



## Cyber Security Program

Nomination Category: Risk Management  
Initiatives

State of West Virginia Office of Technology

## **B. Executive Summary**

With Governor Joe Manchin taking office, it was recognized that the State lacked uniformity across the state's technology landscape, including lack of strong leadership and focus on the issue of information system and data security in the context of growing prevalence and seriousness of cyber threats. Pockets of best practices existed within departments that could provide funding for this concern, but the state's network was shared by all agencies, some of which had a serious lack of resources and expertise to properly protect their systems from intrusions. The need for across-the-board improvement in this area was recognized.

The overarching goal was, and is, to reduce risk in the technology environment across the Executive Branch, and bring a consistent focus and best practices to bear on the challenge of data security, within all state departments.

An Information Security Strategic Plan was developed and, over time, resources and tools have been acquired and committed to the Information and Cyber Security challenge of overall risk-reduction through strong controls and heightened awareness.

Information and Cyber Security is not the end-result of a one-time project, event, or initiative. Rather, it is a year in, year out, process that involves layers of defenses. The technical layers include tactical operational controls such as firewalls, anti-virus, SPAM filters, WEB monitoring and blocking, access and authorization controls, encryption, vulnerability management, and the like. The strategic governance and administrative layers include policies, audit, confidentiality agreements, awareness training, enforcement, etc. Development of this program started in 2008 with the basic framework implemented in May 2009. The program continues to evolve.

### **C. Description:**

**Problem:** Before 2005, there was limited leadership and cohesiveness in the information and cyber security posture across the Executive Branch. There were small pockets of expertise available within organizations, but there was not a security standard throughout the entire Executive Branch. Because of the lack of a general standard throughout the Executive Branch, an uneven risk environment was created. Within the uneven risk environment were unmanaged, or inadequately managed, networks and systems.

**Solution:** In 2005, Governor Joe Manchin, and CTO Kyle Schafer, recognized that stronger leadership and controls were needed to reduce risk associated with State information systems and data. Further, the governor recognized a need to create a strong link between the state's Privacy Initiatives and the Information and Cyber Security Initiatives that were envisioned. To implement improvements across the Executive Branch several actions were taken earlier in the Manchin administration:

- A Chief Information Security Officer (CISO) was hired
- Enabling legislation was passed giving the CISO information security accountability across the Executive Branch
- The Governor Issued Executive Order 6-06 requiring mandatory security training for all Executive Branch employees

The legislation and Executive Order combined to define and require the development of Executive-wide policy, training, audit for compliance, and mitigation of vulnerabilities. In addition, Executive Order 6-06 called for the formation of an Executive Branch Information Security Team and a Privacy Management Team. The Governor's Executive Information Security Team (GEIST) was subsequently established, enlisting high-level Departmental operatives to extend the reach of the Office of Information Security and Controls.

The following critical initiatives have been realized since 2005:

- 1) Enterprise-wide policies and procedures have been developed
- 2) Executive Branch wide online cyber security awareness training has been deployed (content provided by Multi State – Information Sharing and Analysis Center (MS-ISAC) and funded by the US Department of Homeland Security)
  - a. **West Virginia was the first state to deploy this cost-effective, ISO-17799-based training**
- 3) Technical and Administrative Team Managers were hired
- 4) Information Security Job Classification series written and adopted by Personnel Board
- 5) Governor's Executive Information Security Team (GEIST) organized and chartered
- 6) Executive-level awareness training was provided to the Governor's Cabinet
- 7) Annual Reports to the Governor and Cabinet have been submitted

- 8) Annual Awareness Events have been conducted in October (Information/Cyber Security Awareness Month), since 2008
  - a. **West Virginia was the first state to offer their event to a worldwide audience using a real-time WEB broadcasting service**
    - i. Invitations to all State employees, NASCIO, InfraGard, MS-ISAC, public schools in WV, colleges and universities in WV, county and local governments, public (through newspaper pre-publicity articles)
    - ii. The theme of the event was to help participants understand that each person has a responsibility in the safeguarding of State systems and data, and their role can be thought of as that of a “Human Firewall”
- 9) Data Classification has been undertaken for the first time ever
- 10) A Data Transfer study identified and stopped sensitive data that was being transported outside the Enterprise in clear-text format
- 11) Office of Information Security and Controls (OISC) established
  - a. Security Operations Center (SOC) organized
    - i. Online Incident reporting and Workflow System
      - 1. Intrusion Detection
      - 2. Event monitoring and correlation
      - 3. Log Analysis
    - ii. WEB filtering across Executive Branch
    - iii. Vulnerability Management process put in place
    - iv. Forensics Laboratory developed
    - v. Hard Drive Encryption Standard established and over 10,000 licenses purchased
    - vi. E-mail Encryption and Data Leakage Solution acquired and implemented
    - vii. Incident Triage and Management Process/Procedure developed
    - viii. Investigations Initiation Process
    - ix. E-Discovery/Litigation Hold Process
    - x. Partnerships with Fusion Center, MS-ISAC, etc.
      - 1. Cold cases solved using skills and tools in SOC
      - 2. WV-ISAC established
    - xi. Distribution of Security Alerts and Bulletins Daily
    - xii. The SOC management mandates that every employee receives a certification every year from GIAC (Global Information Assurance Certification). This certification is based upon ISO-17799.
  - b. Audit Function launched
    - 1. SAS 70 engagement – Ernst and Young

