Information Security Industry Overview

Presented By Peter Benson, CEO

© 2007 Security-Assessment.com

Who and Where

- Founded 2003
- Only ‘pure-play’ information security assurance company in Australasia
- Audit, assess, advise and assure large and medium enterprises
- Global authority –NZ VISA/MasterCard certified auditor
- Offices in Auckland, Wellington, Sydney, Canberra
- Consultants in Palo Alto, Toronto, Manchester
- Expertise in Finance, E-Commerce/EFTPOS, Government, Telcos, Utilities,.
- Focus on Security and Vulnerability Research, Forensic Research
- Global Presenters, Global Brand

© 2007 Security-Assessment.com

Actual Headlines

- House Committee Wants NRC to Conduct Deeper Investigation Into Data Spike at Alabama Power Plant (May 18, 2007)
- Two Arrested in Hospital Computer Theft (May 11& 15, 2007) Two men have been arrested in connection with the theft of two laptop computers. A recovered computer is thought to have contained personal data of more than 13,000 patients at the time it was stolen;
- Illinois State Database Suffers Security Breach (May 19, 2007) A database holding personally identifiable information of approximately 300,000 people who have applied for or hold certain professional licenses.
- MessageLabs uncovered some interesting trends in its report on online threats for March. The most common of the 249 low-volume, high-value attacks identified by the company consisted of a single e-mail sent to one person.

© 2007 Security-Assessment.com

Actual Headlines

- Australia's essential services including electric, water and transport are not secured against cyber terrorist attacks, the Federal Government has warned.
- In last year's AusCERT Computer Crime and Security Survey, 58 per cent of companies surveyed reported having laptops stolen, up from 53 per cent in 2005. Nine per cent of companies said handhelds had been stolen last year, up from 8 per cent in 2005.
- Lax security led to TJX breach. Despite a market capitalization of almost $13bn, it appears the company couldn't afford to secure its Wi-Fi network with anything more than Wired Equivalent Privacy.
- McAfee unveiled a study showing that 33% of respondents said they believe a major data-loss incident involving accidental or malicious distribution of confidential data could put them out of business.
- Hackers fake Howard heart attack
- More than 100 HSBC Australia customers had their banking details, names and home addresses, as well as other personal financial information exposed in a serious security breach by staff.

© 2007 Security-Assessment.com

- **Threats are still being underestimated by organisations:**
  Attack vector types and intelligence of attacks are increasing. Business and crime is driving the serious threats.

- New Spam is still booming
- Spyware, keyloggers, trojans etc are on the increase
- Time to exploit of vulnerabilities is decreasing.
- Hacking for profit (cyber-extortion) is a real threat.
- State Sponsored…?
- New technologies are opening up organisations to unimaginable risks.
- Targeted Attacks huge!
- Most organisations are struggling to just to keep up with the basics, let alone keep pace with new and emerging threats.

© 2007 Security-Assessment.com

Weaknesses

- IT Centric View of Security
- Systems View rather than Service View
- Complex Environments have Inherent Weaknesses
- New Technology Not Mature
- End to End / Enterprise Considerations
- Lack of Visibility (Current Compromises >5%)
- Security Risk vs Business Risk

© 2007 Security-Assessment.com

- Wireless Attack
  - Internal
  - External

© 2007 Security-Assessment.com

Outrage Management

- Typical Risk Calculation Risk = Threat x Vulnerability x Impact
- Risk = Hazard x Outrage
- Lack of transparency
- Breach disclosure management
- When or if you Disclose
- Service Management Focus?

