



ISOAG Meeting October 5, 2016

Welcome to CESC



Welcome and Opening Remarks

Michael Watson

October 5 , 2016



ISOAG October 5, 2016 Agenda

- | | |
|-----------------------------------------|----------------------------|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. Date Points Update | Jon Smith/Ed Miller |
| III. Web Scanning Update | Bill Freda |
| IV. Archer Update | Mark Martens |
| V. Threat Update | Kathy Bortle |
| VI. Cloud Security Update | Mark Craft |
| VII. Upcoming Events | Mike Watson, VITA |
| VIII. Partnership Update | Northrop Grumman |



Virginia Information Technologies Agency

Data Points Review

Ed Miller

Director IT Security Governance

Jonathan Smith

Director IT Risk Management



IT Security Audit Program

On the Governor's Report, this appears as:

Commonwealth Overall Audit Program Score

The Commonwealth's IT security and IT security audit standards require agencies to develop and maintain an agency IT security audit program.



IT Security Audit Program

Agencies are required to:

- Appoint an ISO,
- Identify sensitive systems,
- Develop an IT security audit plan,
- Conduct IT security audits on those systems at a minimum of every three years,
and
- Develop and carry out corrective action plans for findings noted during the audits.



IT Security Audit Program

- Audit Plans, Audits, and Corrective Action Plans will be held to a higher standard from now going forward.
- Audit Plans must line up to Sensitive Systems and Sensitive Systems must be associated to Devices and line up to Business Processes and Data Sets.
- APA audits only accepted if accompanied by a statement or email from the APA indicating the specific IT systems and specific IT security control families that the audit reviewed.
- Audit findings must be closed in a timely manner.



IT Security Audit Program

Per SEC502; the IT Security Audit Standard

- *All IT security audits must follow either the generally accepted government auditing standards GAGAS Yellow Book (**Generally Accepted Government Auditing Standards**) or the international standards for the professional practice of internal auditing IIA Red Book (**Institute of Internal Auditors' Standards**).*



IT Security Audit Program

To be GAGAS or IIA compliant,

- *Follow the Standards/Framework as published by the GAO or IIA*
- *That includes:*
 - *Ethics*
 - *Independence*
 - *Competence*
 - *Quality Control and Assurance*



IT Security Audit Program

Independence:

- *Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. (per IIA)*
- *...are considered independent...if the head of the audit organization...is accountable to the head or deputy head of the entity or those charged with governance (per GAS)*



IT Security Audit Program

Quality Assurance:

- *External assessments must be conducted at least once every 5 years by a qualified, independent reviewer from outside the organization. (per IIA)*
- *..have an external peer review performed by reviewers independent of the audit organization being reviewed at least every 3 years. (per GAS)*



IT Security Audit Program

Office of the State Inspector General

- *OSIG has been reviewing the Internal Audit structure for all agencies with Internal Auditors.*
- *OSIG is forming a committee to review those structures to determine if they meet the requirements as set forth by IIA.*



Virginia Information Technologies Agency

ISO Certification

Ed Miller

Director IT Security Governance





ISO Certification

To be certified:

- *Attend October meeting*
- *Take IS Orientation within the last 2 years*
- *Take 1 course in the KC if you have an industry certification or 3 courses if you don't*

Knowledge Center is being updated from Oct 21 through Nov 3. You will have to take KC courses before or after that window.

To be re-certified:

- *Attend October meeting*
- *Take IS Orientation once every 2 years*
- *Take 20 hours of Continuing Education in the CY (including 1 course in the KC)*



Virginia Information Technologies Agency

Centralized Services Update

Ed Miller
Director IT Security Governance



Centralized Services Update

- 26 agencies signed up so far
- Several agencies still have MOUs that are not signed
- Several agencies still have revised IT Security Audit Plans and IT Risk Assessment Plans that they need to submit



Centralized Services Update

IT Security Audit out-sourcing

- SOW for IT security auditing is nearly final.
- The SOW work plan is aggressive. 3 teams of auditors will be used.





IT Risk Management Program

Agencies are required to:

- Complete and submit a complete BIA, once every three years and perform a review annually
- Submit an IT risk assessment plan annually
- Perform risk assessments of sensitive systems once every three years, at a minimum
- Report risk treatment plans and quarterly update
- Conduct quarterly vulnerability scans
- Submit IDS reports quarterly
- Complete the Commonwealth wide risk assessment (New)



Business Impact Analysis (BIA)

- Submission requirements:
 - Full BIA conducted and submitted to CSRM once every three years, at a minimum.
 - Review/update annually, at a minimum
- How to submit, review, or update BIA:
 - BIA spreadsheet for import to Archer
 - Direct entry in Archer (create new or modify)
 - Archer entries will be reviewed and approved by CSRM
 - Existing business processes in archer that are missing required fields will be set to rejected so that the you can update the missing information



BIA (cont'd)

- Mandatory fields in Archer
 - Agency name
 - Process name
 - Business purpose
 - Business owner
 - Mission essential function (yes/no)
 - Impact ratings: Life, safety, confidentiality, customer service, legal, finances, regulatory
 - Recovery point and time objectives (RTO/RPO)
- All applications must be aligned with business process's, devices, and datasets



Risk Assessment Plan

- Risk assessment plan:
 - Annual submission
 - Each sensitive system must be listed on the plan
 - Scheduled risk assessment should be within 3 years of the last IT risk assessment conducted for each system
 - Use risk assessment plan template
 - The agency name, agency abbreviation and agency number,
 - The contact information of individual submitting the plan,
 - The date of submission,
 - The system full name and abbreviation (must match CETR/Archer records)
 - The planned assessor,
 - The date the last risk assessment was conducted for the system,
 - Scheduled assessment completion date.



Risk Assessment Reporting

IT risk assessment template

- IT System Name
- Risk ID
- Sensitivity rating (e.g. Confidentiality, Integrity and availability)
- Date of risk assessment
- Risk vulnerability family (e.g. SEC 501 control)
- Vulnerabilities
- Threats
- Risk Summary
- Magnitude of impact (e.g. low, moderate, high, critical)
- Controls in place (brief description)



Risk Treatment planning

- Risk treatment plan template
 - IT System affected
 - Authoritative source (e.g. SEC 501, enterprise policy, operating instruction)
 - Control ID (e.g. AC-1)
 - Date risk identified
 - Risk summary
 - Risk rating (Low, Med-Low, Med, Med-High, High, Critical)
 - Status
 - Status Date
 - Planned resolution;
 - Resolution due date
- Due 30 days after completion of risk assessment
- Updates are due quarterly until risks have been sufficiently mitigated



Vulnerability Scanning

- CSRM is currently standing up the web application vulnerability scanning service.
- Agencies operating infrastructure assets outside of the partnership enterprise are responsible for the vulnerability scanning of those infrastructure assets
- This datapoint will change moving forward as the vulnerability scanning service is put in place. Future datapoint may focus on vulnerability remediation in addition to the completion of the required scans.



