Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

August 1, 2012

Virginia Information Technologies Agency

ISOAG August 2012 Agenda

I.	Welcome & Opening Remarks	Michael Watson, VITA
II.	Cyber Agent	SA Jason Fullerton, FBI
III.	ISO Family Feud	Ed Miller, VITA
IV.	Travel Security Best Practices	Bob Baskette, VITA
V.	Upcoming Events & Other Business	Michael Watson, VITA
VI.	Partnership Update	Bob Baskette, VITA Mike Clark, NG

FBI
1970 E Parham Road
Richmond VA 23228
804-261-1044

JASON FULLERTON
SPECIAL AGENT
FBI RICHMOND

Cyber Agent

FBI
1970 E Parham Road
Richmond VA 23228
804-261-1044

Slides Intentionally Omitted

Virginia Information Technologies Agency

ISO Family Feud

Ed Miller
Commonwealth Security & Risk Management

ISOAG Meeting

OBJECT

Teams try to provide all of the answers to a question that has multiple correct answers before getting 3 strikes (for providing wrong answers)

FACEOFF

Each round starts with a Faceoff
One player from each family comes to the podium.
Each player takes a buzzer
Reveal the game board (each game board is a round)
I'll read the question
First person to buzz gets to answer
If it's a right answer the family can decide to pass or play.

GAME PLAY

If the family decides to play, each team member gets to answer in sequence.
For game play, family members stay at the table.
I'll ask the next family member in sequence to give their answer
Each right answer scores 10 points for the team
Each wrong answer gets a STRIKE (X).
If the team reveals all answers before they get 3 strikes, they win the round, and 10 points for each revealed answer.
If the team gets 3 strikes before all answers are revealed, the other team gets to "steal" the round and all the points if they can come up with one of the remaining answers.
Points awarded each round are added to each team's cumulative score.
Highest cumulative score at the end wins the game.

FACE OFF

ISO FAMILY FEUD

Name a castaway on Gilligan's Island:

1) X X X X X X

2) X X X X X X

3) X X X X X X

4) X X X X X X

5) X X X X X X

6) X X X X X X

7) X X X X X X

Time

Yes!

No

Name a castaway on Gilligan’s Island:

- Gilligan
- the Skipper
- Professor
- Thurston Howell, III
- Lovie Howell
- Ginger
- Mary Ann

Time

Yes!

No

Commonwealth ISO Family Feud

Thanks for playing!

Virginia Information Technologies Agency

Travel Security Best Practices

Bob Baskette

Senior Manager, Security Operations and Architect

Background

- It is the policy of Commonwealth of Virginia to ensure the confidentiality, integrity, and availability of data provided to and generated by the Commonwealth of Virginia.

- Trustworthy data, whether classified as sensitive or non-sensitive, is critical to the daily operations of the Commonwealth.

Preparing for the Trip

- If the purpose of the trip can be accomplished without the computing asset, leave it at the office.

- Review the information required for the trip. Do not take information that is not needed to accomplish the purpose of the trip, including sensitive contact information.

Preparing for the Trip

- Consider the consequences if the information were stolen by a foreign government or a malicious individual. If the device is lost, stolen, or otherwise compromised, the sensitive data could also be compromised.

Preparing for the Trip

- Private data that is required for the trip, but cannot be stored on a computer must be copied onto an encrypted USB memory device.

- Please note in some countries, customs officials may not permit you to enter with encrypted information.

Preparing for the Trip

- The agency should research such restrictions prior to departure and contact the appropriate federal agency (U.S. Department of State, etc.) to file any necessary requests for exemption, if available.

- Use encryption with complex passwords to protect confidential files.

Preparing for the Trip

- Back up all information required for the trip and secure the backed-up data at the office.

- If operationally feasible, acquire temporary computer assets system for use during the trip.

Preparing for the Trip

- Change the password for any account to be used during the trip

- Never store passwords, phone numbers, or sign-on sequences on any device or in its case.

