



# Welcome and Opening Remarks

**Mike Watson**

Oct. 7, 2020



# Oct ISOAG AGENDA

- **Welcome and Opening Remarks - Mike Watson, VITA, CISO**
- **Remote Security Threats – Randy Marchany, Virginia Tech**
- **Risk Management Update – Jon Smith- VITA, CSRM Risk Management**
- **Security Awareness Training Project- Tina Harris Cunningham/Ed Miller, VITA CSRM IT Security Governance**
- **Data Points Update - Joy Young / Ed Miller – VITA- CSRM IT Sec Governance**
- **Ransomware Readiness Project – Renea Dickerson/Marlon Cole, VITA- CSRM IT Security Governance**
- **Centralized IT Sec Audit Service Update - Mark McCreary, VITA, CSRM Audit Services**
- **Website Vulnerability Remediation – Bob Baskette, VITA, CSRM Security Incidents and Architecture**

## *Zero Trust Networks: A New Twist*

**Randy Marchany**

CISO, Virginia Tech

marchany@vt.edu

<https://security.vt.edu>

Twitter: @randymarchany



# *Most Common Security Mistakes Made by Individuals (2001)*

- Poor password management
- Leaving your computer on, unattended
- Opening e-mail attachments from strangers
- Not installing anti-virus software ✓
- Laptops on the loose
- Blabber mounts (file access open to the world)
- Plug and Play without protection
- Not reporting security violations
- Always behind the times (OS, application patches)
- Keeping an eye out inside the organization

# *Border? What Border?*

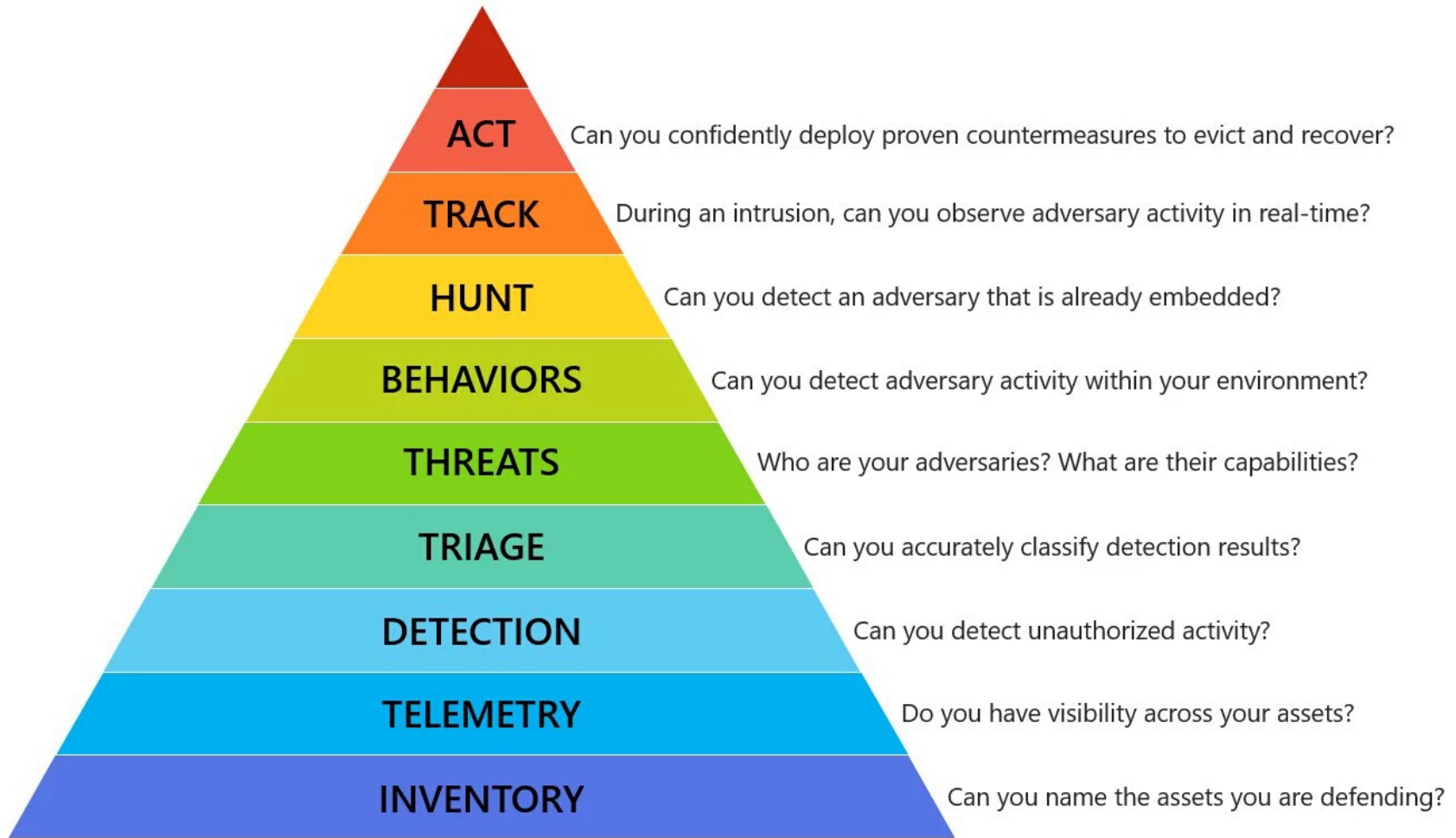
- Internet 1.0 – static servers, endpoints
- Internet 2.0 – static servers, mobile endpoints
- **Internet 3.0 – mobile servers (containers, serverless), mobile endpoints (laptops, phones, tablets, IoT, ICS)**
- Current security architectures are somewhere between Internet 1.0 and Internet 2.0.
- We need to adapt to Internet 3.0 now

# *WFH and Zero Trust*

- Can your IT scan computers at your house?
  - Probably not. May be blocked by your ISP
- Can you “disconnect” a host from your network?
  - ISP will get abuse complaints not your org
- What network traffic visibility exists from computers at your house?
  - None probably, unless you require VPN
- What type of logs will you need to collect in this new WFH environment?

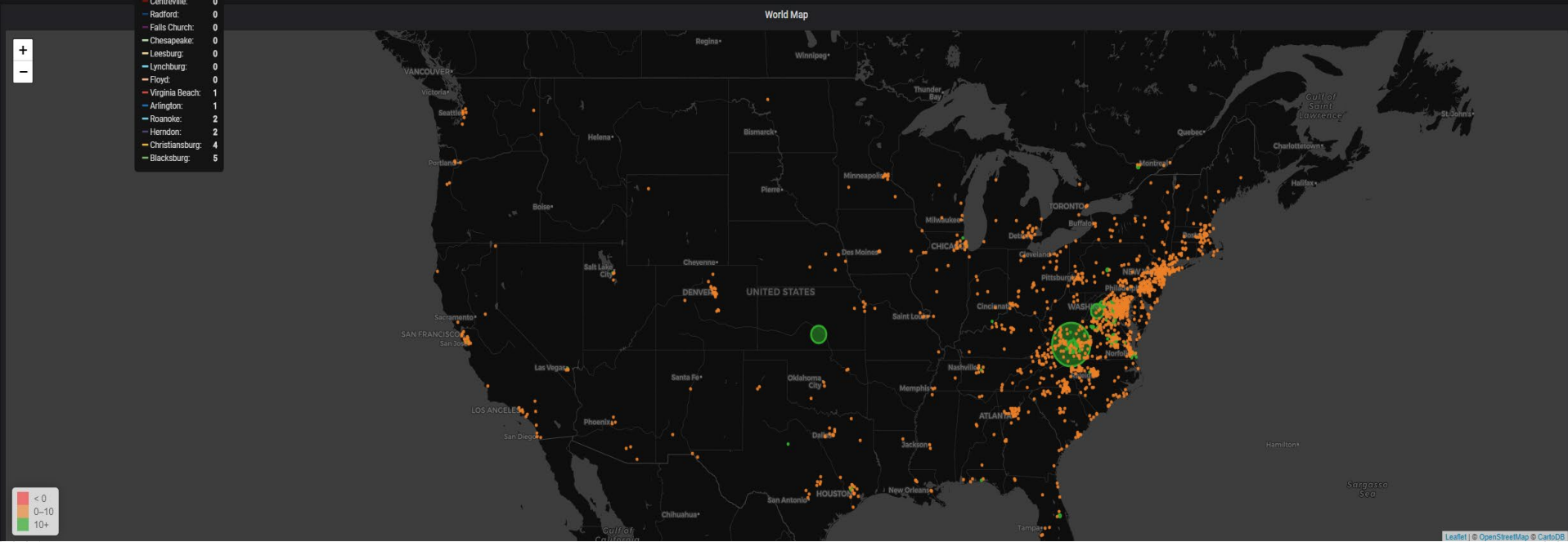
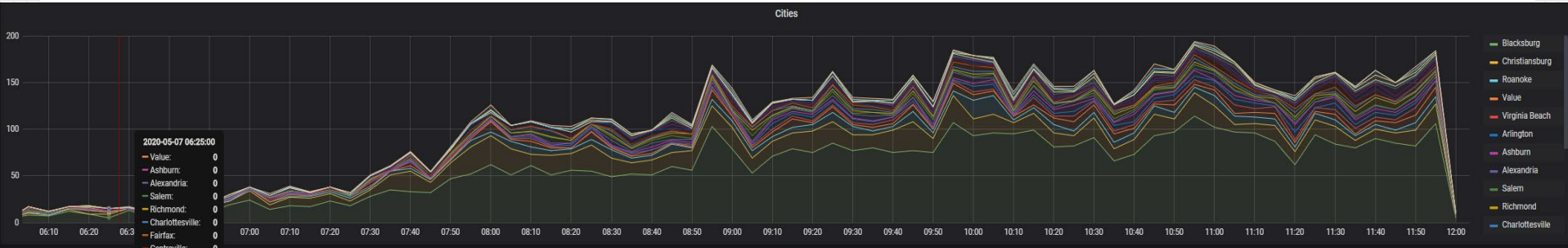
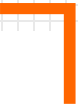
# *Your Home Computer Became Your Work Computer - 1*

