



Virginia Information Technologies Agency

Cyber Security within the Commonwealth of Virginia

Sam Nixon and Michael Watson
CIO and CISO

Joint Commission on Technology and Science
October 16th 2012



Recent Cyber Security Headlines

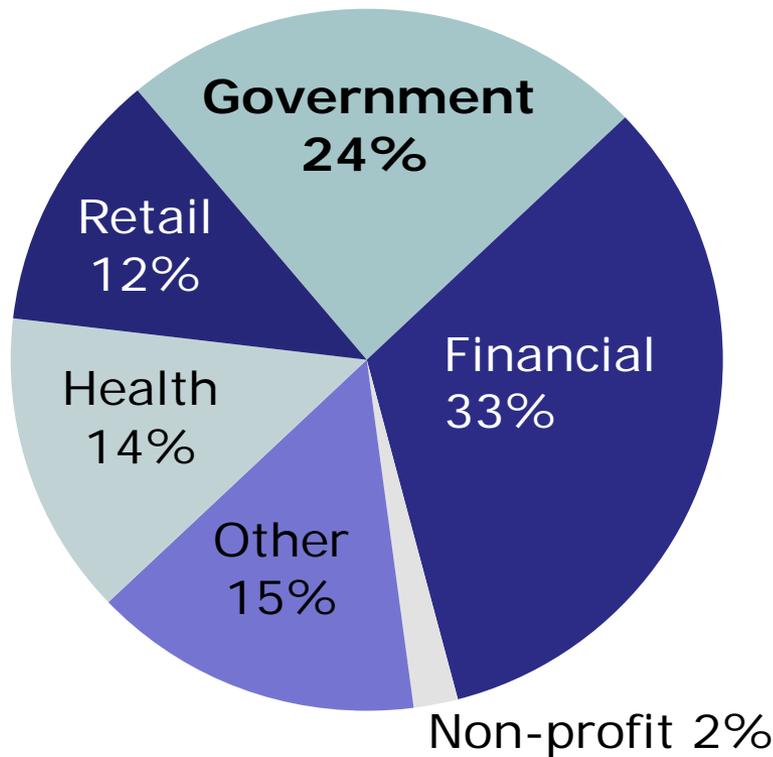
- Utah Department of Health
 - 580,000 citizen records compromised
 - Cost between \$2 and \$10 million dollars
- South Carolina Department of Revenue
 - 3.6 million citizen records compromised
 - Cost of approximately \$26 million dollars
- State of Alabama
 - Unknown current compromise of systems
- Federal Reserve Bank
 - Anonymous compromised systems



Cause of the incidents

- Lack of basic security controls
 - Some not required, some not in place
- Password policies not strict enough
 - Default password not changed
- Agencies not following security recommendations
 - Not using centralized services
 - Not following security policies, standards, or guidelines

