



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

May 20, 2009

May



MEMORIAL DAY



ARMED FORCES DAY



ISOAG May 2009 Agenda

- | | | |
|------|---|--|
| I. | Welcome and Opening Remarks | Peggy Ward, VITA |
| II. | A Fresh Look at Data Classification | Shirley Payne, UVA &
Darlene Quackenbush, JMU |
| III. | Personal Identity Scanning Tools & Practice | Randy Marchany &
Brad Tilley, Virginia Tech |
| IV. | Server Admin./Privileged Access Process | Don Kendrick, VITA &
Eric Taylor, NG |
| V. | 2009 COV Security Policy & Standard | John Green, VITA |
| VI. | Commonwealth Information Security Council | John Willinger, DMHMRSAS |
| VII. | Upcoming Events | Peggy Ward, VITA |

A FRESH LOOK AT DATA CLASSIFICATION

SHIRLEY PAYNE, UVA

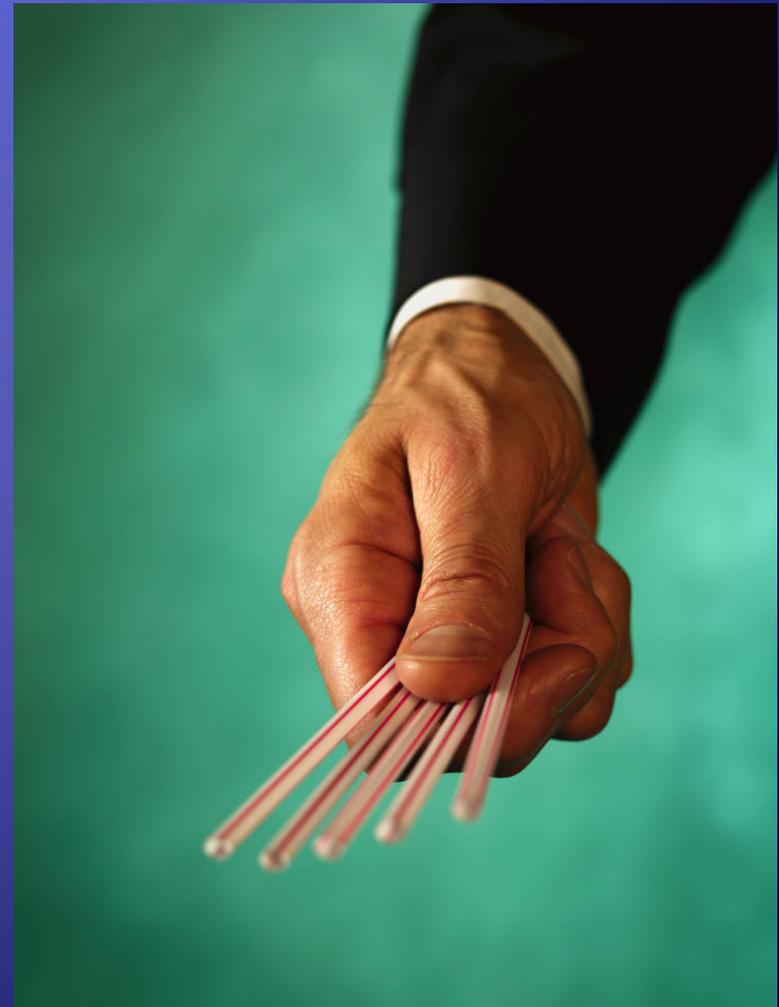
DARLENE QUACKENBUSH, JMU

Agenda

- ◆ Data classification then and now
- ◆ New strategies replacing old ones
- ◆ Current challenges
- ◆ Case histories/futures

Classification –1990s and earlier

- ◆ Data mostly housed centrally
- ◆ Classification choices determined primarily by *business needs* (e.g. staff productivity and cost) and *organizational culture*
- ◆ Data owners (aka stewards) called the shots



Change Happened...

