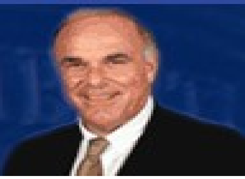
Commonwealth of Pennsylvania

Edward G. Rendell, Governor

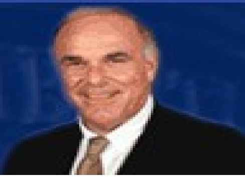


Cyber Threat Preparedness

Robert L. Maley
Chief Information Security Officer
Commonwealth of Pennsylvania

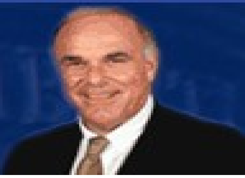
What Cyber threats should we prepare for?

- Identity Theft?
- Phishing? Spam?
- Spyware?
- Trojans, Worms & Viruses?
- Attacks / Zero Day Exploits
- In-secure Security Software?
- Wireless & Mobile Data threats?



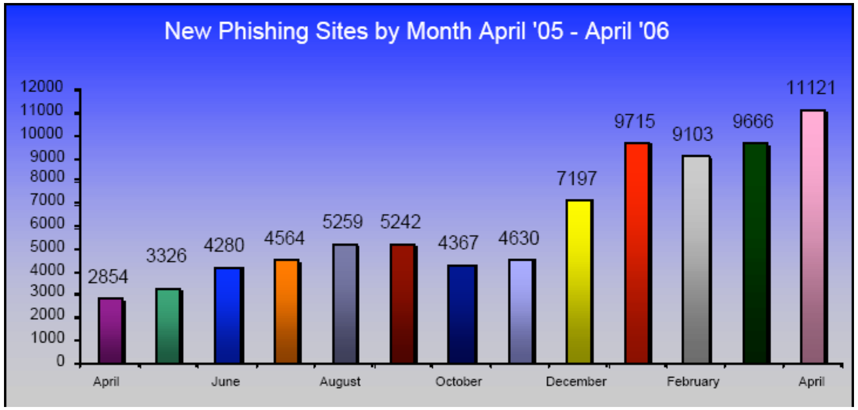
Identity Theft

- Giant says lost ID data lists only ex-workers
- Veterans' ID Theft May Be Largest Ever
- Red Cross warns blood donors of possible ID thefts in Midwest.
- Credit Card Breach Exposes 40 Million Accounts
- Bank Of America Loses A Million Customer Records
- Pentagon Hacker Compromises Personal Data
- Online Attack Puts 1.4 Million Records At Risk
- Hacker Faces Extradition Over 'Biggest Military Computer Hack Of All Time'
- Laptop Theft Puts Data Of 98,000 At Risk
- Medical Group: Data On 185,000 People Stolen
- Hackers Grab LexisNexis Info on 32000 People
- ChoicePoint Data Theft Widens To 145,000 People
- PIN Scandal 'Worst Hack Ever'; Citibank Only The Start
- ID Theft Hit 3.6 Million In U.S.
- Georgia Technology Authority Hack Exposes Confidential Information of 570,000 Members
- Scammers Access Data On 35,000 Californians
- Payroll Firm Pulls Web Services Citing Data Leak
- Hacker Steals Air Force Officers' Personal Information
- Undisclosed Number of Verizon Employees at Risk of Identity Theft



Phishing

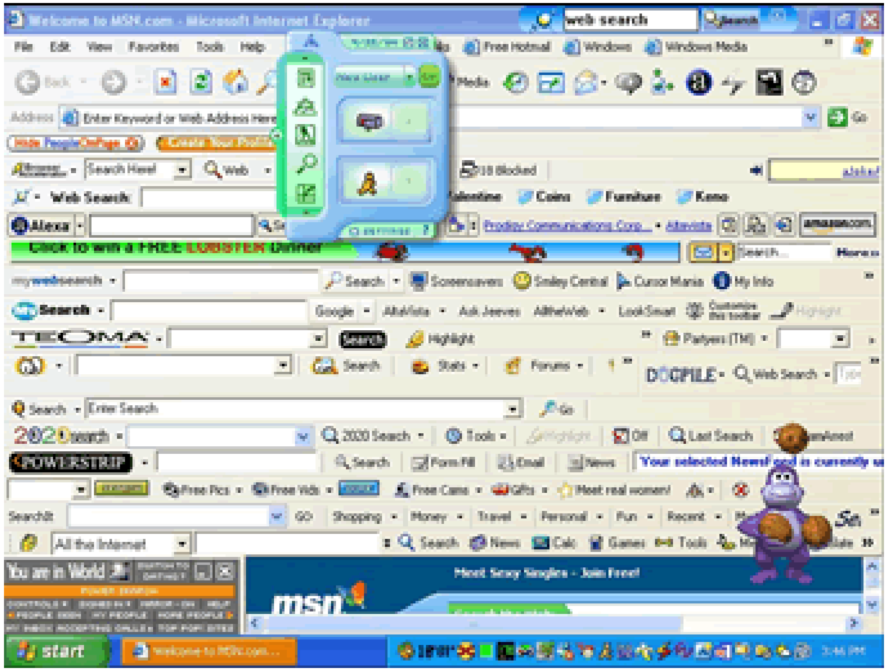
- Phishing attacks are sophisticated operations with emails and fake websites that appear almost identical to the real thing.
- Scam emails that form the basis of phishing attacks often pose as 'security check' emails from well-known businesses
- In June 2004, the Gartner Group reported that online bank accounts had been looted of $2.4 billion just in the previous 12 months.