© 2007 Security-Assessment.com

Figures and Examples

- Last Week Verified Attacks (Zone-H.org)
- Total attacks: **7002** of which **1056** single ip and **5946** mass defacements
  - Linux (75%) (up)
  - Win 2003 (12.5%) (down)
  - Win 2000 (4.5%)
  - FreeBSD (7.2%)
  - All others (0.57%)

© 2007 Security-Assessment.com

Figures and Examples

- 499 .nz sites mirrored in the last month
  - Those are only the ones zone-h.org hears about
  - 461 .co.nz, remainder .org.nz, .net.nz

© 2007 Security-Assessment.com

Methods of Attack – Zone-H

- configuration / admin. mistake 18.5%
- known vulnerability (i.e. unpatched system) 14.5%
- undisclosed (new) vulnerability 12.5%
- File Inclusion 10.2%
- brute force attack 7.4%
- FTP Server intrusion 5.7%
- Other Web Application bug 4.3%
- Attack against the administrator/user (password stealing/sniffing) 4.3%
- social engineering 3.4%
- SQL Injection 3.4%

© 2007 Security-Assessment.com

Norton Internet Security

Chronology of Data Breaches

Go to Breaches for 2005, 2006, or 2007

DATE MADE PUBLIC	NAME (Location)	TYPE OF BREACH	NUMBER OF RECORDS
2005			
Jan. 10, 2005	George Mason University (Fairfax, VA)	Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the university's main ID server.	32,000
Jan. 18, 2005	Univ. of CA, San Diego (San Diego, CA)	A hacker breached the security of two University computers that stored the Social Security numbers and names of students and alumni of UCSD Extension.	3,500
Jan. 22, 2005	University of Northern Colorado (Greeley, CO)	A hard drive was apparently stolen. It contained information on current and former University employees and their beneficiaries -- name, date of birth, SSN, address, bank account and routing number..	30,000
Feb. 12, 2005	Science Applications International Corp. (SAIC) (San Diego, CA)	On Jan. 25 thieves broke into a SAIC facility and stole computers containing names, SSNs, and other personal information of past and current employees. Stolen information included	45,000 employees

- There's money on the Internet and lots of it:
  - Spamming, Phishing, Porn
  - Cyber-extortian, Hacking for Profit
  - Pirating / Warez
- New attack vectors and targeted attacks continue to grow:
  - Applications are easy targets yet risks not well understood by most
  - Network Access Control / End Point Security is hot !
  - VoIP vulnerable / SPAM?
  - Attacks and compromises can be very well hidden

© 2007 Security-Assessment.com

What we are seeing from a management perspective:

- Reliance on technology is creating a false sense of security.
- Obligations and Duties not understood. Business Risk!
- Very few organisations have an effective IT Security, ISMS, SSMF, or Risk Management strategy in place.
- Most believe that cyber-threats are not as real as reported!
- Most organisations have little understanding of the risks they face.
- Most wouldn't know if they have been compromised (>35%?).
- Most underestimate the repercussions of an incident. (Outrage)
- You're on your own – with hundreds of so-called standards to help you!
- Compliance vs. Security – two different objectives ?

© 2007 Security-Assessment.com

What we are seeing from an implementation perspective:

- New whizz-bang technologies STILL seen as silver bullets.
- Patch management and IDS/IPS seen as total solutions vs. vulnerability management
- Organisations want security to be automated totally!

We cannot Manage what we cannot Measure.
Throwing more Technology and People at the problem is not an option anymore

- New technologies being deployed without careful security review eCommerce systems, Web Services, VoIP etc etc etc.
- Lack of Enterprise Perspective
- Compliance is driving behaviours but in some cases to the detriment of security!

© 2007 Security-Assessment.com

Disturbing Trends and Myths

- Security is built into applications and systems (Not!)
- Someone else has tested this product before us (Not!)
- Testing just before we go live gives us assurance (Not!)
- Security is an IT issue (Not!)
- Now that we have gone live, Operations should be able to keep it secure (Not!)
- We have a large organisation, but are focussed on security, and so are secure enough (Not!)
- We have never had a security incident (Really?)
- What we don't know won't hurt us (Really?)
- Our perimeter is secure, that's enough (Not!)
- VoIP can be deployed easily and securely (Not!)

© 2007 Security-Assessment.com

Questions?

http://www.security-assessment.com
Peter.benson@security-assessment.com

© 2007 Security-Assessment.com