



# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

March 4, 2015



# ISOAG March 4, 2015 Agenda

- I. Welcome & Opening Remarks Mike Watson, VITA
- II. "Bad Advice, Unintended Consequences, Steve Werby, Fortune 500 Company and Broken Paradigms"
- III. ITRM SEC 514 Updates Bob Baskette, VITA
- IV. Mobile Device Security Compliance Bob Baskette, VITA
- V. Windows 2003 Server Update Bob Baskette, VITA
- VI. Windows XP Update Bob Baskette, VITA
- VII. Security Standards and Policy Committee Update Bob Auton, VITA
- V. Upcoming Events Bob Baskette/Michael Watson, VITA
- VI. Partner/Operation Update Bob Baskette, VITA, Michael Clark, NG



# Welcome and Opening Remarks

Michael Watson

March 4, 2015



Steve Werby, Fortune 500 Company,

"Bad Advice, Unintended Consequences,  
and Broken Paradigms"

March 4, 2015

Bad Advice,  
Unintended Consequences,  
and  
Broken Paradigms:

Think and  
Act Different

Steve Werby  
Researcher, Befriend  
Sec. Architect, F500 Co.  
COV ISOAG, March 4, 2015





goto fail; goto fail;

- Don't have a strategy
- Serve as an obstacle
- Don't engage our stakeholders
- Scream about irrelevant vulnerabilities
- Want to solve everything with shiny things
- Can't state how [in]effective we are
- But think we're right



# Disclaimer

“I am Jack’s raging bile duct.”

My Goal for You

Think and act different.

Do information security  
better.

Get better outcomes.

# Sneak Peak



! [0-day | worm | insecure

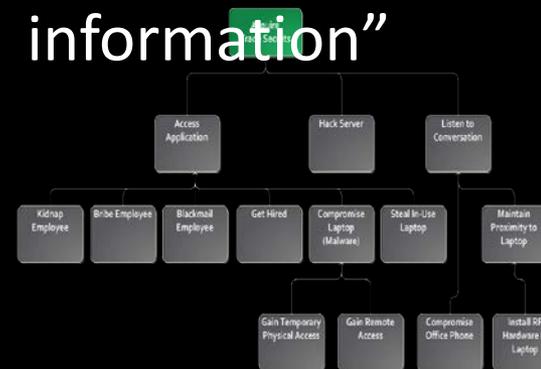
cy  
What if someone stole CEO's laptop while he was using it at the park?

Compliant, but weak, reused, and similar

Average # of days to patch a vulnerability

Deployment Rule Sets, EMET...

"I focus on measures that prevent a person from entering and forget to take measures that prevent a person from taking away information"



# What Information Security Is (Allegedly)

- Information security is the practice of defending information against unauthorized access, use, disclosure, modification, or destruction



# What Information Security Is (Really)

- Information security is the practice of defending information against unauthorized access, use, disclosure, modification, or destruction
- Information security is the defense of **information** and **IT systems** in alignment with **stakeholders'** direction for addressing **risk** and **opportunities**

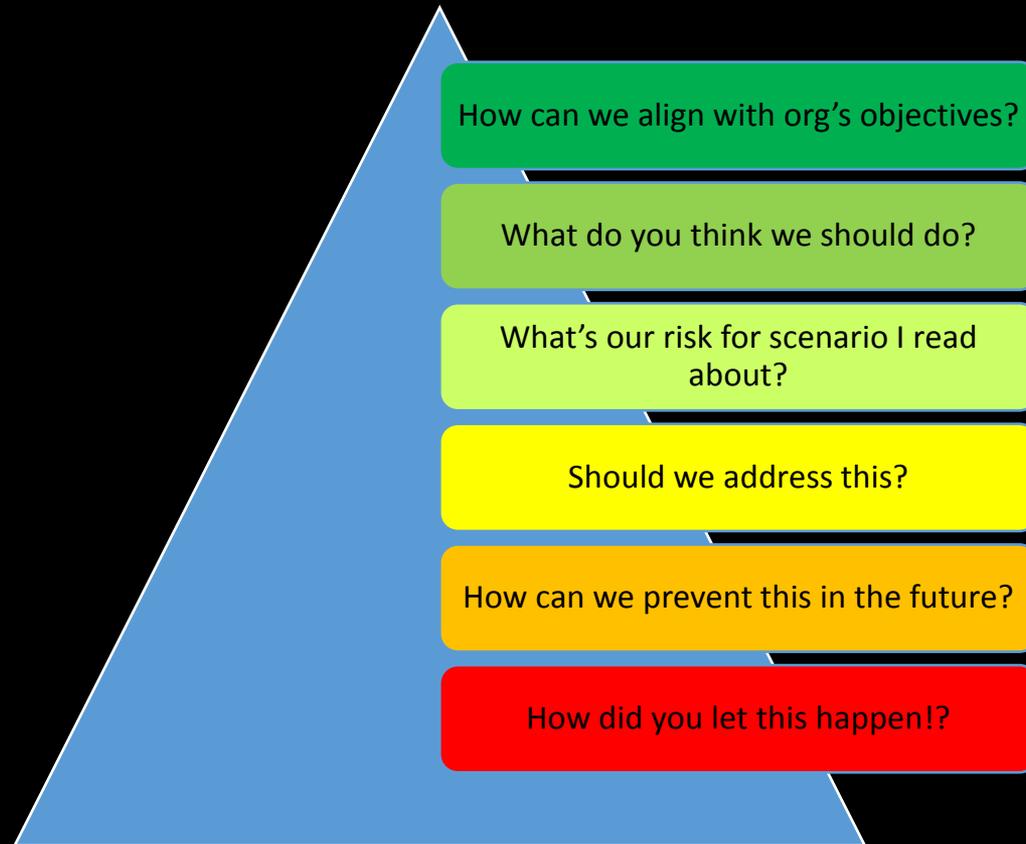
# What Information Security Is (Really)

- Information security is the defense of **information** and **IT systems** in alignment with **stakeholders'** direction for addressing **risk** and **opportunities**
- Breaking it Down
  - What information do we have?
  - What IT systems use it?
  - Who are stakeholders?
  - What are our risks?
  - What are our opportunities?

