



# ISOAG Meeting October 11, 2017

Welcome to CESC



# Welcome and Opening Remarks

Michael Watson

October 11, 2017



# ISOAG October 11, 2017 Agenda

- |  |                        |
|--|------------------------|
| I. Welcome & Opening Remarks                 | Mike Watson, VITA      |
| II. MSI Update                               | Mike Watson, VITA      |
| III. Risk Management                         | Jon Smith, VITA        |
| IV. PGR/OSI Process                          | Jon Smith, VITA        |
| V. Security Standard Changes (501/525)       | Joy Young, VITA        |
| VI. Cyber Security Awareness Month/ISO Cert  | Tina Harris Cunningham |
| VII. Archer Datapoints/Updates (CETR)        | Mark Martens, VITA     |
| VIII. Auditing Issues with Contracted Audits | John Musgrove          |
| IX. Threat Overview                          |                        |
| X. Upcoming Events                           | Mike Watson, VITA      |



# IT Sourcing Update – Security Services

**Michael Watson, CISO**

VITA

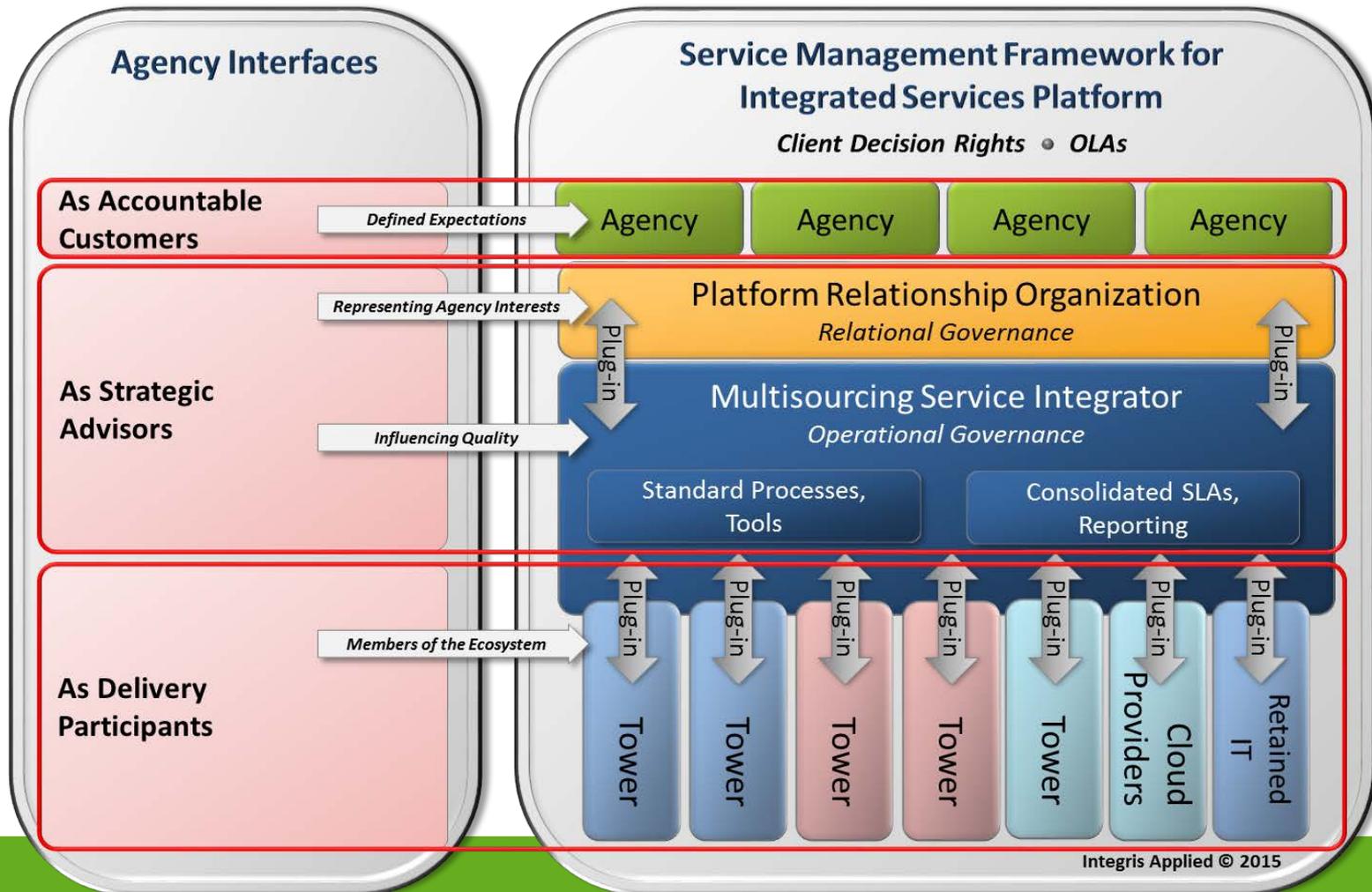
---

ISOAG

October 11, 2017



# Future Services Delivery Platform



# Current Security Environment



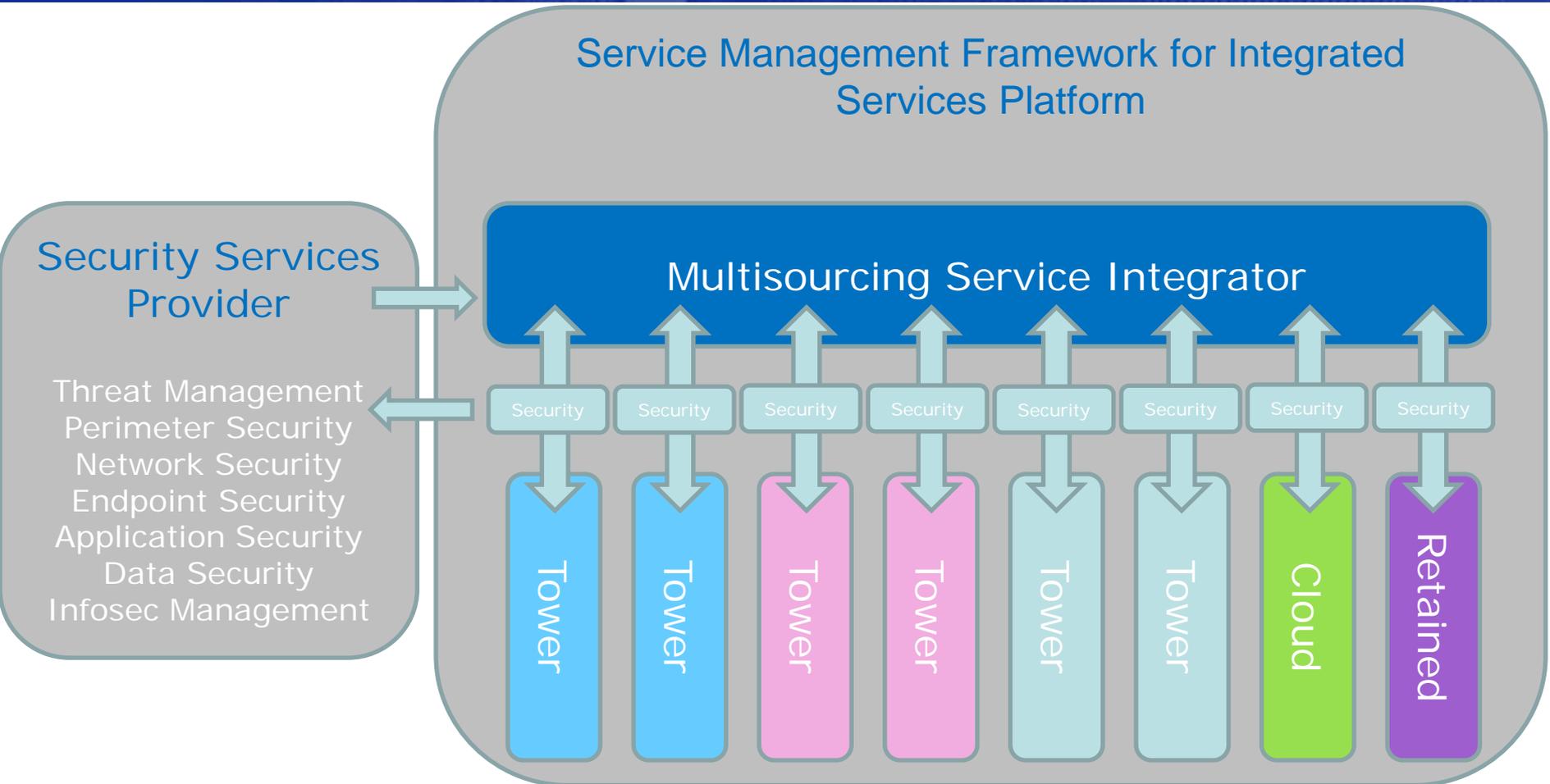


## Service Areas

- Perimeter Network (DMZ)
- Internal Network
- Endpoint (Server and Workstation)
- Data Protection
- Application
- Threat Management
- Information Security Program



# Security Services Delivery





# ITISP Improved Security Environment

- Separation of Duties
  - Removes the conflict of interest in identifying and reporting vulnerabilities
  - Prevents disabling security tools in favor of easier operational circumstances
- Improved Transparency
  - Allows direct access to security tools so that VITA and agencies can react more quickly to threats in the environment
- Opportunities for New Technology
  - Established refresh rate
  - New security tools and technology can be integrated as the market releases them



## Possible Changes

- Out of Scope Definition
- Agency Integration into Security Services
- Increased Technical Security Focus
- More Uniform Application of Technical Security Controls



# Questions?





# Risk Management

Jonathan Smith

---





# Agenda

- **Nationwide Cyber Security Review (NCSR)**
- **Cyberstorm VI (National Cyber Security Exercise)**
- **Risk Management activities**



# Nationwide Cyber Security Review (NCSR)

## What is the NCSR?

- Free annual self assessment based on the NIST Cybersecurity Framework, sponsored by DHS and MS-ISAC
- NCSR evaluates cybersecurity maturity across the nation
- Using the results of the NCSR, DHS delivers a biyearly anonymous summary report to Congress providing a broad picture of the cybersecurity maturity across the State, local, territorial, and tribal (SLTT) communities



