



# Cyber Security within the Commonwealth of Virginia

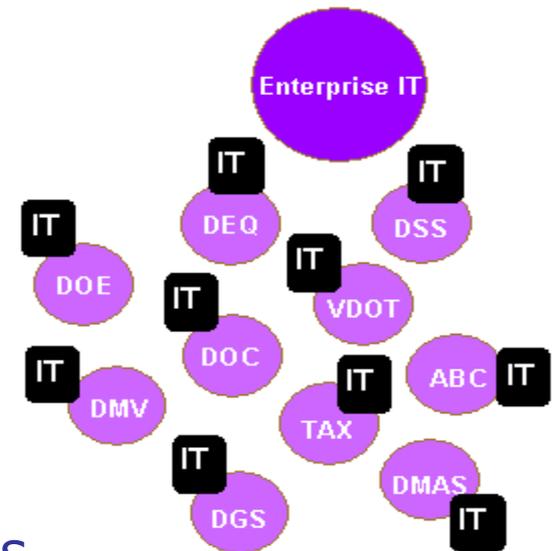
**Sam Nixon and Michael Watson**  
CIO and CISO

---

Joint Commission on Technology and Science  
October 16<sup>th</sup> 2012

# State of Technology, Pre-VITA

- 90+ independent, autonomous IT shops
  - Duplicative systems
  - Few metrics on performance & spending
  - Inability to leverage buying power or manage investments
- Aging, decades-old infrastructure
  - Inadequate security
  - Limited disaster planning
  - Obstacles to sharing data across agencies
- Millions \$ in failed IT projects
  - No project management
- Unsustainable





# Mandate for Change

- Executive & Legislative Branch leaders called for
  - ***Business-like approach to managing IT services across the enterprise of state government***
- Step 1: 2003 - Virginia Information Technologies Agency
  - Introduced Concept of “Shared Services” (private cloud)
    - Statewide IT *infrastructure* for in-scope government entities
  - Centralized oversight of IT projects, security, procurement, standards, policy and procedures
  - Excludes direct control of agency applications
- Step 2: 2005 - IT Program with Northrop Grumman, Transformation
- Step 3: Facilitate Enterprise Applications and Services
  - Enterprise Email
  - Performance Budgeting, Cardinal, eSOA, EDM, CAS