# Information Security Made Simple

- Do the basics (which work)
- Consider threats
- Have a target state
- Share gaps and share plan
- Share status
- Reassess
- Repeat

# The Stakeholder [Im]maturity Model



# We're Doing it Wrong

Jeweller's perspective on theft security	Common perspective on cyber security
I know which assets to protect and have set up the appropriate measures.	I take measures without a having a clear idea of the assets it is essential to protect.
I perceive theft as a risk in the business and know that realistically I can't be in business if I want 100% security.	I see cyber crime as something exotic and strive to achieve 100% security.
I focus on measures that prevent a person from leaving with valuable goods.	I focus on measures that prevent a person from entering and forget to take measures that prevent a person from taking away information.
I do not let security suppliers spook me and I make my own purchasing decisions.	My security policy depends on the tools available in the market place, without knowing exactly what I need.
When it goes wrong or almost goes wrong, I learn a lesson.	When it goes wrong or almost goes wrong, I panic.
I train employees in how to reduce the risk of theft and talk to them when they make mistakes.	I view cyber security as mainly a matter for specialist professionals and don't want to burden the rest of the organisation with it.
I invest in tools because they assist the continuity of my business.	I invest in tools because it is mandatory and because the media reports on incidents every day.

# Bad Advice – Passwords

- Make them complex
- Memorize them
- Change them regularly

# Unintended Consequences – Passwords

- ~~Make them complex~~
- ~~Memorize them~~
- ~~Change them regularly~~
  - Compliant, but weak, reused, and similar
  - Write them down, but poorly protected
  - Only if forced, increment/rotate
- Hard to guess
- Protect them
- Hard to crack the hash

# Think & Act Different – Passwords

- Make it loooooooooooooooooong
- Disallow common topologies<sup>1</sup>
- Require a Unicode character
- Audit them
- thinkandactdifferentinfosec
- ~~ullllldd~~
- passw?rd
- If too easily guessed, force change

<sup>1</sup> Source: “Pathwell Topologies” on KoreLogic Security Blog

# Broken Paradigms – Policy

- Legalese
  - Verbose
  - What to [not] do
  - Comprehensible
  - Retainable
  - What to [not] do and why
- 
- Great for CYA, but don't understand it, can't retain it
  - Don't read it
  - Don't know why and think we don't get it

# Think & Act Different – Policy

- Keep traditional policy if you want, but translate and/or create cheat sheet

Create a password which isn't guessable by someone who knows you or is similar to one you currently or previously used here or anywhere else. Protect it by never sharing it with ANYONE, being wary of phishing attacks, and by memorizing it or writing it down in securely.

Adversaries are good at tricking people and using their knowledge of typical approaches for constructing passwords.

Don't let them gain access to your personal accounts and info or the company information you have access to.

