



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

September 7, 2011



ISOAG September 2011 Agenda

- | | | |
|------|--|---|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Application Security:
Threat & Vulnerability Analysis | Deloitte & Touche: Ray Soriano,
Bharan Balasubramanian |
| III. | Penetration Test Execution | Eric Taylor, NG |
| IV. | 2011 Commonwealth Security
Annual Report | Michael Watson, VITA |
| V. | Upcoming Events & Other Business | Michael Watson, VITA |
| VI. | Partnership Update | Bob Baskette, VITA
Michael Clark, NG |

Application Security – Threat and Vulnerability Analysis

Deloitte & Touche LLP

September 7, 2011



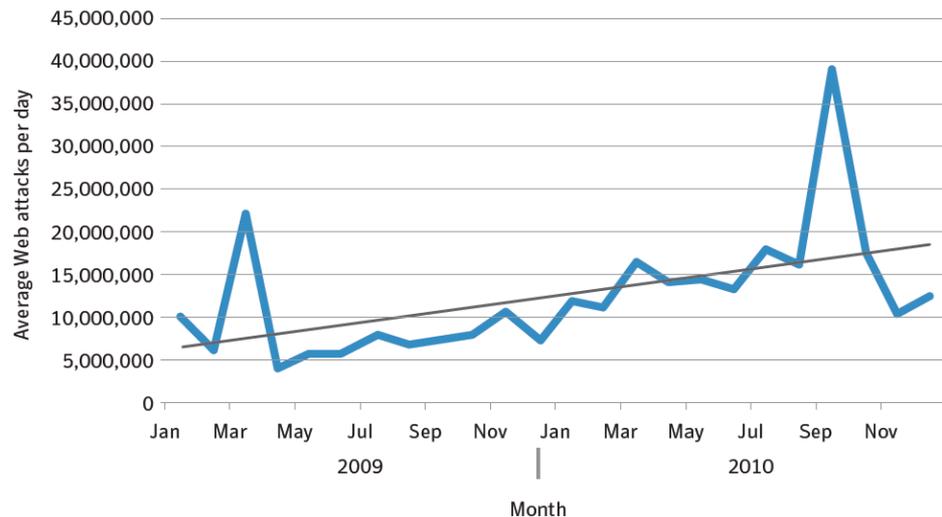
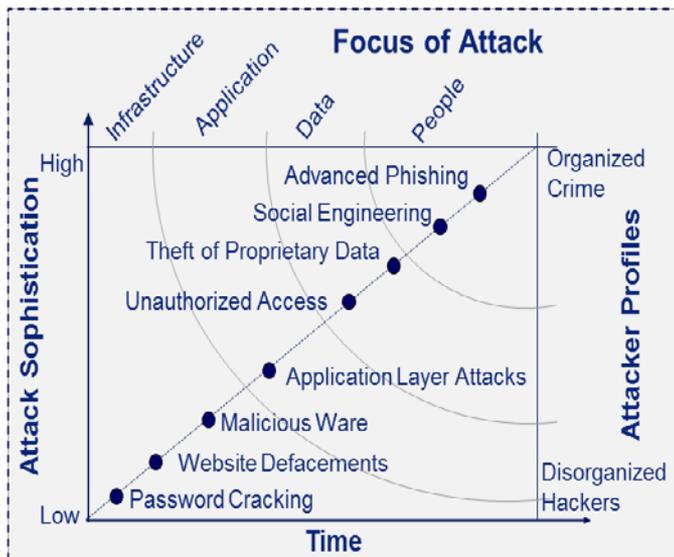
Contents

Threat-Vulnerability landscape	2
Key findings of Deloitte-NASCIO cybersecurity study	3
Application security vulnerability testing	5
Secure development lifecycle	10
Case study	13
Sample vulnerabilities from manual testing	16

Threat-Vulnerability landscape

Increased sophistication, organized cyber crime and rise in web based attacks

- “93% increase in web based attacks” – Symantec Internet Security Threat Report 2010
- “Web Application vulnerabilities represent a significant risk to the modern enterprise” – IBM X-Force® 2010 Trend and Risk Report
- “Roughly 57 percent of all vulnerabilities pertained to Web applications and related technologies” – Cenzic Q3-Q4 2010 Web Application Security Trends Report
- State and local government agencies account for more than 20% of data breaches reported in United States – 2010 Deloitte-NASCIO Cybersecurity Study¹
- Cyber crime is more prevalent; remains an invisible threat that is easy to overlook



Average Web-based attacks per day, by month, 2009–2010

¹ 2010 Deloitte-NASCIO cybersecurity study – “State Governments at Risk”

Source: Symantec Internet Security Threat Report 2010

Key Findings from 2010 Deloitte-NASCIO cybersecurity study¹

Q36. How often does your State conduct vulnerability assessments?

	Quarterly	Semi-Annually	Annually	Ad hoc	Never
Internal penetration testing	13%	4%	13%	62%	2%
External penetration testing	13%	7%	9%	64%	2%
Penetration testing conducted by third party	9%	2%	20%	51%	7%
Application security vulnerability testing and code review	9%	2%	11%	60%	2%

- Threats to Personally Identifiable Information (PII) and Personal Health Information (PHI) are growing—both from the inside and the outside the agency
- States are still in the early stages of establishing programs and deploying technology to protect sensitive data
- CISOs expect to face a host of threats over the next 12 months, ranging from “zombie” networks to social engineering and employee lapses

