



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

September 4, 2013



ISOAG September 2013 Agenda

- | | | |
|------|-------------------------------------|---|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | China's Computer Network Operations | Dr. Larry Worzel,
Asia Strategies & Risk, LLC |
| III. | Cyber Security Awareness Month | Ed Miller, VITA |
| IV. | Commonwealth Data Points | Ed Miller, VITA |
| V. | Application Testing Via Fuzzing | Bob Baskette, VITA |
| VI. | Upcoming Events & Other Business | Michael Watson, VITA |
| VII. | Partnership Update | Bob Baskette, VITA
Julia Reisenwitz, Casey Rhoton
Michael Clark, NG |



China's Computer Network Operations

- Dr Larry Wortzel, President
Asia-Strategies and Risks, LLC

U.S.-China Economic and Security Review Commission Legislative Mandate

- Created by Congress in October 2000 by the Floyd D. Spence National Defense Authorization Act.
- PNTR drove the decision
- Established to monitor, investigate, and submit to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China.
- Report annually on eight issue areas: (1) proliferation practices, 2) economic transfers, 3) energy, 4) access to capital markets, 5) regional economic and security impacts, 6) bilateral programs, 7) WTO compliance, and 8) freedom of expression.

Commissioners

Speaker Boehner

- 1) Larry Wortzel
- 2) Dan Slane
- 3) Peter Brookes

Leader Pelosi

- 1) Carolyn Bartholomew
- 2) Michael Wessel
- 3) Jeff Fiedler

Senate Majority Leader Reid

- 1) William Reinsch (Chairman)
- 2) Sen. Carte Goodwin
- 3) Katherine Tobin

Leader McConnell

- 1) Dennis Shea (Vice Chairman)
- 2) Sen. Jim Talent
- 3) Robin Cleveland

Objectives for China's Malicious Cyber Activities

1. **Strengthen domestic control** – bolster the CCP's, detect dissent
2. **Collect intelligence** – gather economic, military, or technical information
3. **Prepare attacks** – reconnoiter, map, and gather targeting information on foreign military, government, civil infrastructure, or corporate networks
4. **Steal IP** for Chinese companies/defense use

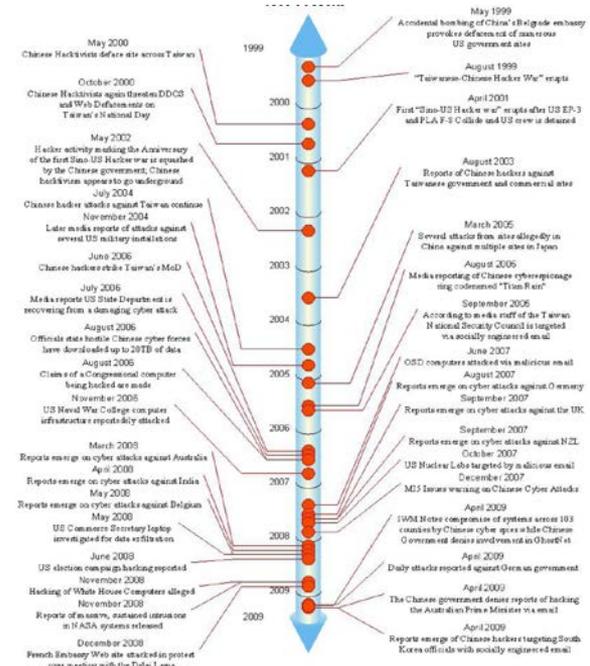
Cyber Espionage vs. Cyber War

Both map, catalogue, and identify sources and targets

- Identify key nodes (people or IT networks)
- Penetrate and take control of part of the network (person)
- Extract data or insert data
- Cyber espionage targets parallel traditional espionage targets
- More data more quickly with cyber

Timeline on Chinese cyber

- ▶ Post 1991: PLA reflects on the first Gulf War
- ▶ ~1993: PLA prepares for “high-tech” war
- ▶ Late 1990’s: PLA debates information war
- ▶ 1999-2001: China weighs the utility of popular “Hactivism”
- ▶ ~2002: PLA prepares for “informationalized” war
- ▶ ~2007-8: Original operational concepts take root



Thumbnail source: NGC for USCC 2009

Intelligence Entities (Civilian)

PRC Security, Foreign Intelligence & Technology Collection Agencies	Institutional Subordination	Primary Missions
Ministry of State Security	PRC State Council/ CCP Politburo Politics and Law Committee	<ul style="list-style-type: none"> • Foreign intelligence collection • Intelligence analysis • Counterintelligence • Suppression of dissident groups
Ministry of Public Security	PRC State Council/ CCP Politburo Politics and Law Committee	<ul style="list-style-type: none"> • Domestic security operations/law enforcement • Counterintelligence
CCP International Liaison Department	CCP Central Committee ¹	<ul style="list-style-type: none"> • Liaison with foreign political parties • Influence operations • Intelligence collection
CCP United Front Work Department	CCP Central Committee ¹	<ul style="list-style-type: none"> • Liaison with non-Communist Chinese groups • Influence operations • Intelligence collection
Various Civilian Scientific Research & Development Institutions	Chinese Academy of Sciences (primary)	<ul style="list-style-type: none"> • Technology acquisition

Intelligence Entities (Military)

PRC Security, Foreign Intelligence & Technology Collection Agencies	Institutional Subordination	Primary Missions
Second Department, PLA General Staff Department (Military Intelligence)	PLA General Staff Department	<ul style="list-style-type: none"> • Foreign intelligence collection (especially military data) • Intelligence analysis • Technology acquisition
Third Department, PLA General Staff Department (Signals intelligence)	PLA General Staff Department	<ul style="list-style-type: none"> • Signals intelligence collection and analysis • Cyber intelligence collection and analysis
Fourth Department, PLA General Staff Department (Electronic Warfare)	PLA General Staff Department	<ul style="list-style-type: none"> • Electronic warfare (jamming, etc.) • Computer network attacks
International Liaison Department, PLA General Political Department	PLA General Political Department	<ul style="list-style-type: none"> • Foreign intelligence collection • Political/psychological warfare
Various Defense Industrial Firms	11 different state-owned defense enterprise group companies	<ul style="list-style-type: none"> • Technology acquisition

Who is involved in Cyber Penetration in China?

MILITARY:

- Third Department (3PLA)
- Fourth Department (4PLA)
- Military Services (PLA Navy, PLA Air Force)
- Technical Reconnaissance Bureaus (TRBs)
- Cyberwarfare Militias

INTELLIGENCE/SECURITY:

- Ministry of Public Security
- Ministry of State Security

“INDEPENDENT”:

- “Hacktivists”
 - (e.g. Patriotic hackers)
- For-profit hackers
 - (e.g. Criminal groups)

“CORPORATE”:

- Information and communications technology (ICT) providers
- Other state-owned or controlled Industries?
 - (e.g. “Strategic industries”?)

Where are the Military Units Located?

Suspected PLA Technical Reconnaissance Bureaus (TRBs)

