



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

October 6, 2009

October





ISOAG October 2009 Agenda

- | | | |
|-------|--|------------------------------------|
| I. | Welcome & Opening Remarks | John Green, VITA |
| II. | Overview of COOP Planning | Chris Miller, VDEM |
| III. | Recognizing National Cyber Security Awareness Month - A Locality Perspective | Sandra Graham, Chesterfield County |
| IV. | Information Security Awareness Month | Nakita Albritton, VITA |
| V. | IronPort Review | Demetrias Rodgers, NG |
| VI. | Encryption Mechanics & Key Management | Bob Baskette, VITA |
| VII. | Data Points | Benny Ambler, VITA |
| VIII. | Upcoming Events and Other Business | John Green, VITA |

COOP?



Overview of COOP Planning

Chris Miller, Virginia Department of Emergency Management

Different types of emergency plans

- Evacuation = run from fire
- Response = put out fire
- Recovery = call LVA – preserve wet or burned documents
- COOP – keep manufacturing widgets
- ITDR – system/equip recovery procedures – should be coordinated with the widget priorities.

Does your organization have a COOP plan?



What should a COOP plan include?

- What does the organization do?
- Who does it?
- Who else does it?
- What do they need to do it?
- How and where do they do it if...
 - No building, No IT, No staff?

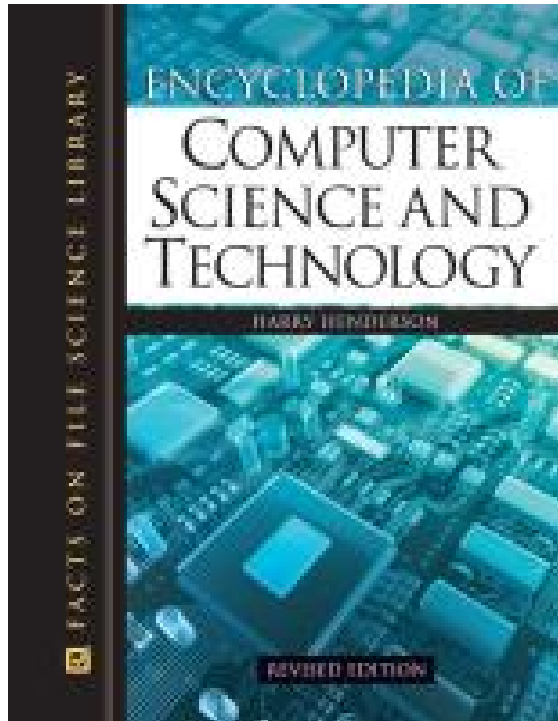
What about H1N1?



TELEWORKING?



LINKING ITDR TO COOP



Are YOU in your COOP plan?

Find out!



Recognizing National Cyber Security Awareness Month



A Locality Perspective

Agenda

- ▶ A Month of Activities
- ▶ Branding
- ▶ Partnerships (Libraries, Schools, Local CATV)
- ▶ Press Releases & Web Announcements
- ▶ Newsletters
- ▶ Cable TV PSA's
- ▶ Cyber Fair
- ▶ Cyber Forum
- ▶ Cyber Seminars
- ▶ BOS Cyber Month Resolution
- ▶ Cyber Awareness Community Outreach
- ▶ Webcasts (MS-ISAC & Internally Recorded Podcasts)

Press Release & Web Announcements

The screenshot shows a Microsoft Internet Explorer browser window displaying the Chesterfield County, VA website. The browser's address bar is empty, and the page title is "County of Chesterfield, VA | Cyber Security Awareness Month - Cyber Security - Microsoft Internet Explorer". The website header includes the county name and logo, a navigation menu with links like "Home", "Government", and "Online Services", and a search bar. The main content area features a "Cyber Security" section with a banner for "OCTOBER IS NATIONAL CYBER SECURITY AWARENESS MONTH" and "OUR SHARED RESPONSIBILITY". Below the banner, a heading reads "Chesterfield County Cyber Security Awareness Month Community Outreach Planned". The text below the heading states: "In recognition of National Cyber Security Awareness Month during October, Chesterfield County is offering a new community outreach program called the Cyber Security Awareness Road Show to promote cyber-security education and awareness for computer users. This program is an extension of the National". To the left of the main content is a "At a Glance" sidebar with a list of links including "Calendar of Events", "Careers", "Chesterfield Businesses", "Chesterfield Schools", "Community Safety", "Department Forms Index", "Family Resources", "Government Information", "Site Help", "Tourism and Leisure", and "Guide to Services". To the right is a "RELATED CONTENT" section with links to "A Memorandum From Your Teen", "About Youth Planning and Development", and "Adolescent Development". The browser's status bar at the bottom shows the URL "http://www.chesterfield.gov/Content2.aspx?id=11594" and "Local intranet".

County of Chesterfield, VA | Cyber Security Awareness Month - Cyber Security - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Print Mail Internet Options

Address Go Links

Google Search + - Bookmarks Check Sign In Convert Select

Today | Departments | Jobs | Login | Contact | Help | Schools | Libraries | CCTV

CHESTERFIELD COUNTY, VA
Chesterfield.gov

Home Government Online Services Community Business Visitors How do I ...

site TOOLS

Cyber Security

At a Glance

- Calendar of Events
- Careers
- Chesterfield Businesses
- Chesterfield Schools
- Community Safety
- Department Forms Index
- Family Resources
- Government Information
- Site Help
- Tourism and Leisure
- Guide to Services

Cyber Security Awareness Month

OCTOBER IS NATIONAL CYBER SECURITY AWARENESS MONTH

OUR SHARED RESPONSIBILITY

Chesterfield County Cyber Security Awareness Month Community Outreach Planned

In recognition of National Cyber Security Awareness Month during October, Chesterfield County is offering a new community outreach program called the Cyber Security Awareness Road Show to promote cyber-security education and awareness for computer users. This program is an extension of the National

RELATED CONTENT

- A Memorandum From Your Teen
A MEMORANDUM FROM YOUR TEEN Re: Me 1. Dont spoil me. I know quite well that I ought not have all I ...
- About Youth Planning and Development
Serves the citizens of Chesterfield County by working to develop and improve the community assets ...
- Adolescent Development
Adolescents and Development

http://www.chesterfield.gov/Content2.aspx?id=11594 Local intranet

Newsletters

▶ Internal Newsletters

The screenshot shows a Microsoft Internet Explorer browser window displaying the CountyNET website. The browser's address bar is empty, and the page title is "CountyNet | Cyber Security Information - Microsoft Internet Explorer". The website header features the CountyNET logo and the tagline "Providing a FIRST CHOICE community through excellence in public service". A navigation menu on the left includes links for Employee Resources, Departments, Forms, and Policies and Procedures. The main content area is titled "Cyber Security Information" and features a graphic of two hands holding a Wi-Fi symbol. Below this, there is a section for "CYBER SECURITY AWARENESS" with the sub-heading "Community outreach planned for Cyber Security Awareness Month". The text in this section mentions National Cyber Security Awareness Month during October and provides a link to the National Cyber Security Alliance (NCSA) website.

CountyNET | Cyber Security Information - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Recycle Bin Mail Print Word Excel PowerPoint Outlook

Address | Go Links >>

Google Search + - Bookmarks ABC Check >> Sign In Convert Select

CountyNET Providing a FIRST CHOICE community through excellence in public service login

- Employee Resources
- Departments
- Forms
- Policies and Procedures

Search CountyNet Go

Cyber Lane Home

- Cyber Security Awareness Training
- Add-Change-Delete-Users
- Awareness Newsletters
- Awareness Brochures and Pamphlets
- Awareness Handbook
- Awareness Print-Ready Posters
- Awareness Tips
- FAQs (Frequently Asked Questions)
- Guidelines and Best Practices
- National Cyber Security Awareness Month
- IST Information Security Liaison User Group

Home | In/OutBoard | Phone Directory | Chesterfield.gov | Help

Home > Cyber Home A+ A- [Print] [Email]

CYBER SECURITY AWARENESS

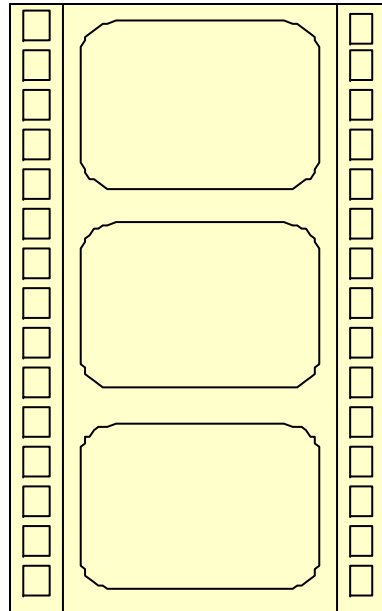
Community outreach planned for Cyber Security Awareness Month

In recognition of National Cyber Security Awareness Month during October, Chesterfield County is offering a new community outreach program to promote cyber-security education and awareness for computer users. This program is an extension of the National Cyber Security Alliance, or NCSA [http://www.staysafeonline.info].

