Changing Exposures in a Tech-Centered World: Managing Network Privacy

Steve Yesko, ARM
Lowers & Associates

Two Presentations

- Risk Mitigation
- Insurance/Legal Aspects

Risk Mitigation Agenda

- Cyber Risk vs. Data Breach
- Types of Breach
- Evolution of the Exposure
- Top 10 Incidents of 2010
- Top 10 Unsolved Crimes
- Today Risk Landscape
- Organizational Risk Trends
- 2011 Forecast
- IT Security Testing - 3 Prong Approach
- IT Risk Mitigation Measures - Be Prepared
- Information Resources

Cyber Risk vs. Data Breach

Cyber Risk Coverage

- Addresses hazards such as unauthorized website access, on-line libel, data loss and repairs to databases after system failures.

Data Breach or Privacy Coverage

- Covers the cost of notification and credit monitoring services for affected persons, PR expense to address reputational harm, breach investigation, legal fees and compensatory damages, judgments and settlements.

Types of Breach

- Theft or Loss
- Inappropriate Handling
- Inadvertent Exposure
- Misuse of Access (Insider Threat)
- Unauthorized Access (External Attack)
- System Compromise (Malware)

The Big Picture

- 1 in 400 emails contains confidential information
- 1 in 50 network files contains confidential data
- 1 in 2 USB drives contains confidential information
- 4 out of 5 companies have lost confidential data when a laptop was lost
- The average cost of a single record disclosed in a data breach is $202 ($240 for Financial Institutions and $243 for first-time breaches. Overall costs can be much higher when related expenses are taken into account)
- The Carolina's included, laws in 46 states (soon to be 47), plus the District of Columbia and Puerto Rico, require organizations to protect confidential data and comply with data breach notification laws.

What's at risk?

Customer/Personal

- Credit/Debit/Stored Value Cards
- SSNs/Gov't IDs
- Medical (PHI)
- Student transcripts
- HR/Payroll
- Loyalty programs
- Motor vehicle
- Insurance claims
- Financial transactions
- Financial records
- Contracts

Corporate Data

- Intellectual property
- Trade secrets
- Customer lists
- Price lists
- Bid data
- M&A targets/plans
- Patent applications
- 3rd party information (NDA)
- Financial transactions/records
- Security policies/provisions
- Network architecture
- Litigation information

Evolution of the Exposure

- From a kid in the basement of his parents home to highly sophisticated organized crime networks
- From IT/computer related to Internet/web-based
- From theft of money to theft of information
- From outside/in to inside/out
- From legal action brought by consumers to legal action by regulators
- From expenses to secure network/servers to expenses for state notification laws
- From an IT issue to a Boardroom issue
- From a national to an international problem

The Biggest Information Security Incidents of 2010

#10. Affinity Health Plan
#9. WellPoint/Anthem BlueCross
#8. CitiGroup
#7. Ohio State University
#6. South Shore Hospital
#5. Lincoln National Financial Securities
#4. AvMed Health Plans
#3. Gawker
#2. Education Credit Management Corp.
#1. Netflix

Source: Software, Information & Network Security News

Top 10 Unsolved Computer Crimes

#10. The WANK Worm (Oct. 89; first hacktivist attack)

#9. UK Ministry of Defense Satellite Hack (Feb. 99)

#8. CDUniverse Credit Card Breach (Jan. 00)

#7. USN Military Source Code Theft (Dec. 00)

#6. Anti-DRM Hack (Oct. 01; Windows Media)

#5. Dennis Kucinich on CBSNews.com (Oct. 03)

#4. Hacking your MBA App (Mar. 06)

#3. The 26,000 Site Hack Attack (Winter 08)

#2. Hannaford/Sweetbay Breach (Feb. 08)

#1. Comcast/Network Solutions Redirect (May 08)

Source: PC Magazine

Today's Risk Landscape

- Data breaches increased significantly in 2010
  - ITRC's 2010 Breach Report cited 662 reported breaches
  - An increase of 33% over 2009
  - Paper Breaches: 20% (no mandatory reporting rqmt.)
  - Insider Theft: 15.4% (doubled since 2007)
  - Hacking: 17% (up 3%)
  - Data on the Move, Accidental, Subcontractor: 34.3%
- Threat Volumes are on the Rise
  - 2005 - 330,000 unique malware samples; 38 web threats per hour
  - 2008 - 16,495,000 unique malware samples; 1,883 web threats per hour
- Threat Vectors are Internet-Based
  - 92% now arrive via the Internet (Websites, Links, Email)
  - 8% arrive via file transfer (removable media)

Today's Risk Landscape (cont'd)

