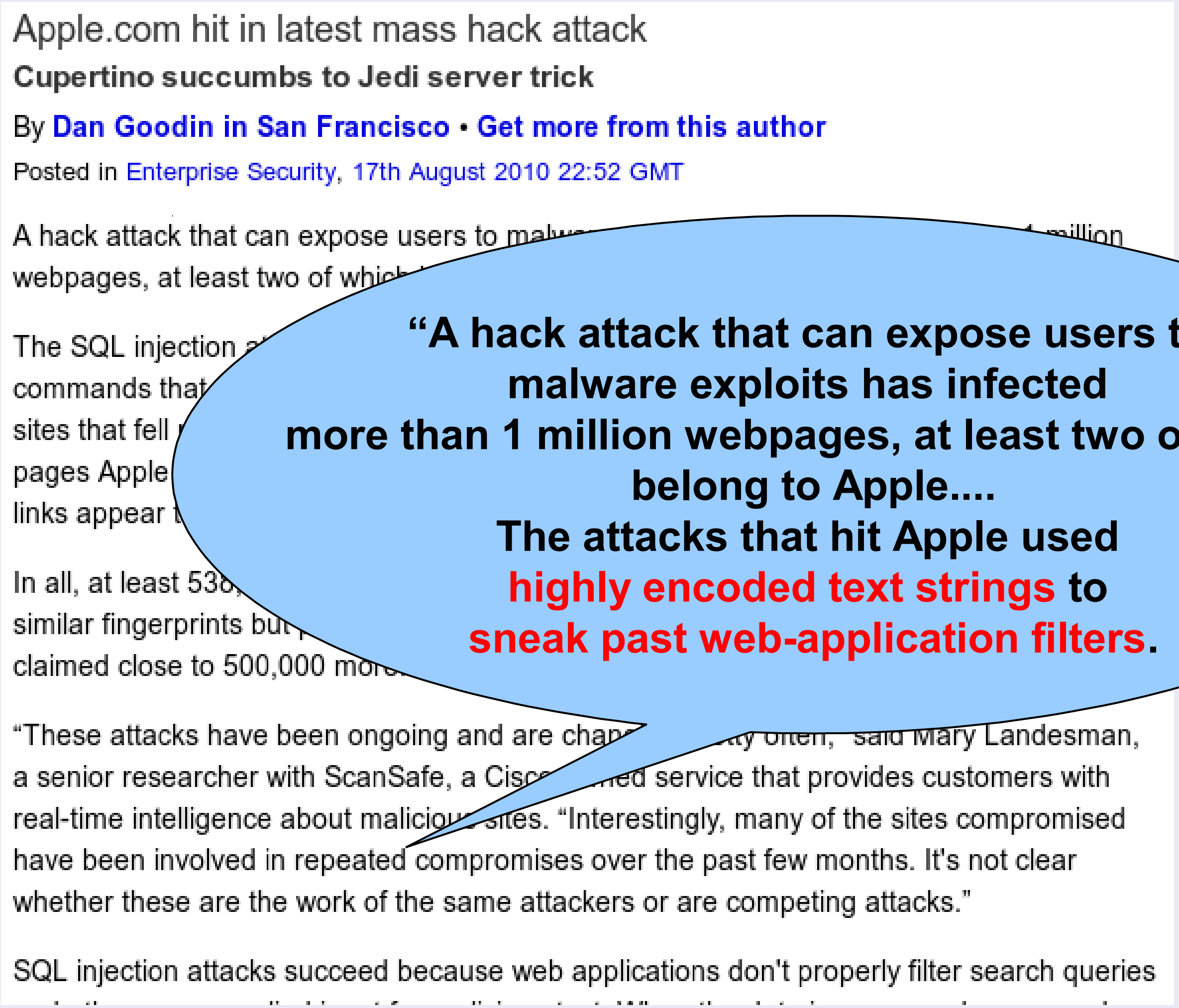
The breach has been **archived** by Zone-H.com, which is a comprehensive database of website takeovers. It sends out a daily alert containing dozens of new compromised websites and

...LG's Australian website was hijacked and defaced with an elaborate message over the weekend and as of this (Monday) afternoon it has still not been restored.

OWASP
The Open Web Application Security Project

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 malw ... 1 million
webpages, at least two of which

The SQL injection a
commands that
sites that fell
pages Apple
links appear t

In all, at least 538,
similar fingerprints but
claimed close to 500,000 mo

“These attacks have been ongoing and are chan ... tly often,” said Mary Landesman,
a senior researcher with ScanSafe, a Cisc ... ned service that provides customers with
real-time intelligence about malicio 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.”

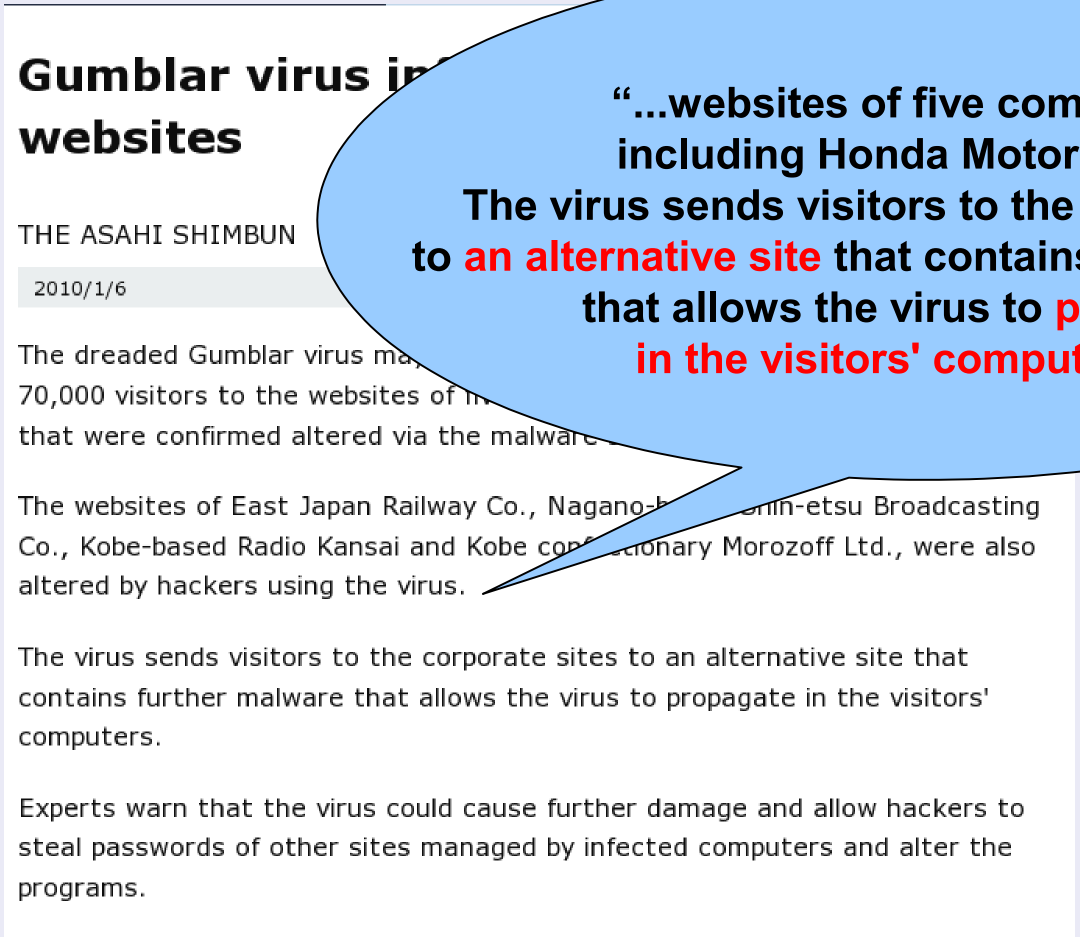
SQL injection attacks succeed because web applications don't properly filter search queries

“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 in
websites

THE ASAHI SHIMBUN

2010/1/6

The dreaded Gumblar virus ma
70,000 visitors to the websites of fi
that were confirmed altered via the malware

The websites of East Japan Railway Co., Nagano-b hin-etsu Broadcasting Co., Kobe-based Radio Kansai and Kobe conf ctionary Morozoff Ltd., were also altered by hackers using the virus.

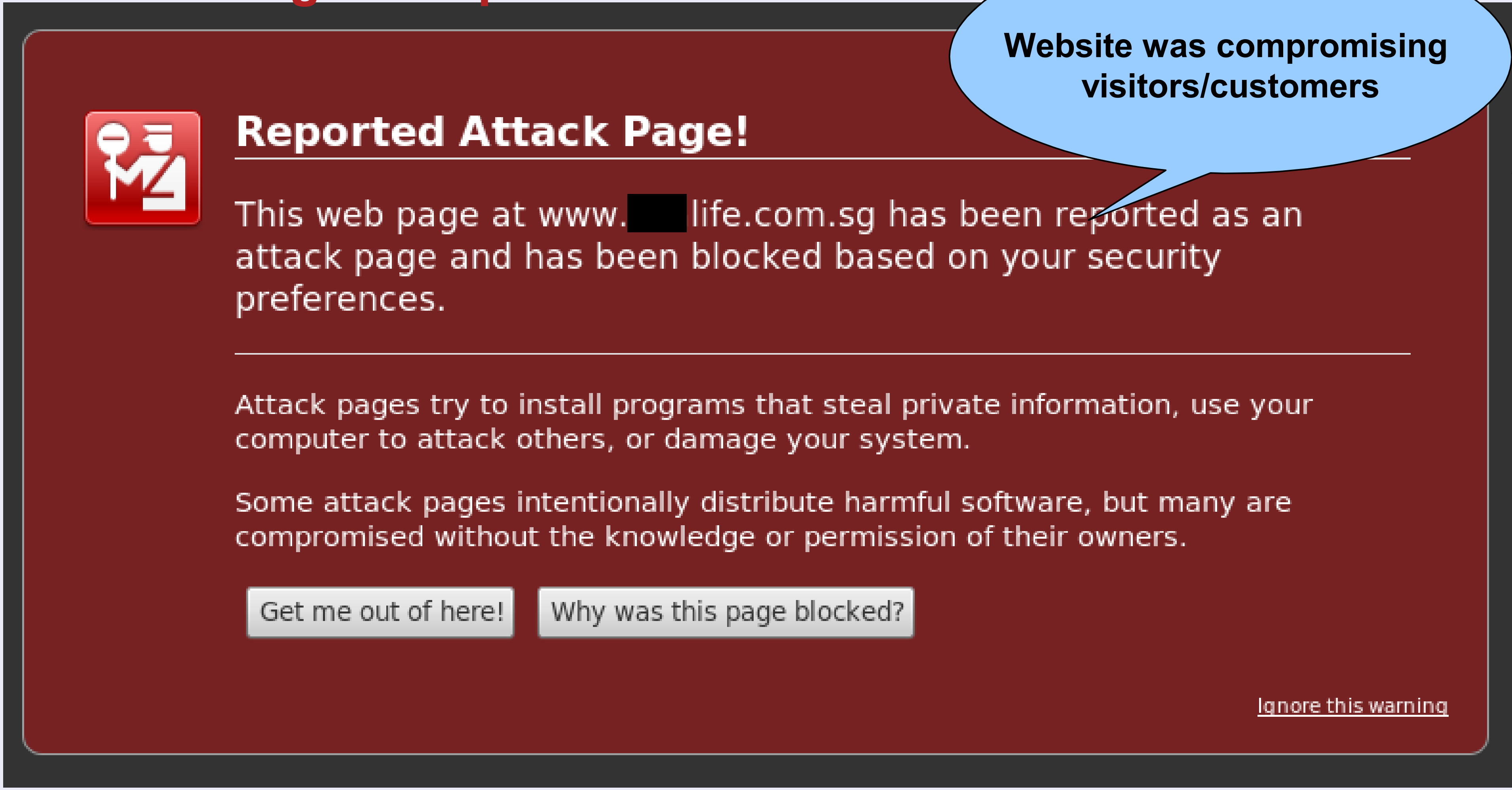
The virus sends visitors to the corporate sites to an alternative site that contains further malware that allows the virus to propagate in the visitors' computers.