Preparing the Computing Asset

- Have the system administrator change the administrator account password.
- Install all operating system security updates.
- Install all anti-virus, firewall, and anti-spyware security application software updates.

Preparing the Computing Asset

- Encrypt the computer hard disk or at least all sensitive information on the device.

- Update the web browser software and implement strict security settings.

Preparing the Computing Asset

- Update all application software to be used during the trip.
- Disable infrared ports, Bluetooth ports, web cameras, and any hardware features not needed for the trip.
- Configure the device to use a VPN connection to create a more secure connection.

Preparing the Computing Asset

- Configure the device to disable sharing of all file and print services.

- Configure the device to disable ad-hoc wireless connections.

General Travel Precautions

- Avoid using computer bags to carry the laptop since it obvious that the bag contains a laptop.
- Transport the laptop in a padded briefcase, suitcase, or backpack that can be locked in a discrete manner.
- Avoid transporting devices in checked baggage.

General Travel Precautions

- Change passwords at least every 4 days for all electronic devices and remotely accessed accounts.
- Use digital signature and encryption capabilities when possible.
- Do not leave electronic devices unattended.

General Travel Precautions

- If you have to leave the device, or the device will not be used for an extended period, remove the battery, any memory or SIM cards and keep them with you.

- Do not use thumb drives given to you as the thumb drive may be compromised or contain malicious software.

General Travel Precautions

- Assume that any computer not provided by the authorized COV IT department is not secure and may be compromised with malicious software. This includes public terminals found in libraries and cyber cafes.

General Travel Precautions

- If a shared system must be used, do not enter sensitive information such as passwords, bank account numbers, or credit cards numbers since any sensitive data sent over the internet from a public access point may be intercepted and logged by unknown parties.

General Travel Precautions

- Do not use the “remember me” feature on websites. Reenter the password for the website every time.
- Terminate connections when not in use.
- Clear the browser session data after each use: delete history files, caches, cookies, URL, and temporary internet files.

General Travel Precautions

- Do not open emails or attachments from any source without verifying the legitimacy of the source and the contents of the message.
- Do not click on links in emails.
- Empty the “trash” and “recent” folders after every system use.

Hotel and Airport considerations

- Do not leave the device at the front desk. It is not the responsibility of the hotel to protect a guest's property.

- If the device must be left in the hotel room, place in the hotel room safe if available.

Hotel and Airport considerations

- If the hotel room does not have a safe, secure the device to a piece of furniture with a security cable.

Hotel and Airport considerations

- Affix contact information as well as shipping information to the device with a promise of a "Reward for return — no questions asked”.

- If traveling by car, keep all devices out of sight by locking the devices in the trunk.

Hotel and Airport considerations

- If traveling by air or rail, hold the bag containing all devices until the person in front of you has gone through the screening process.

- Avoid setting the bag containing the devices on the floor since this is an easy way to forget or lose track of the bag.

Traveling outside the Continental USA

- All assigned COV electronics must remain within the Continental USA.

- Travel outside the Continental USA requires the use of temporary devices that contain the absolute minimum data to accomplish the purpose of the trip.

Traveling outside the Continental USA

- Be aware that government security agencies in some countries may log all Internet activity without prior notification.

- Be aware that in some countries it is common practice for the government or businesses to copy data from any computer system without the user's knowledge or consent.

Traveling outside the Continental USA

- Be aware that all personal belongings may be searched multiple times and electronic media may be copied.

- Many countries do not grant any expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries and hotel rooms are often searched.

Traveling outside the Continental USA

- Do not transfer sensitive information onto a computer that has left the continental USA.

- Do not attach any removal media such as a thumb drive or memory card to a foreign computer. The system may contain malicious software and should be considered compromised.

Traveling outside the Continental USA

- Foreign Security services and criminals can track your movements using the hardware insider the computing asset and can enable hardware such as the web camera or microphone without any warning. To prevent this, remove the battery, if possible, and disable the camera and microphone capabilities on all electronic devices when those functions are not being used.