Done Local intranet

Cable TV PSA's

- ▶ Film a Publics Services Announcement about your event!



Cyber Fair

OCTOBER IS NATIONAL CYBER SECURITY AWARENESS MONTH

FRIDAY, OCT. 23 ~ 10 A.M.-2 P.M.

PUBLIC SAFETY TRAINING CENTER ~ CLASSROOMS A-D

LEARN ABOUT:

- *WHAT SAFETY STEPS TO TAKE TO SAFEGUARD YOUR COMPUTER FROM ONLINE THREATS*
- *HOW TO RESPOND TO CYBER-CRIME INCIDENTS* • *PLUS OTHER TIMELY CYBER-SAFETY ISSUES*

AT NOON:



“HOW CAN YOU PROTECT YOUR CHILDREN, WORKPLACE AND COMMUNITY FROM ONLINE RISKS AND PREDATORS?”
Featured Speaker Dr. Peter Fonash *Fonash is the chief technology officer and acting director for the Department of Homeland Security's National Cyber Security Division.*

“WHAT COULD GET YOU LOCKED UP IN A CYBER SECURITY WORLD”
Duncan Minton, Chesterfield County's Juvenile and Domestic Relations Court

BRING YOUR OWN BROWN-BAG LUNCH.

FRUIT AND JUICES WILL BE PROVIDED.

VISIT VENDOR BOOTHS 10 A.M.-2 P.M.

**GIVEAWAYS! REGISTER FOR A GRAND PRIZE DRAWING
— A MINI-LAPTOP!**

**HOSTED BY CHESTERFIELD COUNTY'S DEPARTMENT OF INFORMATION
SYSTEMS TECHNOLOGY AND OFFICE OF SECURITY MANAGEMENT**



**OUR SHARED
RESPONSIBILITY**



Cyber Forum & College/Career Fair



Dr. Gurpreet Dhillon is Professor of Information Systems in the School of Business, Virginia Commonwealth University, Richmond



Barry Condrey, Chief Information Officer (CIO), Chesterfield County



Jerry L. Davis is the Deputy Chief Information Officer (DCIO), IT Security for the National Aeronautics and Space Administration (NASA).



Alex Robertson, Chesterfield County Public Schools - Technical Center Cisco Student Alumni

OCTOBER IS NATIONAL CYBER SECURITY AWARENESS MONTH

COMMUNITY FORUM & COLLEGE JOB FAIR

WEDNESDAY, OCT. 28 ~ 6-9 P.M.
CHESTERFIELD TECHNICAL CENTER ~ 10101 COURTHOUSE ROAD



- **KEYNOTE SPEAKER: DR. LYNDA GILLESPIE**, director of Instructional Technology for Chesterfield County Public Schools
"THE DANGERS AND WONDERS OF THE INTERNET—HOW TO SAFELY EXPLORE THE WIRED WORLD"
- **COMMUNITY FORUM** — Join us for a moderated forum by a panel of cyber security experts and practitioners to discuss cyber security. Learn about Internet risks and tips to secure computers. Avoid being a victim of phishing attempts, identity-theft scams and learn to protect your children and community from Internet predators.
FORUM MODERATOR: DR. GURPREET DHILLON, professor of Information Systems in the School of Business, Virginia Commonwealth University
- **CAREER AND JOB FAIR** — Focuses on fields of study and job opportunities in cyber security, homeland security and public safety. Participants include: VCU, Old Dominion University, the FBI, Department of Homeland Security and the Chesterfield County Police Department.

HOSTED BY CHESTERFIELD COUNTY'S DEPARTMENT OF INFORMATION SYSTEMS TECHNOLOGY AND OFFICE OF SECURITY MANAGEMENT



OUR SHARED RESPONSIBILITY

Seminars

Presenter: Virginia Federal Credit Union

Abstract

- ▶ We all know the economy has fallen on tough times. With credit not as readily accessible some people are desperate enough to traipse on names and credit histories of friends and family to keep up with their lifestyles or just to get by. The National Crime Prevention Council communicated, “Raising public awareness is the best approach to preventing Identity Theft.” In this presentation attendees learn:
- ▶ What is identity theft? How is it perpetrated? Can it be avoided and how? What to do if one becomes a victim?

“The Realities of Identity Theft”

Develop Partnerships

OCTOBER IS NATIONAL CYBER SECURITY AWARENESS MONTH

SAFE SURFING FOR TWEENS USING FACEBOOK
Thursday, Oct. 15 - 7-8 p.m.
Central Library

SAFE SURFING FOR SENIORS AND AVOIDING IDENTITY THEFT
Wednesday, Oct. 21 - 7-8 p.m.
Central Library

ALSO LEARN ABOUT:

- What safety steps to take to safeguard your computer from online threats
- How to respond to cyber crime incidents
- Plus other timely cyber safety issues

OUR SHARED RESPONSIBILITY

BOOKS FOR TWEENS

Angels on Sunset Boulevard
Melissa De La Cruz YA FIC DEL

Are U 4 Real?
Sara Kadefors YA FIC KAD

Click Here (To Find Out How I Survived the Seventh Grade)
Denise Vega YA FIC VEG

Fake Boyfriend
Kate Brian YA FIC BRI

Feed
M.T. Anderson YA FIC AND

The Gospel According to Larry
Janet Tashjian YA FIC TAS

Head Games
Mariah Fredericks YA FIC FRE

Rob&Sara.com
P.J. Petersen YA FIC PET

Romiette and Julio
Sharon Draper YA FIC DRA

Secrets of My Suburban Life
Lauren Baratz-Logsted YA FIC BAR

Stuffed
Eric Walters YA FIC WAL

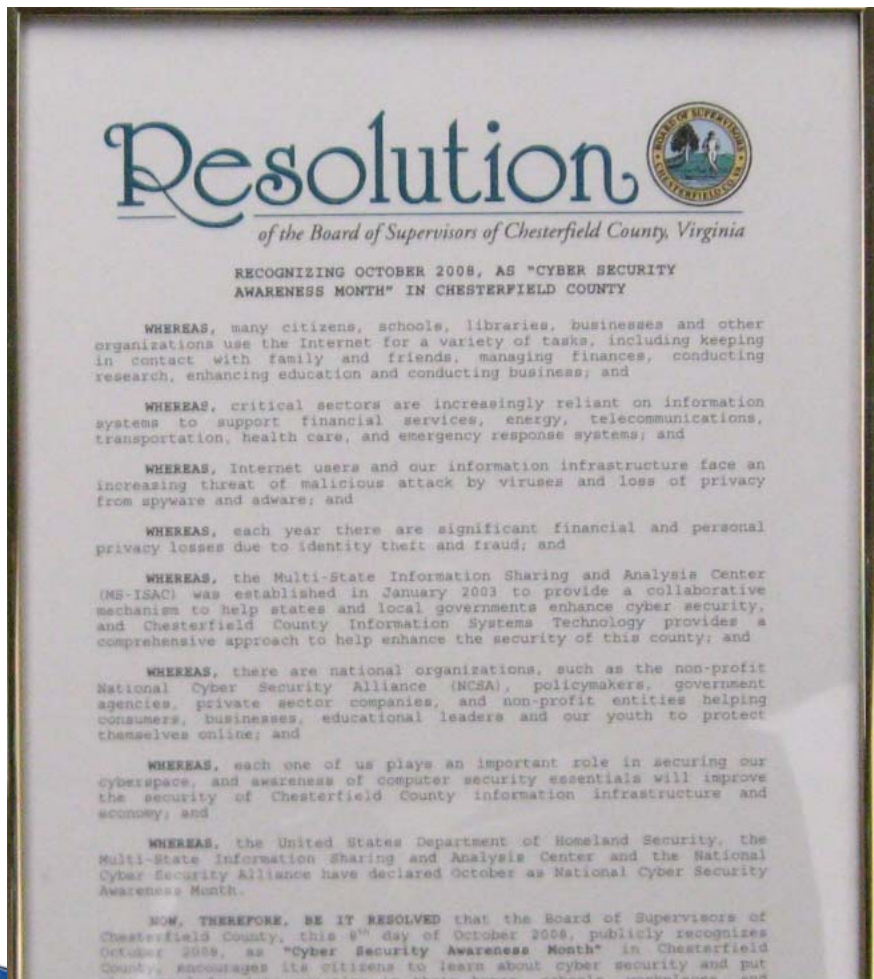
TTYL (Also, TTFN and L8r, G8r)
Lauren Myracle YA FIC MYR

Today'sGirls.com (series)
Various authors: Ask your librarian to help you find these titles, or search Today'sGirls.com on our online catalog at library.chesterfield.gov.

