



Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

October 23, 2007



Columbus Day!



Evaluation Time!



Cooler Weather

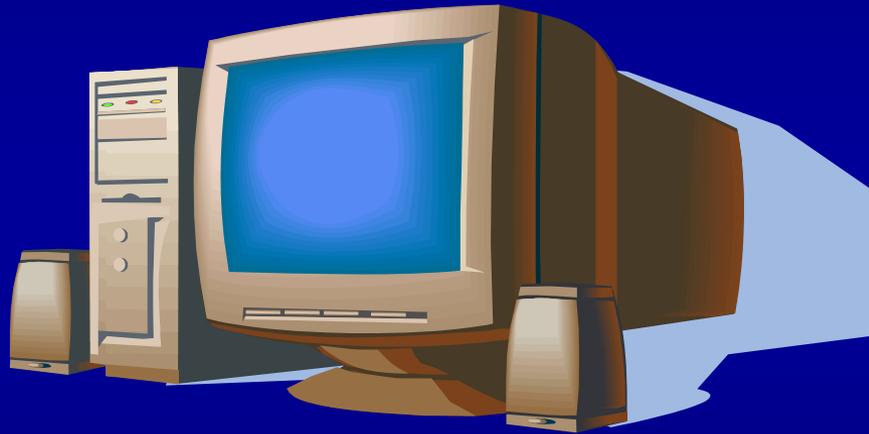




ISOAG October 2007 Agenda

- | | | |
|-------|---|------------------------------------|
| I. | Welcome and Opening Remarks | Peggy Ward, VITA |
| II. | Computer Crimes Security Update | Gene Fishel, OAG |
| III. | Computer Evidence Recovery Unit Part II | Richard Seweryniak, VSP |
| IV. | IT Asset Movement & Data Removal | Michael VonSlomski, IT Partnership |
| V. | IT Asset Surplus Disposition | Brad Crawford, DGS |
| VI. | Cyber Security Awareness | John Karabaic, DMAS |
| VII. | IT Security Audit | Cathie Brown, VITA |
| VIII. | Citizens Awareness Banner & Guide to On-Line Protection | Tripp Sims, VITA |
| IX. | Recursive DNS, The Storm Worm, and You | Tripp Sims, VITA |
| X. | Data Breach Notification | Peggy Ward, VITA |
| XI. | Upcoming Events & Other Business | Peggy Ward, VITA |

OFFICE OF THE VIRGINIA ATTORNEY GENERAL



Computer Crimes Overview and Security Update



PRESENTED BY :
VIRGINIA ATTORNEY GENERAL
BOB MCDONNELL



GENE FISHEL
SENIOR ASSISTANT ATTORNEY GENERAL
CHIEF, COMPUTER CRIME SECTION

OUTLINE

- Virginia Law and Resources
- Notable Security Threats
- SPAM
- Identity Theft
- Child Exploitation

Virginia Law and Resources

- **Computer Crimes Act: Title 18.2-152.1 – 152.15**
 - Computer Fraud
 - Computer Trespass
 - Computer Invasion of Privacy
 - Theft of Computer Services
 - Harassment by Computer
 - Using Computer to Gather ID Info (Phishing)

Virginia Law and Resources

- Virginia Attorney General Office (Computer Crime Section) and U.S. Attorney Offices (EDVA and WDVA)
- Virginia State Police and Local Law Enforcement
- Federal law enforcement (FBI, Postal Inspectors, Secret Service, FTC)
- ISP's

Notable Security Threats

- Phishing

- § [18.2-152.5:1](#). Using a computer to gather identifying information; penalties.
- A. It is unlawful for any person...to use a computer to obtain, access, or record, through the use of material artifice, trickery or deception, any identifying information...Any person who violates this section is guilty of a Class 6 felony.
- B. Any person who violates this section and sells or distributes such information to another is guilty of a Class 5 felony.
- C. Any person who violates this section and uses such information in the commission of another crime is guilty of a Class 5 felony

Notable Security Threats

- **Phishing Variations**
 - **Banking Trojans**
 - Website Based
 - **“Vishing”**
 - VOIP Based
 - **Spear Phishing**
 - Individual Targeting

Notable Security Threats

- Pharming
- Malicious Viruses
 - Spyware

SPAM

- **Virginia Anti-Spam statute: Virginia Code Section 18.2-152.3:1**
- **Federal CAN-SPAM ACT**
- **Criminalizes the use of fraudulent means to transmit unsolicited bulk e-mail**

SPAM

- Commonwealth v. Jeremy Jaynes
- Nation's first felony spam conviction

Kilgore Announces Nation's First Felony Spam Arrest

- World's Eighth-Worst Spam Kingpin Ensnared by Tough New Virginia Law -

Thursday, November 4, 2004

Duo convicted of sending spam to AOL users

The brother is sentenced to 9 years and his sister is fined \$7,500 in the nation's first trial on e-mail fraud.

By Matthew Barakat / Associated Press

LEESBURG, Va. - A brother and sister who sent unsolicited junk e-mail to millions of America Online customers were convicted Wednesday in the nation's first felony prosecution of distributors of spam.

Jurors who convicted Jeremy D. Jaynes, 30, and Jessica DeGroot, 28, sentenced Jaynes to a nine-year prison term and fined DeGroot \$7,500 with fraudulent and untraceable routing information.

A third defendant, Richard Rutkowski, was acquitted of similar charges including the penalty phase.

Prosecutors compared Jaynes and DeGroot, both of the Raleigh, N.C., area, to snake-oil salesmen who used the Internet to peddle junk like a "FedEx refund processor" that supposedly allowed people to earn \$75 an hour while working from home.

In one month alone, Jaynes received 10,000 credit card orders, each worth \$39.95, for the processor. "This was just a case of fraud," state prosecutor Samuel E. Fishel said. "This is a snake-oil salesman in a new format."

Prosecutors asked the jury to impose a maximum sentence of 15 years for Jaynes and a maximum sentence of 15 years for his sister.

Defense lawyers asked jurors to spare the defendants prison terms.

Kilgore today announced the nation's first trial on e-mail fraud. The Loudoun County grand jury has indicted the brother and sister on three counts each of sending spam and acquitted the third co-defendant in the nation's first felony spam trial that ended Wednesday.

Spammer Jailed, Fines Issued In Landmark Case

Dan Telvock



Nov 03, 2004 -- A Loudoun County Circuit Court jury convicted a brother and sister from North Carolina on three counts each of sending spam and acquitted the third co-defendant in the nation's first felony spam trial that ended Wednesday.

The trial lasted five days and the jury deliberated for about one-and-a-half days. The jury recommended that Jeremy Jaynes, 30, of North Carolina, serve nine years in prison.

Three on Trial in Loudoun in Felony Spam Case

N.C. Defendants Accused of Illegal E-Mail Operation Targeting AOL Accounts

By Karin Brullia
Washington Post
Wednesday, Oct 27, 2004

'Snake-oil' spammers feel wrath of US law

By Matthew Barakat
Leesburg, Virginia
November 5, 2004

A brother and sister who sent unsolicited junk email to millions of America Online customers have been convicted in the nation's first felony prosecution of spam distributors.

A North Carolina e-mail spammer and his sister were convicted Wednesday of sending millions of spam e-mails to AOL users.

Jurors who convicted Jeremy Jaynes, 30, and Jessica DeGroot, 28, on Wednesday later sentenced Jaynes to a nine-year prison term and fined DeGroot \$US7500 (\$A9931) for three convictions each of sending emails with fraudulent and untraceable routing information.

A third defendant, Richard Rutkowski, was acquitted of similar charges.

Jeremy Jaynes, 30, of North Carolina, was sentenced to nine years in prison and his sister, Jessica DeGroot, 28, was fined \$7,500.

Prosecutors compared Jaynes and DeGroot, of North Carolina to modern-day snake-oil salesmen who used the internet to peddle junk like a "FedEx refund processor" that supposedly allowed people to earn \$75 an hour while working from home.

In one month alone, Jaynes received 10,000 credit card orders, each for \$39.95, for the processor.

"This was just a case of fraud," state prosecutor Samuel Fishel said. "This is a snake-oil salesman in a new format."

9 Year Sentence For

Spammer

Trial Shows How Spammers Operate

Trial of Prolific E-Mail Spammer Shows How Operate E-Mail Pitches, Made Money

AP Associated Press

LEESBURG, Va. Nov 14, 2004 — As one of the world's most prolific spammers, Jeremy Jaynes pumped out at least 10 million e-mails a day through the help of 16 high-speed lines, the kind of Internet capacity a 1,000-employee company would need.

Jaynes' business was remarkably lucrative; prosecutors say he got \$750,000 per month. If you have an e-mail account, chances are good you've gotten your attention, pitching software, pornography and work-at-home schemes.

04/11/2004

US spammer Jeremy Jaynes could face up to nine years in prison following the recommendation of a Virginia jury that found him guilty of clogging inboxes with unsolicited commercial e-mail.

Jaynes, 30, his sister, Jessica DeGroot, 28, and a third defendant, Richard Rutkowski, all from North Carolina, were charged by Virginia state prosecutors with violating the state's tough anti-spamming laws, which came into force in July last year.

The legislation was the first in the US to introduce custodial sentences for the worst offenders, and applies when the spammer:

is convicted in the nation's first felony spam case that Jeremy Jaynes was sentenced to nine years in prison in North Carolina and his sister was fined \$7,500.

Prosecutors asked the jury to impose a maximum sentence of 15 years for Jaynes and a maximum sentence of 15 years for his sister.

Prosecutors compared Jaynes and DeGroot, of North Carolina to modern-day snake-oil salesmen who used the internet to peddle junk like a "FedEx refund processor" that supposedly allowed people to earn \$75 an hour while working from home.