IDS Reporting Requirements

- For full service VITA customers, with all assets residing on the partnership infrastructure, these reports are submitted on the agency's behalf
- Agencies with networks external to the partnership enterprise must submit IDS reports for those networks to CSRM quarterly
- CSRM is evaluating this datapoint as we move toward our new sourcing model



IDS Requirements

- Agencies shall report the following IDS information to CSRM at the end of each quarter:
 - Name of Agency
 - Date Range for the Report
 - Total number of attacks per month (Total, high, medium, and low)
 - Top 10 high attacks & number of attacks seen
 - Top 10 source IPs
 - Top 10 destination IPs
 - Top 10 countries of origin of attacks with percentages per month
 - Top 10 types of attacks
 - Top 10 inbound attacks by protocol/service/port
 - Top 10 outbound attacks by protocol/service/port



Commonwealth Risk Assessment

Nationwide Cyber Security Review (NCSR)

- Approximately 100 questions based on NIST cybersecurity framework
- Measurement scale is based on program maturity in the 5 functions of the cyber security framework
 - Identify
 - Detect
 - Protect
 - Respond
 - Recover
- November 1, 2016 – December 31, 2016
- Results and participation will be included in the 2016 Annual Report on Information Security



NCSR FAQ

How do I register for the NCSR?

CSRM is coordinating with CIS to import the questionnaire into our Archer instance to facilitate the NCSR.

How long will the NCSR take to complete?

The assessment took about 2 hours in 2016

What if I cannot take the entire assessment at once?

Users have the ability to save the assessment and return to complete



Questions





Web Application Vulnerability Scanning

VITA
Commonwealth Security
& Risk Management

October 5, 2016



New Web Application Vulnerability Scanning Program

- VITA Commonwealth Security and Risk Management (CSRM) has established a Web Application Vulnerability management program to identify common web application vulnerabilities. This program includes target identification, agency involvement, Archer GRC integration, web application scanning, vulnerability reporting and remediation recommendations. Scans will be conducted on a quarterly cycle. Agencies will be notified when a scan is complete and given instructions on how to obtain the scan report. The quarterly scan reports will measure the vulnerability remediation progress as well as any newly identified vulnerabilities. Reporting includes the recording and tracking of targets, scans, vulnerabilities, and vulnerability remediation progress. Agencies will be required to remediate vulnerabilities in a timely manner.
- July 1, 2016



Authority

- Title 2.2, Chapter 20.1, Code of Virginia
- 2.a . The Virginia Information Technologies Agency shall perform vulnerability scans of all public-facing websites and systems operated by state agencies. All state agencies which operate such websites and systems shall cooperate with the Virginia Information Technologies Agency in order to complete the vulnerability scans.



We need your Assistance

- **Agency Web Site Reconciliation & Identification**
 - Update CETR
 - Include all Public Facing and Sensitive Browser based Applications
 - The CETR information will be Update Archer
 - This will likely be a 2016 Datapoint



CETR Flags we are using

- Web Category = Public Web Site or Public Web Application
- A valid URL <http://something.virginia.gov>
- Client Type = Thin Client - Browser Only or Thin Client – plug in required
- Used by Public = Yes for public facing
- Used by Public = No for internal browser applications

“Web Category” to Web Site or Public Web

Field Name	Description and Use
<p>▼ Web Category</p>	<p>Select the value that best describes the application:</p> <ul style="list-style-type: none"> • Public Web Site: Application is a web site used by the general public (e.g., DMV web site) • Public Web Application: Application is a web application (possibly accessed via your web site) used by the public (e.g., public-facing driver’s license renewal application) • Neither: Application is neither a web site or a public web application <p>Note: if you select either Public Web Site or Public Web Application, a new field will open up:</p> <div data-bbox="606 1035 1715 1225" style="border: 1px solid #ccc; padding: 5px;"> <p>Web Category:</p> <p><input checked="" type="radio"/> Web Site</p> <p><input type="radio"/> Public Web App</p> <p><input type="radio"/> Neither</p> <p>URL: <input type="text"/></p> </div> <p>Enter the ▼ URL for your web site or public web application.</p>



A valid URL

- All public facing URL's should work when clicked
 - HTTP and HTTPS
 - Internal Applications - Rights
- We will visit other services as the program matures

"Client Type"

- Thin Client – Browser Only
- Thin Client – plug in required.
 - Example, Application that requires Java.

<p>▼ Client Type:</p>	<p>Select the value that best describes the desktop components of this application:</p> <ul style="list-style-type: none">• Thin Client – browser only• Thin Client – plug-in required• Thick/Fat Client• Emulator• Desktop Only• Not Applicable
-----------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

“Used by Public”

- Used by Public = Yes for public facing
- Used by Public = No for internal browser applications

Field Name	Description and Use
▼ Used by Public	Select Yes if the general public uses this application and select No if the general public has no access to the application.



Archer's Role

- Scheduling
- Scan Tracking
- Vulnerability Tracking
- Scan Report Transfer
- Reporting

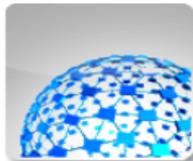


Agency Role

- Scan Times
- Someone Available
- Scan Report Distribution
- Vulnerability Remediation

More Information – IT Service Catalog

Web Application Vulnerability Scanning Services



Description

The purpose of these services is to provide your agency with a method to help identify web application vulnerabilities and secure your web applications while maintaining compliance with Commonwealth of Virginia information security standards. The service is able to identify over 600 web application vulnerabilities including the OWASP Top 10, configuration errors and many others. This service is intended to provide guidance for agencies with limited or advanced web application security expertise in house.

- Provides cybersecurity expertise with a diverse knowledge base
- Helps secure web applications and web services
- Eliminates cost of purchasing, implementing, maintaining and mastering web application vulnerability assessment tools
- Offers scanning and reporting for public-facing and internal web applications and services
- Delivers a platform-independent assessment with specific results
- Produces easy-to-read and interpret reports
- Delivers automated and manual scanning with manual results verification
- Provides remediation guidance and finding resolution validation

Web Application Vulnerability Scan and Reporting

The service includes an automated web application vulnerability scan, with manual crawl if required, a manual review of findings and a default report. The URL is then added to a scheduler for automated quarterly scanning and reporting. This enables your agency to identify vulnerabilities and focus remediation efforts, gauging the results and identifying new findings every 90 days from the reports. The commonwealth security and risk management (CSRM) web application vulnerability team will assist with interpreting scan results. Your agency is responsible for verifying and remediating the vulnerabilities that are identified.

