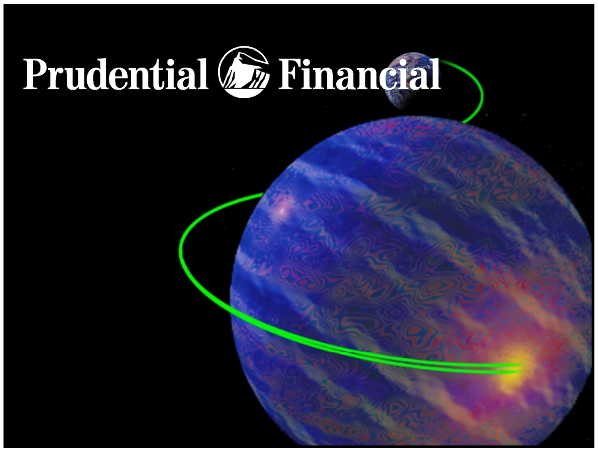
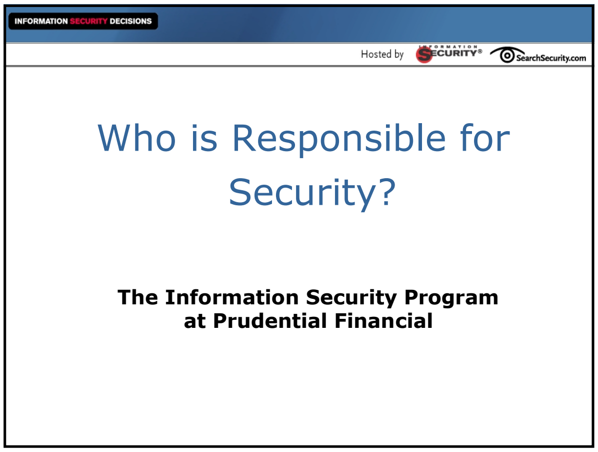


Prudential Financial

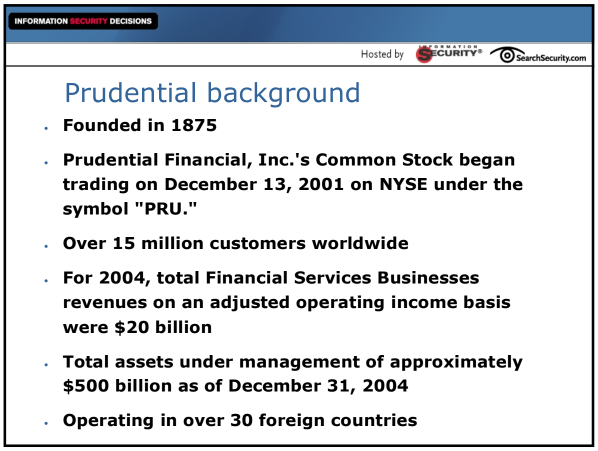


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY® SearchSecurity.com

Who is Responsible for Security?

The Information Security Program at Prudential Financial

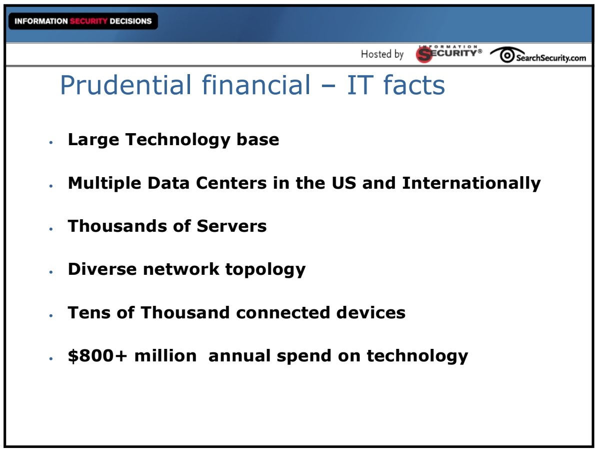


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY® SearchSecurity.com

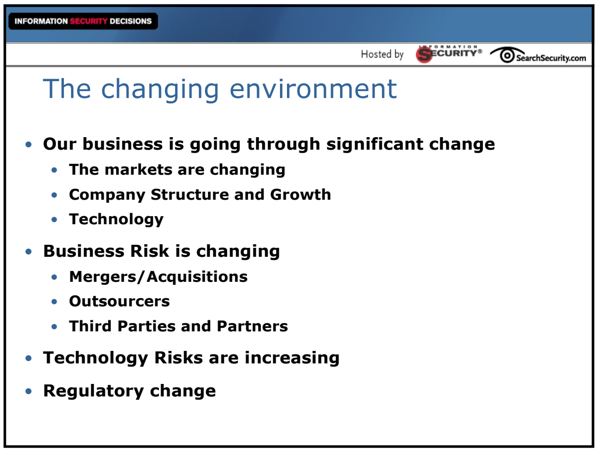
Prudential background

- **Founded in 1875**
- **Prudential Financial, Inc.'s Common Stock began trading on December 13, 2001 on NYSE under the symbol "PRU."**
- **Over 15 million customers worldwide**
- **For 2004, total Financial Services Businesses revenues on an adjusted operating income basis were $20 billion**
- **Total assets under management of approximately $500 billion as of December 31, 2004**
- **Operating in over 30 foreign countries**


INFORMATION SECURITY DECISIONS
Hosted by

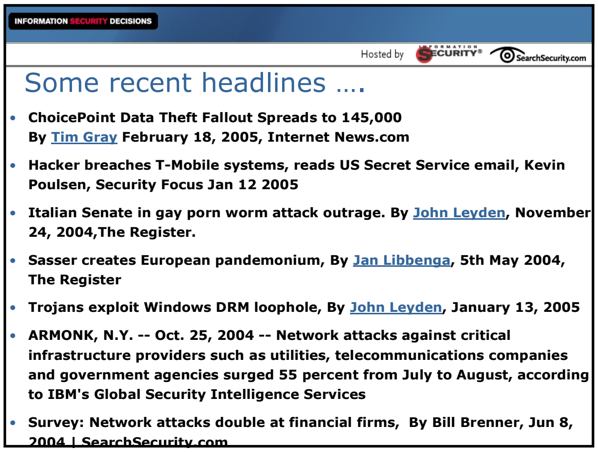
Prudential financial – IT facts

- Large Technology base
- Multiple Data Centers in the US and Internationally
- Thousands of Servers
- Diverse network topology
- Tens of Thousand connected devices
- $800+ million annual spend on technology