Pre December 2003



December 2003



December 2004



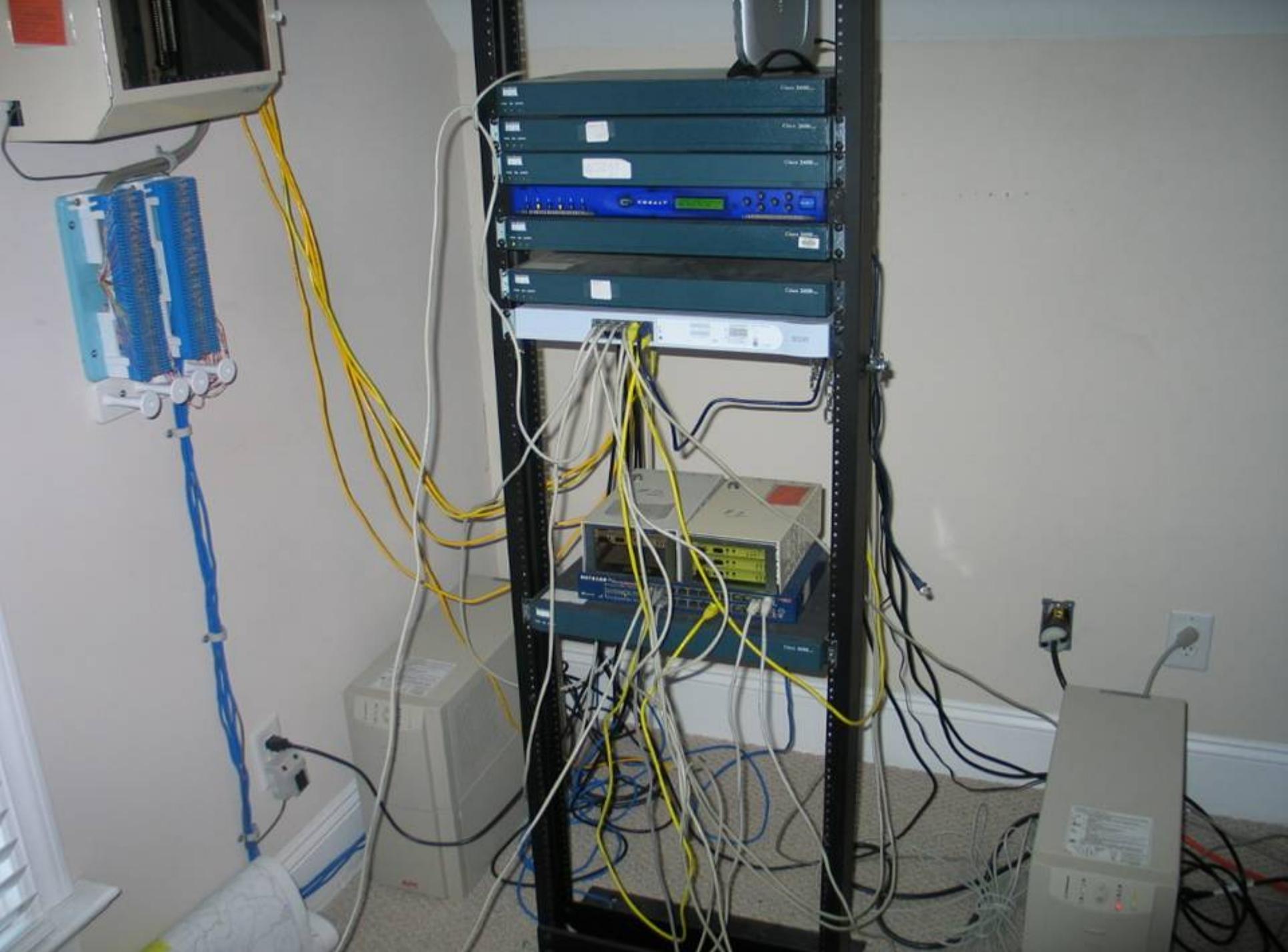
Office



Residence







Identity Theft

- Identity Theft Protection Act
 - State Agencies Regulated (2.2-3800)
 - Virginia Code Section 18.2-186.3
 - Felony for acquiring and misusing personal identifying information

Identity Theft

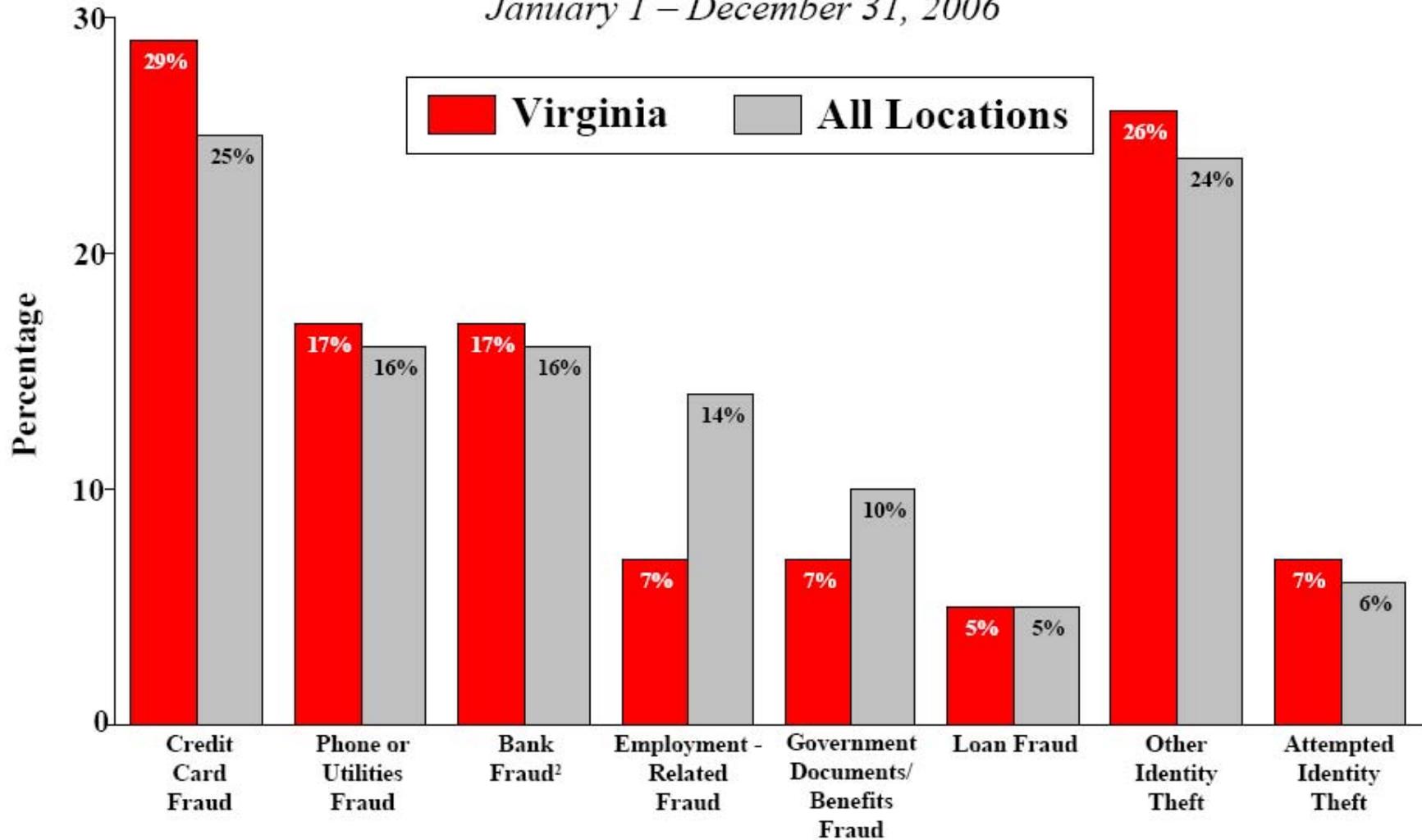
- Database Breaches
 - 2006 Legislation
 - Unauthorized acquisition 50 or more persons in same transaction prohibited (18.2-186.3)
 - Felony: Up to 10 years
 - Response to Choicepoint, Lexis-Nexis, DSW



Figure 1

How Victims' Information Is Misused¹

January 1 – December 31, 2006



¹Percentages are based on the total number of complaints in the Identity Theft Data Clearinghouse: 5,137 from Virginia victims and 246,035 from victims in all locations. Note that 17% of identity theft complaints from Virginia victims and 18% from victims in all locations include more than one type of identity theft.