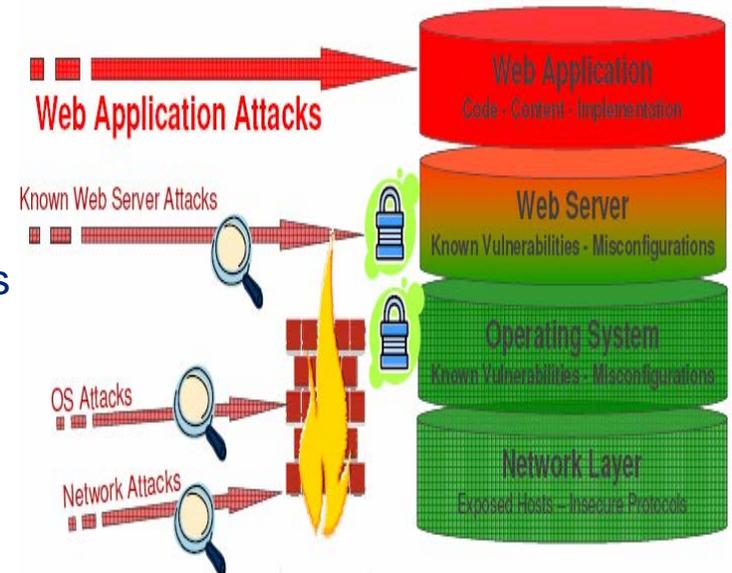
¹ 2010 Deloitte-NASCIO cybersecurity study – “State Governments at Risk”

<http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.PDF>

Why application security assessments?

Increase in citizen data available on the application layer

- Web enablement of citizen centric solutions providing internet based users access to sensitive citizen data
- Mature infrastructure protection measures lead potential attackers to the application layer
- High customizable application layer protocols makes it difficult to develop and configure application layer protection solutions
- Usage of secure transmission protocols provides an encrypted channel, not a secure application
- Vulnerabilities in software leads potential attackers directly to the data
- Most infrastructure security products cannot detect attacks launched on encrypted channels



**HTTP = Universal
Firewall Bypass
Protocol (UFBP)?**

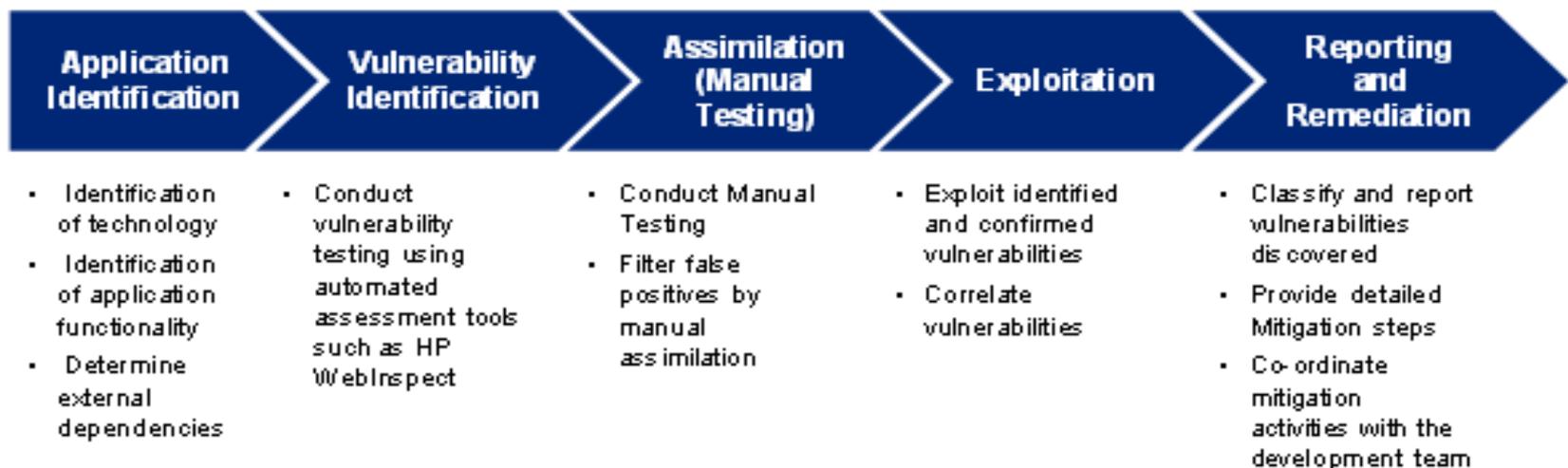
Application security vulnerability testing

Manual and automated techniques

Application security vulnerability testing

Identify security vulnerabilities that impact the application layer

- Defined as the process used to identify security vulnerabilities that may impact the Confidentiality, Integrity or Availability of data and the application itself
- Commercially available products includes IBM Rational AppScan, HP WebInspect, Cenzic Hailstorm and Acunetix WVS
- Deloitte's demonstrated application vulnerability assessment methodology



Common web application vulnerabilities

Deloitte brings several years of application security experience and uses a demonstrated methodology

- Unauthorized access and privilege escalation
- SQL Injection
- Cross site scripting
- Broken authentication and session management
- Insecure direct object reference
- Failure to restrict URL access (Forceful browsing)
- Unvalidated redirects and forwards
- Insecure cryptographic storage
- Information leakage and improper error handling

Manual security vulnerability testing

Performing automated vulnerability scans alone are insufficient

Automated tools can help provide a baseline of technical vulnerabilities (known) within the application. Manual testing aims to understand the business processes handled by the application and attempt to assess security vulnerabilities impacting these processes

- Tests conducted from perspective of a hacker as an end-user
 - Perform In-depth analysis of each request and response (cause and effect)
- Correlate actions, events and vulnerabilities
 - Identify consequences on other pages, and/or on the entire system/module
- Explore additional threats and potential new attack vector(s)
 - Forceful browsing
 - Unauthorized access to restricted records
 - Privilege escalation
 - Session Management
- Understanding business process and identify potential security impacts

Passive vulnerability assessment

Use the power of search engines to mine agency's publically available information