- Does your home computer meet any regulatory requirements imposed on the data you use?
- **Create a separate userID for work stuff.** Keeps personal separate from work.
  - Browser history, photos, personal sensitive data vs. work sensitive data. Can limit ransomware damage.
  - When you're done #WFH, you can delete that account



source: <https://github.com/swannman/ircapabilities>

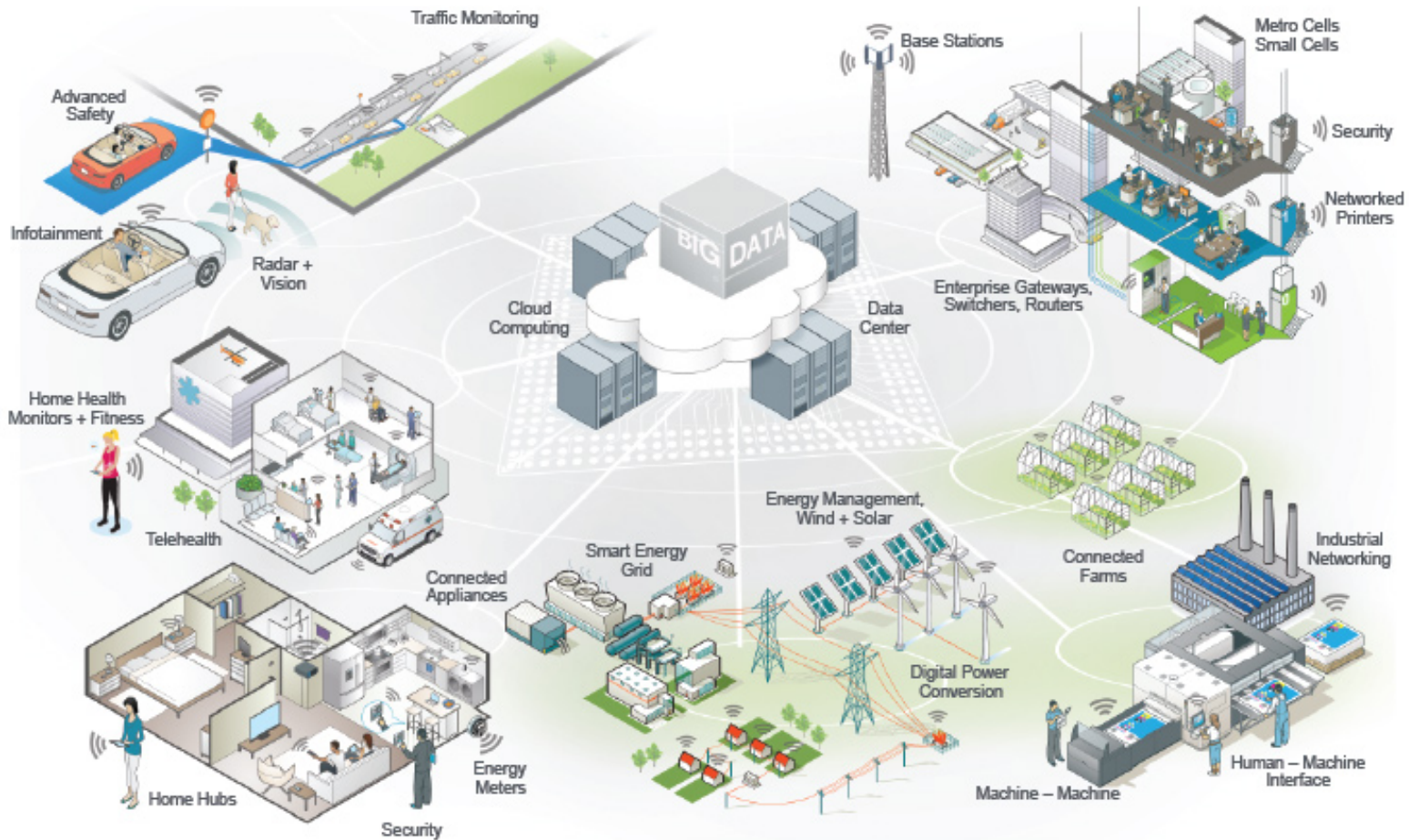


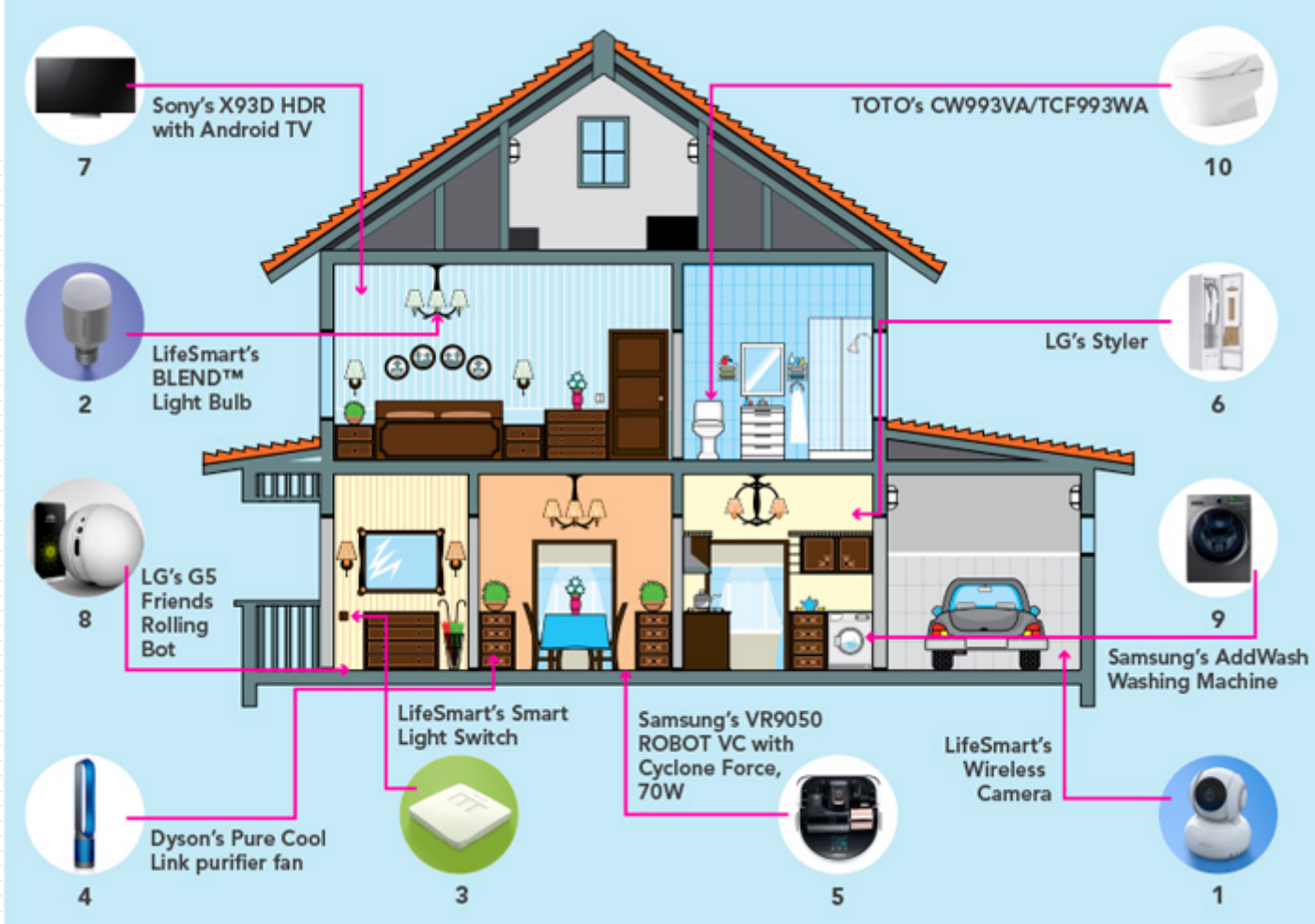


Leaflet | © OpenStreetMap © CartoDB



# ENABLING SMART CONNECTED SOLUTIONS FROM THE END NODE TO THE CLOUD





# *EDU (now) vs. Corporate Structure (future)*

- **Administrative** – the process that runs the institution (**CORP**)
  - Payroll, HR, purchasing, facilities, legal, etc.
  - **Security model closest to corporate model**
- **Academic/Instructional** – the process that supports teaching/learning (**ISP**)
  - Learning mgmt. systems such as CANVAS, Blackboard, Moodle
  - Course delivery systems – Zoom, Webex, etc.
  - Heavily BYOD – all flavors, types
  - **Security model closest to an ISP**
- **Research** – **hybrid** of the previous 2
  - Intellectual property protection, high-risk, visibility
  - **Security model is a hybrid of corporate and ISP**

# Museum Defense in Depth



© 2018 FireEye | Private & Confidential

- Control access points
  - Limited but **free flowing** access points
  - Additional barriers around high risk assets
- Pervasive monitoring tools
  - Cameras, motion sensors, etc.
- Active response
  - Guards, on-demand barriers, fire suppression
- Recovery measures
  - Insurance
  - Tracking devices
- Assume hostiles are inside

Used with permission of Christian Schreiber

# Zero Trust Networks(ZTN) Assumptions\*

- The device is no longer the border. **A user's identity/Data pair is the new border.**
- Pillar 1: The network is always assumed to be **hostile**
- Pillar 2: Assume the hostiles are already **inside your network**
- Pillar 3: Network locality (segmentation) is **not sufficient** for deciding trust in a network

\* "Zero Trust Networks: Building Secure Systems in Untrusted Networks", Evan Gilman, Doug Barth

# ZTN Assumptions

- Pillar 4: **Every** device, user and network flow is authenticated and authorized
- Pillar 5: **Policies** must be dynamic and calculated from as many sources of data as possible
- Pillar 7: **Containers, serverless and cloud** computing are the new disruptors of traditional security architectures.
- Pillar 8: Mobile users, mobile apps, mobile storage

# *What are You Defending? What Should You Defend?*

- Systems? Not really but that's what we thought should be defended.
- Networks? Safe answer.
- DATA – what we should be defending.




# Another View of ZTN





- “As we **move our data outside of the firewall**, we have to adopt a zero-trust type model, “ [Chris] Townshend said. “We are shifting our security enforcement out to the data itself, and **you have to have a security policy that follows that user no matter where that user is or what device they are using to access the data**”
  - “The new cyber landscape”, Patrick Marshall, GCN Magazine, vol 37, #1
- In other words, data and identity become the border.



# *ZTN Trust: Users*

- Authoritative identity
    - MFA
  - Trust scores determine if additional authentication is required
  - Single sign-on
- 

## Key Components of an Employee's Remote Work Profile

	 <b>Employee Role</b>	 <b>Remote Work Strategy</b>	 <b>Client Compute(s)</b>	 <b>Application and Data</b>
	<ul style="list-style-type: none"> <li>• Access:                             <ul style="list-style-type: none"> <li>– Applications</li> <li>– Structured Data</li> <li>– Unstructured Data (e.g., Email)</li> </ul> </li> <li>• Technological Savviness</li> <li>• Fit to Remote Work</li> <li>• Risks Exposure</li> </ul>	<ul style="list-style-type: none"> <li>• Frequency:                             <ul style="list-style-type: none"> <li>– Not Suitable – Impossible</li> <li>– Emergency Only</li> <li>– Occasional</li> <li>– Part Time</li> <li>– Most Time</li> </ul> </li> <li>• Work Location                             <ul style="list-style-type: none"> <li>– Fixed (e.g., Home, Co-working Space, Flex Office)</li> <li>– Mobile (e.g., Travel)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Managed Laptop</li> <li>• Bring Your Own Device (BYOD)</li> <li>• On-Premises Workstation Accessed Remotely</li> <li>• Desktop as a Service (DaaS)</li> <li>• Virtual Desktop Infrastructure (VDI)</li> </ul>	<ul style="list-style-type: none"> <li>• On-Premises:                             <ul style="list-style-type: none"> <li>– Public Facing</li> <li>– Internal</li> <li>– Air Gapped (e.g., SOC)</li> </ul> </li> <li>• IaaS</li> <li>• SaaS</li> </ul>
<b>Stakeholder</b>	Business Leaders	HR, Business, Finance	CIO	CIO
<b>CISO's Role</b>	<b>Understand</b>	<b>Adapt</b>	<b>Influence</b>	<b>Influence</b>

Source: Gartner  
724856\_C

Source: <https://siliconangle.com/2020/09/05/three-steps-design-security-remote-work-first-enterprise/>

eduroam is proud to be a founding member of WBA OpenRoaming



ONE GLOBAL WI-FI NETWORK



**“ eduroam has been doing federated Wi-Fi roaming since over a decade with many of the building blocks that meanwhile underpin Passpoint®. Now that Passpoint® and OpenRoaming™ provide a coherent vision and technology to enable inter-federation roaming in a scalable way, it is only natural for eduroam to join forces and take this exciting next step as a first-to-market pioneer participant. ”**

Paul Dekkers  
Chair of the Global eduroam Governance Committee in GÉANT



#### Get Connected

Students, researchers and educators – connect your phone, tablet or laptop to eduroam!



