



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

October 14, 2010



ISOAG October 2010 Agenda

- | | | |
|------|------------------------------------|------------------------|
| I. | Welcome & Opening Remarks | John Green, VITA |
| II. | Doing "The Cloud" Right | Bob Ballard, Microsoft |
| III. | Security & Compliance in the Cloud | Ahmer Sabri, Microsoft |
| IV. | Discovering Your Own | Eric Taylor, NG |
| V. | 2010 COV Security Annual Report | John Green, VITA |
| VI. | Upcoming Events & Other Business | John Green, VITA |
| VII. | Partnership Update | Craig Drain, NG |

The background of the slide is a stylized, semi-transparent American flag. The stars are visible in the upper left, and the stripes flow across the bottom and right. The overall color palette is dark, with the flag's colors appearing as lighter, muted tones against the black background.

Doing “the Cloud” Right

Charting a Course for State and Local Governments

Bob Ballard
Government IT Strategy Advisor

“Cloud Computing”

There is a lot of hype...and the word itself is not helpful...



...because the cloud is not a destination...

...it is a powerful (potential) tool in your toolbox to solve business problems.

Sometimes...



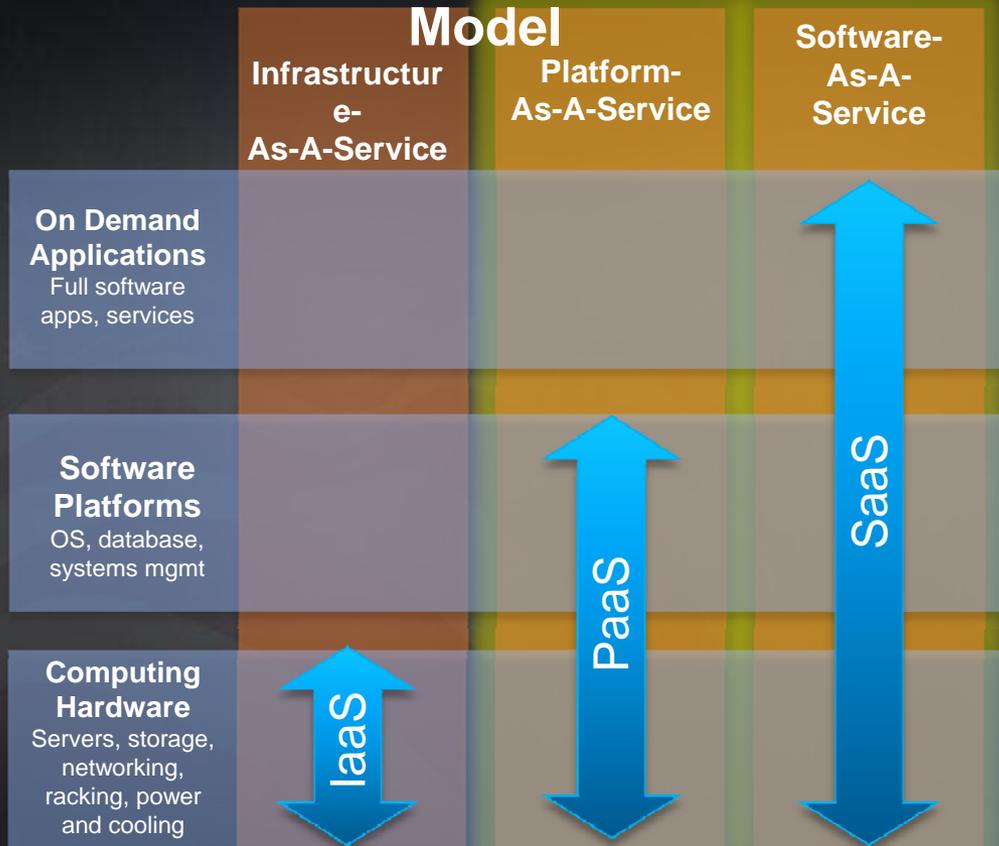
...I don't want to own the
TV station....



...I just wanna watch TV.

Which Cloud Model For What ?

Choose A Service Delivery



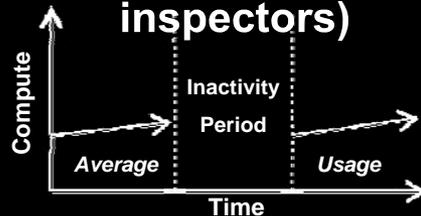
Choose A Provider Model



Highlighted models will be main focus for today.