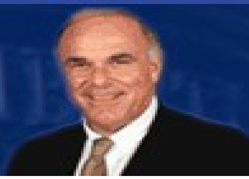


http://www.antiphishing.org/

Spyware / Malware

- Malware email
  - The e-mail purports to be from Microsoft and it is notifying the recipient of "a new vulnerability [that] has been discovered in the Microsoft WinLogon Service". It further states that the vulnerability can allow an attacker access to the unpatched system.
  - Of course, the user is advised to install the patch which can be downloaded from the included link.
- Spyware
  - any program that tracks activities on the computer and then saves or transmits a record of them. Spyware infects some 80 percent of PCs, according to a study by the National Cyber Security Alliance and America Online Inc


Welcome to MSN.com - Microsoft Internet Explorer
web search
File Edit View Favorites Tools Help
Free Hotmail Windows Windows Media
Enter Keyword or Web Address Here
Web Search
Alexa
Click to win a FREE LOBSTER Dinner
Screensavers Smiley Central Cursor Mania My Info
Google AltaVista Ask Jeeves AlltheWeb LookSmart
TEOMA
Highlight
DOGPILE Web Search
Enter Search
2020search 2020 Search Tools Last Search
POWERSTRIP
Your selected NewsFeed is currently
Free Pics Free Vids Free Cams Gifts Meet real women!
Shopping Money Travel Personal Fun Recent
All the Internet
Search News Calc Games Tools
You are in World
Meet Sexy Singles - Join Free!
msn
start
Welcome to MSN.com...

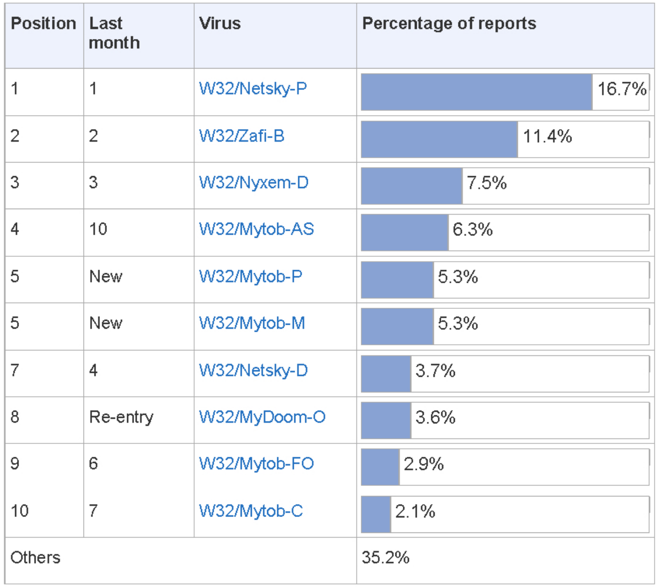


Trojans, Worms & Viruses

- Sophos identified 1,538 new threats in May. The majority of the new threats (85.1%) were Trojan horses, while just 12.3% were worms or viruses.

- The proportion of email which is virus infected has dropped considerably over the last year as hackers have turned from mass-mailing attacks to targeted Trojan horses. In May 2005, one in every 38 emails was infected, now this number is just one in 141.

- The threat environment is actually becoming much more sinister, as we see more targeted malware attacks use spyware technology to snoop upon individuals and businesses," said Carole Theriault, senior security consultant at Sophos. "Businesses need to think more holistically about their IT defences. Anti-virus protection at both the gateway and the desktop must be accompanied by firewalls, regular security patch upgrades and safe computing best practice."



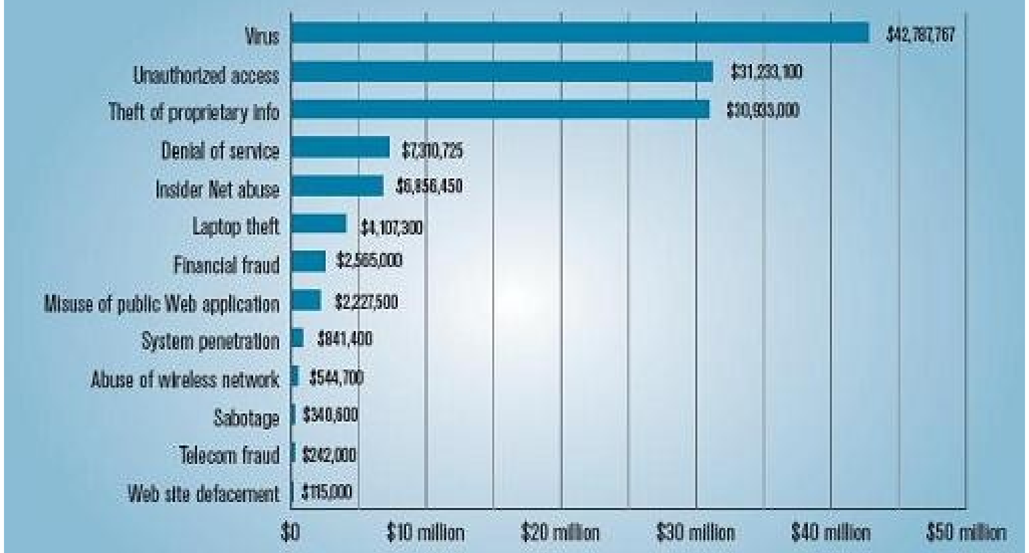
Position	Last month	Virus	Percentage of reports
1	1	W32/Netsky-P	16.7%
2	2	W32/Zafi-B	11.4%
3	3	W32/Nyxem-D	7.5%
4	10	W32/Mytob-AS	6.3%
5	New	W32/Mytob-P	5.3%
5	New	W32/Mytob-M	5.3%
7	4	W32/Netsky-D	3.7%
8	Re-entry	W32/MyDoom-O	3.6%
9	6	W32/Mytob-FO	2.9%
10	7	W32/Mytob-C	2.1%
Others			35.2%

http://www.sophos.com/pressoffice/news/articles/2006/06/toptenmay06.html

Attacks & Threats

- CSI/FBI 2005 Crime & Security Survey
  - Virus losses topped the list ($42M)
  - Unauthorized access and theft of information both over $30M
- Total reported losses in 2005 were $130M
- Over $200K average per respondent
- Denial of Service (DOS) Attacks
- Insider Abuse / Fraud / Misuse
- Sabotage / Disgruntled Employees