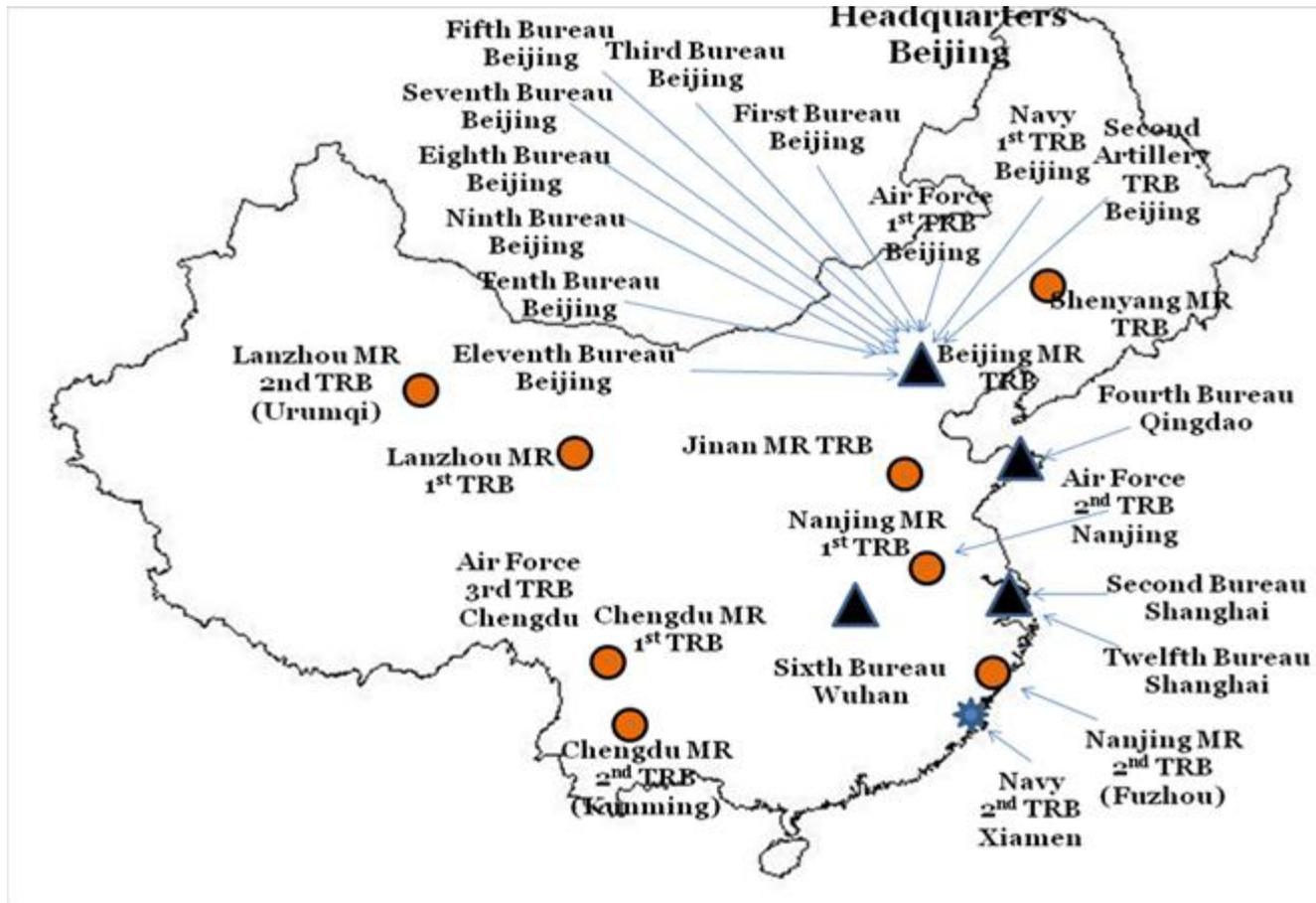


Image source: Project 2049 Institute 2011

How the Operate

YOUR NETWORKS:

- ▶ Target the high and low ends of the company (organization)
- ▶ Social engineering of attacks
- ▶ Targeted phishing
- ▶ Personal accounts and systems (including social media and mobile devices)
- ▶ High value nodes
- ▶ High traffic nodes

ADJACENT & UPSTREAM NETWORKS:

- ▶ Associates & contractors
- ▶ Service providers (Internet? Data centers? “Cloud” systems?)

Command, control, and staging can be located anywhere; but eventually may control a network

Top Targets

GENERAL:

- ▶ Information and communications technology
- ▶ Military (marine, aerospace)
- ▶ Civilian and dual-use (advanced materials and manufacturing, pharmaceutical, agricultural technologies)
- ▶ Business information (energy and resources, business deals, macroeconomic information)

MILITARY:

- ▶ Information systems
- ▶ Lasers, optics, and sensors
- ▶ Aeronautics systems
- ▶ Electronics
- ▶ Marine systems (propulsion and weapons control)
- ▶ PNT
- ▶ Information security
- ▶ Armaments and energetic materials
- ▶ Space and ground systems

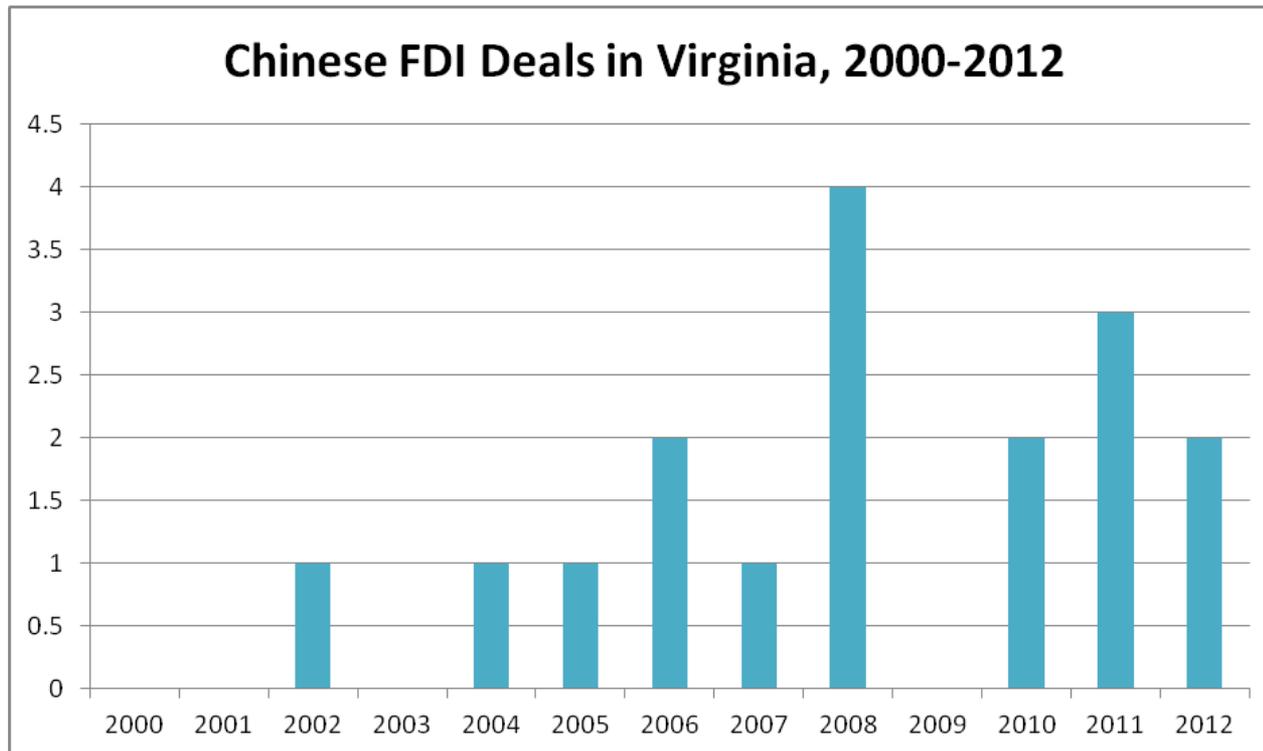
Sources: NCIX 2011, DSS 2011

Chinese Investment in Virginia by Year, Sector, and Deal, 2000-2012

Chinese FDI Deals and Total Investment in Virginia by Year, 2000-2012

Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	TOTAL
Number of Deals	0	0	1	0	1	1	2	1	4	0	2	3	2	17
Total Investment (millions)	\$0	\$0	\$13	\$0	\$3	\$1	\$2	\$1	\$15	\$0	\$1,633	\$11	\$16	\$1,695

Source: Rhodium Group China Investment Monitor: <http://rhg.com/interactive/china-investment-monitor>



Chinese Investment in Virginia, 2000-2012

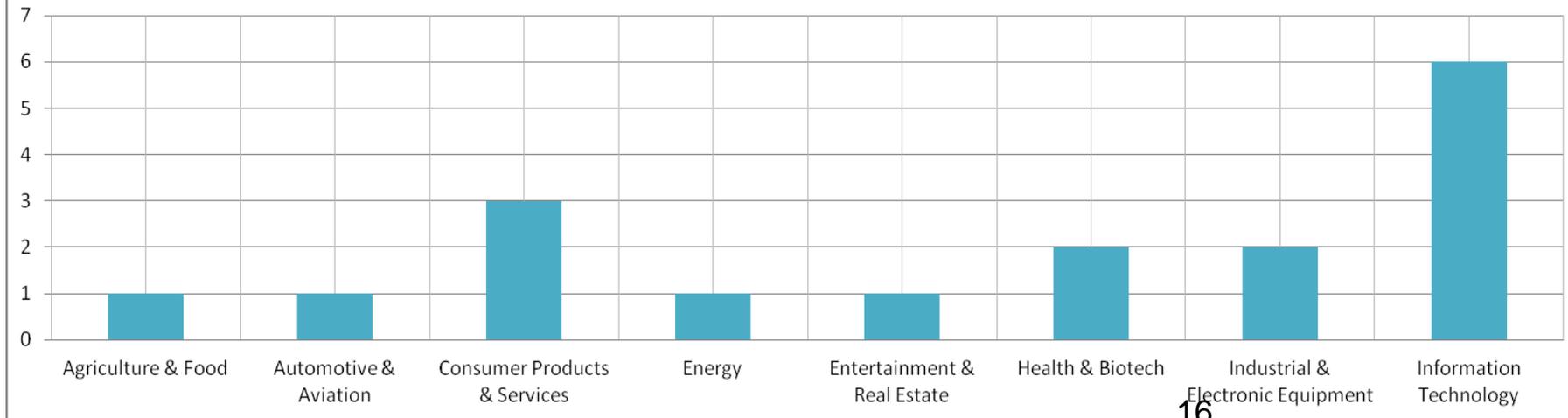
Deals and Percentage Invested by Sector

Chinese FDI in Virginia by Sector, 2000-2012

Sector	Deals	Quantity (millions)	Percentage of Total Quantity
Agriculture & Food	1	\$3	0.2%
Automotive and Aviation	1	\$3	0.2%
Consumer Prod. & Serv.	3	\$15	0.9%
Energy	1	\$1,581	93.3%
Entertain. & Real Estate	1	\$52	3.1%
Health & Biotech	2	\$6	0.4%
Ind. & Electronic Equip.	2	\$3	0.2%
Information Technology	6	\$32	1.9%
TOTAL	17	\$1,695	100.00%