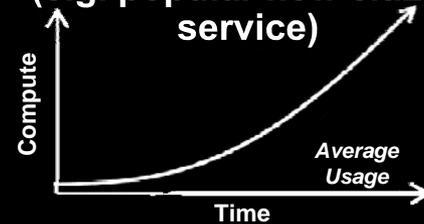
Workload Patterns Optimal for Cloud

“On and Off“ (e.g. pool inspectors)



- On and off workloads (e.g. batch job)
- Over provisioned capacity is wasted
- Time to market can be cumbersome

“Growing Fast“ (e.g. popular new citizen service)



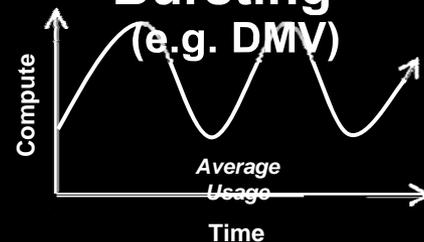
- Successful services need to grow/scale
- Keeping up w/growth is big IT challenge
- Complex lead time for deployment

“Unpredictable Bursting“ (e.g. disaster response)



- Unexpected/unplanned peak in demand
- Sudden spike impacts performance
- Can't over provision for extreme cases

“Predictable Bursting“ (e.g. DMV)



- Services with micro seasonality trends
- Peaks due to periodic increased demand
- IT complexity and wasted capacity

Why Cloud Computing ?

flexibility

transparency

cost

efficiency

collaboration

carbon footprint

remote access

focus

agility

disaster

recovery

Cloud Business Models Matter

One Example - Mail

MICROSOFT®
Exchange Server

Designed for



Established in
1996
Used by most
Fortune 500,
State and Local,
Federal
agencies



 Windows Live™
Hotmail.

Designed for



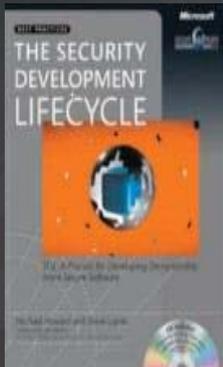
Established in
1996
Used by
450M
consumers

The decision was not difficult.
Enterprise foundation for an enterprise cloud offering.

Not All Code in the Cloud Is Created Equal

SECURITY

"Microsoft becomes high priest of secure software development." – [CNET](#)



"Many of the world's most knowledgeable security experts are urging their favorite software vendors to follow in the footsteps of Microsoft." -

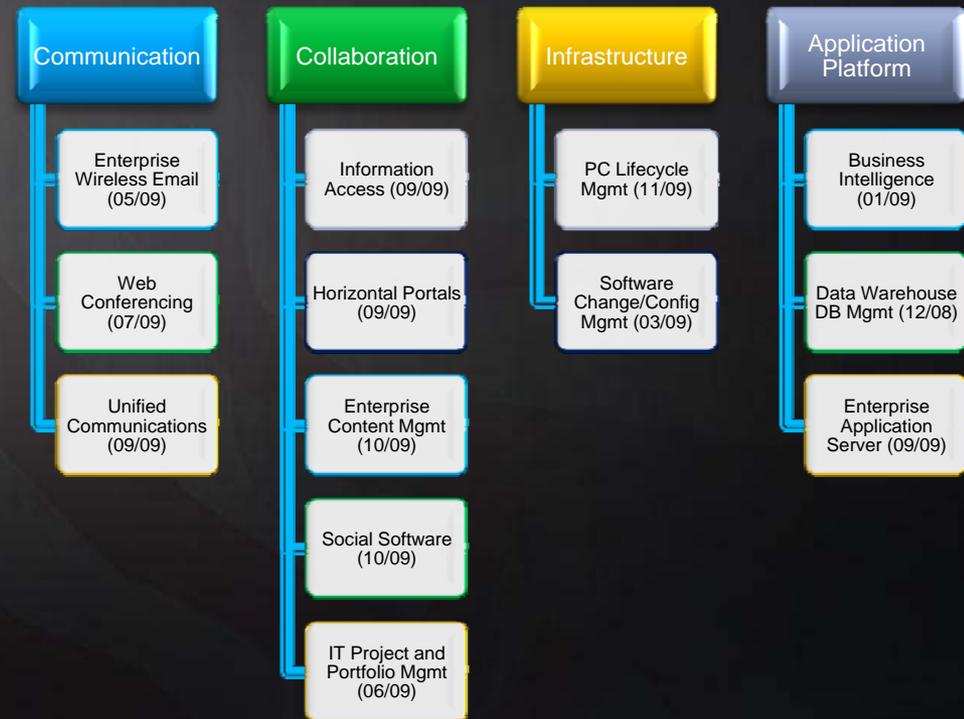
[Infoworld](#)

"As an industry we should recognize the sea change in Microsoft's approach to security, and encourage other vendors to follow Microsoft's lead." -- [SANS](#)

[NewsBites](#)

MATURITY / INNOVATION

(Relevant Gartner LQs in 2009/2010)