## NCSR – How does it work?

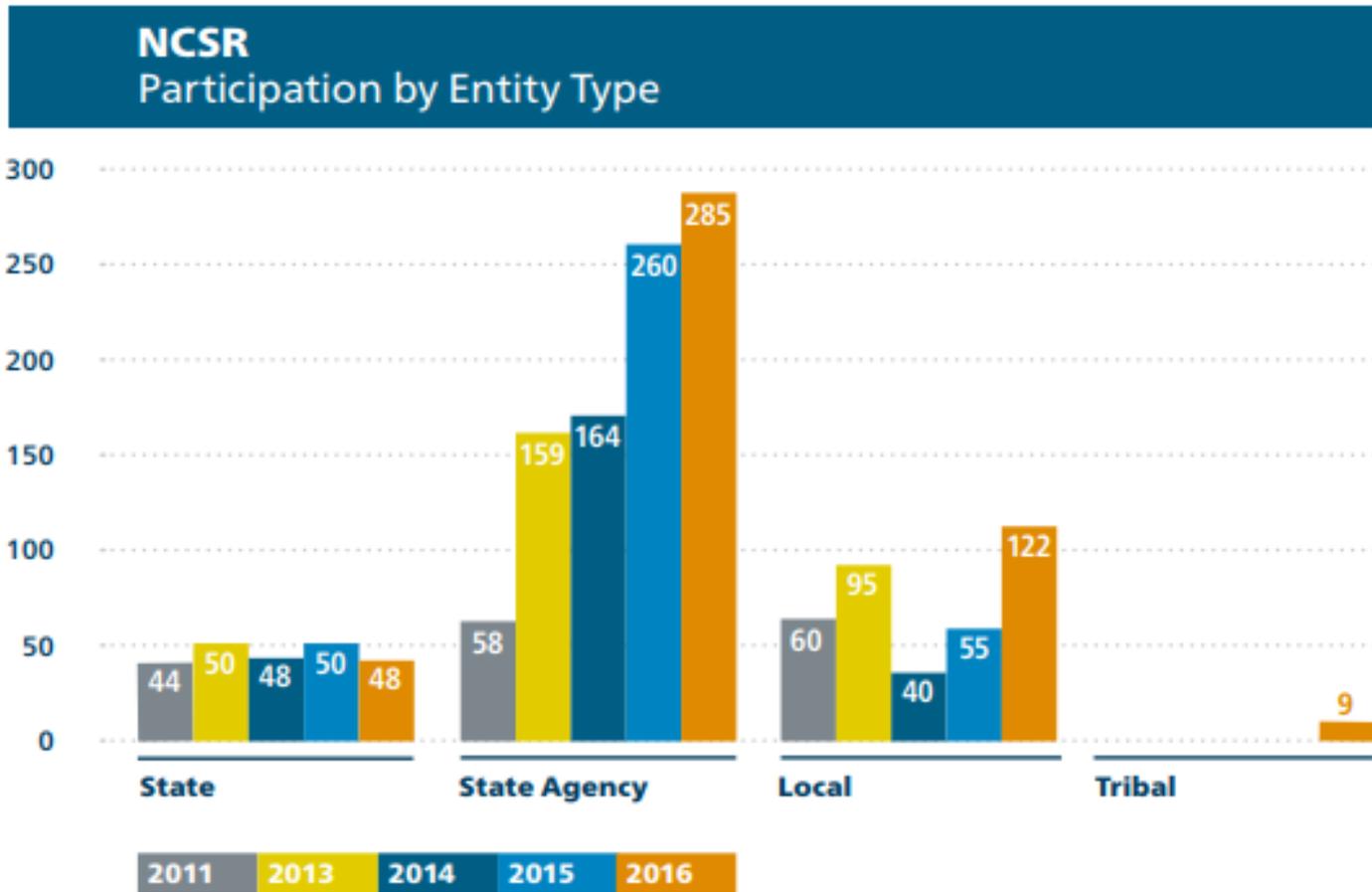
- Question set is based on the NIST Cybersecurity Framework
- Covers core components of cybersecurity and privacy programs
- Designed to measure entities' progress against the Cybersecurity Framework
- Hosted on the Commonwealth RSA Archer application
- Designed to be completed in about an hour



## NCSR (continued)

- **Virginia (CSRM) has participated in the NCSR since 2012 at an enterprise level**
- **2015 - Commonwealth agencies were asked to participate**
  - 50 States participated
  - Approximately 15 Commonwealth agencies participated
- **2016 – NCSR was moved to the Archer application and provided to CSRM to facilitate to agencies**
  - 48 States participated
  - 53 Commonwealth agencies completed the assessment
- **2017 – NCSR is seeking expanded state agency participation to further grow the peer groups (public safety, health, transportation, etc...)**

# NCSR (continued)





## NCSR – 2017 Timeline

- The 2017 NCSR will be uploaded to the Archer for each agency after testing is completed
- Agency ISO's will be notified of the availability of the NCSR and instructions via email from Commonwealth Security
- Deadline for the completion of the NCSR is Dec. 15, 2017
- Participation will be tracked as a data point for the 2017 Annual Report on Information Security
- Questions regarding the 2017 NCSR should be directed to your CSRM security analyst or emailed to [commonwealthsecurity@vita.virginia.gov](mailto:commonwealthsecurity@vita.virginia.gov)



## Cyberstorm VI

- Cyberstorm is a cyber incident response exercise sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and part of ongoing efforts to assess and strengthen cyber preparedness; examine incident response processes in response to ever-evolving threats; and enhance both information sharing and partnerships among federal, state, international, and private sector partners
- Play focuses on policy, procedure, information sharing, coordination, and decision-making during a simulated cyber crisis



## Cyberstorm (Continued)

- Participants represent a diverse set of DHS stakeholders, including federal agencies, State governments, critical infrastructure sectors, private industry, and international partners.
- Exercise will take place in May 2018
- Some scenarios being considered include impacts to state election systems, transportation systems, critical infrastructure, and state agencies.
- CSRM is seeking participation from Commonwealth agencies as both players and planners. Please contact [jonathan.m.smith@vita.virginia.gov](mailto:jonathan.m.smith@vita.virginia.gov) for more information.



## Risk Management activities

- BIA
- Data set inventories
- Asset (system/device) inventories
- Risk assessments and quarterly updates
- Findings remediation (audit, risk, ORI, vulnerability scans)
- Procurement Governance
- IT Strategic Planning & Operational Risks/issue



## ORIs

### Operational Risks/Issues

- Findings that represent a potential risk or issue to the operations of business processes
  - Examples include, but are not limited to end of life software/hardware, insufficient audit or security/risk management programs, etc...
- ORIs require a business requirement for existing technology (BReT) in the agency IT Strategic Plan (ITSP)
- What if an ORI appears to be incorrect or has been remediated?
  - Contact your CAM or CSR
  - Be prepared to show evidence, such as a work request.



# Questions?





# Policy Update Preview SEC501, SEC525, and SEC520

**Joy Young**  
Information Assurance Analyst

---

ISOAG  
October 11, 2017



## Policy Updates

- **SEC501: IT Information Security Standard**
- **SEC525: Hosted Environment Security Standard**
- **SEC520: IT Risk Management Standard**



## SEC501 and SEC525

- **CA-8 Penetration Testing**
- **1.5 Exceptions to Security Program**
- **SC-28 Protection of Information at Rest**
- **IA-5 Authenticator Management**
- **MP-1-COV Media Protection Policy**



## SEC525

- **RA-5-COV**
- **SC-7 Boundary Protection**
- **PE-18-COV Location of Information System Components**



## SEC520

- **Framework**
- **Business Impact Analysis**
- **Risk Assessment Planning**
- **Vulnerability Scanning**



*Virginia Information Technologies Agency*



# Thank You



*Virginia Information Technologies Agency*

# October is: National Cyber Security Awareness Month





## National Cyber Security Awareness Month

### Governor's PSA on NCSAM:

<https://www.youtube.com/watch?v=LPxM2A98mxE&feature=youtu.be>

### Proclamation:

<http://governor.virginia.gov/newsroom/proclamations/proclamation/2017-cybersecurity-awareness-month/>

### MS ISAC 2018 "Kids Safe Online Poster Contest"

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



Virginia Information Technologies Agency

# ISO Certification





## ISO Certification

### To be Certified:

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

### To be Re-certified:

- *Agree to the Commonwealth IT Security Code of Ethics*
- *Attend mandatory annual October Meeting*
- *Take IS Orientation once every 2 years*
- *Take 20 hours of Continuing Education in the CY (including 1 course in the LMS)*



## Mandatory ISO Meeting

- *We will have a mandatory meeting of all ISOs in October.*
- *We encourage all primary ISOs to attend this meeting in person.*
- *If you are a primary ISO, and cannot attend, you may designate the backup ISO to attend in your place.*



## Attend IS Orientation at least once every 2 years

- All primary ISOs are required to attend this 2 hour session at least once every 2 years. The requirement to attend cannot be delegated to a backup ISO or other person unless approved by the CISO. However, backup ISO's and other interested persons are encouraged to attend.
- We are continually changing and evolving the content provided in the IS Orientation session. Some sessions will be offered that will look closer at specific ISO learning areas: Risk Assessments, Policies, Control Implementation, Security Plans, etc. **Search ISO Academy in the LMS for courses.**
- Schedule of orientation sessions and registration link:
- <http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>
  - Last Orientation is Dec. 14th



## Meeting Continuing Education Requirements

- *Take additional IT security courses in the LMS ISO Academy (1 course=1 hr)*
- *Attend training courses or seminars related to IT Security*
- *Attend IT security conferences*
- *Attend ISOAG Meetings*
- *Attend chapter meetings of a recognized IT security organization*
- *Take IT security related academic courses at a higher ed institution*



## Meet Continuing Education Requirements

- *Complete IT Security related webcasts, podcasts or other computer based training*
- *Read IT security related books or articles (50 pages = 1 hour) (limit of 10 hrs/year)*
- *Publish an IT Security related book or article*
- *Attend vendor sales/marketing presentations (limit of 5 hrs/year)*
- *Teach or present on an IT security related topic*
- *Serve or volunteer for committee work on the COV Security Council*



## Contacts

- *[Edward.Miller@vita.virginia.gov](mailto:Edward.Miller@vita.virginia.gov)*
- *[Tina Harris-Cunningham@vita.virginia.gov](mailto:Tina.Harris-Cunningham@vita.virginia.gov)*



# 2017 Data Points

**Mark Martens**

Information Assurance Analyst  
IT Security Governance

---

ISOAG

October 11<sup>th</sup> , 2017



## Data Point Emails

Data point emails going out with increasing frequency as we get closer to the end of the year.