# CoVA IT Infrastructure

## Computers

57,977 PCs  
3,485 servers

## Mailboxes

59,866 accounts

## Data storage

1.4 petabytes

## Mainframes (2)

IBM  
Unisys

## Communications

~55,000 desk phones  
~3,600 handhelds (PDAs)  
~11,000+ cell phones

## Networks

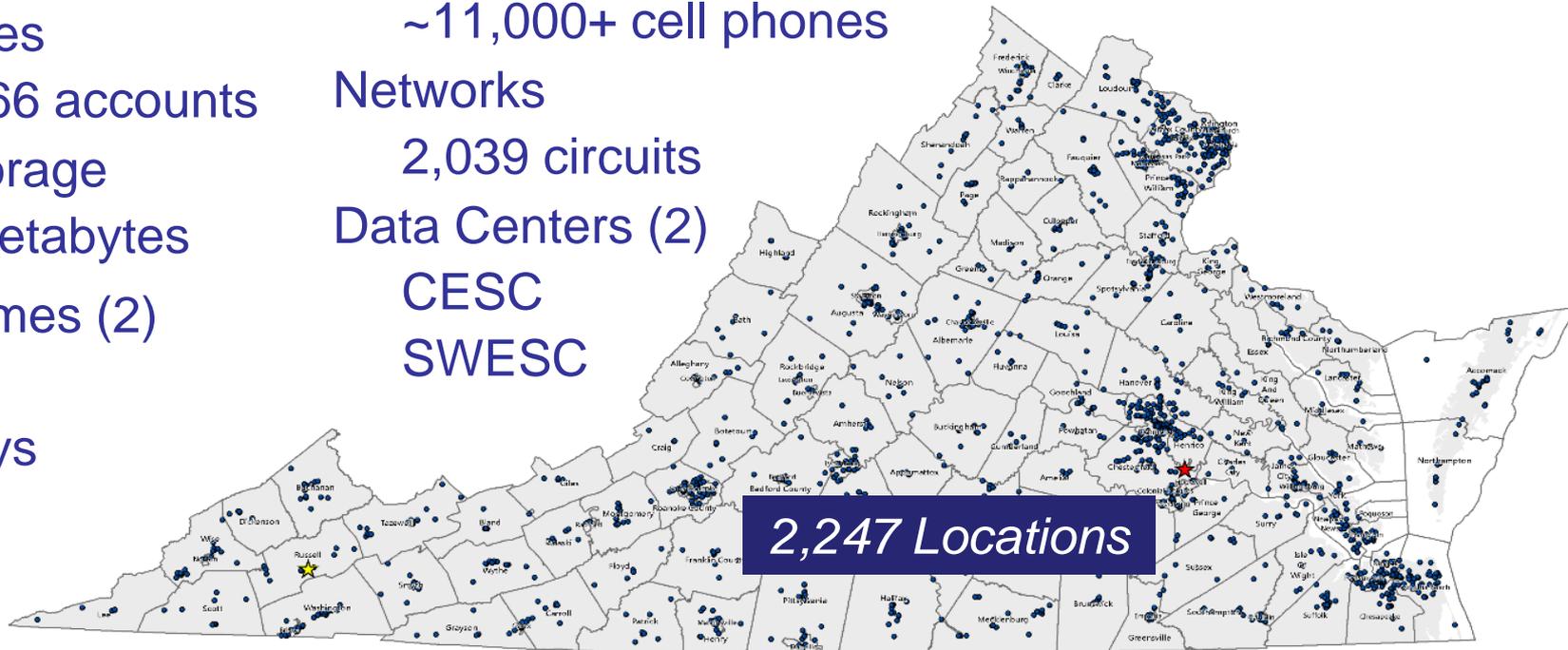
2,039 circuits

## Data Centers (2)

CESC  
SWESC

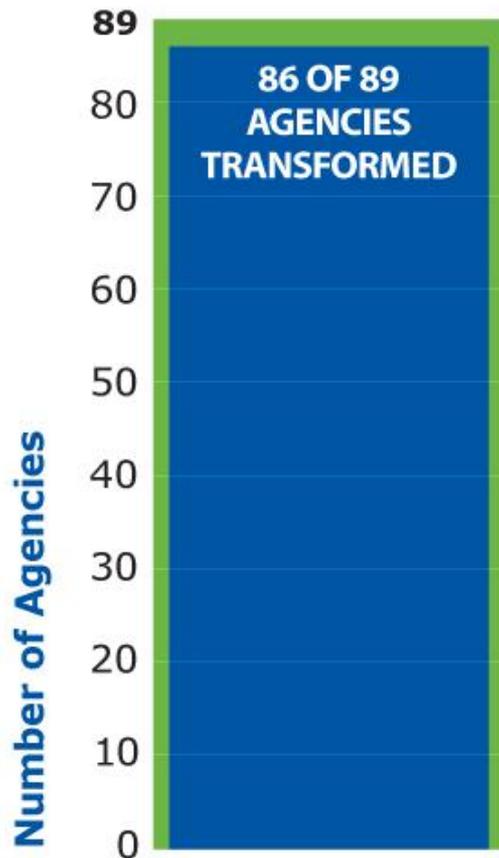
## Printers

5,674 network  
22,000+ desktop





# Transformation Status



- *Critical mass* achieved
  - 95+% complete
- Standard, reliable and secure
- Remaining agencies:
  - VDEM, VSP, & VEC



## Technology Roadmap

- Transformed agencies benefit from continuous upgrades, including:
  - 14,000 PCs refreshed (Jan 11 – Aug 12)
  - Enterprise Email System migration complete
  - Windows 7 (underway)
  - Office 2010 (underway)
  - Enterprise Storage Systems (CESC)
  - Mainframe Upgrades (IBM, Unisys)
  - Support systems and tools
    - Help desk, monitoring, network, security and more