- a. Office of Technology will have a base audit that can satisfy requirements of multiple audits conducted throughout the year, saving significant time for repeated audits on same control set.
  - 2. Rolling Audit program established
  - 3. Audit oversight and assistance provided
- c. Awareness Training deployed, promoted, and tracked
  - i. Drove acquisition of OT Learning Management System
    - 1. Deployed to 18,000 employees
    - 2. Completion logged.
    - 3. Reports to Departments on completion progress
- d. Policy
  - i. Numerous Executive-wide policies developed
- e. Security Tips published to WEB site
- f. WEB Site for Information Security organized and recently enhanced

## 12) Governance

- a. Strategic Information Security Plan Developed
- b. Annual report to the Governor and Cabinet
- c. Collaboration with State Privacy Office
- d. Participation on NASCIO Security and Privacy Committee
- e. Participation on MS-ISAC Training and Awareness, Outreach and Operations Committees
- f. Membership in West Virginia Chapter of InfraGard
- g. Three OICS team members graduates of FBI Citizen's Academy
- h. Policy
- i. Annual Awareness (October) Event
  - i. National and Internationally known speakers
  - ii. State and Federal Officials
  - iii. Internationally Broadcast using real-time WEB system
  - iv. Video Taped and available on-demand on WEB Site
- j. Ad Hoc Alerts and Security Reminders to Executive Branch employees

#### **D. Significance of the Project:**

The significance of the development of an Executive Branch-wide Information and Cyber Security Program is the substantial reduction of risk to State information systems and data through the application of standards-based policies and controls, the increased use of best practices, greater visibility into the network with automated identification of anomalous events, and raised awareness on the part of most State employees.

The Office of Technology has delivered security best-practices and protocols to the Executive Branch as a whole through online training, security events, and periodic alert broadcasts to the Enterprise employee community to heighten awareness about a currently prevalent threat, such as a Phishing e-mail that is passing through the SPAM filter into the e-mail environment. Daily e-mails are now sent out about security news events, which alert 20,000 + people at a time.

The OISC operates, and provides the variety and level of services that it does, on approximately 3% of the Office of Technology (IT infrastructure) budget, and approximately .5% of the annual IT spend in the State of West Virginia.

The provision of an umbrella Information Security Program across the Executive Branch of West Virginia State government has significantly leveled the playing field in terms of access by agencies and employees to information security skills. Our staff assists with identifying the sources of inappropriate e-mails, recovering evidence that has been deleted and investigating employee activities at the request of Director-level requestors.

Cost avoidance is an important goal of an Information Security organization, but it is difficult to measure the dollars saved if.... The breach does not happen when the lost or stolen laptop had an encrypted hard drive and presents no risk to the agency who was storing sensitive data on that hard drive. The Phishing email does not lure an educated community of employees to a criminal's site to harvest credentials, or other information that can be used to steal an identity, exploit the victim, and do genuine harm. The WEB site is blocked that would have otherwise launched the download of a key-logger, Trojan, worm, or other malware. The virus outbreak is avoided that would have cost hundreds of dollars to flatten and rebuild scores of infected machines. The strong password is not easily guessed, cracked, or forgotten. The password is not written down and kept near the PC. The password is not shared. The workstation is not left logged-on, unattended.

Many of the dollars saved as a result of a vital Information Security practice are intangible, but in the Benefits section on the following page, some tangible dollar savings are identified.

There is not 100% solution in the Information Security solution set. No "Silver Bullet" has yet been offered by a vendor. There is, however, an undeniable reduction of risk that is inherent in a community of security-aware employees.

## **E. Benefit of the Project:**

There has been a steady increase in end-user questions, reported concerns, and identification of incidents by employees, all of which demonstrate increased awareness of the employee's role and responsibility for system and data security, and resulting diligence. This increase of reported incidents has arguably led to a reduction of risk. Data Classification allows the State for the first time to apply controls to data based upon its level of criticality, and its level of sensitivity. Identification of system and data owners increases accountability and promotes the proper management of the data, and reduction of risk. Audits serve to identify areas where there are deficiencies in policy compliance and application of controls, and the reports from audits serve to raise awareness about the security posture in the audited area. Mitigation actions reduce risk. The SAS 70 audit engagement provides a baseline audit to facilitate many of the technology component of audits that are conducted throughout the year, and is intended to save cost in two ways: Reduce the resources (personnel time/cost) required to respond to the multiple audits that are conducted annually, and reduce the overall spend on audits, since the OT audit component should not need to be repeated by individual auditors, requiring them to reduce their bid cost to remain competitive as they compete for audit projects.

In addition to the GEIST, which provides a direct channel of communications between the Information Security Office and the Departmental leadership, the WVOT has developed the West Virginia Information Sharing Analysis Center (WV-ISAC), which is geared strictly toward West Virginia giving awareness to city and local governments. On October 19, 2009, the WVOT held a cyber security public awareness seminar themed: "Becoming a Human Firewall." This event was open to government officials, the general public, and members of the online community across the world, including NASCIO members, MS-ISAC members, InfraGard members, public schools and higher education. While there was considerable effort to make this a quality event focused on October as Information/Cyber Security Awareness Month, and to broadcast it real-time to a (world)wide audience (10,000 potential endpoints), the Information Security and Awareness effort is ongoing throughout the year, to increase vigilance, and reduce risk throughout the enterprise.

Tangible Cost Savings: In addition to these many intangible, risk-reduction benefits, West Virginia has saved around \$130,000 by leveraging open source technology instead of commercial technology in the intrusion detection area, and focusing training on Linux-based systems. West Virginia has saved a projected \$48,000 – the cost of a commercial awareness training product – by utilizing the MS-ISAC developed online training courseware.

By in-sourcing our security monitoring, we have reduced the cost of monitoring a single "point of interest" from \$17,000 per point, to \$1667 per point, and increased our monitoring from a single POI to approximately 30 POIs, a hugely cost-effective result.