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

• 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
• 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?

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!

Inbound attacks against users are blocked.
Outbound Data Loss Protection (DLP) prevents users from leaking information.
Inbound attacks to DMZ are blocked.
No Protection!

OWASP
The Open Web Application Security Project

Internet

Trusted / Internal

DMZ / Data Center

DMZ / Data Center

No Protection!

Internet

Outbound Data Loss Protection (DLP) prevents users from leaking information.

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

<table>
<thead>
<tr>
<th></th>
<th>Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Sarbanes-Oxley Act (2002), HIPAA, GLBA - U.S.</td>
</tr>
<tr>
<td>3</td>
<td>Data Protection Act – UK</td>
</tr>
<tr>
<td>4</td>
<td>Personal Information Protection Act – Japan, Korea</td>
</tr>
<tr>
<td>5</td>
<td>Personal Data Protection Act – Malaysia, China, Taiwan, Singapore</td>
</tr>
<tr>
<td>6</td>
<td>Information Technology Act – India</td>
</tr>
<tr>
<td>7</td>
<td>Privacy Act – Australia, New Zealand</td>
</tr>
<tr>
<td>8</td>
<td>Personal Data Ordinance – Hong Kong</td>
</tr>
</tbody>
</table>
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.
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.
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
<table>
<thead>
<tr>
<th>Industry</th>
<th># U.S. Records Lost from Web Servers (2005-2008)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>2,269,656</td>
</tr>
<tr>
<td>Education</td>
<td>588,846</td>
</tr>
<tr>
<td>Healthcare</td>
<td>529,034</td>
</tr>
<tr>
<td>Financial</td>
<td>114,745</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>46,000</td>
</tr>
<tr>
<td>Retail</td>
<td>22,735</td>
</tr>
<tr>
<td>Real Estate</td>
<td>13,000</td>
</tr>
<tr>
<td>Security</td>
<td>5,878</td>
</tr>
<tr>
<td>Utilities</td>
<td>3,000</td>
</tr>
<tr>
<td>Internet</td>
<td>2,750</td>
</tr>
<tr>
<td>Legal</td>
<td>530</td>
</tr>
<tr>
<td>Logistics</td>
<td>465</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>3,596,639</strong></td>
</tr>
</tbody>
</table>

### Industry
<table>
<thead>
<tr>
<th>Industry</th>
<th># U.S. Records Lost from Web Servers (2009-2012)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>168,280,885</td>
</tr>
<tr>
<td>Others</td>
<td>92,523,918</td>
</tr>
<tr>
<td>Government</td>
<td>13,611,652</td>
</tr>
<tr>
<td>Financial</td>
<td>3,406,956</td>
</tr>
<tr>
<td>Healthcare</td>
<td>807,076</td>
</tr>
<tr>
<td>Education</td>
<td>2,099,219</td>
</tr>
<tr>
<td>Non-profit</td>
<td>109,314</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>280,839,020</strong></td>
</tr>
</tbody>
</table>

Increase by 78x (7800%)!!!
4 common causes of information leakages from web servers / cloud

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

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

3. Configuration 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.

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

- 80% Redirects from legitimate sites
- 20% Direct from malicious sites
Compromised websites is the most popular way to spread malware.
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."
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?

For decades, we had been chasing after hackers by focusing 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**

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.

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?
Outbound security prevents hackers from succeeding regardless of their means.

A new and more effective way to defeat the hackers!
Top 10 steps to address outbound risks.

1. Output Encoding
   - Effective against XSS.
   - Available from OWASP ESAPI: `ESAPI.encoder().encodeforXXX()`
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
Content Security Policy
- Whitelist authorized sources of images, scripts, videos and etc...

Validate inputs
- To minimize risks from injections.

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
The following slides contain graphic examples which may cause sleepless nights to IT management.
Singapore's statutory body confirms Web site hack

Summary: [UPDATE] People's Association, which promotes racial and social cohesion in the country, admits hackers penetrated its main Web site and other subsidiary sites, over the weekend.

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

New hacking group hits government websites, leaks stolen data
Posted on 04 May 2012.

....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.
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 key online properties offline after discovering a "sophisticated," widespread attack. Our preliminary investigation has found no evidence that any consumer data is impacted. But as a precaution, we have 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...
LG Australia's website hacked

Asher Moses
October 24, 2011

Hacked by Intra
your security --------------------
Intra
Website Security Exploit Team

INTRA
From Within

...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.