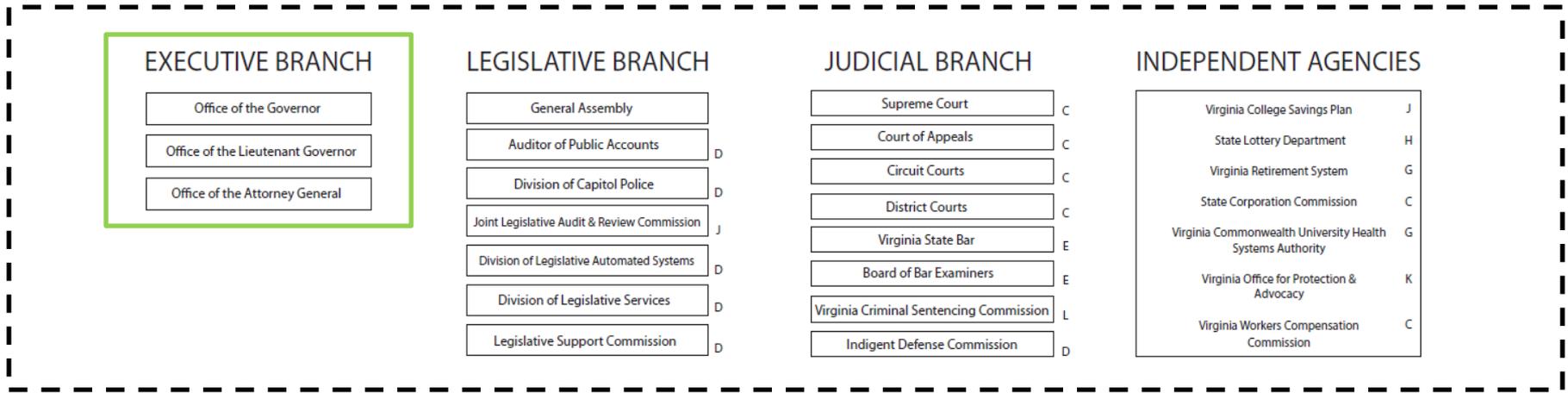


## Cyber Security in the Commonwealth

- Information security framework
- Threats to the Commonwealth
- State of security in the Commonwealth
- Existing challenges
- Future plans



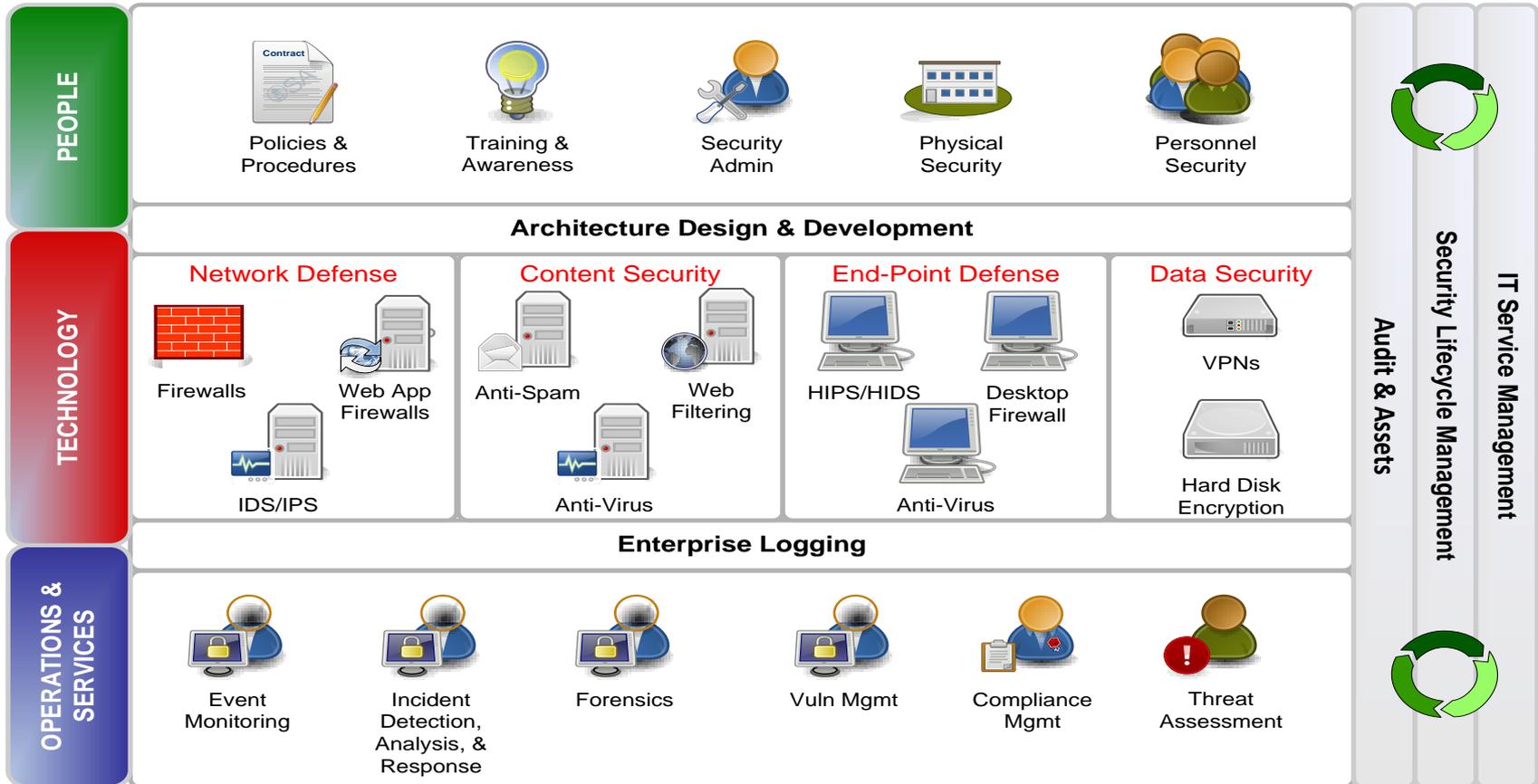
# Information Security in the Commonwealth



VITA is tasked with security governance over all three branches of state government.

VITA controls the infrastructure (hardware) of executive branch agencies. Agencies remain responsible for application management.