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 1: Compromised Web Servers

Large European Insurance Firm in



Reported Attack Page!

This web page at www.[redacted]life.com.sg has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

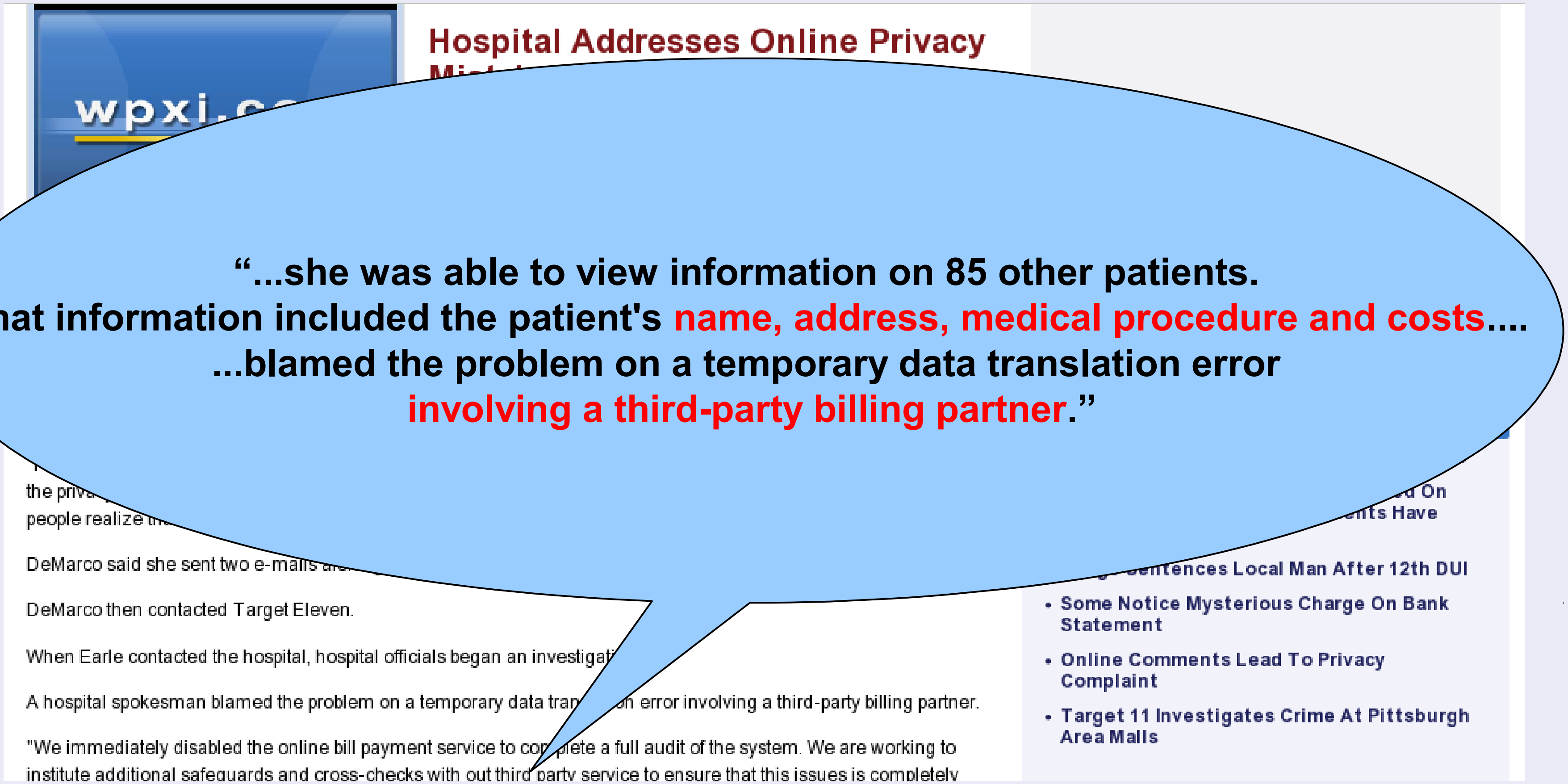
Website was compromising visitors/customers

Scenario 1: Compromised Web Servers

OWASP
The Open Web Application Security Project

West Penn Hospital

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



wpxi.co

Hospital Addresses Online Privacy Mi

the priva

people realize th

DeMarco said she sent two e-mails al

DeMarco then contacted Target Eleven.

When Earle contacted the hospital, hospital officials began an investigati

A hospital spokesman blamed the problem on a temporary data tran on error involving a third-party billing partner.

"We immediately disabled the online bill payment service to co plete a full audit of the system. We are working to institute additional safeguards and cross-checks with out third party service to ensure that this issues is completely

d On
ents Have

entences Local Man After 12th DUI

- Some Notice Mysterious Charge On Bank Statement
- Online Comments Lead To Privacy Complaint
- Target 11 Investigates Crime At Pittsburgh Area Malls

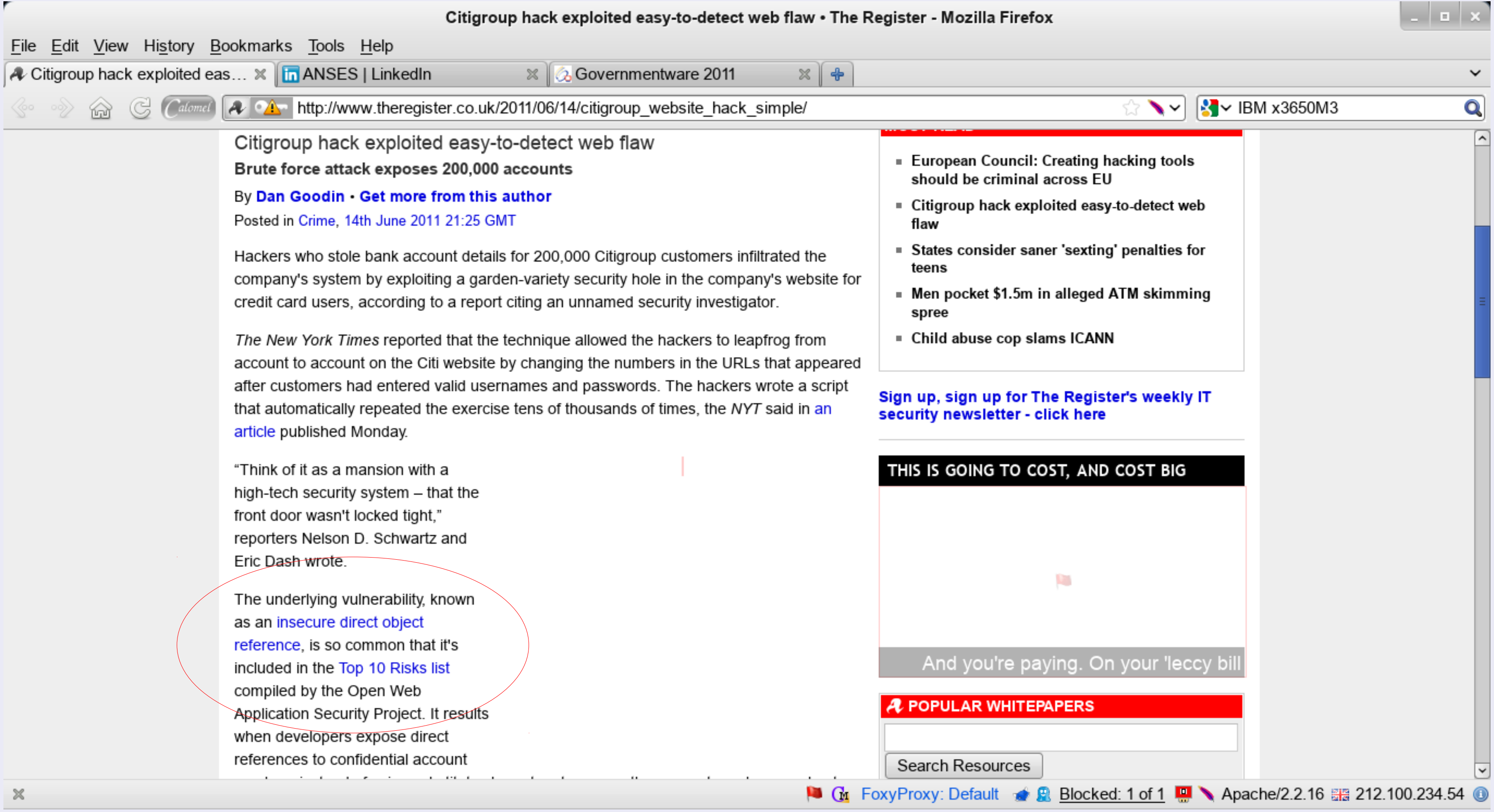
**“...she was able to view information on 85 other patients.
That information included the patient's name, address, medical procedure and costs....
...blamed the problem on a temporary data translation error
involving a third-party billing partner.”**

Scenario 1: Compromised Web Servers

OWASP
The Open Web Application Security Project

Citibank, US

360,000 accounts/credit card information was lost



Citigroup hack exploited easy-to-detect web flaw • The Register - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Citigroup hack exploited eas…
ANSES | LinkedIn
Governmentware 2011
http://www.theregister.co.uk/2011/06/14/citigroup_website_hack_simple/
IBM x3650M3
FoxyProxy: Default
Blocked: 1 of 1
Apache/2.2.16
212.100.234.54

Citigroup hack exploited easy-to-detect web flaw

Brute force attack exposes 200,000 accounts

By **Dan Goodin** • **Get more from this author**

Posted in Crime, 14th June 2011 21:25 GMT

Hackers who stole bank account details for 200,000 Citigroup customers infiltrated the company's system by exploiting a garden-variety security hole in the company's website for credit card users, according to a report citing an unnamed security investigator.

The New York Times reported that the technique allowed the hackers to leapfrog from account to account on the Citi website by changing the numbers in the URLs that appeared after customers had entered valid usernames and passwords. The hackers wrote a script that automatically repeated the exercise tens of thousands of times, the *NYT* said in an article published Monday.

"Think of it as a mansion with a high-tech security system – that the front door wasn't locked tight," reporters Nelson D. Schwartz and Eric Dash wrote.