## What do we do with that info?

Check to see what you are missing and need to submit to us.

Be wary of having submitted something December 2016.



## What else do we do?

Review the steps from the Agency Executive Dashboard



## How?

Dashboard: Agency Executive Dashboard

Welcome, Mark Martens

### Datapoints Step-by-Step

Agencies should use the following steps to ensure that their agency has addressed any issues regarding the data used to evaluate an agency's information security programs. The steps help ensure the information used to create the annual report evaluating agency information security programs is as accurate as possible. Please follow the below steps to make sure there aren't any discrepancies in the data provided to Commonwealth Security and Risk Management. If there are any issues, please contact your analyst or CommonwealthSecurity@vita.virginia.gov.

- Step 0 - Review CETR

- A initial check of CETR should be done by the agency to make sure that the application inventory is as up to date as possible. Applications that are not listed in CETR are not included in Archer. Systems must be added to CETR to be available in Archer. If your agency does not use CETR, contact your CSRSM analyst.

- Step 1 - BIA

- [Review business processes \(BIA\)](#). --

NOTE: If changes are required open the business process and change the **Agency Submit Status** field from **Submitted** to **In Process**. Changing the value of the status field will allow the fields to be edited by the agency.

- Step 2 - Data Sets

- [Map data sets that aren't mapped to applications \(click SEARCH after you click this link\)](#)
- [Data Classification Inventory](#)

- Step 3 - Applications

- [Review Applications that are not associated to Business Process and/or Data Sets](#)
- [Associate Devices that are not mapped to Applications](#)
- [Associate Applications that are missing Devices](#)
- [Identify if the Application appears to be marked with the incorrect sensitivity level](#)
  - Does the Business Process indicate Sensitive?
  - Does the Data Set indicate Sensitive?

- Step 4 - Risk/Audit Plans

- [Sensitive applications missing scheduled audits or risk assessments in the next 3 years](#)



# Help Icons to the Rescue

## ▼ AGENCY SCORECARD DATA



ISO  
Certification  
Status:

## ISO Certification Status

**Pass** - The primary ISO is certified due to attending IS Orientation biennially, 1-3 hrs KC Training annually, and the October ISOAG Meeting

**Incomplete** - The ISO met all other requirements but did not attend the mandatory ISOAG meeting in October

**N/C** - The primary ISO is NOT certified



# More help with helpers

## 3 Year Audit Obligation

X% - The percentage of audit work completed as measured against the agency's security audit plans over the past three years

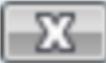
N/A - Not applicable as the agency had no audits due

N/C - The agency head has not submitted a current security audit plan



# Help with BIA Status

## BIA Status



"N/C" - the data provided is incomplete, and there is an active application without any business processes

x% - This is the percentage of business processes that have approval at this time



# Help with 3 Year Risk Assessment

## 3 Year Risk Assessment Obligation

X% - The percentage of risk assessment work completed as measured against the agency's sensitive systems over the past three years

N/A - Not applicable as the agency had no risk assessments due

N/C - The agency head has not submitted an audit plan



## What if there is no helper icon?

- That often happens when no calculation is necessary on Archer's part.
- The field is likely not scored with a percentage and either your agency submitted, didn't submit, or submitted some sort of partial and that is what is reflected in the scoring.



## Still need help

- Phone a friend -
- CSRM Analyst is listed above your agency scorecard



## Vulnerability Scan Results

- As long as you are working with Bill Freda to allow him to scan, you should be good
- Vulnerability Scan calculations (for future use)
  - Sensitive System
  - Public Web App
  - In Production
  - Checks for scan associated with app every quarter



# Vulnerability Scan Results

- Findings and high level scan info viewable in Archer



## CETR

- December target for asking AITRs to use Archer in place of CETR
- Certify Data moves to Archer
- AITRs in Archer...



## What Can AITRs do in Archer

- Enter new applications
- Retire existing applications
- Certify their data
  - Reports, Dashboards, instructions coming soon



## Certify Data

- Looks for each application to have an association with a:
  - Business Process
  - Data Set
  - Device

🔍 Certify Data:

🔍 Cannot Certify due to: No business process associated - No device associated

Sensitivity Conflict: No



## What can ISOs enter in Archer

- Business Processes
- Data Sets
- **IT Security Audit Plans**
- **Scheduled IT Security Audits**
- **Risk Assessment Plans**
- **Scheduled Risk Assessment Plans**
- Devices
- Remediation Plans (quarterly updates)



## Workflows updated

- Agencies **submit new**
- CSRM receives notification
- CSRM reviews and approves/rejects
- Agency receives notification



## Editing Existing Record

- Agency ISO enters record
- Agency ISO clicks “edit”
- Agency ISO changes “agency submission status” from “Submitted” to “In Process”
- Agency edits relevant record fields
- Agency changes “agency submission status” to “Submitted”



## Eliminate Duplication

- Agency head must still be copied on IT Security Audit Plans
- Audit Plans can be entered directly in Archer for approval by CSRM.
- Once entered, can be exported as PDF and sent to [commonwealthsecurity@vita.virginia.gov](mailto:commonwealthsecurity@vita.virginia.gov) with agency head copied



## Maintenance & Cleanup

- Archer searches now populate with more relevant fields
- Unused fields removed
- More emails go out when CSRSM approves submissions (Risk, Audit, BIA)
- Alerts now go out for expiring Risk Assessment Plans



# More Maintenance & Cleanup

- Eliminated Duplicative fields between CETR/Archer
- Calculated C,I,A from data sets and Business Processes (takes highest)

## ▼ APPLICATION RISK INFORMATION

Application Inherent Risk: ●

Application Residual Risk: **Not Rated**

Criticality Rating: **Not Rated**

🔗 Sensitive as to Yes  
Confidentiality:

🔗 Sensitive as to Availability: Yes

Last Agency IT Risk  
Assessment:

Next Agency IT Risk  
Assessment:

Last IT Security Audit: 12/31/2014

Next Scheduled IT Security  
Audit:

🔗 Sensitive as to Integrity: Yes



## Even More Maintenance & Cleanup

- Many lows in a Business process no longer add up to a value of “High” for Availability
  - Impact to Life
  - Impact to Safety
  - Impact to Customer Service
  - Impact to Finances
  - Mission Essential Function still makes it “High”



## Maintenance & Cleanup for days

- Not rated changed to “No Impact” for business process impacts
- Streamlined BIA template can be found on Vita’s website. The fields and values that can be selected are an exact match to Archer.



## Future Plans

- Consolidate IT info under one tool
- Allow agencies to conduct Risk Assessments using Archer generated assessments
- Migration of Data exchange from CETR to Archer
- Migration of application languages from CETR to Archer



## Random Stats

- 535 applications with no business process
- 47 Sensitive systems not audited, no planned audits
- 1051 Sensitive Systems
- 277 Sensitivity conflicts (marked not-sensitive but associated with business process or data set marked sensitive)



# Questions

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

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



Virginia Information Technologies Agency

# Outsourced IT Security Audits

**John Musgrove, MS, CISA**

Director, IT Security Audit Services

---

Group/Event Name

Date



## Introduction

- Director, IT Security Audit Services @VITA
- Formerly at VCU/H Audit & Compliance
- IT Geek, Navy Veteran, World Traveler



## IT Security Audits

- IT Security Audit Standard (502) Requires
  - Sensitive Systems be audited every 3 years
  - Adherence to auditing standards
  - Standard clearly stated in audit report
  - Agency Head / designee provide CAP
  - Submission to Commonwealth Security



## Audit Standards

- Audit methodology adherence to
  - GAGAS: Generally Accepted Government Auditing Standards, also known as Yellow Book
  - IPPF: International professional practice framework, also known as Red Book
- Alternatively, with explicit declaration
  - ITAF: ISACA's Professional Practice Framework for IS Audit/Assurance
  - AICPA: American Institute of CPAs standard



## Audit Report Language

- Should state, unequivocally:
  - Standard used for audit framework
  - Any suspected independence conflict
  - Period of review
  - Scope of work
  - Control families NOT considered/tested



## Corrective Action Plan (CAP)

- Agency Head / Designee Must
  - Submit CAP with report
  - Review unresolved issues annually
  - Approve exception requests for acceptance of risk



## Outsourced Work

- Agency is responsible for:
  - Managing engagement
  - Submission to CSRM
  - Ensuring compliance with standards
- CAI adding language to SOR/SOW
  - Requires disclosure of standard
  - Requests Proof of compliance
    - Peer Review (yellow) QAR (red), or equivalent
    - New Firms: QA, charter, procedures, Review Date



# Compromised Independence

- Audit Team  $\neq$  Risk Assessment Team
  - Independence can be compromised if the same personnel do both
  - Teams, if separate, should not share data
  - Inherent risk of COI for an agent to 'find' an issue, then charge to correct it



## Contact Me

- [John.Musgrove@vita.virginia.gov](mailto:John.Musgrove@vita.virginia.gov)
- 804-416-5424 Desk at CESC
- On LinkedIn
- [in/john-musgrove-69366728](https://www.linkedin.com/in/john-musgrove-69366728)



# Upcoming Events





Virginia Information Technologies Agency

# 2017 Threat Analysis

**Kathy Bortle & Dean Johnson**

Commonwealth Security & Risk Management  
Incident Response Team

---



## Year In Review

### Threat Trends -

- Business Email Compromise – \$5.2 Billion estimated loss, surpassed Ransomware.
- Phishing becomes the # 1 attack vector for data breaches.
- Malicious spam (malspam) becomes the #1 attack vector for malware infections.