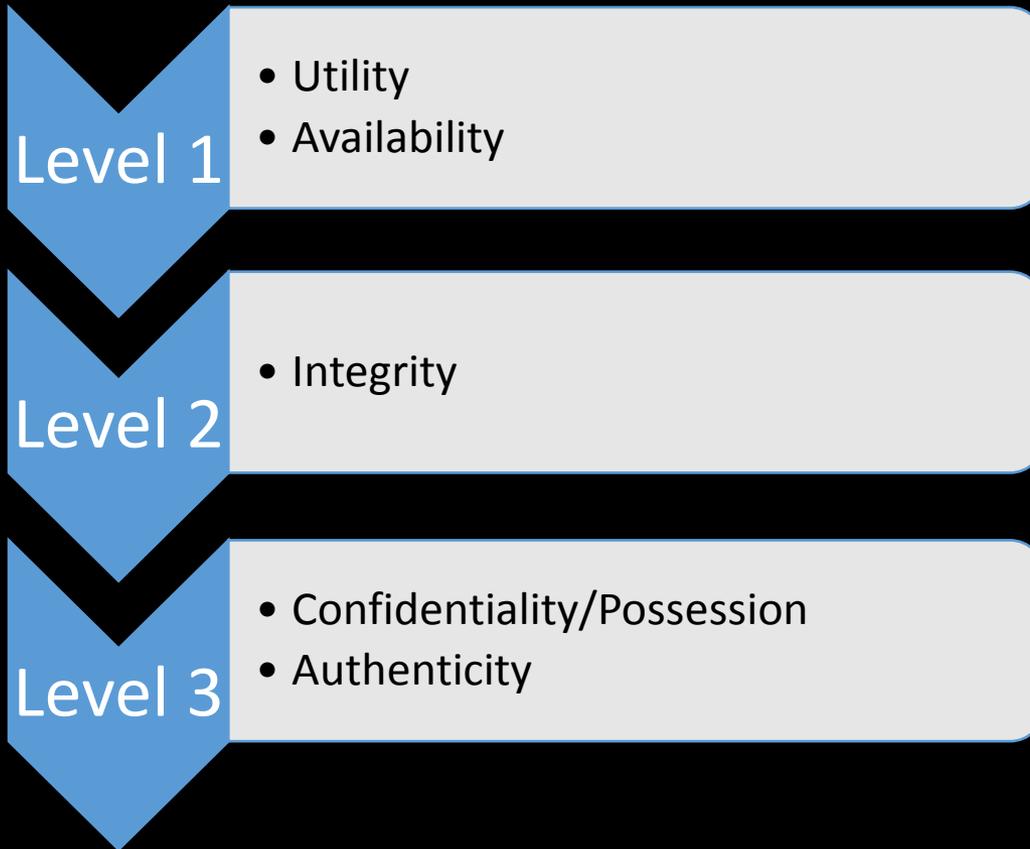
# Broken Paradigms – CIA Triad



# Broken Paradigms – CIA Triad



# Werbian Quintet





# Broken Paradigms – The Quartet of Doom

Passwords

Firewalls



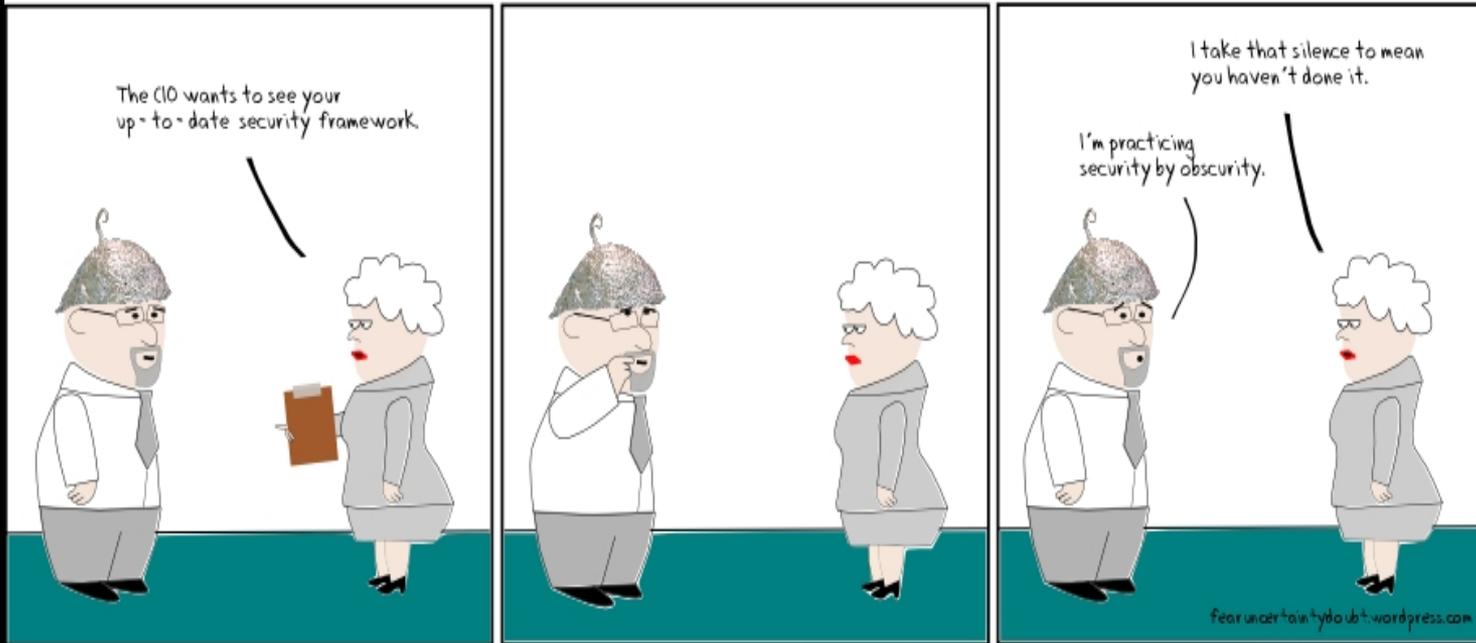
OS Patching

Antivirus

“I am Jack’s cold sweat.”

# If This is You, You're Doing it Wrong!

F.U.D.



# If This is You, You're Doing it Wrong!

USER FRIENDLY by J.D. "Illiad" Frazer

Please create a password.

\*\*\*\*\*

Password strength: Weak  
Please try again.

TAP TAP TAP TAP TAP TAP  
TAP TAP TAP TAP TAP  
SHIFT TAP TAP TAP  
TAP TAP



\*\*\*\*\*

Password strength: Mediocre  
Please try again.

TAP SHIFT TAP TAP SHIFT TAP SHIFT  
TAP TAP TAP SHIFT TAP TAP TAP TAP  
SHIFT TAP SHIFT TAP TAP TAP TAP  
TAP TAP SHIFT TAP



\*\*\*\*\*

Password strength: Adequate  
Thank you for creating your  
password. You will be asked  
to change it tomorrow.



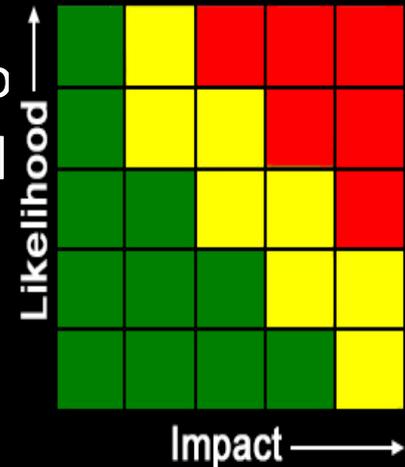
COPYRIGHT © 2007 J.D. "Illiad" Frazer [HTTP://WWW.USERFRIENDLY.ORG/](http://www.userfriendly.org/)

# Broken Paradigms – Vulnerability Management

- Unlocked, 20-year old, empty beaten up car in middle of full parking lot
- Unlocked house with \$10MM in diamonds in the middle of the desert and only 1 person knows it's there
- Context is critical
- Insignificant impact
- Improbable threat