The underlying vulnerability, known as an insecure direct object reference, is so common that it's included in the Top 10 Risks list compiled by the Open Web Application Security Project. It results when developers expose direct references to confidential account

- **European Council: Creating hacking tools should be criminal across EU**
- **Citigroup hack exploited easy-to-detect web flaw**
- **States consider saner 'sexting' penalties for teens**
- **Men pocket $1.5m in alleged ATM skimming spree**
- **Child abuse cop slams ICANN**

Sign up, sign up for The Register's weekly IT security newsletter - click here

POPULAR WHITEPAPERS

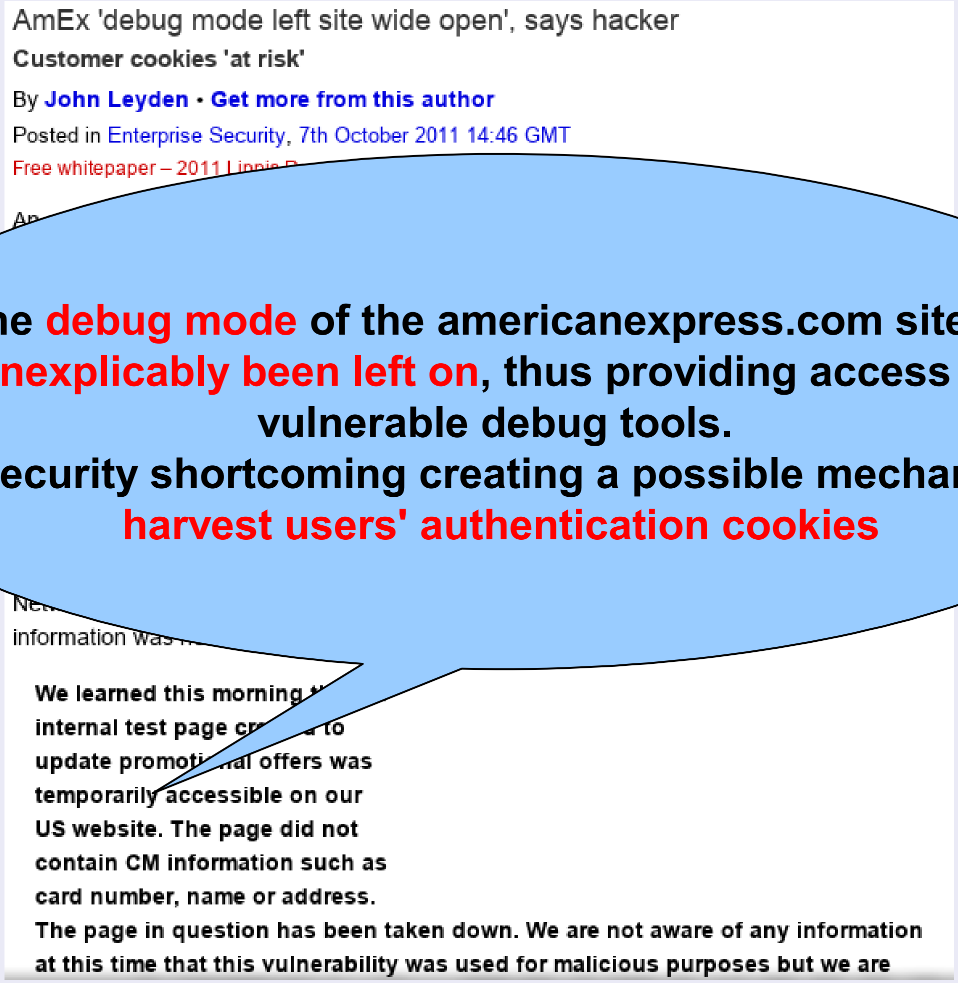
Search Resources

Scenario 3: Misconfiguration

OWASP
The Open Web Application Security Project

American Express

Debug mode accidentally left on.



AmEx 'debug mode left site wide open', says hacker

Customer cookies 'at risk'

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

Posted in Enterprise Security, 7th October 2011 14:46 GMT

Free whitepaper – 2011 Linnis R

An

Net

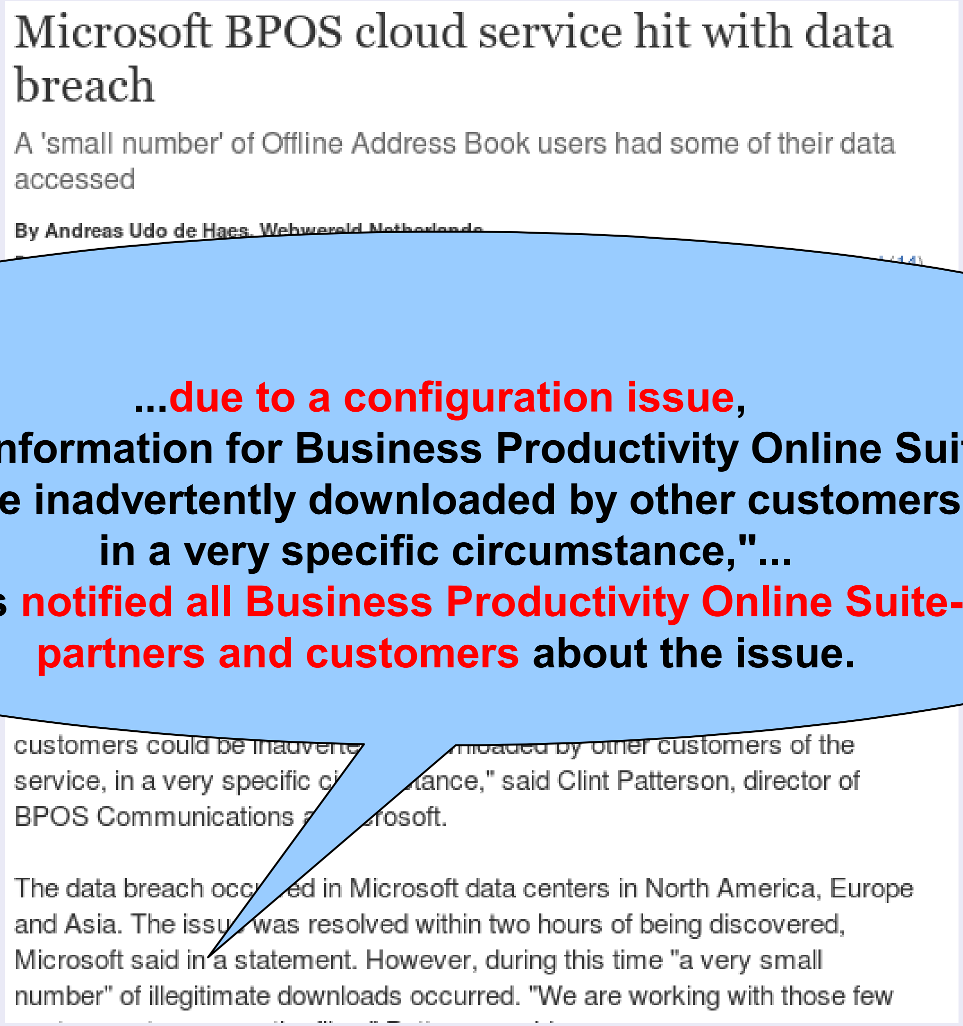
information was n

We learned this morning t
internal test page cr to
update promoti al offers was
temporarily accessible on our
US website. The page did not
contain CM information such as
card number, name or address.
The page in question has been taken down. We are not aware of any information
at this time that this vulnerability was used for malicious purposes but we are

...the debug mode of the americanexpress.com site had inexplicably been left on, thus providing access to vulnerable debug tools.
The security shortcoming creating a possible mechanism to harvest users' authentication cookies

Scenario 3: Misconfiguration

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

customers could be inadverte nloaded by other customers of the service, in a very specific ci tance," said Clint Patterson, director of BPOS Communications a crosoft.

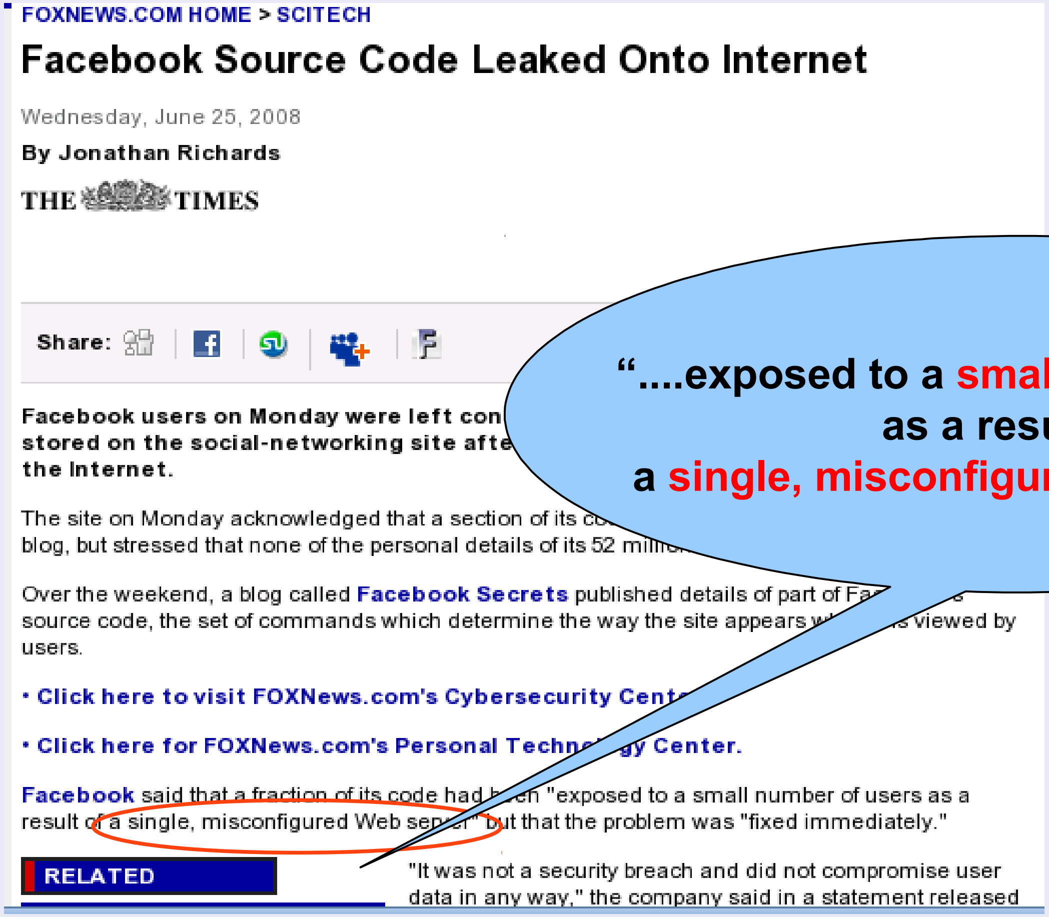
The data breach occ ed in Microsoft data centers in North America, Europe and Asia. The issu was resolved within two hours of being discovered, Microsoft said in a statement. However, during this time "a very small number" of illegitimate downloads occurred. "We are working with those few

...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.

Scenario 3: Misconfiguration

Facebook

Source codes were leaked.



FOXNEWS.COM HOME > SCITECH

Facebook Source Code Leaked Onto Internet

Wednesday, June 25, 2008

By Jonathan Richards

THE TIMES

Share:

**Facebook users on Monday were left con
stored on the social-networking site afte
the Internet.**

The site on Monday acknowledged that a section of its co
blog, but stressed that none of the personal details of its 52 millio

Over the weekend, a blog called **Facebook Secrets** published details of part of Fa
source code, the set of commands which determine the way the site appears w s viewed by
users.