INFORMATION SECURITY DECISIONS
Hosted by

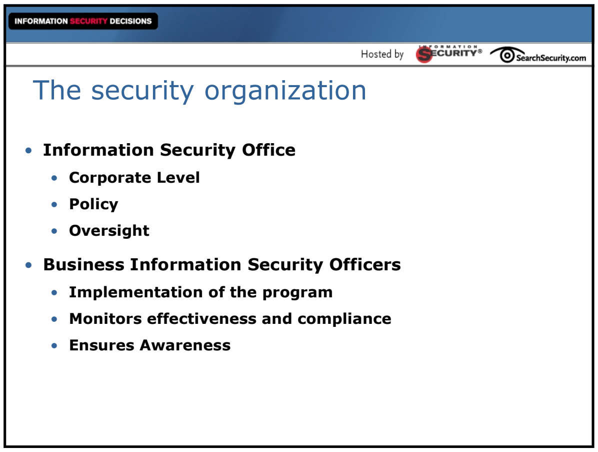
The changing environment

- Our business is going through significant change
  - The markets are changing
  - Company Structure and Growth
  - Technology
- Business Risk is changing
  - Mergers/Acquisitions
  - Outsourcers
  - Third Parties and Partners
- Technology Risks are increasing
- Regulatory change


INFORMATION SECURITY DECISIONS
Hosted by

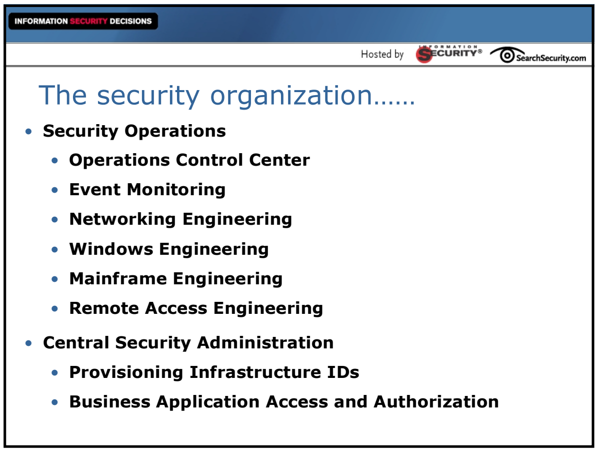
Some recent headlines ….

- ChoicePoint Data Theft Fallout Spreads to 145,000
  By Tim Gray February 18, 2005, Internet News.com
- Hacker breaches T-Mobile systems, reads US Secret Service email, Kevin Poulsen, Security Focus Jan 12 2005
- Italian Senate in gay porn worm attack outrage. By John Leyden, November 24, 2004,The Register.
- Sasser creates European pandemonium, By Jan Libbenga, 5th May 2004, The Register
- Trojans exploit Windows DRM loophole, By John Leyden, January 13, 2005
- ARMONK, N.Y. -- Oct. 25, 2004 -- Network attacks against critical infrastructure providers such as utilities, telecommunications companies and government agencies surged 55 percent from July to August, according to IBM's Global Security Intelligence Services
- Survey: Network attacks double at financial firms, By Bill Brenner, Jun 8, 2004 | SearchSecurity.com



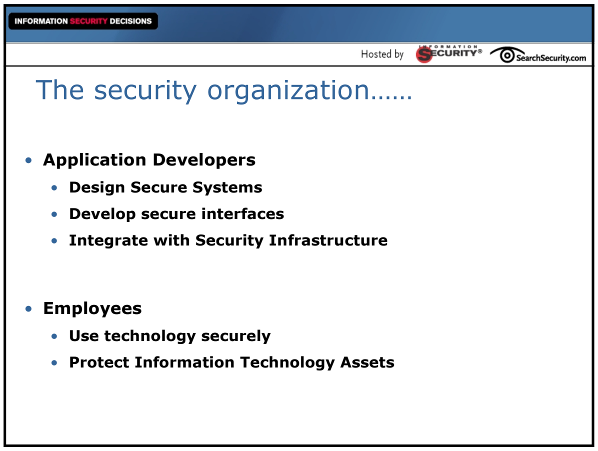
The security organization

- Information Security Office
  - Corporate Level
  - Policy
  - Oversight
- Business Information Security Officers
  - Implementation of the program
  - Monitors effectiveness and compliance
  - Ensures Awareness



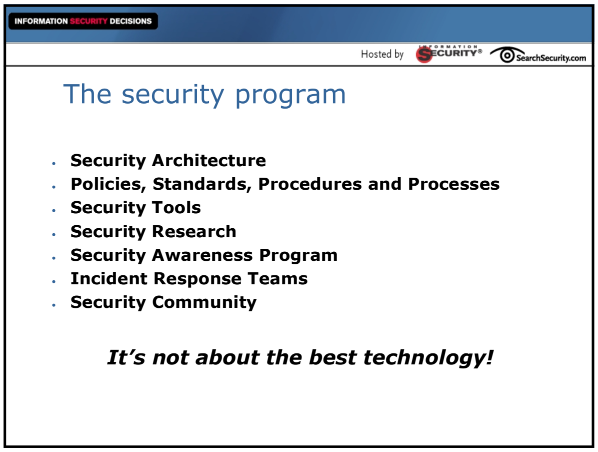
The security organization……

- Security Operations
  - Operations Control Center
  - Event Monitoring
  - Networking Engineering
  - Windows Engineering
  - Mainframe Engineering
  - Remote Access Engineering
- Central Security Administration
  - Provisioning Infrastructure IDs
  - Business Application Access and Authorization