Source: Rhodium Group China Investment Monitor

Chinese FDI Deals in Virginia by Sector, 2000-2012



Chinese Companies in Virginia

- ▶ China Telecom (2008), \$2m, IT , corporate offices
- ▶ China Investment Corp (2010), \$1.5b, Energy investments, M&A
- ▶ General Gene (2011), \$2m, Health and biotech, Richmond R&D
- ▶ GOK International (2012), \$13m, furniture assembly, Danville, (avoid import duties)
- ▶ Shuanghui (Shineway) International??? (\$7.1 billion)

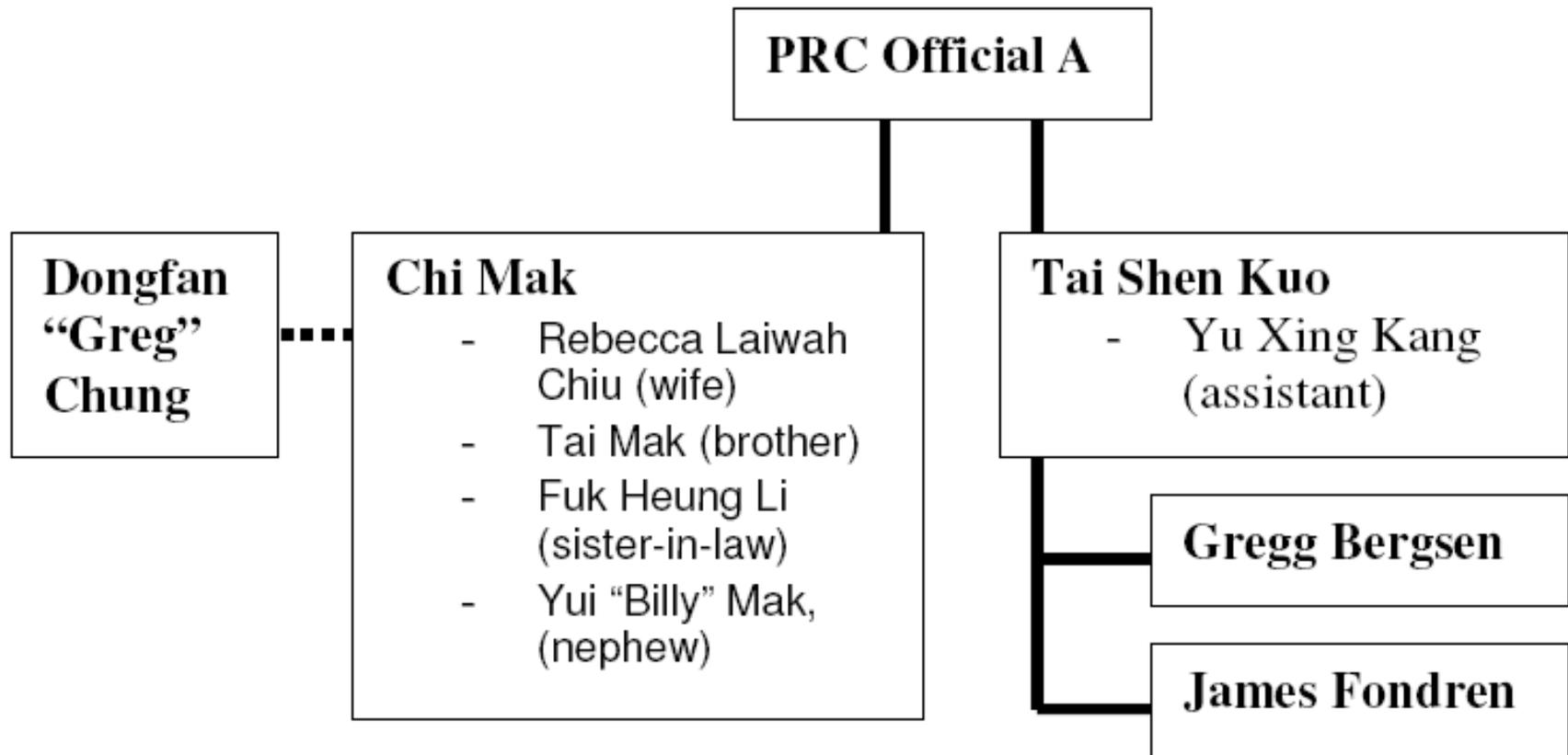
Why?

- ▶ Avoid time and money for research and development
- ▶ Leapfrog gaps in R&D capacity
- ▶ Provide advantage in a negotiation
- ▶ Steal IP and get a product out first
- ▶ Develop market share and brand
- ▶ Viewed as effective way to target superior military force
- ▶ Seeks to provide a tactical advantage at the outset of a conflict or negotiation

- ▶ **For the Chinese military, part of a larger war fighting and “antiaccess” strategy**

Select sources

- ▶ *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, (Washington, DC: Office of the National Counterintelligence Executive, October 2011). pp. 8-11.
- ▶ “Huawei Annual Report Details Directors, Supervisory Board for First Time,” Open Source Center, October 5, 2011, pp. 3-4.
- ▶ Krekel et. al., *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, (Washington, DC: NGC for USCC, 2009) p. 67.
- ▶ Krekel et. al., *Occupying the Information High Ground*, (Washington, DC: NGC for USCC, 2012).
- ▶ Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units* (Alexandria, VA: Mandiant Corp., February 18, 2013) http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
- ▶ Mulvenon, James, “PLA Computer Network Operations,” in Kamphausen et. al., (eds) *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle, PA: U.S. Army Strategic Studies Institute, 2009). pp. 253-85.
- ▶ Stokes et. al., “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure,” (Washington, DC: Project 2049 Institute, November 11, 2011). p. 7.
- ▶ *Targeting U.S. Technologies*, (Washington, DC: Defense Security Service, 2011). p. 30.
- ▶ U.S.-China Economic and Security Review Commission: 2009 Annual Report to Congress (pp. 167-81); 2010 Annual Report to Congress (pp. 221-47); 2011 Annual Report to Congress (pp. 155-220). Available at <http://www.uscc.gov>.
- ▶ Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Washington, Potomac Books, 2013).



Questions?





Virginia Information Technologies Agency

Cyber Security Month

Ed Miller
Security Analyst, VITA



Cyber Security Awareness Month

October is National Cyber Security Awareness Month (NCSAM).

NCSAM has been conducted every October since 2001. It is sponsored by the Department of Homeland Security in cooperation with the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).



October 2013 Theme: **Our Shared Responsibility**

- NCSAM reminds us that being safer and more secure online is a ***shared responsibility***.
- Emerging cyber threats require engagement from the entire American community—from government and law enforcement to the private sector and most importantly, members of the public – to create a safer cyber environment.



Why is Cyber Security Awareness Important?

To protect the confidentiality, integrity, and availability of information in the Commonwealth requires that all employees:

- Understand their roles and responsibilities related to the Commonwealth and agency mission
- Understand the Commonwealth & the agency's information technology security policy, procedures, and practices
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible



Why is Cyber Security Awareness Important?

- Cyber security awareness programs impress upon users the importance of cyber security and the adverse consequences of its failure.
- “Awareness” may sometimes just reinforce knowledge that is already gained, but over time & with enough repetition, awareness can produce security behaviors that are automatic.
- The goal is to make "thinking security" a natural reflex for everyone in the Commonwealth. Awareness activities can build in these reflexes both for the security professional and for the everyday user.



How and where do we start?

- Getting ready for National Cyber Security Awareness Month takes a little planning and some effort.
- Here's a "How To..." that I found. It has the steps to take in planning for NCSAM. You might find these helpful.



How to plan for NCSAM?

1. What cyber security awareness needs does your agency have?

How cyber security savvy are your employees already?