- **Click here to visit FOXNews.com's Cybersecurity Cent**
- **Click here for FOXNews.com's Personal Techn gy Center.**

Facebook said that a fraction of its code had been "exposed to a small number of users as a result of a single, misconfigured Web server" but that the problem was "fixed immediately."

RELATED

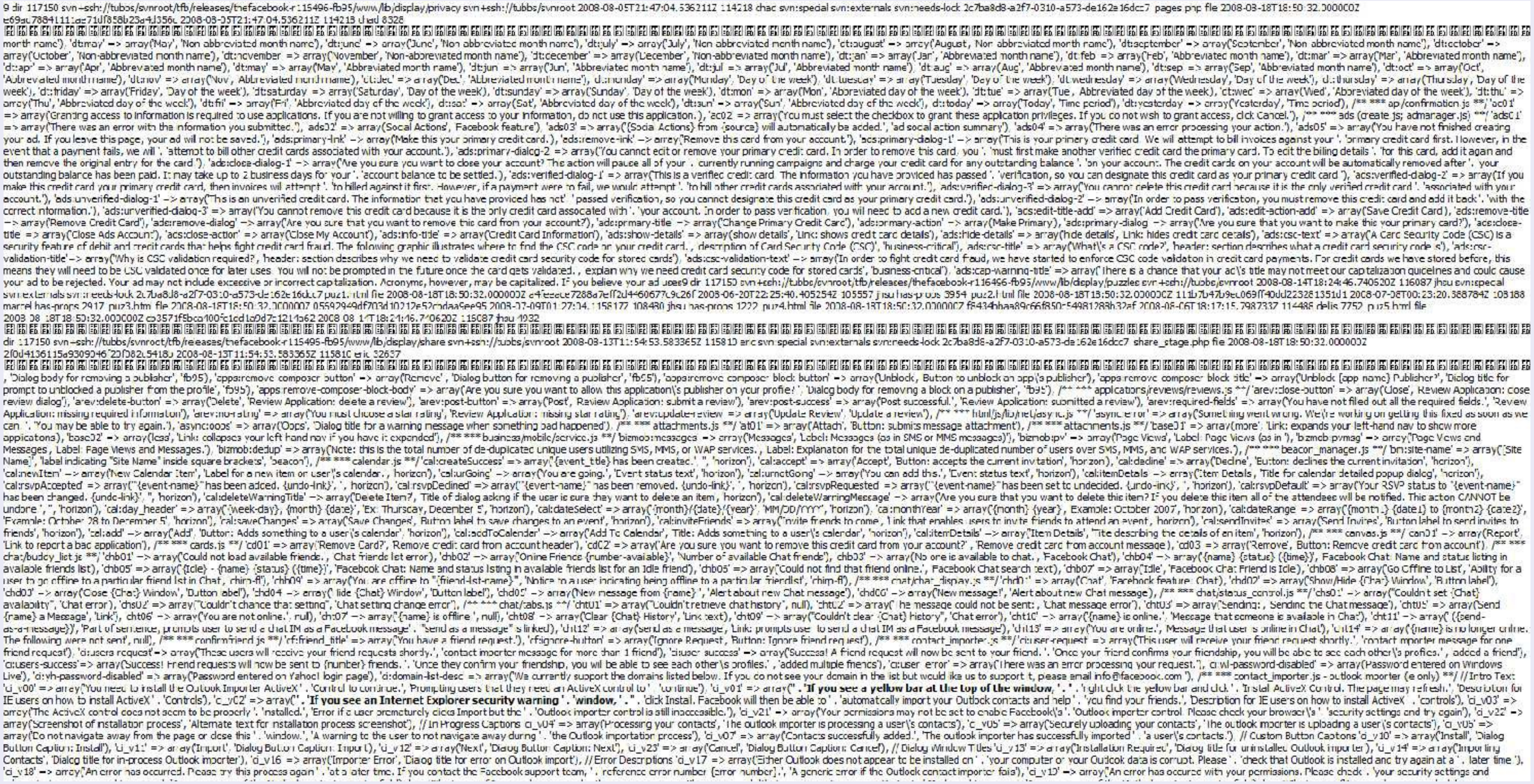
"It was not a security breach and did not compromise user data in any way," the company said in a statement released

**"....exposed to a small number of users
as a result of
a single, misconfigured Web server..."**

Scenario 3: Misconfiguration

Facebook

One of the “small number of users” posted on his blog the source code of Facebook home page