Figure 16. Dollar Amount Losses by Type



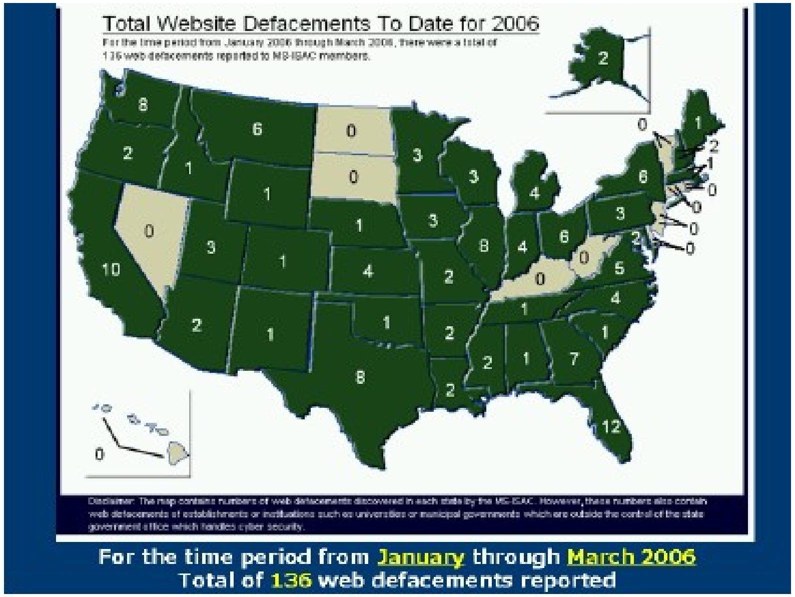
Total Losses for 2005 were $130,104,542

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 639 Respondents

Attacks & Threats

- Blackmail
  - MySpace Extortion Plot
    - hacked MySpace by exploiting a service vulnerability that let them steal users' personal information
    - threatened to release new exploit code unless MySpace came up with $150,000
    - Arrests made (http://internetweek.cmp.com/news/188500411;jsessio)
- Insiders
  - Skype, P2P, Instant Messaging
- Website Defacements
  - Pennsylvania Borough, County and City defacements this year.

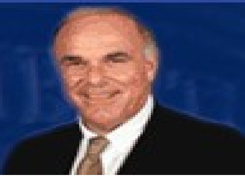


Total Website Defacements To Date for 2006

For the time period from January 2006 through March 2006, there were a total of 136 web defacements reported to MS-ISAC members.

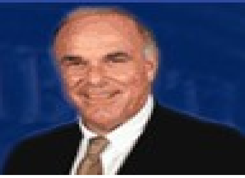
Disclaimer: The map contains numbers of web defacements discovered in each state by the MS-ISAC. However, these numbers also contain web defacements at establishments or institutions such as universities or municipal governments which are outside the control of the state government office which handles cyber security.

For the time period from January through March 2006
Total of 136 web defacements reported



Zero Day Exploits

- May 19, 2006, Microsoft Word XP & 2003 buffer over-flow
  - discovered in the wild as a "Zero-day" while investigating a system compromised
  - Patch schedule for June 13th.
  - Microsoft work-around published May 22, 2006
- December 27, 2005, Windows Metafile (WMF) Flaw
  - Within hours sites on the Internet using the exploit
  - 6 days later WMFMaker available on the Internet
  - 9 Days later a patch was released



In-secure Security Software?

- 5/25/2006 Symantec AntiVirus Worm Hole Puts Millions at Risk
  - http://news.yahoo.com/s/zd/20060525/tc_zd/179335
- 3/2004 -The fast-moving Witty worm exploited a zero-day buffer overflow in security products sold by Internet Security Systems.

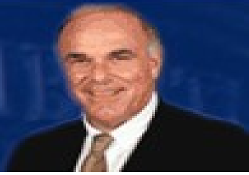
Wireless & Mobile Data Threats

Conference held in January

- Some topics covered in this presentation:
    - Attack Time
    - Attack Time on Shorter flights
    - Idle Hands
        - Change background image
        - Find pr0n on target, make that the background image
        - Launch MP3s with Parental Advisory lyrics
        - Rap, death metal, industrial (make a political statement)
        - Install a server and serve up pr0n to the rest of the aircraft
        - Repeat earlier bullet item on multiple machines
        - Cover your tracks! Upload your tools, attack other machines, then attack your own machine (plausible deniability)
- Contributing Factors
    - Laptops with built-in WiFi
    - Excellent Windows wireless integration
    - Connectivity friendliness of Windows in general

Hacking the Friendly Skies

ShmooCon - Jan 2006
Simple Nomad
nomad mobile research centre



More SmooCon Details

Best Target Locations

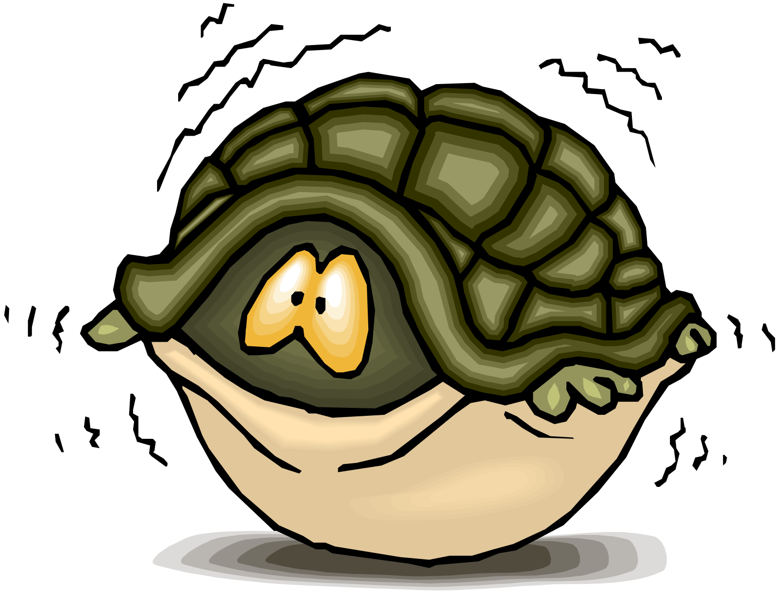
- Airline 31337 Flyx0r clubs, but this is regular laptop-to-laptop hacking
- Business commuter flights
  - Early Monday flights are best
  - Major business hauls
    - Eg LGA – DCA, EWR – BOS, ORD – LAX, HOU – ATL especially in and out of high tech areas
  - Get a seat near front part of coach
    - Road warriors request these seats in advance to get off the plane quicker
    - Aircraft with limited power outlets usually have outlets there
    - Better able to visually shoulder-surf during recon phase, helps with OS detection
    - Flights with lower passenger loads will have road warriers in First Class due to upgrades