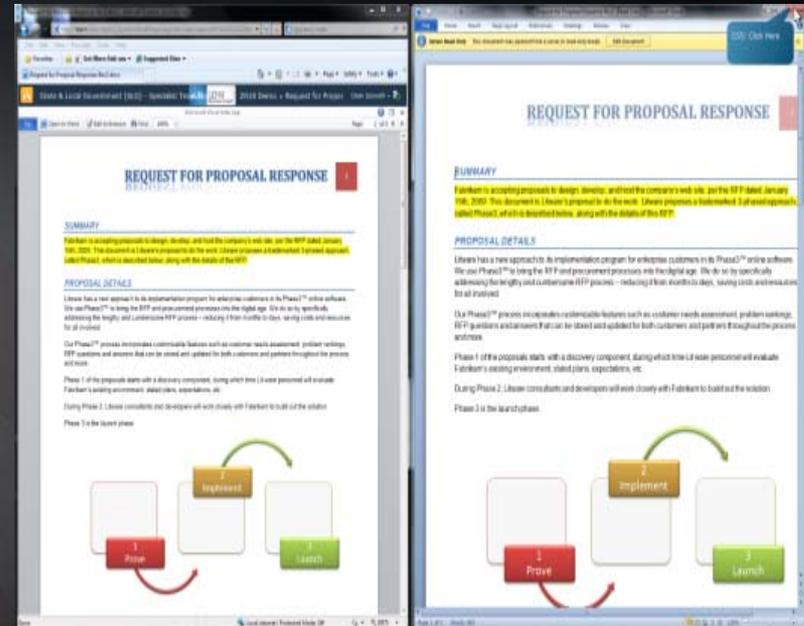


Compliance / Governance

Section 7.143. Form and Method of Transmission.

- (a) An authorized filer should visually inspect each instrument prior to transmitting to ensure compliance with existing statutory recording requirements.
- (b) Electronic submissions shall carry sufficient information to identify the authorized filer and to uniquely identify the instrument to be recorded.
- (c) Instruments transmitted electronically shall:
- (1) provide fidelity to the original appearance of any instrument at the time such instrument was first created, whether by electronic or other means;
 - (2) retain the original content; and
 - (3) provide for a non-proprietary digital file format.

Sample state records management statute

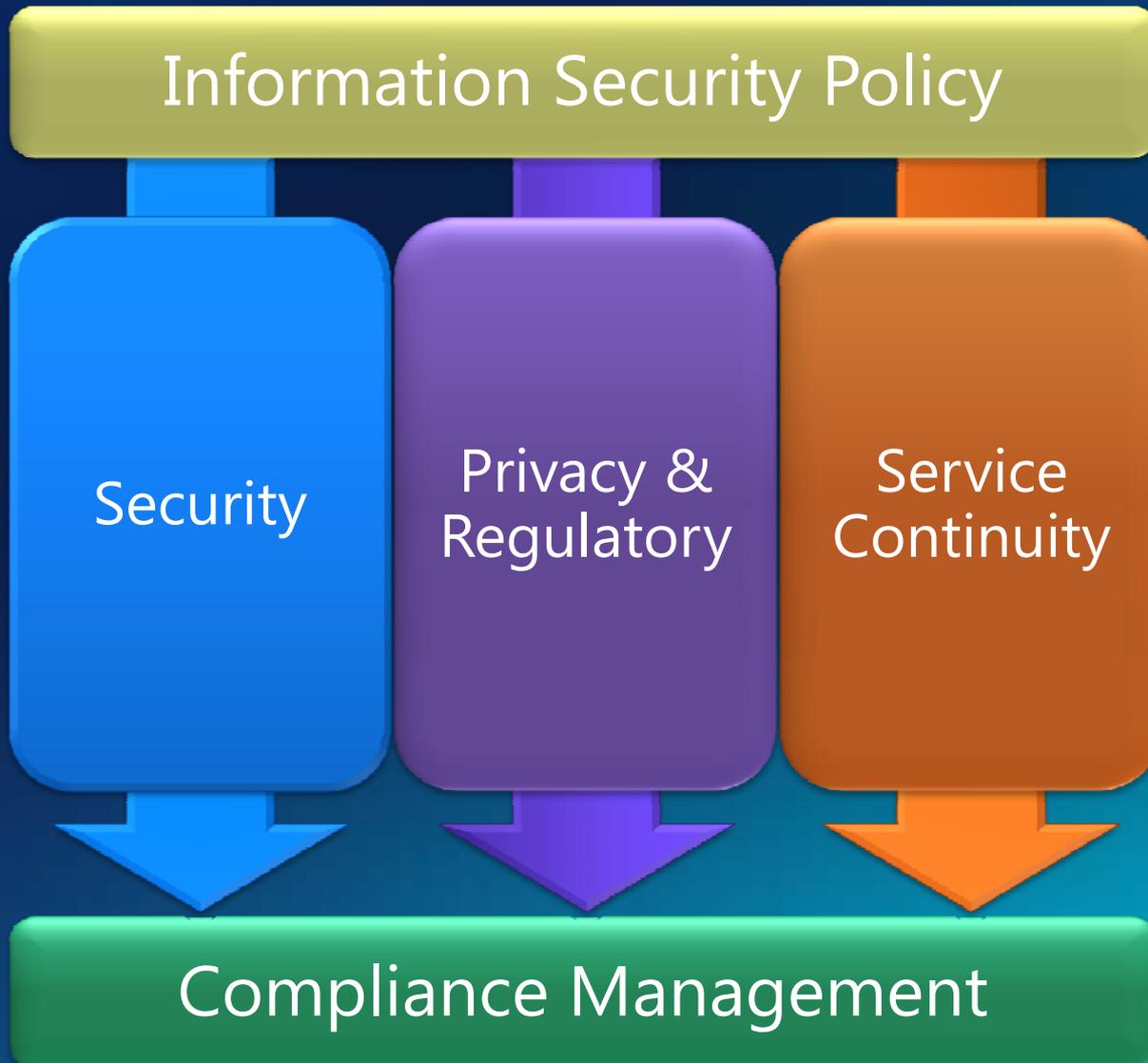


Document fidelity in Word and Word web app

Security and Compliance in the Cloud

Ahmer Sabri
Microsoft Corporation

Key Areas to Discuss with Vendor



Policy

What Certification and Regulations Does the Vendor Follow?