### Top 5 Malware Infections in the Wild –

- Redmya/Ramdo
- Kovter\*
- Zeus
- Timba
- Emotet\*



## Year In Review (cont.)

### Important Events for 2017

#### January -

- SHA-1 Certificates End of Life – Firefox v52 & Chrome v57 drop support. Microsoft to drop support mid-2017.
- Microsoft eliminates monthly security bulletins. Patch Tuesday is now done by CVE instead of product.
- DHS declares election systems critical infrastructure

#### February -

- Tax Fraud Reporting Scams
- W-2 Info Phishing Scams



## Year In Review (cont.)

March – Apache Struts vulnerability that leads to Equifax breach

May -

- WannaCry Ransomware released. Exploits Microsoft SMB shares.

June –

- Purchase Order Fraud Email Scams

July 4<sup>th</sup> 2017 – FBI takes down AlphaBay Marketplace.

AlphasBay was a site on the dark web owned by Alexandra Cazes. The site contained listings for Fraud, Drugs & Chemicals, Guides & Tutorials, Counterfeit Items, Digital Products, Jewels & Gold, Weapons, Carded Items, Services, Other Listings, Software & Malware, and Security & Hosting. This site was accessible using a TOR client.



## Year In Review (cont.)

August –

- CEO Compromise Scam - Results in a wire transfers, targets finance depts., spoofed or compromised executive account, millions lost
- Attorney Impersonation Scams
- Purchase Order Scams continue
- CCleaner - distribution channel is compromised. Malware (FloXif) included in Aug 15<sup>th</sup> & Aug 24<sup>th</sup> releases. Vulnerability update released on Sept 15<sup>th</sup>. Users should check versions.



## Year In Review (cont.)

September –

- Hurricane Related Scams – Attackers creating fake domains to get donations rerouted to them.
- Equifax Breach Announced – Attackers also creating fake domains to steal personally identifiable information (PII).
- BOD 17-01 - Sept 13<sup>th</sup> – DHS issued BOD (Binding Operational Directive) 17-01 directing federal agencies to discontinue using Kaspersky products
- Sept 19<sup>th</sup> - Email Hoax Extortion Scheme – Attacker threaten to execute a Distributed Denial of Service (DDOS) attack on company if not make a Bitcoin payment.



## Year In Review (cont.)

### Important Events for 2017

October forward....

DNSSEC Key Signing Key Rollover –

Oct 11, 2017 – New KSK begins to sign the root zone key set

Jan 11, 2018 – Old Key is revoked.

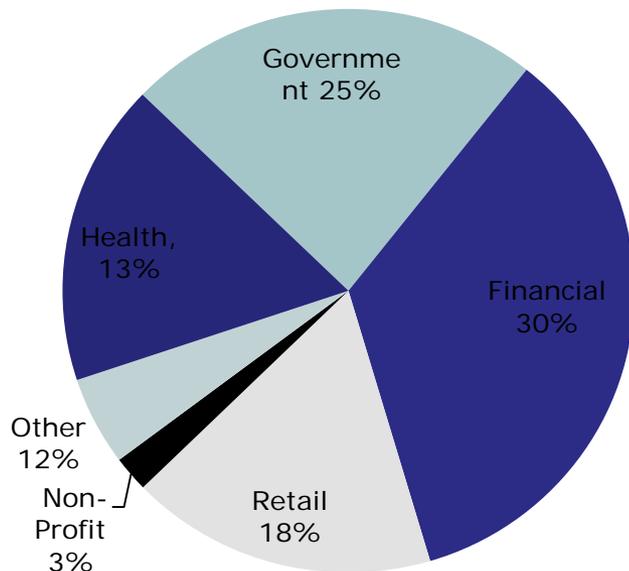
If you use DNSSEC enabled and are using the Root Zone ("."), then you need to update the Root Key. – Configured automatic key rollover or manually update the key

## Government Data Breaches & Attacks

Jan 2017 – Sept 2017

### Virginia

- 29,551,652 attack attempts
- 477,362,569 spam messages blocked
- 324,391 pieces of malware blocked

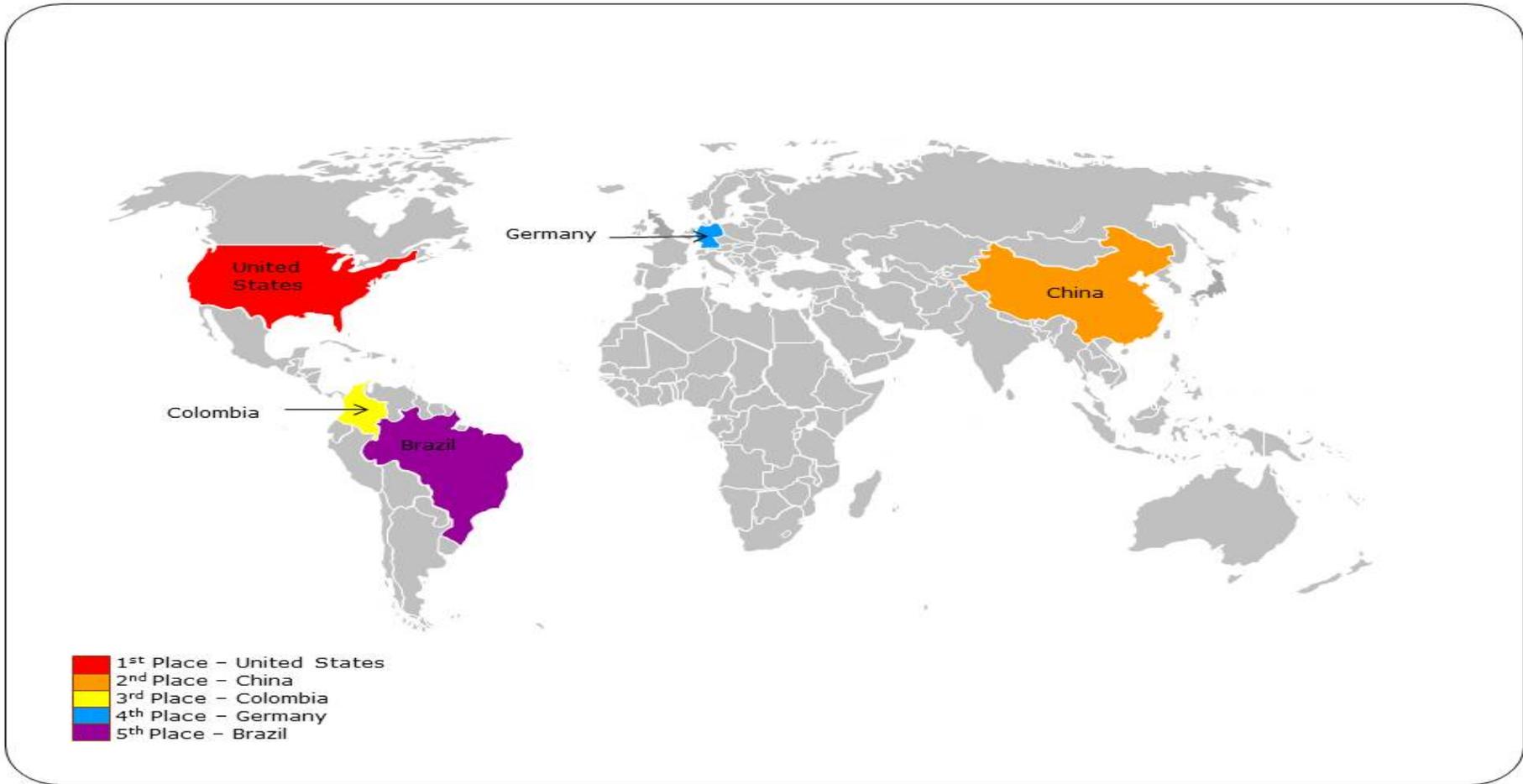


\* transformed agencies only.

### Security breaches of over 1 Million records

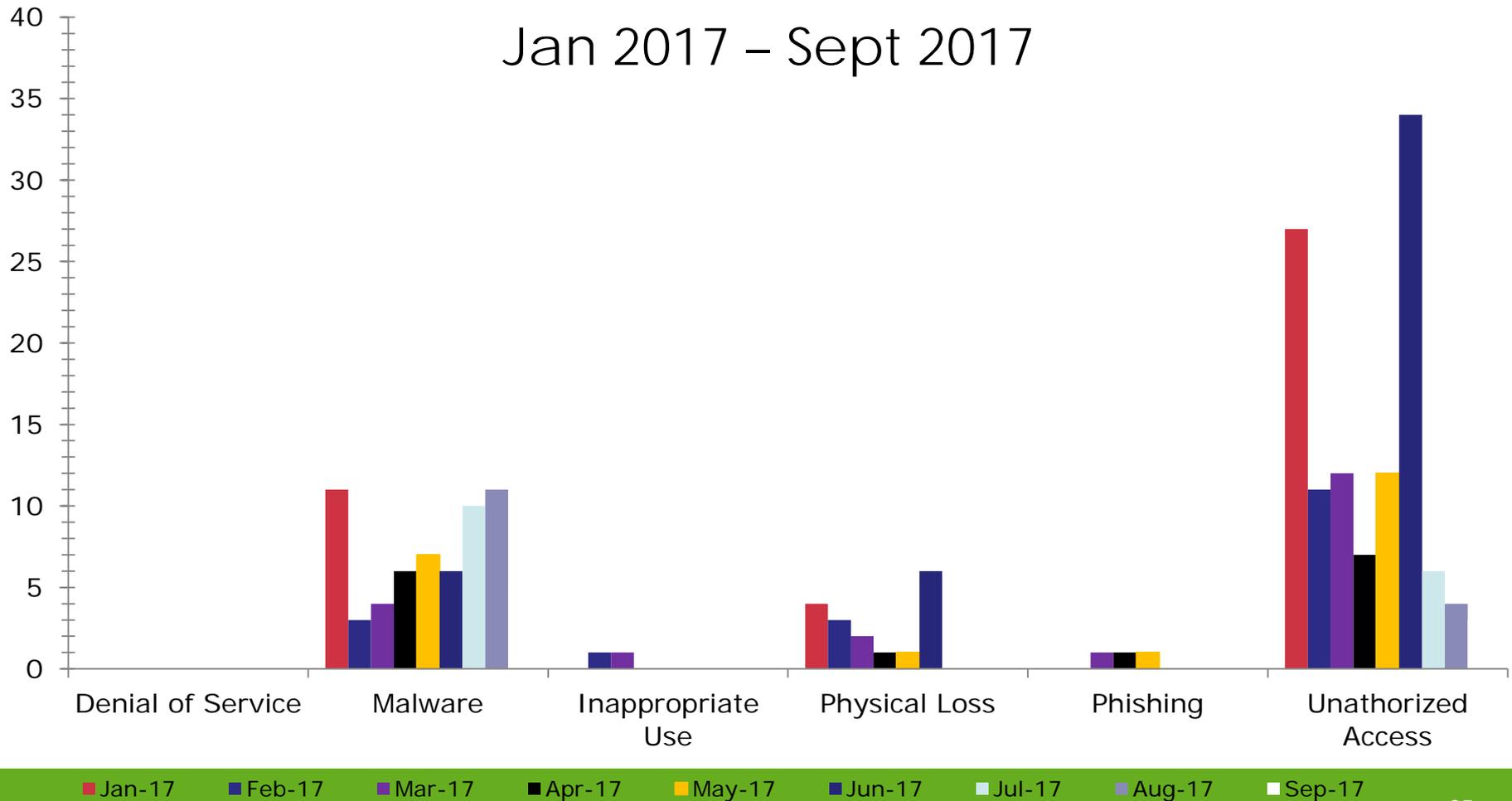
Source: Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, Jan 2015