Waiting for You
Susane Colasanti YA FIC COL

If you would like to schedule Cyber Security Outreach for your organization, please call the RSVP line at: (604) 318-8118

Board of Supervisors Resolution



RECOGNIZING OCTOBER 2009, AS "CYBER SECURITY AWARENESS MONTH" IN CHESTERFIELD COUNTY

WHEREAS, many citizens, schools, libraries, businesses and other organizations use the Internet for a variety of tasks, including keeping in contact with family and friends, managing finances, conducting research, enhancing education and conducting business; and

WHEREAS, critical sectors are increasingly reliant on information systems to support financial services, energy, telecommunications, transportation, health care, and emergency response systems; and

WHEREAS, Internet users and our information infrastructure face an increasing threat of malicious attack by viruses and loss of privacy from spyware and adware; and

WHEREAS, each year there are significant financial and personal privacy losses due to identity theft and fraud; and

WHEREAS, the Multi-State Information Sharing and Analysis Center (MS-ISAC) was established in January 2003 to provide a collaborative mechanism to help states and local governments enhance cyber security, and Chesterfield County Information Systems Technology provides a comprehensive approach to help enhance the security of this county; and

WHEREAS, there are national organizations, such as the non-profit National Cyber Security Alliance (NCSA), policymakers, government agencies, private sector companies, and non-profit entities helping consumers, businesses, educational leaders and our youth to protect themselves online; and

WHEREAS, each one of us plays an important role in securing our cyberspace, and awareness of computer security essentials will improve the security of Chesterfield County information infrastructure and economy; and

WHEREAS, the United States Department of Homeland Security, the Multi-State Information Sharing and Analysis Center and the National Cyber Security Alliance have declared October as National Cyber Security Awareness Month.

NOW, THEREFORE, BE IT RESOLVED that the Board of Supervisors of Chesterfield County, this 14th day of October 2009, publicly recognizes October 2009, as "Cyber Security Awareness Month" in Chesterfield County, encourages its citizens to learn about cyber security and put that knowledge into practice in their homes, schools, workplaces, and businesses.

Outreach Road Show

Elementary School “Keeping Our Kids Safe Night”


Date: October 20, 2009
Time: 6:00 pm – 8:00 pm

Golden Fleet Senior Ministry

Date: October 21, 2009
Time: 9:00 am – 10:30 am

Chesterfield County Cyber Security Awareness Month Community Outreach Events Planned

CONTACT:
Barry Condrey
Information Systems Technology
Chesterfield, VA 23832
(804) 748-1590
--condreyba@chesterfield.gov--



Chesterfield, VA – [Insert Date Here] – In recognition of National Cyber Security Awareness Month (NCSAM) during October 2009, Chesterfield County is announcing a new Community Outreach program that will sponsor a “Cyber Security Awareness Road Show” as an education and awareness program to promote cyber security awareness for the benefit of computer users in the Chesterfield and surrounding areas. This program is an extension of the National Cyber Security Alliance (NCSA) organization (<http://www.staysafeonline.info/>). National Cyber Security Awareness Month (NCSAM), conducted every October since 2001, is a national public awareness campaign to encourage everyone to protect their computers and our nation’s critical cyber infrastructure.

Cyber security requires vigilance 365 days per year. However, the Department of Homeland Security (DHS), the National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the primary drivers of NCSAM, coordinate to shed a brighter light in October on what home users, schools, businesses and governments need to do in order to protect their computers, children, and data.

The Road Show will feature speakers discussing such topics as identity theft protection, safe computing, phishing scams, personal security and more. As part of October’s National Cyber Security Awareness Month, the road shows will be provided at no charge to interested civic and social organizations on a request basis.

All requests must be submitted by August 30, 2009 in order for the outreach to be scheduled and planned for the October Road Show.

To submit a Request:

To request a speaker for this outreach program please contact: the Cyber Month Road Show Request Line at: [Insert Phone Number Here] or visit the Chesterfield Website www.chesterfield.gov to submit an email request to: cyberroadshowrequest@chesterfield.gov to request a Cyber Month Road Show Speaker.

Webcasts & Podcasts

County Administrator's Message to Employees U173U09 UUh U5m [Video](#)

Information Services Security Awareness Contents

Name	Date	Duration	
Identity Theft	10/28/08	00h 56m	Video
Protecting Kids on the Internet	10/24/08	00h 39m	Video
No Tech Hacking - Johnny Long	10/24/08	01h 08m	Video

Copyright © 2007 Chesterfield County IST - All Rights Reserved

[Home](#) | [Phone Directory](#) | [In/Out Board](#) | [Help](#) | [Wiki](#)

Done Unknown Zone (Mixed)



Commonwealth of Virginia Information Security Awareness Month

Nakita Albritton, CISSP, PMP, CISA
Information Security Manager/
Continuity of Operations Coordinator



Governor's Proclamation

NOW, THEREFORE, I, Timothy M. Kaine, Governor of the Commonwealth of Virginia, do hereby proclaim the month of October 2009, as **INFORMATION SECURITY AWARENESS MONTH** in the Commonwealth of Virginia and encourage all the citizens of this Commonwealth to learn about information security and put that knowledge into practice in their homes, schools, workplaces, and businesses.



Now Is The Time!

- If you have not begun planning for your Information Security month activities, it is not to late, but time is ticking.
- Start now.



Information Security Month Ideas

- Activities
 - Presentations, Brown Bag Presentations, Demonstrations, Puzzles, Drawings, Videos, Contest
- Resource Material
 - Brochures, Booklets, Bookmarks, Calendars,
- Festive Environment
 - Balloons, Banners, Posters



Toolkit: www.vita.virginia.gov/security/default.aspx?id=5146



Web Banner

INFORMATION SECURITY AWARENESS MONTH

INFORMATION SECURITY STARTS WITH "YOU"

Think Before You Click
 Keep your software and operating system up-to-date.
 Keep your data safe and secure.
 Use hard-to-guess passwords.

MS-ISAC Resource Materials

2010 Cyber Security Calendar

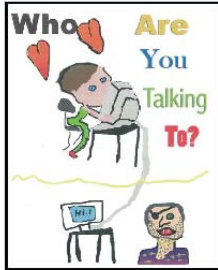
1st Place Winner

1st Place Winner

1st Place Winner



Jessica — State of New York
2009 National Poster Contest



Daniel — State of New Jersey
2009 National Poster Contest



Alyssa — State of Maryland
2009 National Poster Contest

The Parent's Guide to Cyberbullies



STATE or ORGANIZATION
to and Branding Information

Cyber Security: It's Up 2 U

Keep Sensitive Data Secure

Avoid Phishing Scams

HELPFUL TIPS

- Do not click on any links listed in an email message and do not open any attachments from untrusted sources
- Do not enter personal information in a pop-up screen
- If it appears to be a phishing email, simply delete it
- Enable/install a phishing filter on your web browser
- Do not respond to emails asking for personal information. Legitimate organizations will not ask you to provide personal information via email

INFORMATION SECURITY TIPS

Security of credit card transactions

April 2009

Vol. 4, Issue 4

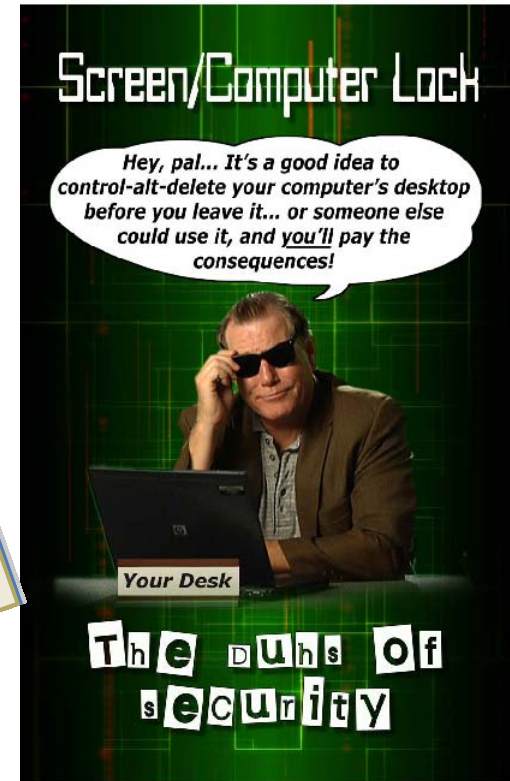
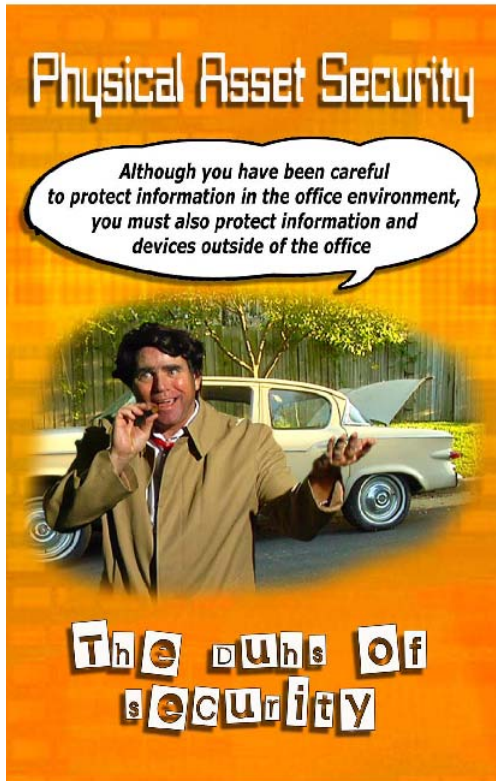
Security of credit card transactions

The use of credit cards to pay for goods and services is a common practice around the world. It enables business to be transacted in a convenient and cost effective manner. However, more than 100 million personally-identifiable customer records have been breached in the US over the past two years. Many of these breaches involved credit card information. Continued use of credit cards requires confidence by consumers that their transactions and credit card information are secure. The following provides information as to how the credit card industry has responded to security issues and steps you can take to protect your information.