ISO 27001 / 27002

SAS 70 Type I and II

EU Safe Harbor or Model Clauses

Security Policy

- Cloud vendors run systems for multiple customers; thus hard to follow a particular customer's security policy
- So how to address?
 - Is the vendor's policy available?
 - Is policy mapped to standards like ISO 27001?
 - How does policy compare to customer's?
 - For the "gaps"
 - Does vendor accomplish in different way?
 - Is the requirement critical?

Security

Does Vendor Have Multi-Layered Defense?

Strategy: employ a risk-based, multi-dimensional approach to safeguarding services and data

Security Management

Data

Threat & Vulnerability Management, Monitoring & Response

User

Access Control & Monitoring, File/Data Integrity

Application

Account Mgmt, Training & Awareness, Screening

Host

Secure Engineering (SDL), Access Control & Monitoring, Anti-Malware

Internal Network

Access Control & Monitoring, Anti-Malware, Patch & Config Mgmt

Network perimeter

Dual-factor Auth, Intrusion Detection, Vulnerability scanning

Facility

Edge Routers, Firewalls, Intrusion Detection, Vulnerability scanning

Physical controls, video surveillance, Access Control

Common Concern: Data Encryption at Rest

- What problem are you trying to solve?
 - Prevent vendor reading data?
 - Prevent readability of sub-poenaed data?
 - Prevent theft of disk drives from data centers?
- Possible Solutions
 - Encrypt data before sending to cloud (but can prevent vendor from indexing)
 - Vendor provided encryption at rest (but may allow vendor to read)
 - Drill into vendors physical security policies and their contractual obligations

What Email Security Features Can the Vendor Offer?

- Required TLS for all mail between customer and partner domain (in and outbound)
- Data Leakage Protection
 - Provided in cloud
 - Or route to customer for local processing
- Anti-virus and anti-spam
 - Provided in cloud
 - Or route to customer (or other vendor)
- Control over outbound routing

Privacy

Privacy

- How does the vendor approach key issues?
 - being transparent about how vendor gathers and use PII
 - allowing customers to direct how vendor uses their PII
 - limiting vendor's use of PII
 - providing a means by which customers can update their PII to ensure accuracy
 - keep PII secure
 - ensure customers can access their data
- How does the vendor approach common privacy regulations?
 - HIPAA, GLBA, FERPA, Mass 201, PIPEDA, EU Data Protection Directive, and more
- What is the right balance between vendor responsibility and customer responsibility?
 - Who should obtain consent from users if required?
 - Do you want the vendor contacting your users?