The service, including the initial and quarterly scans and reports, is provided to all executive branch agencies and non-exempt institutions of higher education at no direct charge.

Cost summary

Price type: Fixed

Billing category: Usage-Based

Cost basis: per service selected

Total: \$0.00

http://shop.vita.virginia.gov/ProductDetail.aspx?id=6442472344&TX_ID=6442469742



Vulnerability Remediation

- The Standard
 - Progress
- Staff Augmentation
 - CIA Contract



Questions?

Bill Freda

CISSP, CRISC, GPEN, GSEC, GWAPT

bill.freda@vita.virginia.gov

804-416-6031



Archer Reporting Overview & 2016 Annual Report Preview

Mark Martens
Information Assurance Analyst

ISOAG
October 5th , 2016



Data Sets

Updates due EOY

Must reconcile to business processes
and audit plan



Reports

Agency Workspace

ent

Application Reports ▼

IT Security Aud

List of All Systems

Sensitive Systems

Non-Sensitive Systems with Sensitive Data Sets

SANS Top 20 Critical Control Findings



Reports

COV:Application Appears to be SENSITIVE

Drag a column name here to group the items by the values within that column.

Agency	Application Name ▲	Sensitive System
<u>Virginia Information Technologies Agency</u>	<u>Cardinal Interface</u>	No

Helper - Sensitivity Conflict Information

Yes - Business Processes FSPRD



Reports

Helper - Sensitivity Conflict

Information

Yes - Business Processes

FSPRD



Inconsistency in Sensitivity Rating

923 Applications



Lack of Remediation

532 Days
2,834 Findings



SANS Top 20 Critical Control Findings

30 agencies

1,785

663 days



Findings Closed current year

17 agencies
223 Findings
425 days



Risk - Bringing it all together

Inherent Risk -

Business Processes inform us about how critical the application is to the business.

Data Sets inform the application as to how confidential that information is and what applicable regulatory compliance that application is subject to.

Residual Risk -

IT Security Audits create findings that let us know what Sec501 Controls are missing

Exception Requests also inform us as to what controls are missing and possibly what compensating controls we have



Future Risk Measurements

Vulnerability Scanning

Vendor Profiles

Facilities Profiles



Questions

????????????????

You may also send any questions to :
CommonwealthSecurity@VITA.Virginia.Gov



Cyber Security Threat Analysis

Kathy Bortle

Commonwealth Security & Risk Management
Incident Response Specialist

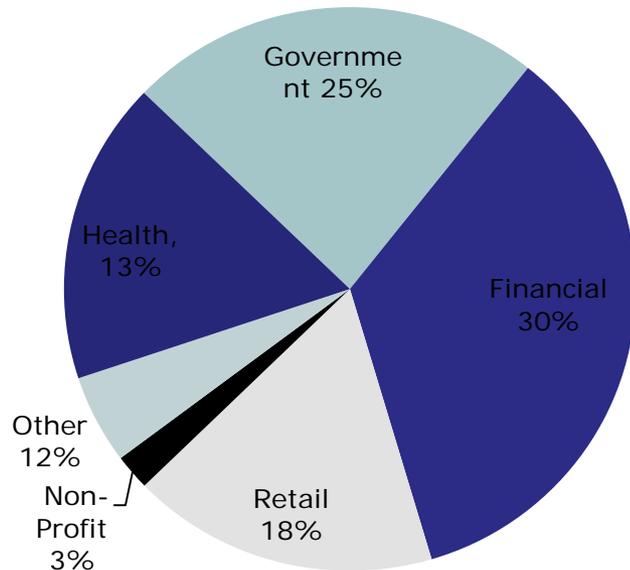
Oct. 5, 2016

Government Data Breaches & Attacks

Jan – Aug 2016

Virginia

- 70,810,780 attack attempts
- 619,971,104 spam messages blocked
- 52,448 pieces of malware blocked

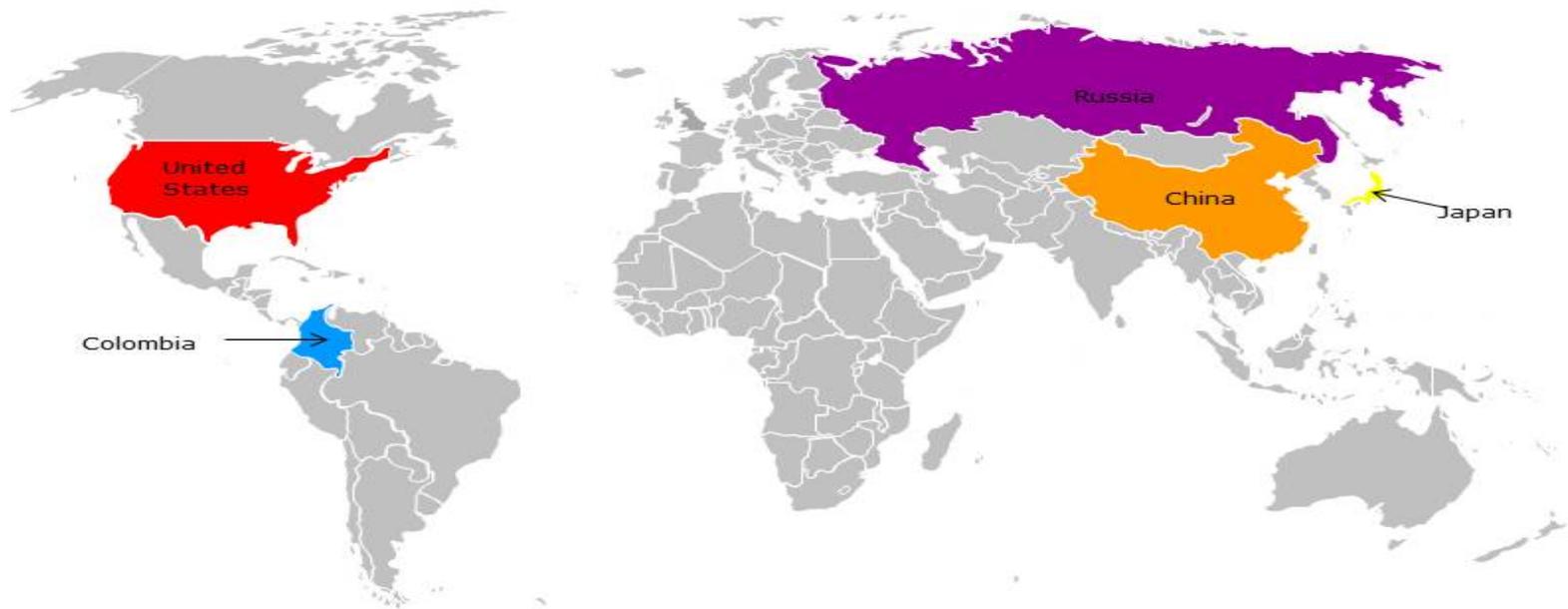


* transformed agencies only.