Traveling outside the Continental USA

- Foreign Security services and criminals can also insert malicious software into your device through any connection they control including any wireless connection enabled on the device.

Traveling outside the Continental USA

- If a customs official demands to examine the computing asset, or if the hotel room is searched while the computing asset is unattended, assume the computing asset's hard drive has been copied.

Traveling outside the Continental USA

- Be cautious of unsolicited requests and questions about the purpose of the trip or other sensitive information.

- It is advisable to not speak about the purpose of the trip or comment on the status of the trip.

Traveling outside the Continental USA

- Avoid political conversations or offering political opinions while in foreign countries, either in person, on the phone, or online.

- Avoid wireless networks if possible. In some countries the wireless networks controlled by State security services; in all cases the networks are not secure.

Upon Returning from the Trip

- Do not connect any device to a COV network until that device has been examined and cleared by the agency IT department.

Upon Returning from the Trip

- Immediately return the device(s) to the Agency IT department
- Have the IT department examine the device(s) for the presence of malicious software.
- Change all system and account passwords using a system within the agency network.

Upon Returning from the Trip

- If the computing asset was used outside the Continental USA the asset must be completely erased in accordance with the COV ITRM SEC 514 Data removal Standard.

Incident Handing or Loss of Device

- Change all account passwords from a secured computing asset to prevent unauthorized access to COV servers.

- If a secured computing asset is not available, contact the Agency IT department to have all affected accounts disabled until the trip ends.

Incident Handing or Loss of Device

- Report the theft to local authorities (police) and to your agency's IT department.

- If traveling outside the Continental USA, report the theft of the computing asset or information to the Agency IT department and the local US embassy or consulate.

Final Thoughts

- It is not a question of IF the system will be compromised, but When will the system be compromised.

- Do not take the device unless it is really, really needed.

Final Thoughts Cont.

- Carefully consider the benefits of traveling with computing assets verses the costs of a successful compromise of your sensitive data

- Use temporary devices for all travel and wipe the device before travel to ensure what is on the device

Final Thoughts Cont.

- Disable all communication ports including Bluetooth, Wi-Fi, cameras, and microphones on all devices.

- If the device is not being used remove the battery to prevent malicious software from enabling communication ports.

Final Thoughts Cont.

- Connect to the Internet only through an encrypted, password-protected channel.

- Many countries prohibit travelers from entering the country with encrypted devices unless they have government permission.

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!

Upcoming Events

Information Security System Association

ISSA

DATE: Wednesday, Aug 8, 2012

LOCATION: Maggiano's Little Italy
11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.
Lunch served at 12.

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

SPEAKER: *TBD*

TOPIC: *TBD*

Virginia Information Technologies Agency

MS-ISAC

National Webcast Initiative

Thursday, Aug 9

2:00 pm – 3:00 pm EDT

Topic: **Botnets and Zombie Attacks: Securing Your Organization Against an Evolving Threat**

Visit MS-ISAC web for more information:

http://www.msisac.org/webcast/

Virginia Information Technologies Agency

COVITS 2012

COVITS is a forum to discuss technology requirements, share valuable lessons from actual case studies, and glimpse the future of government interaction with its customers.

September 6 & 7

Hilton Richmond Hotel @ Short Pump

12042 West Broad Street, Richmond, VA 23233

Register Here: https://events.govtech.com/events/covits2012/reg

Virginia Information Technologies Agency

September ISOAG

1:00 – 4:00 pm at CESC

Wednesday - Sept 5, 2012

Topic: ***RSA – Advanced Persistent Threat***

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

IS Orientation Sessions

Tuesday - Aug 7, 2012 1:00 – 3:30p (CESC)

Email CommonwealthSecurity@VITA.virginia.gov if you are interested in attending.

IS Orientation also available via webinar!

Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to: **CommonwealthSecurity@VITA.Virginia.Gov**

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

Aug 1, 2012

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

ADJOURN

Source: www.pcmag.com