Government Subpoenas

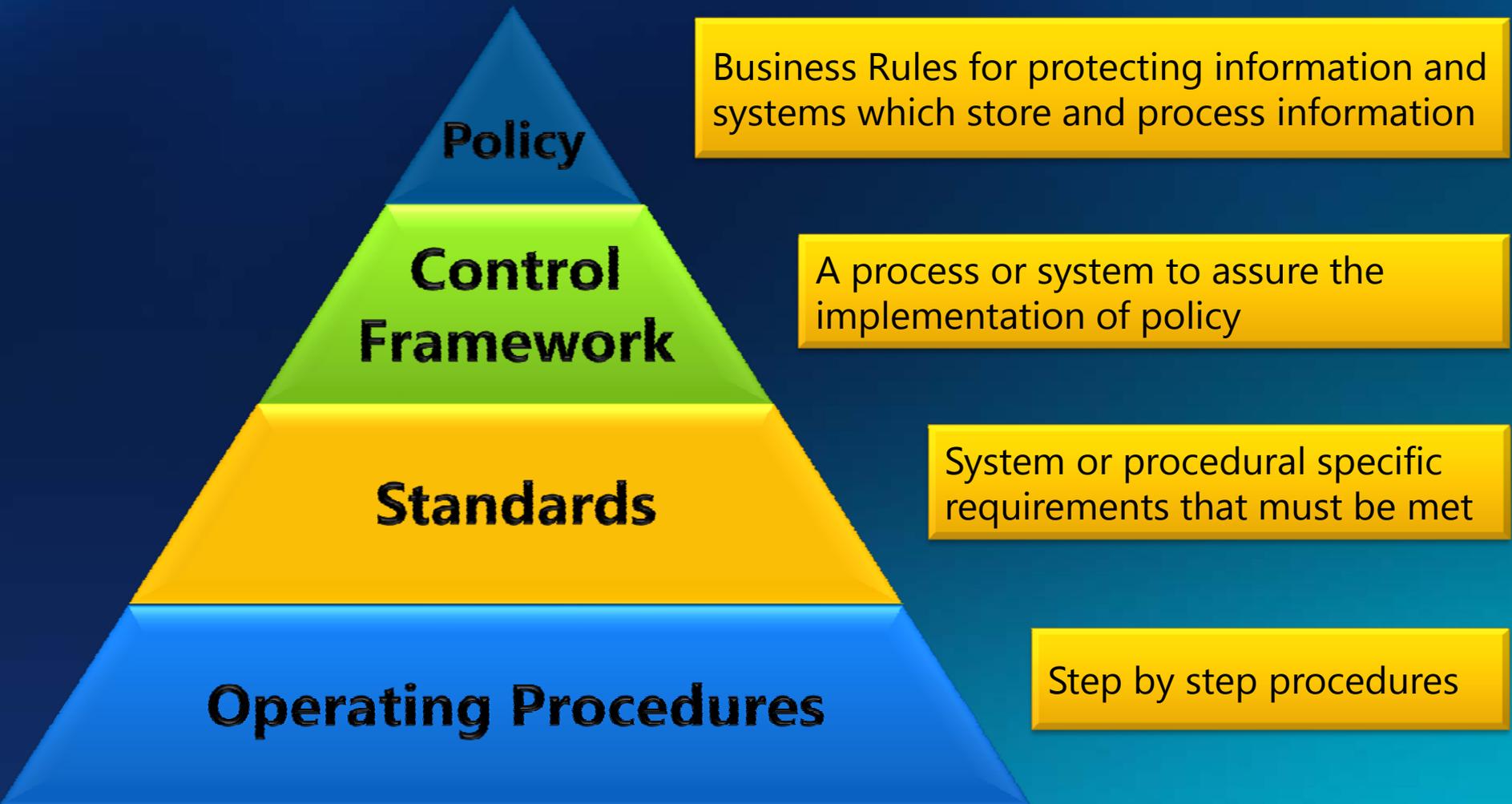
- Vendors must comply with law
 - Is this a risk customer can take?
- Is the vendor clear about their approach?
 - Are they straightforward in how they address subpoenas?
 - Will vendor attempt to redirect subpoenas to the customer?
 - If vendor cannot redirect will they limit records provided?

Data Location and Transfers

- What matters most to the customer?
 - Where data is stored at rest?
 - Where support and operations staff work from?
 - Citizenship of vendor's staff?
 - Do requirements vary for different types of data?
- How does the vendor approach?
 - Can the vendor state where data is stored at rest?
 - Does the vendor offer US only options?
 - What regulations does the vendor comply with?

Compliance

Example Compliance Management Framework: What does your Vendor have?



Thinking through Audit Needs

- Does customer *really* need to conduct their own audits?
- What does "audit" mean?
- Can needs be addressed in different ways that still allow taking advantage of the cloud?
 - What certifications does vendor maintain?
 - What 3rd party audits does vendor offer?
 - What transparency does vendor provide over security policies and procedures?

Supporting Customer Compliance

- Customizable and feature-rich Microsoft Online offerings to suit a customer's compliance needs
 - Use our features to implement your policies
 - Retention policies, archiving, legal hold, etc.
- Third party audits and attestations
- Compliance from end to end (physical infrastructure to services development & operation)

Service Continuity

Does the Vendor have a Comprehensive Service Continuity Program Framework?



- Based on Business Continuity Industry Best Practices
- Provides a standardized approach across the enterprise
- Ensures consistent and sustainable processes
- Focusing on internal core competencies
- Identifies impacts, dependencies, and gaps
- Implements solutions and plans for remediation
- Exercises on a regular basis to ensure processes are operating as intended
- Meet established RTOs and RPOs

Continuity Questions for Vendor

- Does vendor have a formalized continuity program in place?
- What RTO and RPO times does the vendor commit to?
- Does each cloud service have the ability to recover from a disastrous event?
- Is the plan exercised (tested) on a regular basis?
- What is the customer's involvement in testing?

Question & Answer



Discovering your own

Eric Taylor

Northrop Grumman Enterprise Security Architect

September 2010



NORTHROP GRUMMAN

Why discovery is important

- Information gathering is one of the most important stages of an attack.
- Attackers use publicly accessible information to gather reconnaissance against the target.
- Discussion and tips for self auditing:

Social Engineering

Metadata

Google Gathering

Password reconnaissance

Web Resources

**MORE INFORMATION = HIGHER PROBABILITY OF
SUCCESSFUL ATTACK**

Gathering for Social Engineering

- Browse the organizational website and look for general information such as contact information, phone and fax numbers, emails, company structure etc.
- How well designed is the target website? How clean is the HTML code?
 - This might give you a clue about their budget in erecting the site, which in turn may infer on the budget to secure it.
- Publicly accessible or social media to determine
 - People and culture
 - **Terminology**
 - Programming language, skill level of developers, technicians and support personal