Government: #2 Target of Cyber Attacks



Security breaches of over 1 Million records

Source: Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, Aug 2012

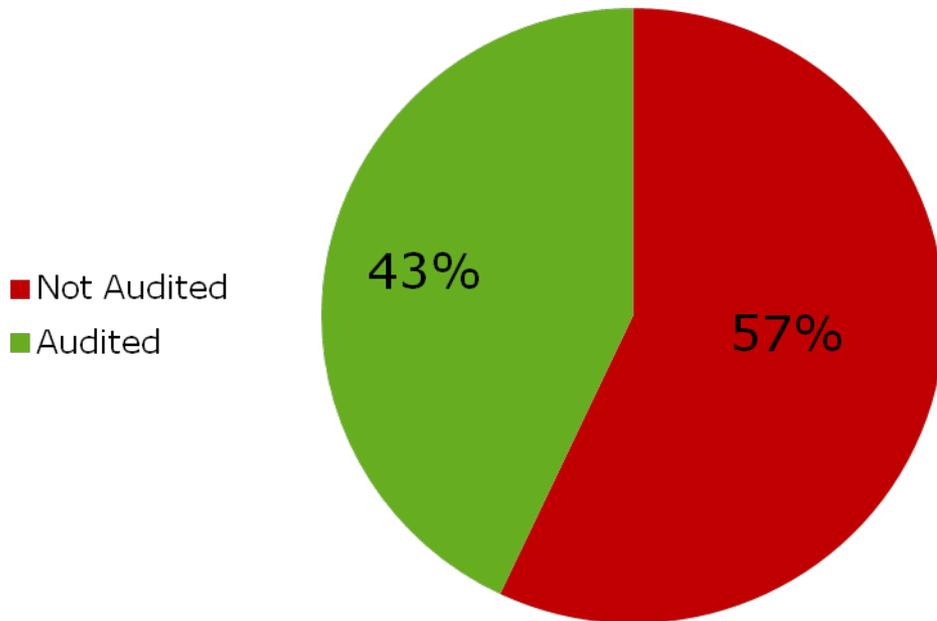
Virginia

- 117,842,683 attack attempts
- 698,942,080 spam messages

*Jan – Dec 2012, transformed agencies only

Annual Review of Agency Security

Sensitive IT Systems Audited in the last 3 years

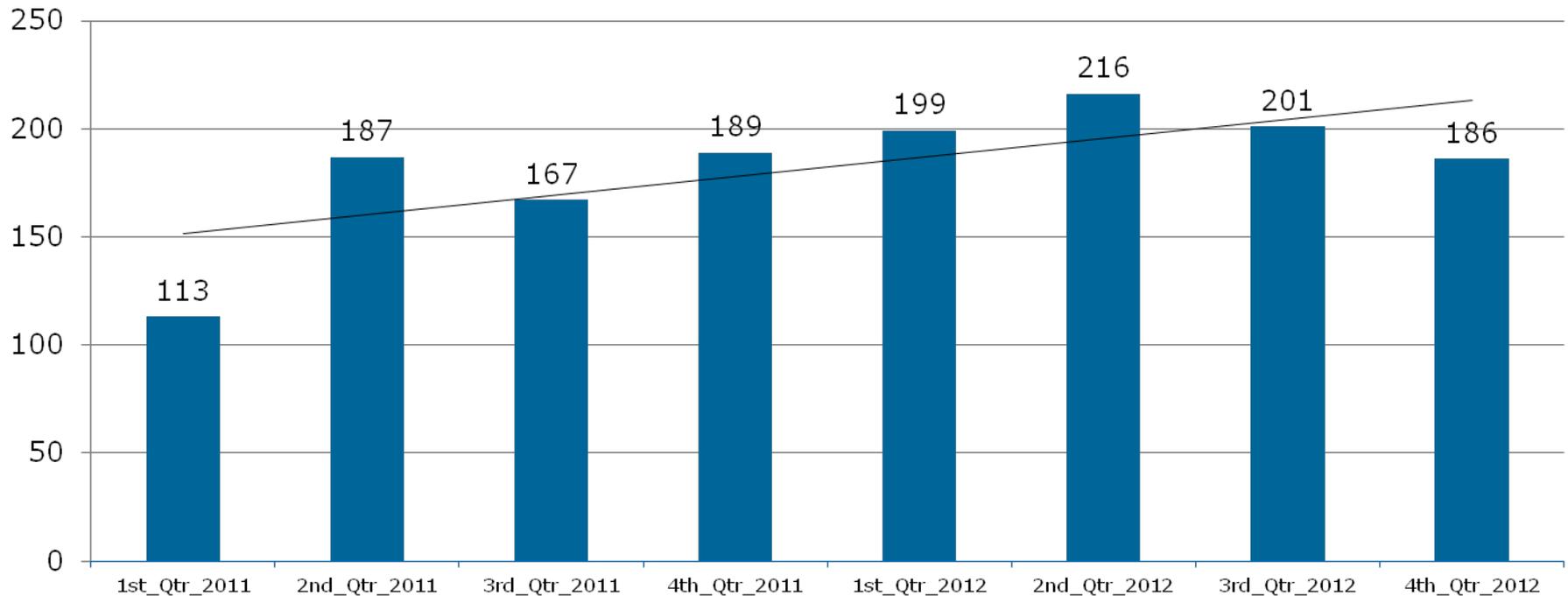


- 2011 Review of IT systems found agency reviews not keeping pace with increased use of IT
- 2012 Review projected at 56%



Increase in Security Incidents

Incident Trends by Quarter
2011 - 2012





Attacks on the Commonwealth - 2012

- Denial of Service
- Theft of agency administrator credentials
- Compromise of unsupported software
- Exploitation of agency administrator accounts
- Nation state infiltration
- Website defacements
- Impersonation of the Commonwealth



What is VITA doing about it?

- Streamline security policies standards and guidelines
 - Align with federal requirements
 - Release template policies for agencies to use
 - Will include an eventual tightening of security controls
- Upgrade security infrastructure
 - New software running on workstations
 - Replaced central intrusion detection devices
 - Adding additional network monitoring devices
 - Introduced additional content filtering
 - Replaced central log collection and correlation device



Upgrades aren't enough

- Additional security services
 - SSL VPN
 - Encryption of data at rest
 - Encryption of all work stations
 - Expansion of two factor authentication (soft tokens)
 - Mobile Device Management
- Risk management program
 - Identify where the most significant risks to the Commonwealth exist
 - Prioritize resources and efforts based on risk