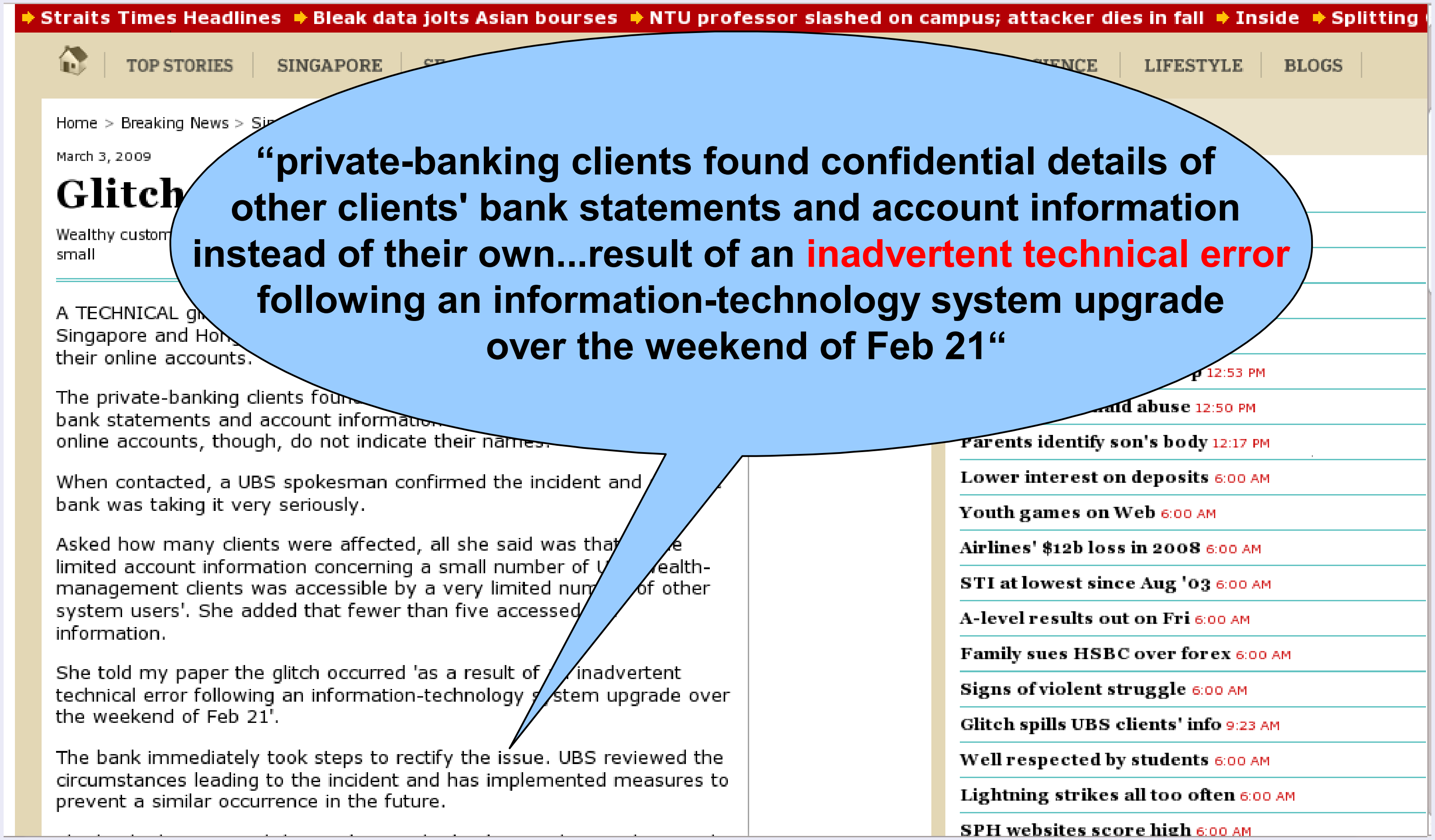
```
9 dir 117150 svn+ssh://tubbs/svnroot/tfb/releases/thefacebook-r115496-fb95/www/lib/display/privacy svn+ssh://tubbs/svnroot 2008-08-05T21:47:04.536211Z 114218 chad svn:special svn:externals svn:needs-lock 2c7ba8d8-a2f7-0310-a573-de162e16dcc7 pages.php file 2008-08-18T18:50:32.000000Z
e69ac7884111ae71df858b23a4d356c 2008-08-05T21:47:04.536211Z 114218 chad 8328
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
month name'), 'dt:may' => array('May', 'Non abbreviated month name'), 'dt:june' => array('June', 'Non abbreviated month name'), 'dt:july' => array('July', 'Non abbreviated month name'), 'dt:august' => array('August', Non abbreviated month name'), 'dt:september' => array('September', 'Non abbreviated month name'), 'dt:october' =>
array('October', 'Non-abbreviated month name'), 'dt:november' => array('November', 'Non-abbreviated month name'), 'dt:december' => array('December', 'Non-abbreviated month name'), 'dt:jan' => array('Jan', 'Abbreviated month name'), 'dt:feb' => array('Feb', 'Abbreviated month name'), 'dt:mar' => array('Mar', 'Abbreviated month name'),
'dt:apr' => array('Apr', 'Abbreviated month name'), 'dt:may' => array('May', 'Abbreviated month name'), 'dt:jun' => array('Jun', 'Abbreviated month name'), 'dt:jul' => array('Jul', 'Abbreviated month name'), 'dt:aug' => array(Aug', 'Abbreviated month name'), 'dt:sep' => array('Sep', 'Abbreviated month name'), 'dt:oct' => array('Oct',
'Abbreviated month name'), 'dt:nov' => array('Nov', Abbreviated month name'), 'dt:dec' => array('Dec', 'Abbreviated month name'), dt:monday' => array('Monday', 'Day of the week'), 'dt:tuesday' => array('Tuesday', 'Day of the week'), 'dt:wednesday' => array('Wednesday', 'Day of the week'), dt:thursday' => array('Thursday', 'Day of the
week'), 'dt:friday' => array('Friday', 'Day of the week'), 'dt:saturday' => array('Saturday', 'Day of the week'), 'dt:sunday' => array('Sunday', 'Day of the week'), 'dt:mon' => array('Mon', 'Abbreviated day of the week'), 'dt:tue' => array('Tue', Abbreviated day of the week'), 'dt:wed' => array('Wed', 'Abbreviated day of the week'), 'dt:thu' =>
array('Thu', 'Abbreviated day of the week'), 'dt:fri' => array('Fri', 'Abbreviated day of the week'), dt:sat' => array('Sat', 'Abbreviated day of the week'), 'dt:sun' => array('Sun', 'Abbreviated day of the week'), dt:today' => array('Today', 'Time period'), 'dt:yesterday' => array('Yesterday', 'Time period'), /** *** ap/confirmation.js **/ 'ac01'
=> array('Granting access to information is required to use applications. If you are not willing to grant access to your information, do not use this application.'), 'ac02' => array('You must select the checkbox to grant these application privileges. If you do not wish to grant access, click Cancel.'), /** *** ads (create.js; admanager.js) **/ 'ads01'
=> array('There was an error with the information you submitted.'), 'ads02' => array(Social Actions', Facebook feature'), 'ads03' => array('{Social Actions} from {source} will automatically be added.', 'ad social action summary'), 'ads04' => array('There was an error processing your action.'), 'ads05' => array('You have not finished creating
your ad. If you leave this page, your ad will not be saved.'), 'ads:primary-link' => array('Make this your primary credit card.'), 'ads:remove-link' => array('Remove this card from your account.'), 'ads:primary-dialog-1' => array('This is your primary credit card. We will attempt to bill invoices against your '. 'primary credit card first. However, in the
event that a payment fails, we will '. 'attempt to bill other credit cards associated with your account.'), 'ads:primary-dialog-2' => array('You cannot edit or remove your primary credit card. In order to remove this card, you '. 'must first make another verified credit card the primary card. To edit the billing details '. 'for this card, add it again and
then remove the original entry for the card.'), 'ads:close-dialog-1' => array('Are you sure you want to close your account? The action will pause all of your '. 'currently running campaigns and charge your credit card for any outstanding balance '. 'on your account. The credit cards on your account will be automatically removed after '. 'your
outstanding balance has been paid. It may take up to 2 business days for your '. 'account balance to be settled.'), 'ads:verified-dialog-1' => array('This is a verified credit card. The information you have provided has passed '. 'verification, so you can designate this credit card as your primary credit card.'), 'ads:verified-dialog-2' => array('If you
make this credit card your primary credit card, then invoices will attempt '. 'to billed against it first. However, if a payment were to fail, we would attempt '. 'to bill other credit cards associated with your account.'), 'ads:verified-dialog-3' => array('You cannot delete this credit card because it is the only verified credit card '. 'associated with your
account.'), 'ads:unverified-dialog-1' => array('This is an unverified credit card. The information that you have provided has not '. 'passed verification, so you cannot designate this credit card as your primary credit card.'), 'ads:unverified-dialog-2' => array('In order to pass verification, you must remove this credit card and add it back '. 'with the
correct information.'), 'ads:unverified-dialog-3' => array('You cannot remove this credit card because it is the only credit card associated with '. 'your account. In order to pass verification, you will need to add a new credit card.'), 'ads:edit-title-add' => array('Add Credit Card'), 'ads:edit-action-add' => array('Save Credit Card'), 'ads:remove-title'
=> array('Remove Credit Card'), 'ads:remove-dialog' => array('Are you sure that you want to remove this card from your account?'), 'ads:primary-title' => array('Change Primary Credit Card'), 'ads:primary-action' => array(Make Primary'), 'ads:primary-dialog' => array('Are you sure that you want to make this your primary card?'), 'ads:close-
title' => array('Close Ads Account'), 'ads:close-action' => array('Close My Account'), 'ads:info-title' => array('Credit Card Information'), 'ads:show-details' => array(show details', 'Link: shows credit card details'), 'ads:hide-details' => array(hide details', Link: hides credit card details'), 'ads:csc-text' => array('A Card Security Code (CSC) is a
security feature of debit and credit cards that helps fight credit card fraud. The following graphic illustrates where to find the CSC code on your credit card.', 'description of Card Security Code (CSC)', 'business-critical'), 'ads:csc-title' => array('What\'s a CSC code?', 'header: section describes what a credit card security code is'), 'ads:csc-
validation-title' => array('Why is CSC validation required?', 'header: section describes why we need to validate credit card security code for stored cards'), 'ads:csc-validation-text' => array('In order to fight credit card fraud, we have started to enforce CSC code validation in credit card payments. For credit cards we have stored before, this
means they will need to be CSC validated once for later uses. You will not be prompted in the future once the card gets validated.', 'explain why we need credit card security code for stored cards', 'business-critical'), 'ads:cap-warning-title' => array('There is a chance that your ad\'s title may not meet our capitalization guidelines and could cause
your ad to be rejected. Your ad may not include excessive or incorrect capitalization. Acronyms, however, may be capitalized. If you believe your ad uses9 dir 117150 svn+ssh://tubbs/svnroot/tfb/releases/thefacebook-r116496-fb95/www/lib/display/puzzles svn+ssh://tubbs/svnroot 2008-08-14T18:24:46.740520Z 116087 jhsu svn:special
svn:externals svn:needs-lock 2c7ba8d8-a2f7-0310-a573-de162e16dcc7 puz1.html file 2008-08-18T18:50:32.000000Z e4feeace7288a7eff2d4460677c9c26f 2008-06-20T22:25:40.405254Z 105557 jhsu has-props 3954 puz2.html file 2008-08-18T18:50:32.000000Z 111b7b47b9ec069ff40dd223281351d1 2008-07-08T00:23:20.388784Z 108188
marcel has-props 2917 puz3.htm file 2008-08-18T18:50:32.000000Z 05592949df703d10212e52cdaa5ee95 2008-07-09T01:27:04.115817Z 108480 jhsu has-props 1222 puz4.html file 2008-08-18T18:50:32.000000Z f8434bbaa89c66f850c54981288b32ef 2008-08-06T18:17:15.798733Z 114486 delis 7752 puz5.html file
2008-08-18T18:50:32.000000Z c53571f5bca100fc1cd1a0d7e1211a62 2008-08-14T18:24:46.740620Z 116087 jhsu 1932
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
dir 117150 svn+ssh://tubbs/svnroot/tfb/releases/thefacebook-r115495-fb95/www/lib/display/share svn+ssh://tubbs/svnroot 2008-08-13T11:54:53.583365Z 115810 eric svn:special svn:externals svn:needs-lock 2c7ba8d8-a2f7-0310-a573-de162e16dcc7 share_stage.php file 2008-08-18T18:50:32.000000Z
2f0d4136115a9309046`20f082c5418b 2008-08-13T11:54:53.583365Z 115810 eric 32637
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
, 'Dialog body for removing a publisher', 'fb95'), 'apps:remove composer button' => array('Remove', 'Dialog button for removing a publisher', 'fb95'), 'apps:remove composer block button' => array(Unblock, Button to unblock an app\'s publisher'), 'apps:remove composer block title' => array('Unblock {app name} Publisher?', 'Dialog title for
prompt to unblocked a publisher from the profile', 'fb95'), 'apps:remove-composer-block-body' => array('Are you sure you want to allow this application\'s publisher on your profile?', 'Dialog body for removing a block on a publisher', 'fb95'), /** *** applications/reviews/reviews.js **/ 'arev:close-button' => array('Close', 'Review Application: close
review dialog'), 'arev:delete-button' => array('Delete', 'Review Application: delete a review'), 'arev:post-button' => array('Post', Review Application: submit a review'), 'arev:post-success' => array('Post successful.', 'Review Application: submitted a review'), 'arev:required-fields' => array('You have not filled out all the required fields.', 'Review
Application: missing required information'), 'arev:no-rating' => array('You must choose a star rating', 'Review Application: missing star rating'), 'arev:update-review' => array('Update Review', 'Update a review'), /** *** html/js/lib/net/async.js **/ 'async:error' => array('Something went wrong. We\'re working on getting this fixed as soon as we
can. '. 'You may be able to try again.'), 'async:oops' => array('Oops', 'Dialog title for a warning message when something bad happened'), /** *** attachments.js **/ 'at01' => array('Attach', 'Button: submits message attachment'), /** *** attachments.js **/ 'base01' => array(more', 'Link: expands your left-hand nav to show more
applications'), 'base02' => array(less', 'Link: collapses your left hand nav if you have it expanded'), /** *** business/mobile/service.js **/ 'bizmob:messages' => array('Messages', 'Label: Messages (as in SMS or MMS messages)'), 'bizmob:pv' => array('Page Views', 'Label: Page Views (as in ')', 'bizmob:pvmsg' => array('Page Views and
Messages', Label: Page Views and Messages.'), 'bizmob:dedup' => array('Note: this is the total number of de-duplicated unique users utilizing SMS, MMS, or WAP services.', Label: Explanation for the total unique de-duplicated number of users over SMS, MMS, and WAP services.'), /** *** beacon_manager.js **/ 'bm:site-name' => array('[Site
Name]', 'label indicating "Site Name" inside square brackets', 'beacon'), /** *** calendar.js **/ 'cal:createSuccess' => array('{event_title} has been created.', '', 'horizon'), 'cal:accept' => array('Accept', 'Button: accepts the current invitation', 'horizon'), 'cal:decline' => array('Decline', 'Button: declines the current invitation', 'horizon'),
'cal:newItem' => array('New Calendar Item', 'Label for a new item on user\'s calendar.', 'horizon'), 'cal:urGoing' => array('You are going.', 'Event status text', 'horizon'), 'cal:urnotGoing' => array('You can add this.', 'Event status text', 'horizon'), 'cal:itemDetails' => array('Item Details', 'Title for calendar detailed popup dialog', 'horizon'),
'cal:rsvpAccepted' => array('"{event-name}" has been added. {undo-link}', '', 'horizon'), 'cal:rsvpDeclined' => array('"{event-name}" has been removed. {undo-link}', '', 'horizon'), 'cal:rsvpRequested' => array('"{event-name}" has been set to undecided. {undo-link}', '', 'horizon'), 'cal:rsvpDefault' => array('Your RSVP status to "{event-name}"
has been changed. {undo-link}', '', 'horizon'), 'cal:deleteWarningTitle' => array('Delete Item?', Title of dialog asking if the user is sure they want to delete an item', 'horizon'), 'cal:deleteWarningMessage' => array('Are you sure that you want to delete this item? If you delete this item all of the attendees will be notified. This action CANNOT be
undone.', '', 'horizon'), 'cal:day_header' => array('{week-day}, {month} {date}', 'Ex: Thursday, December 5', 'horizon'), 'cal:dateSelect' => array('{month}/{date}/{year}', 'MM/DD/YYYY', 'horizon'), 'cal:monthYear' => array('{month} {year}', Example: October 2007', 'horizon'), 'cal:dateRange' => array('{month1} {date1} to {month2} {date2}',
'Example: October 28 to December 5', 'horizon'), 'cal:saveChanges' => array('Save Changes', Button label to save changes to an event', 'horizon'), 'cal:inviteFriends' => array('Invite friends to come', 'Link that enables users to invite friends to attend an event', 'horizon'), 'cal:sendInvites' => array('Send Invites', 'Button label to send invites to
friends', 'horizon'), 'cal:add' => array('Add', 'Button: Adds something to a user\'s calendar', 'horizon'), 'cal:addToCalendar' => array('Add To Calendar', Title: Adds something to a user\'s calendar', 'horizon'), 'cal:itemDetails' => array('Item Details', 'Title describing the details of an item', 'horizon'), /** *** canvas.js **/ 'can01' => array('Report',
'Link to report a bad application'), /** *** cards.js **/ 'cd01' => array('Remove Card?', 'Remove credit card from account header'), 'cd02' => array('Are you sure you want to remove this credit card from your account?', 'Remove credit card from account message'), 'cd03' => array('Remove', 'Button: Remove credit card from account'), /** ***
chat/buddy_list.js **/ 'chb01' => array('Could not load available friends.', 'Chat friends list error'), 'chb02' => array('Online Friends {number-available}', 'Number of available Chat friends'), chb03' => array('No one is available to chat.', 'Facebook Chat'), 'chb04' => array('{name} {status} ({time})', Facebook Chat: Name and status listing in
available friends list'), 'chb05' => array('{Idle} - {name} {status} ({time})', 'Facebook Chat: Name and status listing in available friends list for an Idle friend'), 'chb06' => array('Could not find that friend online.', Facebook Chat search text'), 'chb07' => array('Idle', 'Facebook Chat: Friend is Idle'), 'chb08' => array('Go Offline to List', 'Ability for a
user to go offline to a particular friend list in Chat', 'chirp-fl'), 'chb09' => array('You are offline to "{friend-list-name}"', 'Notice to a user indicating being offline to a particular friendlist', 'chirp-fl'), /** *** chat/chat_display.js **/ 'chd01' => array('Chat', 'Facebook feature: Chat'), 'chd02' => array('Show/Hide {Chat} Window', 'Button label'),
'chd03' => array('Close {Chat} Window', 'Button label'), 'chd04' => array('Hide {Chat} Window', 'Button label'), 'chd05' => array('New message from {name}', 'Alert about new Chat message'), 'chd06' => array('New message!', 'Alert about new Chat message'), /** *** chat/status_control.js **/ 'chs01' => array("Couldn't set {Chat}
availability", 'Chat error'), 'chs02' => array("Couldn't change that setting", 'Chat setting change error'), /** *** chat/tabs.js **/ 'cht01' => array("Couldn't retrieve chat history", null), 'cht02' => array('The message could not be sent:', 'Chat message error'), 'cht03' => array('Sending:', 'Sending the Chat message'), 'cht05' => array('Send
{name} a Message', 'Link'), cht06' => array('You are not online.', null), 'cht07' => array('{name} is offline.', null), 'cht08' => array('Clear {Chat} History', 'Link text'), 'cht09' => array("Couldn't clear {Chat} history", 'Chat error'), 'cht10' => array('{name} is online.', 'Message that someone is available in Chat'), 'cht11' => array('({send-
as-a-message})', 'Part of sentence, prompts user to send a chat IM as a Facebook message', '"send as a message" is linked'), 'cht12' => array('send as a message', 'Link: prompts user to send a chat IM as a Facebook message'), 'cht13' => array('You are online.', 'Message that user is online in Chat'), 'cht14' => array('{name} is no longer online.
The following were not sent', null), /** *** confirmfriend.js **/ 'cf:friend_title' => array('You have a friend request.'), 'cf:ignore-button' => array('Ignore Request', 'Button: Ignore friend request'), /** *** contact_importer.js **/ 'ci:user-request' => array('This user will receive your friend request shortly.', 'contact importer message for one
friend request'), 'ci:users-request' => array('These users will receive your friend requests shortly.', 'contact importer message for more than 1 friend'), 'ci:user-success' => array('Success! A friend request will now be sent to your friend. '. 'Once your friend confirms your friendship, you will be able to see each other\'s profiles.', 'added a friend'),
'ci:users-success' => array('Success! Friend requests will now be sent to {number} friends. '. 'Once they confirm your friendship, you will be able to see each other\'s profiles.', 'added multiple friends'), 'ci:user-error' => array('There was an error processing your request.'), 'ci:wl-password-disabled' => array('Password entered on Windows
Live'), 'ci:yh-password-disabled' => array('Password entered on Yahoo! login page'), 'ci:domain-list-desc' => array('We currently support the domains listed below. If you do not see your domain in the list but would like us to support it, please email info@facebook.com '), /** *** contact_importer.js - outlook importer (ie only) **/ //Intro Text
'ci_v00' => array('You need to install the Outlook Importer ActiveX' . 'Control to continue.', 'Prompting users that they need an ActiveX control to ' . 'continue'), 'ci_v01' => array('' . 'If you see a yellow bar at the top of the window, ' . '' . 'right click the yellow bar and click ' . 'Install ActiveX Control. The page may refresh.', 'Description for
IE users on how to install ActiveX' . 'Controls'), 'ci_v02' => array('' . 'If you see an Internet Explorer security warning ' . 'window, ' . '' . 'click Install. Facebook will then be able to ' . 'automatically import your Outlook contacts and help ' . 'you find your friends.', 'Description for IE users on how to install ActiveX ' . 'controls'), 'ci_v03' =>
array('The ActiveX control does not seem to be properly '. 'installed.', 'Error if a user prematurely clicks Import but the ' . 'Outlook importer control is still inaccessible.'), 'ci_v21' => array('Your permissions may not be set to enable Facebook\'s ' . 'Outlook importer control. Please check your browser\'s ' . 'security settings and try again'), 'ci_v22' =>
array('Screenshot of installation process', 'Alternate text for installation process screenshot'), // In Progress Captions 'ci_v04' => array('Processing your contacts', 'The outlook importer is processing a user\'s contacts'), 'ci_v05' => array('Securely uploading your contacts', 'The outlook importer is uploading a user\'s contacts'), 'ci_v06' =>
array('Do not navigate away from the page or close this ' . 'window.', 'A warning to the user to not navigate away during ' . 'the Outlook importation process'), 'ci_v07' => array('Contacts successfully added.', 'The outlook importer has successfully imported ' . 'a user\'s contacts.'), // Custom Button Captions 'ci_v10' => array('Install', 'Dialog
Button Caption: Install'), 'ci_v11' => array('Import', 'Dialog Button Caption: Import'), 'ci_v12' => array('Next', 'Dialog Button Caption: Next'), 'ci_v23' => array('Cancel', 'Dialog Button Caption: Cancel'), // Dialog Window Titles 'ci_v13' => array('Installation Required', 'Dialog title for uninstalled Outlook importer'), 'ci_v14' => array('Importing
Contacts', 'Dialog title for in-process Outlook importer'), 'ci_v16' => array('Importer Error', 'Dialog title for error on Outlook import'), // Error Descriptions 'ci_v17' => array('Either Outlook does not appear to be installed on ' . 'your computer or your Outlook data is corrupt. Please ' . 'check that Outlook is installed and try again at a ' . 'later time.'),
'ci_v18' => array('An error has occurred. Please try this process again ' . 'at a later time. If you contact the Facebook support team, ' . 'reference error number {error number}.', 'A generic error if the Outlook contact importer fails'), 'ci_v19' => array('An error has occurred with your permissions. Please check ' . 'your security settings and
```