#### Connect Your Institution

Find out how and why universities, research institutes, schools and other institutions should get eduroam.



#### Connect Your R&E Network


Provide this valuable service to your research and education community.


## Sign In


E


Log in or create a profile

Or use InCommon Federation login

 Virginia Tech

 Washington State University

 Washington University in St. Louis

 Wayne State College

Enter Identity Provider Name

Show all

Looking to [manage your .edu domain](#)? You do not need an EDUCAUSE profile.

Not an EDUCAUSE Member? [Membership](#) is at an organizational level. When you join, everyone at your organization benefits.

[Need Help?](#) | [About InCommon Federation](#) | [Web Accessibility Assistance](#)

# Login

 SIGN IN WITH GOOGLE

 SIGN IN WITH FACEBOOK

 SIGN IN WITH AZURE AD

Have an invitation code?

# *Some Suggestions*

- Start small – ZTN a lab or smaller departmental net
- Build a system diagram of your network traffic patterns
- Profile your traffic
  - Do you know where your inbound traffic originated?
  - Where does your outbound traffic go?
- Do you trust your network?
- Log, log, log!

# *ZTN and Today's Network*

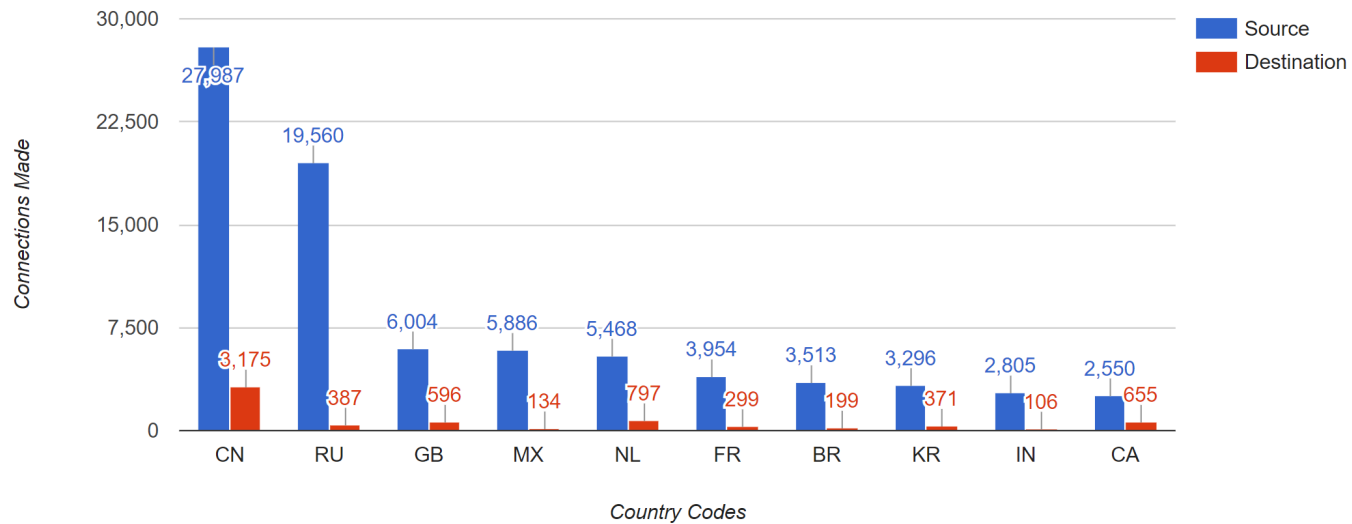
- Traditional net filtering, monitoring - significant factor in ZTN.
- Its application is non-traditional
- Net flow authentication/authorization a key component
- Monitor outbound traffic with threat intel data
- Configure host based FW/IDS
- Profile your net traffic
  - Direct lateral movement between hosts is rare? y/n
- Log, Log, Log



# Sample In/Out Traffic Profile

## Top Source & Destination Countries - By Connection

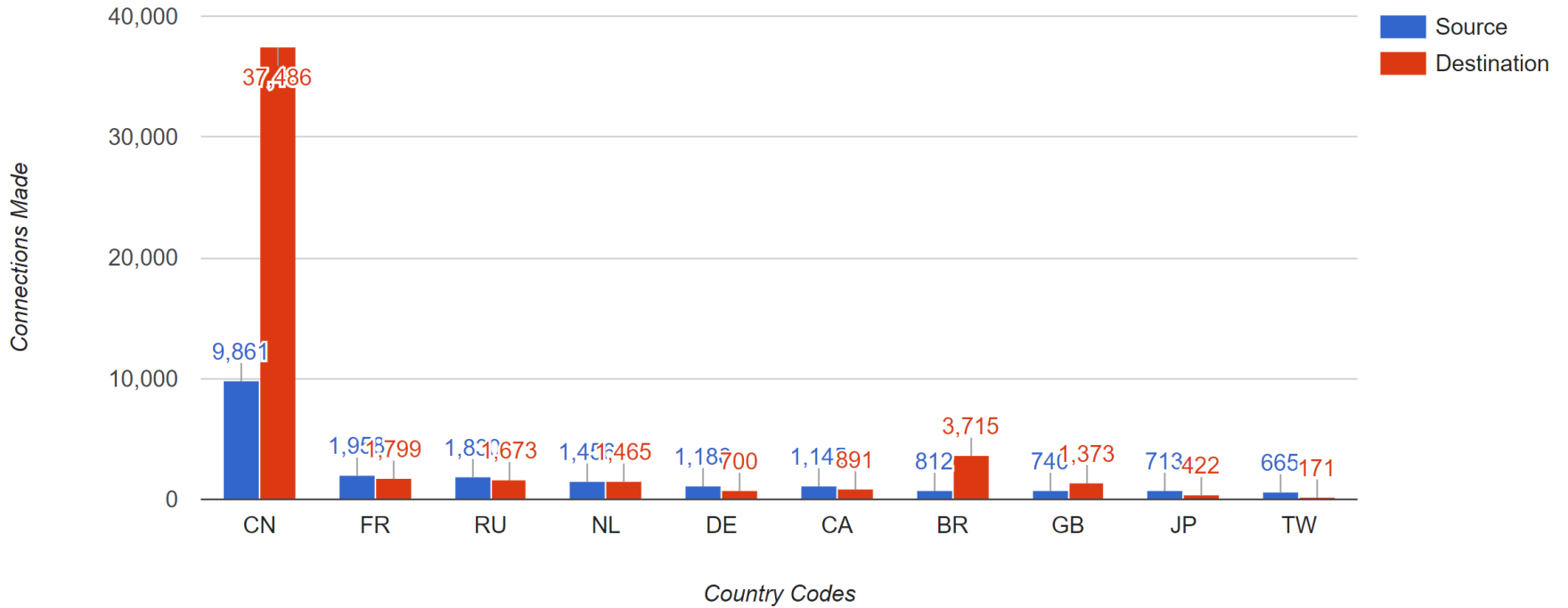
Aug 01, 2017 to Aug 31, 2017 - ITSO Argus Data



Country Code	Country Name	Source Count	Destination Count
US	United States	91396	206186

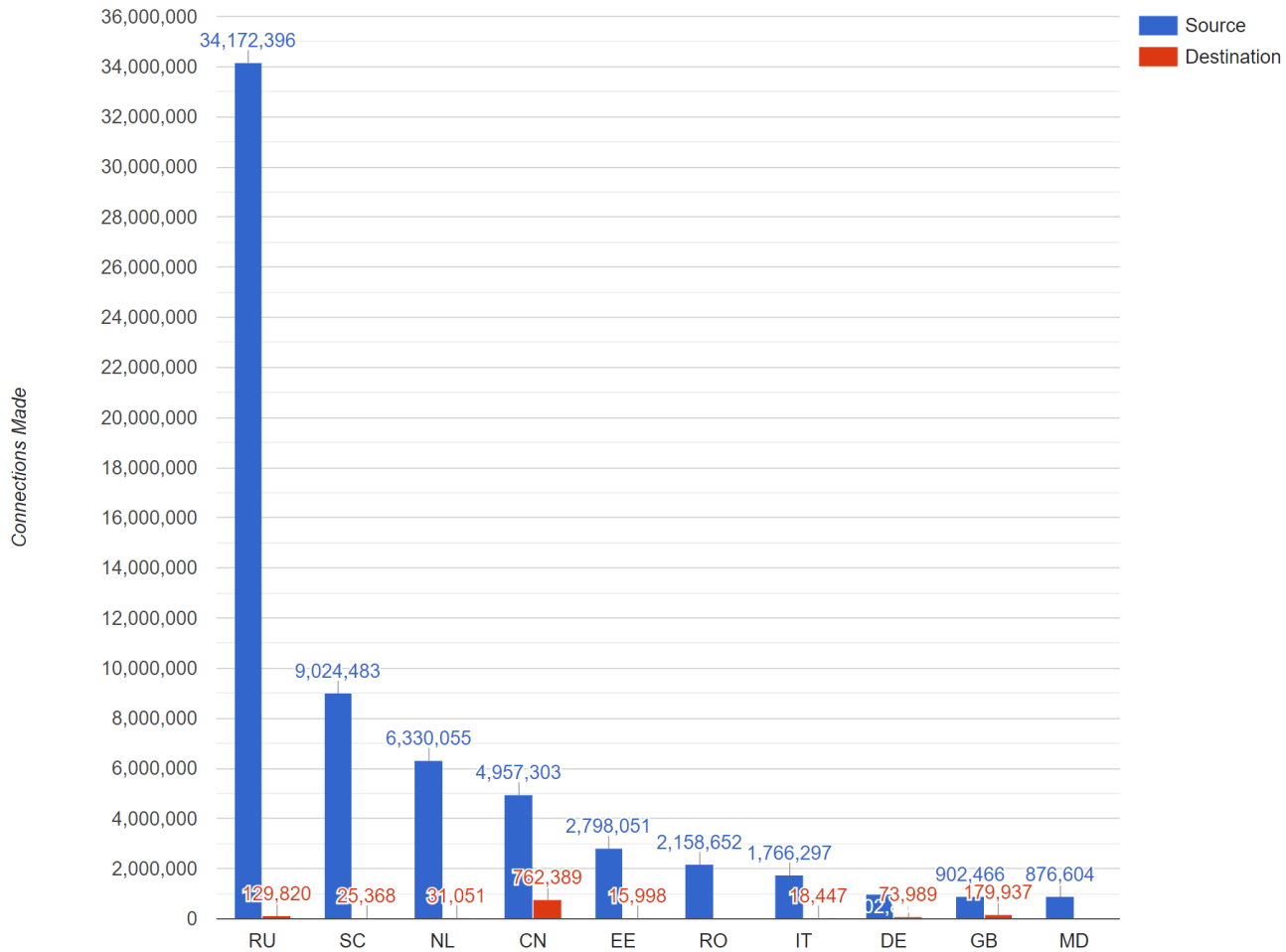


Nov 01, 2014 to Dec 01, 2014 - ITSO Argus Data



Country Code	Country Name	Source Count	Destination Count
US	United States	136701	104575