# Security Strategy



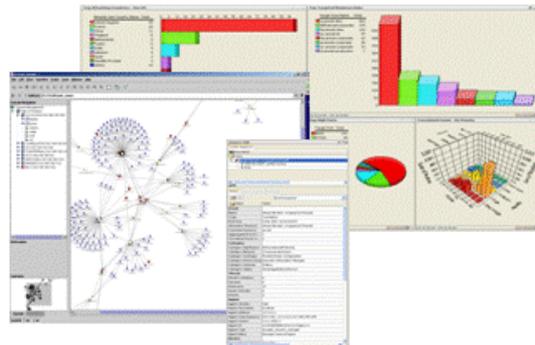


# The Information Security Program

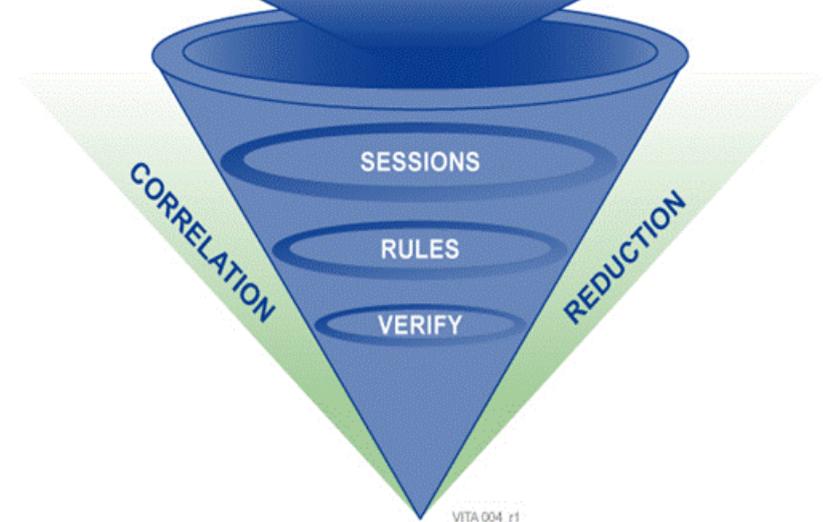
- Two Primary Documents
  - Information Security Policy (SEC500)
  - Information Security Standard (SEC501)
- Policy Directives
  - Must comply with security baseline in SEC501
  - Agency head responsible for maintaining security
- Standard Requirements
  - Includes required security controls to protect Commonwealth data

# Security Situational Awareness

- Enterprise Security Operations & Visibility
  - 24x7 operations
  - Event logging and alerts across the enterprise
  - Understanding of the enterprise defense posture
  - Shared SA across agencies



Firewall Log	IDS Event	Server Log
Switch Log	Firewall Cfg.	AV Alert
Switch Cfg.	NAT Cfg.	App Log
Router Cfg.	Netflow	VA Scanner



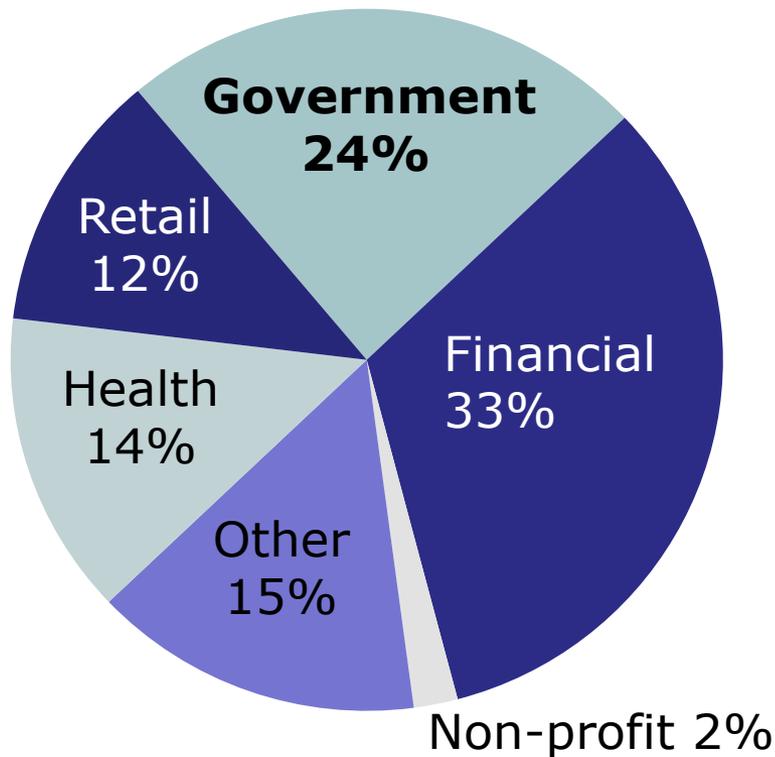
VITA 004\_r1



## IT Security – Current State

- Security Architecture and Standards
- Protecting CoVA Data 24 x 7 x 365
  - Intrusion detection & vulnerability scanning
  - Antivirus & firewalls
  - Spam & web content filtering
  - Centralized & automated software patching
  - Secure remote network access (2-Factor VPN)
  - Encrypted internal email
- Intelligence & Information Sharing
  - Collaborating with FBI, DHS and others