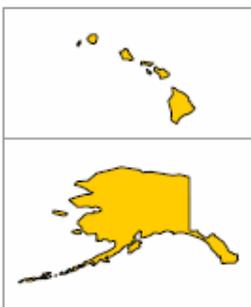
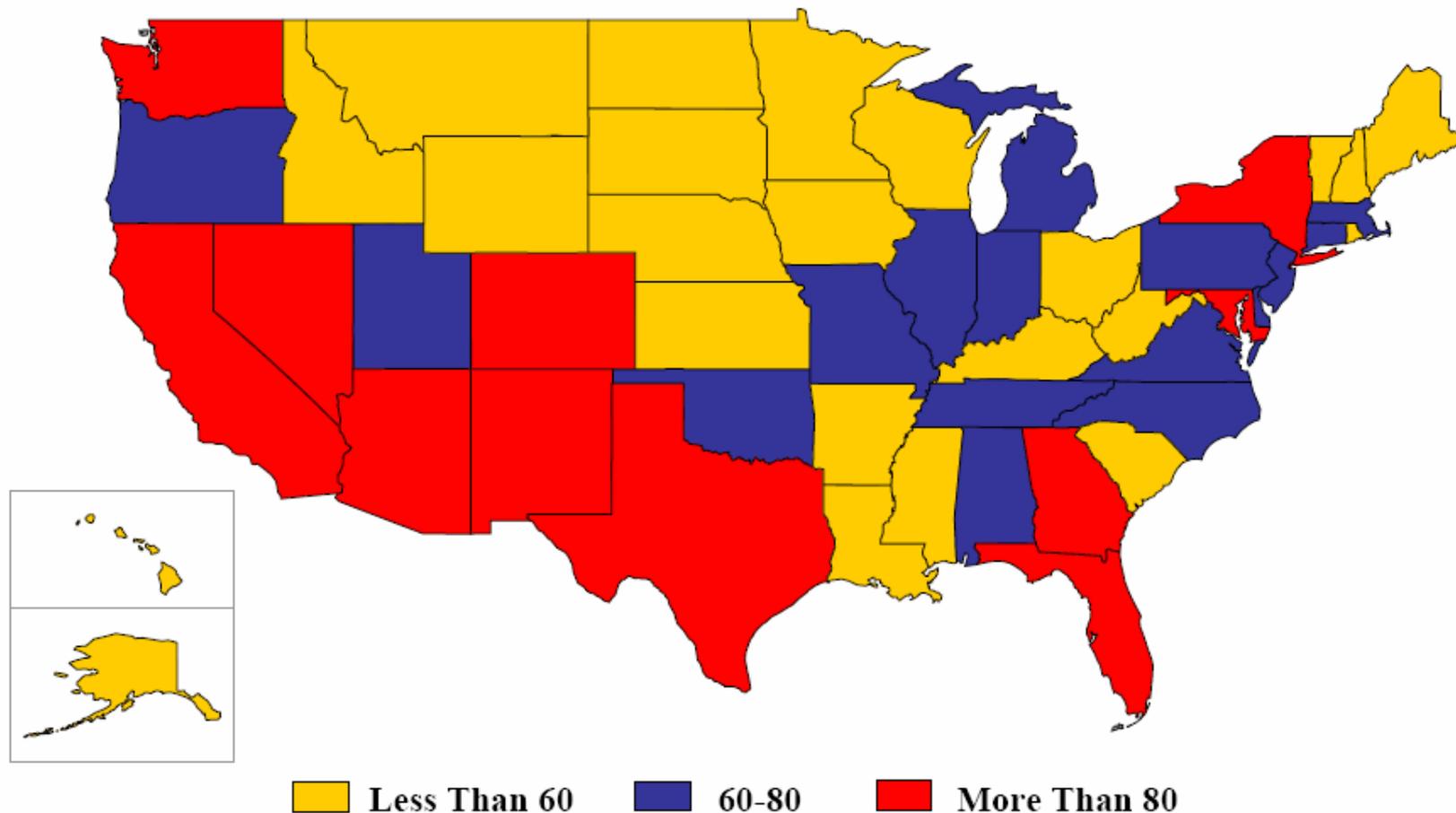
²Includes fraud involving checking and savings accounts and electronic fund transfers.



Figure 4b

Identity Theft Victims by State (Per 100,000 Population)¹

January 1 – December 31, 2006



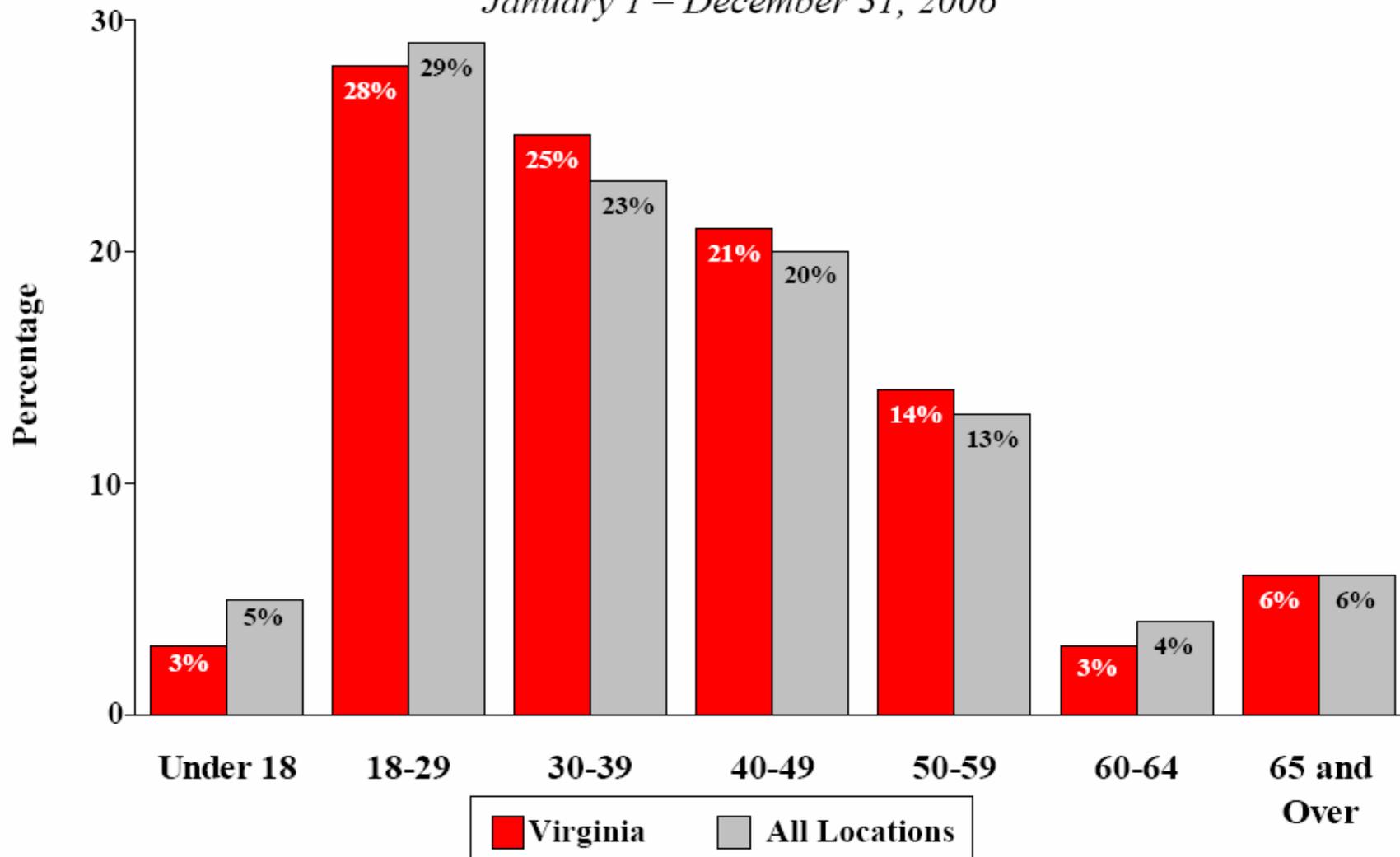
¹Per 100,000 unit of population estimates are based on the 2006 U.S. Census population estimates (Table NST-EST2006-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2006). Numbers for the District of Columbia are 765 victims and 131.5 victims per 100,000 population.



Figure 3

Complaints by Victim Age¹

January 1 – December 31, 2006



¹Percentages are based on the number of identity theft complaints where victims reported their age: 4,626 from Virginia victims and 225,532 from victims in all locations. 94% of victims from Virginia and from all locations who contacted the Federal Trade Commission directly reported their age.

Child Exploitation

- Child pornography and online solicitation
- Found in SPAM, newsgroups, websites
- Report to:
 - Virginia Attorney General's Office
 - State and Local law enforcement
 - National Center for Missing and Exploited Children (NCMEC)

Child Exploitation

- Virginia Code Sections 18.2-372 - 381
 - Obscenity
 - Production, Reproduction, Distribution of Child Pornography
 - Possession of Child Pornography
 - Online Solicitation of Minors

Gene Fishel

**Senior Assistant Attorney General
Chief, Computer Crime Unit**

Office of the Attorney General

804-786-2071

sfishel@oag.state.va.us

WWW.VAAG.COM



Information Security Officers Meeting October 2007

Virginia State Police

Introduction



Mr. Richard Seweryniak
Digital Forensic Examiner

(804) 674-2593

richard.seweryniak@vsp.virginia.gov

Master of Science,
Information Technology
specializing in Information Assurance
University of Maryland

Introduction



Bureau of Criminal Investigation
Criminal Intelligence Division
Computer Evidence Recovery Unit

State Police Headquarters
7700 Midlothian Turnpike
Richmond VA, 23235

CERU

Computer Evidence Recovery Unit of the Virginia State Police provides assistance to local, state and federal law enforcement agencies with on-scene execution of search warrants for computer-related evidence, evidence recovery through forensic examination, and quarterly training classes in computer search and seizure.

CERU

- Investigate the crime or incident, not the technology
 - Network intrusion
 - Peer-to-peer networks
 - Concealed digital cameras
- Not a replacement for internal security
- CERU is "evidence recovery"

Other, national level

- Many agencies have their own digital forensics and incident response units
 - FBI field offices
 - Homeland Security
 - Department of Defense
 - Secret Service
 - National Ground Intelligence Center
 - ... and many others

HTCU, seven statewide

- High Tech Crime Units are located in each of 7 divisions with at least one high tech agent
- Considered “first responders”
- Investigators
- May assist local law enforcement

CERT, national level

Computer Emergency Response Team
Based at Carnegie Mellon University,
CERT is a federally funded research
and development center created in
response to an Internet worm that
spread in November 1988, crippling
about 10% of the existing Internet at
that time

Types of media examined



- Computers
 - hard drive
 - cd-rom media
 - dvd media
 - other storage media
- Servers (file, web, e-mail)
- Digital cameras
- Cell phones
- Blackberry and pda devices
- *USB drives*

Types not examined

- Items with no storage media
- Items that have been tampered which jeopardize the evidence – maintain proper chain of custody and forensic procedures!