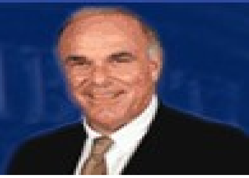
Contributing Factors

- Bad weather/delays means increased laptop usage in terminal
- Certain airports have no wireless
  - Charlotte, NC for example
  - Virtually all non-WEP/WPA SSIDs are ad-hoc

- Atlanta, GA Midweek
  - Largest city in the region, lots of businesses
  - Weather delay, sat on tarmac in DFW ½ mile from terminal for 1 hour while thunderstorm passed
  - MD80 aircraft, half full flight, 8 laptops out and running
  - 2 ad-hoc networks
  - 3 live targets, 2 Windows XP, 1 Windows 2000
    - Windows XP fully patched with firewalling
    - Windows 2000 vulnerable to MS05-039
- Charlotte, NC Midweek
  - Heavy banking/insurance town
  - Weather delay, target-rich environment in Charlotte (dozens of ad-hoc networks) at the gate before flight
  - MD80 aircraft, full flight, 12 laptops out and running
  - 5(!) ad-hoc networks
  - 5 live targets, 2 Windows XP, 1 Windows 2003, 2 Windows 2000
    - Only Windows 2003 fully patched with firewall
    - Rest vulnerable to MS05-017 and/or MS05-039
- ToorCon 7 Return Flight, Monday Morning
  - In terminal, very few laptops out (it was 6am), only 1 ad-hoc network named tmobile
  - 757 aircraft, full flight, 22 laptops out and running
  - 1 ad-hoc network formed named 249143
  - 2 additional nodes had attached to it (apparently clueless they had done so)
  - 3 live targets - 2 Windows XP, 1 Windows 2000
    - Windows 2000 vulnerable to MS05-039
      - Dlink technician
      - Windows XP Pro, vulnerable to MS05-017
    - Windows XP at SP1, vulnerable to MS05-017
      - This guy was across the aisle, VP of a physical security company.

How do we prepare?



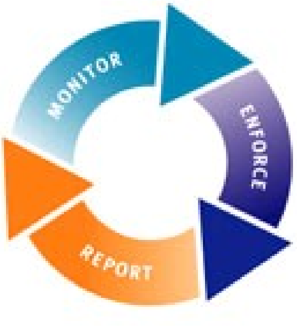


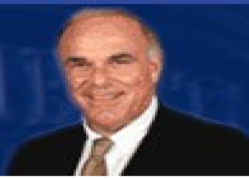
In The Case of Wireless

- Easy workarounds
  - Turn off your wireless connection when not in use
  - Set your wireless to only talk to infrastructure networks (advanced settings)
  - Personal firewalls will help, and on XP SP1 or later make sure the firewall is on
- Per the Microsoft Security Response Center, patches will be included in the next service pack releases to prevent the auto-advertising of adhoc networks

Security Should be a process, not a project!

- Security is an ongoing process
  - The bad guys have plenty of time to learn new techniques and how to defeat technology, our goal is to stay ahead of them.
- Regular Security Assessments & Vulnerability Scanning
  - Create a security baseline
- Security Awareness Training at all levels
- Ongoing Security Training at all levels
- Good policies, procedures and standards
- Beyond Patching





Regular Security Assessments & Vulnerability Scanning

- Develop a process & procedures to conduct regular security assessments
  - Self and external assessments
  - Regulatory requirements in some cases (PCI, etc.)
  - Self Assessment Toolkit available via the Commonwealth
    - http://www.oit.state.pa.us/eashare/cwp/view.asp?a=3&Q=204732&PM=1&easharePNavCtr=|#9485