# 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

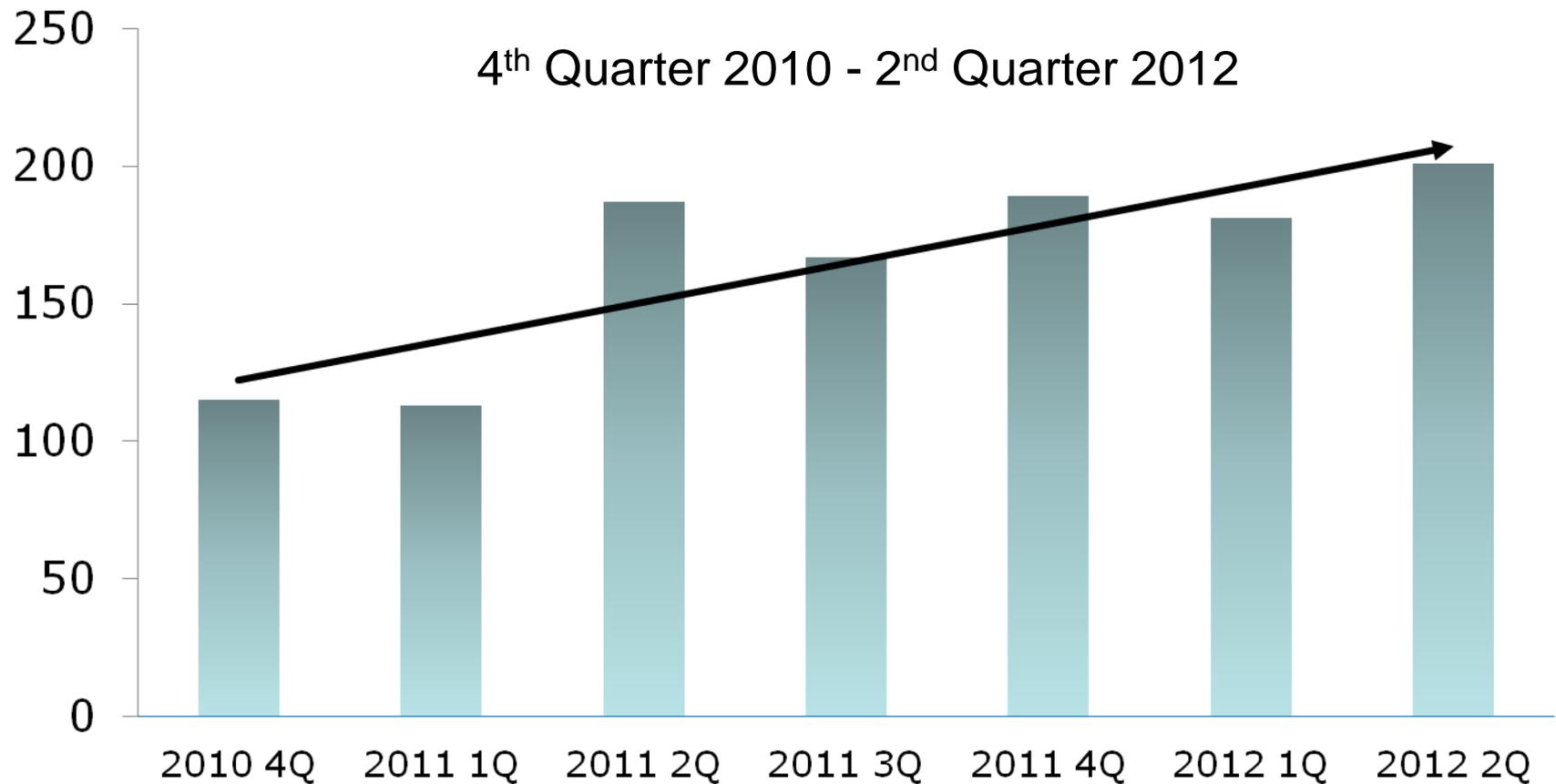
- 70,947,657 attack attempts
- 323,064,576 spam messages