1990s &
earlier

Today

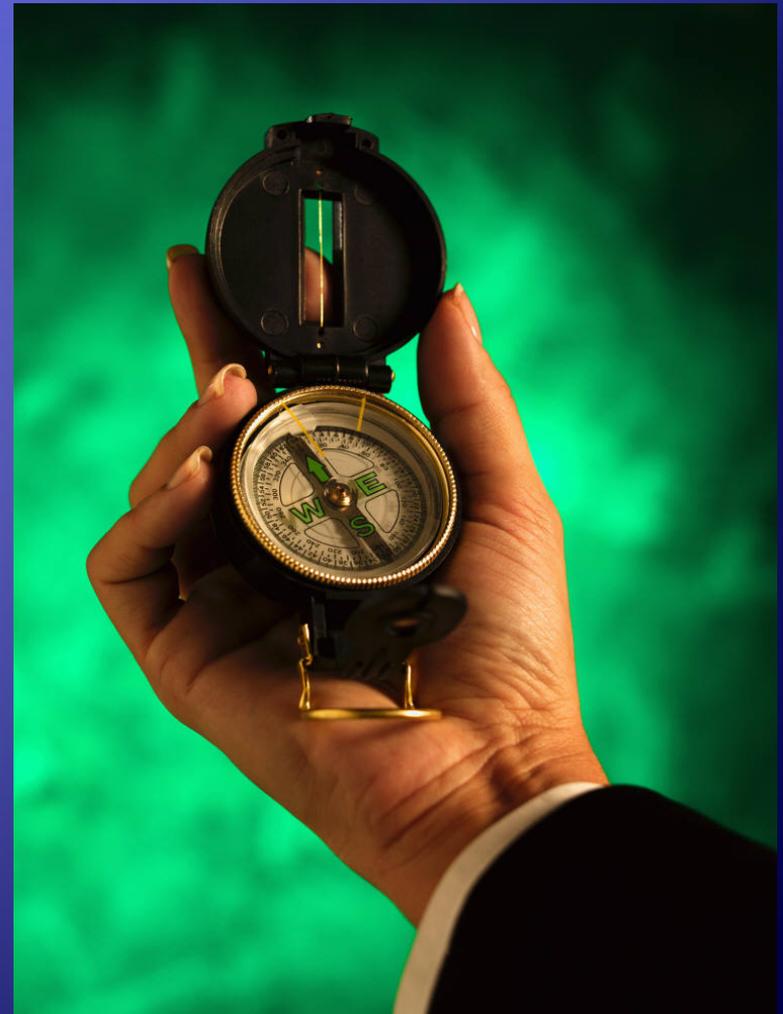


Change Happened...



Classification – Today

- ◆ Data more dispersed
- ◆ Classification choices mostly dictated by external forces
- ◆ Data protection requirements often trump other decision factors



The Search for New Strategies . . .

Replacing Old Strategies

Strategic Focus

- ◆ Value proposition
- ◆ Support new business models
- ◆ Decisions not just documentation & distribution
- ◆ Risk management

Replacing Old Strategies

Strategic Focus

Meaningful

- ◆ Translates easily
- ◆ Leverages regulation (PII, HIPAA, GLBA, FERPA, etc.)
- ◆ Risk based

Replacing Old Strategies

Strategic Focus

Meaningful

Least Privilege

- ◆ Minimum necessary access
- ◆ Role / job function
- ◆ Deliberate control

Replacing Old Strategies

Strategic Focus

Targeted

Least Privilege

Organic

- ◆ Constantly changing sources and uses
- ◆ Adapts to transformation
- ◆ Mobility

Replacing Old Strategies

Strategic Focus

Targeted

Least Privilege

Organic

Comprehensive protection

- ◆ Standards
- ◆ Across environments
- ◆ Technical & policy

New Strategies

- ◆ Strategic
- ◆ Meaningful
- ◆ Least Privilege Access
- ◆ Organic
- ◆ Comprehensive protection

Challenges to Implementation

- ◆ Analysis -- know where the real issues are
- ◆ Link data management and information security
- ◆ Reduce exposure / maintain flexibility
- ◆ Apply security by data type
- ◆ Awareness → Education → Understanding
- ◆ Enforcement
- ◆ On-going Commitment