- The Underground Economy is More Profitable
  - $100 billion per year marketplace
  - Malware: $50 - $3,500
  - Email Addresses: $0.001 per Address
  - Hour of usage on a Botnet of 8,000 to 10,000 computers: $200
- Email Threats Continue to Increase
  - 115 billion spam messages per day
  - Targeted Phishing Attacks (Spearphishing, Whaling)
- Web and Application Threats are Growing
  - 450,000 SQL/XSS Injection Attempts per Day
  - DNS Changers Re-Directing Users to Malware
- Mobile Threats Being Introduced
  - With PC-like Vectors
- Botnets are Proliferating
  - As of 2008, 34.3 million PCs infected w/ bot-associated malware

Phishing

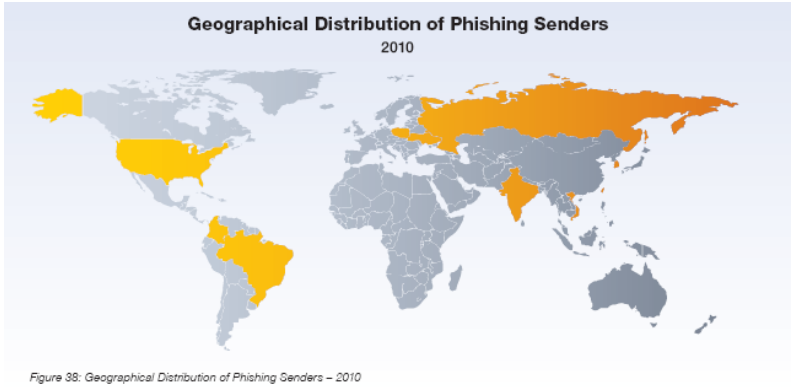


Figure 38: Geographical Distribution of Phishing Senders – 2010

Country	% of Phishing
India	15.5%
Russia	10.4%
Brazil	7.6%
USA	7.5%
Ukraine	6.3%

Country	% of Phishing
South Korea	4.7%
Colombia	3.0%
Taiwan	2.2%
Vietnam	2.2%
Poland	1.8%

Country of Origin of Phishing Emails

- Phishing = Deceptive emails
- Spearphishing = Targeted phishing
- Pharming = DNS based phishing
- SMiShing = Targets cellular texting
- Bluesnarfing = Bluetooth connections

Source: IBM X-Force 2010 Trend Statistics

Phishing targets by Industry:

- Financial Institution 50%
- Credit Card 19%
- Auction 11%
- Government 7.5%
- On-line Payment 5.7%
- On-line Shop 4.9%

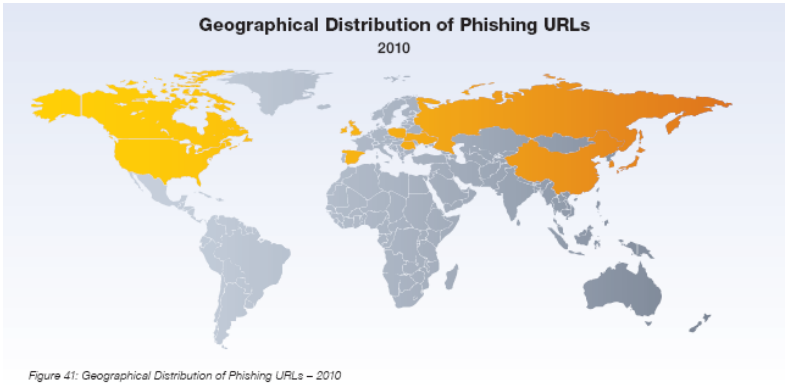


Figure 41: Geographical Distribution of Phishing URLs – 2010

Country	% of Phishing URLs
Romania	18.8%
USA	14.6%
China	11.3%
South Korea	9.8%
United Kingdom	7.2%

Country	% of Phishing URLs
Canada	4.7%
Japan	4.3%
Spain	3.2%
Poland	3.0%
Russia	2.9%

Country of Origin for Embedded Web Links

The Cyber Crime Black Market

Organizational Risk Trends

- Advanced Persistent Threats
  New!
- Strong Rising Threats
  - Unstable Third Party Providers
  - Insecure Trading Partners
- Rising Threats
  - Malicious/Disgruntled Insiders
  - Careless/Overworked Employees
  - Reduced Security Budgets
- Steady Threats
  - Remote Workers
  - Software Downloading

Why Risk Management?