\*Jan – Jun 2012, transformed agencies only

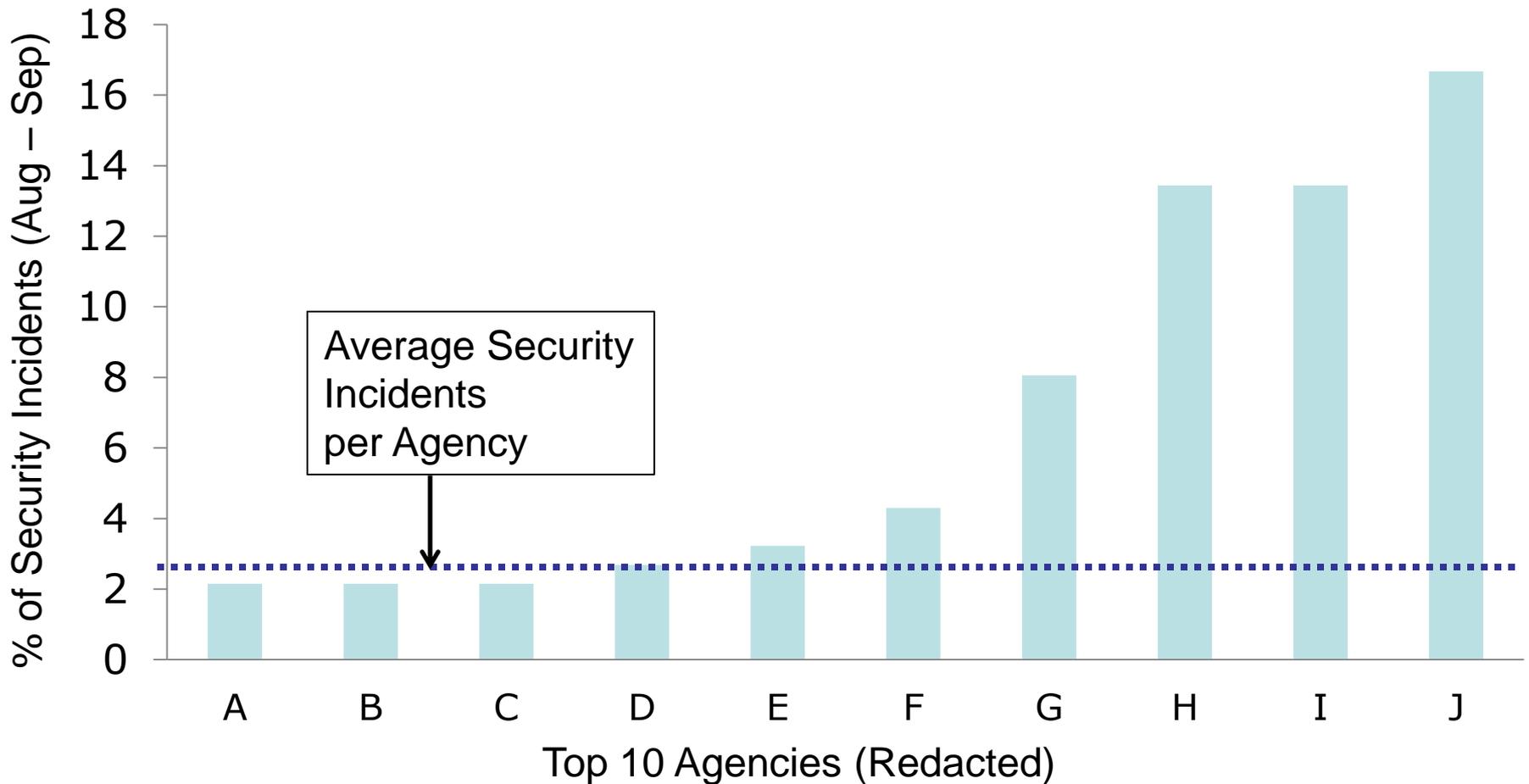
# Attack Attempts on CoVA Network



# Increase in Security Incidents

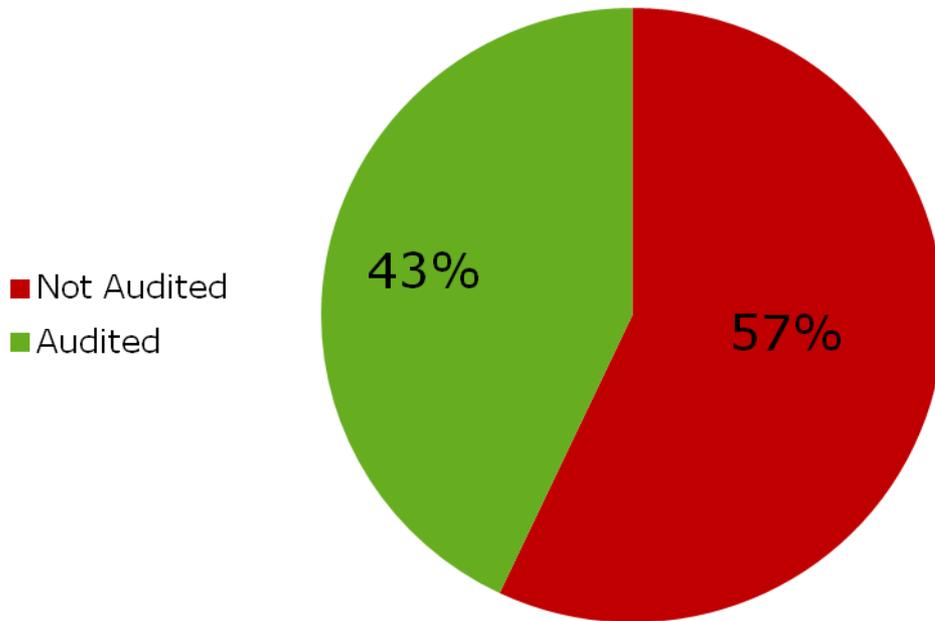