Case Histories/Futures

- ◆ JMU
- ◆ UVA

JMU Environment

- ◆ Approx. 18,500 Students; 2,500 faculty/staff
- ◆ Centralized IT management
- ◆ ERP in late 1990's
- ◆ Becoming more distributed internally
- ◆ Increasing research and partnerships interests

Analyze ... Understand

- ◆ Senior Advocate
- ◆ Sensitive Data Workgroup
- ◆ Data Verification initiative
 - ◆ Who's collecting what? (SSNs, CCs, & PII)
 - ◆ Who's storing what?
 - ◆ Who's sharing what?
 - ◆ Reasonable justification/approvals
 - ◆ Appropriate care
- ◆ Project Initiation Questionnaire (PIQ)

Reduce Exposure

- ◆ Evaluate business processes
- ◆ Limit collection
- ◆ Delete unnecessary data
- ◆ Control access
- ◆ Apply safeguards

New Policy

- ◆ Appropriate Assignment of Responsibilities
- ◆ Reasonable Collection and Distribution of Data
- ◆ Appropriate Use
- ◆ Emphasize Protection Standards

Data Classification

- ◆ Revise classifications
 - ◆ Public
 - ◆ Internal General
 - ◆ Internal Restricted
- ◆ Clearly Defined w/
Actionable Controls
- ◆ Based on Risk/Impact

Highly Confidential

Protected

Public

Data Standards

- ◆ STARTSAFE/RUNSAFE protections
- ◆ Additional protections for highly confidential
 - ◆ Specialized approval
 - ◆ Encryption
 - ◆ Looking toward two-factor

Education → Understanding

- ◆ Risks, impacts, restrictions
- ◆ Classifications
- ◆ Policy messages
- ◆ Day-to-day decisions
 - ◆ Product selection/ business process
 - ◆ Access
 - ◆ Security protections

Enforcement

- ◆ Security role/access reviews
- ◆ Security controls as part of DTM
- ◆ Risk reviews
 - ◆ Project , ARMICS, departmental self-studies, etc.
- ◆ Scans
- ◆ Audit

Commitment

- ◆ The never ending story . . .
 - ◆ Evaluate for new concerns
 - ◆ Develop new strategies
 - ◆ Repeat

- ◆ On-going partnership
 - ◆ Data management and information security
 - ◆ Internal and external

Case Histories/Futures

- ◆ JMU
- ◆ UVA

UVA's Data Environment

- ◆ Three agencies:
 - ◆ Academic
 - ◆ Medical Center
 - ◆ UVA at Wise
- ◆ Both shared and separate ERPs
- ◆ Within Academic Division, many departmentally-managed applications, databases, servers, and individual-use computing devices
- ◆ \$340 million in research funding (and the databases to prove it!)

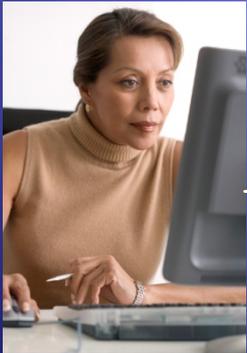
Strategies Underway

- ◆ Data Minimization Initiative
 - ◆ Minimizing collection and use of SSNs, credit card numbers, HIPAA data, etc.

