Enterprise Security 2008

Information Security & Business Continuity

June 2008

Chia-Wei Yen
IDC Security Taxonomy 2008

Security Products & Services

Security Hardware
- Hardware Authentication
  - Biometrics
  - Tokens
  - Smart Cards
- Threat Mgmt. Security Appliances
  - FW/VPN
  - Unified (UTM)
  - IDS&IPS
  - SCM
  - Other

Identity & Access Mgmt. (IAM)
- Advanced Authentication
- Web SSO
- Host SSO
- Legacy Authorization
- User Provisioning
- (Directory Services)

Security & Vulnerability Mgmt. (SVM)
- Event Management
- Vulnerability Management
- Policy and Compliance
- Other (i.e., Forensics)

Secure Content & Threat Mgmt.
- Web
- Applications
- Network
- Network Admission Control (NAC)/EndPoint

Other Security Software (e.g., Encryption)
- Consulting
- Implementation
- Managed Services
- Education

© 2008 IDC Jun-08
Security Services Forecast

World Wide Security Services Forecast

- Americas
- Asia/Pacific
- EMEA

Year:
- 2006
- 2007
- 2008
- 2009
- 2010
- 2011

M$:
- $0
- $5,000
- $10,000
- $15,000
- $20,000
- $25,000
- $30,000
- $35,000
- $40,000

$37.9B
$23.8B
$25,000
$30,000
$35,000
$40,000

© 2008 IDC
Jun-08
Factors Driving Security In 2008?
Players in the Threat Ecosystem

- Professionals
- Organized Crime
- Sophistication

- Financial Gain
- Identity Theft
- System Uptime

- Insiders
- Trust
- Access
- Data Leaks
- Policy Violations
- Compliance Violations

- Amateurs
- Script Kiddies
- Vandals

- System Downtime
- Web Site Defacement
- Denial of Service
- Notoriety
- Thrill Seeking

- Fraud
- Credit Cards

Jun-08 © 2008 IDC
Motivation No Longer for Fun and Notoriety!

**Money $$** Now Driving Attacks by:

- Highly Skilled Individuals
- Organized Crime
- Industrial Espionage
Traditional Security Threats Continue:

- Hackers
- Malware (Trojans, Viruses, Worms etc.)
- Spam
How would you rate the items below on the threat each poses to your company’s enterprise network security? (Scale: 5 = significant threat; 1 = no threat)

<table>
<thead>
<tr>
<th>Threats To The Enterprise</th>
<th>% responding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojans, Viruses, Worms and other malicious code</td>
<td>57%</td>
</tr>
<tr>
<td>Spyware</td>
<td>50%</td>
</tr>
<tr>
<td>SPAM</td>
<td>45%</td>
</tr>
<tr>
<td>Employee Error (unintentional)</td>
<td>47%</td>
</tr>
<tr>
<td>Application Vulnerabilities</td>
<td>37%</td>
</tr>
<tr>
<td>Data Stolen by employee or business partner</td>
<td>37%</td>
</tr>
<tr>
<td>Hackers</td>
<td>37%</td>
</tr>
</tbody>
</table>
Growing Enterprise Threats Include:

- Thefts of Private and Confidential Information
- Insider Threats
- Phishing
- Botnets
## Personal Data Thefts On The Rise

### Motives
- Financial gain is the #1 driving force behind attacks today

### The Threat
- Increasing volume and sophistication of attacks mean there’s always a new threat around the corner (key logging, etc)