- Search engines allows for a great deal of target reconnaissance that results in little or no exposure for the attacker
- Readily available unsophisticated utility, accessible to any web surfer
- Almost all data on the web has been indexed, including many of the file formats
- Almost anything can come down to a particular "search string"
- An organization's foot print can be determined by simple search queries

Sample search queries – inurl:select inurl:from; inurl:upload files;
inurl:userid; inurl:password

Secure Development Lifecycle

Integrate security principles throughout
System development process

The Need for Secure Development Lifecycle

Early integration of security in the SDLC enables agencies to maximize ROI

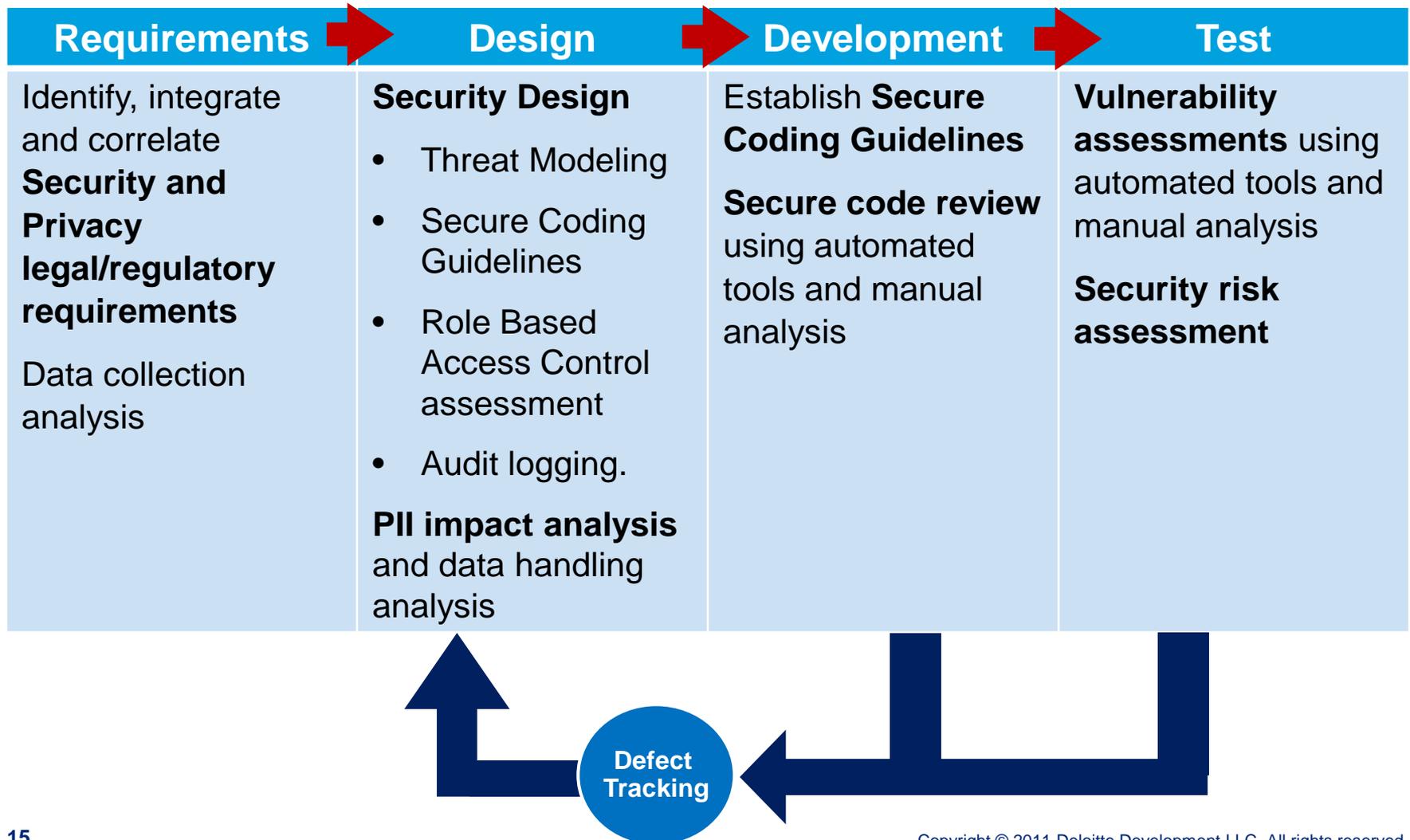
To be most effective, information security and privacy principles must be integrated into the SDLC from system inception through:

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation
- Awareness of potential engineering challenges caused by mandatory security controls
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner

Reference: NIST SP800-64

Sample Secure Development Lifecycle

Incorporates security and privacy principles as an integral part of each phase of systems development