Are there certain types of incidents, compromises, or support issues that are occurring frequently?

What are the messages you want to emphasize? Which needs are most critical?



How to plan for NCSAM?

2. Who is your targeted audience?

Will your awareness efforts be aimed at the entire agency or just a subset (employees, citizens, executives, IT admins, etc.)?

Another way to identify your audience is to think about who in the agency most needs to hear about computer security threats & how to protect against them. Does one group of users pose more of a security risk to your information technology environment than another group?



How to plan for NCSAM?

3. Is your intended audience in one geographic area, or dispersed?

One geographic location would allow for events such as a security fair or invited speakers, while dispersed locations may require a strategy involving e-mailings or publications instead.



How to plan for NCSAM?

4. What types of awareness methods tend to work in your agency?

For some agencies, a speaker series might draw a large % of the audience & be most effective. In others, email tips and alerts may have the most impact.

Consider what methods of communication work best in your environment. What has been successful in the past? Which methods capture the attention of the most people?



How to plan for NCSAM?

4 (continued). **What types of awareness methods tend to work in your agency?**

Some examples include:

Book Marks

Brochures

Checklists

Flyers

Games

Handouts

Post Cards

Presentations

Pamphlets

Links Security Web Page(s)

Videos

Security Awareness Documents

Security Cards

Security Quizzes

Surveys

Security Tools



How to plan for NCSAM?

5. How much money do you have to spend?

Your budget will influence many of your decisions, and usually this is not much. However, there are many inexpensive and free resources you can utilize.



How to plan for NCSAM?

6. How many people are available to assist?

How many staff from your agency can assist with this effort? Can you solicit volunteers, interns, and partnerships with other divisions or units?

Remember that this doesn't have to be strictly an IT security effort. HR, Finance, Admin, Communications & many other business units within a typical agency are all stakeholders that benefit from a successful cyber security campaign.



How to plan for NCSAM?

7. How much lead time do you have?

National Cybersecurity Awareness Month is October.

Make sure you have enough lead time to take on the things you want to do. Consider print time and delivery time if you want to create printed material.

The more lead time you have the better. However, if you have little lead time, don't give up! There are many resources available that you can pull together quickly.



Resources



Resources: Web links

- <http://www.stopthinkconnect.org/>
- <http://www.staysafeonline.org>
- <http://www.microsoft.com/security>
- <http://www.dhs.gov/national-cyber-security-awareness-month>
- <http://msisac.cisecurity.org/>
- <http://onguardonline.gov>
- <http://protect.iu.edu/cybersecurity/downloads>



Resources: Blogs

- Check out these blogs to learn more ways to protect yourself and help keep the web a safer place for everyone.
 - [Facebook Security Blog](#)
 - [Google Online Security Blog](#)
 - [Krebs on Security](#)
 - [McAfee Family Safety Blog](#)
 - [Microsoft Security Tips & Talk Blog](#)
 - [RSA Speaking of Security Blog](#)
 - [Sophos Naked Security Blog](#)
 - [Stay Safe Online Blog](#)
 - [Symantec Security Blogs](#)
 - [The Security Skeptic](#)
 - [U.S. Department of Homeland Security Cybersecurity Blog](#)
 - [Visa Security Sense Blog](#)



Resources: Social Media Safety

- [Facebook/SaferOnline](#)
- [Twitter/SaferOnline](#)
- [YouTube/MSFTOnlineSafety](#)

Resources: Quizzes, Games, Videos



Onguardonline.gov
(sponsored by the
FTC)



Cyber Security Month at VITA

- At VITA, we try to do a little extra something every year for our employees to promote Cyber Security Month.
- We encourage all agencies to try to promote it within their organization as well.



Planning your message

- Generally, it is more effective to identify one or a few focused messages and repeat those many times rather than to try to be very general.
- Consider focusing on one message/topic per each week in October, or one message/topic for the entire month with sub-topics each week.



Sample Cyber Security Month Agenda

- Each Monday: a Security Buzz (a security email tip related to the focus of the week)
- Each Wednesday: a link to a Security Quiz, Video or Game
- Each Friday: a security crossword or word search puzzle (also related to the security focus of the week).
- October 16: Cyber Security Day at VITA (Peter Miller / FTC and VSP Mobile Command Unit tours)

NCSAM OCTOBER 2013

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Theme – What is Cyber Security?	<p>Cyber Security Kickoff / Governor's Proclamation</p> <p>Cyber Security Buzz: Email employees a theme related video link, game or puzzle and related news item</p>	<p>1</p> <p>NG/VITA Interactive Game or Information Table setup in CESC common area</p>	<p>2</p> <p>1:00 ISOAG/ Speakers: H. Leininger/Kore Logic: Password Cracking & J. Segreti/Kore Logic: Secure App Coding & J. Schanke/US Secret Service</p>	3	<p>4</p> <p>Email to employees: Cyber Security Pledge reminder</p>	5
6 Theme – The Security Risks of Social Media	<p>7</p> <p>Cyber Security Buzz: Email employees a theme related video link, game or puzzle and related news item</p>	<p>8</p> <p>NG/VITA Interactive Game or Information Table setup in CESC common area</p>	9	<p>10</p> <p>NG Brown Bag Lunch: End User Remote Access</p>	<p>11</p> <p>Email to employees: Cyber Security Pledge reminder</p>	12
13 Theme – Privacy - Protect Your Privacy on the Internet	<p>14</p> <p>Cyber Security Buzz: Email employees a theme related video link, game or puzzle and related news item</p>	<p>15</p> <p>NG/VITA Interactive Game or Information Table setup in CESC common area</p>	<p>16</p> <p>1:00 Peter Miller, Chief Privacy Officer/ FTC</p> <p>Mobile Command Post Vehicles from VSP, ABC and DMV will be in the CESC parking lot</p>	17	<p>18</p> <p>Email to employees: Cyber Security Pledge reminder</p>	19
20 Theme - Mobile Device Security	<p>21</p> <p>Cyber Security Buzz: Email employees a theme related video link, game or puzzle and related news item</p>	<p>22</p> <p>NG/VITA Interactive Game or Information Table setup in CESC common area</p>	23	<p>24</p> <p>NG Brown Bag Lunch: McAfee Host and Network Intrusion Detection Systems</p>	<p>25</p> <p>Email to employees: Cyber Security Pledge reminder</p>	26
27 Theme – Keeping Children Safe Online	<p>28</p> <p>Cyber Security Buzz: Email employees a theme related video link, game or puzzle and related news item</p>	29	<p>30</p> <p>1:00 SA John Houlberg – VSP Internet Crimes against children</p>	<p>31</p> <p>Halloween Costume Contest (CVC fund raiser) VITA Cyber Security Game Booth (CVC fund raiser)</p>		



Let us know

- Finally, we are interested in the efforts that you've made at your agency in promoting cyber security awareness.
- If you have powerpoint presentations, posters, tips, speaker sources, that you'd be willing to share, please let us know.
- Remember, October is just the peak month. A successful cyber security awareness campaign really needs to run all year long.



Ed Miller

VITA

Commonwealth Security and Risk Management

edward.miller@vita.virginia.gov

(804)-416-6027



Virginia Information Technologies Agency

Commonwealth Data Points

Ed Miller
Security Analyst, VITA



2013 Commonwealth of Virginia Information Security Report

- The 2013 Commonwealth Information Security Report will be the 6th annual report prepared by VITA and presented to the Governor and the General Assembly as required by **§2.2-2009(C)** of the *Code of Virginia, Additional Duties of the CIO relating to security of government information.*



Duties of the CIO per 2.2-2009

- Directing the development of policies, procedures & standards for assessing security risks
- Determining the appropriate security measures & performing security audits of electronic government information
- Developing policies, procedures & standards that address the scope of security audits and the frequency of such security audits



Duties of the CIO per 2.2-2009

- Receiving reports of security incidents while taking such actions as are necessary, convenient or desirable to ensure the security of the Commonwealth's electronic information and confidential data
- Making the annual report to the Governor and General Assembly regarding agencies' information security programs
- Develop and implement a Commonwealth information technology risk management program



2013 Information Security Report

- The 2013 COV Information Security Report will build on a baseline first created in 2008 for assessing the strength of the information security programs that state agencies have established to protect Commonwealth information.