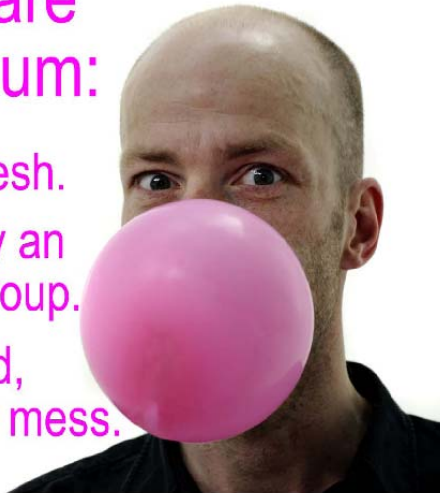
Multi-State Information Sharing and Analysis Center
www.msisac.org

VITA Security Video and Posters



Other Agency Created Resources

Passwords are like bubble gum:

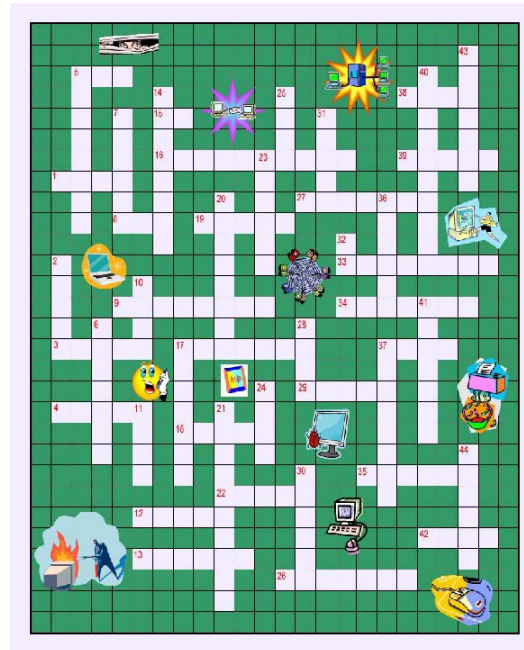


Strongest when fresh.

Should be used by an individual, not a group.

If left laying around, will create a sticky mess.

1	Across	You can turn the pages in a ____ in your hand or read one online.	
2	Down	When creating a Password, do not use words from your favorite _____. -<28 Down> __ hobby, recording artist, or <29 Across>_____.	
3	Across	Before you throw something in the _____, ask yourself, "Is this something I would give to an unauthorized person or want to become publicly available?"	
4	Across	Don't transmit any ____ letters via email.	
5	Across	____, Peer-to-Peer, is an informal network that allows users to share music, games, software, or other files with other users online.	
5	Down	Don't share your user _____. -<5> _____ or <15 Across>_____.	
6	Down	Criminals sometimes use _____ - programs like viruses and spyware - to get into your computer. Once there, they can steal information, send _____, and _____.	



our laptop safe: Keep it _____ . . . use a _____.

tion] is a means of accessing the Internet at high speed phone lines.

ries of web sites are blocked for one or more of the reasons: <19 Across> Risk, <20 Down> Risk, or <9> Risk.

ur laptop safe: Treat it like _____.

password must be at least _____ characters long.

ogram that can sneak onto your computer - often through email - and then make copies of itself, quickly using up all available space.

egment of Internet space denoted by the function or type of domain name. Current ones include ".com" for commercial, ".gov" for governmental ones, and ".org" for non-commercial ones.

hardware or software that helps keep hackers from getting into your computer to send out your personal information without your permission. It watches for outside threats, protects your system and block communications that you don't permit.

if user <5 Down> _____ or <15> _____.

the scrambling of data into a secret code that can be read only by a set to decode the information.

oftware program that may be installed on your computer to monitor your use, send pop-up ads, redirect your traffic to other websites, or record keystrokes, which could lead to identity theft.

a clear and specific _____ line in your email.



Printing Services

- Brochures, Booklets, Bookmarks, Calendars, Posters
 - Department of Motor Vehicles (DMV) has graciously offered to provide printing services.
 - For a price quote, please contact Damian M. McInerney by email at DAMIAN.MCINERNEY@dmv.virginia.gov or by phone at 804-367-0925.



Let Us Hear From You

In early November, please share a brief summary of your Information Security month activities with us by emailing us at VITA-Access-Training@VITA.Virginia.Gov.

WE ARE LOOKING FORWARD
TO HEARING FROM YOU!





1st Annual InfoSec Conference

“Information Security: Mission Possible!”

The Holiday Inn Select

Koger South-

Conference Center

November 2, 2009

8:00 am to 4:30 pm

Registration Fee: \$48



www.vita.virginia.gov/security/securityconference/default.aspx?id=10128





IronPort Review

Messaging Operations

Sensitive to VITA

Northrop Grumman Private/Proprietary Level I

Demetrias Rodgers, NG



NORTHROP GRUMMAN

Agenda

- Description of CISCO IronPort[®] anti-spam appliances
- Features/Benefits
- Detailed anti-spam review
- VITA/NG Partnership IronPort[®] Architecture
- Production Reports/Statistics
- Future Growth/Upgrades
- Questions

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted

Intentionally Omitted



Encryption Mechanics and Key Management

Bob Baskette:
CISSP-ISSAP CCNP/CCDP RHCT
Commonwealth Security Architect



Cryptography Basics

- Use of deception and mathematics to render data unintelligible through the transformation of data into an unreadable state and to ensure that a message has not been altered in transit.
- Protects transmitted information from being read and understood by anyone except the intended recipient.
- Cryptography ensures integrity, confidentiality, authentication, authorization, and using certain mechanisms non-repudiation
- Cryptography does not support availability

Cryptography Basics Continued

- Cryptosystem
 - Set of transformations from a message space to ciphertext space
 - Includes the encryption algorithm, keys, and necessary software components and protocols.
- Cryptographic Algorithm
 - Step-by-step procedures used to encipher plaintext and decipher ciphertext
- Cryptoanalysis
 - Study of techniques for attempting to defeat cryptographic techniques

Cryptography Basics Continued

- Key = crypto-variable
 - Sequence that controls the operation of the cryptographic algorithm
 - Determines the behavior of the algorithm and permits reliable operations
 - Comprises a large sequence of random bits
- KeySpace
 - Range of values that can be used to construct a key
 - Used by the algorithm to generate new random keys
 - The total number of possible values of the keys in a cryptographic algorithm



Cryptography Basics Continued

- Clustering
 - Situation in which a plaintext message generates identical ciphertext when using the same algorithm but different crypto-variables or keys
- Collision
 - When a hash function generates the same output for different inputs
- Avalanche Effect
 - A minor change in the either the key or plaintext will have a significant change in the resulting cipher text

Steganography (Hidden-writing)

- Secret communication in which the existence of the message is hidden in another media type
- The contents of the message is not encrypted
- The least-significant bit of each word in an image can be used to encode a message with causing any significant change to the image
- Can be used to create digital watermarks (the addition of identification information into a file or document)

Initialization Vector

- Non-secret binary vector used to initialize the input algorithm for encryption
- Random values used to ensure patterns are not created during encryption
- Used with keys and does not need to be encrypted during distribution
- Increases security by introducing additional cryptographic variance and synchronize cryptographic equipment

Strength of Cryptosystem

- Specifies the difficulty of uncovering the algorithm or key (whichever one if kept private)
- Determined by:
 - The time and resources needed to break algorithm or key
 - Algorithm
 - Secrecy of key
 - Initialization vectors



Important elements of encryption:

- Use an algorithm without flaws
- Use a large key size
- Use all possible values within the keyspace
- Protection of the key



Kerckhoff's Law

- A cryptosystem should be secure even if everything about the system, except the key, is public knowledge
- Algorithm should be in the public domain to reduce the vulnerabilities in algorithm