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

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...
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.
At least 73,000 visitors may be infected...

5 major Japanese companies...

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...
Large European Insurance Firm in Singapore

Scenario 1: Compromised Web Servers

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.

Get me out of here! Why was this page blocked?

Ignore this warning
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.”
Citibank, US

360,000 accounts/credit card information was lost

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.

“They 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 information that users can access via the web.
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 Unix R

...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

We learned this morning that an internal test page created to update promotional 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
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.
Facebook Source codes were leaked.

“....exposed to a small number of users as a result of a single, misconfigured Web server...”
One of the "small number of users" posted on his blog the source code of Facebook home page.

Scenario 3: Misconfiguration

Facebook Scenario 3: Misconfiguration

The Open Web Application Security Project (OWASP)

One of the "small number of users" posted on his blog the source code of Facebook home page.

Scenario 3: Misconfiguration

Facebook Scenario 3: Misconfiguration

The Open Web Application Security Project (OWASP)
Bank customer records were leaked during system upgrade

"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"
Princeton Review
108,000 student records were leaked

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Nama</th>
<th>No. K/P</th>
<th>Alamat</th>
<th>Penempatan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mohd Ghuzaimi Bin</td>
<td>14-5881</td>
<td>Bandar Tun Abdul Razak,</td>
<td>Selangor</td>
</tr>
<tr>
<td></td>
<td>Hasbullah</td>
<td></td>
<td>Kuala Lumpur</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Norazura Binti Aiska</td>
<td>10-5622</td>
<td>Puchong, 47000 Selangor</td>
<td>Selangor</td>
</tr>
<tr>
<td></td>
<td>Ahmad</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Amerul Hazriq Bin</td>
<td>43-5141</td>
<td>Semenyih, 47000 Selangor</td>
<td>Selangor</td>
</tr>
<tr>
<td></td>
<td>Ahmad</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Mohd Nur Azimina</td>
<td>03-5139</td>
<td>Balakong, Jalan Klang</td>
<td>Selangor</td>
</tr>
<tr>
<td></td>
<td>Anwar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Mohamad Ridwa Jumari</td>
<td>14-6255</td>
<td>Off Jalan Klang,</td>
<td>Selangor</td>
</tr>
<tr>
<td></td>
<td>Ali</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Norsbazzina Binti</td>
<td>14-5178</td>
<td>Jalan Klang,</td>
<td>Jalan Duta</td>
</tr>
<tr>
<td></td>
<td>Zirah</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mohd Khairul Aziz</td>
<td>11-5325</td>
<td>Jalan Klang,</td>
<td>Jalan Duta</td>
</tr>
<tr>
<td></td>
<td>Mohamed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Norhamiza Binti</td>
<td>08-6358</td>
<td>Jalan Klang,</td>
<td>Jalan Duta</td>
</tr>
<tr>
<td></td>
<td>Akim</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Muhamad Al Hafiz</td>
<td>56-5129</td>
<td>Jalan Klang,</td>
<td>Jalan Duta</td>
</tr>
<tr>
<td></td>
<td>Mohd Shukri</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Government Agency, Malaysia**

Scenario 4: Negligence
Telco A, Singapore

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

<table>
<thead>
<tr>
<th>I/C</th>
<th>Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>11H</td>
<td>Mr. CHAN</td>
</tr>
<tr>
<td>18I</td>
<td>Mr. JEREM</td>
</tr>
<tr>
<td>90C</td>
<td>Ms. TANG</td>
</tr>
</tbody>
</table>

**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:**

<table>
<thead>
<tr>
<th>I/C</th>
<th>Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>72N</td>
<td>Mr. HUANG</td>
</tr>
<tr>
<td>93Q</td>
<td>Mr. HUNGER</td>
</tr>
<tr>
<td>23W</td>
<td>Mr. ASHOK</td>
</tr>
<tr>
<td>02P</td>
<td>Mr. TAN KAK</td>
</tr>
<tr>
<td>43G</td>
<td>Mr. TOH YEOW</td>
</tr>
<tr>
<td>29J</td>
<td>Mrs. CHOO HONG</td>
</tr>
<tr>
<td>03D</td>
<td>SAINI BIN SAEED</td>
</tr>
<tr>
<td>12J</td>
<td>MR. ROKIAH</td>
</tr>
</tbody>
</table>
Private information of election candidates was leaked

Private information of election candidates was leaked

Elections Department, Singapore

Private information of election candidates was leaked

Elections Department boo boo

May 8, 2011 - 10:56pm
By: Tan Siang Liang

... 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
Military secrets were leaked from an online PDF

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.”