Top 10 Source/Destination Countries - 2019-04-11T08:05:01-04:00




# ZTN - Theory

- Easier said than done. Not all of the technology and components available today....not yet.
- **All data must be secured regardless of location.** Encryption at rest or in transit. Have to find it first!
- **User identities must be confirmed.** Access to data strictly enforced. Default of minimum privileges
- **All network traffic should be logged and analyzed.**
  - “trust but verify” -> “Verify and never trust”
- Eliminates distinction between trusted-inside-perimeter and untrusted activity that crossed the perimeter



# *ZTN Characteristics*

- Treat all hosts as internet-facing (take that, .com, .gov, .mil ...)
  - Use existing tech in novel ways
  - Perfect fit for cloud
- 

# ZTN Trust: Network Traffic

- Where to apply ZTN controls in the network stack
  - TLS – used mostly application layer protocols
  - IPsec – used mostly to secure traffic (VPN). Well positioned to provide secure comms for all traffic
- Filtering
  - Host – filter traffic at the host. Handles inbound traffic
  - Bookend – apply policy in both directions. Egress filtering
  - Intermediary – “traditional” FW placement

# ZTN and the 20 Critical Security Controls

- HW Inventory
- SW Inventory
- Continuous Vuln Mgmt
- Controlled use of Admin Priv
- Secure config for devices
- Log Analysis, maintenance
- Email, Browser Security
- Malware Defenses
- Limit Ports, Protocols, Services
- Data Recovery
- Secure config for net device
- Boundary Defense

# *ZTN and the 20 Critical Security Controls*

- Data Protection
- Need to Know
- Wireless Access Control
- Acct Monitoring, Control
- Security Training
- Application Software Security
- Incident Response and Mgmt
- Penetration Testing and Red Team Exercises



# Compliant




*Secure!*





# Summary

- Need an architecture that can handle:
    - Data mobility, protection
    - Cloud, containers, serverless apps
  - What will the tech environment be in 5 yrs? 10yrs?
  - We've been doing pieces of ZTN for years
- 

# References

- “Zero Trust Networks”, Gilman, Barth,  
<http://shop.oreilly.com/product/0636920052265.do>
- “Building Security into Your Network’s DNA: The Zero Trust Approach”, John Kindervag, 2010
- “Single Packet Authorization: A Comprehensive Guide to Strong Service Concealment using fwknop”, Michael Rash,  
<http://www.cipherdyne.org/fwknop/docs/fwknop-tutorial.html#design>

## About Me

- Degree in Computer Science, Electrical Engineering, 3 cybersecurity patents, SANS Institute Senior Instructor since 1992, Center for Internet Security founding member
- Musician Indie Award Winner, wrote original theme song for NPR program, “World Café”, toured US, Europe, No Strings Attached
- Assistant Volleyball Coach, VA Tech, USVA Club, Bronze medal winner (Handball, 1993 VA Commonwealth games)
- Biking (bicycle, motorcycle)

# Simple Steps to Protect Your Computer

- Password protect your userID, screen lock
  - Update your OS and software
  - Think before click
  - You have a firewall already
  - Adjust browser security, privacy settings
- Encrypt sensitive data
    - Use Microsoft Office tool
    - Remember your password!
  - <https://www.us-cert.gov/ncas/tips/ST15-002>  
“How to Secure Your Home Network”
  - <https://privacy.net/how-to-secure-your-computer/>

<https://privacy.net/how-to-secure-your-computer/>

OCT. 7, 2020

# RISK MANAGEMENT PROGRAM

JONATHAN SMITH

Director, Risk Management

ISOAG, OCTOBER 2020





- SEC 520 Risk Management Standard
- 2020 Nationwide Cybersecurity Review (NCSR)
- VITA Program Risk Management
- Security Incident Response Tabletop Exercise
- Operational Risks and Issues (ORI's)
- Quantitative Risk Management
- Risk/Vulnerability Reports and Risk Alerts





- Updated to remain aligned with changes to the NIST cybersecurity framework
- Added the following:
  - IT system and data sensitivity classification
  - Sensitive IT system inventory and definition
  - System security plans
  - Nationwide cybersecurity review
- Updated vulnerability scanning requirements
- Currently on ORCA until Oct. 28, 2020



- Maturity based self assessment of your agency's cybersecurity and risk management programs
- Based on the NIST cybersecurity framework
- Sponsored by DHS and MSISAC
- Questionnaire is preloaded in Archer for each agency
- 141 questions
- Designed to take approximately one hour to complete
- Agency participation is included in the annual report for information security
- A communication with instructions has been sent out to agencies
- Please complete by Dec.15, 2020



- Risk management integrated into the VITA program governance model
- Identify and track security risks and issues within service towers
- Escalate issues as necessary
- Risk management committee
  - 13 Agency ISO's, CSRMs and VITA staff
  - Meets first Wednesday of each month
- Issue risk alerts to the VITA program
- Service tower supplier (STS) annual security plans and system security plans



- Objectives:
  - Exercise and evaluate security incident response plans and playbooks around multiple security incident scenarios
  - Identify areas of improvement and update plans and playbooks
- TTX date: Oct. 29, 2020 8a.m. - 3 p.m.
- Hot wash: Oct. 30, 11a.m. - noon
- Participants
  - VITA Incident response
  - Seven service towers
  - 20 Commonwealth agencies



- Purpose: To identify and track until remediation, risks and issues within the Commonwealth IT environment
- Types of ORI's include, but not limited to:
  - IT security audit and risk management programs
  - Enterprise architecture (end-of-life (EOL), unmanaged networks, etc)
  - Configuration issues
- Sources for ORI's:
  - Annual report on information security
  - System inventories (CMDB, Archer, etc)
  - Vulnerability scans
  - Security incidents
  - Other



- Where are ORI's located?
  - Archer (findings)
  - Commonwealth technology portfolio (CTP)
- What should be done with ORI's
  - Risk treatment plans should be updated and maintained in Archer for remediation plans and activities
  - Open ORI's will require a business requirement (BReT) in agency IT strategic plans to address the risk or issue
- How to close an ORI?
  - Risk/Issue must be remediated
  - Update the remediation action in Archer and submit for closure



- In 2019, CSRM began looking at how to quantify risk values within the Commonwealth environment in order to better inform decision making processes, such as
  - IT Investment
  - Security enhancements
  - Security exceptions
  - Cyber liability insurance
  - Protect AAA bond rating
- Initially looked at the FAIR model
- Wanted to use data that VITA already has access to
- Created a hybrid model
- Worked with Dept. of Treasury on their procurement of an umbrella cyber liability insurance policy

# Quantitative Risk Analysis

- Based on the number of records
- Baseline risk assumes all controls are in place
- Residual risk accounts for missing controls/findings

▼ APPLICATION RISK INFORMATION

Criticality Rating: 🟡

🔵 Sensitive as to Confidentiality: Yes

🔵 Sensitive as to Availability: No

🔵 Sensitive as to Integrity: Yes

🔵 **Default Records at Risk: 71,140**

🔵 Records at Risk Override:

Last Agency IT Risk Assessment: 12/27/2018

Next Agency IT Risk Assessment: 8/31/2021

Last IT Security Audit: 12/31/2018

Next Scheduled IT Security Audit: 12/31/2021

🔵 **Application Baseline Risk: \$ 2,090,815**

🔵 **Application Residual Risk: \$ 2,655,335**



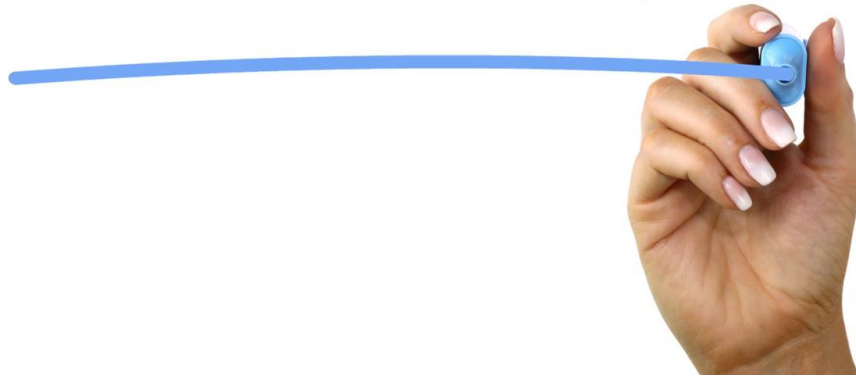


- Agency Risk/Vulnerability reports
  - Automating vulnerability reports specific to agencies systems and technologies
- Risk assessment questionnaire update
- Agency risk alerts
  - Identifying and reporting risks above risk thresholds
  - Require risk treatment plans to address the findings
  - Could impact future projects/procurements

# Questions?



# QUESTIONS



[jonathan.m.smith@vita.virginia.gov](mailto:jonathan.m.smith@vita.virginia.gov)

# Commonwealth of Virginia Security Awareness Training

## HB 852 VITA: REQUIRED INFORMATION SECURITY TRAINING PROGRAM

What is HB 852 §2.2-2009 of the Code of Virginia

**Virginia Information Technologies Agency; required information security training program for state employees.** Requires the Chief Information Officer of the Virginia Information Technologies Agency (the CIO) to develop by November 30, 2020, and annually update a curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats. The bill requires the Commonwealth's executive, legislative, and judicial branches and independent agencies, beginning January 1, 2021, to provide annual information security training for each of its employees using the curriculum and materials developed by the CIO.

<https://lis.virginia.gov/cgi-bin/legp604.exe?201+ful+HB852ER>

## CURRICULUM REQUIREMENTS

*The curriculum shall include the following:*

- *Activities,*
- *Case studies*
- *Hypothetical situations*
- *And other methods of instruction:*
  - (i) that focus on forming good information security habits and procedures among state employees and
  - (ii) that teach best practices for detecting, assessing, reporting, and addressing information security threats.

## AGENCY REQUIREMENTS

- ▶ Each state agency shall:
  - monitor and certify the training activity of its employees to ensure compliance with the annual information security training requirement
  - evaluate the efficacy of the information security training program,
  - forward to the CIO such certification and evaluation, together with any suggestions for improving the curriculum and materials, or any other aspects of the training program.