Miscellaneous Web Resources

- **Whois Reconnaissance** - Whois databases contain nameserver, registrar, and in some cases full contact information about a domain name.
 - <http://whois.domaintools.com/>
 - <http://www.networksolutions.com/whois/index.jsp>
 - <http://ripe.net>
 - <http://whois.sc>
- **Netcraft:** Netcraft is an Internet monitoring company based in Bradford-on-Avon, England. Their most notable services are monitoring uptimes and providing server operating system detection.
 - <http://searchdns.netcraft.com/>

Miscellaneous Web Resources

- **XSSed:** The XSSed project was created in early February 2007 by KF and DP. It provides information on all things related to cross-site scripting vulnerabilities and is the largest online of XSS vulnerable websites.
 - <http://www.xssed.com>

Google Information Gathering

- Inadvertently exposing sensitive information on that web site due to various web server misconfigurations.
- Email harvesting is an effective way of finding out possible emails (and possibly usernames) belonging to an organization.
 - @vita.virginia.gov = 6,690,000 results
 - emails can be used as a distribution base of a client side attack
- **Google Hacking Database (GHDB)**

Advisories and Vulnerabilities	Pages containing login portals
Error Messages	Pages containing network or vulnerability data
Files containing juicy info	sensitive Directories
Files containing passwords	Various Online Devices
Files containing usernames	Vulnerable Files
Footholds	Vulnerable Servers

How to audit yourself

- Use the site: directive to find a history of files with sensitive information.
 - filetype:
 - Intitle:
 - Intext:
- `site:virginia.gov filetype:xls`
- `site:virginia.gov filetype:doc`
- `site:virginia.gov robots.txt`
- `Site:virginia.gov filetype:sql`

MetaData Information Leakage

- Most types of documents have some metadata in them.
- The following types are the most interesting

Pdf

Xls, xlsx

Doc, dot, dox

Jpg, jpeg

Ppt, pot, pptx

Html, hml (hidden form elements)

- Information gather, attackers could review documents for
 - Usernames
 - Versions information
 - Directories, file locations or websites
 - Email addresses

How to audit yourself

- Retrieving Documents from the Internet
 - `wget -nd -r -A pdf,doc,docx,xls,xlsx -P /tmp targetdomain`
- Metadata tools
 - Exiftool – command line tool
 - `Exiftool filename.doc`
 - FOCA
 - The Metadata Extraction Tool was developed by the National Library of New Zealand
 - Strings – Command line tool from Microsoft Sysinternals
 - `strings filename.doc`
 - Many other ways

Username and Password Reconnaissance

- “Password Profiling” refers to the process of building a custom password list which is designed to guess passwords of a specific entity
- Information gathered using the public website or applications
 - Password Guessing
 - Password Spraying
 - Large amount of users / small amount of password
 - Avoids account lock outs
- Default Application passwords
 - Still out there..

How to audit yourself

- CeWL is a ruby application which spiders a given URL to a specified depth
 - `./cewl.rb -d 1 -w pass.txt site.virginia.gov`
- Using WGET
 - `wget -r -l 2 targetwebsite`
 - `grep -h -r "" source | tr '[:space:]' '\n' | sort | uniq > wordlist.txt`
 - Remove HTML stuff -- `grep -v '<' wordlist.txt > newlist.txt`
 - Compare to existing passwords database or run password guess tool against applications, etc. ***Know your account lockout policy..***

Maltego

- Maltego is an open source intelligence and forensics application.
- It offers mining and gathering of information as well as the representation of this information in a easy to understand format
- Community and Commercial version

References

- Meta Extractor - <http://meta-extractor.sourceforge.net/>
- Strings - <http://technet.microsoft.com/en-us/sysinternals/bb897439.aspx>
- WGET - <http://gnuwin32.sourceforge.net/packages/wget.htm>
- EXIFTOOL - <http://www.sno.phy.queensu.ca/~phil/exiftool/>
- Maltego - <http://www.paterva.com/web5/>
- Google Hacking Database - <http://www.hackersforcharity.org/ghdb/>
- XSSED - <http://www.xssed.com>
- NetCraft - <http://searchdns.netcraft.com/>
- CeWL - <http://www.digininja.org/projects/cewl.php>
- Windows Grep - <http://www.wingrep.com/> or command line - <http://gnuwin32.sourceforge.net/packages/grep.htm>



Virginia Information Technologies Agency

2010 Commonwealth Security Annual Report

John Green
Chief Information Security Officer



§ 2.2-2009

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.



Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Acronyms:

- ISO:** Information Security Officer
- IS:** Information Security
- CAP:** Corrective Action Plan
- CISO:** Chief Information Security Officer of the Commonwealth

ISO Designated: The Agency Head has

Yes - designated an ISO with the agency within the past two years

No – not designated an ISO for the agency since 2006

Expired –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

Attended IS Orientation:

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to “Extra Credit!”