2013 Information Security Report

- The report is based on an analysis of data and information reported by agencies to the CISO as of December 31, 2013.
- The COV Information Security Policy, Security Standard & Audit Standard require that certain data be reported by agencies to the CISO, and these data serve as the basis for the individual agency component of this report, including whether an agency head has:



2013 Information Security Report

- Designated an information security officer (ISO) within the past two years
- Submitted a current IT security audit plan for sensitive systems
- Provided IT security audit reports
- Provided corrective action plans for completed information security audits
- Submitted IT security exceptions
- Supplied quarterly status updates for corrective actions
- Audited sensitive systems within the required three-year period

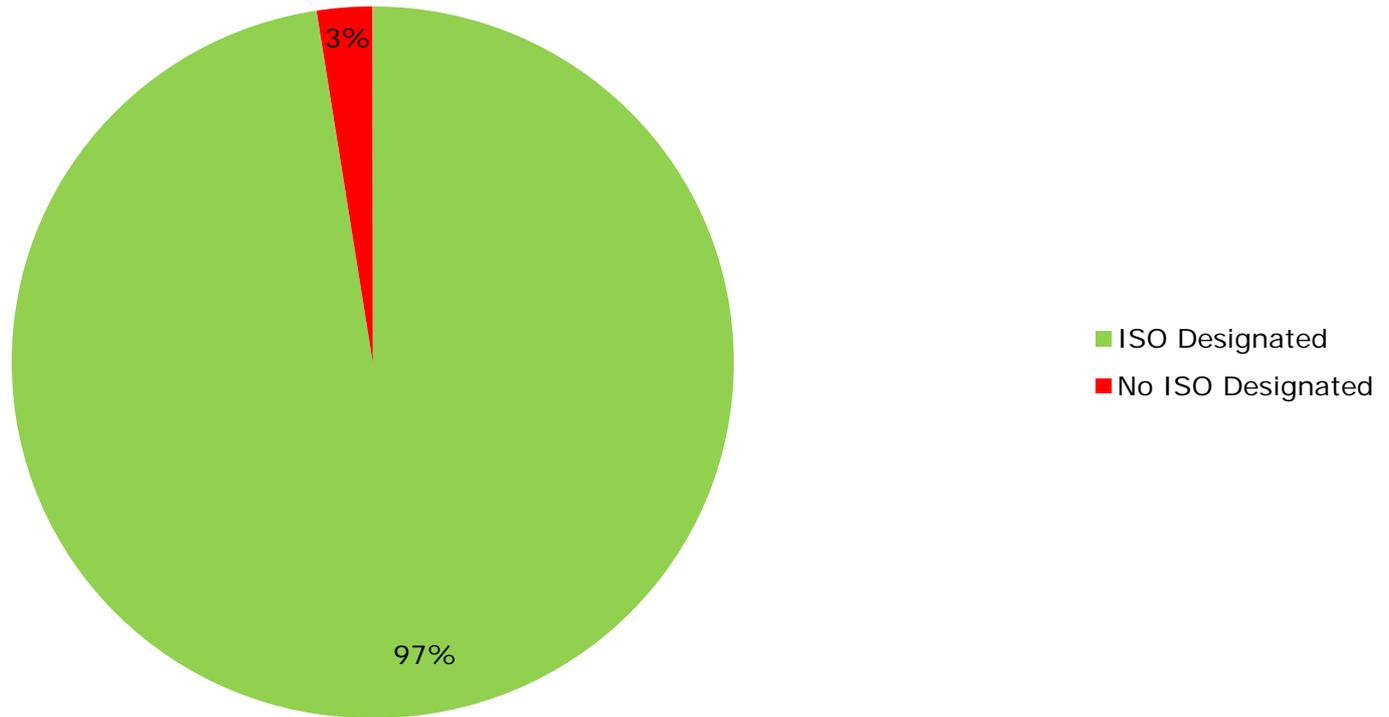


2013 Information Security Report

- Supplied quarterly status updates for corrective actions
- Audited sensitive systems within the required three-year period
- Had personnel attend a information security orientation session at least once every 2 years
- Submitted Agency Risk Assessments
- Submitted Agency Business Impact Analyses
- Submitted Agency threat metrics
- New for 2013: Whether the primary ISO is “COV certified”