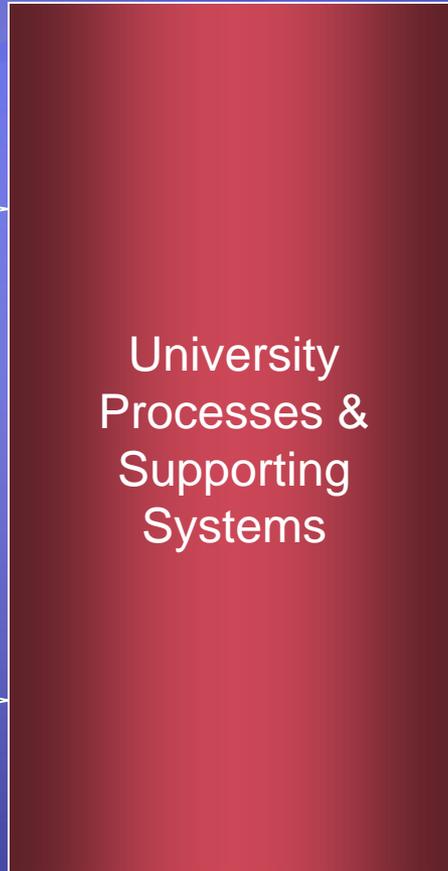
Data Minimization Initiative



Confidential data requested only when essential



Confidential data access authorized to least # of people



Confidential data provided only when essential



Confidential data stored only in highly secured devices and file cabinets

- Clear confidential data use policy exists
- Responsibilities for data protection well communicated
- Compliance verification processes in place

Strategies Underway

- ◆ Data Minimization Initiative
 - ◆ Minimizing collection and use of SSNs, credit card numbers, HIPAA data, etc.
 - ◆ Implemented new SSN Protection and Use Policy and Electronic Storage of Highly Sensitive Data Policy
 - ◆ Scanning individual and shared storage records using Identity Finder™
 - ◆ Intensified institutional data protection education program
 - ◆ Revamping data classification and stewardship policies
 - ◆ Established stricter, mandatory standards for protection of data in each classification

Redefined Data Classifications

Highly
Sensitive

Examples:

- Data that enables identity theft
- HIPAA-protected data

Moderately
Sensitive

Everything
In between

Not
Sensitive

Examples:

- University financial statements
- University statistics, e.g. employees by gender

Data Protection Standards

Responsibility

- VPs and Deans
- Department Managers & Chairs
- Faculty, staff, student workers, contractors

Transmission

- Email and other messaging services
- Fax
- FTP, HTTP, and other transmission protocols

Storage & Destruction

- General purpose storage and workspaces
- Physical media production and storage
- Destruction of electronic and physical media

Data Protection Standards

Shared Devices

- Basic security configuration
- Access permissions
- Recovery and physical security
- Other requirements depending upon server function

Individual-Use Devices

- Basic security configuration
- Server connections
- Other requirements

Assurance

- Assessments with automated tools, e.g. web application code vulnerability scanning
- Risk management
- Auditing

Questions



Personal Identity Scanning Tools and Practices

Randy Marchany & Brad Tilley
Virginia Tech

Introductions

- **Brad Tilley – Author of Find_SSNs, IT Security Analyst**
- **Randy Marchany – Director IT Security Lab**

Background

- **SB1386 – California**
- **40-something (46?) states have similar laws**
- **NYS data breach notification law**
- **Virginia data breach notification law**
- ***Code of Virginia* [2.2-3820](#)**

A. The General Assembly finds that the Commonwealth, as steward of sensitive personal information, has an obligation to notify in a timely manner any individual whose personal information has been compromised and where harm to that individual could reasonably be expected as a consequence.

Personally Identifiable Information

- **NIST defines it as:** "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."
- **PII data types vary from state to state**
 - Almost always means Social Security Numbers
 - Credit card numbers
 - Driver's license numbers
- ***In general, information useful to perpetrate identity theft***