Security breaches of over 1 Million records

Source: Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, Jan 2015

Top 5 Origins of Attack Jan - Aug 2016

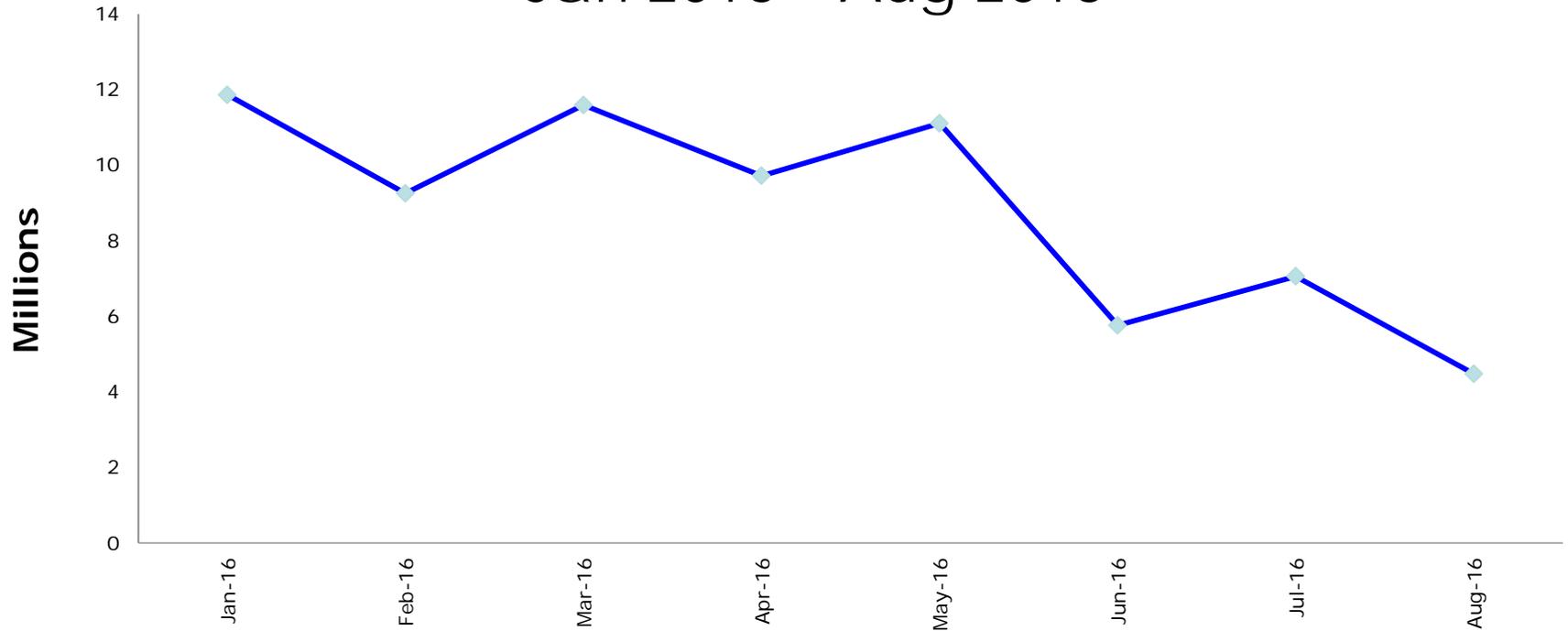


- 1st Place - United States
- 2nd Place - China
- 3rd Place - Japan
- 4th Place - Colombia
- 5th Place - Russia