Case study

HHS agency

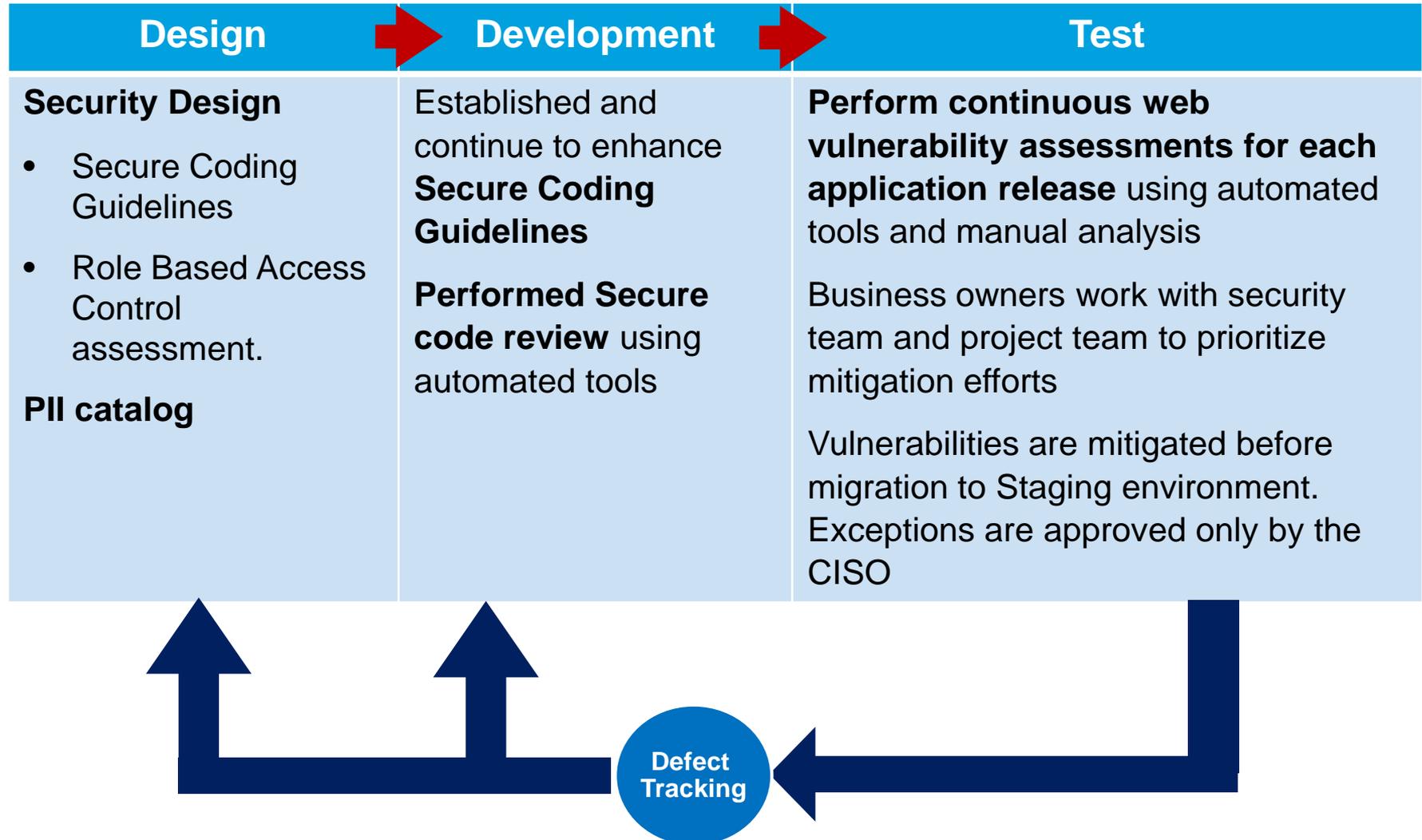
The Approach

Our approach established a security baseline followed by periodic assessments.

- Recognized the need for Application Security Vulnerability Assessment
- Identified & procured automated Vulnerability Assessment tools
 - HP DevInspect to perform secure code review
 - HP WebInspect to perform application vulnerability assessment
- Established a standard for continuous vulnerability assessment
 - Every release of a web application must be tested in Integration test environment
 - Results must be submitted with mitigation plan as part of Systems Acceptance Test deliverable
 - High severity vulnerabilities must be mitigated before being deployed to Production
- Conduct Security Baseline Testing
 - For applications that are in production, a security baseline test was conducted
 - Mitigation timeline is prioritized by business owners and monitored by the security office. Participation of business stakeholders to determine business impacts.
- Perform manual vulnerability testing to complement automated testing efforts

The established process

Enforces mandatory security vulnerability testing for each web application release



Sample vulnerabilities
identified from manual
analysis

Example 1: Combined POST & Querystring Parameter Tampering exposed consumer PII

Unauthenticated User

Address: `phdn_SessionId=1447318224243062608154611&phdn_ApplicationNum=355022`

Pick a Password

The password must be **7 to 14 characters long**. It must contain the following three criteria:

- At least **one uppercase letter**
- At least **one lowercase letter**
- At least **one number**

Do not enter any spaces in the password. The password helps keep information entered on the **Form** private. Please make note of the **selected password** exactly as it was entered--be aware that the password is case-sensitive. The *e-Form* number and password may be used to access the **Form**.

The **Form** number is: `0355022`

Choose a Password: *

Re-enter Password: *

A question and answer may be selected now and be used to later access the **Form** in the case that a password is forgotten and something not known to many people.

Hint Question

Hint Answer

Reference

Annotations:

- The following page requests to pick a password for the application
- But he/she notices that the application reference has changed
- Modified Application Number: 355022
- The attack was successful
- Information contained in an already completed application was shown to the user, thus leading to a compromise of consumer PII (in subsequent pages)

Step 1 Step 2 Step 3 Step 4 Step 5

Example 2: Querystring parameter tampering leads to unauthorized access

The screenshot shows a Microsoft Internet Explorer browser window titled "e-Form - Microsoft Internet Explorer". The address bar contains the URL: `?hdn_SessionId=8995343252791090408111548&hdn_ApplicationNum=346759`. A green callout box in the top right corner identifies the user as an "Authenticated User".

The main content area displays a form titled "Your e-Form Number" with the value "W0346759". Below this, a list of form fields is shown, including "e-Form Number", "Date", "Community Organization Provider Number", "Organization Name", "Type of Community Based Organization", "Benefits Selected", "Preferred Language", and "Interpreter Needed?". A callout box points to the "e-Form Number" field, which contains the value "W0346759 - APPLICATION". A blue callout box explains: "- User has unauthorized access to the restricted application, 346759".