## VITA TASKS ASSIGNMENTS

VITA formed a security awareness training committee to address the requirements of HB 852. The committee is comprised of Information Security Officers from various state agencies.

The task of the committee is as follows:

1. Prepare a security awareness curriculum for training all state employees.
2. Develop a certification form that agencies must complete on an annual basis attesting compliance of a mandatory security awareness training solution or platform.
3. Develop a security awareness training standard

## SECURITY AWARENESS TRAINING SOLUTIONS

- Many agencies already have procured security awareness software training solutions
- The committee has evaluated a number of the most popular training solutions and determined the curriculum requirements that they currently meet or do not meet
- Software or training solutions that we have not evaluated will also be considered. Agencies will need to let us know what they are using so we can review them
- Role-based training will be part of the required curriculum
- Agencies will be expected to comply with all curriculum requirements.
- VITA will assist agencies in identifying gaps in curriculum coverage and provide alternative means to fulfill those requirement gaps
- One of the requirements in HB852 will be for agencies to inform VITA of improvements that we can make to the overall training program.



## TIMELINES

HB 852 Passed - **April 2020**

Mandatory training curriculum will be developed and IT Security Awareness Training Standard will be completed – **November 30, 2020**

VITA will be requesting agencies to identify their current or proposed security awareness training program or solution – **December 1, 2020**

HB 852 requirements become effective - **January 1, 2021**

Per HB 852, agencies must certify that their employees and contractors have met mandatory training requirements by an official notification to VITA– **January 31, 2022**

## SECURITY AWARENESS TRAINING COMMITTEE

Joe Walton (DBHDS) – Chair

Deborah James (RBC) – Co Chair

Mike Riggs (Supreme Court of Va)

Dave Burhop (DLAS)

Simon Xue (TAX)

Jim Husband (DWR)

Stephanie Williams-Hayes (VDH)

Marlon Cole (VITA)

Ed Miller (VITA)

Tina Harris-Cunningham (VITA)

Contact [Edward.miller@vita.virginia.gov](mailto:Edward.miller@vita.virginia.gov) or [Tina.Harris-Cunningham@vita.virginia.gov](mailto:Tina.Harris-Cunningham@vita.virginia.gov) if you have questions.



# 2019 IT SECURITY GOVERNANCE

**ED MILLER**

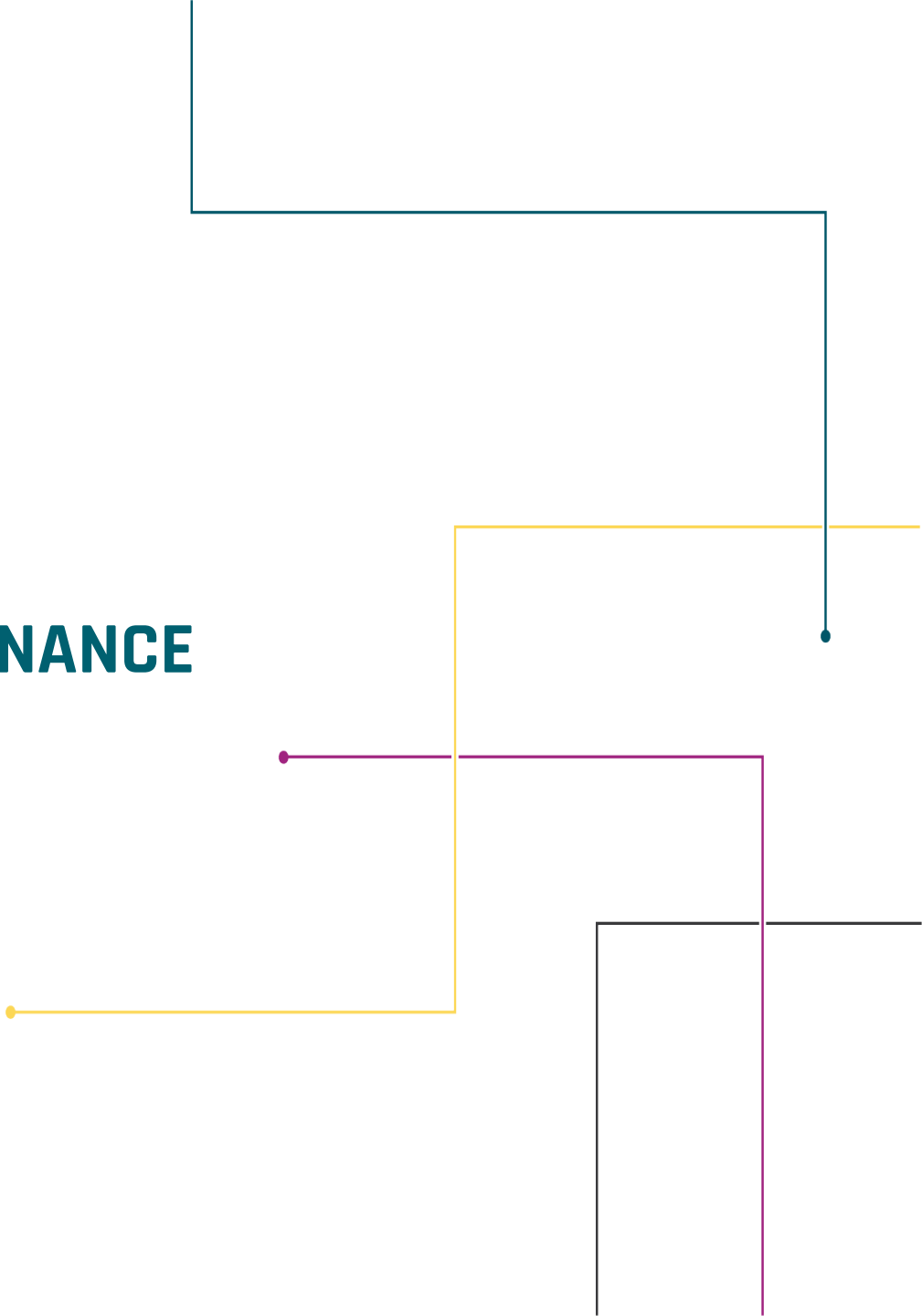
DIRECTOR IT SECURITY GOVERNANCE

**JOY YOUNG**

IT ANALYST

ISOAG

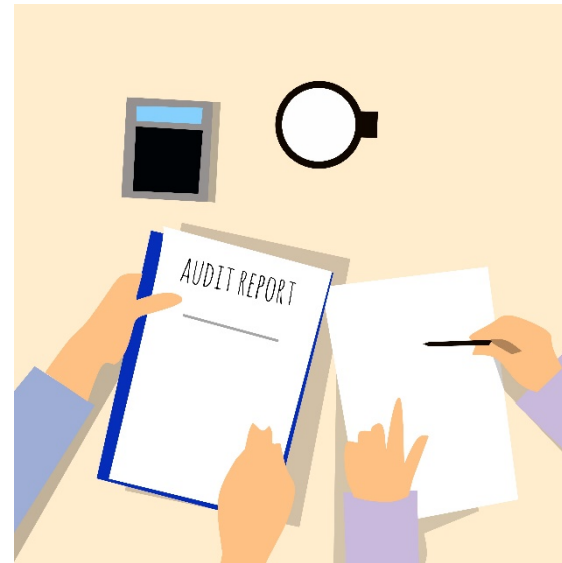
OCT. 7, 2020





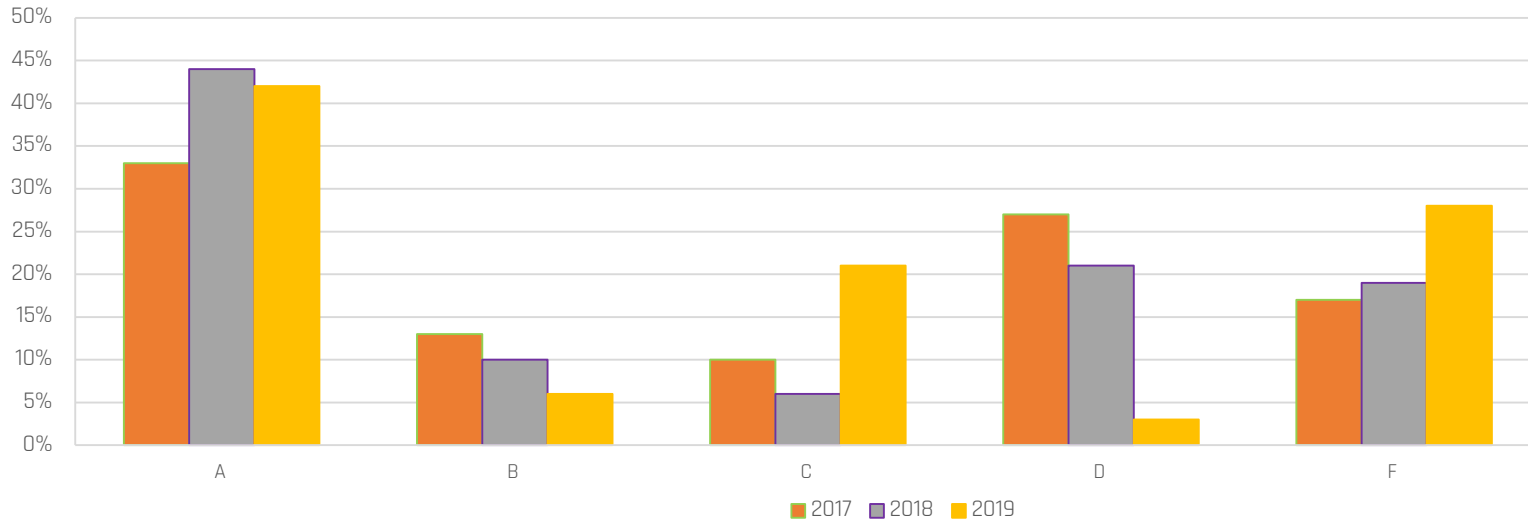
## IT SECURITY AUDIT

- Overall audit compliance declined 2%
- 90% of agencies submitted audit plans as required
- Three-year audit obligation improved by 4%, with 40% of agencies completing the audits of their sensitive systems as required