# Incident Rate Varies by Agency



# Annual Review of Agency Security

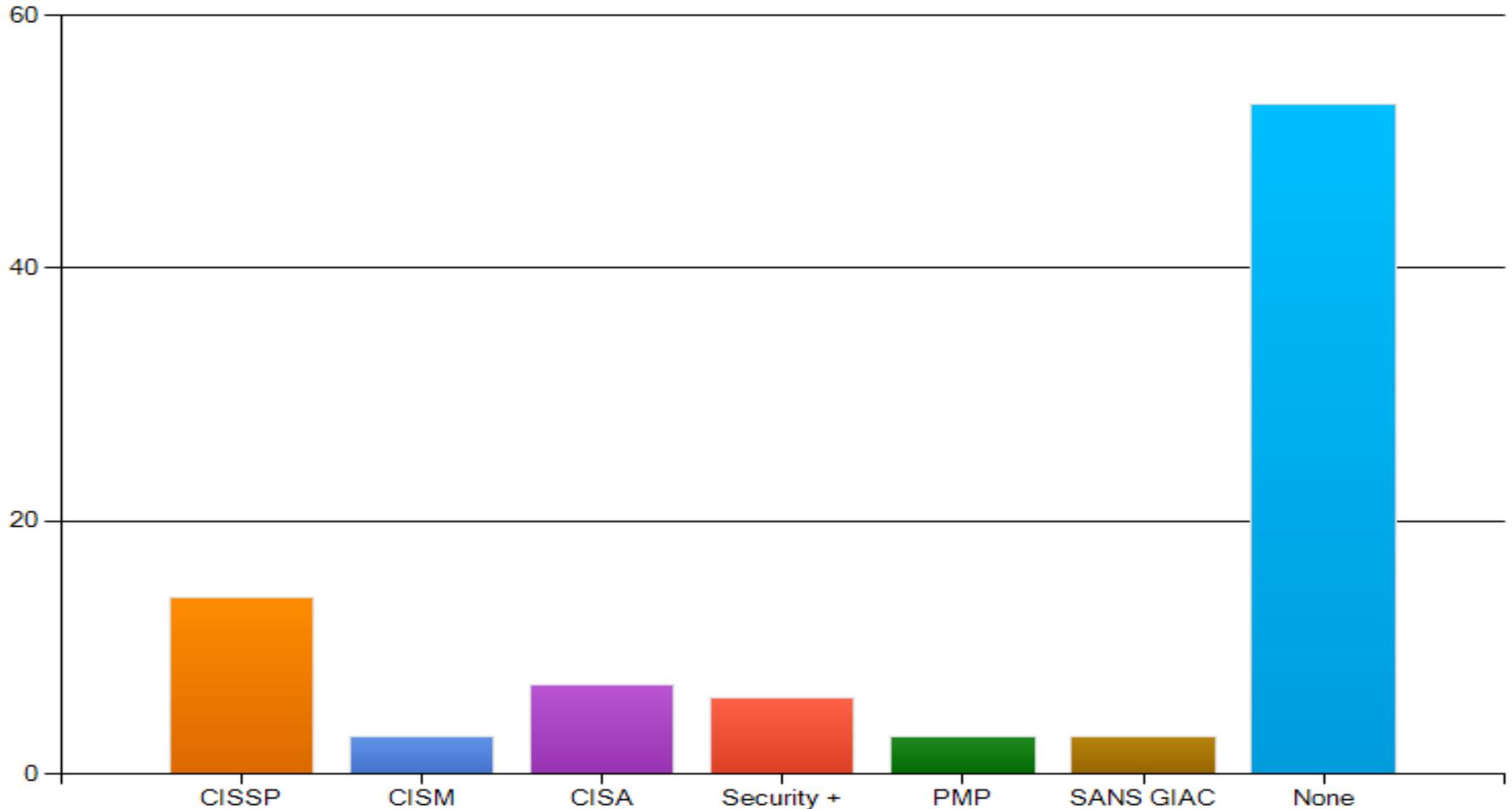
## Sensitive IT Systems Audited in the last 3 years