The security organization……

- Application Developers
  - Design Secure Systems
  - Develop secure interfaces
  - Integrate with Security Infrastructure
- Employees
  - Use technology securely
  - Protect Information Technology Assets

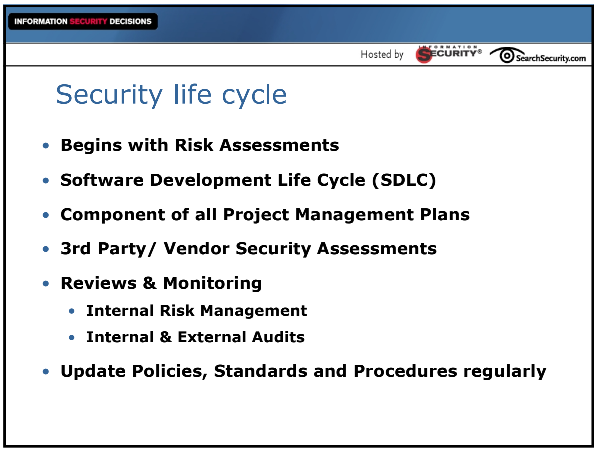

INFORMATION SECURITY DECISIONS

Hosted by

The security program

- Security Architecture
- Policies, Standards, Procedures and Processes
- Security Tools
- Security Research
- Security Awareness Program
- Incident Response Teams
- Security Community

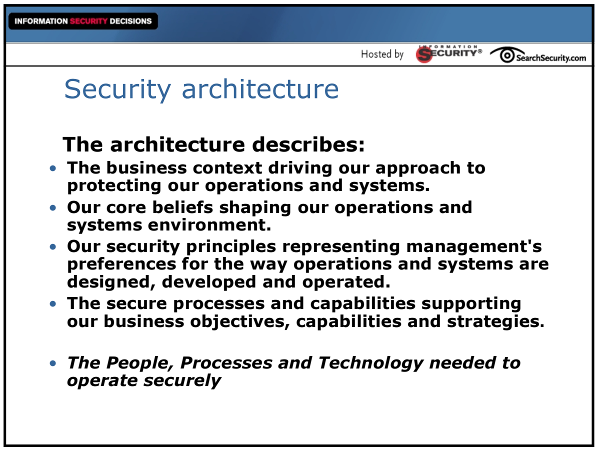
It's not about the best technology!


INFORMATION SECURITY DECISIONS

Hosted by

Security life cycle

- **Begins with Risk Assessments**
- **Software Development Life Cycle (SDLC)**
- **Component of all Project Management Plans**
- **3rd Party/ Vendor Security Assessments**
- **Reviews & Monitoring**
  - **Internal Risk Management**
  - **Internal & External Audits**
- **Update Policies, Standards and Procedures regularly**

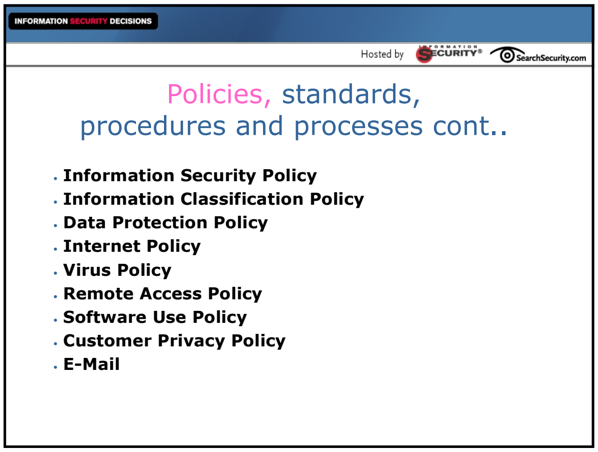

INFORMATION SECURITY DECISIONS

Hosted by

Security architecture

The architecture describes:

- **The business context driving our approach to protecting our operations and systems.**
- **Our core beliefs shaping our operations and systems environment.**
- **Our security principles representing management's preferences for the way operations and systems are designed, developed and operated.**
- **The secure processes and capabilities supporting our business objectives, capabilities and strategies.**
- ***The People, Processes and Technology needed to operate securely***

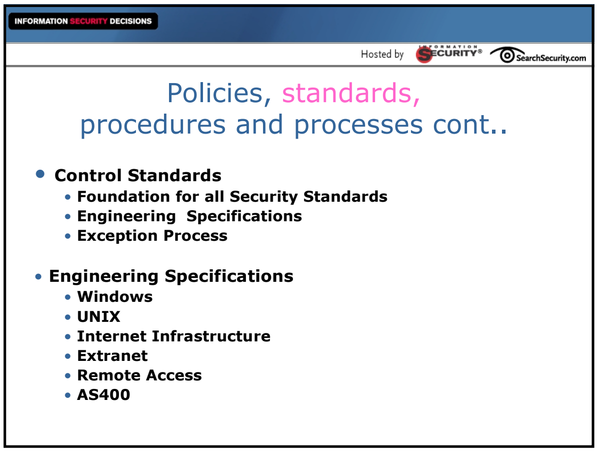


INFORMATION SECURITY DECISIONS

Hosted by

Policies, standards, procedures and processes cont..