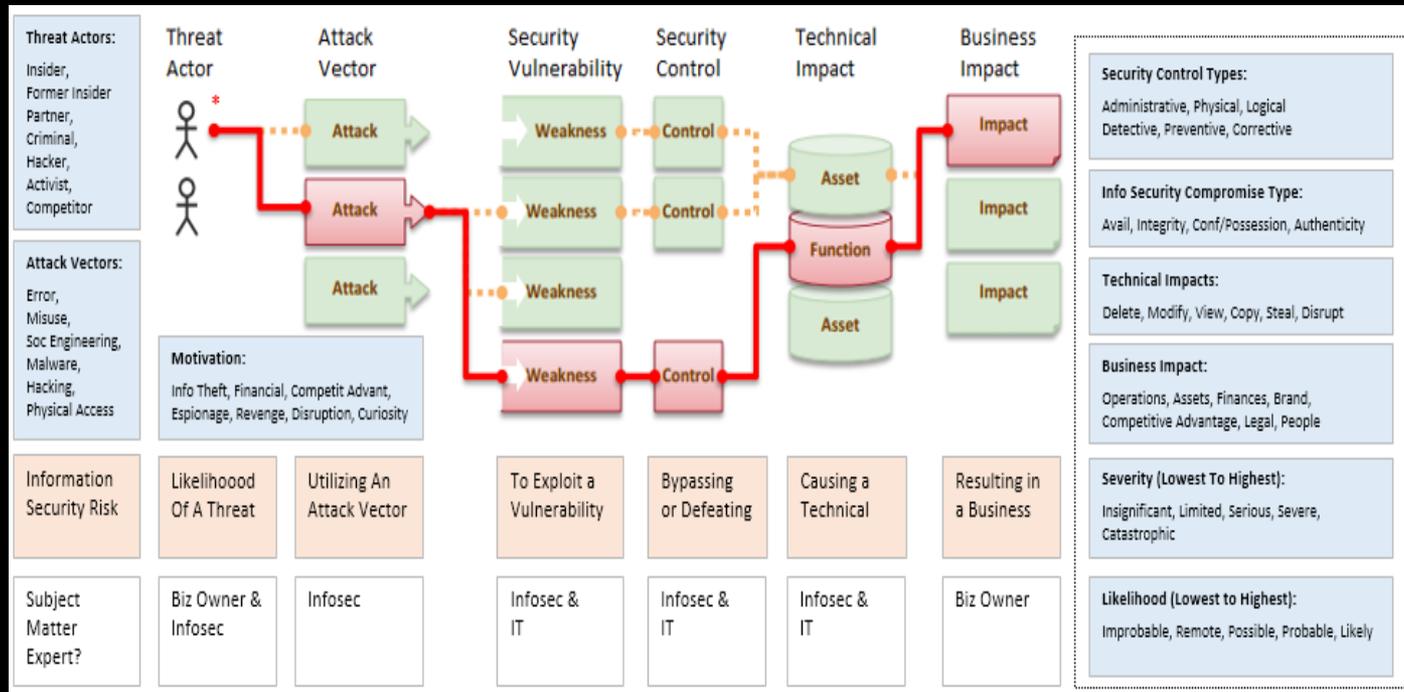
# Risk is This...Because Algebra

- $R = \text{Threat} * \text{Vulnerability} * \text{Impact}$
- $R = \text{Likelihood} * \text{Impact}$ 
  - Almost certainly a range of impact/likelihood
  - Likelihood of threat exploiting a vulnerability resulting in impact



“I am Jack’s wasted life.”

# Risk Assessment Model and Infosec Lexicon



- Iteration 1: Impacts and threats – impact, threat actor, likelihood
- Iteration 2: Exploitation likelihood – attack vectors, likelihood
- Iteration 3: Assessment of controls – controls, residual risk, risk appetite
- Iteration 4: Controls architecture – define controls, residual risk, risk appetite

# Threat Actor / Motivation Likelihood Matrix

		Motivation							
		Info Theft	Financial Crime	Competitive Advantage	Espionage	Revenge	Disruption	Curiosity	Do Job
Threat Actor	Insider	9	5	3	1	3	2	9	9
	Former Insider	7	3	1	1	5	3	3	0
	Partner	5	3	3	1	1	0	7	7
	Criminal	9	9	0	1	0	4	1	0
	Hacker	9	3	0	0	0	2	9	0
	Activist	3	0	0	0	5	7	1	0
	Competitor	1	0	2	3	2	2	5	0

Likelihood of Threat Actor Materializing		
Likely	9	90%
Probable	7	75%
Possible	5	60%
Remote	3	35%
Improbable	1	10%
Unicorny	0	~0%

# Think & Act Different – Ask Questions

(Direction)

- Are we meeting stakeholder expectations?
  - Who are our stakeholders?
  - What are their goals and concerns?
  - Are we helping them achieve their goals?
  - Are we reporting our progress?
  - Do they understand what we're telling them?
  - What has their feedback been?

# Think & Act Different – Ask Questions (Risk Scenarios)

- What if someone stole the CEO's laptop while he was using it at the park?
  - Are there preventive or detective controls in place?
  - Does he know who to contact?
  - Do you know what info and systems are accessible?
  - Is there an incident response plan for this scenario?
  - How long will the incident take to contain?

# Think & Act Different – Ask Questions

(Capabilities)

- What percentage of critical vulnerabilities for systems in our environment are exploited in the wild before we've remediated them? Exploited in our environment?
  - How does this compare to the previous quarter?
  - Patch frequency?
  - Target (and actual) turnaround between patch release and implementation?
  - How might we reduce this from X% to Y%?