The form is divided into sections: "Name and Address Information" and "Household History". The "Name and Address Information" section includes fields for Name, Street Address, City, State and Zip, County, and various phone numbers. The "Household History" section includes a table with the following data:

Question	Answer
Has the household lived in [redacted] for the past 12 months?	Yes
Has the household ever received benefits in PA?	No
Has the household ever applied for [redacted] in another U.S. state?	No
Have the household members ever [redacted] a different name or social security number?	No

A blue callout box on the right side of the page says "to the". A blue callout box at the bottom left of the page says "Step 3".

Example 3: Cookie manipulation – User Impersonation

Authenticated User

Entity: [TEST_ENTITY_ONE] / Caseload: []

Select	Individual Name	BSU	SSN	
<input type="checkbox"/>	EI, SECONDDUSER	[REDACTED]	[REDACTED]	290320313
<input type="checkbox"/>	MINOR, CONSUMER	[REDACTED]	[REDACTED]	530321693
<input type="checkbox"/>	BARBER, BILLU	[REDACTED]	[REDACTED]	530321992
<input type="checkbox"/>	EI, SC	[REDACTED]	[REDACTED]	530321646
<input type="checkbox"/>	INTSIXONE, EIFIRSTUSER	[REDACTED]	[REDACTED]	530321935
<input type="checkbox"/>	ALDO, SCEI	[REDACTED]	[REDACTED]	290320281
<input type="checkbox"/>	FREY, EIISPTEST	[REDACTED]	[REDACTED]	420320111
<input type="checkbox"/>	HENDERSON, SALLY	[REDACTED]	[REDACTED]	950319544
<input type="checkbox"/>	EI, USERONE	[REDACTED]	[REDACTED]	530321282
<input type="checkbox"/>	PRIMARYSC, SCEI	[REDACTED]	[REDACTED]	530321481
<input type="checkbox"/>	TEST, CAND	[REDACTED]	[REDACTED]	530322099
<input type="checkbox"/>	TESTUSER, AGENT	[REDACTED]	[REDACTED]	530322136
<input type="checkbox"/>	NOSERVICE, NOTES	[REDACTED]	[REDACTED]	000000196
<input type="checkbox"/>	IRVING, SCEI	[REDACTED]	[REDACTED]	070319531
<input type="checkbox"/>	SATPATCHFIVE, EISECONDDUSER	[REDACTED]	[REDACTED]	530321684
<input type="checkbox"/>	INTSIXONE, EITHIRDUSER	[REDACTED]	[REDACTED]	290320504
<input type="checkbox"/>	INTG, NEWCLIENT	[REDACTED]	[REDACTED]	000000007
<input type="checkbox"/>	SATPATCHFIVE, SECONDEIUSER	[REDACTED]	[REDACTED]	530321687
<input type="checkbox"/>	SATADHOCPATCH, EIFIFTHUSER	[REDACTED]	[REDACTED]	950319557
<input type="checkbox"/>	EISEPT, EIUSERFIRST	[REDACTED]	[REDACTED]	530321970
<input type="checkbox"/>	JEFFERSON, EIISPTEST	[REDACTED]	[REDACTED]	530322191
<input type="checkbox"/>	ALERT, TESTING	[REDACTED]	[REDACTED]	530322193
<input type="checkbox"/>	REPORT_EVALUATION	131231312	[REDACTED]	000000160

- Impersonated user able to perform all the operations of TTE1SS1

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6

Example 4: Web Page Caching leads to unauthorized access to sensitive information

The screenshot shows a PDF document in Adobe Reader. The document contains a form with several sections, some of which are redacted with black boxes. The sections are:

- Consumer Demographics**
 - Primary Demographics**

First Name:	[REDACTED]
Registration County/Joinder:	[REDACTED]
Date Of Birth:	[REDACTED]
Gender:	[REDACTED]
County Of Residence:	[REDACTED]
Home Phone:	[REDACTED]
Work Phone:	[REDACTED]
Mobile Phone:	[REDACTED]
Other Phone:	[REDACTED]
Confidential:	No
Confidential Details:	
Status:	Active
Reason Status:	New Referral
 - Address**

Address Type:	[REDACTED]
Address Line1:	[REDACTED]
Address Line2:	[REDACTED]
Address Line3:	[REDACTED]
City:	[REDACTED]
State:	[REDACTED]



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

In addition, this presentation discusses the results of a survey conducted in part by Deloitte. The information obtained during the survey was taken “as is” and was not validated or confirmed by Deloitte.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