70,810,780 Attack Attempts on CoVA Networks

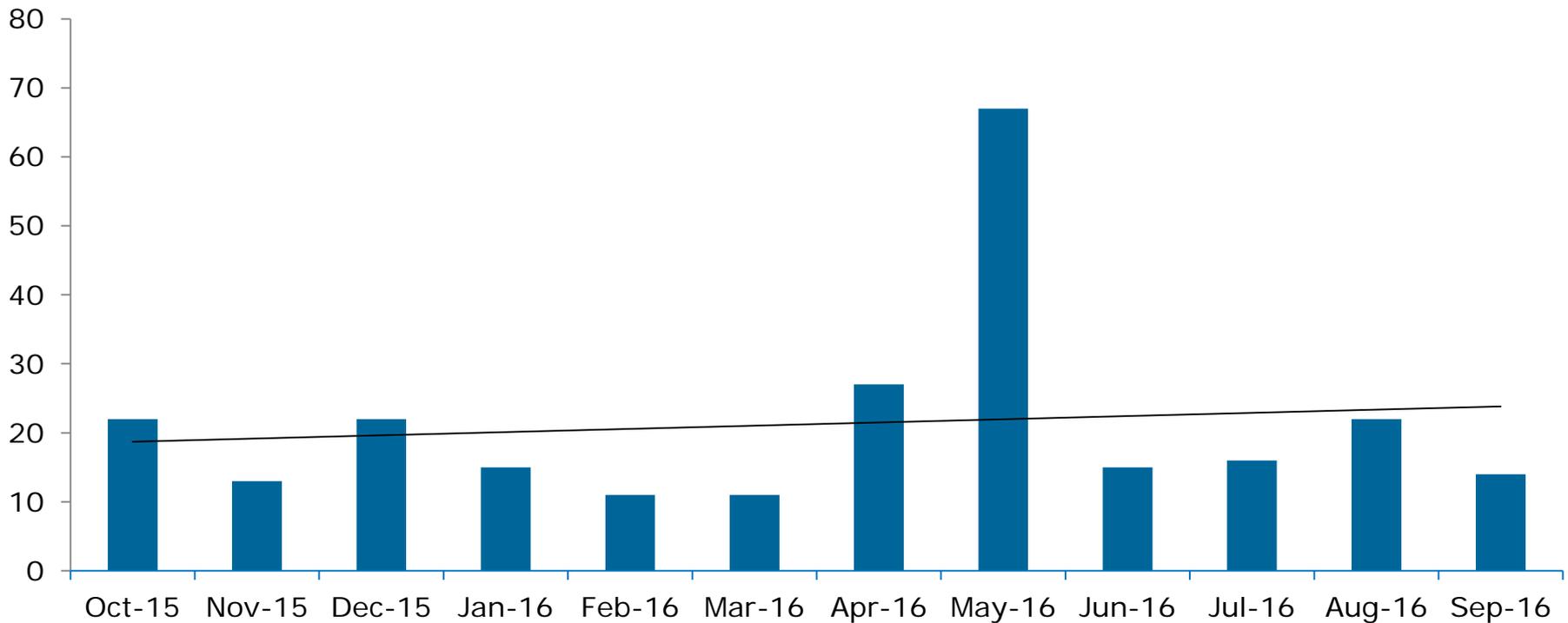
Jan 2016 – Aug 2016





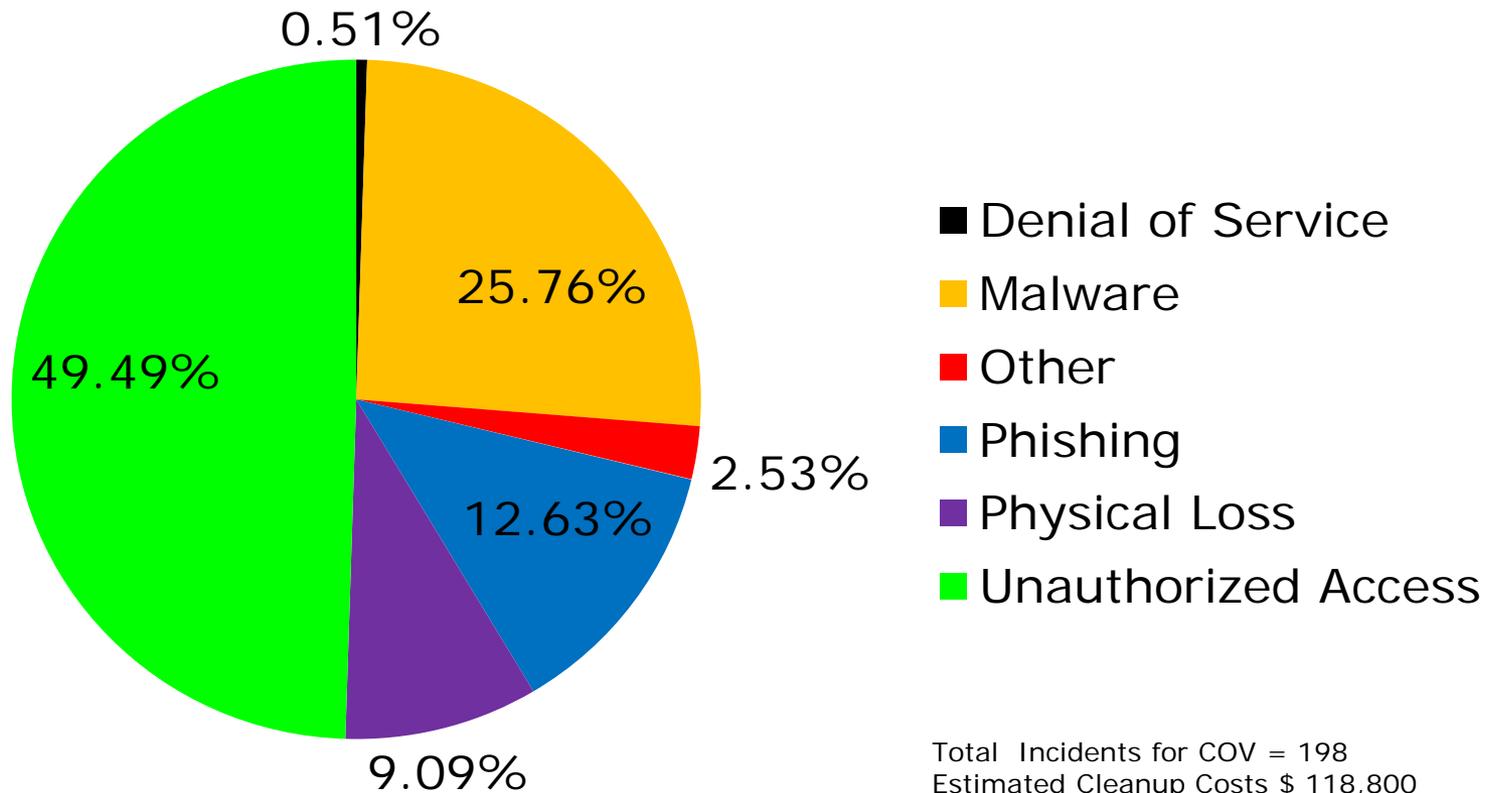
Increase In Cyber Security Incidents

Oct 2015 – Sept 2016



Security Incidents by Type

Jan – Sept 2016

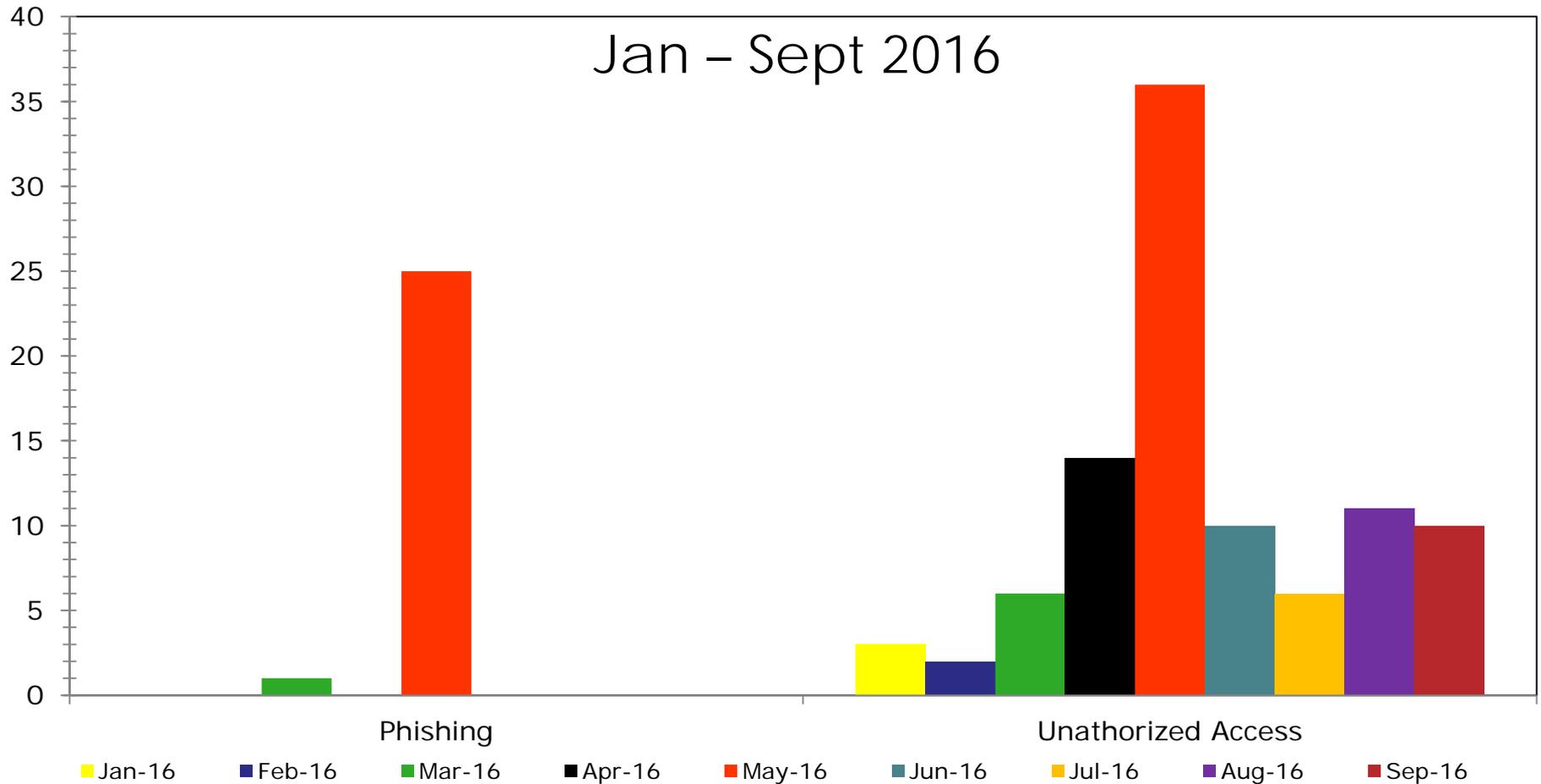




Cyber Security Threat Analysis

- 88 % of COV incidents are a result of Phishing Attacks and Malware infections.