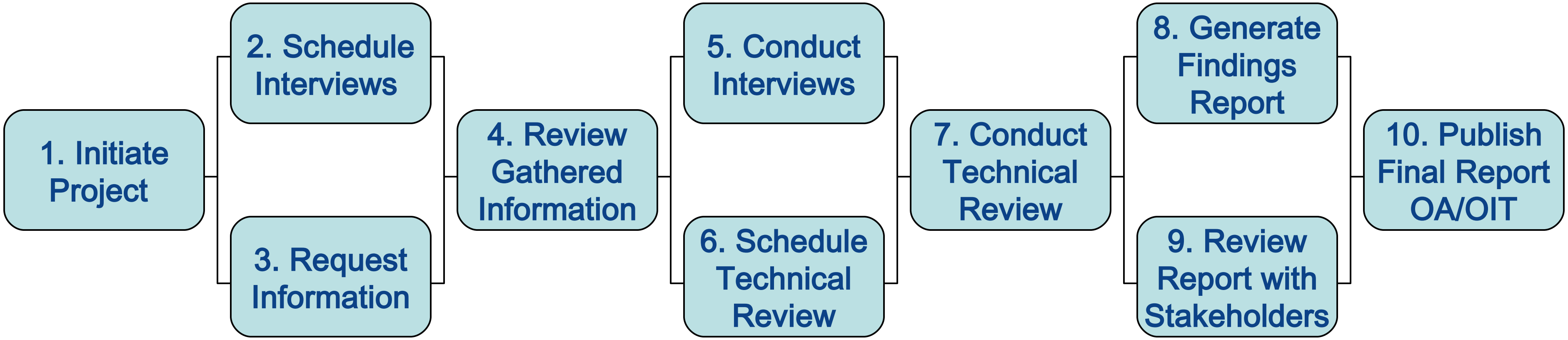
Self Assessment Toolkit

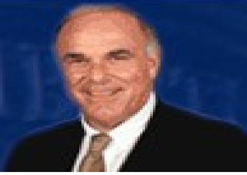
- OA/OIT has identified ISO 17799:2005 as the Commonwealth's security best practices benchmark.
- ISO 17799:2005 consists of eleven security clauses. The eleven clauses are listed below:
  - Security Policy;
  - Organizing Information Security;
  - Asset Management;
  - Human Resources Security;
  - Physical and Environmental Security;
  - Communications and Operations Management;
  - Access Control;
  - Information Systems Acquisition, Development and Maintenance;
  - Information Security Incident Management;
  - Business Continuity Management;
  - Compliance.

1. <u>Clause (11)</u>
   a. <u>Security Category (39)</u>
      1. Control Objective
      2. Controls

Security Assessment Methodology

- Below is the Commonwealth’s proposed methodology for assessing compliance with security best practices and legal regulations.
- The assessment methodology is modular in fashion. The initial intent is to perform a baseline assessment utilizing the provided ISO 17799 checklist (phases one – five). This initial assessment is interview and documentation review based.
- The results of the baseline assessment should provide a general understanding of the entity’s overall security posture and identify areas which require further review.
- During the project initiation phase, the assessment stakeholders identify the scope of the assessment.


1. Initiate Project
2. Schedule Interviews
3. Request Information
4. Review Gathered Information
5. Conduct Interviews
6. Schedule Technical Review
7. Conduct Technical Review
8. Generate Findings Report
9. Review Report with Stakeholders
10. Publish Final Report OA/OIT

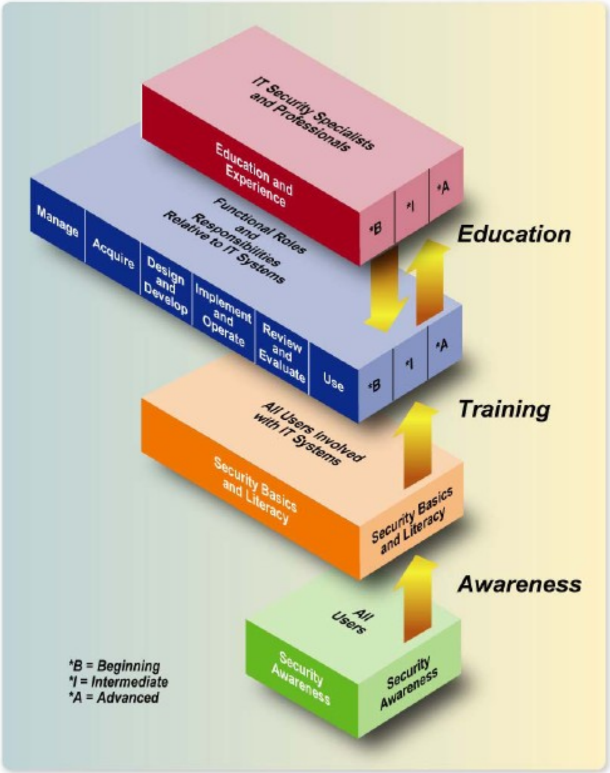


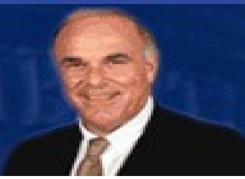
Security Awareness

- CyberSecurity Awareness Month – October, 2006
  - National Webcast
    - ***October 4, 2006*** - Kids Safe ONLINE – Produced by *Plays for Living*
- National Webcast Initiative
  - The US Department of Homeland Security, through its Computer Emergency Readiness Team (US-CERT), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) have launched a joint partnership to develop a series of national webcasts which will examine critical and timely cyber security issues.
  - **Wednesday, June 28, 2006:** Remote Access
  - **Wednesday, August 16, 2006:** Instant Messaging
  - http://www.cscic.state.ny.us/msisac/webcast/

Security Training & Policies

- While 87 percent of consumers polled said they were confident they could recognize fraudulent e-mails, 61 percent failed to identify a legitimate e-mail. Most respondents categorized all e-mails in the study as fake, even though one of them was legitimate
    - National Cyber Security Alliance Online Fraud Report, May 31, 2006
  - While they were aware of the threat, they weren't trained to recognized the difference
- Establish, train and enforce employee procedures for remote access, according to documented information management policies for physical and wireless teleworking, including:
  - Software download policies
  - Use and transport of agency-owned and configured computers, networking and security technology for access to business systems, versus employee-owned (personal) systems; and,
  - Use of external storage media (hard disk drives, thumb drives, CD's, etc.).
- Make adherence to information security practices a performance objective.

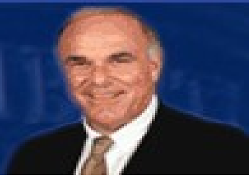




Resources

PA-ISAC (Information Sharing & Analysis Center)

- Monthly Cyber Security Tips Newsletter
- Major alerts, incidents and viruses
- Current issues for the State including any relevant reports or statements relating to the Commonwealth
- Upcoming major events for the Commonwealth
- IT security issues facing county and local governments
- Communication between the Commonwealth and County/Local Government will be at least once per month by conference call
- Conference calls may occur more frequently if warranted by significant events or incidents
- Face-to-Face meetings will occur on an annual basis



PA-ISAC (Information Sharing & Analysis Center)

Tools & Resources

Cyber Security Toolkit
A Toolkit has been created and distributed to states through the Multi-State Information Sharing and Analysis Center. The Toolkit is designed to promote the delivery of a consistent cyber security awareness message by reinforcing core themes in practical, informative, entertaining, and usable ways.