- Information Security Policy
- Information Classification Policy
- Data Protection Policy
- Internet Policy
- Virus Policy
- Remote Access Policy
- Software Use Policy
- Customer Privacy Policy
- E-Mail

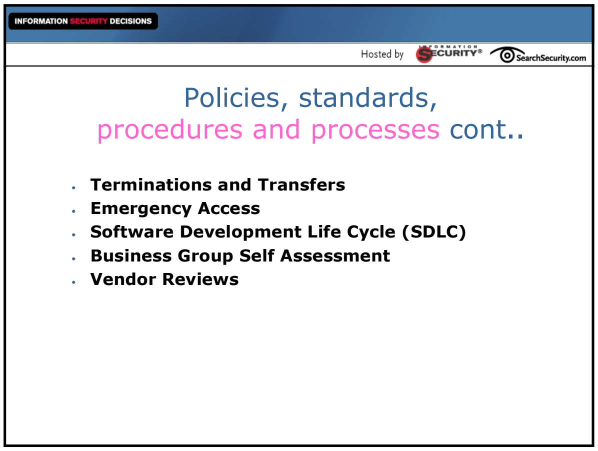


INFORMATION SECURITY DECISIONS

Hosted by

Policies, standards, procedures and processes cont..

- Control Standards
  - Foundation for all Security Standards
  - Engineering Specifications
  - Exception Process
- Engineering Specifications
  - Windows
  - UNIX
  - Internet Infrastructure
  - Extranet
  - Remote Access
  - AS400

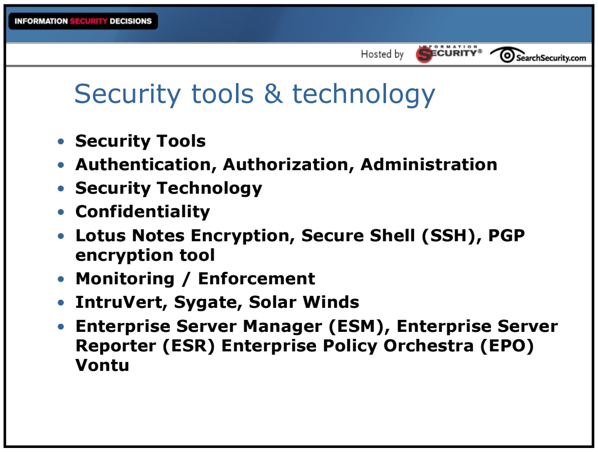


INFORMATION SECURITY DECISIONS

Hosted by

Policies, standards, procedures and processes cont..

- Terminations and Transfers
- Emergency Access
- Software Development Life Cycle (SDLC)
- Business Group Self Assessment
- Vendor Reviews

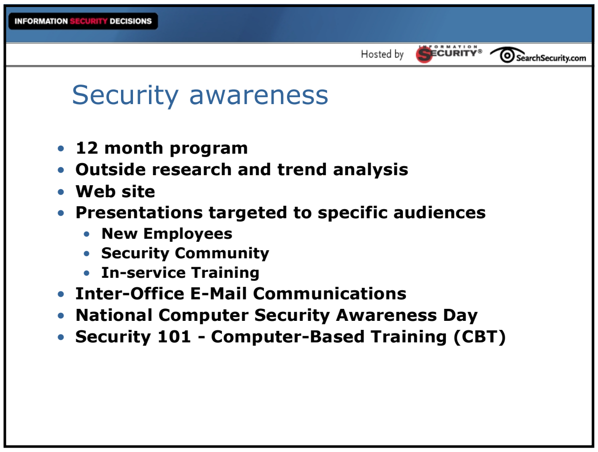


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

Security tools & technology

- Security Tools
- Authentication, Authorization, Administration
- Security Technology
- Confidentiality
- Lotus Notes Encryption, Secure Shell (SSH), PGP encryption tool
- Monitoring / Enforcement
- IntruVert, Sygate, Solar Winds
- Enterprise Server Manager (ESM), Enterprise Server Reporter (ESR) Enterprise Policy Orchestra (EPO) Vontu

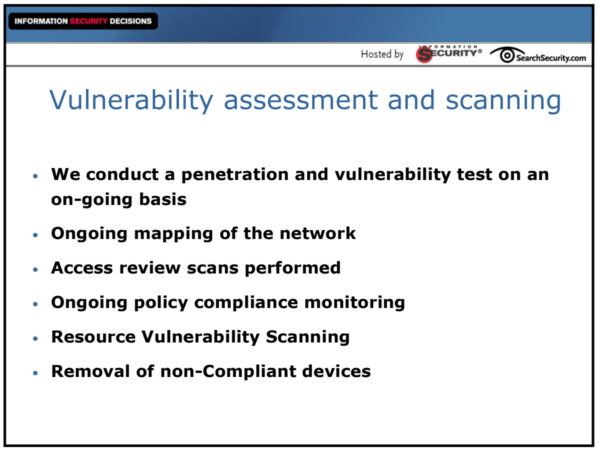


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

Security awareness

- 12 month program
- Outside research and trend analysis
- Web site
- Presentations targeted to specific audiences
  - New Employees
  - Security Community
  - In-service Training
- Inter-Office E-Mail Communications
- National Computer Security Awareness Day
- Security 101 - Computer-Based Training (CBT)