Copyright © 2011 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited



Penetration Test Execution

*Eric Taylor, Cyber Security Architect
IT Infrastructure Partnership Team*

September 2011



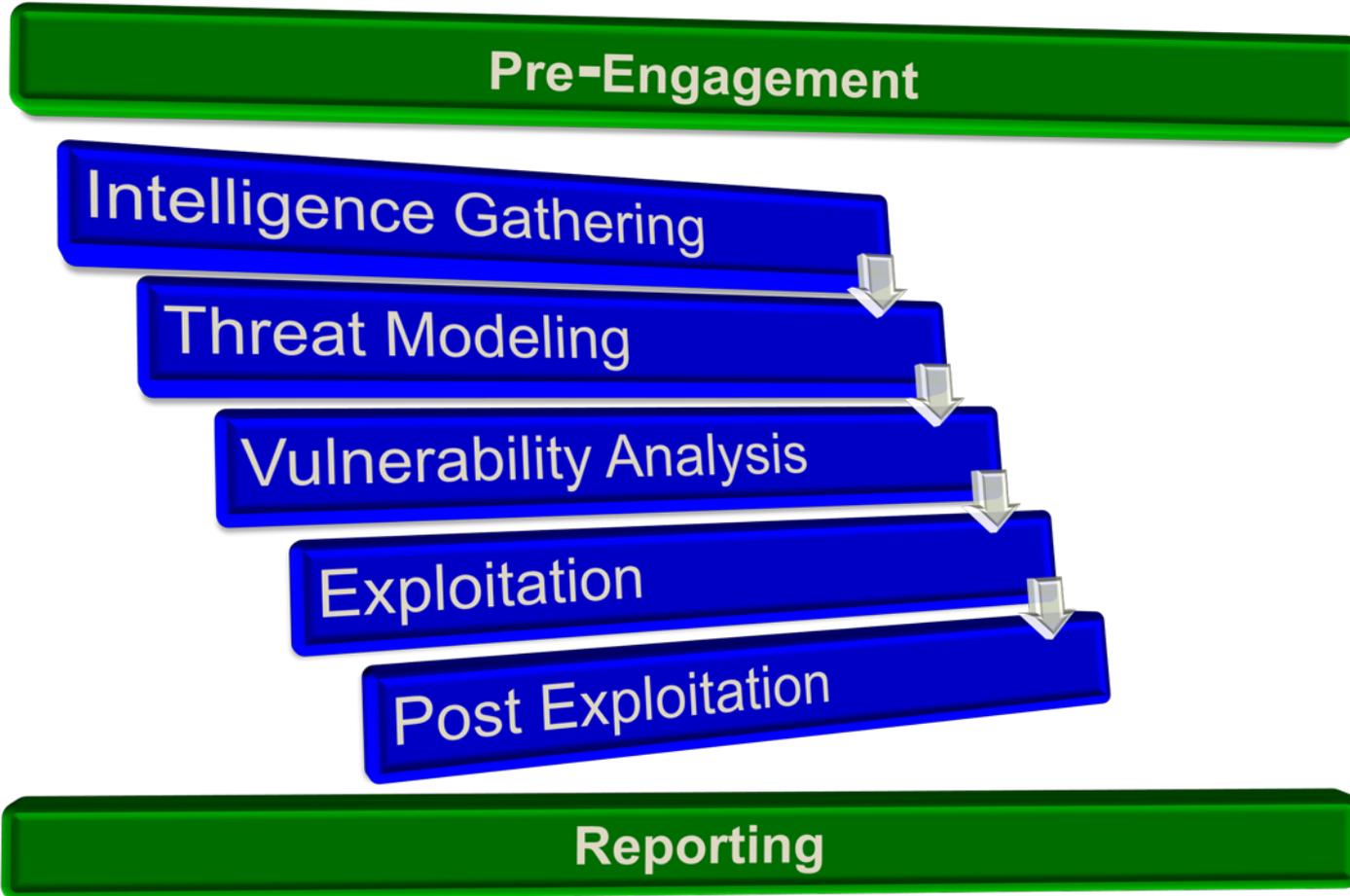
NORTHROP GRUMMAN

- Penetration Testing 101
- Phases of Penetration Testing
 - Pre-engagement Interactions
 - Intelligence Gathering
 - Threat Modeling
 - Vulnerability Analysis
 - Exploitation
 - Post Exploitation
 - Reporting
- A live walk through of the exploitation of a typical corporate network
 - Open Source tools and frameworks
 - Pen Tester vs. real attacks

"The best defense is a good offense"

- Method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders
- Huge difference between running an automated vulnerability assessment tool and a real pen test
 - Often requires manual interaction to exploit logic flaws in applications
- Penetration tests are valuable *
 - Determining the feasibility of a particular set of attack vectors
 - Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence
 - Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
 - Assessing the magnitude of potential business and operational impacts of successful attacks
 - Testing the ability of network defenders to successfully detect and respond to the attacks

* Source: http://en.wikipedia.org/wiki/Penetration_test²⁷



- Define Scope
 - Clearly Defined Contractually (Avoid Scope Creep)
 - The audit must clearly explain the limits of any security tests
 - Types of Testing
 - Blind (Black Box) / Grey Box / Tandem (White Box)
 - Applications / System / Physical / Social Engineering
 - Systems & Applications
 - Physical Sites
- Define Rules of Engagement
 - What / When / How
 - Point of Contact for any service interruption, legalities, etc.
 - Prohibited types of testing (DoS)



- Internet Search

- Google
- Forums
- Social Media (LinkedIn, FaceBook)
- Email Harvesting
- Document Leakage

- Covert Gathering

- On-location
- Dumpster Diving
- Employee Behavior

- External Footprinting

- Whois / Registers
- Application Reconnaissance's
- Banner Grabbing
- Network Scanning



```

nmap -6 -sT -P0 fe80::80a5:26f2:8db7:5d04%12
Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-22 22:42 Eastern Daylight Time
Nmap scan report for lancelet (fe80::80a5:26f2:8db7:5d04)
Host is up (1.0s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
3389/tcp  open  ms-term-serv
5000/tcp  open  upnp
5001/tcp  open  complex-link
5002/tcp  open  rfe
5003/tcp  open  filemaker
5004/tcp  open  avt-profile-1
5357/tcp  open  wsdapi
10243/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 287.05 seconds
  
```

- Looks at the organization as the adversary to identify potential attack vectors
- Combines the intelligence gathered with pre-engagement information to paint the threat landscape
- Business Process & Assets
 - Technical Infrastructure
 - 3rd Party Business Partners
 - Business Work Flow
 - Contracts and Negotiations
 - Critical Personnel
 - Services



How Do Current Operations Work?

How do they work differently from how management thinks they work?

How do they need to work?