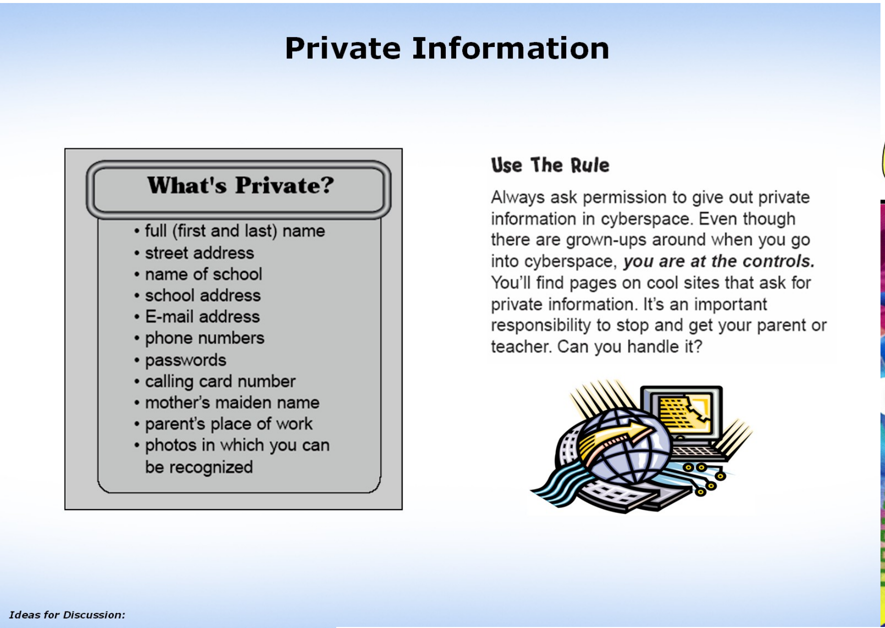
The toolkit includes:

- Instructions for Calendar and Poster Printing and Branding *(pdf)*

- Cyber Security Awareness Brochure
  - MS-ISAC Cyber Security Brochure *(pdf)*
  - Cyber Security Brochure Template

- Cyber Security Awareness Calendars *(MS powerpoint)*
  - MSISAC/USCERT - *geared for government/businesses and citizens*
  - iKeepSafe - *geared for children*
  - NCSA - *geared for teenagers*
  - CyberSmart! 2006 Cyber Security Calendar- *geared for 4th and 5th graders*

- Cyber Security Awareness Posters *(pdf)*



Private Information

What's Private?

- full (first and last) name
- street address
- name of school
- school address
- E-mail address
- phone numbers
- passwords
- calling card number
- mother's maiden name
- parent's place of work
- photos in which you can be recognized

Use The Rule

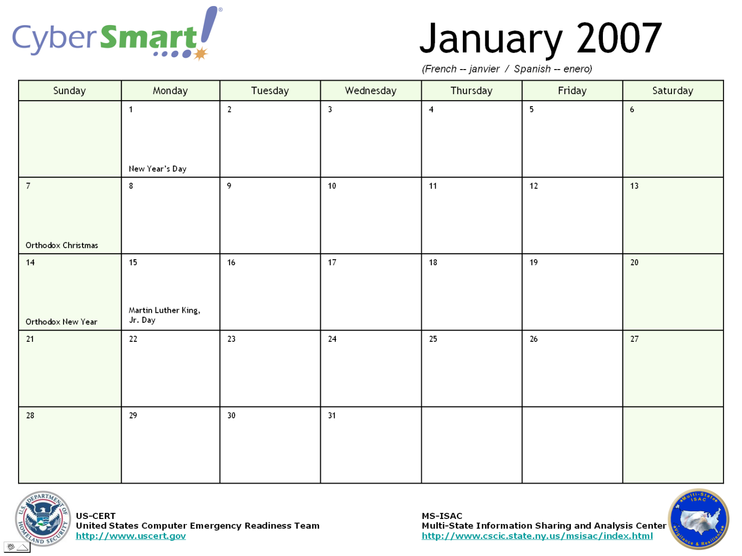
Always ask permission to give out private information in cyberspace. Even though there are grown-ups around when you go into cyberspace, ***you are at the controls.*** You'll find pages on cool sites that ask for private information. It's an important responsibility to stop and get your parent or teacher. Can you handle it?

Ideas for Discussion:

1) Take the rule into cyberspace. What sites do you com

2) What is the safety rule to remember?

007 Cyber Security Calendar



CyberSmart!

January 2007

(French -- janvier / Spanish -- enero)

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1 New Year's Day	2	3	4	5	6
7 Orthodox Christmas	8	9	10	11	12	13
14 Orthodox New Year	15 Martin Luther King, Jr. Day	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

US-CERT
United States Computer Emergency Readiness Team
http://www.uscert.gov

MS-ISAC
Multi-State Information Sharing and Analysis Center
http://www.cscic.state.ny.us/msisac/index.html

CyberSmart!