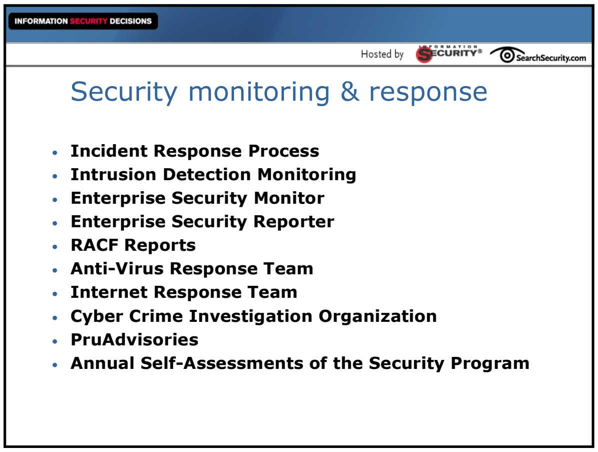


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

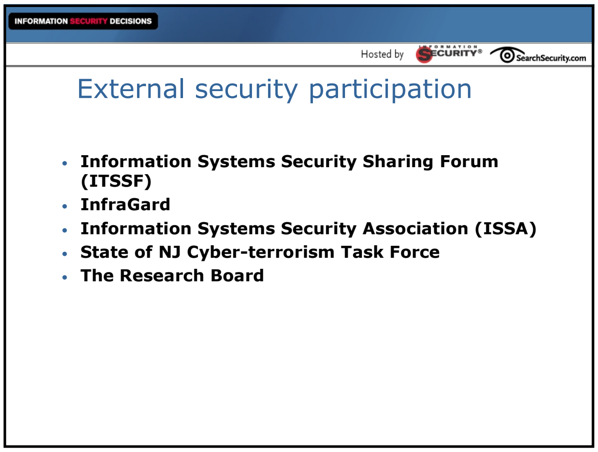
Vulnerability assessment and scanning

- We conduct a penetration and vulnerability test on an on-going basis
- Ongoing mapping of the network
- Access review scans performed
- Ongoing policy compliance monitoring
- Resource Vulnerability Scanning
- Removal of non-Compliant devices



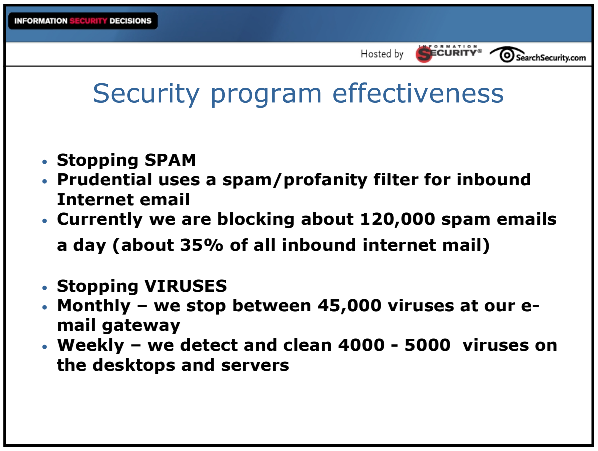
Security monitoring & response

- **Incident Response Process**
- **Intrusion Detection Monitoring**
- **Enterprise Security Monitor**
- **Enterprise Security Reporter**
- **RACF Reports**
- **Anti-Virus Response Team**
- **Internet Response Team**
- **Cyber Crime Investigation Organization**
- **PruAdvisories**
- **Annual Self-Assessments of the Security Program**



External security participation

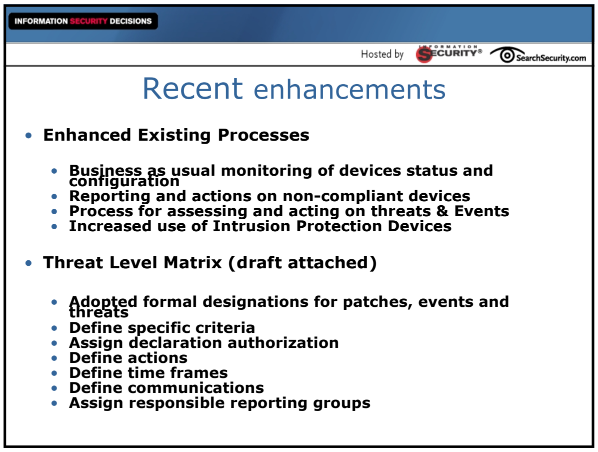
- **Information Systems Security Sharing Forum (ITSSF)**
- **InfraGard**
- **Information Systems Security Association (ISSA)**
- **State of NJ Cyber-terrorism Task Force**
- **The Research Board**



Security program effectiveness

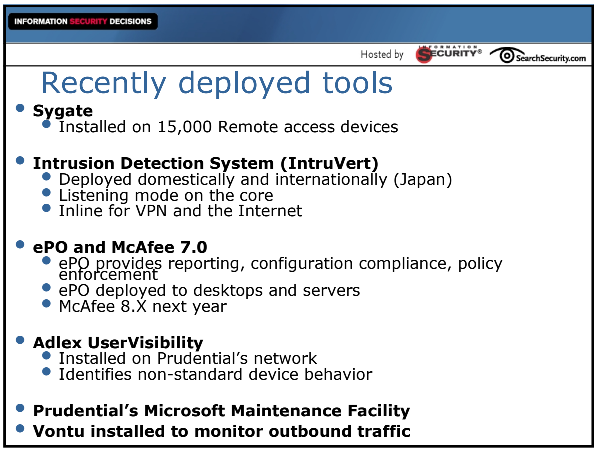
- **Stopping SPAM**
- **Prudential uses a spam/profanity filter for inbound Internet email**
- **Currently we are blocking about 120,000 spam emails a day (about 35% of all inbound internet mail)**

- **Stopping VIRUSES**
- **Monthly – we stop between 45,000 viruses at our e-mail gateway**
- **Weekly – we detect and clean 4000 - 5000 viruses on the desktops and servers**



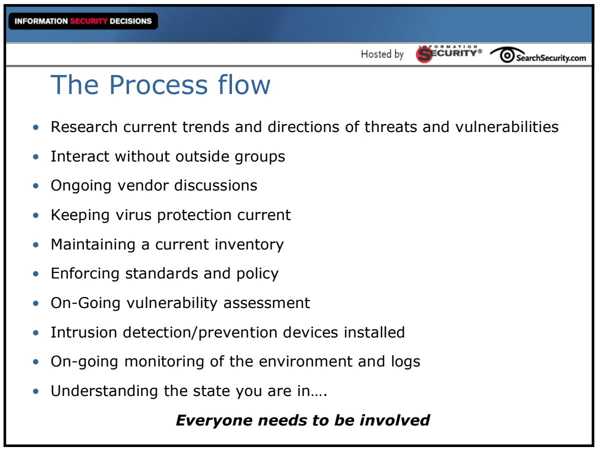
Recent enhancements

- **Enhanced Existing Processes**
  - **Business as usual monitoring of devices status and configuration**
  - **Reporting and actions on non-compliant devices**
  - **Process for assessing and acting on threats & Events**
  - **Increased use of Intrusion Protection Devices**
- **Threat Level Matrix (draft attached)**
  - **Adopted formal designations for patches, events and threats**
  - **Define specific criteria**
  - **Assign declaration authorization**
  - **Define actions**
  - **Define time frames**
  - **Define communications**
  - **Assign responsible reporting groups**