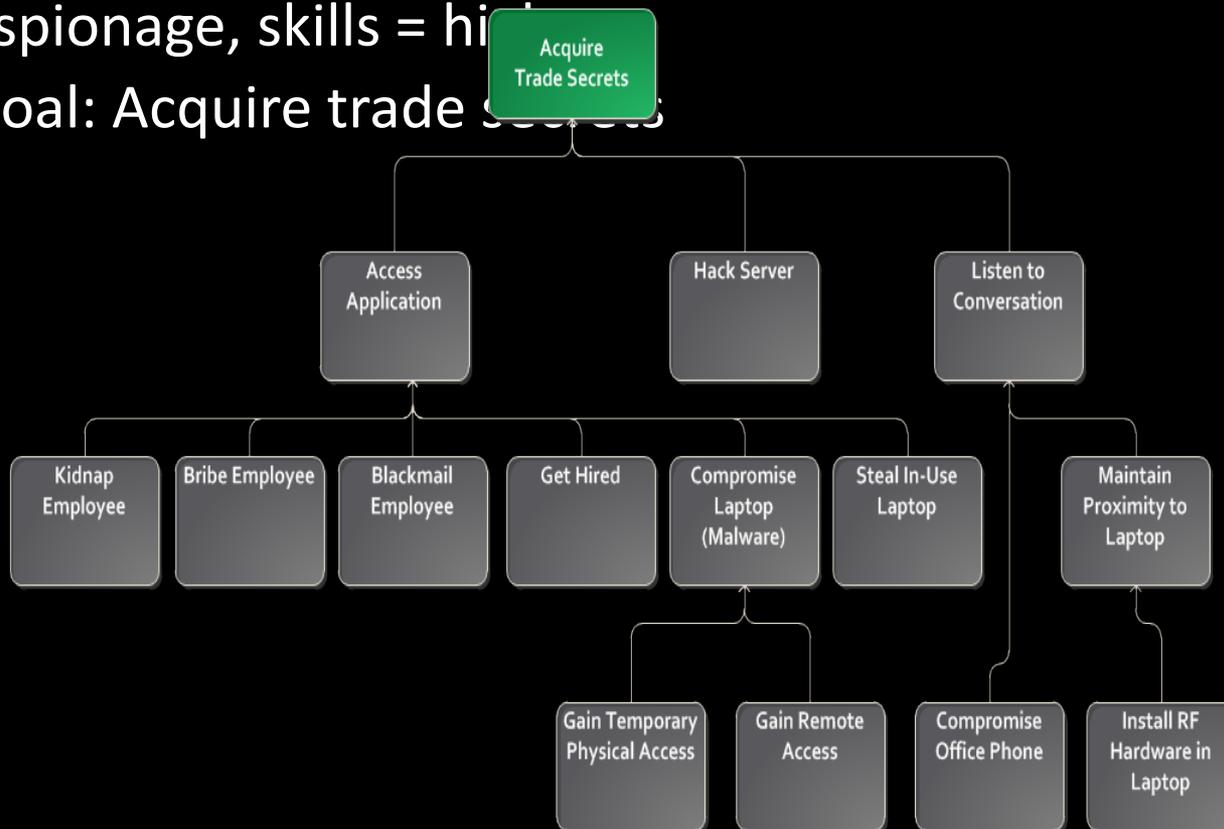
# Think & Act Different – Ask Questions

(Assessment of Controls)

- What if an attacker enumerated all of our AD accounts to intentionally lock them out?
  - Are there preventive or detective controls in place?
  - Do you know what the impact would be?
  - Is there an incident response plan for this scenario?
  - How long will the incident take to contain?
  - What was the objective of the control and is the objective being met?

# Think & Act Different – Attack Trees

- How can we better protect our CEO's devices when he travels to China?
  - Assumption: Threat actor = competitor, motivation = espionage, skills = high
  - Goal: Acquire trade secrets



# Think && Act Different – How Might We?

- Install RF hardware in laptop (or modify BIOS or modify a component)
- Ask yourself “How might we?”
- How might we:
  - Mitigate a HW modification?
  - Detect a HW installation?
  - Mitigate the risk after CEO’s return?
  - Tamper-proof tape
  - Weigh the laptop
  - Destroy laptop or sanitize and sell

# Think && Act Different – How Might We?

- Steal in-use laptop
- Ask yourself “How might we?”
- How might we:
  - Prevent it or mitigate it?
  - Not use it in public
  - Stay-alive code
  - Proximity device to trigger logout

“I am Jack’s epiphany.”

# Think && Act Different – Assume Failure

- Before a project, initiative, or major change, assume it will fail
  - Do individually, more than one individual, discuss
  - Ideally seek input from range of stakeholders
  - Acknowledge risks and issues and account for if appropriate

# Think & Act Different – Metrics

- Average # of days to patch a vulnerability
- # of people who opened phishing security awareness communication
- % of web apps with VAs performed last year

# Think & Act Different – Metrics

- ~~Average # of days to patch a vulnerability~~
- ~~# of people who opened phishing security awareness communication~~
- ~~% of web apps with VAs performed last year~~
- Describe outcomes, capabilities, or progress towards target state
- Answer questions or allow you to formulate new questions
- Are meaningful and actionable
- % of vulns patched after threshold & median days > threshold
- % of users exhibiting undesired phishing response by awareness status
- % of web apps with VAs having repeat OWASP Top 10 findings

# Think & Act Different – Understand Stakeholders

- Identify stakeholders
- Define roles
- Understand goals/needs
- You, CFO, CIO, Audit, Law, Owner, User
- RACI model
- CFO – fiscal responsibility, ROI  
CIO – deliver value, cut costs  
Audit – assurance of controls  
User – effectiveness, efficiency

# Think & Act Different – Engage Stakeholders

- Establish channels
- Speak their language
- Educate them
- Concise, defensible
- Choices
- Formal group, leverage group, survey
- ! [0-day | worm | insecure]
- Lexicon, role, bidirectional collaboration
- Strategy, roadmap, progress, risk environ
- Menu, considerations, likely outcomes

# Think & Act Different – Get What You Want

- Make it benefit them
- Longer password by giving up expiration
- Reduce patch frequency if implement app whitelisting and DLP
- Less restrictive content filtering if demonstrate acceptable security behavior

# Think & Act Different – Gorge on Data

## ■ You'll find:

- Baselines
- Patterns
- Correlations
- New questions to ask
- ECM documents accessed daily by user
- 19% of users' passwords are ULLLLLLNS
- 317% more likely to forget password if changed entering weekend, holiday, or vacation
- What are USB flash drives being used for?