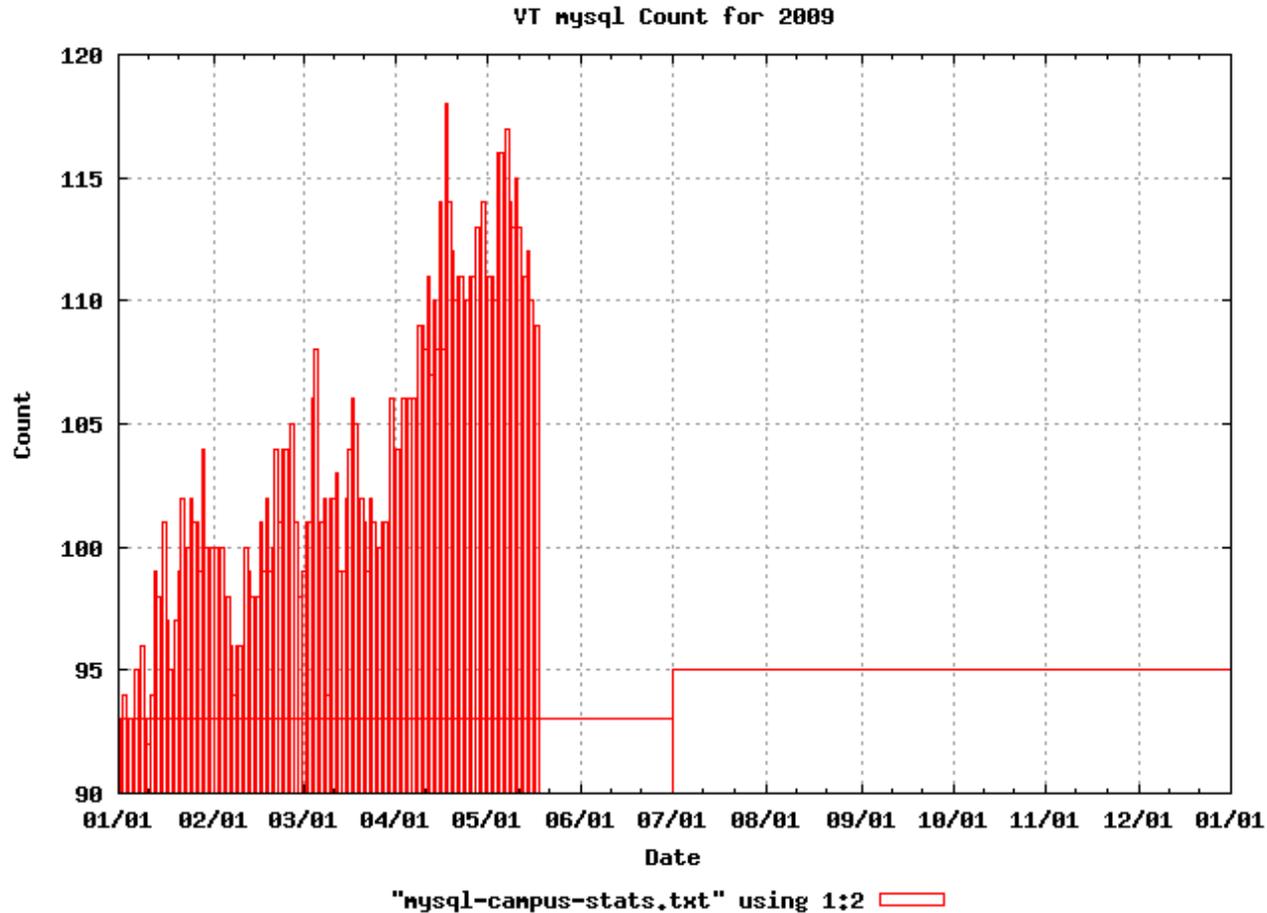
VA Tech's Response

- www.policies.vt.edu
 - Policy 1060 – Policy on SSN
 - Policy 7025 – Safeguarding Nonpublic Customer Information
 - Policy 7105 Policy for Protecting University Information in Digital Form
- **Sensitive Data Standards**
 - Standard for Protecting Sensitive University Information Used in Digital Form
 - Standard for Storing and Transmitting Personally Identifying Information
 - Security Standards for Social Security Numbers
 - <http://security.vt.edu/sensitiveinfo.html>

VA Tech's Response

- **If it's sensitive data, it must be encrypted at rest and in transit**
- **Vendors must comply with this standard or VT has a compensating control**
- **We have to FIND the sensitive data before we can PROTECT it.**