Recently deployed tools

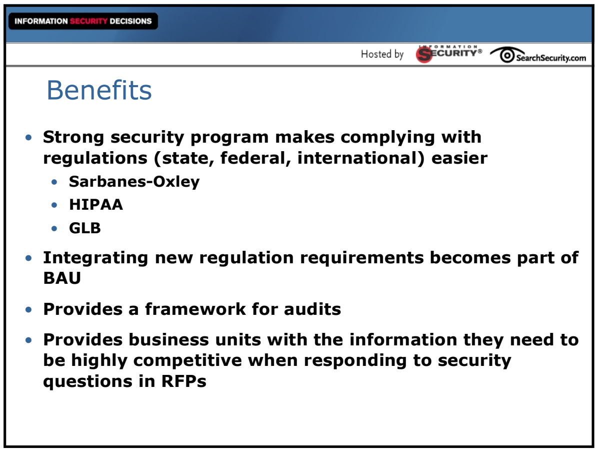
- **Sygate**
  - Installed on 15,000 Remote access devices
- **Intrusion Detection System (IntruVert)**
  - Deployed domestically and internationally (Japan)
  - Listening mode on the core
  - Inline for VPN and the Internet
- **ePO and McAfee 7.0**
  - ePO provides reporting, configuration compliance, policy enforcement
  - ePO deployed to desktops and servers
  - McAfee 8.X next year
- **Adlex UserVisibility**
  - Installed on Prudential’s network
  - Identifies non-standard device behavior
- **Prudential’s Microsoft Maintenance Facility**
- **Vontu installed to monitor outbound traffic**



The Process flow

- Research current trends and directions of threats and vulnerabilities
- Interact without outside groups
- Ongoing vendor discussions
- Keeping virus protection current
- Maintaining a current inventory
- Enforcing standards and policy
- On-Going vulnerability assessment
- Intrusion detection/prevention devices installed
- On-going monitoring of the environment and logs
- Understanding the state you are in….

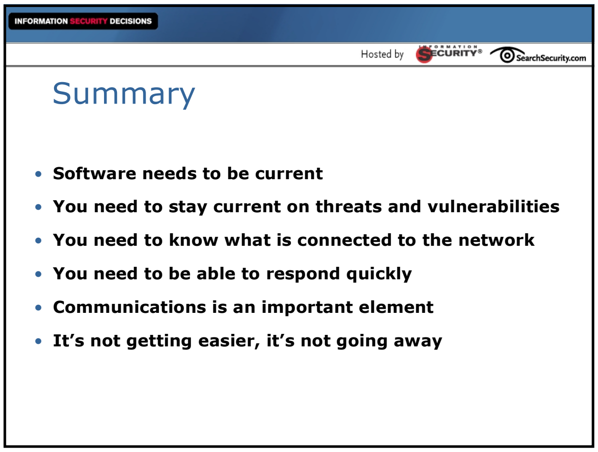
Everyone needs to be involved


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY® SearchSecurity.com

Benefits

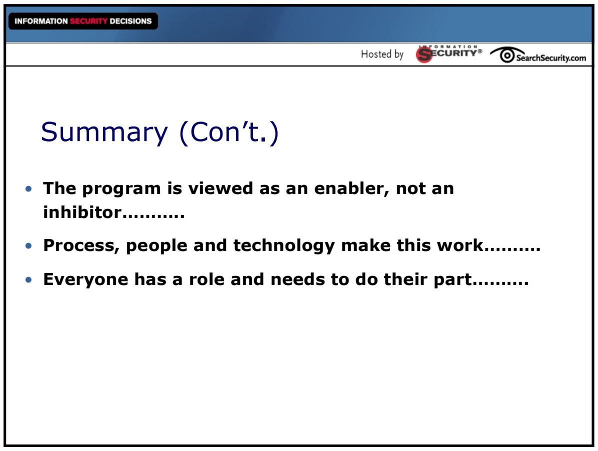
- Strong security program makes complying with regulations (state, federal, international) easier
  - Sarbanes-Oxley
  - HIPAA
  - GLB
- Integrating new regulation requirements becomes part of BAU
- Provides a framework for audits
- Provides business units with the information they need to be highly competitive when responding to security questions in RFPs


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY® SearchSecurity.com

Summary

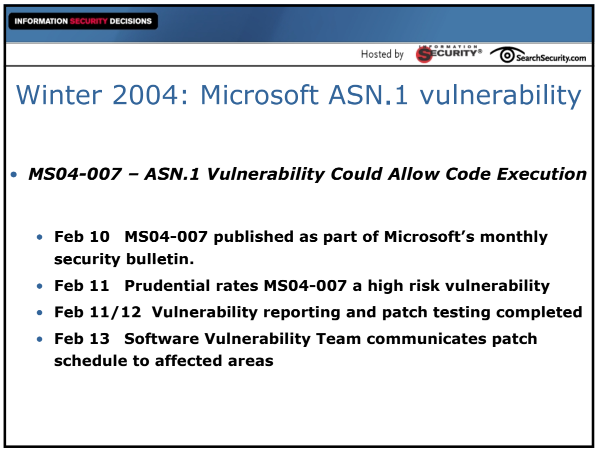
- Software needs to be current
- You need to stay current on threats and vulnerabilities
- You need to know what is connected to the network
- You need to be able to respond quickly
- Communications is an important element
- It’s not getting easier, it’s not going away


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY® SearchSecurity.com

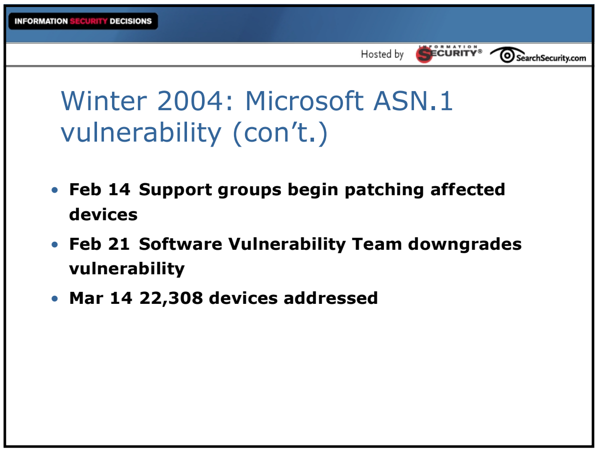
Summary (Con’t.)