### COV Audit Compliance Grades 2017-2019





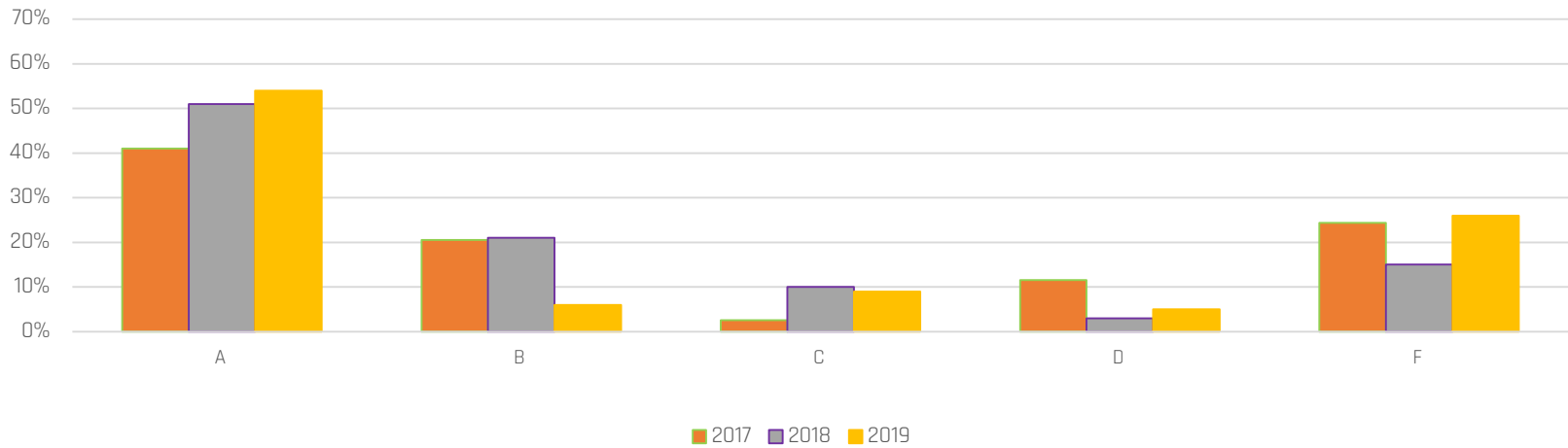
## IT SECURITY AUDITS

- Most agencies (77%) that completed IT security audits provided audit findings updates (corrective actions plans) as required



# RISK

## COV RISK COMPLIANCE GRADES 2017-2019



## RISK

- Most agencies (82%) submitted a risk assessment plan
- Almost half of agencies (49%) with a risk assessment plan completed the required risk assessments







## RISK

- Most agencies (90%) have appointed an information security officer (ISO)
- Over half of agencies ISO's (55%) comply with the requirement to report directly to their agency head



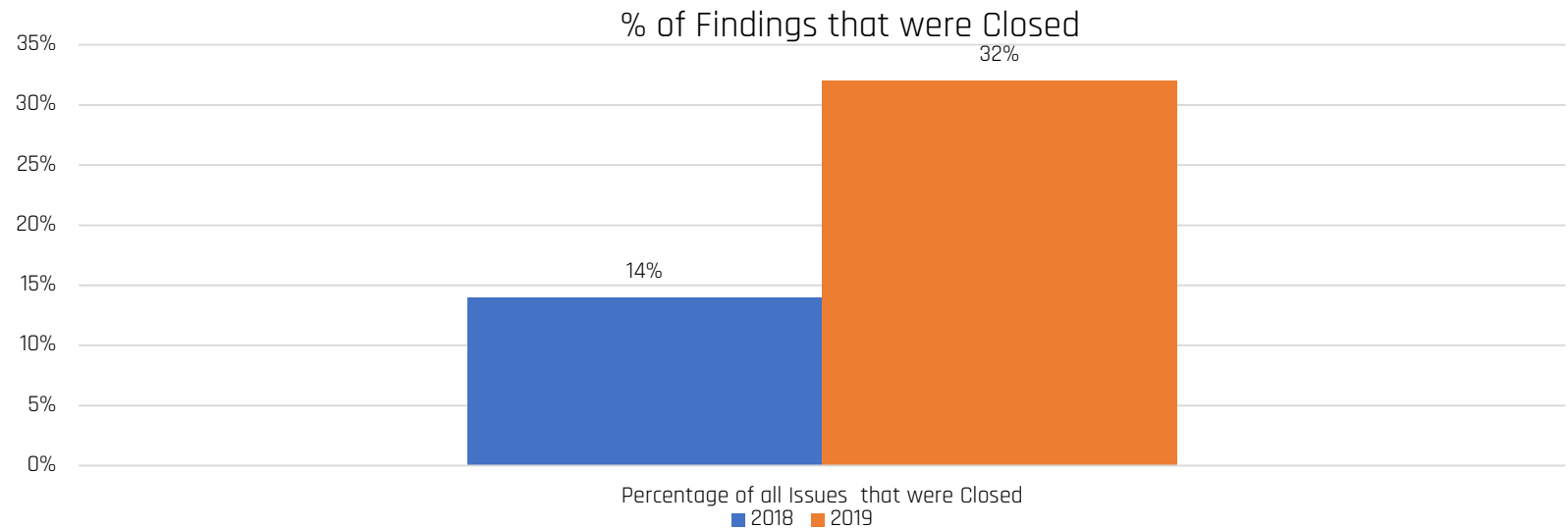
## RISK

- Business impact analysis metrics remained stable (declined by 1%)



## FINDINGS ANALYSIS

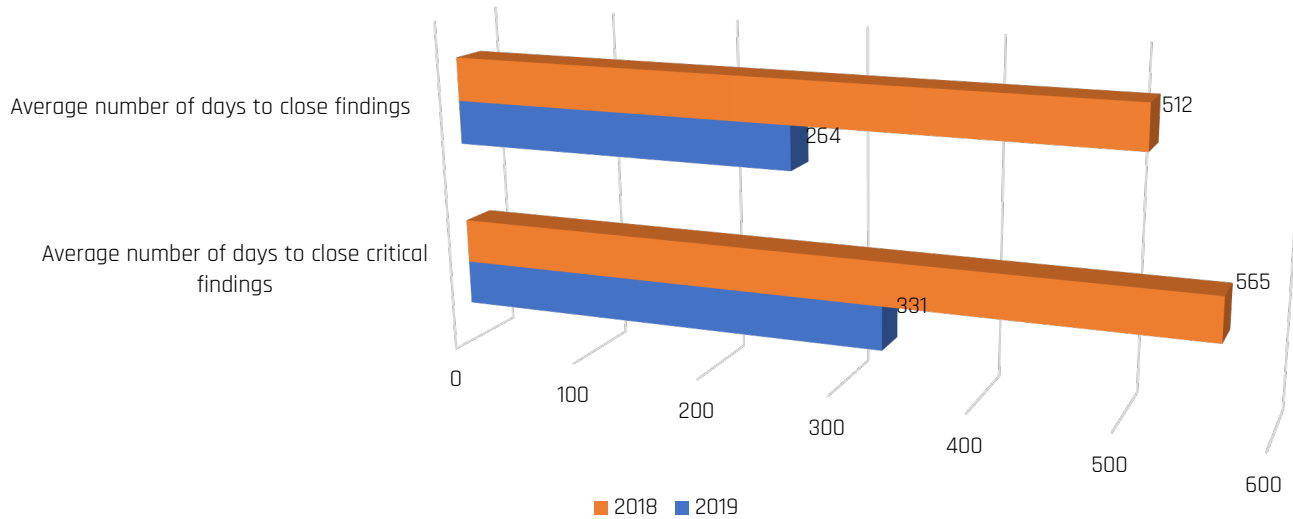
More IT security audit findings are being remediated





## FINDINGS ANALYSIS

Average # of Days to Close Findings





## TOP 5 MOST COMMON CONTROL FAMILIES IDENTIFIED IN AUDIT FINDINGS:

- Access control
- Audit and accountability
- Contingency planning
- Configuration management
- System and services acquisition



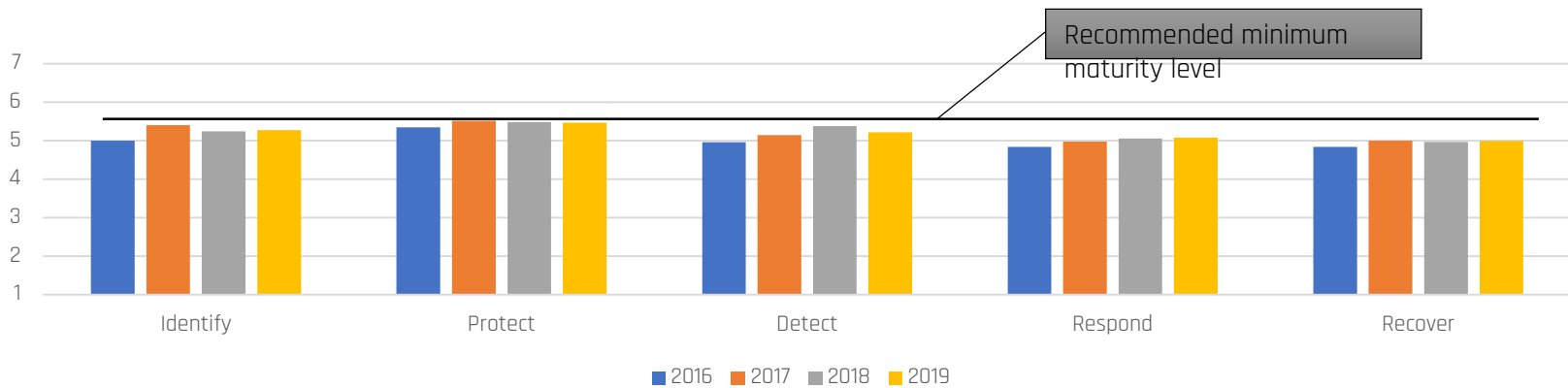
## NCSR SURVEY

- The number of commonwealth agencies who participated in the survey increased from 65 agencies in 2018 to 70 agencies in 2019, an increase of 7%



## NCSR SURVEY

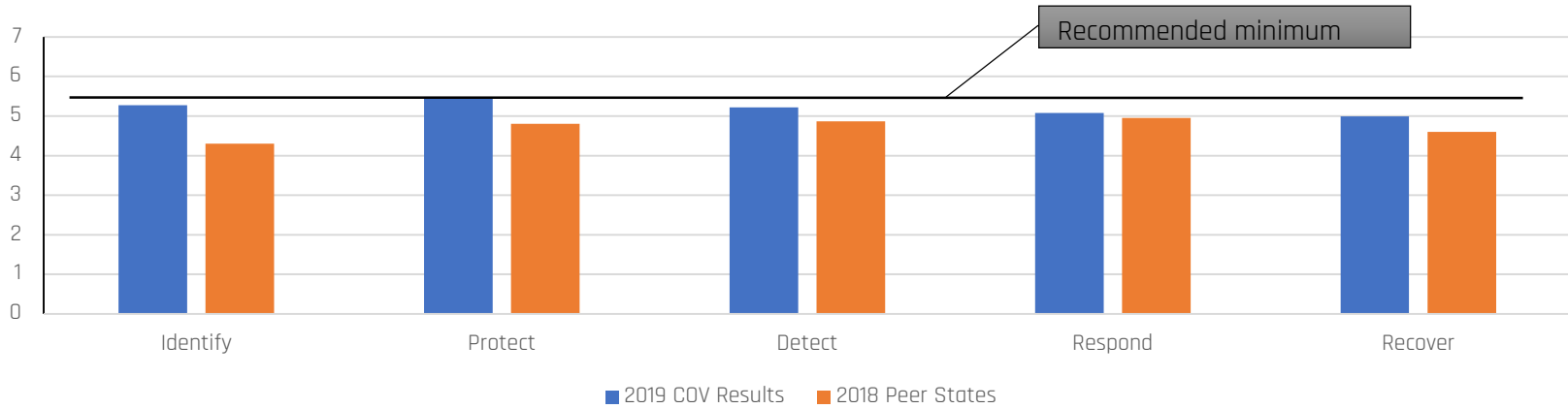
NCSR Results for Commonwealth Agencies  
Year over Year Comparison





## NCSR SURVEY

NCSR Results  
COV to Peer States Comparison







## POLICY AND STANDARDS

- Updates to SEC519 IT Security Policy
- Updates to SEC501/SEC525 to reflect changes in NIST 853 rev 5:
  - Rev 5 does include additional control families that may be included
    - PII Processing and Transparency Family (PT)
    - Supply Chain Risk Management Family (SR)
- Updates to SEC502 IT Security Auditing Standard (leveraging SOC and third party audits)
- Updates to SEC520 Risk Management Standard
- Updates to SEC514 Media Disposal Standard



## POLICY AND STANDARDS

- New standards are also being developed
  - Identity and Access Management Security Standard
  - Industrial Control Systems (ICS) Security Standard – SEC526



## ADDITIONAL NOTES

- ISO's reporting to agency head is a requirement for ISO certification
- Critical findings that are not closed/remediated within 90 days will require an exception. Corrective action plans with planned due dates longer than 90 days are not acceptable and will require an exception.