Identifying Sensitive Data on Campus

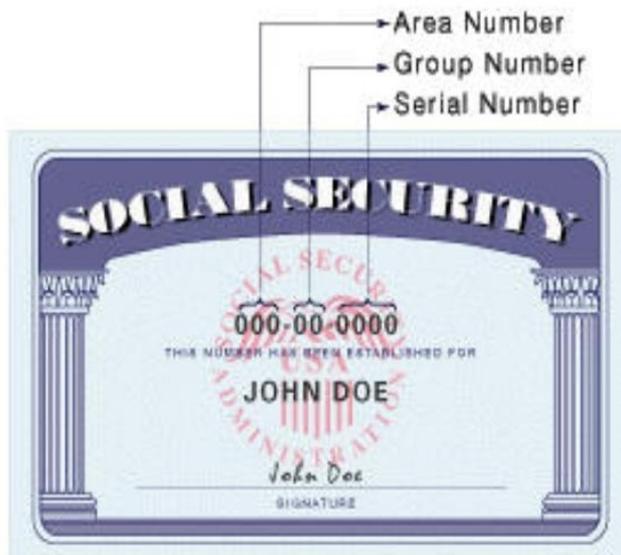


The Challenge: PII is Everywhere

- **SSN used as unique identifier for 20+ years.**
- **Fed/State/Local reporting requirements.**
- **66% of systems have some, 90% of systems have at least PII of owner.**

Data Formats

How To Recognize a Legitimate Social Security Number



- Area
 - Cannot be 000
 - Cannot be 666
 - Cannot be 734 - 749
 - Cannot be >772
- Group
 - Cannot be 00
- Serial
 - Cannot be 0000

Data Formats

How To Recognize a Potential American Express Credit Card Number



- Number must begin with 34 or 37.
- Number must be 15 digits long.
- Number may be contiguous or (four six five) segmented.
- 3700 000000 00000
- 3400000000000000

Data Formats

How To Recognize a Potential MasterCard Credit Card Number



- Number must begin with 51,52,53,54 or 55 (55 may also be a Diners Club US/Canada card).
- Number must be 16 digits long.
- Number may be contiguous or broken.
- 5400 0000 0000 0000
- 530000000000000000

Data Formats

How To Recognize a Potential Visa Credit Card Number



- Number must start with 4
- Number must be 16 digits long. Old Visa cards were 13 digits.
- Number may be contiguous or broken into four fours.
- 4000 0000 0000 0000
- 4000000000000000

Data Formats

How To Recognize a Potential Discover Card Number



- Number must begin with 6011 or 65.
- Number must be 16 digits long.
- Number may be contiguous or broken into four fours.
- 6011 0000 0000 0000
- 6500000000000000

Data Formats

➤ Online Number Validation Test

➤ https://black.cirt.vt.edu/valid_ssn

➤ Generate some test numbers.

➤ Process helps users understand why some numbers are valid while others are not.

Why You'll Never Find it All

- Architectures for which no scan tool exists
- Non-participants
- Weird Data formats
 - 20D949C7
 - !!""""""""
 - DD736673F5F5F2F2F2F2F2F2

Institutional Support

- **The Law, institutional liability, and all that**
- **Data classification policy**
- **Support from the top, or near the top**
- **IT Buy-in: it'll be their burden, they need to be on-board**

Do Your Homework

- **You've found sensitive data, now what?**
- **Encryption: what do you offer, how do you support it, issues of business continuity**
- **Data destruction**
- **Centralization**
- **Shadow Systems**
- **Vulnerability Assessments**

Sensitive Data Discovery Tools

Tool Considerations

- **Self-service or centralized**
- **Platform**
- **Detection depth and breadth**
- **Scan over the network, scan file servers, databases, Web sites, etc?**
- **Cost**

Find_SSNs

- **Virginia Tech Sensitive Number Finder**
- **Python, Cross-Platform, Runs Anywhere**
- **Find_SSNs was the first Sensitive Number Scanner - 2004**
- **BSD License**
- **http://security.vt.edu/Find_SSNs**

SENF

- **University of Texas Sensitive Number Finder**
- **Java, cross-platform; run anywhere**
- **Creative Commons License**
- **Primitive Number Validation**
- **<http://www.utexas.edu/its/products/senf/>**

Spider 2008

- **Cornell University PII search tool**
- **Windows-only, lesser capabilities in Mac/UNIX**
- **GNU Public License v2**
- **Very User Friendly**
- **<http://www.cit.cornell.edu/security/tools>**

IdentityFinder

- **Various capabilities at different levels**
- **Windows/Macintosh**
- **Commercial**
- **<http://www.identityfinder.com>**

Demos, Demos, Demos!