# Top 5 Origins of Attack 2017



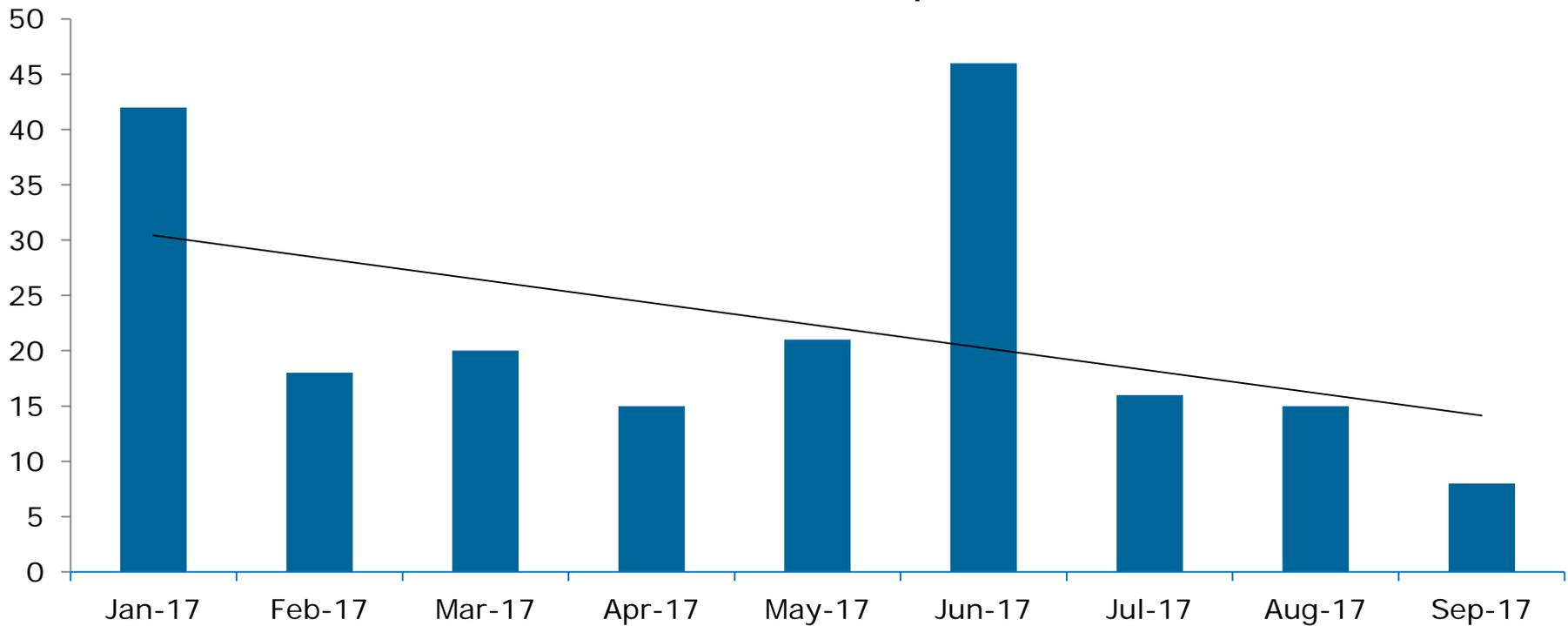
# CoVA Cyber Security Incidents by Category

Jan 2017 – Sept 2017



## Increase In Cyber Security Incidents

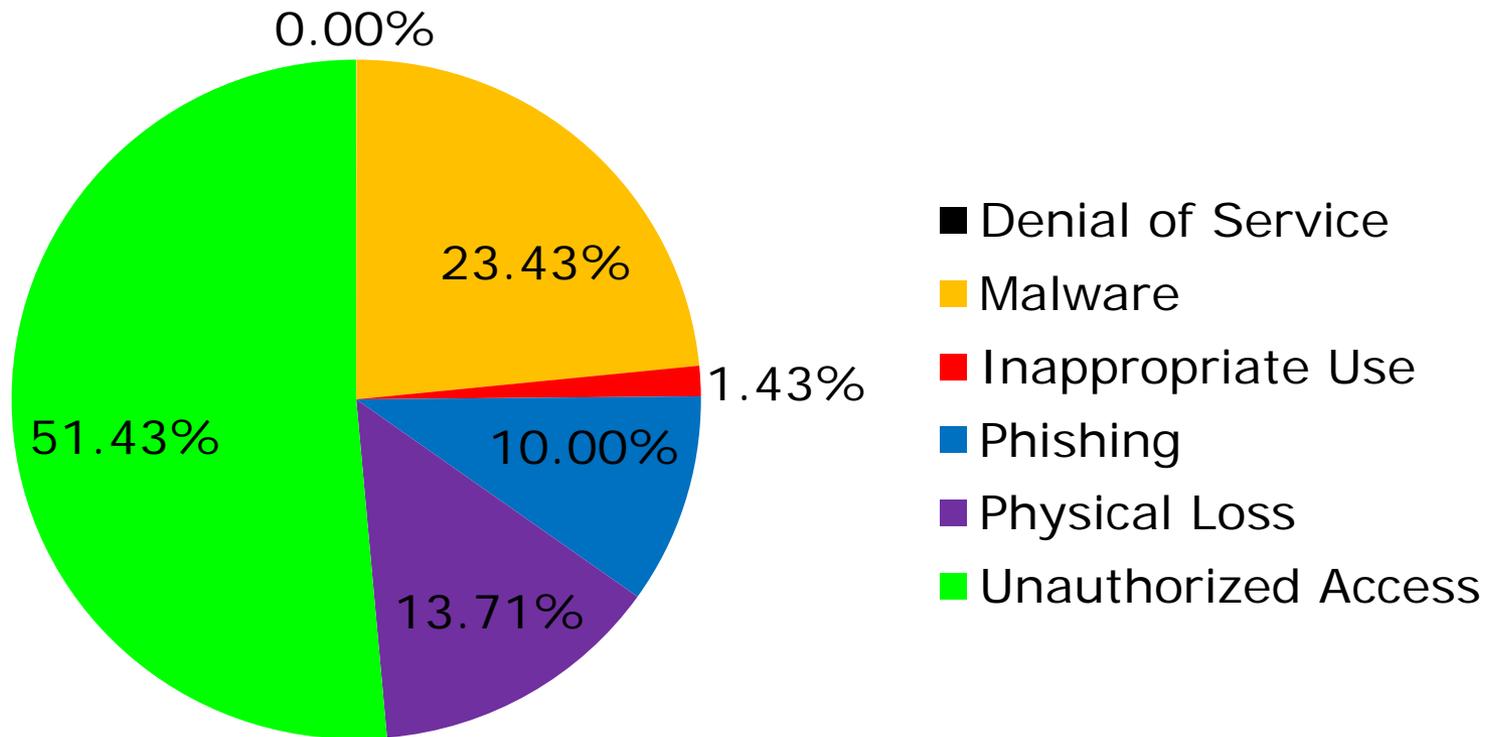
Jan 2017 – Sept 2017



\* Spikes in Jan & Jun due to successful phishing attacks.