- 80 % of Phishing attacks result in unauthorized access to COV systems.
- 64 % of Malware infections can be contributed to Trojan infections and Ransomware.

Phishing Attacks



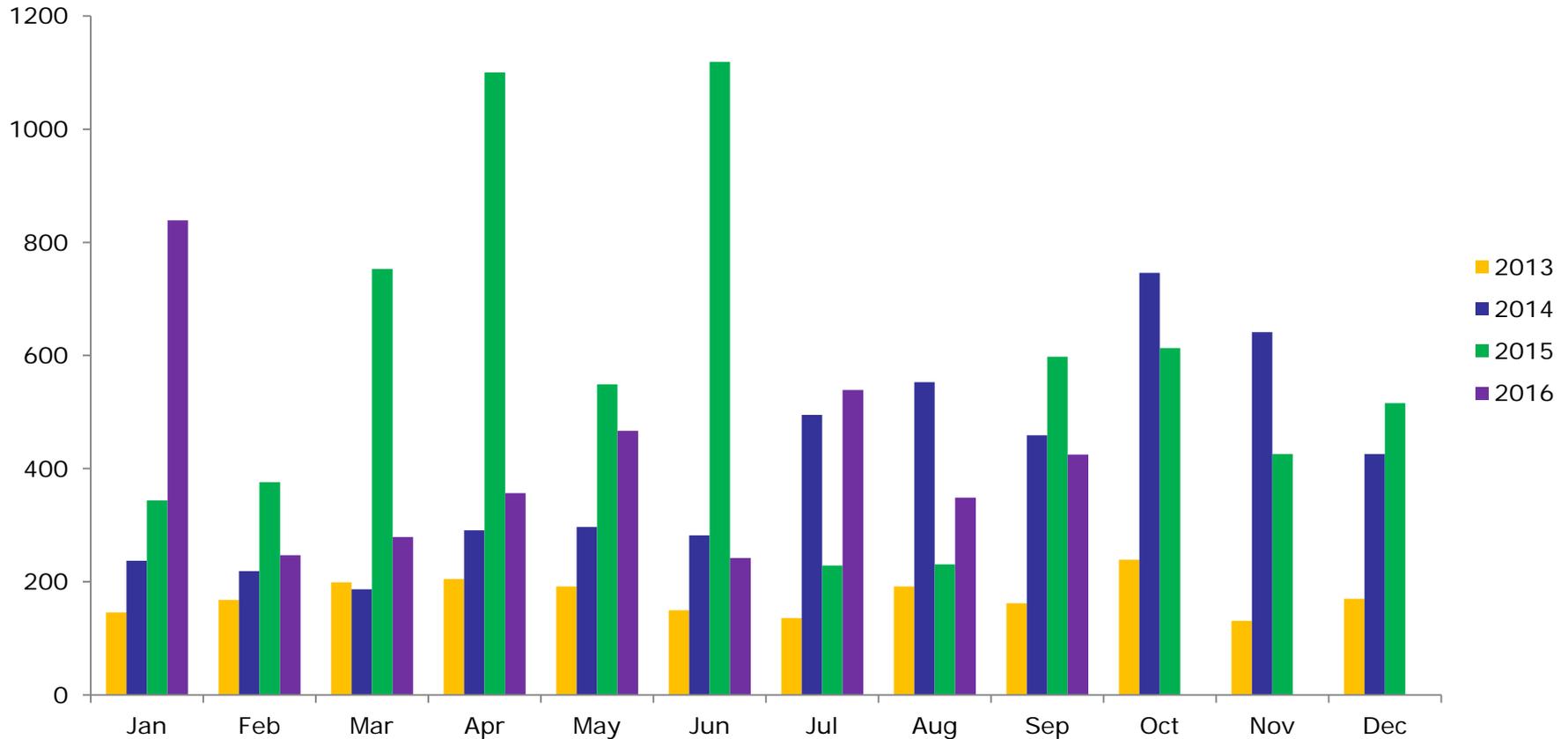


How to mitigate Phishing Attacks

- Security Awareness Training
- Use Simulated Phishing Campaigns to reinforce the training
- Discourage usage of state email address for personal accounts