- The program is viewed as an enabler, not an inhibitor………..
- Process, people and technology make this work……….
- Everyone has a role and needs to do their part……….



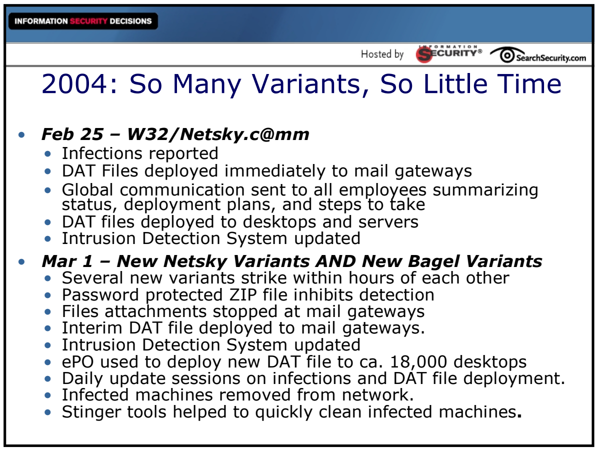
Winter 2004: Microsoft ASN.1 vulnerability

- ***MS04-007 – ASN.1 Vulnerability Could Allow Code Execution***
  - **Feb 10 MS04-007 published as part of Microsoft's monthly security bulletin.**
  - **Feb 11 Prudential rates MS04-007 a high risk vulnerability**
  - **Feb 11/12 Vulnerability reporting and patch testing completed**
  - **Feb 13 Software Vulnerability Team communicates patch schedule to affected areas**



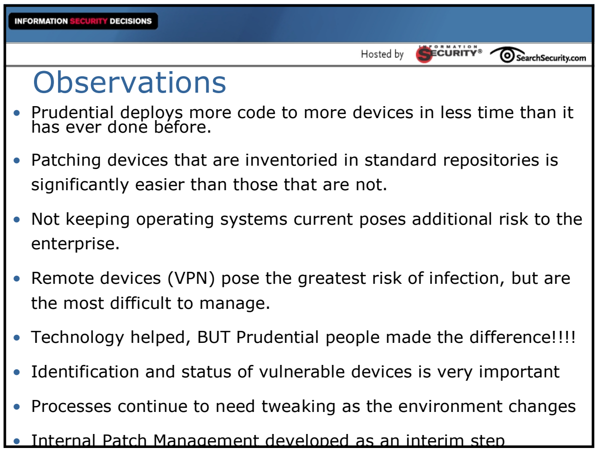
Winter 2004: Microsoft ASN.1 vulnerability (con't.)

- **Feb 14 Support groups begin patching affected devices**
- **Feb 21 Software Vulnerability Team downgrades vulnerability**
- **Mar 14 22,308 devices addressed**



2004: So Many Variants, So Little Time

- ***Feb 25 – W32/Netsky.c@mm***
  - Infections reported
  - DAT Files deployed immediately to mail gateways
  - Global communication sent to all employees summarizing status, deployment plans, and steps to take
  - DAT files deployed to desktops and servers
  - Intrusion Detection System updated
- ***Mar 1 – New Netsky Variants AND New Bagel Variants***
  - Several new variants strike within hours of each other
  - Password protected ZIP file inhibits detection
  - Files attachments stopped at mail gateways
  - Interim DAT file deployed to mail gateways.
  - Intrusion Detection System updated
  - ePO used to deploy new DAT file to ca. 18,000 desktops
  - Daily update sessions on infections and DAT file deployment.
  - Infected machines removed from network.
  - Stinger tools helped to quickly clean infected machines**.**

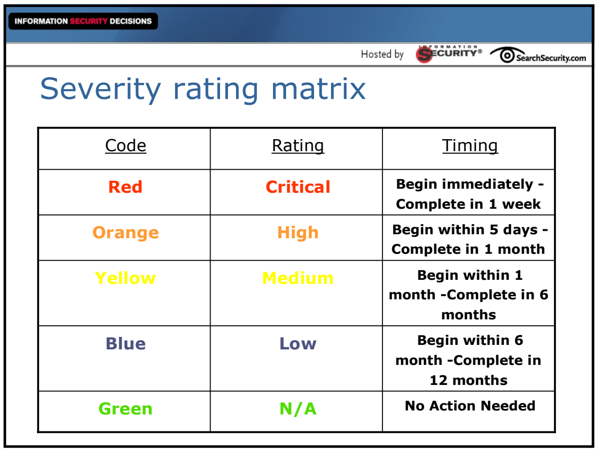


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

Observations

- Prudential deploys more code to more devices in less time than it has ever done before.
- Patching devices that are inventoried in standard repositories is significantly easier than those that are not.
- Not keeping operating systems current poses additional risk to the enterprise.
- Remote devices (VPN) pose the greatest risk of infection, but are the most difficult to manage.
- Technology helped, BUT Prudential people made the difference!!!!
- Identification and status of vulnerable devices is very important
- Processes continue to need tweaking as the environment changes
- Internal Patch Management developed as an interim step