## Security Incidents by Category

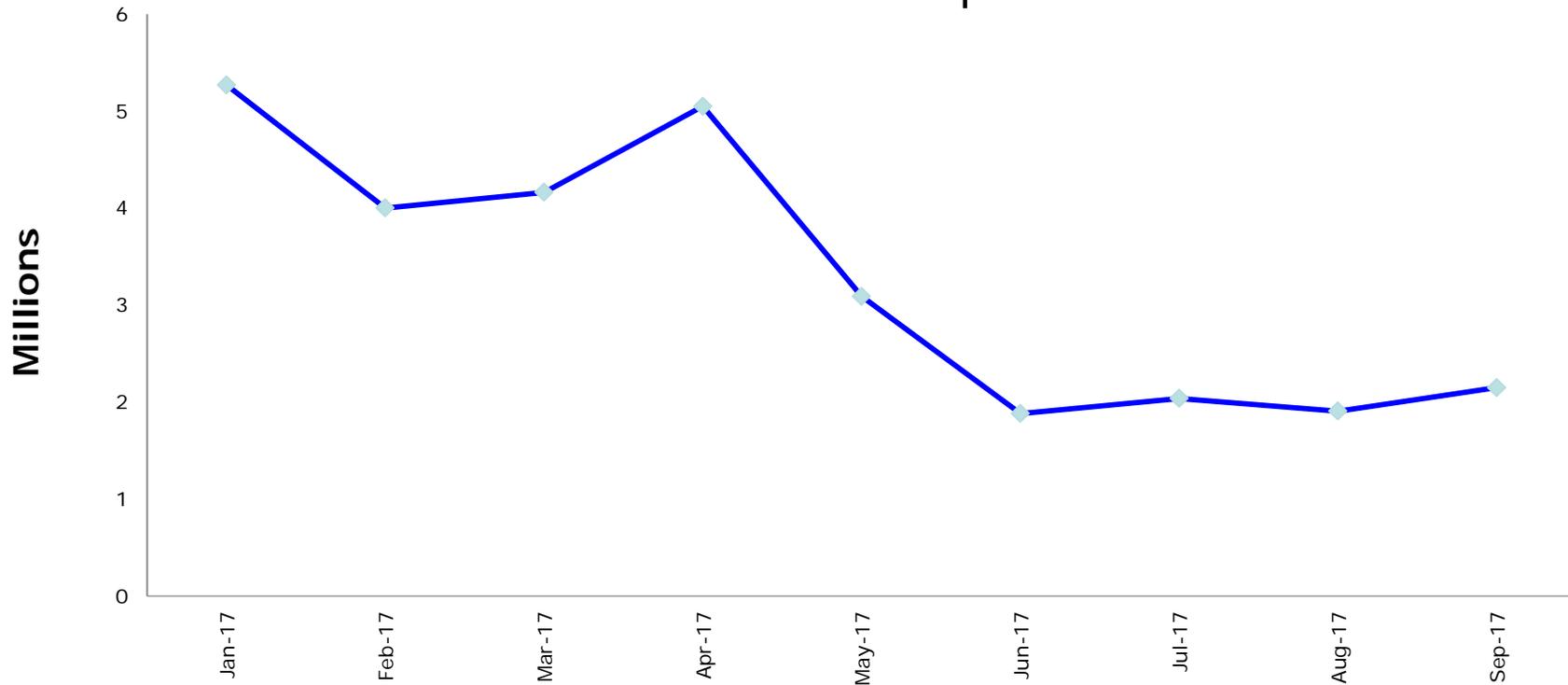
Jan 2017 – Sept 2017



Total Incidents for COV = 201  
Estimated Cleanup Costs \$ 120,600

# 29,551,652 Attack Attempts on CoVA Networks

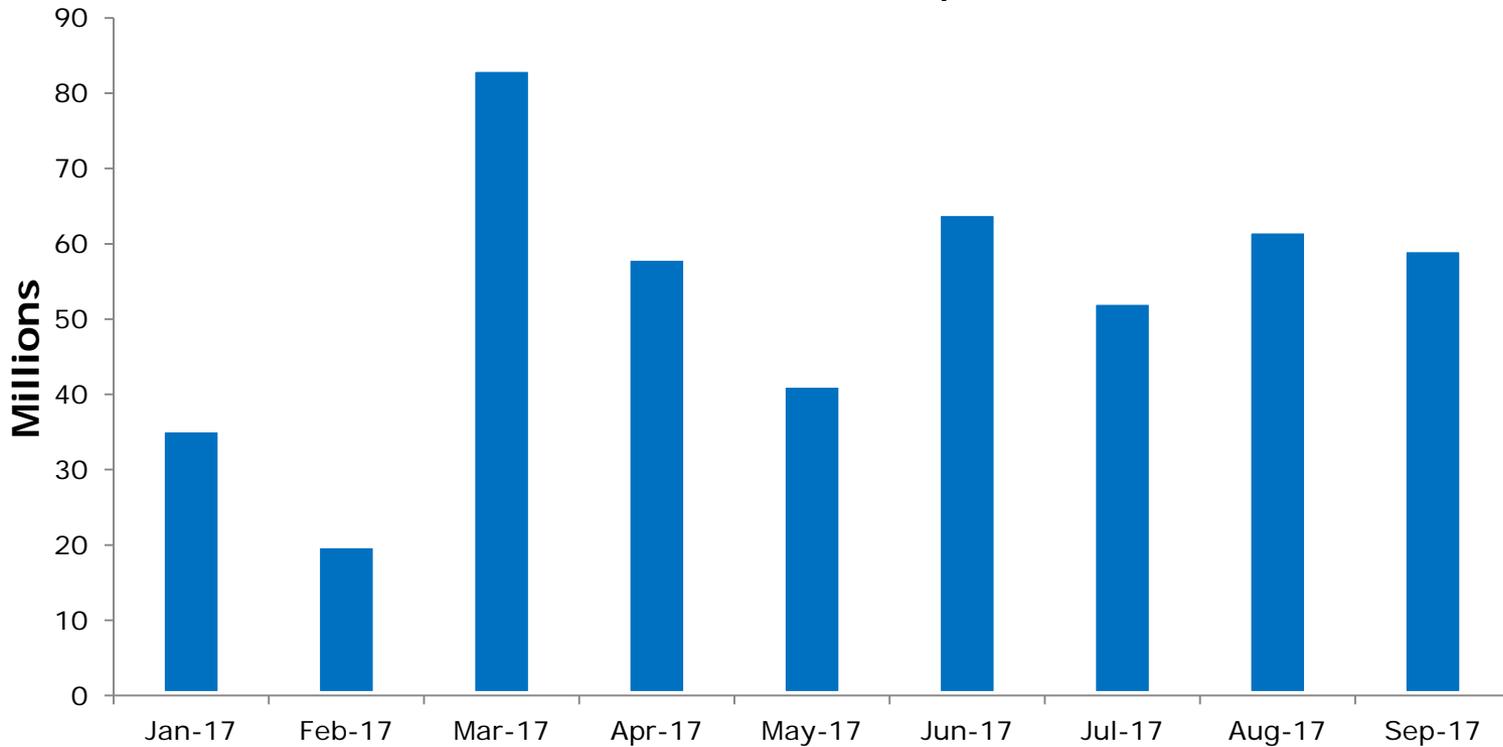
Jan 2017 – Sept 2017





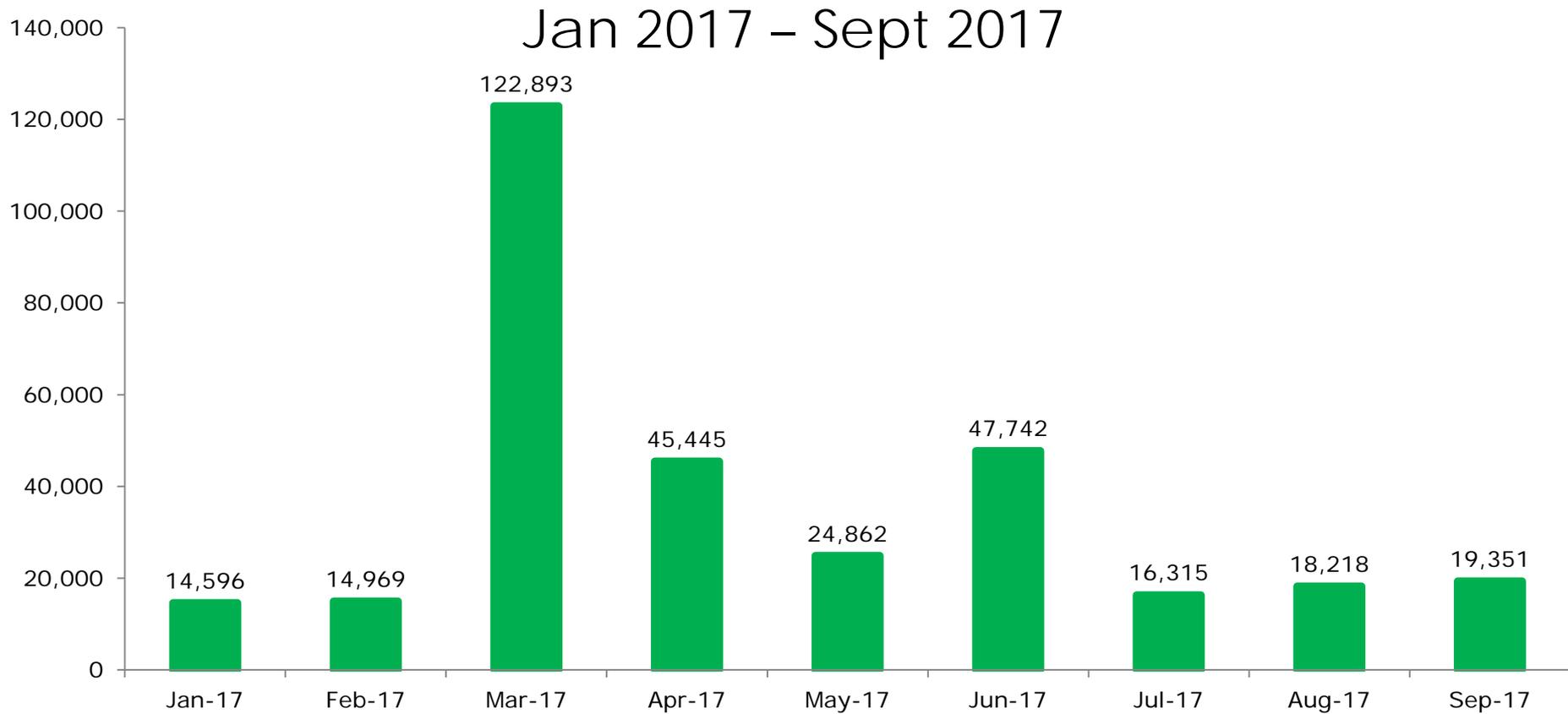
# 477,362,569 Spam Messages Blocked

Jan 2017 – Sept 2017



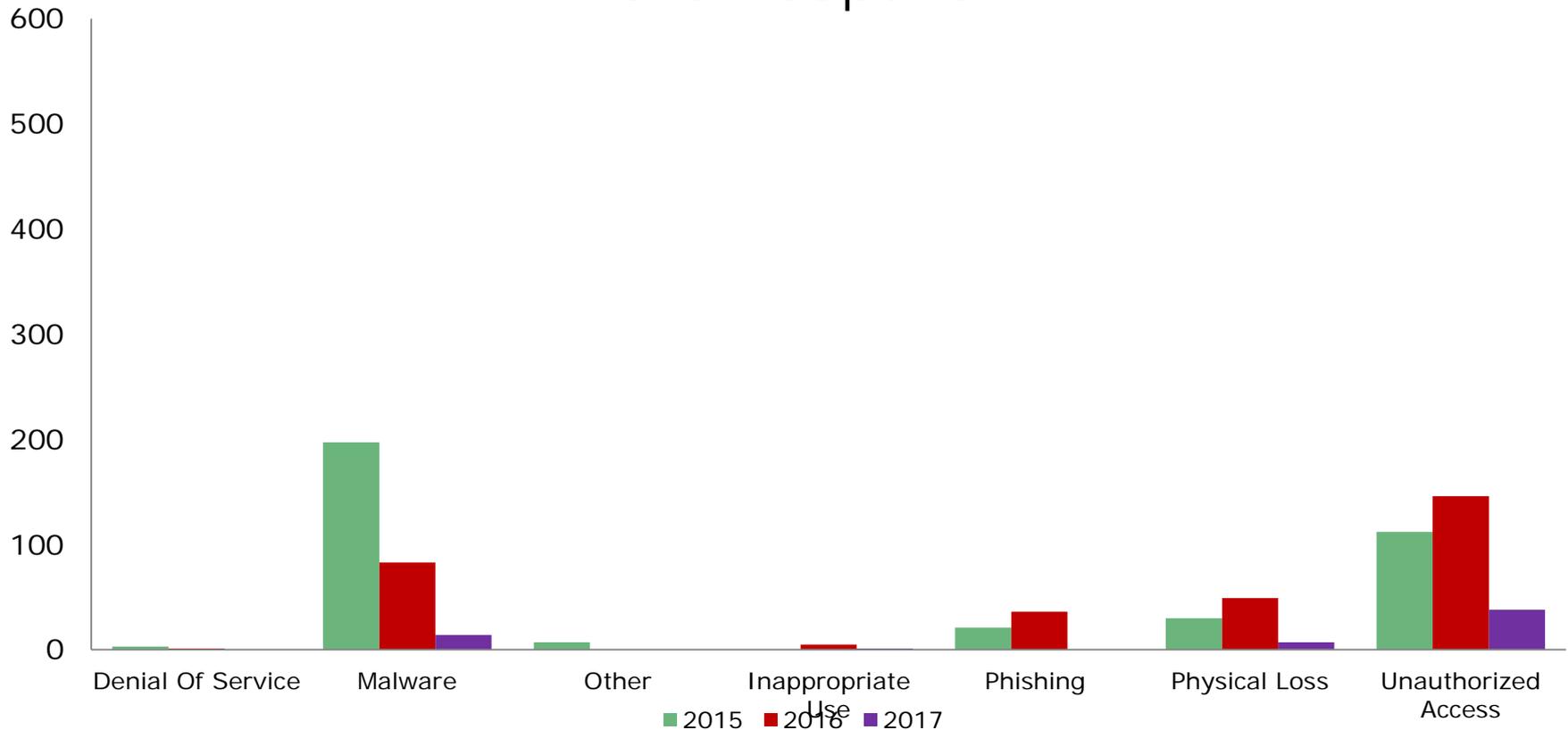