### Security Breaches

<table>
<thead>
<tr>
<th>Organization</th>
<th>Date</th>
<th>Type</th>
<th>Stolen Details</th>
<th>Stolen Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ministry of Defense</td>
<td>Jan. 2008</td>
<td>Stolen: Personal Records</td>
<td>600,000 Recruits</td>
<td></td>
</tr>
<tr>
<td>Monster.com</td>
<td>Aug. 2007</td>
<td>Stolen: personal records for</td>
<td>1.3 million resumes</td>
<td></td>
</tr>
<tr>
<td>TJX</td>
<td>Jan. 2007</td>
<td>Stolen: credit card details for</td>
<td>45.7 million people</td>
<td></td>
</tr>
<tr>
<td>UCSF</td>
<td>Apr. 2007</td>
<td>Stolen: personal data for</td>
<td>40,000 people</td>
<td></td>
</tr>
<tr>
<td>UCLA</td>
<td>Nov. 2006</td>
<td>Stolen: personal data for</td>
<td>800,000 students</td>
<td></td>
</tr>
<tr>
<td>LexisNexis</td>
<td>Mar. 2005</td>
<td>Stolen: consumer data for</td>
<td>310,000 people</td>
<td></td>
</tr>
<tr>
<td>Bank of America</td>
<td>May 2005</td>
<td>Stolen: consumer data for</td>
<td>108,000 customers</td>
<td></td>
</tr>
</tbody>
</table>

Note: TJX has taken a charge in excess of $120M
Enterprise Challenges – Personal Information Leaks

Information Leakage Occurrences are Real and Costly

- Customer records
- Intellectual Property

### Data Lost in Transit

<table>
<thead>
<tr>
<th>Company</th>
<th>Date</th>
<th>Type of Data Lost</th>
<th>Affected:</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMRC – UK</td>
<td>Nov. 2007</td>
<td>Personal Data</td>
<td>25 million people</td>
</tr>
<tr>
<td>ACS</td>
<td>Mar 2007</td>
<td>Personal data</td>
<td>2.9 million people</td>
</tr>
<tr>
<td>CardSystems</td>
<td>June 2006</td>
<td>Credit card details</td>
<td>40 million people</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Feb 2005</td>
<td>SS numbers</td>
<td>1.2 million customers</td>
</tr>
<tr>
<td>CitiGroup</td>
<td>June 2005</td>
<td>Personal data</td>
<td>3.9 million customers</td>
</tr>
<tr>
<td>Time Warner</td>
<td>May 2005</td>
<td>SS numbers</td>
<td>600,000 employees</td>
</tr>
</tbody>
</table>

* Her Majesty’s Revenue and Customs
* Affiliated Computer Services
Enterprise Compliance Complexity
Inside Threats are an IT Growing Concern
Q: Do you believe that the most serious threats to your company's enterprise IT infrastructure originate from internal or external sources?
Data Loss Prevention (DLP)
Data Loss Prevention (DLP)

DLP includes solutions discover, protect, and control sensitive information including:

- **Data-in-motion.** Data-in-motion includes solutions that monitor, encrypt, filter, and block outbound content contained in email, instant messaging, peer to peer, file transfers, Web postings, and other types of messaging traffic.

- **Data-at-rest.** Data-at-rest includes solutions that discover, protect, and control information on desktops, laptops, file/storage servers, USB drives, and other types of data repositories.

- **Data-in-use.** Data-in-use includes solutions that protect and control information in use. These solutions are used to maintain the integrity of sensitive information such as contracts, term sheets, and other business-critical documents.
Confidential Information Leak Sources

- Corporate Email: 56%
- Lost/stolen laptop: 51%
- Web Email or Web posting (message board, blog, etc.): 37%
- Instant messaging: 33%
- Lost/stolen mobile device (PDA, Smart Phone): 33%
- Media devices (USB, iPod): 19%
- Other: 12%
Encryption Use Grows In 2008
Encryption Is Growing Rapidly Due To:

✓ Compliance
✓ Privacy Disclosures

➤ Encryption Key Management & Recovery Are Major Issues

➤ Interest In Encrypted e-Mail Is Growing

➤ File Encryption For Laptops And Mobile Devices Are Hot

➤ Secure Storage With Protection Of Data At Rest Is Hot
Major Security Trends 2008

- Movement Away From Software Towards Appliances and Bladed Solutions
- Convergence of Security, Storage, Systems and Networking management (3SN)
- Security-based Solutions for Regulatory and Internal Policy Compliance
- Single Approach to Compliance, Not a Series of Point Products
- Consolidated Dashboards, Agents, Reporting Tools, and Log Management Systems
- Granular Content Filtering With Layers of Managed Services, Appliances, and Software
Thank You
Chia-Wei Yen

Please email me at:
cwyan@idc.com