Transposition/Permutation

- Process of re-ordering plaintext to hide the message
- Key is used to determine the positions the values are moved
- Rearranges the original bits, characters, or blocks of characters to hide message
- Used in Symmetric algorithms



Substitution

- Process of exchanging one letter or byte for another (Caesar Cipher, monoalphabetic cipher, subset of the Vigenere polyalphabetic cipher)
- Can be attacked by frequency analysis
- The frequency of characters shown in the use of the alphabet's letters in a particular language are used.
- Uses a key to dictate how the substitution should be performed.
- Used in Symmetric algorithms

Confusion

- Commonly carried out via substitution
- Mixing or changing the key values used during the repeated rounds of encryption
- Provides added complexity
- Pertains to making the relationship between the key and the resulting ciphertext as complex as possible to prevent the key from being recovered from the ciphertext



Diffusion

- Commonly carried out via transposition
- Takes place as individual bits of a block are scrambled through the block
- Mixing up the location of the plaintext throughout the ciphertext
- A single plaintext bit has influence over several ciphertext bits such that changing a plaintext bit should change many ciphertext bits
- Through transposition, the location of the first character of the plaintext may change several times during the encryption process



SP-Networks

- Process used in block ciphers to increase the strength
- SP is substitution and permutation
- Most block ciphers do a series of repeated SP actions to add confusion and diffusion
- S-Boxes handle the substitution
- Strong ciphers require Confusion and Diffusion
- Randomness of key and complexity of mathematical functions dictate level of Confusion and Diffusion

Monoalphabetic / Polyalphabetic Substitution Ciphers

- **Mono**
 - Substitution of one alphabet letter for another
- **Poly**
 - Use of several alphabets for substituting the plaintext
 - Resistant to frequency analysis
 - List plaintext above multiple alphabets
 - Use substitution row based on the number position of the letter in the plaintext word
- **Blais de Vigenere**
 - Polyalphabetic cipher developed for Henry III using a key word and 26/27 alphabets (each one off-set by one place)
 - Top-row used for the plaintext
 - First column uses to find the row based on the key.



Running Key Cipher

- Does not require an electronic algorithm
- Could use components of real world
- If implemented by real world objects = pre-define objects and list order of objects in a continuous stream of symbols
- The key is repeated for the same length as the plaintext input.
- Cipher uses text (from a book or other well-known source) to encrypt the plaintext
- Text is matched character for character with the plaintext
- Uses modulo 26 addition
- Eliminates periodicity (when substitution repeats)
- Can be attacked by exploiting redundancy of key

One-Time Pad = Vernam Cipher

- Technique where the key has the same length as the message
- Key is used to encipher one character of plaintext
- Key is truly random
- Implemented as a stream cipher using XOR function
- Decrypt by XOR function of ciphertext and key



One-Time Pad = Vernam Cipher

- Not practical for megabyte or gigabyte messages
- Each key letter is added modulo 26 to each letter of plaintext
- Uses principle of the Running Key using the numerical values of the letters and adding those to the value of the key.
- Considered unbreakable if:
 - Key is used only once and never used again (prevent pattern detection)
 - Key (pad) must be as long as plaintext message
 - Key (pad) must be securely distributed
 - Key (pad) must be truly random



Encryption Key Types

- Secret
 - Symmetric Encryption
 - Also known as
 - Private-key
 - Shared-key
- Session
 - Symmetric Encryption
 - Key used only for one transmission session
- Public
 - Asymmetric Encryption
- Quantum
 - Symmetric Encryption
 - Key sent using Quantum Mechanics



Symmetric Cryptography

- Can use either substitution or transposition
- Use of a single key for both encryption and decryption
- Security of encryption is completely dependent of protection of key
- Sender and receiver use the same key
- Will require a different key for each receiver to maintain Confidentiality
- Will require $n(n-1)/2$ keys



Symmetric Algorithm Advantages

- Very fast
- Secure method for confidentiality with large key size
- Algorithms can be implemented in hardware or software at little cost

Symmetric Algorithm Disadvantages

- Requires a separate secret key per communications partner (scalability)
- Challenge of Key management
 - Keys cannot be sent in the same channel as the messages
 - Requires some sort of out-of-band medium
- No support for non-repudiation, message integrity, access-control, or digital signatures



Symmetric Cryptography Methods

- **Stream**
- **Block**



Stream-based Symmetric Cryptography Methods

- Encryption on a bit-by-bit basis
- Each plaintext bit will be transformed into a different ciphertext bit each time it is encrypted
- Stream-based is usually implemented in hardware since they require more processing power
- Stream-based relies primarily on substitution
- Governed by the cryptosystem and controlled by the cipher key
- Key provides randomness to operation (prevents plaintext/ciphertext XOR revealing Key)



Block-based Symmetric Cryptography Methods

- Operates on blocks of bits or chunks of text
- Plaintext is divided into blocks of plaintext
- Each block is put through mathematical functions
- Uses combination of substitution and transposition (confusion and diffusion)
- Changing one plaintext bit could change half of the ciphertext bits
- Key determines what functions are applied to the plaintext and in what order (provides randomness to process)



Block-based Symmetric Cryptography Methods

- Usually stronger than Stream-based enciphering
- More expensive to implement
- Block-based is usually implemented in software
- Block Cipher Modes
 - Electronic Code Book (ECB)
 - Cipher Block Chaining (CBC)
 - Cipher Feedback (CFB)
 - Output Feedback (OFB)
 - Counter Mode (CTR)



Symmetric Algorithms

- Caesar
- Spartan scytale
- Enigma machine
- DES
- 3DES
- Blowfish
- Twofish
- IDEA
- RC4, RC5, RC6
- SAFER
- Serpent
- AES



DES = Data Encryption Standard = FIPS 46-3

- Based on the Lucifer algorithm 128-bit algorithm (IBM) (Harst Feistel)
 - Introduced complex mathematical equations and functions
 - NSA modified to use 64-bit key
 - The actual algorithm is DEA
 - DES is the standard
 - 1988 NSA stopped endorsing DES
- Uses a 56-bit key(length is 64-bit/8-bits used for parity)
- Symmetric block encryption algorithm
- Divides the message into blocks/operates one block at a time



DES = Data Encryption Standard = FIPS 46-3

- Operates on 64-bit blocks of data broken into 32-bit blocks
- Output is 64-bit blocks
- Key-Space is 2^{56}
- Uses transposition and substitution/controlled by key
- 16-round cryptographic system
- Can be implemented in hardware
- Uses confusion and diffusion to improve encryption



Block Modes of DES

- **ECB = Electronic Code Book Mode**
- **CBC = Cipher Block Chaining Mode**



ECB = Electronic Code Book Mode

- Native DES mode
- Operates like a code book by providing the combination of substitutions and permutations performed on the data block with the selection controlled by the Key
- Best used with small blocks of data
- Operates on input blocks independently
 - Operation is not order dependant since blocks encrypted independently
 - Will generate the same output block if two input blocks match since each block is encrypted with same key and therefore the same code book, which can expose the key or code book
 - Only good for short messages of less than 64-bits in length since this method does not provide enough randomness for use with large messages
- Uses 64-bit plaintext blocks
 - Will add padding if block is not 64-bits in length
 - Will divide block into two 32-bit blocks called Right and Left blocks
 - Bits are copied to produce two 48-bit blocks
 - Each 48-bit blocks will be XOR with 48-bit key



CBC = Cipher Block Chaining Mode

- Stronger than ECB
- Each block of text, the key, and the value based on the previous block are processed in the algorithm and applied to the next block of text
- Provides dependence between blocks and hides any patterns
- Each input block will generate a different output block
- Uses a randomly generated 64-bit initialization vector (IV) to XOR with the first block of plaintext to introduce randomness with the result encrypted with DES key to make it less predictable
 - $IV \text{ xor } \text{Plaintext1} = \text{ciphertext1}$
 - $\text{ciphertext1} \text{ xor } \text{plaintext2} = \text{ciphertext2}$
- Different IV with same message will yield different encrypted message
- Operates with plaintext blocks of 64-bits
- Since this method chains blocks any error will be propagated

Stream Emulation Modes of DES

- DES is a block cipher that can simulate stream mode
- Block ciphers can be subject to problems of latency or delay in processing
- Used when data to be encrypted is a stream of continuous data instead of finite block
- Stream Mode Types:
 - **CFB = Cipher Feedback Mode**
 - **OFB = Output Feedback Mode**
 - **CTR = Counter Mode**



CFB = Cipher Feedback Mode

- Use to send large or continuous stream of data
- Example is terminal to terminal server (CBC operates on blocks of 64-bits) (stream data is usually 8-bits at a time)
- Cipher text is used as feedback into the key generation source to develop the next key stream
- Key and IV are used to generate the key-stream (random set of bits)
- Size of ciphertext needs to match size of plaintext (prevents patterns)
- Ciphertext generated by XOR of plaintext with key stream that has same number of bits as the plaintext and can propagate errors

CFB = Cipher Feedback Mode

- Input is separated into individual segments
 - 8-bit = size of one character
 - Each 8-bit are XOR inside a shift register
 - Once the XOR is complete the 8-bits are transmitted
- Can suffer failure if a single bit is corrupted or altered since all following data is corrupted
- Uses the same encryption process to encrypt and decrypt
- Need to use a new IV per message since message size is smaller enough for pattern matching



OFB = Output Feedback Mode

- Works well with small blocks of continuous stream data
- Values used to encrypt next block of plaintext come directly from the key-stream and not from the ciphertext
- Generates ciphertext by XOR plaintext with key stream
- Feedback is used to generate key stream
- Size of key-stream needs to match plaintext (prevents patterns)
- Key stream will vary
 - Errors are not propagated
 - Feeds the encrypted key-stream back into the shift register to create the next portion of the key-stream
- Does not chain the ciphertext
- Good for digitized video and digitized voice since the entire key-stream can be generated in advance and store for later use.