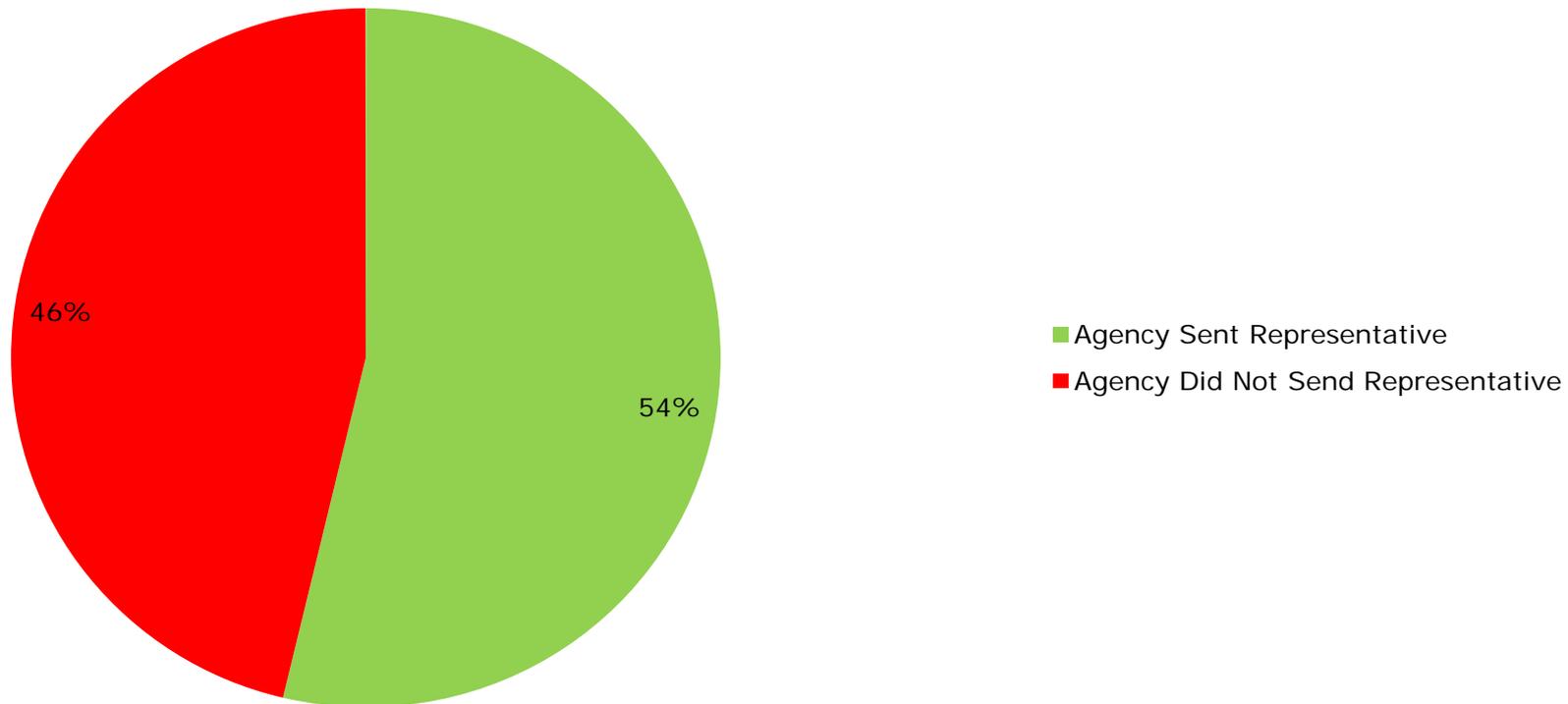
Last year: ISO Designation

ISO Designation



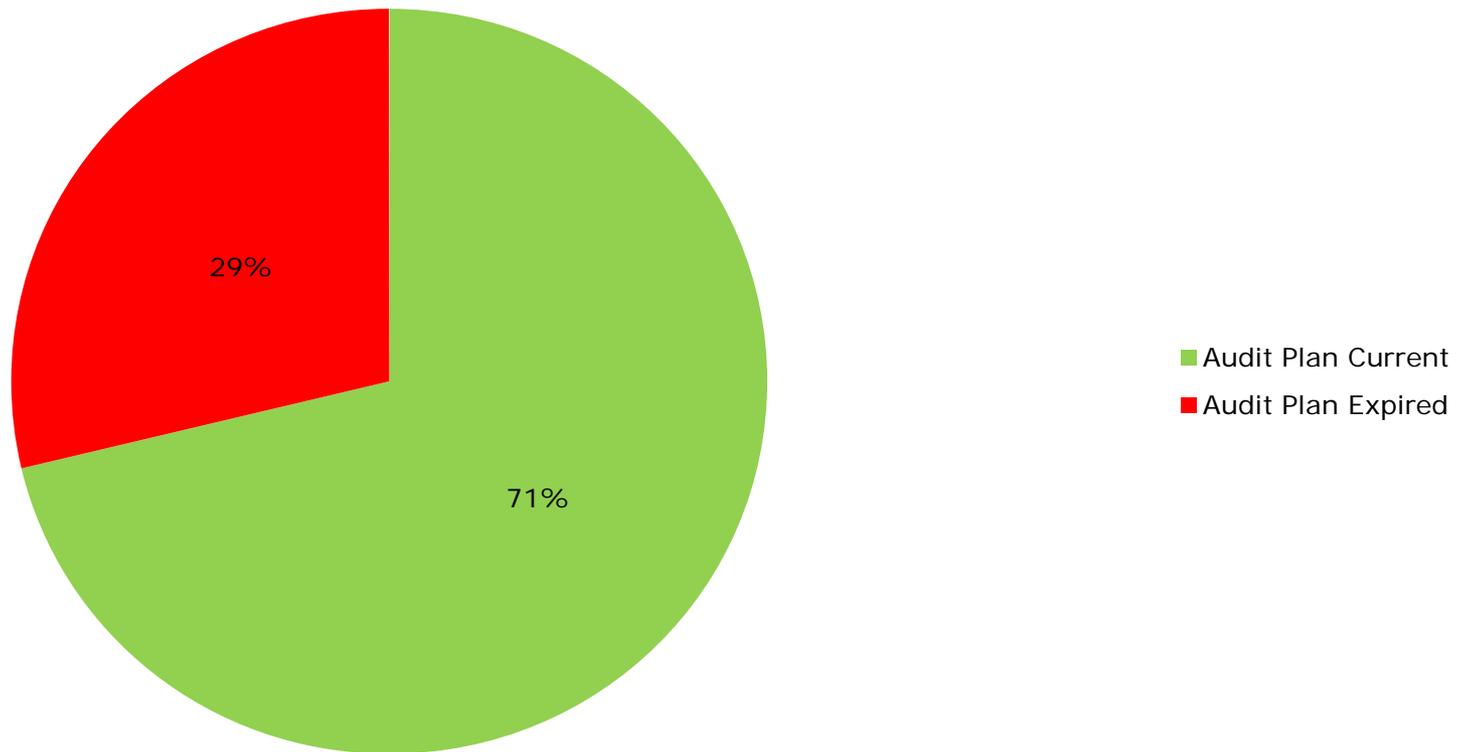
Last year: Attended IS Orientation

Information Security Orientation



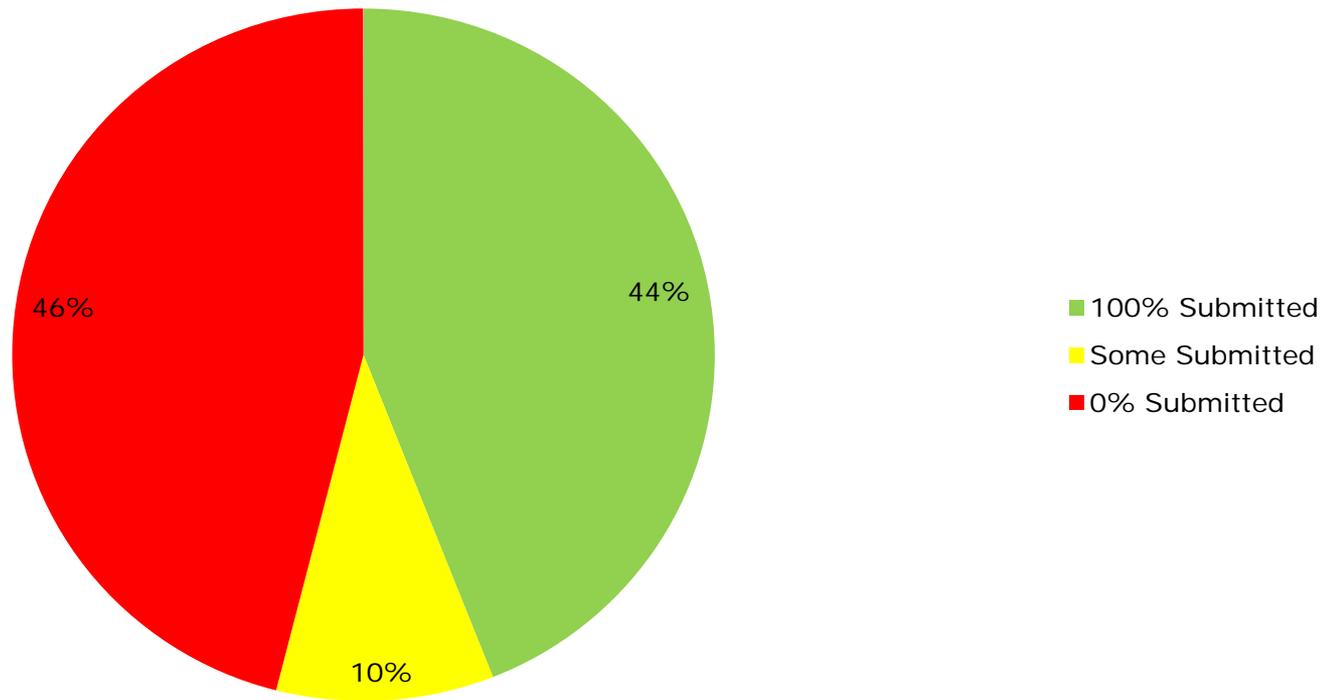
Last year: Submitted IT Audit Plan

IT Security Audit Plan



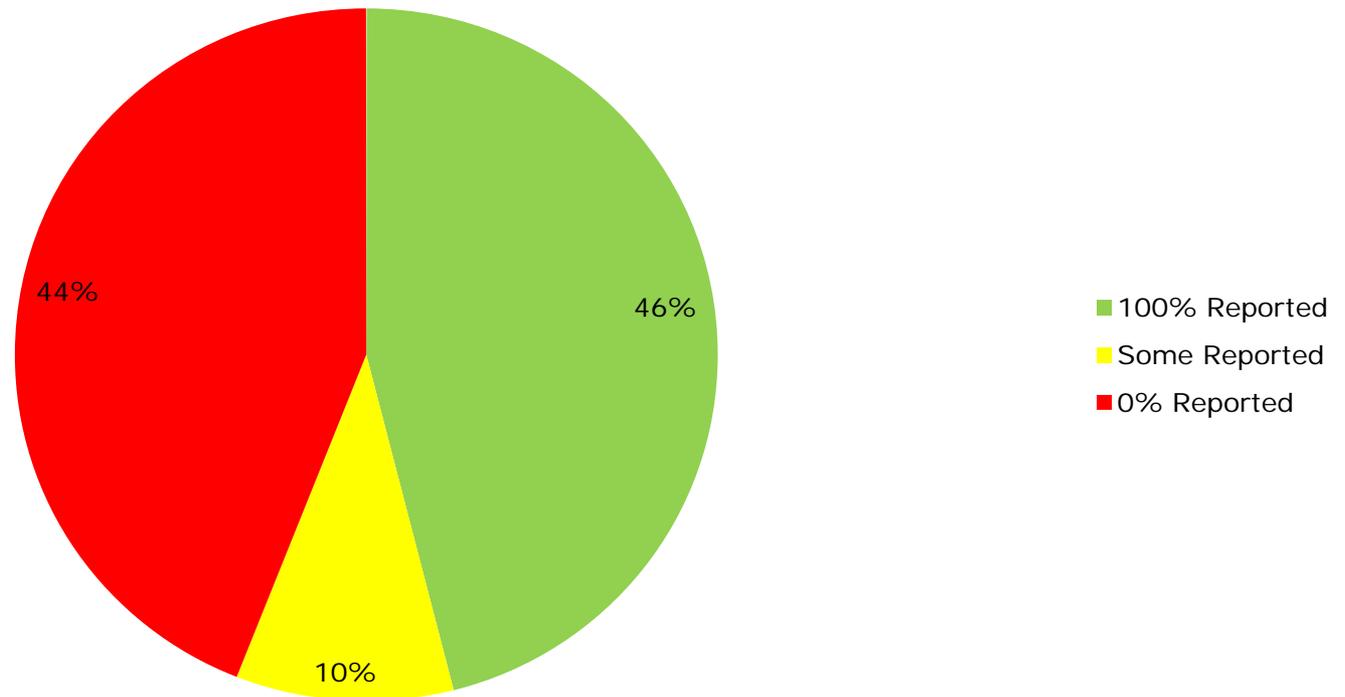
Last year: Submitted IT Audit Reports

Audit Reports



Last year: Submitted CAPs

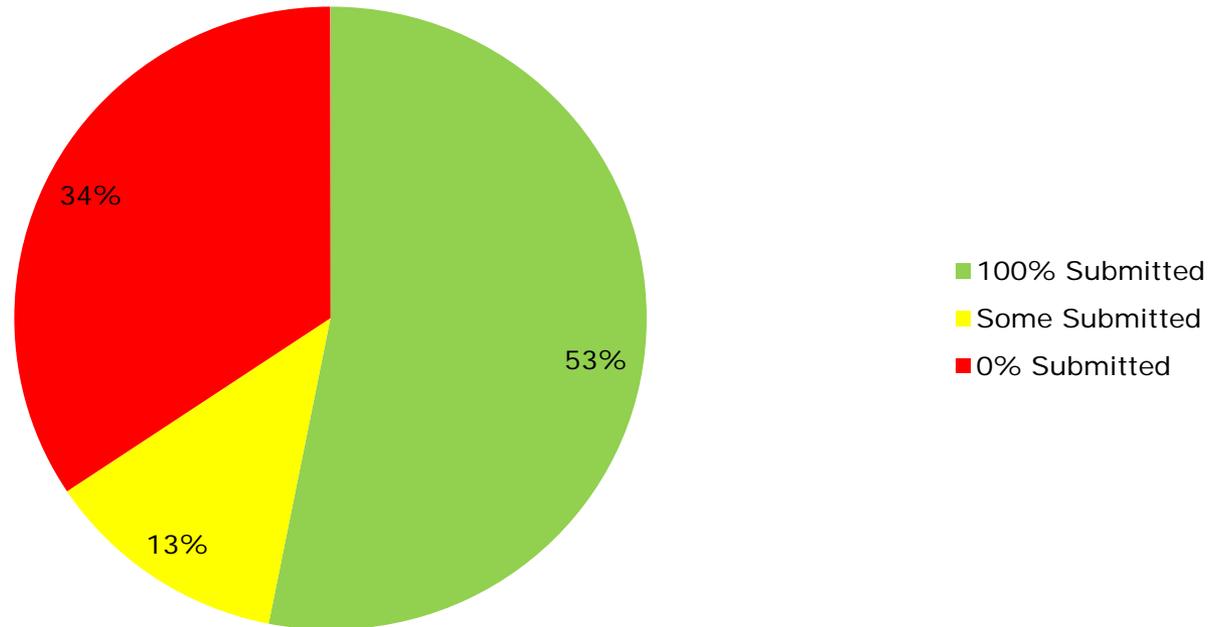
Corrective Action Plans





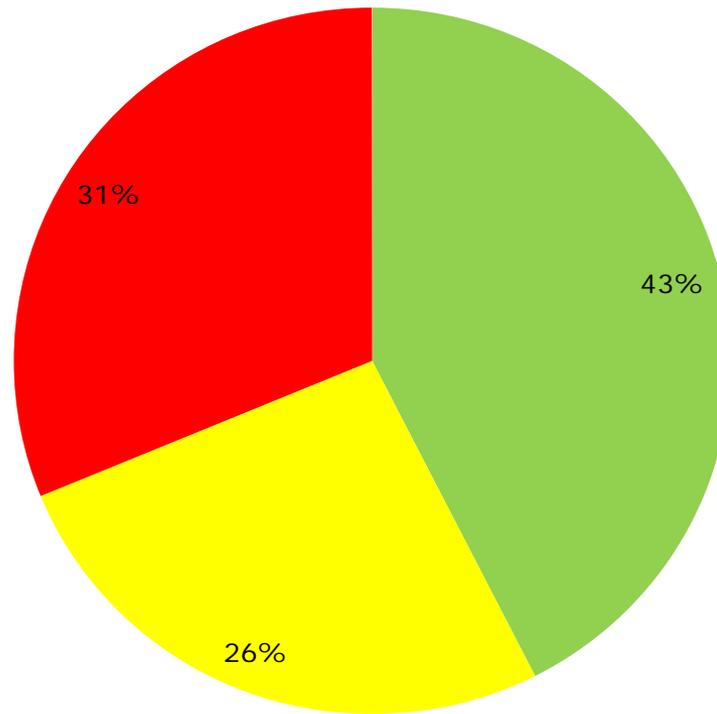
Last year: Submitted Quarterly Updates

Quarterly Updates



Last year: % of Audit Obligation

Audit Obligation Completed

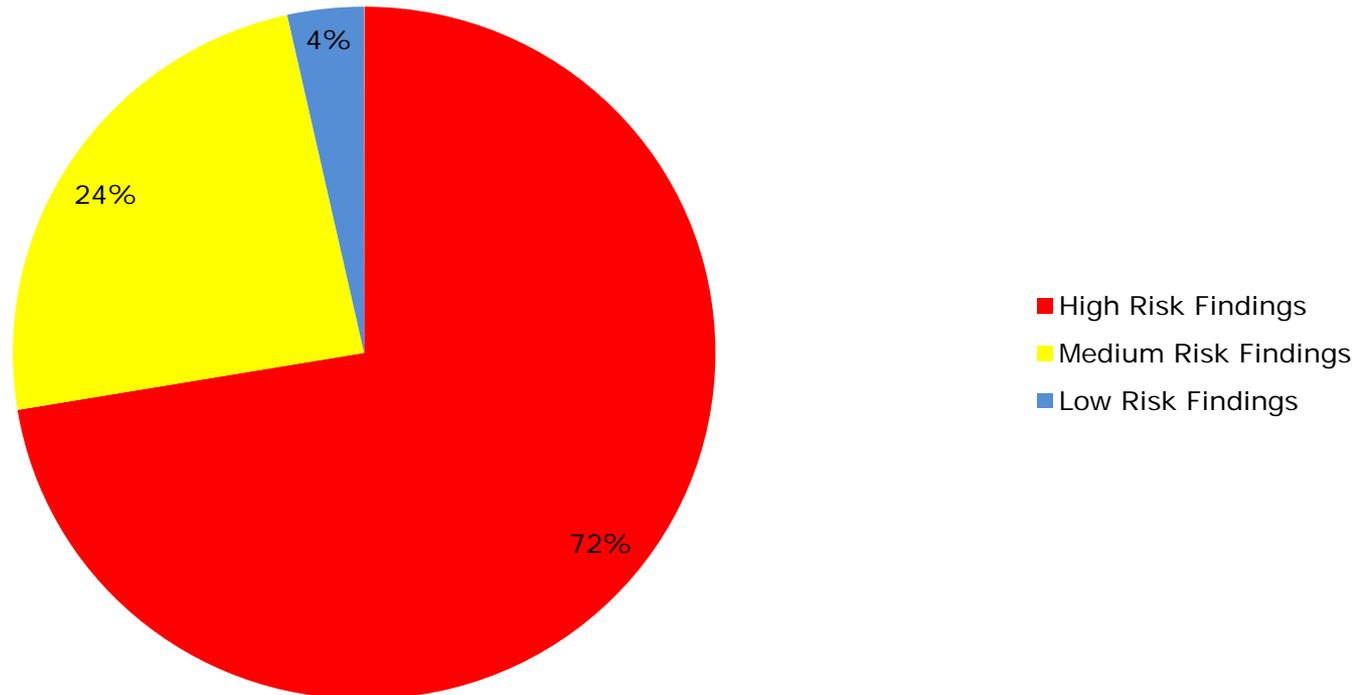


- 100%
- Some
- 0%

Measures the requirement to audit all sensitive systems at least once every 3 years

Last year: Unresolved IT Audit Findings

IT Security Audit Findings





Last year: BIA/RA/IDS Reports

All documentation received as requested information about the agency's:

- BIA,
- RA(s)
- and IDS reports



By the end of fall 2013 & sooner if we can

All agencies should have “read” access to the ARCHER program

ARCHER will allow you to see your current status. It will allow you to track where you are & correct us where we’re wrong.

We will use ARCHER to further development better and stronger data points for 2014.



Summary

- Please review what you have sent us or need to send us
- Consult with your audit department or AITR if you need to
- It's not too late to make improvements in your score for 2013.