## 324,391 Malware Blocked



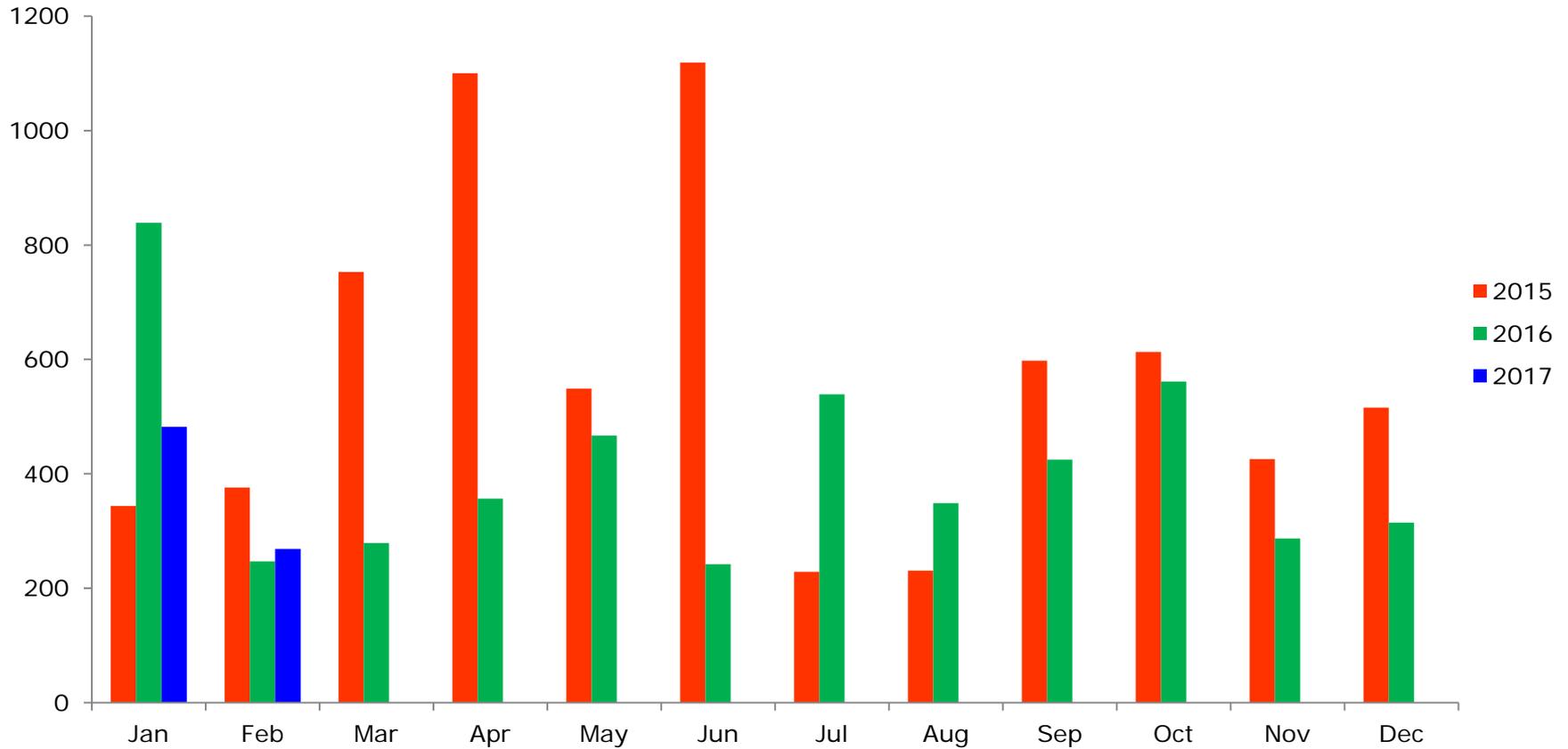
# Cyber Security Incident Trends by Category

2015 – Sept 2017



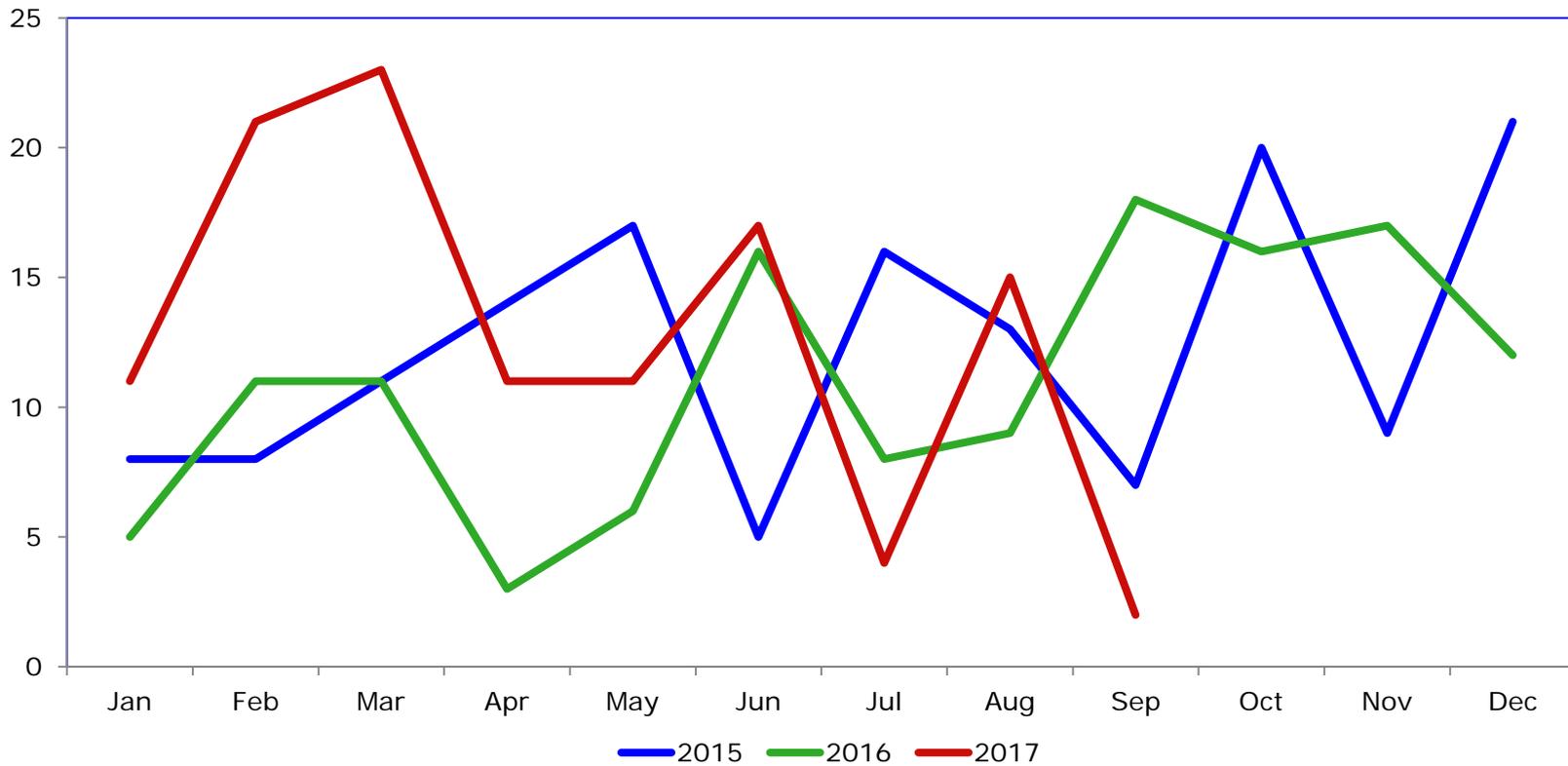
## Vulnerabilities by Month

2015 – Feb 2017



## Critical Exploits

2015 – Feb 2017





## Lessons to be Learned

- 1) Watching others go Phishing.
- 2) Kaspersky Antivirus – Friend or Foe?
- 3) Equifax – Back to basics.