When in doubt...

- Contact your nearest Virginia State Police High Tech Crime Unit for assistance from an experienced and trained special agent



Digital Artifacts

"Digital Artifacts" refer to evidence generated by computer and other electronic devices on storage media and can be retrieved for forensic examination

Digital Forensics

- Digital forensics differs greatly from biological or chemical forensic analysis
- Tests for DNA or drugs result in a yes or no response.
- Digital forensics involves much more data that includes, dates, times, locations, users, access permissions, physical data and logical data

Physical vs. Logical Data

- What's the difference?
- Physical data refers to the bits and bytes of the storage media, containing fragments of other data overwritten
- Logical data is the interpretation into usable format, such as an e-mail or document

Logical Data

- Logical data can be viewed by just about any computer user by opening an application such as Outlook or Word
- Copying logical files from one storage media to another will lose "RAM slack" and "file slack"

Physical Data

- Physical data contains much more information and is essential to investigations
- Who has permissions for files, when was it modified, trace evidence of a crime in files not completely overwritten
- Also traces of data not intended to be written to permanent files such as temporary files, "swap files", and "slack"

CERU stats, 2004

- In 2004, the CERU assisted with 89 investigations involving 3,946 gigabytes of data on 134 computers and 2,145 digital equipment items
- 54 of those investigations were conducted for federal, state and local law enforcement agencies in support of ongoing criminal investigations

CERU stats, 2006

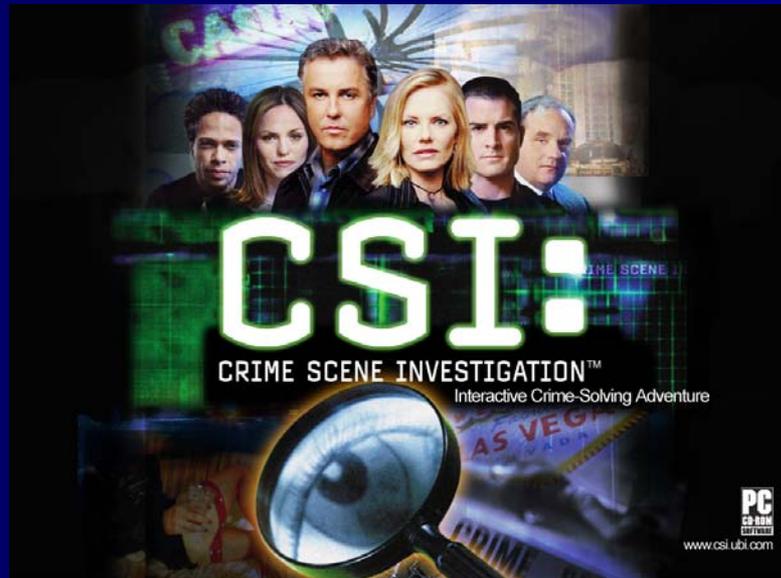
- In 2006, that number increased to 92 investigations involving 14,406 gigabytes of data on 130 computers and 1,224 digital equipment items
- This represents a shift from removable media such as cd-rom and floppy disks to larger capacity hard drives

Lots of ones and zeros!

- The number of examinations completed and the number of computers involved does not account for the complexity of each case
- Seven GB of data equals one 48' tractor trailer completely full of printed documents
- Last year alone, CERU processed the equivalent of more than 2000 tractor trailer loads full of data !



After these messages...



- CSI might be able to crack a case before the next commercial
- Real life takes an average of just over two weeks each and varies due to type of investigation and amount of data to examine
- Backlog is currently about 4-5 months for lower priority cases

Why so long?

- Digital evidence is examined thoroughly and acquired in a forensic manner which takes a very long time
- Must ensure that no data is overwritten or modified, booting Windows XP modifies literally hundreds of files just by "rebooting"
- Care must be taken to preserve the integrity of the data and all physical data is examined, not just the logical files, for the "needle in a haystack"

Preserving the data

- Take pictures, especially if the computer is on and applications are running
- Laptop computers: *remove battery*
- Desktop computers: *pull power plug*
- Servers: *do not shut down*
- Cellular devices: *protect from electronic signals*



Acquiring the data

- Bitwise copy, not a logical file copy
- Logical file copy would miss items in slack, files marked as deleted by operating system
- Bitwise grabs every one and zero
- Maintain a forensic environment to preserve integrity of the evidence
- Verify with MD5 hash calculations

MD5 uniqueness



- MD5 hash calculates a unique number for the media and will change if any one or zero is altered
- MD5 hash has a uniqueness value of 2^{128}
- That's 340 billion billion billion billion
- Many times more accurate than DNA analysis

Warrants

- Traditional item seizure of physical records took only documents mentioned
- Modern seizure of electronic records acquires all data on the storage media then limits the examination to items listed in the search warrant

First Amendment Rights

- “Free speech” claims do not always apply to employees using company resources on company time.
- Computer Use Policies for computer use serve as agreements between employee and employer.
- Serve as contract which carries stated penalties including written warnings and dismissal.

Computer Use Policy

- Employees generally receive upon employment, can be reminded before login with pop-up notice.
- Computer use policy should state clearly that the employer has an implied consent to search.
- Computers, e-mail, data storage all belong to the employer, not the employee.
- What is **your** computer use policy?

Security Policies

- Effective security policies make frequent references to standards and guidelines that exist within an organization.
- Security Policy should be an integral part of the Computer Use Policy.
- Include consequences for violations such as written notice and dismissal.
- Does yours address what can be sent using e-mail attachments to outsiders?

Policy

- Outlines specific requirements or rules.
- "Acceptable Use" policy would cover the rules and regulations for appropriate use of computers, network resources, and data.
- Extremely important for HIPAA and other types of confidential content.

Standard

- System-specific or procedural-specific requirements that must be met by everyone.
- Generally apply to methods or usage rather than rules with consequences.
- How to securely store data on a network server with access permissions.

Guideline

- System-specific or procedural-specific "suggestions" for best practice.
- Not requirements, but are strongly recommended.
- Employee using passwords to access data would be covered by a Policy; how the passwords are used by the computers would be a Standard; using letter, numbers and special characters to create a secure password would be a Guideline.

HIPAA

- HIPAA stands for Health Insurance Portability and Accountability Act.
- Designed to protect confidential healthcare information by using improved security standards and federal privacy laws.
- Defines requirements for storing patient information before, during and after electronic transmission.
- Identifies compliance guidelines for awareness training, creating an audit trail, information access control, and encryption methods.
- <http://www.hhs.gov/ocr/hipaa/>

HIPAA – 3 Safeguards

- **Administrative Safeguards:** Policies and procedures for day-to-day operations; managing the conduct of employees with electronic protected health information (ePHI); and managing the selection, development, and use of security controls.
- **Physical Safeguards:** security measures meant to protect an organization's electronic information systems, as well as related buildings and equipment, from natural hazards, environmental hazards, and unauthorized intrusion.
- **Technical Safeguards:** security measures that specify how to use technology to protect EPHI, particularly controlling access to it.

ePHI

- ePHI stands for Electronic Protected Health Information. It is any protected health information (PHI) which is created, stored, transmitted, or received electronically.
- Protected Health Information (PHI) under HIPAA means any information that identifies an individual.
 - The individual's past, present or future physical or mental health.
 - The provision/type of health care to the individual.
 - The past, present or future payment for health care which includes health insurance information (policy, plan, member information).

ePHI Data

- ePHI includes any device used to store, transmit, or receive PHI electronically.
- Computers with hard drives and network connections.
- Removable storage devices, such as iPods, USB memory sticks, CDs, DVDs, and floppy diskettes
- PDA's, smart phones (patient calendar entries).
- Electronic transmission includes data exchange (e.g., email or file transfer) via wireless, ethernet, modem, DSL or cable network connections.
- Telecommuting employees.

Have you considered?



- “Furby” was banned from CIA, FBI, and the Pentagon because of its voice recording capabilities.
- Removable thumb drives and iPods for personal use in the office that can store data.

Computer Trespass

- Code of Virginia § 18.2-152-4
- A. It shall be unlawful for any person, with malicious intent, to:
 - 1. Temporarily or permanently delete or deny data, programs or software
 - 2. Temporarily or permanently cause a computer to malfunction
 - 3. Alter, disable, or erase any data, programs or software
 - 6. Use a computer or network to make unauthorized copy (printed or electronic form) of computer data, programs or software residing in, communicated by, or produced by a computer or computer network;
- C. Nothing in this section shall be construed to prohibit the monitoring of computer usage of, the otherwise lawful copying of data of, or the denial of computer or Internet access to a minor by a parent or legal guardian of the minor.

Computer invasion of privacy

- Code of Virginia § 18.2-152.5
- A. Uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or identifying information relating to any other person.
- Must be intentional, not accidental.
- Increased penalties if data sent to another person or used in another crime such as fraud.
- F. Does not apply to any person collecting information that is reasonably needed to (i) protect the security of a computer, computer service, or computer business, or to facilitate diagnostics or repair in connection with such computer, computer service, or computer business or (ii) determine whether the computer user is licensed or authorized to use specific computer software or a specific computer service.