- IT + Business + Financial Risk
- Part of broader governance, risk or compliance initiative
- IT => Information Security focus
- Regulatory Compliance
- Measuring threats and costs

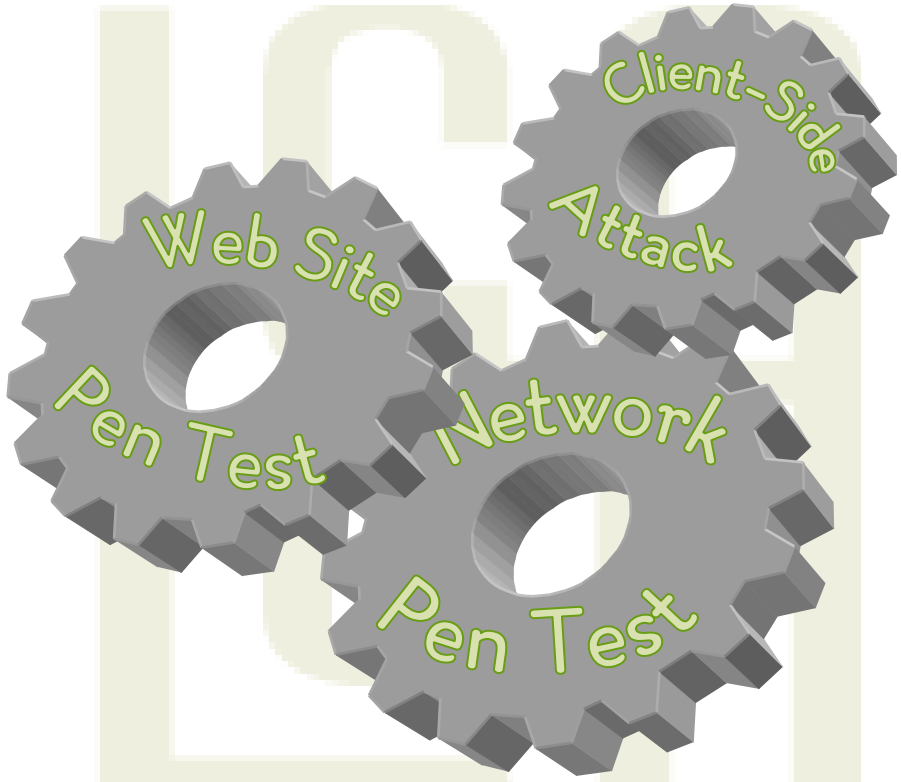
Mitigating Cyber Risk

- Avoid it
- Ignore it (we are not a target)
- Accept it as part of doing business
- Manage it (controls/processes)
- Transfer it (insurance, escrow)

Risk Mitigation Measures

- IT/Information Security Risk Assessments
- Internal / External *and* Independent Testing:
  - Vulnerability (Scan) Analysis (network, application, database)
  - Penetration Testing (same, plus client-side)
  - Controls Testing (SAS-70, ISO-2700*n*, CoBIT, PCI, BITS FISAP)
- Implement, Test, and Continuously Improve:
  - Data Classification & Protection Measures
  - Training & Awareness
  - Logging & Monitoring
  - Patch/Configuration Management
  - Network, Server, *and* Endpoint DLP
  - AV, IDS/IPS, Proxies & Filters, DSRA
- Develop WISP - BR Team, BR Plan, COOP Approach
- Social Media Policies
- Compliance Audits

IT Security Testing
A Three-Pronged Approach



2011-12 Forecast

- Sophisticated, blended, APTs for the FIs
- More smaller, reported breaches elsewhere
- Social networking policy implementation rises
- Ransomware and ransom attacks will grow
- Data minimization and cloud solutions advance
- Mobile data is ripe for the picking
- Low-tech theft of data/devices increases
- Alternative O/S attacks will increase
- Microsoft still targeted; Web 2.0 is here to stay

2011 Forecast

- More prevalent/deceptive social engineering methods
- Privacy awareness / breach preparedness advances
- Third-party data collection faces greater scrutiny
- The underground economy will continue to flourish
- Identity theft and spam will increase worldwide
- Continuing exposure due to lost devices
- Data encryption seen as means to compliance ends
- Federal breach notification legislation comes in 2012?
- Collaboration + Openness = Vulnerability to breach

Information Resources

- PGP/Ponemon Study (www.ponemon.org)
- Verizon Data Breach Investigations Report (www.verizonbusiness.com)
- IBM X-Force Trend & Risk Report (www.ibm.com)
- Betterley Report (www.betterley.com)
- U.S. Dept. of Health & Human Services (www.hhs.gov)
- Privacy Rights Clearinghouse (www.privacyrights.org)
- ePlace (www.eplacesolutions.com)
- Sedona Conference Working Group on eDiscovery (www.thesedonaconference.org)
- BITS FISAP (www.bitsinfo.org)
- Identity Theft Resource Center (ITRC) Report (www.idtheftcenter.org)
- Internet Crime Complaint Center (IC3) Report (www.ic3.gov)
- Center for Strategic & International Studies (CSIS) (www.csis.org)
- Forrester Research (www.forrester.com)

LOWERS
& ASSOCIATES
International Risk Mitigation Partners

Stephen Yesko, ARM
VA Office: (540) 338-7151
NY Office: (718) 775-9198
syesko@lowersrisk.com
www.lowersrisk.com