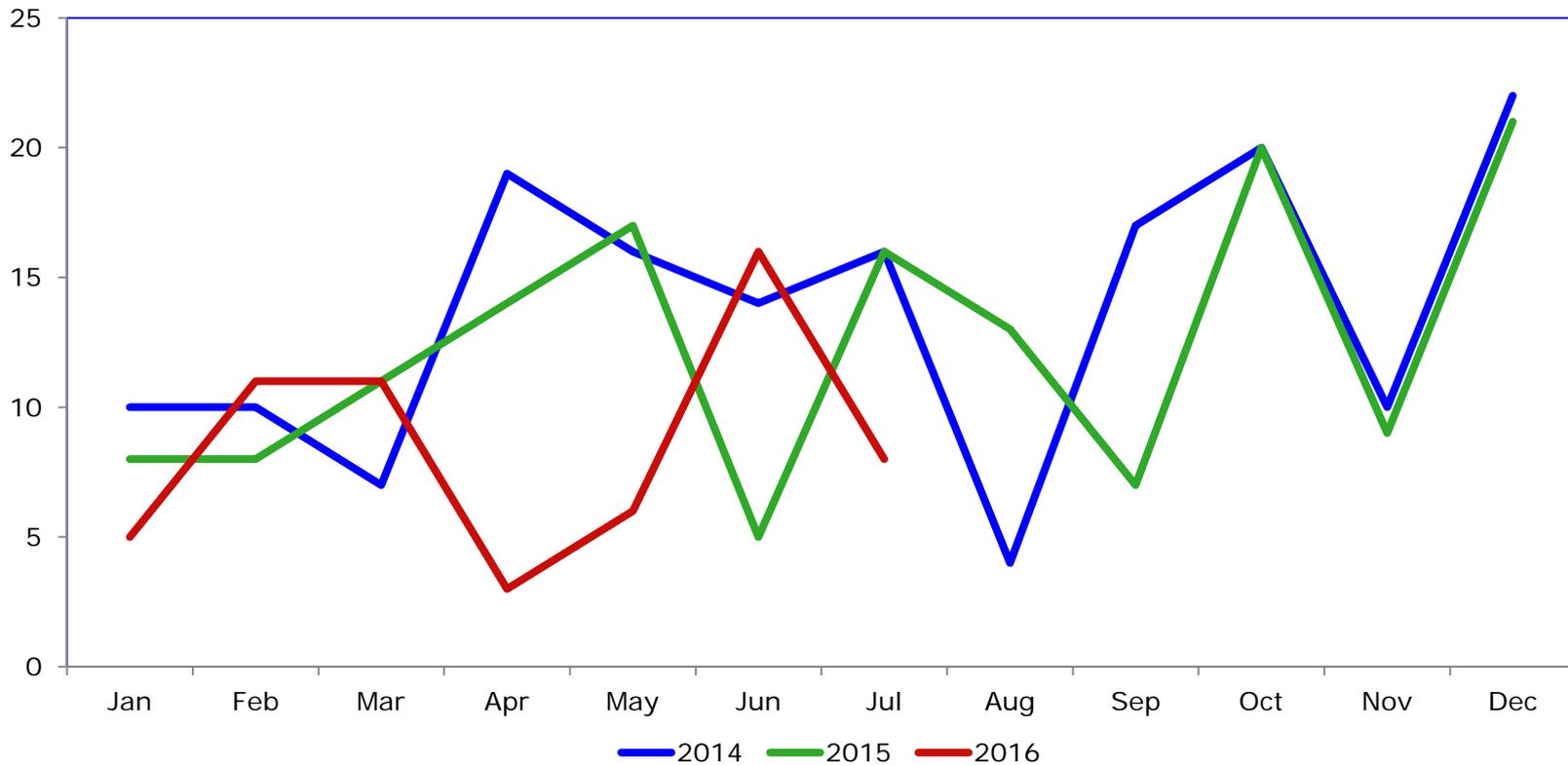
Vulnerabilities by Month

2013 – Sept 2016

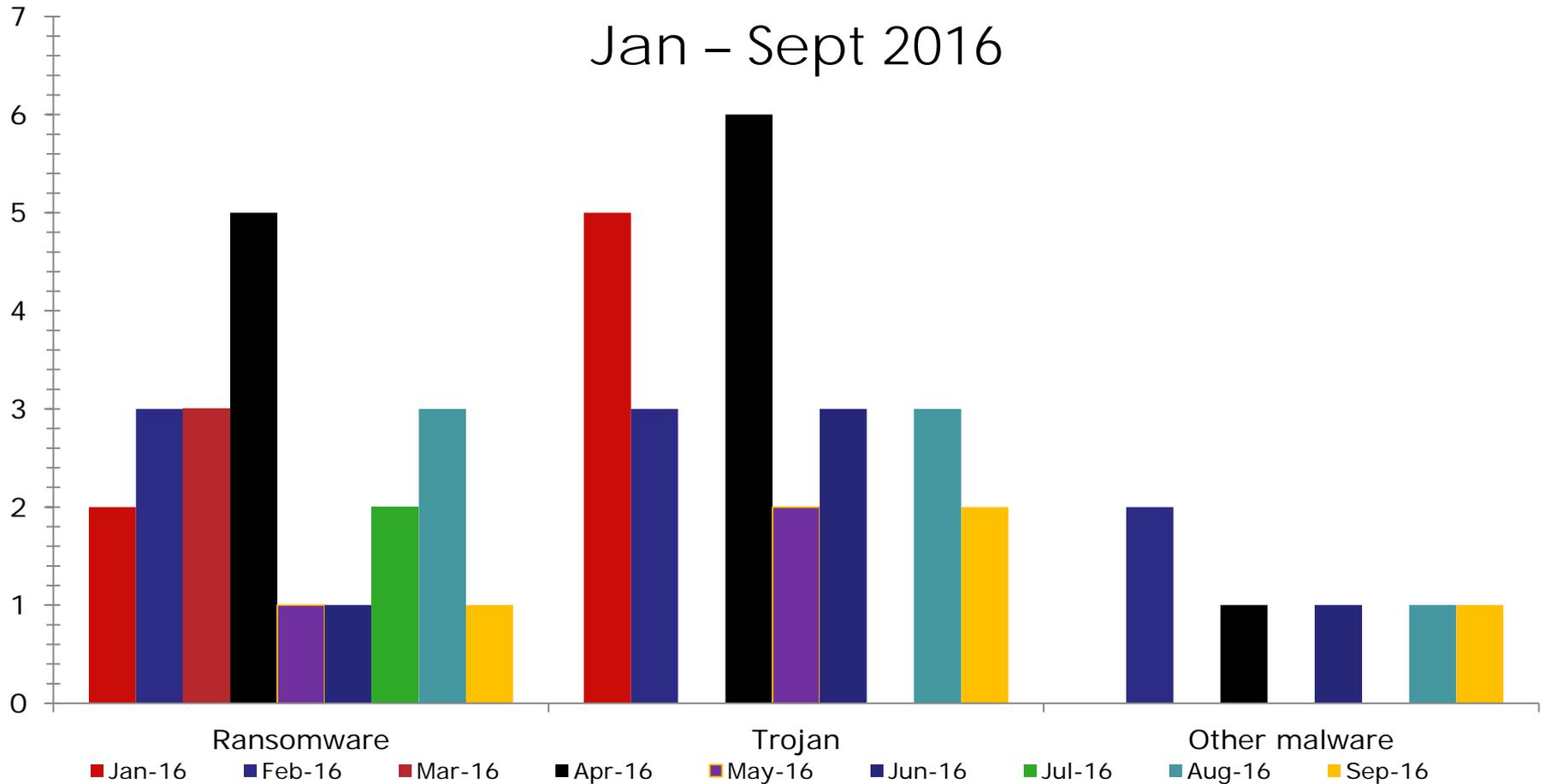


Critical (High) Vulnerabilities

2014 – Aug 2016



Malware Infections – COV systems



How to mitigate Malware infections

- Don't install any unnecessary software on devices.
- Keep virus protection up to date.
- Patch systems as soon as possible after appropriate testing.