- 2011 Review of IT systems found agency reviews not keeping pace with increased use of IT



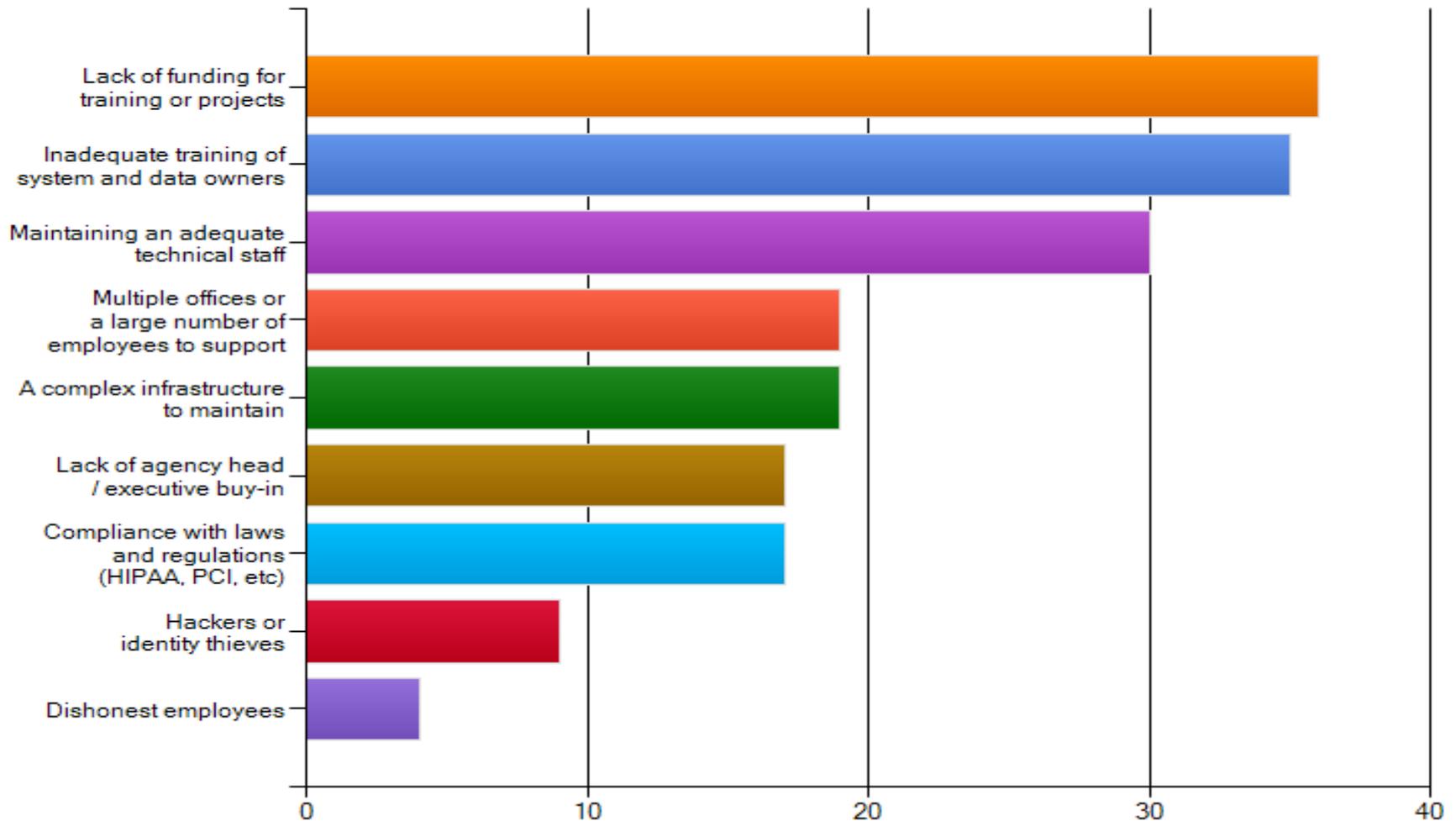
What professional certifications do you currently hold and maintain (including vendor specific, e.g. Cisco, Redhat, Microsoft, etc.)?



Source: Survey of security representatives from Commonwealth agencies



## 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



## Future Governance of IT Security

- Future Governance Considerations
  - Federal regulations & third-party mandates require new security efforts for agencies
  - Agency constraints impede security gap correction & limit auditing to find unknown gaps
    - EX: Annual security reviews, JAVA, Win 7
  - Implementing a Commonwealth wide IT risk management program
  - CIO has limited authority to ensure compliance



## Future Operational IT Security

- Upgrade of end point and network security infrastructure
- Added capability to record and analyze a week or more worth of network traffic
- Mobile device security strategy



# Questions?