OWASP
The Open Web Application Security Project

Scenario 3: Misconfiguration

UBS

Bank customer records were leaked during system upgrade



Straits Times Headlines Bleak data jolts Asian bourses NTU professor slashed on campus; attacker dies in fall Inside Splitting

TOP STORIES | SINGAPORE | SE… …IENCE | LIFESTYLE | BLOGS

Home > Breaking News > Si

March 3, 2009

Glitch

Wealthy custom
small

A TECHNICAL gl
Singapore and Hon
their online accounts.

The private-banking clients foun
bank statements and account informatio
online accounts, though, do not indicate their names.

When contacted, a UBS spokesman confirmed the incident and
bank was taking it very seriously.

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

She told my paper the glitch occurred 'as a result of inadvertent
technical error following an information-technology ystem upgrade over
the weekend of Feb 21'.

The bank immediately took steps to rectify the issue. UBS reviewed the circumstances leading to the incident and has implemented measures to prevent a similar occurrence in the future.

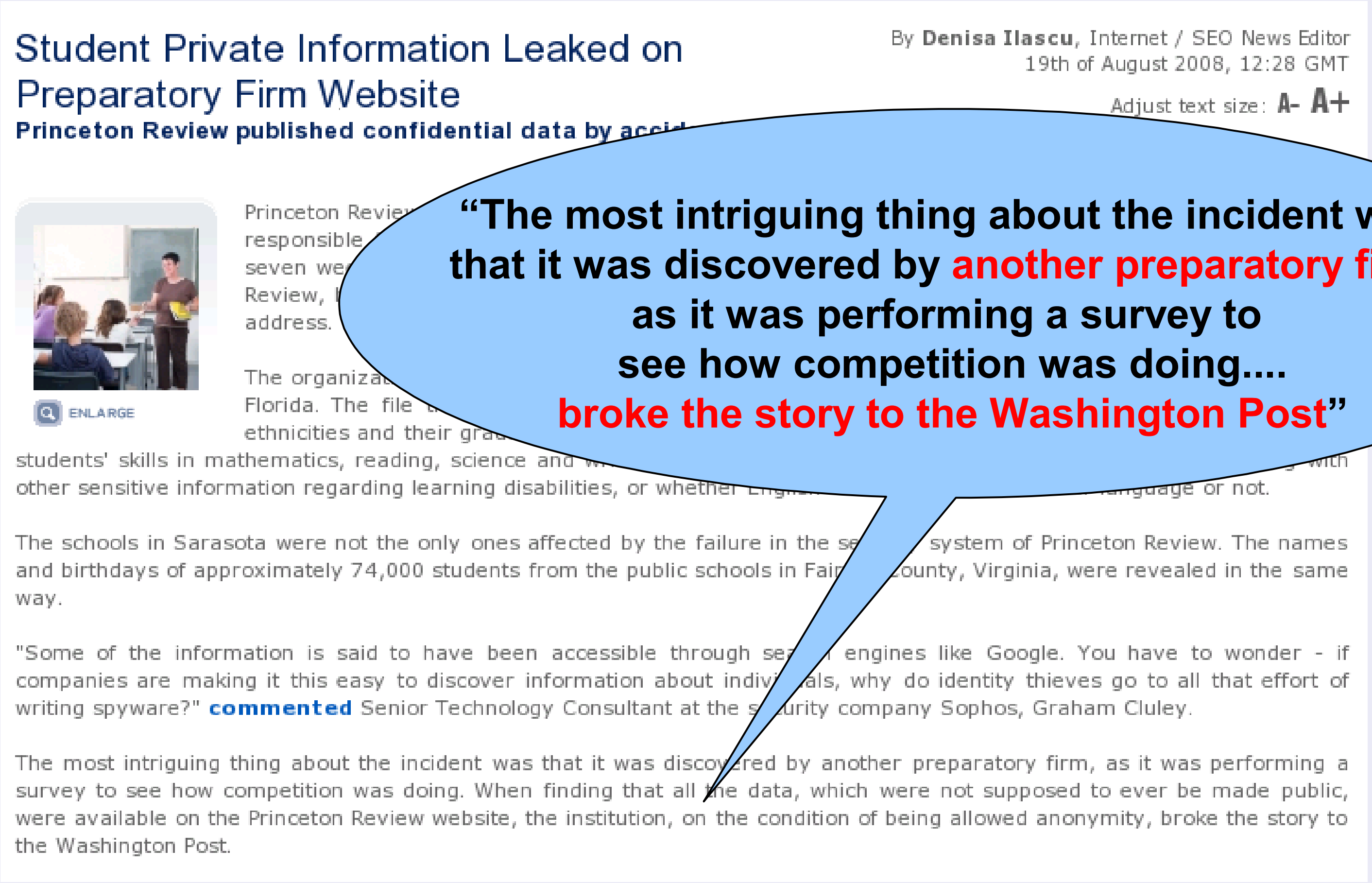
p 12:53 PM
aid abuse 12:50 PM
Parents identify son's body 12:17 PM
Lower interest on deposits 6:00 AM
Youth games on Web 6:00 AM
Airlines' $12b loss in 2008 6:00 AM
STI at lowest since Aug '03 6:00 AM
A-level results out on Fri 6:00 AM
Family sues HSBC over forex 6:00 AM
Signs of violent struggle 6:00 AM
Glitch spills UBS clients' info 9:23 AM
Well respected by students 6:00 AM
Lightning strikes all too often 6:00 AM
SPH websites score high 6:00 AM

"private-banking clients found confidential details of other clients' bank statements and account information instead of their own...result of an inadvertent technical error following an information-technology system upgrade over the weekend of Feb 21"

Scenario 4: Negligence

Princeton Review

108,000 student records were leaked



Student Private Information Leaked on Preparatory Firm Website

Princeton Review published confidential data by accid

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

Princeton Revie
responsible
seven we
Review,
address.