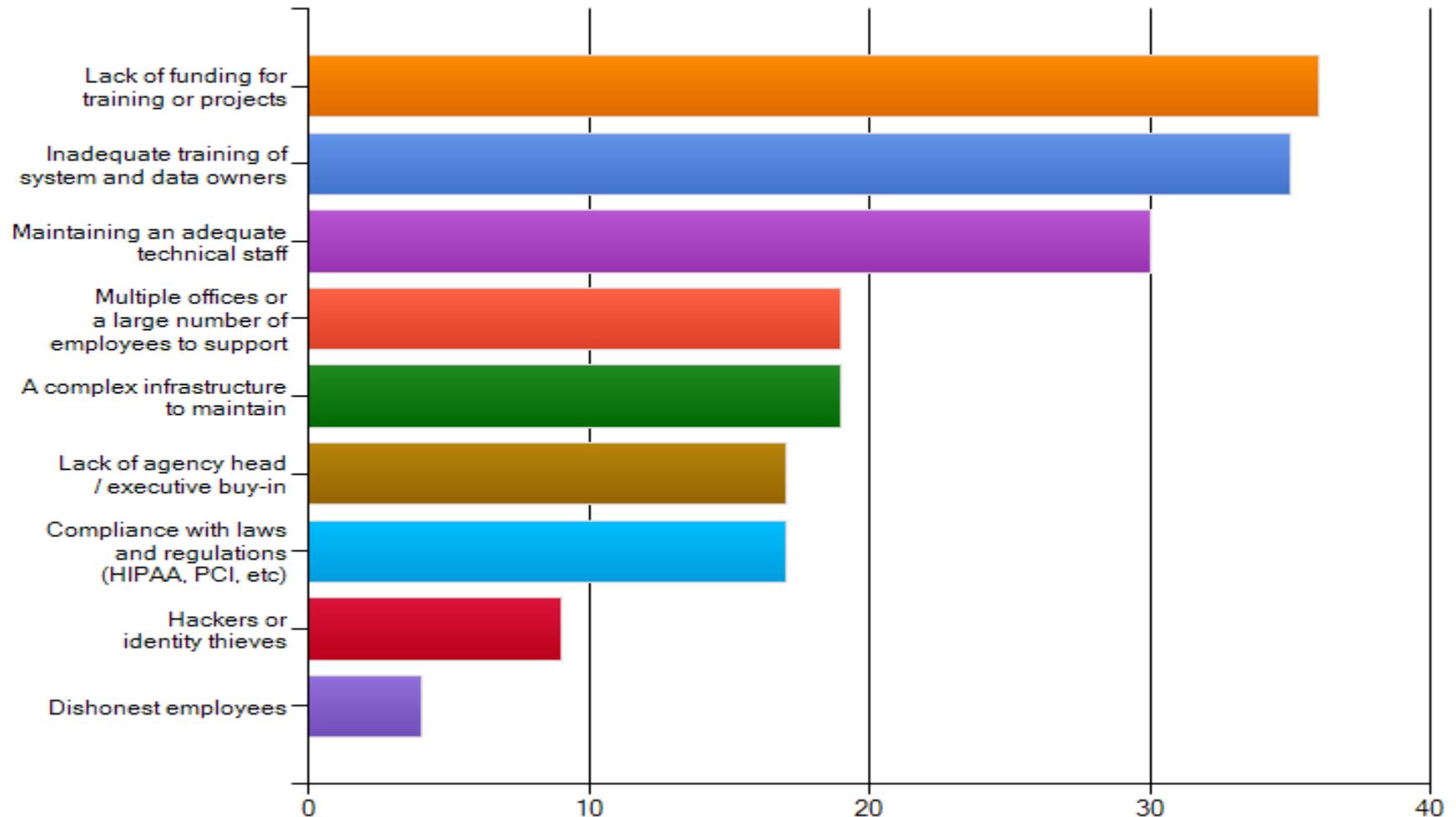


Okay VITA, sounds like you've got this...

- Agencies need to move more quickly with security issues
 - Local Administrator Account Project – 2 years running
 - JAVA – 9 months to get approvals
 - Windows 2000 still exists out at agencies
 - SQL 2000 over 200 agency supported installs on servers alone (not including workstations)
- VITA cannot continue to repeatedly request that agencies comply with security requirements and efforts



What challenges do you feel are the most significant in terms of information security (select up to 3)?



Source: Survey of security representatives from Commonwealth agencies



What do you want to do about it?

- Implementation of a Commonwealth risk management program
 - More frequent and accurate reporting of agency risk level
- Investigating options to require agencies remain in good standing
 - Agency is on track to remediate end of life software
 - Agency participates in planning for mitigation of security issues and/or risks
 - Sensitive systems have been audited
 - Corrective action plans are progressing at a reasonable rate



Questions?