Other laws

<http://leg1.state.va.us/000/src.htm>

- § 18.2-152.6. Theft of computer services
- § 18.2-152.5:1. Using a computer to gather identifying information
- § 18.2-152.7:1. Harassment by computer; penalty.
 - If any person, with the intent to coerce, intimidate, or harass any person, shall use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act

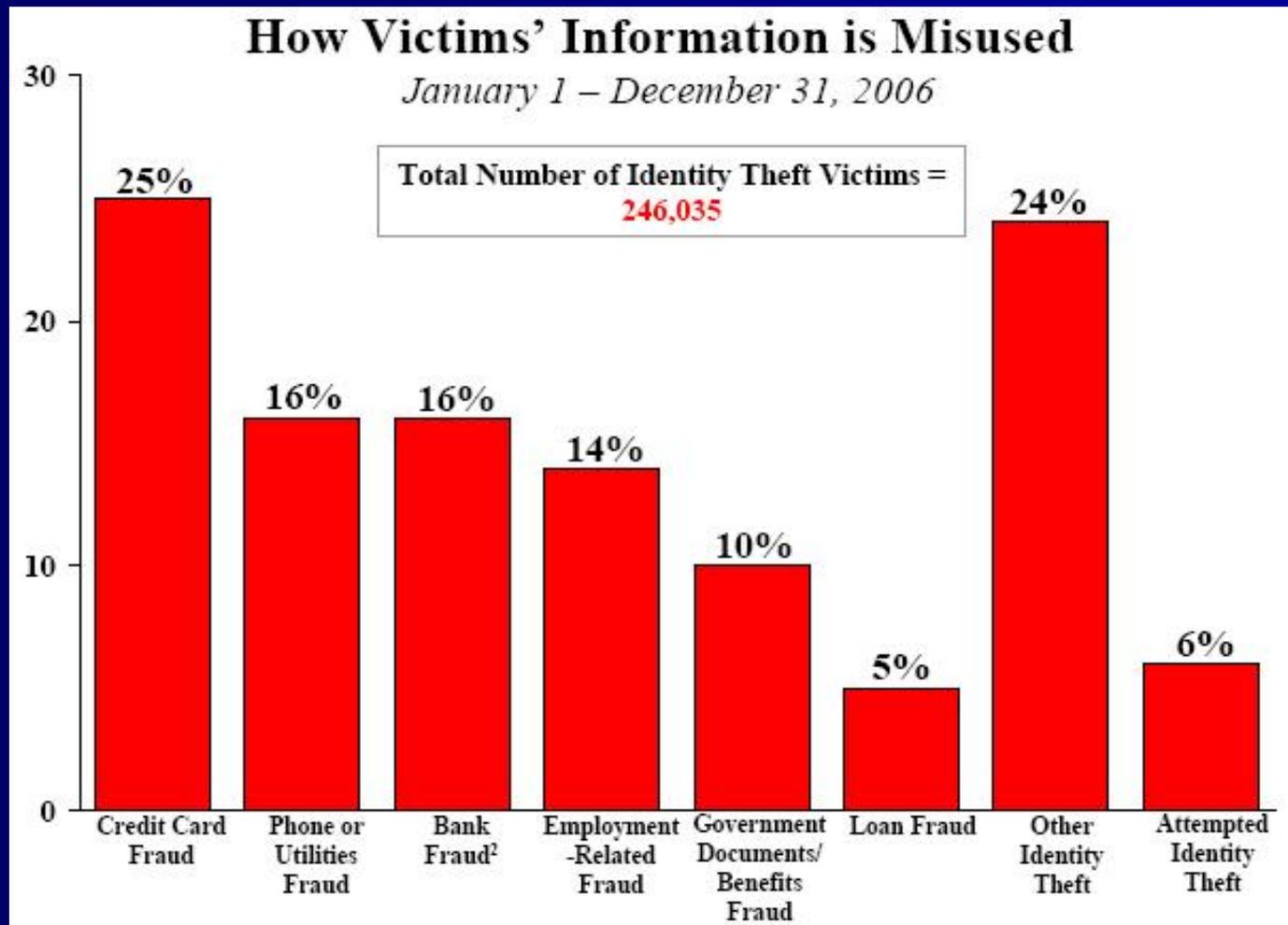
Identity Theft

<http://www.ftc.gov/bcp/edu/microsites/idtheft>

- FTC data for 2006 stated that 62% of victims did not notify the police once they discovered they were the victim of identity theft!
- To protect yourself and your family, it's important to recognize how your identity can be stolen and misused.

Types of Identity Theft

source: Federal Trade Commission, "ID Theft Clearinghouse Data," 2007



Acquiring

- Discarded bank statements and credit card offers provide plenty of data.
- Receipts that contain your signature.
- Fraudulent web sites collect data using bogus login screens, password change requests, or "confirm your information" solicitations. Considered an "intercept" method.

Protecting



- SSL – Secure Socket Layer for web sites, look for the lock symbol and sites that begin with https://
- Beware of e-mail requests and forged e-mail messages.
- Shred your documents, junk credit card offers, and bank statements!
- Talk to your kids about what they should never reveal about themselves and your family online.

Forged e-mail headers

Return-Path: [fake@address.com] Received: from server.mymailhost.com (mail.mymailhost.com [126.43.75.123]) by mail.donutshop.gov (8.10.2/8.10.2) with ESMTP id NAA23597; Fri, 19 Oct 2007 16:11:20 -0400 (EDT)

Received: from aol.com (127-34-56-98.dsl.mybigisp.com [127.34.56.98]) by server.mymailhost.com; Fri, 19 Oct 2007 13:09:38 -0700 (PDT)

Date: Fri, 19 Oct 2007 13:09:38 -0700 (PDT)

From: Hot Summer Deals hot_deals@aol.com

To: cops@mail.donutshop.gov

Subject: Free Donuts!!!

Analyzing the headers

Mail server IP address: 126.43.75.123

- This is the Internet IP address from which Pilot received the message.

Mail server domain name: mail.mymailhost.com

- This is the domain name (DNS name) which matches the above IP address.

Mail server identification: server.mymailhost.com

- Should match between each sequential header.

Originating IP address: 127.34.56.98

- This is the Internet IP address from which the remote mail server received the message.

Originating domain name: 127-34-56-98.dsl.mybigisp.com

- Report to administrator at abuse@mybigisp.com

Common Online Fraud

- Sending a forged check for more than the amount and requesting a refund, your bank will deduct the bounced amount from your account and charge a fee.
- Lottery winner, Nigerian royalty, inheritances, "phishing" for information especially.
- Used car sales ("send me your address, lowest price, and best time to view the vehicle").
- Be cautious of online auctions, particularly ones requesting Western Union. Use eBay escrow accounts for large purchases if possible. Check feedback ratings, confirmed PayPal accounts, and BBB of companies.

Protecting your data

- In the office (3 slides)
- At home (2 slides)
- Online (4 slides)
- Credit card data (1 slide)
- Password protect, strong passwords (1 slide)
- Removable storage devices, usb drives (1 slide)
- Prohibited items in the workplace (furby as recording device, usb drives) (1 slide)
- Maintain confidentiality (HEPA, transferring confidential/classified to home computer) (2 slides)

Strong passwords

- Include punctuation marks (, . ;), special characters (! # \$ % ^) and numbers.
- Mix capital (uppercase), lowercase.
- Create a unique acronym based upon a sentence or phrase, just like in grade school for naming the order of planets; consider a description of a family or pet photo near the computer.
- **MBMAr00!** My Beagle Moxley 'Aroo!'



Telecommuters

- Firewall and e-mail server settings for attachments, file types.
- Policies, Standards, Guidelines for usage and data transmission.
- How do your remote employees protect, log, and comply with laws of HIPAA, ePHI, confidential data?
- Physical security access to the computer in addition to VPN encryption to the network?

Online Pornography Stats

source: Family Safe Media, "Pornography Statistics," 2007

- 12% of all web sites are porn sites
- 25% of all search engine requests
- 35% of all Internet downloads
- 20% of men surveyed admit to accessing it at work
- 72% male, 28% female; porn site visitors
- 89% of all chat room sex solicitations are towards minors
- 90% of 8-16 year olds report having viewed pornography online -- mostly from online ads, pop-ups, and masked or redirected sites -- while trying to do valid homework

Video messaging

source: CampusKiss.com, "CampusKiss and Tell University and College Sex Survey," Feb 2006.

- 87% of university students polled have virtual sex mainly using Instant Messenger, webcam, and telephone.
- AOL, Yahoo, MSN all have the ability to use video conferencing using webcam.
- Transmitting digital pictures with file sharing, e-mail, and instant messenger
- Saved and rebroadcast online or uploaded to other sites without the person's consent.
- Revengeful ex-boyfriends and ex-girlfriends.
- Video capabilities of smart phones can capture, upload and send instantly.

What you can do about it

- Filters at home and in the workplace.
- Log terminal and site to identify users, monitor large amounts of web traffic during and after regular business hours.
- Do NOT download the data and present it to law enforcement (distribution). Logs are just fine!
- Talk to your kids about the dangers, predators, what kinds of data they can disclose online, and keep an honest communication line open with them so they do not fear “getting in trouble”.
- 7-17 year olds will freely give out (29%) home address and (14%) e-mail address online.

Thank You!

Mr. Richard Seweryniak
Digital Forensic Examiner

(804) 674-2593

richard.seweryniak@vsp.virginia.gov

Bureau of Criminal Investigation
Criminal Intelligence Division
Computer Evidence Recovery Unit

State Police Headquarters
7700 Midlothian Turnpike
Richmond VA, 23235



Disposition Process

October 23, 2007

Michael VonSlomski



NORTHROP GRUMMAN

Agenda

- CRVA
- CRVA Clients
- Disposition Process
- High Level Disposition Flow Chart
- Department of General Services Refreshed Surplus
- Sample Forms

CRVA

- Founded in February 2001, the mission of Computer Recycling of Virginia, Inc. (CRVA) is to place educationally-useful equipment into Virginia's schools and non-profit organizations free of charge, while promoting electronics recycling throughout the Commonwealth of Virginia.
- We accept all computer related equipment and most any electronic device. Computers, laptops, networking, and telephone equipment, even cables and mice, are a few of the items that we process daily. All acquired components are reused or recycled in accordance with all Federal, State, and Local regulations. None of the equipment we process is sent to the landfill!
- Reuse, refurbishment, and recycling has enabled CRVA to donate over 12,000 pieces of equipment to Virginia schools, non-profits, and youth programs. Over 4,000 tons of e-Waste has been diverted from Virginia's landfills helping our children, and protecting the environment
- In 2006, CRVA donated 4,199 pieces of electronic equipment to schools, non-profits, and local government organizations. CRVA's ability to continue to donate this much needed equipment is directly related to the donations of equipment that CRVA receives from businesses and individuals for recycling. Help CRVA reach our goal of 6,000 pieces of electronic equipment donated during 2007 by donating your electronic equipment to CRVA today.