CyberSmart! ® is a registered trademark of The CyberSmart Education Company

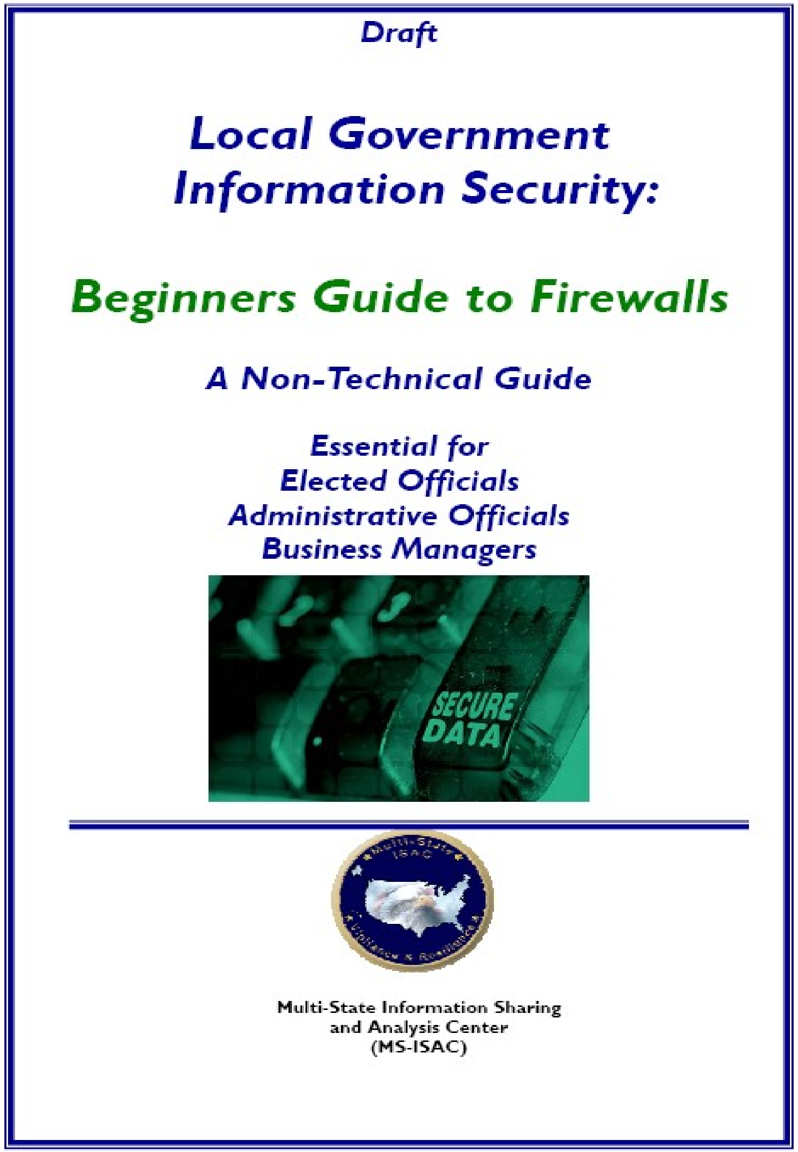
Multi-State ISAC
Pennsylvania ISAC

PA-ISAC (Information Sharing & Analysis Center)

Tools & Resources

- Computer Based Training
  - Interactive with voice and text instruction.
  - Eight modules based in ISO 17799.
  - Each module has an assessment at the end.
  - Includes an administrative module that will interface with Active Directory 2000/2003.
- Local Government Guide
  - Information Security: Getting Started
  - Why Cyber Security is important
  - Top ten Cyber Security action items

Multi-State ISAC
Pennsylvania ISAC



Draft

Local Government Information Security:

Beginners Guide to Firewalls

A Non-Technical Guide

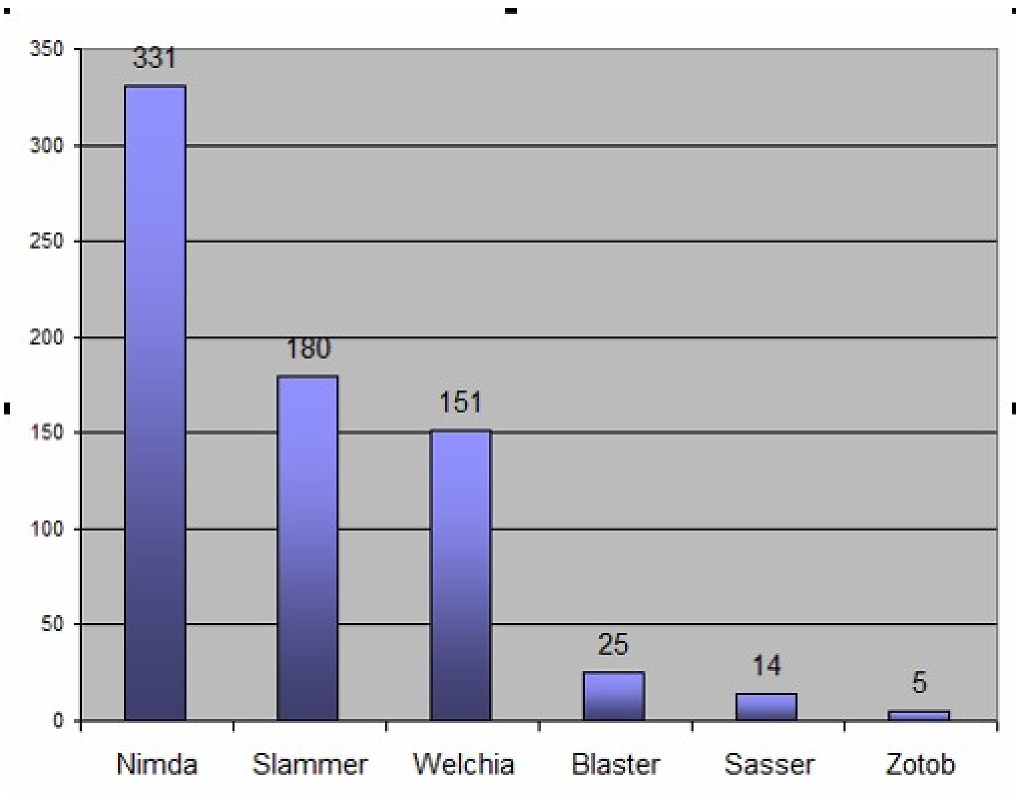
Essential for
Elected Officials
Administrative Officials
Business Managers

Multi-State Information Sharing
and Analysis Center
(MS-ISAC)

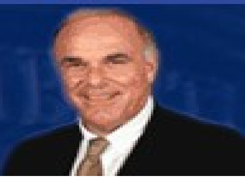
Beyond Patching

- Patching is becoming a 2nd or 3rd line defense, like backups
- You do it regularly but hope you never need it
- Automated attacks require automated response
- Investments made before the next worm will make all the difference
- All about layers that protect you even when you're not patched

Days between update and exploit



What to do next?