Ed Miller

VITA

Commonwealth Security and Risk Management

edward.miller@vita.virginia.gov

(804)-416-6027



Application Testing via Fuzzing

Bob Baskette
Senior Manager, Security Operations
and Architect



Fuzz Testing Background

- Software testing technique used to expose security issues in applications by introducing invalid, unexpected, or random data into the inputs of an application
- The application is monitored to detect process exceptions such as faults or failing built-in code assertions



Fuzz Testing Background

- The concept and term originates from a class project conducted at the University of Wisconsin Madison in 1989
<http://www.cs.wisc.edu/~bart/fuzz/>
- Fuzz testing is normally considered a Black Box testing technique since all testing is performed from an external view

Why Perform Fuzz Testing

- Fuzz testing is based on the assumption that coding errors exist within every application and therefore a systematic approach will expose the errors
- Fuzz testing will provide another point of view to classical software testing techniques such as code reviews and debugging because Fuzz testing uses a non-human approach



Why Perform Fuzz Testing

- Fuzz testing improves application security because it can detect defects which may be overlooked by human testers due to the complexity of the application coding
- Fuzz testing is an essential part of the Software Development Lifecycle



Fuzzy Testing Targets

- Application code issues to be tested include:
 - Buffer overflows
 - Format strings
 - Code injections
 - Dangling pointers
 - Race conditions
 - Denial of service conditions



Fuzz Testing Targets

- File formats and network protocols are the most common targets of testing, but any type of program input can be Fuzz tested
- Of primary importance is any input that crosses a trust boundary
- Any untrusted source of data input is considered to be insecure and inconsistent



Fuzz Testing Simple Example

- An application that records the selection between three items would use an integer to store a value between 0 – 2. The Fuzz test would determine what would happen if the application attempted to store a larger value than the integer could hold (buffer capacity) or a value not consistent with the application (logic issue)



Fuzz Testing Advantages

- Application errors uncovered by Fuzz testing can be severe, exploitable coding errors that could be used by a real attacker
- Fuzz testing can be used to uncover the same application issues used by malicious individuals since the same techniques and tools are now used by attackers to exploit deployed software



Fuzz Testing Advantages

- The greatest advantage of Fuzz testing is that the test conditions are extremely simple to design and that the test conditions are free of preconceptions about system behavior

Fuzz Testing Disadvantages

- The primary concern with Fuzz testing is that basic/simple inputs will usually only yield simple coding errors. The quality of the output is solely depended upon the quality of the input
- The randomness of inputs used in fuzzing is often seen as a disadvantage, as catching a boundary value condition with random inputs is highly unlikely

Fuzz Testing Disadvantages

- The technique can only provide a random sample of the system's potential behavior
- In many cases passing a Fuzzing test may only verify that an application can handle exceptions without crashing, rather than behaving correctly



Fuzzy Analysis Common Steps

- Identify the target and inputs
- Generate Fuzz data
- Execute Fuzz data
- Monitor the output
- Determine the exploitability

Fuzz Testing Initialization

- It is important to configure the Fuzz testing tool to record the input data (including the pseudo-random number-generated seed value) to be used in the test to a file prior to executing the test.
- The file will be needed to reproduce the testing errors if the Fuzzing software causes the system to crash



Fuzz Testing Requirements

- Documentation on target and protocol
- Target to fuzz
- Fuzzing tools
- Monitoring and analysis tools
- Time
- More time
- Lots more time
- Creativity



Fuzz Testing Techniques

- Static Test Case
- Randomized
- Mutation
- Intelligent Mutation



Static Test Case Fuzz Testing

- Uses static data and conditions
- Analysis of target to determine unique conditions and protocol violations
- Does not require coding skills



Static Test Case Fuzz Testing

- Very time intensive
- Lots of up front development time
- Limited by creativity of analyst
- Test cases easy to reproduce since test cases are stored in files



Randomized Fuzz Testing

- Start with valid protocol frame or data set and randomize portions of data
- Little protocol knowledge needed
- Short setup time

Randomized Fuzz Testing

- Has infinite run-time since the amount of random data available is infinite
- Truly random data can lead to minimal code coverage since most random data is simply rejected
- May be difficult to pin-point cause of crash



Mutation Fuzz Testing

- Similar to Randomized Fuzzing
- No significant set up time since no protocol analysis is performed
- Start with valid protocol frame or data set and performs an iterative replacement of values throughout the data



Mutation Fuzz Testing

- Has finite run-time since the test stops after all mutations for each portion of the data has been tested.
- Will change one byte of data at a time for each field to be tested
- Has limited ability to test for flaws in string handling processes



Intelligent Mutation Fuzz Testing

- Uses protocol grammar to describe operation and framing behavior of a protocol
- Can provide the most granular access to evaluating the target
- Can reach deeper into the code paths than other methods



Intelligent Mutation Fuzz Testing

- Requires tremendous up-front analysis time to define the available components of the protocol and the expected behaviors
- Grammar is used to identify fields to be fuzzed



Protocol-Based Fuzz Testing

- Protocol awareness can be used to generate Fuzz testing criteria and send forged packets to the target application
- The testing criteria can be generated from scratch, or the criteria can be mutated from examples from test suites or real data



Protocol-Based Fuzz Testing Limitations

- Testing will not be successful until the protocol specification is relatively mature since the specification is a prerequisite for writing the test condition
- Many useful protocols are proprietary or utilize proprietary extensions. If the test conditions are based only on published specifications the test results will be limited



Fuzz Testing Conditions/Vectors

- Define lists of "known-to-be-dangerous values" for each type
 - For integers: zero, negative, very big numbers
 - For chars: escaped, interpretable characters / instructions
 - For SQL Requests, quotes / commands
 - For binary: random ones



Application Fuzz Testing

- The attack vectors are within the I/O
- For a desktop application:
 - The UI (testing all the buttons sequences / text inputs)
 - The command-line options
 - The import/export capabilities (see file format fuzzing below)



Application Fuzz Testing

- The attack vectors are within the I/O
- For a web application
 - URLs
 - Forms
 - User-generated content
 - RPC requests



File Format Fuzz Testing

- Generates multiple malformed samples and processed the samples sequentially
- When the application generates a fault the debug information is kept for further investigation.



File Format Fuzz Testing

- Attack vectors include:
 - The codec/application layer
 - Lower-level attacks/ application internals
 - The parser layer (container layer)
 - File format constraints
 - File format structure
 - File format conventions
 - File format field sizes
 - File format flags



Fuzz Testing Summary

- Fuzz testing is intended to provide an assurance of overall quality rather than an end-all bug-finding tool
- Fuzz testing can suggest which parts of an application should get special attention
 - Code audit
 - Static analysis
 - Partial rewrites



Questions???

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

Thank You!



Virginia Information Technologies Agency

Upcoming Events





Governor's Proclamation

Governor McDonnell has proclaimed
October 2013
as
Cyber Security Awareness Month

Proclamation will be located at the Governor's Portal:

<http://www.governor.virginia.gov/OurCommonwealth/Proclamations/>

or VITA Information Security Awareness Toolkit:

<http://www.vita.virginia.gov/security/toolkit/default.aspx?id=9930>



COVITS 2013

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 9 & 10

Richmond Marriott

500 East Broad Street, Richmond, VA 23219

Register Here: <http://www.govtech.com/events/COVITS-2013.html>



Information Security System Association

ISSA

DATE: Wednesday, September 11, 2013

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

More info located here: <http://centva.issa.org/central-va-issa-feb-2013-meeting/>



IS Orientation

When: Thursday, Sept 5, 2013

Time: 10:00 am to Noon

Where: CESC , Room 1221

Register here:

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

Next IS Orientation will be held on Dec 5, 2013



October ISOAG

October Cyber Security Month

Oct 2

1:00 – 4:00 pm @ CESC

Keynote Speakers:

Hank Leininger, Kore Logic

on “Passwords & Password Cracking”

And

Joe Segreti, Kore Logic

on “Secure Source Code”

And

John Shenke, U.S. Secret Service

on “Cyber Security Investigations”

ISOAG meets the 1st Wednesday of each month in 2013



VA SCAN

2013 Virginia Alliance for Secure Computing and Networking Conference

Schedule: October 3-4, 2013

Location: Old Dominion University's multidisciplinary research center in Suffolk, Virginia

Registration Cost: \$125 for conference. An additional fee of \$150 is applicable for those attending the SANS training course

Registration Deadline: September 27th, 2013

Conference website: <http://occs.odu.edu/vascan/>



CISM Security+ Boot Camp Offering

Global Knowledge is hosting a Security+ boot camp onsite at Northrop Grumman's CESC facility and we have seats available!

Security+ Boot camp

Dates: Monday Oct 7th – Friday Oct 11th

Time: 8:00 am – 6:00 pm

Cost: \$1,625

**Register and pay by Sept 13 to reserve seat*

If you would like to register, please contact Kristen Miller at 252-756-4757 / Kristen.miller@globalknowledge.com with payment or if you have any questions. Payment in the form of a company funded PO or credit card will secure your seat and is required before class starts.



DOA Training Offering

Auditing the Internal Network

Instructor: David Cole (SysAudits)

Date: October 29 & 30, 2013

Time: 8:15-4:45

**Location: James Monroe Building
Conf. Rm. B, 1st FL**

Cost: \$ 320.00

Register: <https://hrtraining.doa.virginia.gov/>



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*

4 September, 2013



NORTHROP GRUMMAN

ADJOURN