CRVA Clients

- Computer Recycling of Virginia has been serving a range of clients over the past several years.

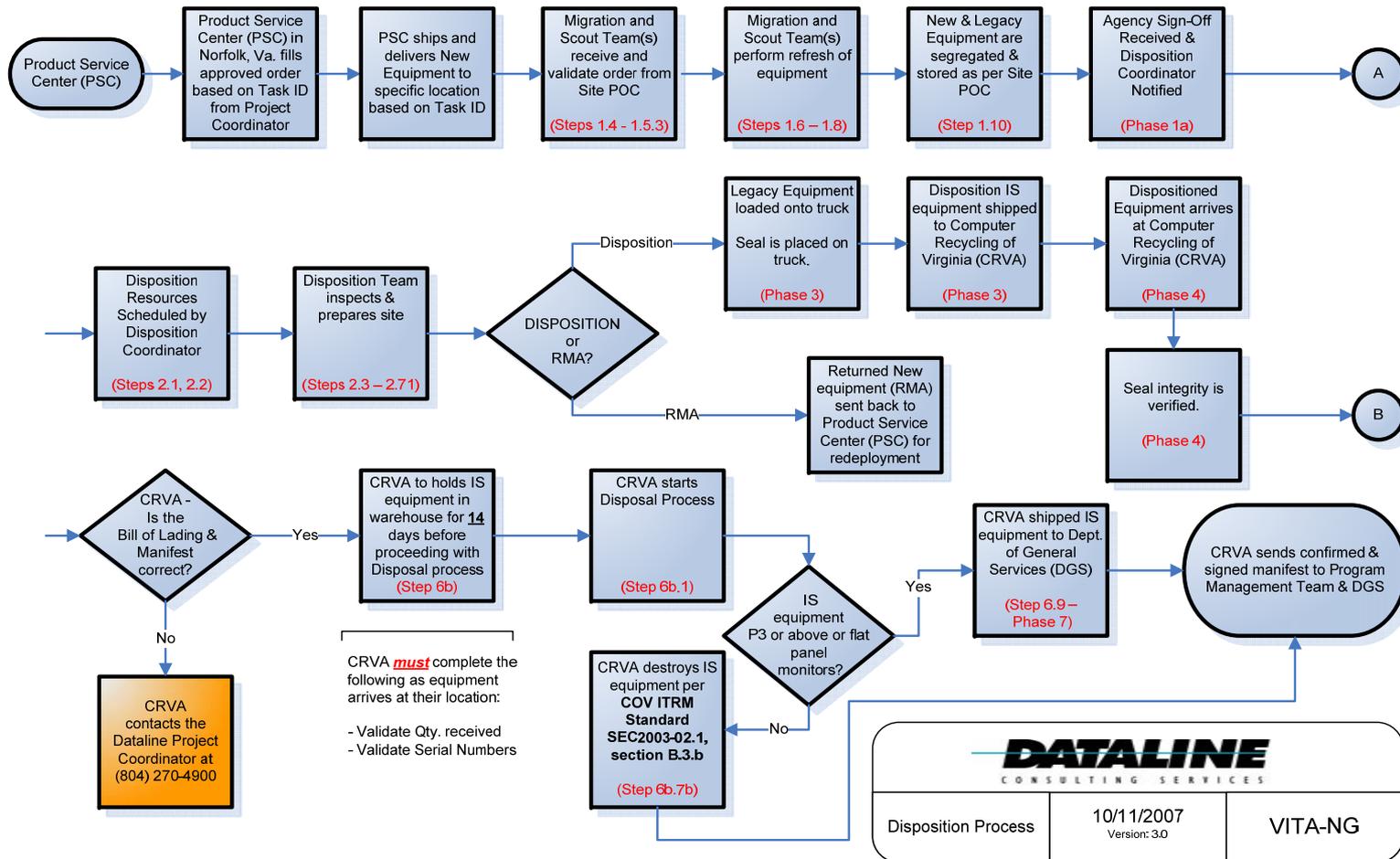




Disposition Processes

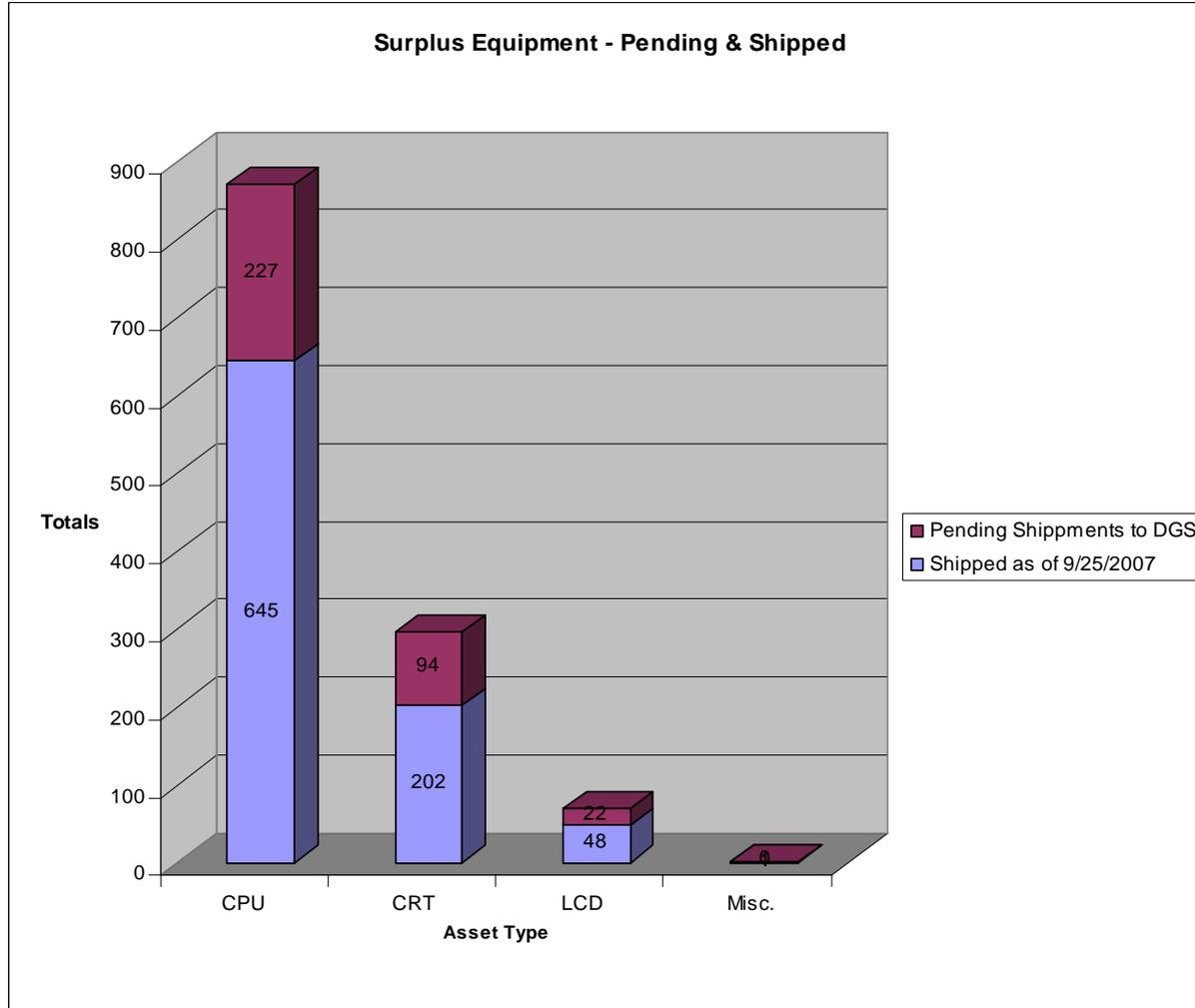
- Dataline Consulting Services and Computer Recycling of Virginia have implemented Disposition operating processes and procedures that align with the current Statement of Work and within the guidelines of the Commonwealth of Virginia (COV) to prevent unauthorized use or misuse of COV data. These policies and procedures are described in the following sections.
- High Level Disposition
 - Dataline Consulting Services and CRVA have developed and implemented the High-Level Disposition Process to show the flow through the Product Service Center (PSC) to CRVA. Once the asst is received at CRVA, we begin the Disposal procedures per COV ITRM SEC2003-02.1 prior to shipment to Department of General Services (DGS). See Appendix 1 for details.
- Asset Tracking and Logging through Disposal
 - Computer Recycling of Virginia has established procedures that track and log COV assets throughout the Disposal life-cycle. This is to include logging DOA assets, Destroyed & Wiped Assets, and assets shipped to Department of General Services (DGS). See Appendix 2 for sample forms and reports. Additionally, refer to “Dead on Arrival (DOA) Procedure-VITA equipment received by CRVA,” DCS-CRVA-0004.
- CRVA Facility Security
 - Computer Recycling of Virginia has agreements in place with Dataline to safeguard facilities and ensure COV equipment therein from unauthorized physical access, tampering, and theft. Computer Recycling of Virginia ensures all COV data and computers are kept in secure, private locations within buildings that are secure from unauthorized access.
- Chain-of-Custody
 - Computer Recycling of Virginia has implemented the policies and procedures to ensure integrity and document Chain of custody once COV assets are received at their facility and then delivery to DGS.