## FUTURE CONSIDERATIONS

- CSRM plans to encourage more participation by Commonwealth institutions of higher education in the 2020 NCSR survey
- Be on the lookout for upcoming updates to the IT security policy and standards. Changes will be posted on ORCA for comments and review. We'll announce those at this meeting.

## QUESTIONS

Email:

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





# RANSOMWARE

**RENEA DICKERSON**

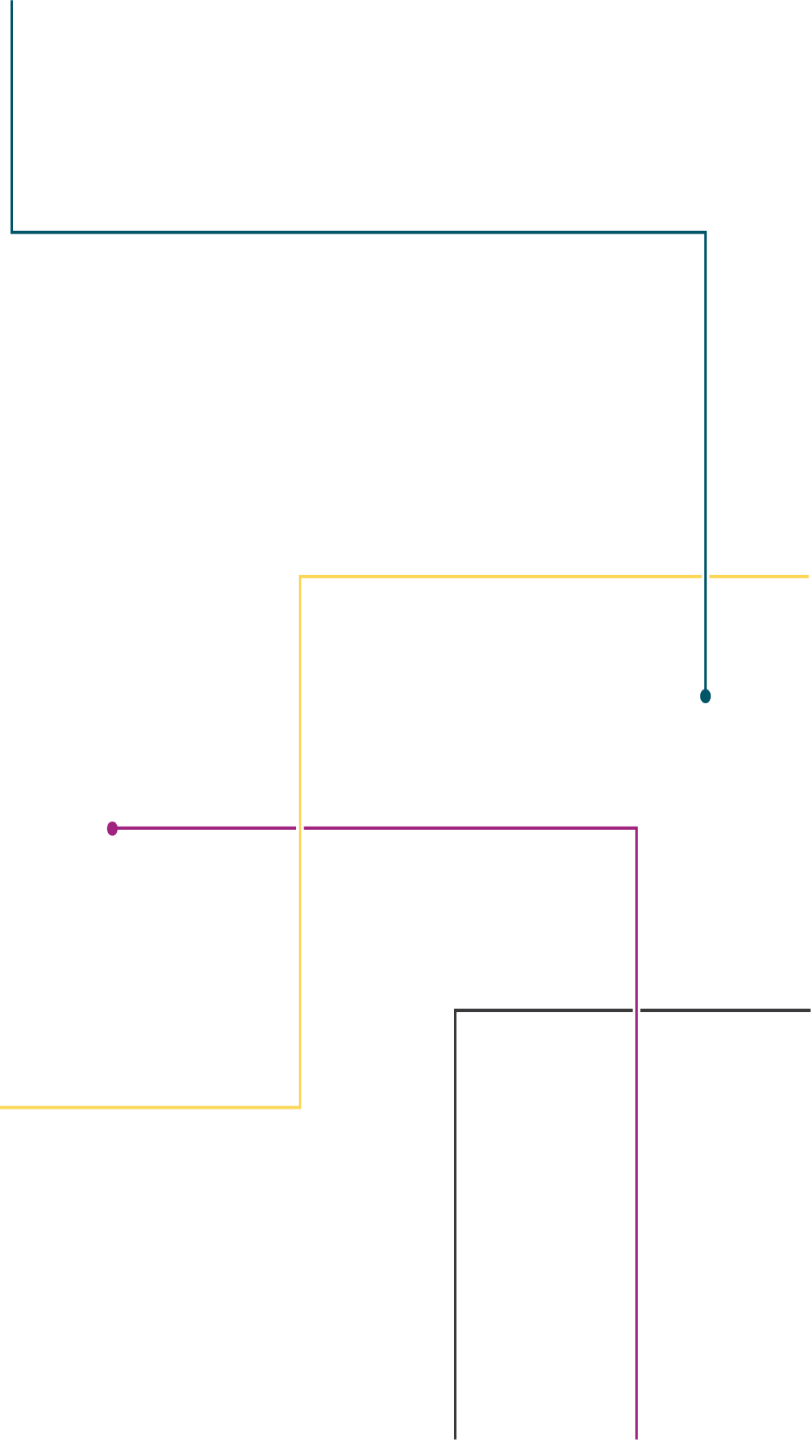
IT ANALYST

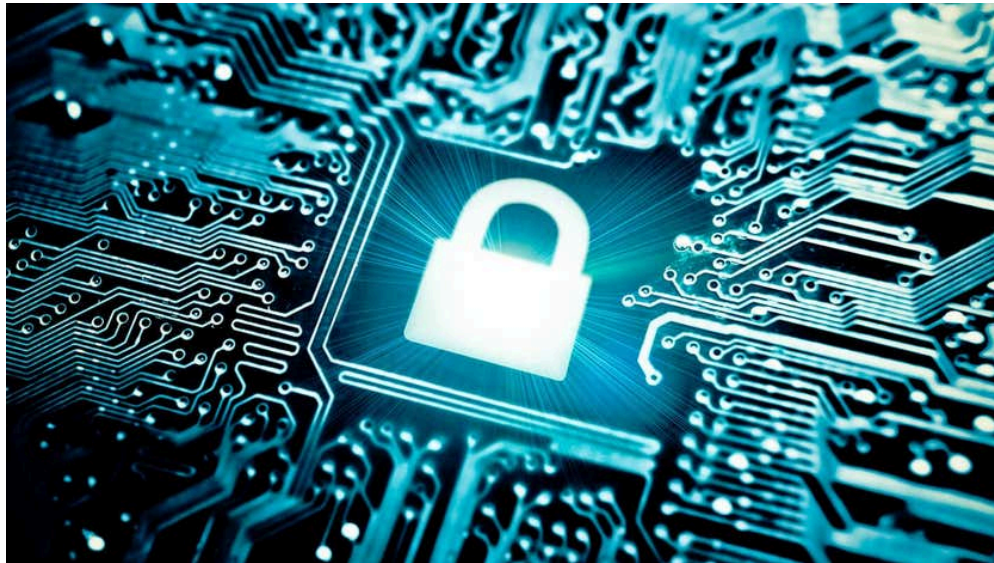
ISOAG

OCT. 7, 2020

**MARLON COLE**

IT ANALYST





***The first instance of what we now know as ransomware was called the AIDS Trojan because of who it was targeting – delegates who'd attended the World Health Organization AIDS conference in Stockholm in 1989.***

***Attendees were sent floppy discs containing malicious code that installed itself onto MS-DOS systems and counted the number of the times the machine was booted. When the machine was booted for the 90th time, the trojan hid all the directories and encrypted the names of all the files on the drive, making it unusable.***

***Victims saw instead a note claiming to be from 'PC Cyborg Corporation' which said their software lease had expired and that they needed to send \$189 by post to an address in Panama in order to regain access to their system.***

***It was a ransom demand for payment in order for the victim to regain access to their computer: that made this the first ransomware.***

***After this attack, it wasn't for another 20 years that ransomware as we know it now started to emerge; and those first attacks were still not complex compared with ransomware today.***

***From: ZDNet, December 19, 2019***



Ransomware is a type of malicious software that uses encryption to hold a victim's information hostage. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access. Ransomware is also often designed to spread across a network and target database and file servers.

IT typically spreads through phishing emails, network intrusion through poorly secured ports and services, such as Remote Desktop Protocol (RDP) or by unknowingly visiting an infected website.

Older versions of ransomware initially only locked users out of their devices. Around 2012, attackers also began encrypting files. With the advent of the Bitcoin boom, ransomware attacks also exploded and ransomware-as-a-service became common place.

Ransomware-as-a-Service (RaaS) borrows from the Software-as-a-Service (SaaS) model. This subscription-based malicious model enables even the inexperienced cybercriminal to launch ransomware attacks without much experience. Various RaaS packages can be found that reduces the need to code malware. It is commonly used by cybercriminals who don't have much technical knowledge of how to create ransomware. This model allows anyone to become an "affiliate" of an established RaaS package or service.

Ransomware has become one of the biggest security problems on the internet and one of the biggest forms of cybercrime that organizations face today.

To determine the extent of the Commonwealth's susceptibility to possible ransomware attacks, the House and Senate passed Bill HJ 64.

**HJ 64 Ransomware attack preparedness; Virginia Information Technologies Agency (VITA) to study.**

**Study; Virginia Information Technologies Agency; ransomware attack preparedness; report. Requests the Virginia Information Technologies Agency (VITA) to study the Commonwealth's susceptibility, preparedness, and ability to respond to ransomware attacks. In conducting its study, the Agency shall (i) assess the Commonwealth's susceptibility to ransomware attacks at the state and local levels of government; (ii) develop guidelines and best practices to prevent ransomware attacks; (iii) evaluate current data encryption and backup strategies; (iv) evaluate the availability of tools to monitor unusual access requests, viruses, and network traffic; (v) develop guidance for state agencies and localities on responding in the event of a ransomware attack; (vi) develop a coordinated law-enforcement response strategy that utilizes forensic investigative techniques to identify the source of ransomware attacks; and (vii) provide recommendations on legislative or regulatory changes to better protect state and local government entities from ransomware. The bill requires VITA to report its findings to the Governor and the General Assembly no later than the first day of the 2021 Regular Session.**



The bill tasks the Virginia Information Technologies Agency (VITA) to study the Commonwealth's susceptibility, preparedness, and ability to respond to ransomware attacks. Some of the areas to be addressed are:

- developing guidelines and best practices to prevent ransomware attacks
- evaluating current data encryption and backup strategies
- evaluating the availability of tools to monitor unusual access requests, viruses, and network traffic
- developing guidance for state agencies and localities on responding in the event of a ransomware attack
- developing a coordinated law-enforcement response strategy that utilizes forensic investigative techniques to identify the source of ransomware attacks
- providing recommendations on legislative or regulatory changes to better protect state and local government entities from ransomware.



To assist with collecting information for the ransomware study to present to the General Assembly in 2021, VITA requested the assistance of the ISO Council.

The ISO Council, in response to this request formed a ransomware committee which consists of representatives from the executive and independent branches and the localities.