- Vulnerability Analysis is used to identify and evaluate the security risks posed by identified vulnerabilities.
- Identification
 - Automated Tools
 - Nessus, OpenVAS, eEye, NeXpose, etc..
 - Web Application Scanners
 - WeInspect, Acunetix, AppScan
 - Misconfigurations
- Validation
 - Public Research
 - Associated Proof Of Concept's
 - Exploit Code



- Combines information from Intelligence Gathering and Vulnerability Analysis to decide on effective approach to gaining access or circumventing security controls
- Exploits Framework or Commercial Exploit tools
 - May Require Custom Exploits



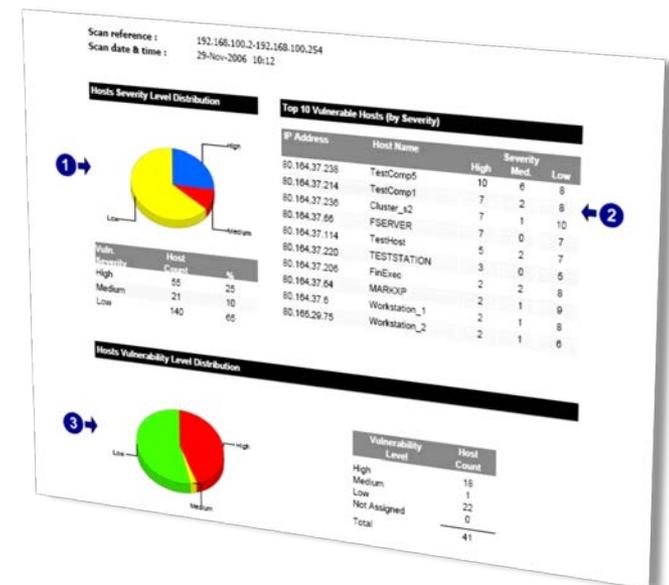
- Taking advantage of Trust Relationships
- Fuzzing – attempting to discover security flaws
- Brute Force Password Guessing
- Default Configurations
- RF (Wireless) Access
- Attacking the User
 - Social Engineering
 - Client Side attacks
- Physical On-site Attacks
 - Man-in-the-middle

- Gather as much information from the system as possible.
- Pillaging
 - Exfiltration of Data
 - Passwords / Hashes / Encryption Keys
- Business impact attacks
 - Redirect or Interrupt Supply Chain
 - Transfer Funds
 - Free Services
 - Personal Information
- Trust Relationships
 - Pivot to other systems

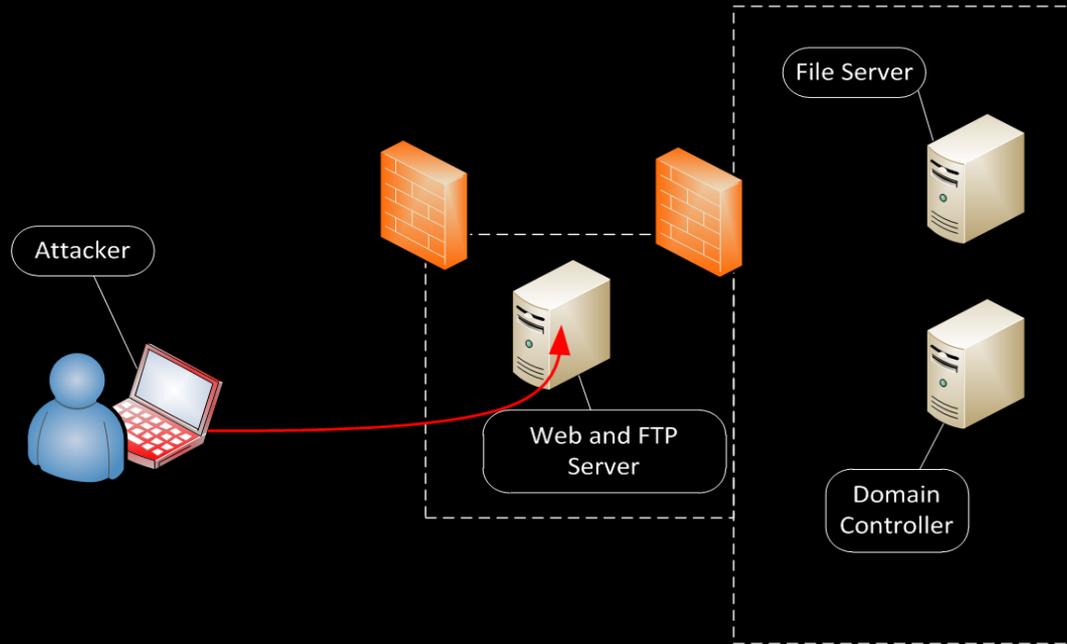


- Cleanup
 - Clear Event Data
 - Time Stomp
 - Delete Test Data
- Persistence
 - Backdoors Services
 - Credentials
 - Remote Access

- The goal is to provide a quality report that encompasses findings for all issues identified
- The report should include the description of the risk and additional elements that allows the organization to prioritize the remediation
 - Impact; damage, affected users
 - Exploitability
 - Reproducibility
- Actionable recommendations for remediation
 - CVE ID, BID #, OSVDB
 - CCE or required configuration change
 - Vendor Specific Solution URL



Simple Corporate Network



- Pentest Standards
 - http://www.pentest-standard.org/index.php/Main_Page
- OSSTMM - Open Source Security Testing Methodology Manual
 - <http://www.isecom.org/osstmm/>
- Metasploit Unleashed
 - [http://www.offensive-security.com/metasploit-unleashed/Metasploit Unleashed Information Security Training](http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training)
- Back Track – Linux Penetration Distribution
 - <http://www.backtrack-linux.org/>
- Wiki Penetration Definitions Page
 - http://en.wikipedia.org/wiki/Penetration_test