High Level Disposition Flow Chart



DATALINE CONSULTING SERVICES		
Disposition Process	10/11/2007 Version: 3.0	VITA-NG

Department of General Services Refreshed Surplus



Hardware Equipment Destroy Record

DATALINE CONSULTING SERVICES	
Hardware Equipment Destroy Record	Document # DCS-CRVA-0003
	Revision Date 2007/10/10
	Version v1.0
	Pages 1 of 3

Hardware Equipment Destroy Record			
Name	CRVA Hardware Equipment Destroy Record		
Description	Details itemized hardware assets		
Purpose	This document provides a list of "Destroyed" hardware assets		
Document Owner	Michael Howell	Owner Org	DCS

VERSION HISTORY				
Version	Date	Author	Template	Change Summary
1.0	2007/08/08	Michael Howell	DCS-CRVA-0003	New release
	2007/10/10	Heidi Schlicher	DCS-CRVA-003	Added additional destroyed assets

Site ID	VITA Shipment	Serial #	HDD Serial #	Reason DOA	Date Destroyed	Technician
1320	Vita 10	6030DHS3A136	3HT3W1HF	Boot Failure	9/28/2007	WTT
1350	Vita 10	6004DHS3K289	B1FAXKEEZ9999	Boot Failure	9/28/2007	WTT
1330	Vita 10	6029DHS3B303	3HT2W7ZZ	Boot Failure	9/28/2007	WTT
DMV	Vita 7	8WDRW01	5FB6NA81	Boot Failure	9/26/2007	WTT

Signed Agency Disposition Record

Hardware Disposition Manifest	Document #	VITA - XXX - 000#	Pages	9 of 11
	Revision Date	2007/09/10	Version	V1.4

ONLY THE ONLINE SYSTEM HAS THE CURRENT VERSION. VERIFY COPY AGAINST THE ONLINE SYSTEM BEFORE USE.

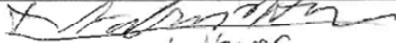
6600 - Staunton - VA School for the deaf and Blind						
#	User First Name	User Last Name	Asset Type	Comments	Serial Tag #	Asset Tag #
196			Monitor		H3MF600047 ✓	100121362 ✓
197			Monitor		H3MG600205 ✓	100121364 ✓
198			Monitor		2742PE80SC59 ✓	100121369 ✓
199			Monitor		2742PE80M458 ✓	100121371 ✓
200			Monitor		2742PE80MK59 ✓	100121375 ✓
201			Monitor		2742PE82N259 ✓	100121381 ✓
202			Monitor		MX08R3394760535SANAQ ✓	100121388 ✓
203			Monitor		ACR83247269 ✓	100121394 ✓
204			Monitor		MX08R3394760535SASHV ✓	100121404 ✓
205			Monitor		2742PEFSV779 ✓	100121410 ✓
206			Monitor		MX08R3394760535SAS29 ✓	100121419 ✓
207			Monitor		MX08R3394760535SAS23 ✓	100121422 ✓
208			Monitor		MX08R3394760535SASHS ✓	100121423 ✓
209			Monitor		MX08R3394760535SAS2A ✓	100121425 ✓
210			Monitor		MX08R3394760535SAS21 ✓	100121427 ✓
211			Monitor		MX08R3394760535SAS1G ✓	100121430 ✓
212			Monitor		MX08R3394760535SAS28 ✓	100121432 ✓
213			Monitor		MX08R3394760535SAS1Z ✓	100121434 ✓
214			Monitor		MX08R3394760535SAS27 ✓	100121436 ✓
215			Monitor		MX08R3394760535SAS2B ✓	100121437 ✓
216			Monitor		MX08R3394760535SASHT ✓	100121438 ✓
217			Monitor		MX08R3394760535SAS2C ✓	100121442 ✓
218			Monitor		2742PE830B59 ✓	100121468 ✓
219			Monitor		2742PE80M259 ✓	100121470 ✓
220			Monitor		2742PE80SY59 ✓	100121472 ✓
221			Monitor	DESKTOP	12899932 ✓	100121473 ✓
222			Monitor		2742PE80XX59 ✓	100121474 ✓
223			Monitor		2742PE82N559 ✓	100121482 ✓

AGENCY RELEASE - SIGNATURE <i>Janice A Rankin</i>	AGENCY RELEASE - PRINTED Janice A Rankin	DATE 10/5/07
DISPOSITION CARRIER - SIGNATURE <i>BJ Coleman</i>	DISPOSITION CARRIER - PRINTED BJ Coleman	DATE 10.5.07
CRVA RECEIPT CONFIRMATION - SIGNATURE	CRVA RECEIPT CONFIRMATION - PRINTED	DATE



NORTHROP GRUMMAN

Truck Seal Tracking

				
Hardware Disposition Manifest	Document #	VITA - XXX - 000#	Pages	11 of 11
	Revision Date	2007/09/10	Version	V1.4
<small>ONLY THE ONLINE SYSTEM HAS THE CURRENT VERSION. VERIFY COPY AGAINST THE ONLINE SYSTEM BEFORE USE.</small>				
Manifest Summary				
Equipment Type	Quantity	# of Boxes	# Of Pallets	
Desktop PCs	141			
Laptop / Tablet PCs	4			
Monitors	By 9591			
Keyboards	By	2		
Mice				
Docking Stations				
Other (1):				
Other (2):				
Other (3):				
Other (4):				
Addendum:				
Seal # 157104 ✓  Gabriel Hoover Wm 7 Wk.				
AGENCY RELEASE - SIGNATURE		AGENCY RELEASE - PRINTED		DATE
		Janice A Rankin		10/5/07
DISPOSITION CARRIER - SIGNATURE		DISPOSITION CARRIER - PRINTED		DATE
				10/5/07



Surplus Electronics Management by Commonwealth of Virginia Agencies

ISOAG meeting
October 23, 2007

Presentation by
Bradley Crawford
Virginia Department of General Services



Surplus Property - Electronics

- Regulation
- Re-utilization
- Recycle



Surplus Property - Electronics

There are several references in § 2.2-1124 specific to electronics

- *2.2-1124 B 10*
- *2.2-1124 B 12*
- *2.2-1124 B 15*



Surplus Property – Electronics

- Re-utilization
 - Make computers/electronics available to Agencies, political subdivisions, qualified non-profits prior to public sale
 - Donations to public schools and specified non-profits
 - Public sales through fixed price sales, live auctions and internet auctions



Surplus Property – Electronics

- Current Marketable Standard
 - Pentium 3&4 computers
 - Black Dell 17" or larger monitors
- Recycle electronics
 - Pentium 2 or older computers
 - Monitors other than stated above
 - Peripherals such as old printers, non working TV's, etc.



Surplus Property - Electronics

- Recycle
 - Dyntek contract provides service to Agencies, political subdivisions to destroy/recycle non-marketable property
 - Commonwealth IT partnership contract provides for destruction/recycle of non-marketable electronics
 - Surplus Property is working with 501(C)3 non-profits such as Goodwill Industries to develop network providing destruction/recycle of non-marketable electronics

Making Information Security an Executive Management Priority

Commonwealth Information Security
Council Committee

John Karabaic, DMAS, Co-Chair

Shirley Payne, UVA, Co-Chair

Need Your Experience!

- Examples of Executive Information Security Awareness Practices
- Information Security Awareness Presentations designed for executives

Contacts

Please send to:

John.Karabaic@DMAS.Virginia.Gov

Or Shirley Payne at scp8b@virginia.ed



IT Security Audits

Cathie Brown, CISM, CISSP
Deputy Chief Information Security Officer



Agenda

- IT Security Audit Guideline Requirements
- What and when to report to VITA
- What not to report to VITA
- Where to Get Help



IT Security Audit Standard (ITRM SEC502-00)

- IT Security Audit SENSITIVE SYSTEMS ONLY
 - An independent review and examination of an IT system's policies, records and activities
- IT Security Auditors
 - CISO personnel, Agency Internal Auditors, the Auditor of Public Accounts, or staff of a private firm that, in the judgment of the Agency, has the experience and expertise required to perform IT Security Audits
- Each Agency shall establish an IT Security Audit Program



IT Security Audit Program

- Develop IT security audit plan annually
- At a minimum, scope must assess effectiveness of the system controls and measures compliance with IT Security Policy (ITRM SEC500-02) and Standard (ITRM SEC501-01)
- Audit work papers must be maintained as documentation of the audit to support conclusions



IT Security Audit Reports

- IT Security Auditor documents the findings of the IT Security Audit
- A draft of the report is presented to the Agency Head or designee
- Agency Head or designee shall be given no less than 10 days to prepare a Corrective Action Plan (CAP)
- The CAP includes concurrence or non-concurrence with each finding

IT Security Audit Reports (con't)

- For each finding with which the Agency concurs, the CAP will include:
 - Planned corrective action
 - Due date for the corrective action
 - Party responsible for the corrective action
- For each finding with which the Agency does not concur, the CAP will include:
 - Agency's statement of position
 - Mitigating controls that are in place
 - Agency's acknowledgment of acceptance of risk



Report to VITA

- IT Security Audit Plan (Initial 2/01/07; annually)
- Each quarter report all IT Security Audits conducted by or on behalf of the Agency **during that quarter**
 - Include all findings and whether the Agency concurs or not
 - For each finding with which the Agency concurs
 - Corrective action planned
 - Due date for the corrective action
 - Responsible party
 - For each finding with which the Agency does not concur
 - Agency's statement of position
 - Mitigating controls that are in place
 - Agency's acknowledgement of acceptance of risk
- Status of outstanding corrective actions for IT Security Audits previously



Do Not Report to VITA

- Letters or notes indicating there is no IT Security Audit information to report
- Audit Workpapers
- Sensitive Information over E-Mail – contact Ed Miller or Benny Ambler
Edward.Miller@VITA.Virginia.Gov

Benny.Ambler@VITA.Virginia.Gov



Where to get help

- Another agency within your Secretariat with internal audit staff
- Small Agency Outreach Committee may provide guidance
- VITA SMSA (Supplier Managed Staff Augmentation) facilitated by CAI (Computer Aid, Inc.)