CTR = Counter Mode

- Used in high-speed applications (IPSec/ATM/802.11i) (packets often arrive out of order)
- Similar to Output Feedback Mode
- Uses an IV counter that increments for each plaintext block that needs to be encrypted
 - Ensures that each block is XORed with a unique key-stream value
- A counter (64-bit random data block) is used as the IV
 - The counter must be different for every block of plaintext
 - Counter will be incremented by 1
- Key-stream is separate from the data
- Ciphertext not used in the encryption process
- Can encrypt individual blocks in parallel
- Uses the same encryption process to encrypt and decrypt

3-DES Keying types

- Using 2 keys (DES-EEE2)
 - encrypt using Key1
 - encrypt using Key2
 - encrypt using Key1
- Using 2 Keys (DES-EDE2) (Allows backward compatibility with DES)
 - encrypt using Key1
 - decrypt using Key2 (used to jumble data/not decrypt data)
 - encrypt using Key1
- Using 3 keys (DES-EEE3)
 - encrypt using Key1
 - encrypt using Key2
 - encrypt using Key3
- Using 3 keys (DES-EDE3)
 - encrypt using Key1
 - decrypt using Key2 (used to jumble data/not decrypt data)
 - encrypt using Key3



AES = Advanced Encryption Standard

- Name of NIST standard
- Work began in 1998
- AES with a 256-bit key is considered by most to be the strongest algorithm
- Requirements outlined in FIPS PUB-197
 - Iterated block cipher (fixed block size of 128-bits)
 - Variable block length and key length that can be independently chosen as 128, 192, or 256 bits.
- Based on the Rijndael block Algorithm (developed by Belgian cryptographers Joan Daemen and Vincent Rijmen)
- Rijndael algorithm properties:
 - Resistance against all known attacks
 - Design simplicity
 - Code compactness and speed



AES Requirements

- **Layer Functions**

- Nonlinear layer is the parallel application of S-Boxes that have optimum worst-case nonlinearity properties
- Linear mixing layer provides a guarantee of a high diffusion of multiple rounds
- Key addition layer is the XOR of the round key to the intermediate state

- Round Key is derived from the cipher key through a key schedule

- Consists of a key expansion and Round key selection
- Total number of Round key bits is equal to the block length x number of rounds + 1
- The Cipher key is expanded into an Expanded Key
- Round keys are taken from the Expanded Key
 - 256-bit key and 256-bit block size = 14 rounds
 - 192-bit key and 192-bit block size = 12 rounds
 - 128-bit key and 128-bit block size = 10 rounds

Session Keys

- One approach to reduce the number of receiver keys used in a Symmetric encryption algorithm is to use a session key
- The session key is used for only one communication session between users
- Forms the basis for most encryption methods
- Use public-key cryptography to transmit a session key to the receiver
- Use timestamps to limit the lifetime of the session key (mitigate replay attacks)



Asymmetric Algorithms / Public Key

- Two keys linked mathematically, but would be mutually exclusive
- One key will encrypt/the other key would decrypt
- User generates two keys
 - Private Key that is kept secret and used to by receiver to decrypt messages
 - Public Key that can be sent to anyone and is used by sender to encrypt messages
- Important key properties:
 - Public key cannot decrypt message it encrypted
 - Private key cannot be derived from the public key
 - Message encrypted by one key can be decrypted by the other key
 - Private key must be kept secret
- Asymmetric algorithms are one-way functions



One-Way Functions

- Makes Asymmetric Cryptography possible
- A mathematical function that is easy to compute in one direction but difficult to compute in the reverse direction
- Function in easy direction provides encryption and digital signature verification and is performed with the public key
- Function in difficult direction provides decryption and signature generation and is performed with the private key
- Work factor for one-way function is the difference in time and effort that carrying out the one-way function in the easy direction takes compared to carrying out a one-way function in the difficult direction

Asymmetric-related terms

- **Trap-Door**
 - A secret mechanism that allows the one-way function to be easily reversed
 - Required to find the private key from the public key
- **Confidentiality**
 - Sender encrypts message with the receiver's public key
 - Only the receiver can decrypt the message
- **Non-repudiation**
 - Security service by which evidence is maintained so that the sender and the recipient of the data cannot deny having participated in the communications
 - Supported via public-key encryption and digital signatures
 - Sender encrypts the message with the sender's private key
 - The receiver opens with the sender's public key

Asymmetric Message Formats

- **Secure Message Format**
 - Encrypting a message with receiver's public key
 - Will provide confidentiality but not authentication or non-repudiation
- **Open Message Format**
 - Encrypting a message with the sender's private key
 - Will provide authentication and non-repudiation but not confidentiality

Asymmetric Key Considerations

- **Asymmetric Key Advantages**
 - Can send messages across unsecure mediums
 - No key management issues
 - Allows for non-repudiation and access-controls
- **Asymmetric Key Disadvantages**
 - Slower than Symmetric Key Cryptography
 - Ciphertext is much larger than the plaintext



Types of Asymmetric Algorithms

- RSA
- Elliptic curve Cryptosystems
- Diffie-Hellman
- El Gamal
- Digital Signature Algorithm
- Knapsack



RSA

- Rivest, Shamir, Adleman
- Public key algorithm
- Most popular for asymmetric algorithms
- Used in Microsoft, Apple, and Novell operating systems
- Can be used as key exchange protocol
 - System uses DES or AES to generate the symmetric key
 - Sends symmetric key encrypted with receiver's public key
- Provides authentication and key encryption



RSA

- Decryption based on the mathematical challenge of factoring the product of two large prime numbers to reveal the two prime numbers used to generate the specific large prime
- Public and private keys are functions of a pair of large prime numbers
- Most widely used public key algorithm and operates on blocks of text by $C = P^e \text{ mod } n$
- Can be used for encryption, key exchange, and digital signatures
- Using its one-way function
 - Provides encryption and signature verification
 - Inverse direction provides decryption and signature generation



RSA attacks

- Brute-force
- Factoring prime numbers
- Timing attacks

Diffie-Hellman

- Developed to resolve the symmetric Key exchange problem by allowing the exchange or negotiate a symmetric key over non-secure medium
- First Asymmetric key agreement algorithm
 - Not key exchange (sending symmetric key encrypted with receiver's public key)
 - Provides for key distribution
 - Does not provide encryption or digital signature functions
- Does not provide message confidentiality
- Based on difficulty of calculating discrete logarithms in a finite field
- Sender uses sender's private key and receiver's public and the D-H algorithm to derive the shared value used to create instances of symmetric keys.