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Security Audit Plan Received: The Agency Head has

Yes - submitted a Security Audit Plan for the period of fiscal year (FY) [2010-2012 or 2011-2013](#) for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2010, Audit Plans submitted shall reflect FY 2011-2013)

No - not submitted a Security Audit Plan since 2006

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY [FY 2010-2012 or FY 2011-2013](#)

Pending –submitted a Security Audit Plan that is currently under review

Corrective Action Plans Received: The Agency Head or designee has

Yes - submitted an adequate Corrective Action Plan or notification of no findings for Security Audits scheduled to have been completed

Some - submitted an adequate Corrective Action Plan or notification of no findings for some, but NOT all Security Audits scheduled to have been completed

No – not submitted any adequate Corrective Action Plans or notification of no findings for Security Audits scheduled to have been completed

Not Due - not had Security Audits scheduled to be completed

N/A - not submitted a Security Audit Plan so not applicable

Pending –submitted a Corrective Action Plan that is currently under review



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Quarterly Updates: The Agency Head or designee has

Yes - submitted adequate quarterly status updates for all corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Some - submitted adequate quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

No - not submitted ANY quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Not Due - no open Security Audit findings

N/A - not submitted a Security Audit Plan or a Corrective Action Plan that was due

Pending - submitted quarterly status update that is currently under review



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Percentage of Audit Obligation Completed:

Percent of sensitive systems reported in 2007 (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *“At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.”*

Agencies that did not submit an IT Security Audit Plan in 2007 were not in compliance and therefore there is no data to report on for 2010.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

N/C – agency not in compliance in 2007, agency did not submit an IT Security Audit Plan in 2007

N/R – agency not required to submit an IT Security Audit Plan until 2008

Pending – currently under review

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved



FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

October 31, 2010



Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Compensation Board	Yes	1	Yes	No	N/A	0%
Dept. of General Services	Yes	3	Yes	No	N/A	0%
Dept. of Human Res. Mgmt	Yes	1	Yes	Yes	Not Due	100%
Dept. Min. Bus. Enterprise	Yes	0	Yes	Not Due	Not Due	N/C
Employee Dispute Resolution	Yes	1	Exception	Exception	Exception	0%
Human Rights Council	Yes	0	Yes	Not Due	Not Due	N/C
State Board of Elections	Yes	0	Expired	Some	No	50%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Forestry	Yes	0	Yes	No	N/A	0%
Va. Dept. of Ag. & Cons. Serv.	Yes	1	Yes	Yes	Yes	66%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Board of Accountancy	Yes	0	Yes	Yes	Not Due	100%
Dept of Business Assistance	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Housing & Community Development	Yes	1	Yes	Yes	Yes	29%
Dept. of Labor & Industry	Yes	0	Yes	No	N/A	N/C
Dept. of Mines, Minerals & Energy	Yes	0	Yes	Yes	Yes	83%
Dept. of Professional & Occupational Regulation	Yes	1	Yes	Yes	Not Due	100%
Tobacco Indemnification Commission	Yes	1	Yes	No	N/A	N/C
Va. Economic Development Partnership	Yes	1	Yes	Not Due	Not Due	N/C
Va. Employment Commission	Yes	1	Yes	Yes	Yes	Exception
Va. National Defense Industrial Authority	Yes	0	Yes	Not Due	Not Due	N/C
Va. Racing Commission	Yes	1	Yes	Yes	Not Due	N/C
Va. Resources Authority	No	0	No	N/A	N/A	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Christopher Newport University	Yes	0	Yes	Not Due	Not Due	0%
Dept. of Education	Yes	1	Yes	Not Due	Not Due	100%
Frontier Culture Museum of Va.	Yes	0	Yes	Not Due	Not Due	N/C
Gunston Hall	Yes	1	Yes	Not Due	Not Due	N/C
Jamestown - Yorktown Foundation	Yes	2	Yes	Yes	Not Due	100%
Library of Va.	Yes	0	Yes	Not Due	Not Due	100%
Norfolk State University	Yes	0	Yes	No	N/A	N/C
Richard Bland College	Yes	0	Yes	Not Due	Not Due	100%
Science Museum of Va.	Yes	1	Yes	Not Due	Not Due	N/C
State Council of Higher Education for Va.	Yes	0	Yes	Not Due	Not Due	N/C
University of Mary Washington	Yes	1	Yes	Yes	Yes	67%
Va. Commission for the Arts	Yes	0	Yes	Not Due	Not Due	N/C
Va. Museum of Fine Arts	Yes	0	Yes	Yes	Some	Exception
Va. School for the Deaf and Blind	Yes	2	Yes	Not Due	Not Due	N/R
Virginia State University	Yes	0	Yes	Yes	Yes	Exception