# Broken Paradigms – The Quartet of Doom

Passwords

Firewalls

Prevent  
authorized access

Barricade  
vulnerable systems



Reduce  
exploitation

Detect  
malicious code

OS Patching

Antivirus

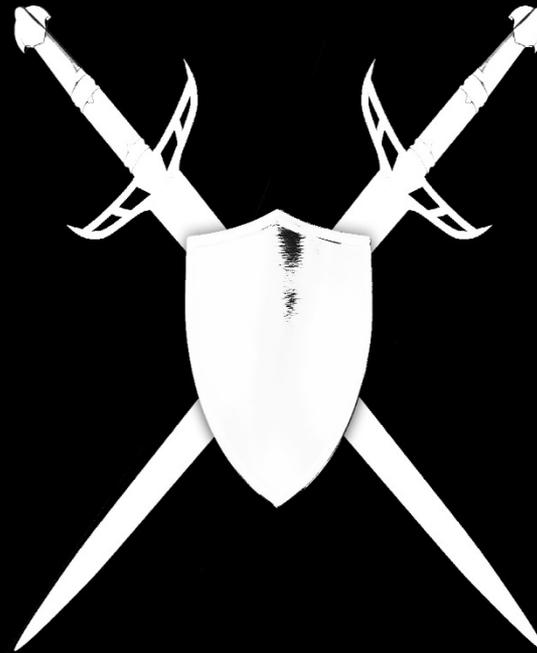
# The Quartet of Potential Hope and Lower Discontent

~~OTPs Passwords~~

~~Firewalls~~ Anomaly Detection

Prevent  
authorized access

Barricade  
vulnerable systems



Reduce  
exploitation

Detect  
malicious code

~~Mitigate Java OS Patching~~

~~Antivirus~~ Malware Sandboxing  
(or App Whitelisting)

# Broken Paradigms – The Quartet of Doom

Control	Success Confidence	Risk Mitigation	User Friction	Implement Burden	Govern/Admin Burden	Org Friction	Cost
✓ Passwords	2*	3	3	-	1	3	1
OTPs	4	4	2	3	4	4	4
Firewalls	1	2	5	-	1	1	1
Anomaly Detection	2	4	3	5	1	4	2
✓ OS Patching	3	1	3	-	3	3	2
Mitigate Java	5	5	5	2	5	5	1
Antivirus	2	1	3	-	2	4	2
Malware Sandbox	3	3	5	2	4	5	3

\* For this model, 1 is equivalent to “Least Desirable” and 5 is equivalent to “Most Desirable”



# Yes, You Can Tame Java

- Deployment Rule Sets (then you can actually patch too!)
  - Install multiple versions of Java per device
  - Limit which applets and applications end user can execute
  - Limit which version of Java is associated with each
- Block User Agent for Java at proxy
  - Query proxy logs for visited hosts that used Java user agent
  - Aggregate by host, sort by frequency, analyze
  - Generate exclusions
  - Attacker can not modify the user agent before exploit attempt
  - Prevents web-based attacks against all operating systems

# Yes, You Can Tame Java

Option	Risk Mitigation	Implement Burden	Govern/Adm in Burden	User Friction
Deployment Rule Sets	H	M	L	L
Patch Acceleration	M	M	M	M
Block Java at Proxy	H	L	L	L
EMET to Protect Java	H	L	L	L

Implementation order

- Block Java at proxy
- EMET to protect Java
- Deployment Rule Sets
- Patch acceleration

# Think & Act Different – Start \*Somewhere\*

- Where?
  - Easiest? Highest value? With person who raises hand?
  - May not be your call
  - Could be based on surprise opportunity
- Be prepared
  - Incident in your environment
  - Incident elsewhere
  - Inquiry from stakeholder
- Crawl, walk, run – gain experience and learn lessons



# Think && Act Different – Start \*Somewhere\*

- Scenario: Single enterprise-wide weak Local Admin password (LA PW) which hasn't been changed in years and was poorly controlled
- Document risk, share options with stakeholders
- Change it to an acceptable password && implement governance
- Create unique LA PW for segments of population
- Create unique LA PW for each device based on root + device attribute
- Create unique random LA PW for each device via PW escrow tool
- Eliminate use of the LA PW
- (Potential use of PIM technology)



# Think & Act Different – Step Out of the Echo Chamber

- Infosec is a field comprised of numerous disciplines
- Social engineering => psychology, marketing, data analytics
- Infosec
  - Risk mgmt
  - Strategy
  - Negotiation
  - Statistics
  - Probability
  - Data analytics
  - Psychology
  - Marketing
  - Education
  - Law
  - Privacy
  - Fraud prevention
  - Finance
  - Human factors engr
  - Operations research
  - Military science
  - Safety

# Think & Act Different – Equal Treatment Not Required

- Some people are riskier
  - Based on system/data access
  - Role/visibility
  - Security hygiene
  - Disgruntled/disciplined/separating
  - Internet presence
- It's OK to treat them differently
  - Different training
  - Different detective and preventive controls
  - If a systems' users are higher risk, so is the system (inherited risk)

# If This is You, You're Doing it Wrong!





# The Challenge

Think and act different.  
Share your experiences.  
Do information security  
better.  
Get better outcomes.

Bad Advice,  
Unintended Consequences,  
and  
Broken Paradigms:

Think and  
Act Differently

Questions? Ideas? Thoughts?

 @steview  
 Steve  
 Steve  
by

Steve Werby  
Researcher, Befriend  
Sec. Architect, F500 Co.  
COV ISOAG, March 4, 2015



*Virginia Information Technologies Agency*

# ITRM SEC 514 Updates

Bob Baskette

Director, Security Architecture,  
Compliance, and Incident  
Management



## ITRM SEC 514 Updates

- SEC 514 requires that all electronic media containing Commonwealth data, whether stored on Commonwealth assets or that of a service provider, shall have all of that Commonwealth data securely removed from the electronic media before the electronic media is surplus, transferred, traded-for, otherwise disposed of, or replaced.