Before You Scan

- **This is an opportunity for housekeeping**
 - Put data on file servers or confine it to user profiles
 - Most people will part with files they know are old
 - Script or automate general cleanup tasks before scanning
 - Clear browser caches (turn off SSL page caching?)
 - Clear temp file locations
 - Empty recycle bin/trash
 - Compact mailboxes, clobber old mail and attachments

Results Analysis

The Guiding Principle: *Sensitive data follows people, not machines.*

Put another way, look in files created by people.

~The End ~



Server Administrative / Privileged Access Process

IT Infrastructure Partnership Team

Don Kendrick, Senior Manager of Security Operations, VITA
Eric Taylor, Information Security Architect, NG



NORTHROP GRUMMAN

Server admin rights pose a security and availability risk.

This poses the risk of ...

- Lost productivity due to downtime
- Lost productivity due to unauthorized changes to the operation system.
- Lost productivity and DR capabilities because of undocumented changed to the system or application environment.
- Malware being installed as admin user

Proper separation of duties will help ensure threats against security and availability are minimized.

Admin rights for non-ITP managed personnel

- This process establishes procedures to implement strong security controls and ensure that the ITP can meet all availability Service Level Agreements (SLA)
- The Infrastructure Technology Partnership (ITP) will manage server administration privileges in the transformed environment.
- As part of the ITP transformation, the ITP must restrict server and work station administrative rights and privileges.
- This process meets COV 501 standard *Logical Access Control* that requires administrative rights given to designated individuals.
- This will apply to both production and test environments

The Reference

Section 5.2.2 of Sec 501-01:

- 1. Grant IT system users' access to IT systems and data based on the principle of least privilege.
- 16. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.
- 17. Require that local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, be granted only to authorized IT staff.

Server rights and privileges management will comply to the below requirements:

- If an Agency requires server administrative rights, a detailed change control ticket describing server actions using administrative privileges must be submitted.
- The ITP will grant access during a pre-defined scheduled maintenance window or according to emergency change procedures
- “Least Privilege” administrative access to server maintenance or application installation activity will be provided
- All Administrators will have a second account with administrator privileges that they will use when performing tasks that require administrative privileges for application management
- ITP tracks and logs all user activity performed.

Managed Windows Environment

- All non-IPT managed personnel will be required to obtain a secondary administrative account from the VCCC.
- Temporary privileged access will be granted by to the secondary account to the local administrative group of the requested server.
- Temporary privileged access will expire after the specified maintenance window.

Full time administrative access can be obtained for Sandboxed Development environments only.

Managed UNIX environment

- All UNIX users requiring privileged accounts require unique ID's, and must logon to a UNIX system using that unique ID.
- In the event the user demonstrates a requirement for “root” access to perform job functionality, the system administrator may, with the appropriate approval, define a “sudo” capability for that user.
- The user may then logon to the system using his/her own ID and use “sudo” as a command prefix to run as a privileged user.
- **The user shall not “sudo” or switch user to the root account.**
 - Accountability is lost if the root account is used to perform daily job functions

Sudo Background

- Sudo operates on a per-command basis.
- When trusted users precede an administrative command with sudo, they are prompted for *their own* passwords.
- Once authenticated and assuming that the command is permitted, the administrative command is executed as if by the root user.
- The ability to restrict which commands a user may run on a per-host basis.
- Sudo does copious logging of each command, providing a clear audit trail of “who did what.” When used in tandem with syslogd, the system log daemon, sudo can log all commands to a central host (as well as on the local host).