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact

CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Accounts	Yes	1	Yes	Yes	Not Due	N/C
Dept. of Planning & Budget	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Taxation	Yes	1	Yes	Yes	Not Due	50%
Dept. of Treasury	No	1	Yes	No	N/A	0%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Health Professions	Yes	4	Yes	Not Due	Not Due	0%
Dept. of Medical Assistance Services	Yes	1	Yes	Yes	Yes	100%
Department of Behavioral Health and Developmental Services	Yes	13	Yes	Yes	Yes	100%
Dept. of Rehabilitative Services	Yes	2	Yes	Yes	Not Due	19%
Dept. of Social Services	Yes	4	Yes	Not due	Not Due	0%
Virginia Foundation for Healthy Youth FSF	Yes	1	Yes	Not due	Not Due	N/C
Va. Dept. for the Aging	Yes	1	Yes	Yes	Not Due	Exception
Va. Dept. of Health	Yes	2	Yes	Some	Some	20%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Conservation & Recreation	Yes	1	Yes	Some	Yes	12.5%
Dept. of Environmental Quality	Yes	2	Yes	Yes	Yes	100%
Dept of Game & Inland Fisheries	Yes	3	Yes	Some	Some	N/C
Dept. of Historic Resources	Yes	1	Yes	No	N/A	0%
Marine Resources Commission	Yes	1	Yes	Yes	Yes	100%
Va. Museum of Natural History	Yes	1	Yes	Not Due	Not Due	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Alcoholic Beverage Control	Yes	5	Yes	Yes	Yes	100%
Commonwealth's Attorney's Services Council	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Correctional Education	Yes	0	Yes	Yes	Yes	N/C
Dept. of Corrections	Yes	3	Yes	Pending	Pending	Pending
Dept. of Criminal Justice Services	Yes	0	Pending	Pending	Pending	20%
Dept. of Fire Programs	Yes	2	Yes	Yes	Yes	N/C
Dept. of Forensic Science	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Juvenile Justice	Yes	2	Yes	Yes	Not Due	33%
Dept. of Military Affairs	Expired	1	No	N/A	N/A	N/C
Dept. of Veterans Services	Yes	1	Yes	No	N/A	N/C
Va. Dept. of Emergency Management	Yes	1	Yes	Not Due	Not Due	N/C
Va. State Police	Yes	1	Yes	Yes	Yes	87%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
The Ctr for Innovative Tech.	Yes	0	Yes	Not Due	Not Due	N/C
Va. Info. Technologies Agency	Yes	4	Yes	Yes	Yes	70%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Motor Vehicles	Yes	1	Yes	Yes	Pending	N/C
Dept. of Aviation	Yes	1	Yes	No	N/A	N/C
Dept. of Rail & Public Trans.	Yes	0	Yes	No	N/A	0%
Motor Vehicle Dealers Board	Yes	0	Yes	Not Due	Not Due	N/C
Va. Dept. Of Transportation	Yes	6	Yes	Yes	Yes	66%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Indigent Defense Commission	Yes	2	Yes	Yes	Not Due	N/R
State Lottery Dept.	Yes	2	Yes	Not Due	Not Due	N/R
State Corporation Commission	Yes	3	Yes	No	N/A	N/R
Va. College Savings Plan	Yes	1	Yes	Yes	Not Due	N/R
Va. Office for Protection & Advocacy	Yes	1	Yes	Not Due	Not Due	N/R
Va. Retirement System	Yes	1	Yes	Some	Some	N/R
Va. Workers' Compensation Commission	Yes	3	Exception	Exception	Exception	N/R

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Office of the Governor	Yes	0	No	N/A	N/A	N/C
Office of the Attorney General	Yes	0	Yes	Not Due	Not Due	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Virginia Information Technologies Agency

Upcoming Events





Governor's Proclamation

- Governor McDonnell has proclaimed October 2010 as
Cyber Security Awareness Month

Proclamation can be located at the Governor's Porthole:

<http://www.governor.virginia.gov/OurCommonwealth/Proclamations/2010/Cyber.cfm>

or VITA Information Security Awareness Toolkit:

<http://www.vita.virginia.gov/security/toolkit/default.aspx?id=9930>



Future ISOAG's

From 1:00 – 4:00 pm at CESC

Tuesday - November 9, 2010

Thursday - December 9, 2010

ISOAG will be held the 1st Wednesday of each month in 2011



Future IS Orientation Sessions

Monday - November 1, 2010 1:00 – 3:30
(CESC)

Tuesday - January 11, 2011 9:00 – 11:30
(CESC)

IS Orientation is now available via webinar!



AITR Meeting

AITR Meeting:

Wednesday, October 20th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: CESC



Information Security System Association

ISSA meets on the second Wednesday of every month

DATE: Wednesday, November 10, 2010

**LOCATION: Maggiano's Little Italy, 11800 W. Broad St.,
#2204, Richmond/Short Pump Mall**

**TIME: 11:30 - 1:30pm. Presentation starts at 11:45 &
Lunch served at 12.**

COST: ISSA Members: \$10 & Non-Members: \$20

SPEAKER: TBD



MS-ISAC Webcast

National Webcast!

Wednesday, December 15, 2010, 2:00 to 3:00 p.m.

Topic: Security Management

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/>



Identity Theft Red Flags Rules Extended Until December 31, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until December 31, 2010. Read the FAQ at:

<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



Virginia Information Technologies Agency

Any Other Business ???????



ADJOURN

THANK YOU FOR ATTENDING