Diffie-Hellman

- Symmetric key used to encrypt data is created from only public information (public keys)
 - Uses two parameters which are both public
 - P = is a prime number
 - G = is the generator and is an integer less than P
- Running the public key through the DH algorithm will generate a common session key.
- D-H is vulnerable to Man-in-the-Middle attack
 - Does not perform authentication prior to public key exchange
 - Use digital signatures or digital certificates to perform authentication

El Gamal

- Extension of D-H
- Can be used for encryption, key exchange, and digital signatures
- Can provide message confidentiality and digital signatures
- Based on discrete logarithms in a finite field
- Very slow algorithm

Markle-Hellman Knapsack

- Based on the “knapsack problem”
- Mathematical dilemma based on the problem of having a set of items with fixed weights and determining which of these items can be added in order to obtain a given total weight
- Can be used for encryption and digital signatures
- Found to be insecure



Elliptic Curve Cryptography

- Has the highest strength per bit of key length
- Allows for shorter keys
- Fast and efficient (great for portable devices/small memory and processor)
- Will require fewer computational and memory requirements
- Suited to hardware applications such as smartcards and wireless devices
- Based on discrete logarithmic algorithms of elliptical curves
- Provides confidentiality, digital signatures, message authentication, and key management
- EC 160-bit key = RSA 1024-bit key



Key Strength Comparison

Asymmetric	vs.	Symmetric
512		64
1792		112
2304		128



PGP = Pretty Good Privacy

- Developed by Phil Zimmerman
- Freeware email security
- First widespread public key encryption system
- Can use RSA public key encryption for key management
- Can use IDEA symmetric cipher for bulk encryption
- Can use MD5 for integrity
- Can provide confidentiality, integrity, authentication, non-repudiation
- Passphrase used to encrypt user's private key on local host
- Does not use a CA to exchange keys / uses web of trust
- Key-ring = collection of public keys collected from other users

Quantum cryptography

- Uses physics to secure data = Also called Quantum Key Distribution = QKD
- QKD is a set of protocols, systems, and procedures used to create and distribute secret keys
- The quantum keys can be used with traditional cryptosystems to encrypt data
- QKD systems can only be used to generate keys and cannot be used as a stand-alone cryptosystem

Quantum cryptography

- Quantum Cryptography solves the issue of needing a secure channel to distribute secure keys because it allows secure key exchange based on the laws of physics
- Uses photon polarization to represent bit (vertical/horizontal/left/right)
- Each user must have the same polarization to binary mapping

Quantum cryptography

- **QKD uses two channels**
 - One channel is used to transmit the quantum key material via a single-photon light pulse
 - The other channel carries all messages including the cryptographic protocols
- **The basic law of QKD**
 - Once a photon has been observed, its state is changed
 - Allows for detection of eavesdropping



PKI = Public Key Infrastructure

- Establishes a level of trust within an environment
- ISO authentication framework that uses public key cryptography and X.509 standard
- Provides authentication, confidentiality, non-repudiation, and integrity of the messages exchanged
- Hybrid system of symmetric and asymmetric algorithms
- Assumes that the receiver's identity can be positively ensured via certificates and that an asymmetric algorithm will automatically carry out the key exchange



PKI Functions

- Identifies the users
- Create and distribute certificates
- Maintain and revoke certificates
- Distribute and maintain encryption keys



PKI Components

- Certificate authorities
- Registration authorities
- Certificate Repository
- Certificate revocation system
- Certificate Revocation List
 - Contains every certificate revoked by the CA
 - Most web browsers do not check the CRL for a CA.
- Key backup and recovery system
- Automatic key update
- Keys
- Users



PKI Digital Certificates

- Each person that wants to participate in PKI needs a digital certificate, which is a credential that contains the public key and other identifying information.
- The certificate must be signed by a Certificate Authority.
- Each individual must trust the same CA to exchange certificates.



Certificate Authority

- Acts as a notary by verifying a person's identity and issuing a certificate that vouches for a public key of the named individual
- Binds the individual to the public key
- Assumes liability for the authenticity of the individual
- Certificate is signed with the CA's private key



Digital Certificate Components

- Subject name
- Subject public key
- Name of the CA
- Serial number
- Version number
- Algorithm information
- Expiration date
- Signature of issuing authority



Certificate Authorities

- CA public key must be cross-certified with another CA
- X.509 standard defines the format for public key certificates
- Directory is simply a repository of public keys



Registration Authority

- Responsible for verifying an individual's identity
- Passes this information to the CA
- CA will then issue the certificate
- Performs certificate life-cycle management functions
- Acts as a broker between user and CA



Rules for Keys and Key management

- The key length should be sufficient to protect the message
- Keys should be stored and transmitted by secure means
- Keys should be extremely random and the algorithm should employ the full key space
- Keys lifetime should correspond to the sensitivity of the message
- Keys should be backed up or placed in escrow
- Keys should be properly destroyed at end of life



Key Recovery

1. Common Trusted Directories
2. Policy requiring all keys to be registered with the security department
3. Use steganography to hide passwords
4. Use a password wallet



Multi-party Key Recovery

- User would break private key into multiple parts and give each part to a trusted source with orders to only reveal that part in an emergency
- ANSI X9.17 was developed to address the need of Financial Institutions to transmit securities and funds securely
 - Based on the hierarchy of keys
 - Bottom used for data keys (DK) to encrypt/decrypt messages and are very short lived
 - Top used for the Master Key (KKM) to encrypt the data keys and have a longer life span

Cryptographic Attacks

- **Brute Force**
 - Exhaustive search of every possible key
- **Known Plaintext**
 - Attacker uses a copy of known plaintext (or parts of known plaintext) and ciphertext to attempt to determine the key
- **Chosen Plaintext**
 - Chose plaintext to be encrypted and the output is compare to the ciphertext
- **Adaptive Chosen Plaintext**
 - Adapt plaintext based on the results of the last Chosen Plaintext
- **Ciphertext only**
 - Attempt to decipher by analyzing several encrypted messages to discover key
 - Most common type of attack/hardest to achieve

Cryptographic Attacks

- **Chosen ciphertext**
 - Chose the ciphertext to decrypt and has access to the decrypted plaintext
- **Birthday attack**
 - Based on the mathematical birthday paradox that exists in standard statistics to find a collision in a hash algorithm.
 - Better than even chance of finding a match
 - Easier to find two matching values in a set of values than finding a specific match in the set.
 - Chance of finding a collision in a Hash algorithm is 2^{-n} (Number of bits in message digest/2). 60-bits = 230 inputs.
- **Meet-in-the-middle**
 - Attack against Double DES
 - Brute-force attack against the plaintext
 - Encrypt known plaintext with all possible keys and create a table with all possible results
 - Attack has same work factor as DES

More Cryptographic Attacks

- **Differential Cryptanalysis**
 - Used on block cipher private key systems
 - Take two plaintext messages and follow changes made as they pass through S-boxes using same key
 - Analysis difference in ciphertext pairs to map probability values in keys
- **Side-Channel**
 - Review the facts and infer value of key
 - Detect power consumption for encryption and decryption
 - Intercept radiation emissions to determine how long process takes
- **Passive**
 - Eavesdropping and sniffing
 - Does not affect the protocol, algorithm, key, message



Wassenaar Agreement

Encryption Algorithms too dangerous to fall into terrorist state hands:

- Symmetric algorithms with key sizes over 56-bits
- Asymmetric algorithms that carry out factorization of an integer with key sizes over 512-bits (RSA)
- Asymmetric algorithms that compute discrete logarithms in a field with key sizes over 512-bits (El Gamal)
- Asymmetric algorithms that compute discrete logarithms in a group with key sizes over 112-bits (ECC)
- Exportation of most encryption tech is now allowed from the US (after technical review) except for those listed as terrorist states
- A technical review is not required if sent to foreign subsidiaries of US firm



Questions???

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

Thank You!



2009 Commonwealth Security Annual Report

Benny Ambler
Enterprise Risk, Assurance & Standards Manager





§ 2.2-2009

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

- C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.



Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

Acronyms:

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

ISO Designated: The Agency Head has

- Yes** - designated an ISO with the agency within the past two years
- No** - NOT designated an ISO for the agency since 2006
- Expired** –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

Attended IS Orientation:

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



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

Security Audit Plan Received: The Agency Head has

Yes - submitted a Security Audit Plan for the period of fiscal year 2009 - 2011 for systems classified as sensitive based on confidentiality, integrity or availability

No - not submitted a Security Audit Plan since 2006

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

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY 2009 – FY 2011

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

Corrective Action Plans Received: The Agency Head or designee has

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

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

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

Not Due - not had Security Audits scheduled to be completed

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

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



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

Quarterly Updates: The Agency Head or designee has

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

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

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

Not Due - no open Security Audit findings

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

Pending - submitted quarterly status update that is currently under review



FAQ!