Virginia Information Technologies Agency

2011 Commonwealth Security Annual Report

Michael Watson
Acting 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	Percentage of CAPs Received	Percentage of Quarterly Updates Received	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	90%	75%	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	Percentage of CAPs Received	Percentage of Quarterly Updates Received	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	90%	75%	100%

Security Audit Plan Received: The Agency Head has

Yes - submitted a Security Audit Plan for the period of fiscal year (FY) 2011-2013 or 2012-2014 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2011, Audit Plans submitted shall reflect FY 2012-2014)

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 2011-2013 or FY 2012-2014

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

Percentage of CAPs Received: The Agency Head or designee has

% – submitted % of CAPs for planned audits listed on submitted Audit Plan

Not Due - not had Security Audits scheduled to be completed

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



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	Percentage of CAPs Received	Percentage of Quarterly Updates Received	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	90%	75%	100%

Percentage of Quarterly Updates Received: The Agency Head or designee has % – submitted % of quarterly status updates received for corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Not Due - no open Security Audit findings

Pending - submitted quarterly status update that is currently under review



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	Percentage of CAPs Received	Percentage of Quarterly Updates Received	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	90%	75%	100%

Percentage of Audit Obligation Completed:

Percent of sensitive systems reported **by 2008** (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 **by 2008** were not in compliance and therefore there is no data to report on for **2011**.

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 by 2008, agency did not submit an IT Security Audit Plan **by 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?

December 31, 2011



Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Compensation Board						
Dept. of General Services						
Dept. of Human Res. Mgmt						
Dept. Min. Bus. Enterprise						
Employee Dispute Resolution						
Human Rights Council						
State Board of Elections						

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						
Va. Dept. of Ag. & Cons. Serv.						

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						
Dept of Business Assistance						
Dept. of Housing & Community Development						
Dept. of Labor & Industry						
Dept. of Mines, Minerals & Energy						
Dept. of Professional & Occupational Regulation						
Tobacco Indemnification Commission						
Va. Economic Development Partnership						
Va. Employment Commission						
Va. National Defense Industrial Authority						
Va. Racing Commission						
Va. Resources Authority						

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						
Dept. of Education						
Frontier Culture Museum of Va.						
Gunston Hall						
Jamestown - Yorktown Foundation						
Library of Va.						
Norfolk State University						
Richard Bland College						
Science Museum of Va.						
State Council of Higher Education for Va.						
University of Mary Washington						
Va. Commission for the Arts						
Va. Museum of Fine Arts						
Va. School for the Deaf and Blind						
Virginia State University						

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						
Dept. of Planning & Budget						
Dept. of Taxation						
Dept. of Treasury						

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						
Dept. of Medical Assistance Services						
Department of Behavioral Health and Developmental Services						
Dept. of Rehabilitative Services						
Dept. of Social Services						
Virginia Foundation for Healthy Youth FSF						
Va. Dept. for the Aging						
Va. Dept. of Health						

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						
Dept. of Environmental Quality						
Dept of Game & Inland Fisheries						
Dept. of Historic Resources						
Marine Resources Commission						
Va. Museum of Natural History						

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						
Commonwealth's Attorney's Services Council						
Dept. of Correctional Education						
Dept. of Corrections						
Dept. of Criminal Justice Services						
Dept. of Fire Programs						
Dept. of Forensic Science						
Dept. of Juvenile Justice						
Dept. of Military Affairs						
Dept. of Veterans Services						
Va. Dept. of Emergency Management						
Va. State Police						

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.						
Va. Info. Technologies Agency						

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						
Dept. of Aviation						
Dept. of Rail & Public Trans.						
Motor Vehicle Dealers Board						
Va. Dept. Of Transportation						

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						
State Lottery Dept.						
State Corporation Commission						
Va. College Savings Plan						
Va. Office for Protection & Advocacy						
Va. Retirement System						
Va. Workers' Compensation Commission						

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						
Office of the Attorney General						

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





Information Security System Association

ISSA

DATE: Wednesday, Sept 14, 2011

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: TBA

TOPIC: TBA



Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - October 5, 2011

Wednesday - November 2, 2011

ISOAG will be held the 1st Wednesday of each month in 2011 and 2012



Future IS Orientation Sessions

Tuesday - September 13, 2011 **9:00 – 11:30a**
(CESC)

Tuesday - November 8, 2012 **1:00 – 3:30p**
(CESC)

IS Orientation is now available via webinar!



COVITS 2011

The Commonwealth of Virginia's Innovative Technology Symposium

COVITS is a forum to discuss technology requirements, share valuable lessons from actual case studies, and glimpse the future of government interaction with its customers along with invaluable networking opportunities for sponsors and attendees.

When: Sept 26 – 27

Where: Hilton Richmond Hotel at Short Pump
12042 West Broad Street
Richmond, VA 23233

REGISTER ON-LINE: <http://www.covits.org/Registration/>

Contact: **Liese Brunner**
Registration Coordinator
(916) 932-1355
lbrunner@govtech.com



2011 VA SCAN CONFERENCE

Virginia Alliance for Secure Computing and Networking
(VA SCAN) annual conference.

WHEN: October 6 - 7, 2011

WHERE: College of William and Mary in Williamsburg, Virginia

“SECURITY WITH OUT BORDERS”

Don't miss this opportunity to hear
leaders in the security field discuss current issues
And effective security practices

Conference will include a SANS class for those who want the opportunity to receive formal security training and/or earn CPE's. SEC567: Power Packet Crafting with Scapy taught by SANS instructor, Judy Novak. Seats for the SANS course are limited to 68 so register early if you want to take the course!

Details / Register: <http://wmpeople.wm.edu/site/page/pckell>

Questions? Contact Pete Kellogg at pckell@wm.edu or 757-221-1822.



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

September 7, 2011



NORTHROP GRUMMAN



ADJOURN