## Phishing Campaigns

- Two agencies have experienced “Reverse” Phishing Campaigns in the last 30 days
- A spoofed email was sent to agency vendors impersonating high level agency staff
- Emails were sent from hacked email accounts hosted with AOL and GoDaddy



## Phishing Campaigns

**From:** State Purchasing & Contracts Office [<mailto:Sandra.Gill@dgs.virginia.gov>]

**Sent:** Tuesday, October 3, 2017 2:03 PM

**Subject:** Bid Notification

We are notifying all diverse suppliers, service providers, contractors, subcontractors and consultants to validate their contact details with the purchasing/contracts division (State of Virginia)

We will be sending project bids to all vendors we have on file. It is mandatory you verify your contact information you have with us to avoid missing out on the contract bids.

Follow the link <http://bit.ly/2wwbPTO> to update your recent contact information and view lists of contracts available for bids.

Requesting Department of General Services

Buyer Name: Sandra Gill

Buyer Phone: 804-786-1600

Buyer Email: [Sandra.Gill@dgs.virginia.gov](mailto:Sandra.Gill@dgs.virginia.gov)

N:B: If your browser won't take you to the contract bid information, look out for our next email.

Regards,

**Director**

Sandra Gill, Interim Director

(804) 786-1600

Fax: (804) 371-7877

[Sandra.Gill@dgs.virginia.gov](mailto:Sandra.Gill@dgs.virginia.gov)



## Phishing Campaigns

### Headers are the key

**X-Originating-IP:** 165.227.223.67

**User-Agent:** Workspace Webmail 6.8.14

**Message-ID:**

20171004104111.7ede2580ebac8b104d0e97533d6fc347.763c  
d24f55.wbe@email11.godaddy.com

**From:** State Purchasing & Contracts Office

Sandra.Gill@dgs.virginia.gov

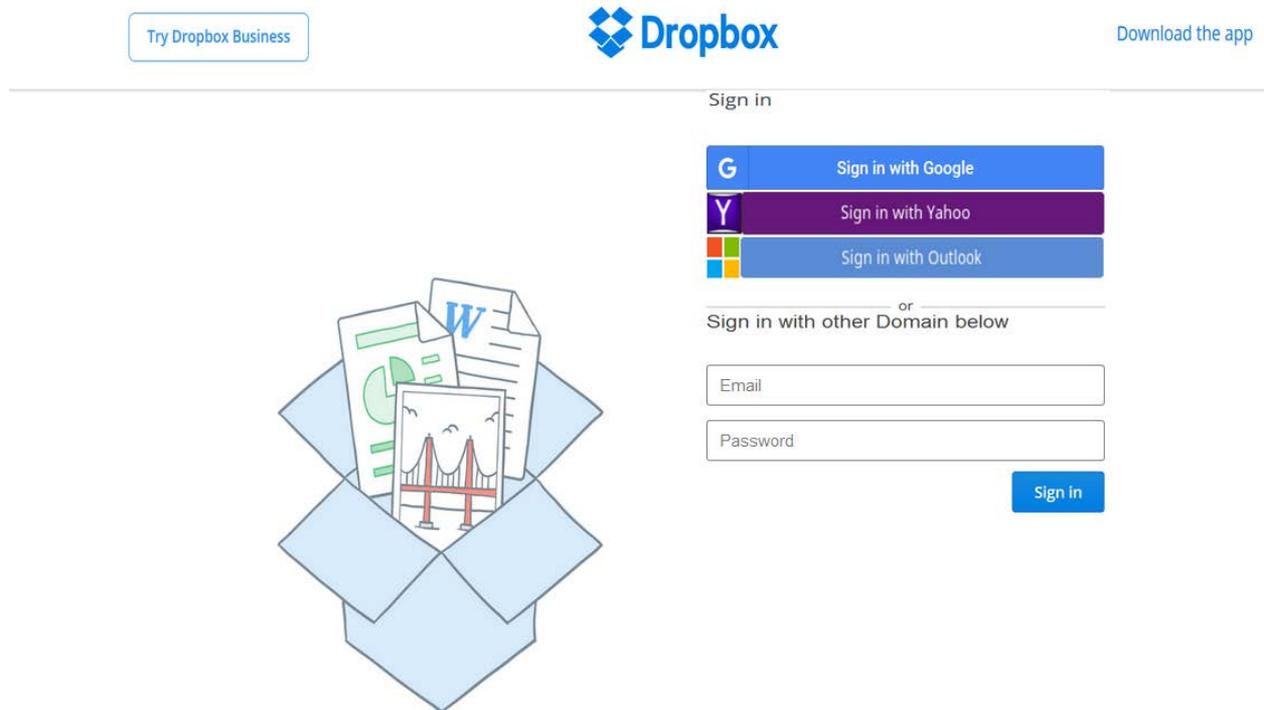
**X-Sender:** boby@mcandlewalsh.com

**To:** Subject: Bid Notification

**Date:** Wed, 4 Oct 2017 10:41:11 -0700

## Phishing Campaigns

The emails used a 'bit.ly' link which finally resolved to a compromised host.



## Phishing Campaigns

### Damage Control

- VITA reports the abuse to the host of the spoofed email account
- VITA contacts the host of the phishing webpage to report the phishing campaign
- Affected agency may notify vendors of the phishing campaign



## Kaspersky – Friend or Foe?

- The reported story is that Russian hackers in 2015 targeted an NSA employee who took home classified data to his home PC, which was running Kaspersky antivirus
- They targeted the employee after they identified the NSA files through the Kaspersky antivirus software.
- The hack included data on how the US "penetrates foreign computer networks, the computer code it uses for such spying, and how it defends networks inside the US."
- The hack has been described as "one of the most significant security breaches" in recent years

## Kaspersky – Friend or Foe?

### So how did Russia acquire the NSA data?

- **THEORY 1:** HACKERS EXPLOITED FLAW IN KASPERSKY TO STEAL DATA
- **THEORY 2:** KASPERSKY DETECTED MALWARE, RUSSIAN SPIES INTERVENED
- **THEORY 3:** KASPERSKY DETECTED AND STOLE MALWARE FOR RUSSIA



## Kaspersky – Friend or Foe?

- Kaspersky products sift through files and upload samples that are flagged as dangerous to be analyzed in the cloud.
- This data is likely sent to servers operated by Kaspersky in Russia.
- Russian law, which "can compel the company's assistance in intercepting communications as they move through Russian computer networks."
- Russian FSB likely intercepted the data due to it being insecurely routed through Russia

## Kaspersky – Friend or Foe?

### Takeaways from the NSA's failure.

- Proper vetting of software and hardware appliances is a must. You need to know what the software is sending back to the Mothership.
- Choosing software made and hosted in the USA allows for greater protections under US law.
- Know the level of data sensitivity your remote/telework employees are working with and ensure proper data protections are in place.

## Data Breaches

### Equifax

- It is estimated that 143 million American consumers had their personal information exposed during this attack.
- The breach lasted from mid-May through July.
- Equifax has confirmed that attackers entered its system in through a web-application vulnerability in Apache Struts that had a patch available in March.

## Data Breaches

### Equifax – Lessons Learned

- Patch your systems regularly as soon as possible.
- Use web application vulnerability scans to your advantage. Do not delay in fixing your findings.

## Conclusion

COV Security Incidents primarily fall into 2 categories:

- Unauthorized access (successful phishing campaign or mis-mailings)
- Malware (drive-by infections, malicious spam, malicious ads)

All these categories can be improved by training the user. The user is your weakest link.

- Require users to take security awareness training annually
- Follow up with simulated phishing campaigns to reinforce training (CSRM/CSIRT team offers these)
- Encourage users to report suspicious activity on their machine or in their email. It will facilitate implementing blocks to protect COV systems and data.



## Conclusion

# Questions?

## Contact Information:

To Report an Incident –

- Web form on VITA site
- <https://vita2.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm>
- Call the VCCC @ 1-866-637-8482
- Email: [CommonweathSecurity@vita.virginia.gov](mailto:CommonweathSecurity@vita.virginia.gov)



## Future ISOAG

**November 1, 2017**

**Speakers: Gregory Bell, CISO DBHDS**

*Gregory Williams, Advisory Services,  
Ernst & Young, LLP*

*Ray Chang & Jennifer Gray, Amazon*

*ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2017*



## IS Orientation

**December 14, 2017**

**1:00-3:00 CESC**

Link for registration:

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

***ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2017***



## IS Orientation

**When: Thursday, Sept 21, 2017**

**Time: 1:00 –3:00 pm**

**Where: CESC , Room 1221**

**Presenter: Ed Miller**

**Register here:**

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



## SAVE THE DATE

# "2018 COVA Information Security Conference: "Expanding Security Knowledge"

April 12 & 13

Location: Altria Theater

# ADJOURN

## THANK YOU FOR ATTENDING