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

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

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

October 31, 2009



Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Human Rights Council	Yes	0	No	N/A	N/A
Dept. of General Services	Yes	3	Yes	Not Due	Not Due
Dept. of Human Res. Mgmt	Yes	1	Expired	No	N/A
Dept. Min. Bus. Enterprise	Yes	1	Pending	Pending	N/A
Employee Dispute Resolution	Yes	2	Expired	Not Due	Not Due
Compensation Board	Yes	1	Expired	No	N/A
State Board of Elections	Yes	1	Expired	No	N/A



Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Forestry	Yes	1	Yes	Not Due	Not Due
Va. Dept. of Ag. & Cons. Serv.	Yes	30	Yes	Yes	Yes



Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept of Business Assistance	Yes	2	Yes	Not Due	Not Due
Board of Accountancy	Yes	0	Yes	Yes	Not Due
Dept. of Housing & Community Development	Yes	1	Yes	Some	Some
Dept. of Mines, Minerals & Energy	Yes	1	Yes	Yes	Yes
Dept. of Labor & Industry	Yes	3	No	N/A	N/A
Dept. of Professional & Occupational Regulation	Yes	1	Yes	Not Due	Not Due
Tobacco Indemnification Commission	Yes	1	No	N/A	N/A
Va. Employment Commission	Yes	2	Yes	Some	Yes
Va. Economic Development Partnership	Yes	0	No	N/A	N/A
Va. Housing Development Authority	Expired	1	No	N/A	N/A
Va. National Defense Industrial Authority	Yes	0	No	N/A	N/A
Va. Resources Authority	No	0	No	N/A	N/A
Va. Racing Commission	Yes	0	Yes	Pending	Pending



Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Education	Yes	2	Pending	Some	N/A
Frontier Culture Museum of Va.	Yes	0	No	N/A	N/A
Gunston Hall	Yes	0	No	N/A	N/A
Jamestown - Yorktown Foundation	Yes	2	Yes	Not Due	Not Due
Library of Va.	Yes	0	Yes	Not Due	Not Due
State Council of Higher Education for Va.	Yes	0	Yes	Not Due	Not Due
Science Museum of Va.	Yes	1	Yes	Not Due	Not Due
Va. Commission for the Arts	Yes	0	Yes	Not Due	Not Due
Va. Museum of Fine Arts	Yes	0	Yes	Yes	Yes



Secretariat: Education (Cont'd)

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Christopher Newport University	Yes	0	Yes	Some	Yes
George Mason University	Yes	1	Pending	Yes	Yes
James Madison University	Yes	1	Yes	Yes	Yes
Longwood University	Yes	1	Yes	Yes	Yes
Norfolk State University	Yes	2	Yes	No	N/A
Old Dominion University	Yes	0	Pending	Yes	Yes
Radford University	Yes	0	Yes	Yes	Yes
Richard Bland College	Yes	0	Yes	Not Due	Not Due
University of Mary Washington	Yes	1	Yes	Yes	Not Due
Va. Community College System	Yes	43	Yes	Yes	Yes
Virginia Military Institute	Yes	0	Pending	No	N/A
Virginia State University	Pending	3	Yes	Pending	Not Due



Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Accounts	Yes	4	Yes	Yes	Not Due
Dept. of Planning & Budget	Yes	1	Yes	No	N/A
Dept. of Taxation	Yes	1	Yes	Pending	Pending
Dept. of Treasury	Yes	3	Yes	Some	Some



Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Health Professions	Yes	2	Yes	Not Due	Not Due
Dept. of Medical Assistance Services	Yes	4	Yes	Yes	Yes
Department of Behavioral Health and Developmental Services DMH/MRSAS	Yes	22	Yes	Some	Some
Dept. of Rehabilitative Services	Yes	0	Yes	Not Due	Not Due
Dept. of Social Services	Yes	1	Expired	No	N/A
Virginia Foundation for Healthy Youth VTF	Yes	1	No	N/A	N/A
Va. Dept. for the Aging	Yes	0	Yes	Pending	Pending
Va. Dept. of Health	Yes	5	Yes	Some	Some



Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Conservation & Recreation	Yes	1	Yes	Yes	Yes
Dept. of Environmental Quality	Yes	4	Yes	Yes	Yes
Dept of Game & Inland Fisheries	Yes	2	Expired	Some	No
Dept. of Historic Resources	Yes	2	Expired	No	No
Marine Resources Commission	Yes	3	Yes	Yes	Yes
Va. Museum of Natural History	Yes	2	No	N/A	N/A



Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Alcoholic Beverage Control	Yes	4	Yes	Yes	Yes
Commonwealth's Attorney's Services Council	Yes	0	No	N/A	N/A
Dept. of Criminal Justice Services	Yes	2	Yes	Yes	Not Due
Dept. of Fire Programs	Yes	2	Yes	No	Not Due
Dept. of Forensic Science	Yes	1	Expired	No	N/A
Dept. of Juvenile Justice	Yes	2	Yes	Not Due	Not Due
Dept. of Military Affairs	Expired	1	No	N/A	N/A
Dept. of Corrections	Yes	2	Expired	Some	No
Dept. of Correctional Education	Yes	1	Yes	No	N/A
Dept. of Veterans Services	Yes	0	Pending	N/A	N/A
Va. Dept. of Emergency Management	Yes	1	No	N/A	N/A
Va. State Police	Yes	2	Yes	Pending	Pending



Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
The Ctr for Innovative Tech.	Yes	1	Expired	No	N/A
Va. Info. Technologies Agency	Yes	31	Yes	Some	Not Due



Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Motor Vehicles	Yes	1	Pending	Not Due	Not Due
Dept. of Aviation	Yes	2	Yes	Not Due	Not Due
Dept. of Rail & Public Trans.	Yes	0	Yes	Not Due	Not Due
Motor Vehicle Dealers Board	Yes	0	Yes	Not Due	Not Due
Va. Dept. Of Transportation	Yes	9	Yes	Pending	Pending



Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Indigent Defense Commission	Yes	4	Expired	Some	Not Due
State Lottery Dept.	Yes	0	Yes	N/A	N/A
State Corporation Commission	Yes	3	Yes	No	N/A
Va. College Savings Plan	Yes	3	Yes	No	N/A
Va. Office for Protection & Advocacy	Yes	1	Exception	Exception	Not Due
Va. Retirement System	Yes	1	Yes	Pending	N/A
Va. Workers' Compensation Commission	Yes	3	Exception	Exception	Not Due



Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Office of the Governor	Yes	1	Exception	Exception	Not Due
Office of the Attorney General	Yes	0	Yes	Not Due	Not Due



Upcoming Events





2009 Information Security Awareness Tools

The Information Security Toolkit has been updated with new materials!

For printing cost estimates you can contact DMV's
Damian McInerney at (804)367-0925
or email: damian.mcinerney@dmv.virginia.gov

Thank you DMV!



UPCOMING EVENTS! Future 2009 ISOAG's

From 1:00 – 4:00 pm at CESC

(please let us know if you want to host in the Richmond area!)

Wednesday - November 18 @ **SCC Building** !

Thank you, Blair Kirtley for organizing this!

*****Special link to register*****

<http://www.vita.virginia.gov/registration/Session.cfm?MeetingID=20>

Wednesday - December 9



UPCOMING EVENTS! Future IS Orientation Sessions

- | | | |
|----------|-------------------|--------------------|
| Monday - | November 9, 2009 | 1:00 – 3:30 (CESC) |
| Monday - | December 14, 2009 | 1:00 – 3:30 (CESC) |
| Monday - | January 11, 2010 | 1:00 – 3:30 (CESC) |
| Monday - | February 1, 2010 | 1:00 – 3:30 (CESC) |



UPCOMING EVENTS: MS-ISAC Webcast

National Webcast!

Thursday, October 8, 2009, 2:00 to 3:00 p.m.

Topic: In Conjunction with October Cyber Security Awareness Month

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/>



Information Security System Association

ISSA meets on the second Wednesday of every month

DATE: Wednesday October 14th

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

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

PRESENTATION: "Internet Single Sign-On: What Is It and Why Should You Care"

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



UPCOMING EVENTS - CIO-CAO Mtg.

CIO-CAO Communications Meeting:

Tuesday, October 27

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: Perimeter Center
9960 Mayland Drive
Richmond, VA



FACTA Red Flag Requirements *NEW DATE

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

Announcement at: <http://www.ftc.gov/opa/2009/07/redflag.shtm>

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>



1st Annual COV Information Security Conference

“Information Security: Mission Possible!”

Date: November 2, 2009

Time: 8:30 a.m. – 4:30 p.m.

Where: Holiday Inn Koger Center, Richmond

Registration Fee: \$48.00

(includes hot buffet breakfast, hot buffet lunch & afternoon refreshments)

(Attendance limited to the first 95 who register)

Agenda:

Gino Menchini, Government IT: *The New Expectations & Challenges*

Walter Kucharski - *Top 10 Commonwealth Information Security Issues/Opportunities/Concerns/Risks*

Randy Marchany - *Unintended Consequences: Don't Create New Risks*

Bob Baskette - *Social Engineering: Building Bridges to Confidential Data*

For more information & registration, please visit:

<http://www.vita.virginia.gov/security/SecurityConference/default.aspx?id=10128>



Management System – Auditing Applications and Controls

When: November 4-5, 2009

Where: James Monroe Building, 101 N. 14th Street,
Richmond, VA (PDS Room #2, next to cafeteria, 1st floor)

Time: 8:15 a.m. – 4:45 p.m.

Cost: \$380.00 (Participants will earn 16 CPEs)

Registration: <https://secure.doa.virginia.gov/hrtraining/login.cfm>

Speaker: John Thompson – a business consultant, auditor, trainer, and speaker with over fifteen years of extensive management and operational experience in developing and implementing policies to manage business risk and business continuity planning.

For questions or problems registering contact:

Tim Sadler, Audit Manager (804-2245-3106, ext. 23 or tim.sadler@doa.virginia.gov)

(Target Audience: IT auditors, IT personnel and managers)



Any Other Business ???????



ADJOURN

THANK YOU FOR ATTENDING!!