IT Security Audit Plan Template

IT Security Audit Plan

Agency Name and Acronym	IT Security Audit Plan				
	Date Submitted	Submitted By			
		Name & Title	Phone Number	E-mail Address	
IT System Name, Acronym, and Designation	Expected Auditor	Next Three Planned Audit Dates Fiscal Years			Areas for Special Emphasis and Additional Audit Requirements
		2008	2009	2010	



Corrective Action Plan - Template

IT Security Audit Quarterly Summary

Audit Name: _____

Audit Finding No. & Agency Concurrence	Short Title	Summary	Risk	Responsible Person(s) and Due Date	Status*	Status Date	Concurs: Planned Action & Status Does Not Concur: Mitigating Controls & Risk Acceptance

* Status Legend: NS = Not Started; U = Underway; C = Completed



Coming Soon.....

- IT Security Audit Guideline



Virginia Information Technologies Agency

Citizen's Awareness Banner For Customer Applications

Tripp Sims

Commonwealth of Virginia Security Architect

ISOAG

October, 2007

Questions & Comments: tripp.sims@vita.virginia.gov



Citizen's Awareness Banner

Due to the ever increasing threats posed by malware running on citizen computers, it is suggested agencies utilize the "Citizen's Awareness Banner" on all Internet facing citizen and partner applications where authentication is required, or where any personally identifiable information may be exchanged between the agency and your customers.



Citizen's Awareness Banner

The Official Web Site of the

Commonwealth of Virginia

Login:

Password:

The security of your personal information is important to us!

Diligent efforts are made to ensure the security of Commonwealth of Virginia systems. Before you use this Web site to conduct business with the Commonwealth, please ensure your personal computer is not infected with malicious code that collects your personal information. This code is referred to as a [keylogger](#). The way to protect against this is to maintain current [Anti-Virus](#) and [security patches](#).

For more information on protecting your personal information online, refer to [Guide to Online Protection](#).

<http://www.vita.virginia.gov/security/default.aspx?id=5146>



Citizen's Awareness Banner

Guide to Online Protection - Protect Your Personal Information

- [Protect Your Personal Information](#)
- [Keeping Your Computer Healthy](#)
- [Protecting Against Malware](#)

Protect Your Personal Information

Because you can control the information you choose to release, there are some easy ways to do this like keeping a record of providing your information only to trusted sources.

Always be skeptical when providing your personal information or when someone requests your information by calling the parent or guardian. Understand why a certain piece of information is needed, do not

Understand Online Risks

E-mail and fraudulent Web sites

A criminal may send you an e-mail that looks like it has come from a legitimate source. E-mails ask you to go to a Web site that also looks legitimate. Legitimate e-mails even caution that if you don't do this, your accounts may be compromised and is a fraud attempt.

'Guide to Online Protection' includes:

- Glossary of terminologies
- Links to Anti-Virus, Anti-Spyware, and Firewall guides
- Secure computing practices
- And more...

Guide is easily maintained and will continue to be developed with more content as the security landscape changes and new threats and defenses come to light.

<http://www.vita.virginia.gov/security/default.aspx?id=5270>



Questions and Answers

Questions?



Storm Worm Trojan A Brief Analysis

Tripp Sims

Commonwealth of Virginia Security Architect

Questions & Comments: tripp.sims@vita.virginia.gov

The many faces of "Storm"

Storm Worm



QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.

aka

Tibs : Peacomm : Zhelatin : NuWar

Today's version still shares code similarities with variants as old as July 2006



Storm's Success

Reasons for Storm Success:

- Peer to Peer Command and Control
- Double Fast Flux DNS
- Intelligent 'Social Engineering' Spreading
- Research Trumps Removal
- Relatively Benign Payload (Until recently)



Storm's Success

- Peer to peer command and control leaves us with no central point to disrupt botnet control.
- Infection of machine usually didn't require you download the .exe if your browser or ancillary browser software was vulnerable.
- Storm has been known to reactively DDoS security firms and researchers who probe the network too aggressively.
- As many as 15 million infections since January. Estimates stand at around 20,000 available computers at any one time today significantly smaller than it once was.



Storm Side Effects

- Zombies which were used as fast-flux name servers for the the Storm network were were observed acting recursively.
- Turf wars for hijacked computers began between the WarezoF and Storm botnet groups.
- Due to the defensive reactions of the botnet it was surmised that third parties could drop victim networks by passing requests to the Storm network trough one exploited host - thus eliciting a strong enough DDoS to take the whole network down.



Recent Developments

- Storm continues to spread itself by sending emails of links to its own hosting infrastructure. Recent attempts to seduce users into clicking the malicious links have been 'Free NFL Tracker', 'Psycho Kitty', and 'Krackin File Sharing'.
- Most recent wave seen installing what appears to be a third party proxy and spam kit from Russian Business Network servers.
- Began segmentation of botnet into smaller pieces. Typically this behavior is indicative of resale preparation.



Effects on the Commonwealth

- Machines on the Commonwealth infrastructure have been implicated in two DDoS attacks due to Storm infections on computers therein.
- Most .pdf and more recently .mp3 spam directed Commonwealth mailboxes have been Storm related - this is outside of its own self-propagation spam.
- Due to the fact that portions of the network are likely now up for sale it is probable that payloads will shift from mostly benign to more malicious key logging payloads. Just in time for the holidays.



Defenses Have Not Changed

- Most spam filters will properly categorize Storm propagation as spam.
- Clicking links in Storm spam has the potential to infect the machine just from viewing the webpage via a browser exploit suite.
- Default deny outbound firewall policies will minimize the ability of Storm to further propagate or spam others should a user not have adequate protection at the desktop and fail to follow best practices



Recursive DNS Sidebar

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

“Snapshot in time” from data collected between August and September

*False positives do exist in the dataset



Recursive DNS Sidebar

- Allowing your DNS to operate recursively makes you more susceptible to cache poisoning by default.
- Allowing your DNS to operate recursively leaves the server open to being used in a DNS amplification attack. Wherein your server(s) are used to attack someone else's infrastructure.
- A cable connection with a 512 Kilobit line could use a DNS amplification attack to increase their DoS potential from 512 Kilobits to a 50 Megabits.



Questions and Answers

Questions?



Date Breach Notification

Peggy Ward





COV ITRM Standard SEC501-01 Section 9.5.2

#'s 3-6

What?

Early adoption of 9.5.2 Data Breach Notification, #'s 3-6 which was approved by the ITIB July 2007 with an original compliance date of July, 2008.

Why?

Borne of participation in the Governor's Working Group for Executive Directive No. 5 "Consumer Privacy" – Requested by Delegate Plum to pave the way for comprehensive data breach legislation in Virginia by leading the way!

When?

Recommending that the Information Technology Investment Board approve a compliance date effective November 1, 2007



COV ITRM Standard SEC501-01 Section 9.5.2 #'s 3-6

Applies to: Personally Identifiable Information (PII) which means Name and any of the following:

- Social Security Number
- Drivers license or Identification card number
- Financial account number, credit or debit card number
- Other personal identifying information, such as insurance data or date of birth.



COV ITRM Standard SEC501-01 Section 9.5.2 #'s 3-6

9.5.2 Data Breach Notification

3. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted PII by any mechanism, including, but not limited to:
 - a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
 - b. Theft or loss of physical hardcopy; or
 - c. Security compromise of any system.

The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #6, below.

4. Provide notification that consists of:
 - a. A general description of what occurred and when;
 - b. The type of PII that was involved;
 - c. What actions have been taken to protect the individual's personal information from further unauthorized disclosure;
 - d. What, if anything, the agency will do to assist affected individuals, including contact information for more information and assistance; and
 - e. What actions the agency recommends that the individual take.



COV ITRM Standard SEC501-01 Section 9.5.2 #'s 3-6

5. Provide this notification by one or more of the following methodologies, listed in order of preference:
 - a. Standard mailing to any affected individuals whose mailing addresses are available.
 - b. Electronic mail to any affected individuals whose email address has been provided to the agency as a contact mechanism.
 - c. In the case of large scale breaches or data breaches where neither form of communication listed above is available or feasible, public communications channels, including:
 - d. Conspicuous notification on the agency website; and
 - e. Notification by statewide public media, including newspaper, radio, and television).

6. Not provide notification immediately following verification of unauthorized data disclosure only if requested by:
 - a. Law Enforcement entities where it would interfere with an ongoing investigation; or
 - b. CISO or designee where it would interfere with a determination of the scope of the data breach or investigation of root cause.



ITIB Motion to Require Earlier Compliance with the Data Breach Notification Requirements

Passed October 18, 2007!

I move that the current compliance date of July, 2008 for the data breach notification requirements as contained in COV ITRM Security Policy, Sec 500-02, Section 3.1.8 and COV ITRM Security Standard SEC 501-01, Section 9.5.2, items #3 - #6 be revised to require compliance not later than November 1, 2007.



Date Breach Notification

??

??Questions??

??



UPCOMING EVENTS!

Wednesday November 14, 2007 1:00- 4:00 ISOAG meeting

Monday November 19, 12- 2:00 p.m. ISO Council Meeting with committee meetings from 2:00 – 3:00

Monday, November 26, 10:00 a.m – 12 ISO Orientation



Any Other Business ?





ADJOURN

**THANK YOU FOR ATTENDING
HAVE A WONDERFUL DAY!**