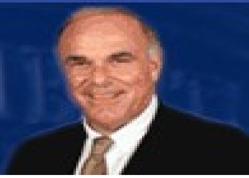


6 Steps to Cyber Threat Preparedness

- Step #1: Know what your assets are
- Step #2: Why are you trying to protect those assets
- Step #3: Understand what the risks are to the asset
- Step #4: Analyze any potential security solutions
- Step #5: Look at the trade-offs of implementing the solution
- Step #6: Is it worth it?

Step #1: Know what your assets are

- It is impossible to protect everything from everything
- Classify assets so you know which ones are critical so you know what to protect



Step #2: Why are you trying to protect those assets?

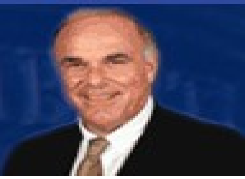
- Compliance with federal/state law or regulation (HIPAA, etc)?
  - Avoid penalties
- Compliance with Security Policy?
- Due diligence
- Avoid negligence
- Enablement to be competitive

Step #3: Understand what the risks are to the asset

- What are the consequences of a security incident?
- Who would want to compromise it?
- How would it be compromised?
- Why would it be compromised?
- Have security incidents already occurred?

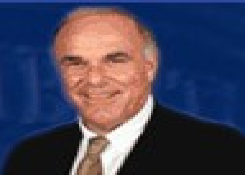
Step #4: Analyze any potential security solutions

- How well does it integrate into its surroundings?
- What are the operational considerations?
- What are the consequences of its failure?
- How well does the solution actually work in real situations against real threats?
- Does the solution provide a log or other evidence of activity?"
- Is this a Proactive or Reactive solution?
- List secondary benefits (reduced Help Desk calls, improved customer experience, etc)



Step #5: Look at the trade-offs of implementing the solution

- Money?
- Convenience?
- Privacy?
- Administrative overhead?
- Reduction in business efficiency?
- Does the solution require other solutions in order to be effective?



Step #6: Is it worth it?

- Is the benefit of mitigating the risk worth the additional risk plus the other trade-offs?
- If yes, then implement the security solution!

Conclusion

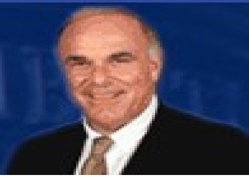
- Cyber-threats are ever changing
- Make Security a process integrated into your business objectives
- Analyze your risk factors and respond accordingly

Questions?

Contact Information

Robert L. Maley
Chief Information Security Officer
rmaley@state.pa.us

Resources



Links to Articles

Giant says lost ID data lists only ex-workers
http://www.pennlive.com/search/index.ssf?/base/news/1149303326123850.xml?pennnews&coll=1

Veterans' ID Theft May Be Largest Ever
http://www.washingtonpost.com/wp-dyn/content/article/2006/05/23/AR2006052301222.html

Red Cross warns blood donors of possible ID thefts in Midwest.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000754

Credit Card Breach Exposes 40 Million Accounts
http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html?tag=nl

Bank Of America Loses A Million Customer Records
http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html?tag=st.rn

Pentagon Hacker Compromises Personal Data
http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html?tag=st.rn

Online Attack Puts 1.4 Million Records At Risk
http://news.com.com/Online+attack+puts+1.4+million+records+at+risk/2100-1029_3-5420149.html?tag=st.rn

Hacker Faces Extradition Over 'Biggest Military Computer Hack Of All Time
http://www.spamdailynews.com/publish/Hacker_faces_extradition_over_biggest_military_computer_hack_of_all_time.asp

Laptop Theft Puts Data Of 98,000 At Risk
http://news.com.com/Laptop+theft+puts+data+of+98,000+at+risk/2100-1029_3-5645362.html?tag=st.rn

Medical Group: Data On 185,000 People Stolen
http://news.com.com/Medical+group+Data+on+185,000+people+was+stolen/2100-7349_3-5660514.html?tag=nl

Hackers Grab LexisNexis Info on 32000 People
http://www.pcworld.com/news/article/0,aid,119953,00.asp

Links to Articles

ChoicePoint Data Theft Widens To 145,000 People
http://news.com.com/ChoicePoint+data+theft+widens+to+145,000+people/2100-1029_3-5582144.html?tag=st.rn

PIN Scandal 'Worst Hack Ever'; Citibank Only The Start
http://www2.csoonline.com/blog_view.html?CID=19868

ID Theft Hit 3.6 Million In U.S.
http://www2.csoonline.com/blog_view.html?CID=19868

Georgia Technology Authority Hack Exposes Confidential Information of 570,000 Members
http://www.itworldcanada.com/a/News/e292f953-5fcc-4a1e-8fad-838344402d61.html

Scammers Access Data On 35,000 Californians
http://news.com.com/Scammers+access+data+on+35,000+Californians/2100-1029_3-5577122.html?tag=nl

Payroll Firm Pulls Web Services Citing Data Leak
http://news.com.com/Payroll+firm+pulls+Web+services,+citing+data+leak/2100-1029_3-5595316.html?tag=st.rn

Hacker Steals Air Force Officers' Personal Information
http://www.washingtonpost.com/wp-dyn/content/article/2005/08/22/AR2005082201259.html

Undisclosed Number of Verizon Employees at Risk of Identity Theft
http://news.com.com/2061-10789_3-6047682.html

References

- Beyond Fear, Bruce Schneier, **ISBN:** 0387026207
- CSI/FBI 2005 Computer Crime and Security Survey
  - http://www.usdoj.gov/criminal/cybercrime/FBI2005.pdf
- Security Absurdity: The Complete, Unquestionable, And Total Failure of Information Security.
  - Noam Eppel
  - http://www.securityabsurdity.com/failure.php