The organiza
Florida. The file
ethnicities and their gra
students' skills in mathematics, reading, science and w with
other sensitive information regarding learning disabilities, or whether Englis language or not.

The schools in Sarasota were not the only ones affected by the failure in the se system of Princeton Review. The names and birthdays of approximately 74,000 students from the public schools in Fair ounty, Virginia, were revealed in the same way.

"Some of the information is said to have been accessible through sea engines like Google. You have to wonder - if companies are making it this easy to discover information about indivi als, why do identity thieves go to all that effort of writing spyware?" **commented** Senior Technology Consultant at the s urity company Sophos, Graham Cluley.

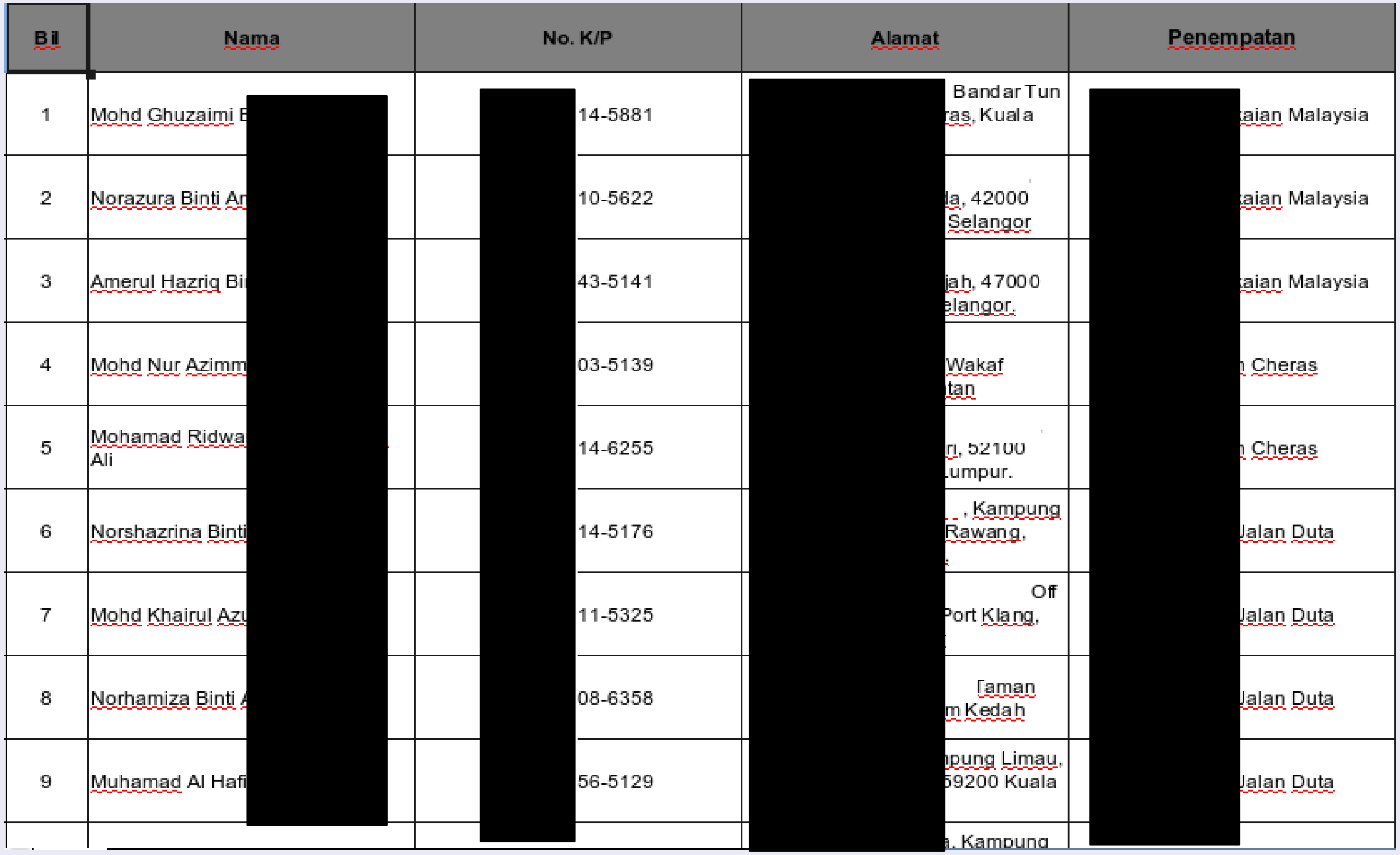
The most intriguing thing about the incident was that it was disco ered by another preparatory firm, as it was performing a survey to see how competition was doing. When finding that all the data, which were not supposed to ever be made public, were available on the Princeton Review website, the institution, 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: Negligence

Government Agency, Malaysia

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

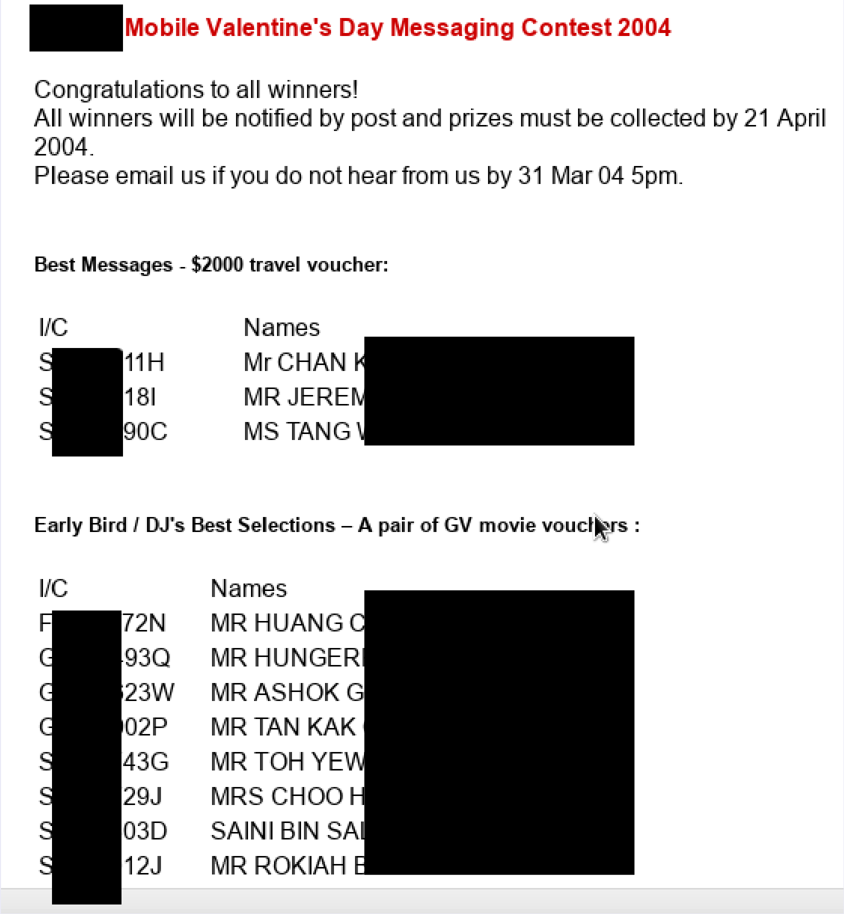


Bil	Nama	No. K/P	Alamat	Penempatan
1	Mohd Ghuzaimi [redacted]	[redacted] 14-5881	[redacted] Bandar Tun ras, Kuala	[redacted] aian Malaysia
2	Norazura Binti [redacted]	[redacted] 10-5622	[redacted] la, 42000 Selangor	[redacted] aian Malaysia
3	Amerul Hazriq [redacted]	[redacted] 43-5141	[redacted] jah,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

Scenario 4: Negligence

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 K[redacted]
S[redacted]18I	MR JEREM[redacted]
S[redacted]90C	MS TANG [redacted]

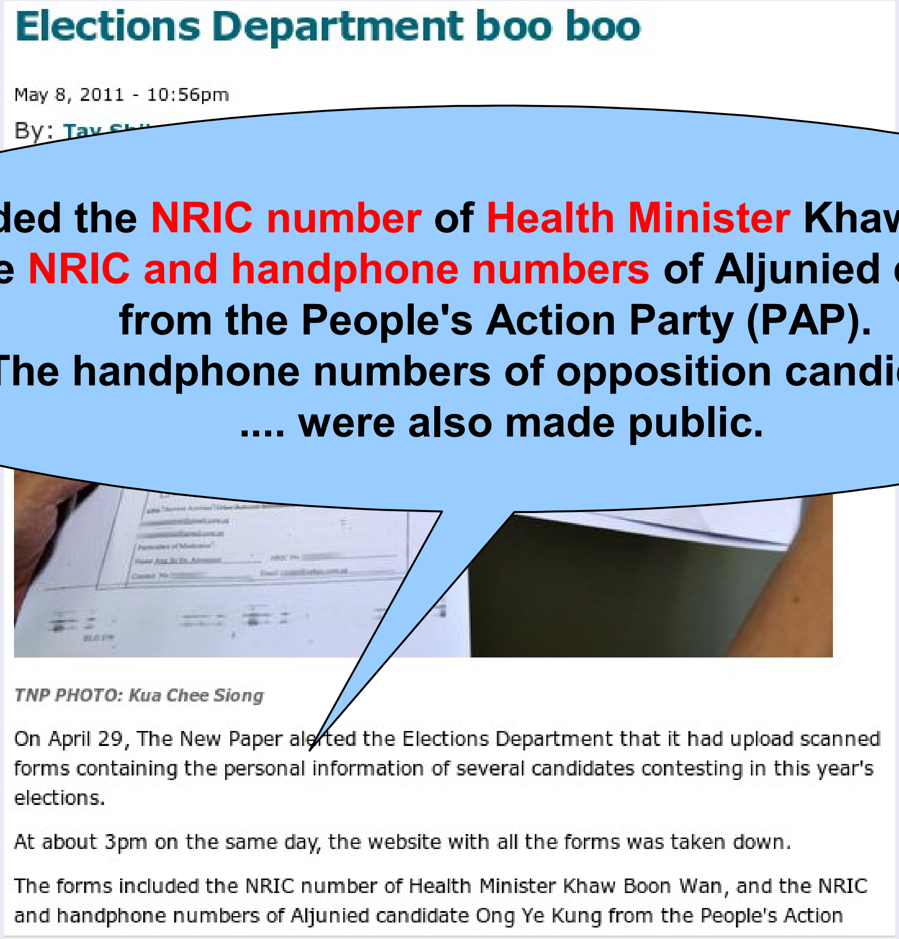
Early Bird / DJ's Best Selections – A pair of GV movie vouchers :

I/C	Names
F[redacted]72N	MR HUANG C[redacted]
G[redacted]93Q	MR HUNGER[redacted]
G[redacted]23W	MR ASHOK G[redacted]
G[redacted]02P	MR TAN KAK [redacted]
S[redacted]43G	MR TOH YEW[redacted]
S[redacted]29J	MRS CHOO H[redacted]
S[redacted]03D	SAINI BIN SA[redacted]
S[redacted]12J	MR ROKIAH [redacted]

Scenario 4: Negligence

Elections Department, Singapore

Private information of election candidates was leaked



Elections Department boo boo

May 8, 2011 - 10:56pm

By: Tay Sh

TNP PHOTO: Kua Chee Siong

On April 29, The New Paper alerted the Elections Department that it had upload scanned forms containing the personal information of several candidates contesting in this year's elections.