Take Away

- Perform Annual Security Awareness Training
- Perform periodic simulated phishing attacks
- Discourage the use of work email address for personal business
- Use different passwords for each system/site to limit exposure
- Configure all accounts based on least privilege. (i.e. limit local admin rights and only use when required)
- Only install required software on systems.
- Patch systems as soon as possible after appropriate testing.
- Report all suspicious email and activity.



Virginia Information Technologies Agency

Cloud Security Update

Mark Craft

Cloud Security Architect



Updates to SEC 525

- Updated on 8/11/2016
- Removal of Section 1.8
 - Requiring all sensitive data be hosted within the geographical bonds of the Commonwealth
- Modified SI-2-COV(b)
 - “Applies all security updates as soon as possible after appropriate testing, not to exceed 30 days for implementation”



Cloud Hosting Evaluation

- Is the vendor FedRAMP Authorized?
 - FedRAMP based on NIST standards
- Does the vendor have a current SOC 2 Type 2 audit?
- Does the vendor have an approved security framework in place?
 - CSRM approved frameworks (TBD)

If Yes – (FedRAMP + Framework or SOC 2 Type 2 + Framework)

- Agency will have 90 days to perform a gap analysis

If No –

- Agency will need to do a full SEC 525 Controls audit or work with an independent third party to perform the audit



Cloud Hosting Evaluation (cont.)

What's next:

- CSRM will review

What we are looking for in this review:

- Do they have a current FedRAMP authorization
- Non-negotiable findings



Cloud Hosting Evaluation (cont.)

There is **no** guarantee of acceptance



Cloud Hosting Evaluation (cont.)

Continual Oversight

- FedRAMP Authorization must be updated
 - Vendor
- Security Audit ever 3 years
 - Agency or Vendor
- Risk Assessment



Questions

Questions??



Virginia Information Technologies Agency

Upcoming Events





Virginia Information Technologies Agency

National Cybersecurity Awareness Month 2016





National Cyber Security Awareness Month



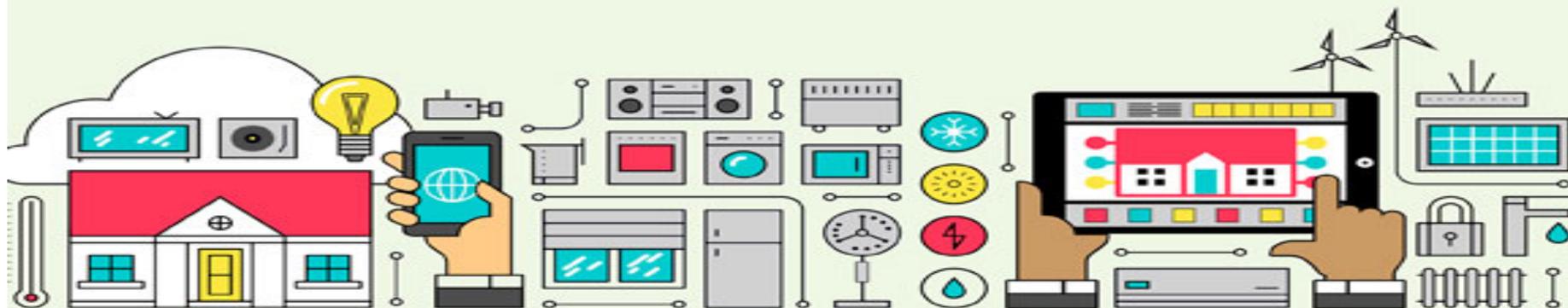
National Cyber Security Awareness Month



CyberAware

securing our online lives is a
SHARED RESPONSIBILITY

*Get involved this October and empower our global digital society to use the Internet **safely and securely.***





Weekly Themes

- | | |
|-----------------------|-----------------------------------------------------------------|
| Week 1: October 3-7 | Every Day Steps Towards Online Safety with Stop.Think.Connect.™ |
| Week 2: October 10-14 | Cyber from the Break Room to the Board Room |
| Week 3: October 17-21 | Recognizing and Combating Cybercrime |
| Week 4: October 24-28 | Our Continuously Connected Lives: What's Your ' App'-titude? |
| Week 5: October 31 | Building Resilience in Critical Infrastructure |



Resource Links

Gov. McAuliffe has proclaimed October as National Cybersecurity Awareness Month in the Commonwealth of Virginia.

<https://youtu.be/LPxM2A98mxE> (video)

To view the official proclamation

<https://governor.virginia.gov/newsroom/proclamations/proclamation/cybersecurity-awareness-month/>

2017 MS-ISAC Poster Contest

<http://www.vita.virginia.gov/security/default.aspx?id=11232>

2016 NCSAM Crossword Puzzle (Courtesy of DMV)

http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Information_Security_Awareness_ToolKit/2016/2016CyberSecurityMonthPuzzle.pdf



Resource Links

https://msisac.cisecurity.org/toolkit_ (update in progress)

www.us-cert.gov/ncas/tips

<https://staysafeonline.org/ncsam/>

<http://cyberva.virginia.gov/>

www.dhs.gov/national-cyber-security-awareness-month

<https://www.consumer.ftc.gov/media>

www.stopthinkconnect.org



Contact

CommonwealthSecurity@vita.virginia.gov
or
Tina.Harris-Cunningham@vita.virginia.gov



2016 VASCAN Conference

October 6 & 7 2016

The University of Mary Washington

Keynote Speaker:

Dr. Phyllis Schneck, Deputy UnderSecretary

Cybersecurity and Communications for the National Protection and
Programs Directorate (NPPD)

For More Information: <http://vascan.umwblogs.org/>



Next InfraGard Meeting

October 20, 2016

2:30pm – 5:45pm

Glen Allen Branch Library

10501 Staples Mill Road

Glen Allen, VA 23060

For More Information, contact Kathy.Bortle@vita.virginia.gov



IS Orientation

When: Thursday, December 8, 2016

Time: 9:30 – 11:30 am

Where: CESC , Room 1221

Presenter: Bill Freda

Register here:

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



Future ISOAG

November 2, 2016 1:00 - 4:00 pm @ CESC

Speakers: Alison P. Gise Johnson, PHD From VUU
Topic: Ethics in IT Security

ISOAG meets the 1st Wednesday of each month in 2016



Virginia Information Technologies Agency



SAVE THE DATE

COV Information Security Conference

Richmond, VA

2017

“Expanding security knowledge”



April 13 & 14

Contact: CovSecurityConference@vita.virginia.gov

ADJOURN

THANK YOU FOR ATTENDING