## ITRM SEC 514 Updates

- The Commonwealth's Removal of Commonwealth Data from Electronic Media standard (ITRM SEC514) will be updated to address new technologies.
  - Multi-Function devices
  - Solid State Drives
  - Mobile Devices
  - Cloud-based Resources (eGOV Vendors)



## ITRM SEC 514 Updates

- Best Practices will be updated to:
  - Ensure that the standard addresses uncommon storage devices that may contain sensitive information so that those devices will be including in the sanitization process.
  - Document a decision tree that can inform agencies as to which sanitization method to use for different types of data classifications.



## ITRM SEC 514 Updates

- Best Practices will also be updated to:
  - Provide a thorough sanitization guidance based on device type, data type and disposal method to include reuse, repurpose, and auction at the end of their useful cycles.
- The updated standard should be on OCRA at the end of March for comment.



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



# Mobile Device Security Compliance

Bob Baskette  
Director, Security Architecture,  
Compliance, and Incident  
Management



## Background

- Mobile devices that access, process, or store Commonwealth data must adhere to the Commonwealth Security Standard as well as the applicable Mobile Device Policy.
- If the device contains or accesses Commonwealth data it must be updated to address known software vulnerabilities.



## Background

- The Commonwealth Security Standard requires that all devices apply available security patches within 90-days of release by the software vendor.
- The Enterprise Mobile Device Policy requires that all devices apply available security patches within 30-days of release by the software vendor.



## Background

- The reduction in the remediation window for mobile devices is due to the increased risk imposed by the mobile device.
- As the name implies, mobile devices are very mobile and are often lost, misplaced, or simply stolen.



## Report on Compliance

- Both the Air Watch and Good Technology services provide a mechanism to determine the patch level of a mobile device each time the device connects to the service.
- The mechanism records the device ID, the device operating system version, the user-id associated with the device, and the last check-in date and time.



## Report on Compliance

- Commonwealth Security is working with Northrop Grumman to determine if an agency-specific report can be generated on a monthly basis and stored on the PSO SharePoint site.
- Until that report is ready, CSRM will generate the agency-specific report from the Enterprise report and forward the data to each ISO once a month.



## Agency Responsibilities

- CSRM requests that each agency ISO review the monthly report to determine if any devices used within the agency require a software update. The report will contain the current supported version of each operating system in the first three rows of the report.



## Agency Responsibilities

- If a device requires a software update, please ask the person associated with the device to preform the software update within the 30-day patch window allowed by the Mobile Device Policy.
- CSRM will allow an agency a 90-day grace period to bring a device into compliance if the patching process would impact business functions.



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



# Windows 2003 Server Update

Bob Baskette  
Director, Security Architecture,  
Compliance, and Incident  
Management



## Windows 2003 Server Update

- Windows 2003 Server will reach End-of-Life on 7/31/2015.
- The server migration project will attempt to upgrade the Windows 2003 servers to Windows 2012 Server prior to 7/14/2015.



## Windows 2003 Server Update

- Windows 2008 R2 Server will be offered as an option for applications not compatible with Windows 2012 Server.
- Each Agency must stipulate the future of each Windows 2003 server as soon as possible.



## Windows 2003 Server Update

- To utilize Windows 2003 Server after 7/31/2015, agencies must submit the following items prior to 5/1/15:
  - Security Exception to CSRM
  - Work request for ESOSS to their CAM
- Any server listed on the work request can be removed if decommissioned prior to 7/31/2015.



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



# Windows XP Update

Bob Baskette  
Director, Security Architecture,  
Compliance, and Incident  
Management



## Windows XP Update

- Microsoft Windows XP reached End-of-Life on 4/08/2014.
- Microsoft has stated that all security patch activities will end on 3/31/2015 and that no security patches will be available after 3/31/2015.



## Windows XP Updates

- All Windows XP should be decommissioned by 3/15/2015.
- Any Windows XP system still performing a critical business function on that date will require a new security exception and must be placed behind a managed firewall.



## Windows XP Updates

- Please contact your CAM to submit a work request for the managed firewall service.
- Each network segment containing a XP system will require a dedicated managed firewall.
- Please contact Commonwealth Security to submit a new security exception.



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



# Security Standards and Policies Committee Update

Bob Auton  
VITA

---

March 4, 2015



## IT Security Standards and Policies Committee

The IT Security Standards and Policies was selected from the six Potential 2014 Information Security Council Committees by the ISOAG Attendees at the November 2013 ISOAG Meeting.

We are fortunate that Grayson Walters, ISO for the Department of Taxation and also a member of the Commonwealth Information Security Council has volunteered to Chair the IT Security Standards and Policies Committee.



## Committee Objective and Deliverables

### **Security Standards and Policies Committee Objective:**

Charged with reviewing and making recommendations to the Commonwealth regarding IT Security Policy and Standards.

### **Planned Deliverables:**

1. Create a vehicle to assist in a practical implementation & adherence.
2. Survey for COV agencies to determine usability.
3. Develop IT Security Policy and Standards Review Process.
4. Provide recommendations to CISO.



## Committee Information

Generally an IS Council Committees will:

- Have 5 to 10 volunteer members
- Usually meet every other month
- Ensure deliverables are achieved in 6 –12 months



## Next Step for Committee

Due to unforeseen circumstances the Security Standards and Policies Committee did not get the opportunity to solicit volunteers from the ISO Community during 2014.

We need volunteers like you to be a part of the Security Standards and Policies Committee!!!

To volunteer please send an e-mail to:

[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Or directly to

[Grayson.Walters@tax.virginia.gov](mailto:Grayson.Walters@tax.virginia.gov)



# Questions

## Questions?

You may also send any questions to :  
[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



Virginia Information Technologies Agency

# Upcoming Events





## VT Hosting SANS class in March

- SANS SEC 511 "Continuous Monitoring & Security Operation", general course description is at <http://www.sans.org/course/continuous-monitoring-security-operations>. Chris Crowley will be the instructor.
- \$1800/person for EDU (Higher Ed, Community College, K-12, any .EDU) or state/local govt employees. \$5140 - full price for commercial or federal govt employees.