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

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

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: Negligence

**Southeast Asian Army**

Sensitive military inventory was leaked

### Resources

<table>
<thead>
<tr>
<th>NR</th>
<th>NOMENCLATURE</th>
<th>MAKE</th>
<th>MODEL</th>
<th>USN</th>
<th>ESN</th>
<th>YR ACQ</th>
<th>STAT</th>
<th>USING UNIT</th>
<th>LOCATION</th>
<th>REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BACKHOE EXCAVATOR</td>
<td>CASE</td>
<td>M1055L</td>
<td>46018854</td>
<td>1991</td>
<td>1 G</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>BACKHOE, LOADER</td>
<td>CASE</td>
<td>580SK</td>
<td>D130029</td>
<td>1991</td>
<td>1 G</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>BACKHOE, LOADER</td>
<td>CASE</td>
<td>580L</td>
<td>536022988</td>
<td>1991</td>
<td>1 G</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>BACKHOE, LOADER (MINI)</td>
<td>YANMAR</td>
<td>JTN75-L-D</td>
<td>01615</td>
<td>2006</td>
<td>1 G</td>
<td>BCoy, 502ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>ROAD ROLLER</td>
<td>DRESSER</td>
<td>VOS2-66B</td>
<td>8320002U1470268</td>
<td>1999</td>
<td>G</td>
<td>ACOY, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>ROAD ROLLER</td>
<td>DRESSER</td>
<td>BOMAG</td>
<td>1964B</td>
<td>1989</td>
<td>1 G</td>
<td>EEMCO, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>ROAD ROLLER</td>
<td>DRESSER</td>
<td>VOS-266B</td>
<td>44284750</td>
<td>1999</td>
<td>1 G</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>ROAD ROLLER PORTABLE</td>
<td>BRDP</td>
<td></td>
<td>1977505</td>
<td>2001</td>
<td>1 G</td>
<td>EEMCO 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>ROAD ROLLER</td>
<td>DRESSER</td>
<td>VOS2-66B</td>
<td>442891750</td>
<td>1999</td>
<td>1 G</td>
<td>EEMCO, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>ROAD ROLLER</td>
<td>DYNAPAC</td>
<td>C5506W</td>
<td>45170728</td>
<td>1991</td>
<td>1 Y</td>
<td>EECO, ES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>ROAD ROLLER VIBRATORY</td>
<td>DRESSER</td>
<td></td>
<td>44280114</td>
<td>1989</td>
<td>1 R</td>
<td>BCoy 502ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>ROLLER, SF 2 DRUM</td>
<td>BROS</td>
<td>M5-1/2</td>
<td>TR-300</td>
<td>1986</td>
<td>1 G</td>
<td>EEMCO, 532ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>ROAD, GRADER</td>
<td>DRESSER</td>
<td>A450E</td>
<td>G750010U100619</td>
<td>1988</td>
<td>G</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>ROAD, GRADER</td>
<td>DRESSER</td>
<td>A450E</td>
<td>G750010U100645</td>
<td>1988</td>
<td>G</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>ROAD, GRADER</td>
<td>DRESSER</td>
<td>A400E</td>
<td>G710002U100419</td>
<td>1988</td>
<td>G</td>
<td>ACOY, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>ROAD, GRADER</td>
<td>C A T</td>
<td>E120G</td>
<td>67V06163</td>
<td>1982</td>
<td>1 R</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>ROAD, GRADER</td>
<td>DRESSER</td>
<td>A450E</td>
<td>G750020U100621</td>
<td>1989</td>
<td>G</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>ROAD, GRADER</td>
<td>DRESSER</td>
<td>A450E</td>
<td>44324450</td>
<td>1989</td>
<td>1 G</td>
<td>BCoy, 542ECB</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why you should invest in your last line of defence

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