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

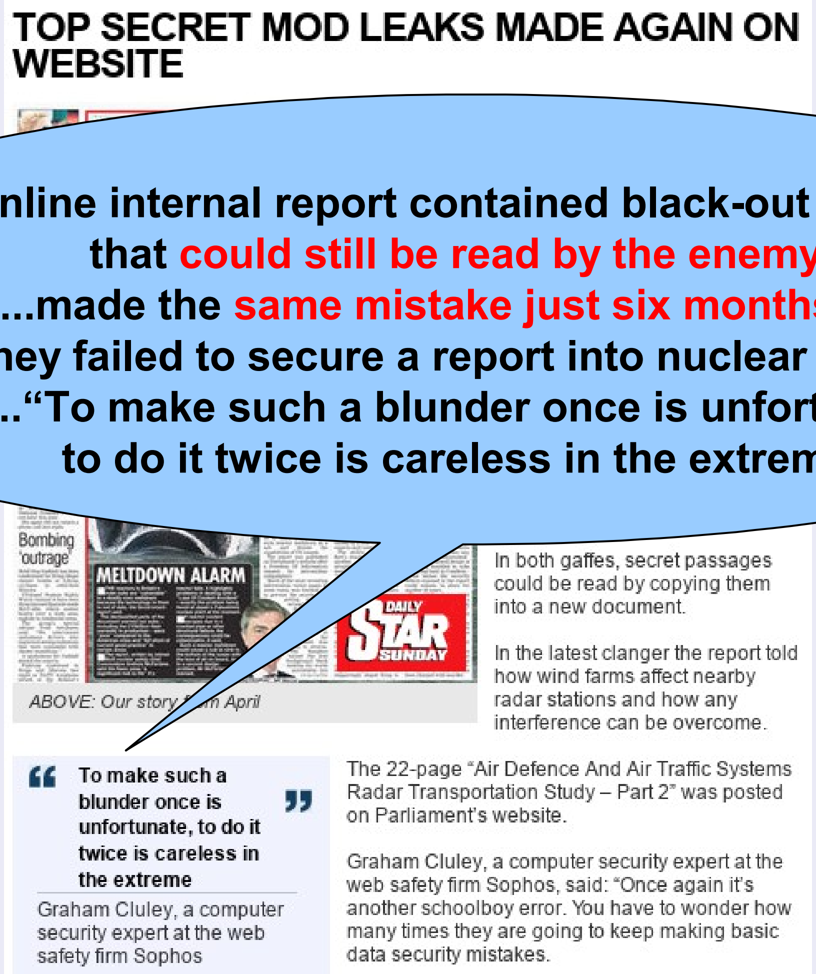
The forms included the NRIC number of Health Minister Khaw Boon Wan, and the NRIC and handphone numbers of Aljunied candidate Ong Ye Kung from the People's Action

... 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.

Scenario 4: Negligence

Ministry of Defence, UK

Military secrets were leaked from an online PDF



TOP SECRET MOD LEAKS MADE AGAIN ON WEBSITE

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.

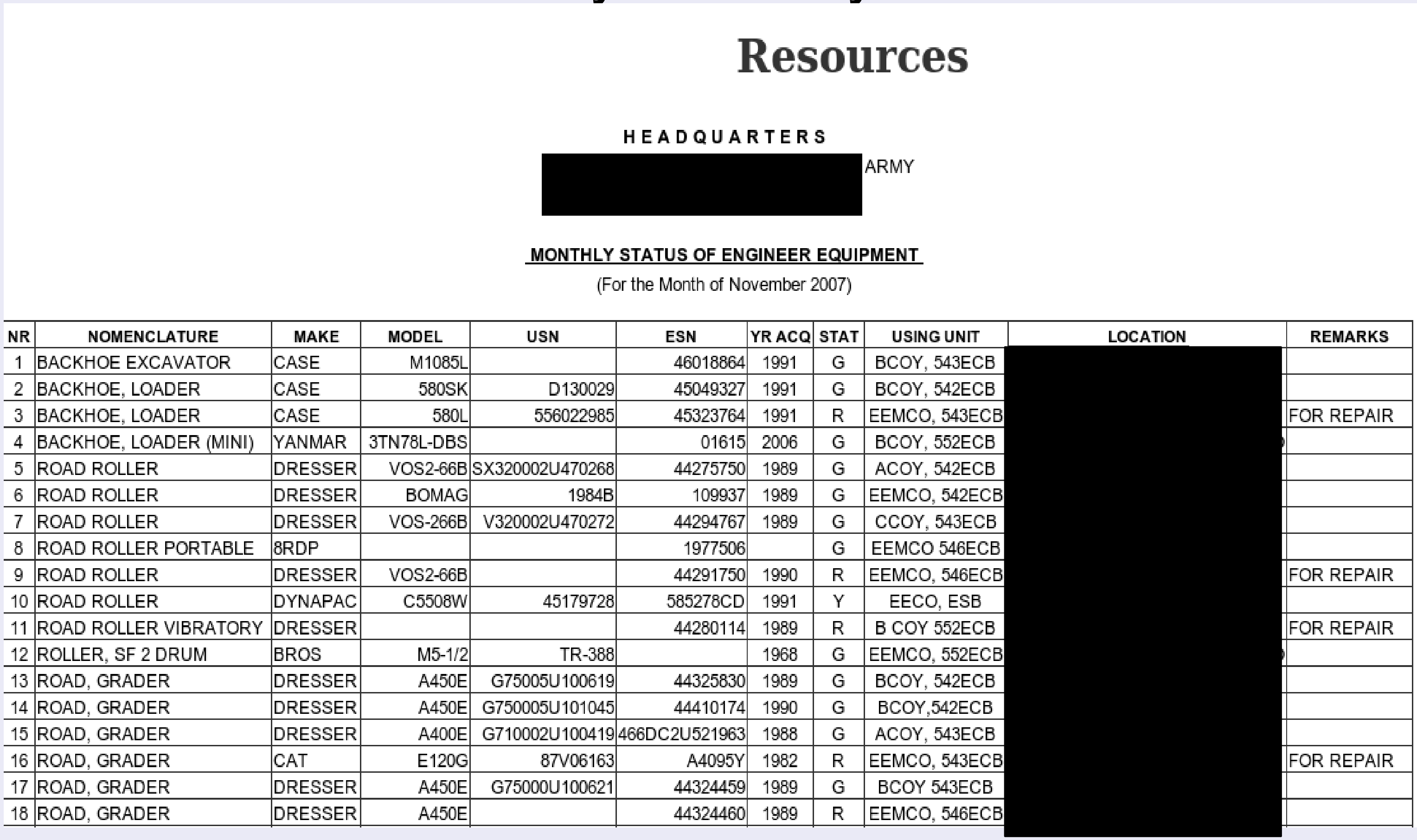
An online internal report contained black-out -passages that could still be read by the enemy...
...made the same mistake just six months ago,
when they failed to secure a report into nuclear submarines...
...“To make such a blunder once is unfortunate,
to do it twice is careless in the extreme.”

Scenario 4: Negligence

OWASP
The Open Web Application Security Project

Southeast Asian Army

Sensitive military inventory was leaked



Resources

HEADQUARTERS
[redacted] ARMY

MONTHLY STATUS OF ENGINEER EQUIPMENT

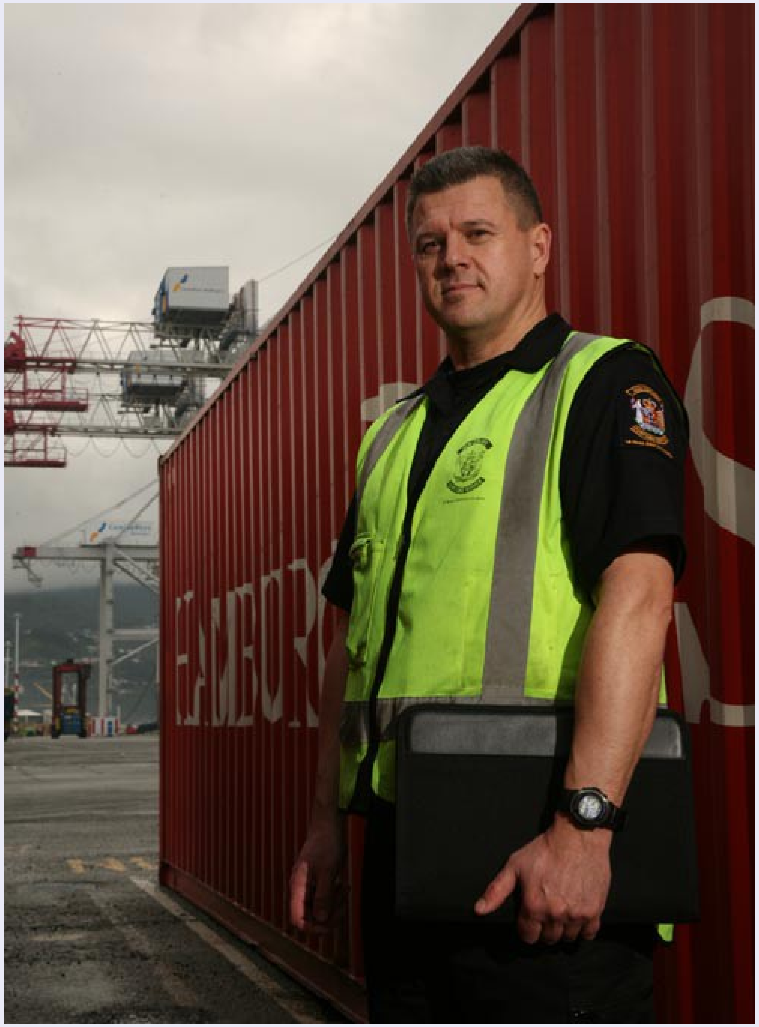
(For the Month of November 2007)

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

Why you should invest in your last line of defence

OWASP
The Open Web Application Security Project

Through outbound protection, you can reap these benefits:



1 Supports BUSINESS by building customer and public confidence in web-based services

2 Supports BUSINESS by avoiding costs such as regulatory penalties and reputation restoration costs.

3 Supports INFORMATION SECURITY by complementing other security systems which primarily look at inbound traffic.

4 Supports OPERATIONS by stopping any leakage or visitor infection arising from change management errors.

Thank You

Wong Onn Chee

ocwong@owasp.org