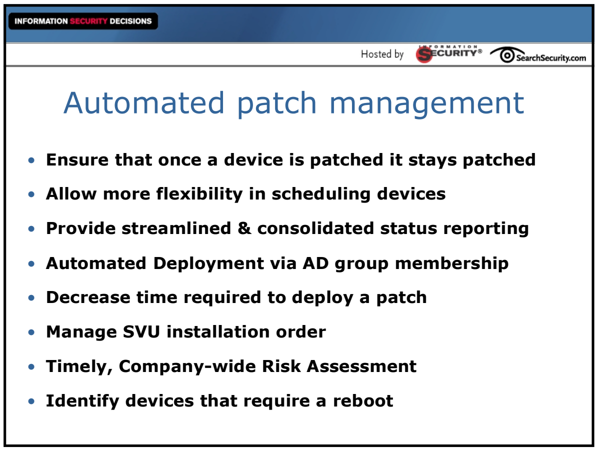


INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

Severity rating matrix

Code	Rating	Timing
Red	Critical	**Begin immediately - Complete in 1 week**
Orange	High	**Begin within 5 days - Complete in 1 month**
Yellow	Medium	**Begin within 1 month -Complete in 6 months**
Blue	Low	**Begin within 6 month -Complete in 12 months**
Green	N/A	**No Action Needed**



INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

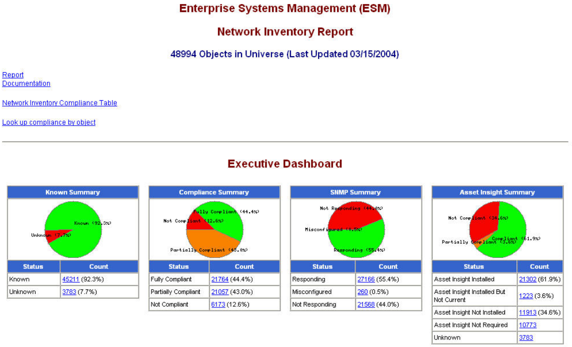
Automated patch management

- **Ensure that once a device is patched it stays patched**
- **Allow more flexibility in scheduling devices**
- **Provide streamlined & consolidated status reporting**
- **Automated Deployment via AD group membership**
- **Decrease time required to deploy a patch**
- **Manage SVU installation order**
- **Timely, Company-wide Risk Assessment**
- **Identify devices that require a reboot**

Patch management summary

- Prudential's operational patch management process uses the existing Active Directory (AD) Organizational Unit (OU) structure to provide server and workstation support groups the ability to add -- according to their schedule and user requirements -- devices to predefined patch groups.
- Once a device is defined to a patch group, it will be patched via SMS/SUS.
- Once in a patch group, a device will remain patched; i.e., if the patch is uninstalled for any reason, SUS will detect this and repatch the machine.
- SMS/SUS also provides detailed reporting capabilities on the status of patches.

Enterprise systems management



Enterprise Systems Management (ESM)

Network Inventory Report

48994 Objects in Universe (Last Updated 03/15/2004)

Report
Documentation

Network Inventory Compliance Table

Look up compliance by object

Executive Dashboard

Known Summary

Status	Count
Known	45211 (92.3%)
Unknown	3783 (7.7%)

Compliance Summary

Status	Count
Fully Compliant	21764 (44.4%)
Partially Compliant	21057 (43.0%)
Not Compliant	6173 (12.6%)

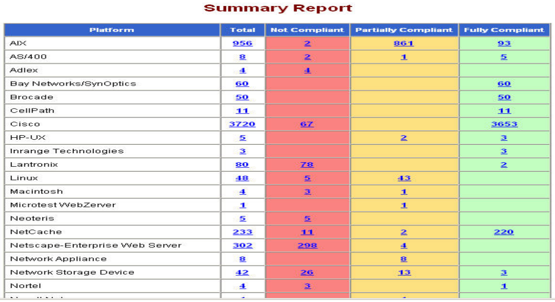
SNMP Summary

Status	Count
Responding	27166 (55.4%)
Misconfigured	260 (0.5%)
Not Responding	21568 (44.0%)

Asset Insight Summary

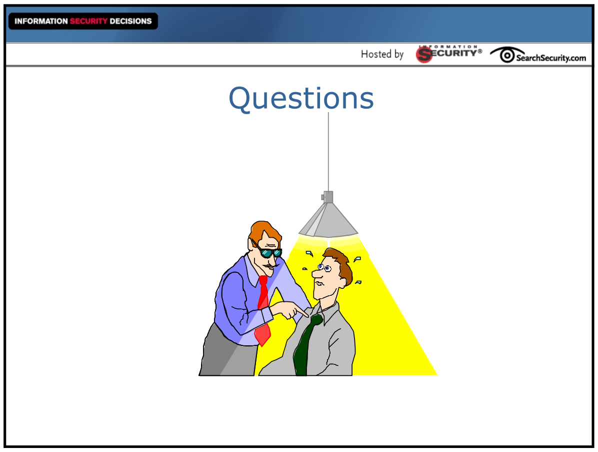
Status	Count
Asset Insight Installed	21302 (61.9%)
Asset Insight Installed But Not Current	1223 (3.6%)
Asset Insight Not Installed	11913 (34.6%)
Asset Insight Not Required	10773
Unknown	3783

Summary report



Summary Report

Platform	Total	Not Compliant	Partially Compliant	Fully Compliant
AIX	956	2	861	93
AS/400	8	2	1	5
Adlex	4	4		
Bay Networks/SynOptics	60			60
Brocade	50			50
CellPath	11			11
Cisco	3720	67		3653
HP-UX	5		2	3
Inrange Technologies	3			3
Lantronix	80	78		2
Linux	48	5	43	
Macintosh	4	3	1	
Microtest WebZerver	1		1	
Neoteris	5	5		
NetCache	233	11	2	220
Netscape-Enterprise Web Server	302	298	4	
Network Appliance	8		8	
Network Storage Device	42	26	13	3
Nortel	4	3		1



INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY® SearchSecurity.com

Questions