Sudo Background

- Sudo uses timestamp files to implement a "ticketing" system. When a user invokes sudo and enters his/her password, he/she is granted a ticket for 5 minutes (this timeout is configurable at compile-time). Each subsequent sudo command updates the ticket for another 5 minutes.
- Helpful Sudo commands
 - *-u username* The **-u** (*user*) option causes **sudo** to run the specified command as a user other than *root*
 - *-l* The **-l** (*list*) option will list the allowed (and forbidden) commands for the invoking user on the current host

Sudo Caveats

- It is not meaningful to run the `cd` command directly via `sudo`, e.g.,

```
$ sudo cd /usr/local/protected
```

since when the command exits the parent process (your shell) will still be the same.
- Shell scripts will be required when using shell commands that require *root* access

Questions?



Policy, Standard and Guidelines

John Green

Deputy Chief Information Security Officer



Policy, Standard & Guidelines Update



1. Collect comments & questions from the IS community during the year
2. Create draft of policy, standard or guideline (PSG) addressing comments...
3. Distribute draft to IS Council for review, input & feedback
4. Collect comments from IS Council, usually giving them a week or so to review
5. Review & address Council comments in the PSG
6. Send draft of PSG to ITIES Directorate for review & comment
7. Aggregate comments from ITIES, usually takes a week or so
8. Comments from ITIES are reviewed with CSRM management & addressed as appropriate
9. Draft of PSG is sent to ITIES for posting to Online Review Comment Application (ORCA)...
10. Gather comments from IS community (ORCA) for at least 30 days
11. Review & address ORCA comments
12. Create responses to comments from ORCA reviewers & distribute through ITIES
13. Send finalized version of PSG to ITIES who sends it to the CIO for approval.
14. If the CIO approves it goes to the ITIB for consideration & approval. If a standard or guideline there is a 5 day comment period & if a policy it must be approved at an ITIB meeting
15. Once approved it is posted to the web





Policy and Standard Highlights

- Online review and comment period for Policy has closed.
 - 13 Comments: 5 Grammar, 2 Flowchart, 6 Clarity
- Online review and comment period for Standard is ongoing – closes June 12.
 - Wireless Security
 - Application Security
 - Encryption
 - Application Vulnerability Scanning
 - Roles and Responsibilities from Policy
 - Non-electronic Information Security Best Practices



Virginia Information Technologies Agency

Commonwealth Information Security Council

John Willinger
DMHMRSAS & COV IS Council





Identity & Access Management Committee

- Contact:

John.Willinger@co.dmhmrsas.virginia.gov





Upcoming Events





UPCOMING EVENTS! Future 2009 ISOAG's

All currently from 1:00 – 4:00 pm at CESC
though working with the Science Museum (thanks!)
(please let us know if you want to host in the Richmond area!)

Wednesday, June 17

Tuesday, July 14

Wednesday, August 12

Register Online at:

<http://www.vita.virginia.gov/registration/Session.cfm?MeetingID=3>



Upcoming Events – ISOAG June 17

Draft Agenda

Data Collection

**Lisa Wallmeyer – Va. Joint
Commission on Technology
and Science**

Friend or Foe: Tips for Evaluating Email

Bob Baskette, VITA

2009 COV Security Policy & Standard

John Green, VITA

COV 2009 Data Points

Peggy Ward, VITA



FACTA Red Flag Requirements *NEW DATE

Implementation Date: **August 1st, 2009**

Are you aware of the red flag requirements in the Fair and Accurate Credit Transactions Act (FACTA) of 2003?

Please read carefully as it is not only banks and financial institutions!

<http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>



SANS Management Training

Management 414: SANS(R) + S(TM) Training Program for the CISSP(R) Certification Exam

Where: University of Virginia, Charlottesville

When: June 2, 2009

Sans Mentor Marty Peterman will be leading the class.

Complete course details can be found at:
<http://www.sans.org/info/442198>



UPCOMING EVENTS: MS-ISAC Webcast

National Webcast!

Wednesday, June 17, 2009, 2:00 to 3:00 p.m.

Topic: Securing Mobile Devices

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



UPCOMING EVENTS! CIO-CAO Mtg.

CIO-CAO Communications Meeting:

Tuesday, June 23

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: Department of Health Professions
Perimeter Center, 9960 Mayland Drive
2nd floor conference center



Any Other Business ???????





ADJOURN

THANK YOU FOR ATTENDING!!