[www.cpe.vt.edu/isect](http://www.cpe.vt.edu/isect). This site contains the class info and registration information.



## VT Hosting SANS class in March

March 9-14, 2015, 0900-1730

2150 Torgersen Hall, VA Tech, Blacksburg, VA 24060

REGISTRATION OPTIONS:

ONLINE (vLive) OPTION: If you plan on taking the class remotely, register at

<http://www.sans.org/onsite/details/38407>. Use the

DISCOUNT CODE: **PART\_38407** to get the **\$1800/person price**.

ONSITE: [www.cpe.vt.edu/isect](http://www.cpe.vt.edu/isect). No discount code needed for onsite class.



## IS Orientation

**When: Thursday, March 19th, 2015**

**Time: 10:00 am to 12:00 pm**

**Where: CESC , Room 1211**

**Register here:**

**<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>**



## Conference Statement

### IT Security Conference

### *“Unifying the Business Enterprise”*

- In addition to hearing expert presentations and sharing ideas with fellow managers, auditors and technical professionals around this theme, conference participants will have the opportunity to:
- **Expand their professional networks.**
- **Learn about security products and services.**
- **Maintain professional certifications.**



# 2015 IS Security Conference

*COV Information Security Conference*

*April 2-3, 2015*

*Richmond, VA*



## Conference Statement

### IT Security Conference

### *“Unifying the Business Enterprise”*

- In addition to hearing expert presentations and sharing ideas with fellow managers, auditors and technical professionals around this theme, conference participants will have the opportunity to:
- **Expand their professional networks.**
- **Learn about security products and services.**
- **Maintain professional certifications.**



## Who Should Attend

### IT Security Conference

### *“Unifying the Business Enterprise”*

- Information Security Officers
- Information Security Analysts and Engineers
- Chief Information Officers
- IT Auditors
- Privacy Officers
- Risk Officers
- Other IT officers, managers, and staff with an interest in security or privacy

## Keynote Speaker – April 2, 2015

### IT Security Conference "Unifying the Business Enterprise"



**Michael Fey**

**President and Chief  
Operating Officer  
BlueCoat**



## Lunch Time Speaker – April 2, 2015

**IT Security Conference**  
*“Unifying the Business Enterprise”*



**Governor**  
**Terry McAuliffe**



## Keynote Speaker – April 3, 2015

### IT Security Conference *“Unifying the Business Enterprise”*



**Karen Evans**  
**Director for the US Cyber Challenge**  
**(USCC).**

## Lunch Time Speaker – April 3, 2015

### IT Security Conference *“Unifying the Business Enterprise”*



**Karen Jackson**  
**Secretary of Technology**



# Conference Topics Day One

Dan Han (VCU) - Managing regulatory compliance in a non-compliant world

Tom Bowers ((ePlus) - The Shared ISO model

Karen McDowell (UVA) - Business, Information Security, and the Internet of Things

Shana Bumpas (TAX) – PCI

Scott K. Hammer ( Driving Value with Information Security Compliance

Jean Rowe (Bitreserve Inc) - ORMS Bootcamp

Andrea Di Fabio (NSU) - Sharing sensitive information in a more secure manner

Doug Streit (ODU) - IT Security Governance - One ISO's journey

**Note: Topics are subject to change prior to conference**



# Conference Topics Day One (Con't)

Michael Light (AT&T) - BigData and (In)Security Considerations

Randy Marchany (VTECH) - Continuous Monitoring Challenges

Peter Allor (IBM) - Security Threats, Frameworks, and Mitigation Efforts How  
Can You Lower Your Risk?

Eric Adkins (Verizon) - Data Breach Security

**Note: Topics are subject to change prior to conference**



## Conference Topics Day Two

Peter Aiken (VCU) - Data - How can you secure it if you can't manage it?

Lorne Joseph (eGRC.COM) - Bringing Governance to Government

Hemil Shah (eSphere Security Solutions Pvt Ltd) - Stop throwing generic security requirement - Who has time!!!

Chandos Carrow (VCCS)- Vulnerability Scanning

Eric Bowlin (Deloitte) - Into the Cyber Security Breach

Karen L. Cole (Assura, Inc.) - Enterprise Risk Management (ERM): Unifying the Organization and Improving Performance Through Shared Management of Risks

Michael Bruemmer (Experian) - Data Breach Resolution Lessons Learned from Mega Breaches

Katie Hutchison (Box) - Cloud as a Security Solution

Jake Kouns - Risk Based Security Vulnerability Stupidity: How Do We Move Towards Intelligence?

**Note: Topics are subject to change prior to conference**



## Vendor Attendees

### IT Security Conference

*“Information Security Enabling the Business”*

**Verizon**  
**Appscour**  
**CAS Severn**  
**Chenega Logistics**  
**Assura Inc.**  
**Sun Management**

**ePlus Technology**  
**Cisco**  
**SHI**  
**Awareity**  
**Data Network**  
**Solutions**  
**FishNet Security**



## Registration Cost

### IT Security Conference *“Unifying the Business Enterprise”*

Registration fee: \$125.00 for Attendees

*Note: Space is limited. Please register early.....*



## How To Register

### IT Security Conference *“Unifying the Business Enterprise”*

You may register for the conference at the following link:

**Website Link:**

<http://www.vita.virginia.gov/2015COVASECURITYCONFERENCE/>



## Payment Method

### IT Security Conference *“Unifying the Business Enterprise”*

You may pay for the conference by: **Credit Card**  
**Check (make payable to VCU  
Conference Services)**

If you have questions, contact:  
**CommonwealthSecurity@vita.virginia.gov**



## Future ISOAG

**April 1st, 1:00 - 4:00 pm @ CESC**

**Speaker: Peter Allor, IBM**

*ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2015*



## 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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)

# ADJOURN

## THANK YOU FOR ATTENDING