The committee and VITA representatives have been meeting since the early part of 2020 to generate an inclusive body of information.

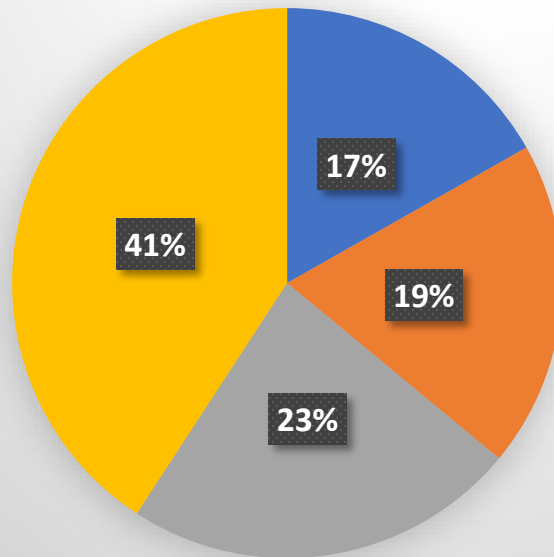
- **Joseph Walton, Department of Behavioral Health and Development Services**
- **Michael, Wickham, Virginia Workers Compensation Commission**
- **Kathy Bortle, Virginia Information Technologies Agency**
- **Marlon Cole, Virginia Information Technologies Agency**
- **Renea Dickerson, Virginia Information Technologies Agency**
- **George Fishel, Office of Attorney General**
- **Daniel Persico, Department of Elections**

- **Broadus Pettiford, Office of Attorney General**
- **Robert Reese, Virginia State Police**
- **John Singleton, Virginia State Police**
- **Mitchell Smith, Virginia State Police**
- **Joshua Heslinga, Virginia Information Technologies Agency**
- **Dean Johnson, Virginia Information Technologies Agency**
- **Edward Miller, Virginia Information Technologies Agency**

To gain insight into the current state of ransomware preparedness within the commonwealth, the ransomware committee and VITA created a survey which was sent to executive, legislative, independent and judicial branches as well as the localities, higher Ed and K-12 schools. The cutoff for the survey was in September and the results are currently being tabulated and analyzed.



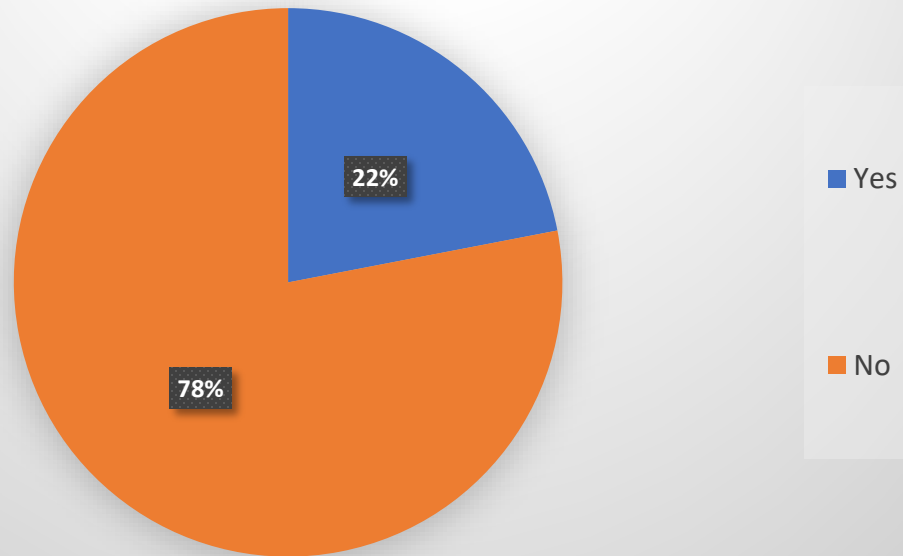
### Percentage of Commonwealth Organizations Surveyed

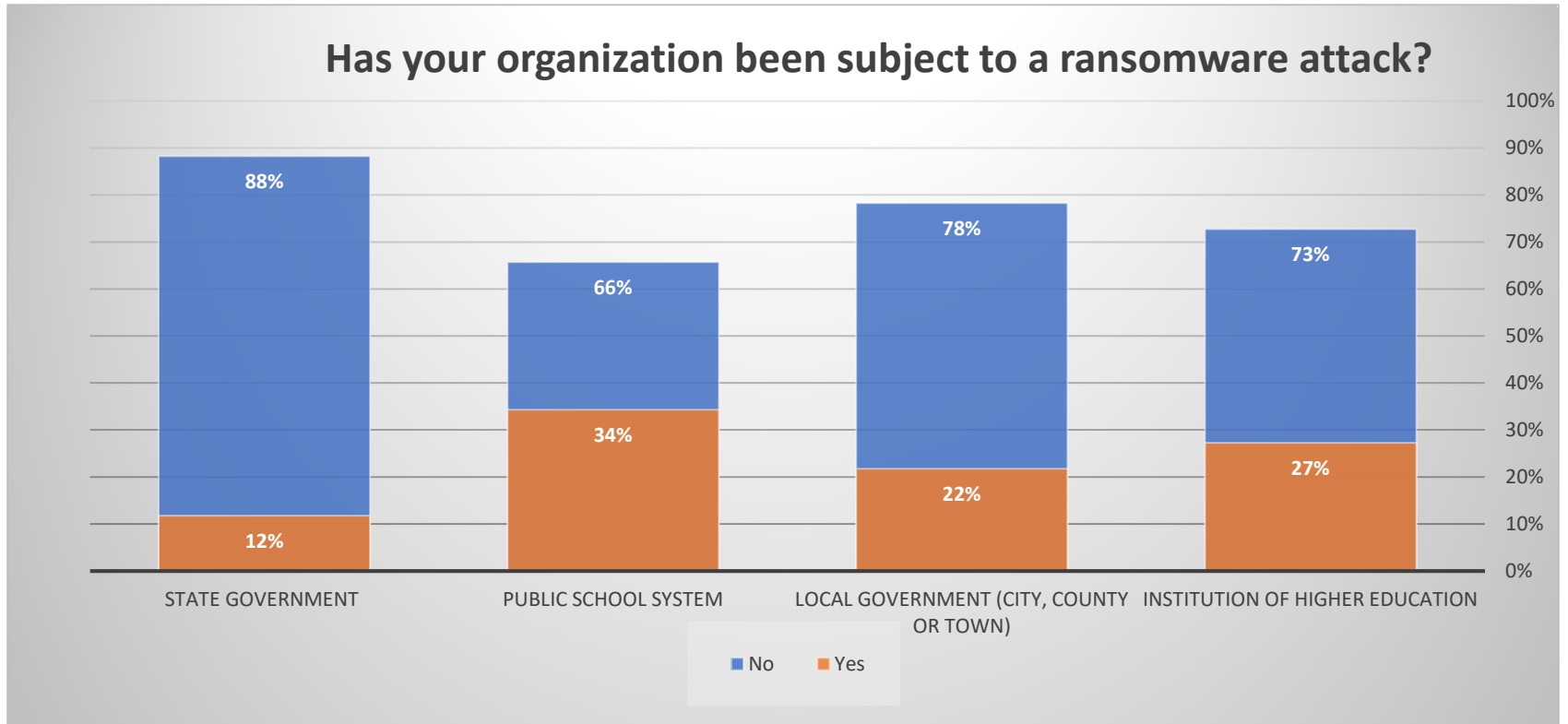


- Institution of higher education
- Local Government (city, county or town)

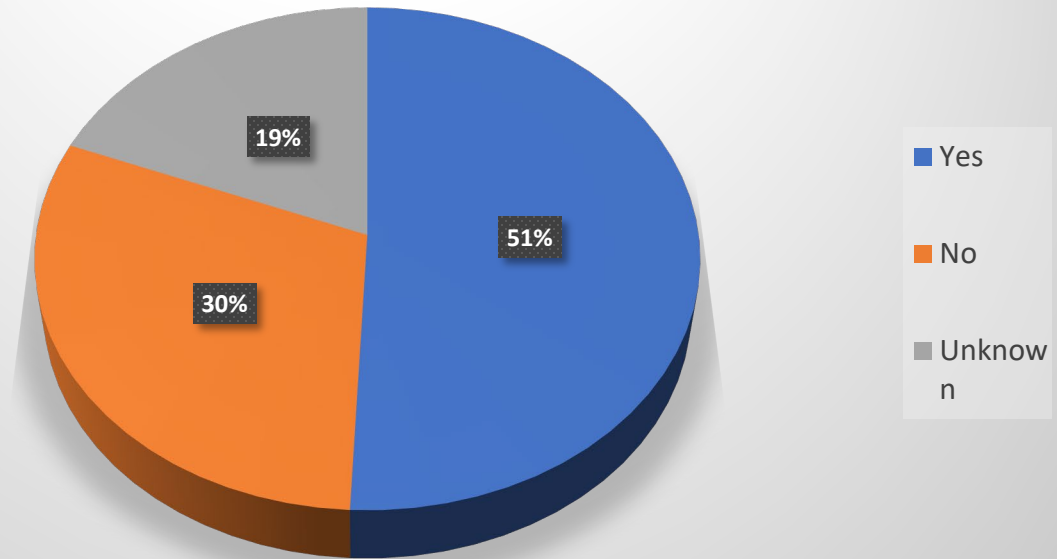


### Has your organization been subject to any ransomware attack?

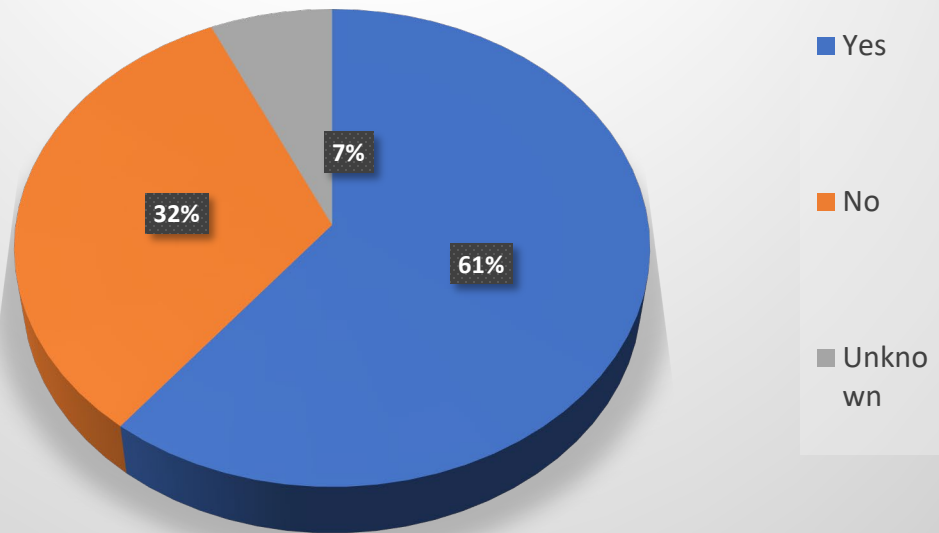




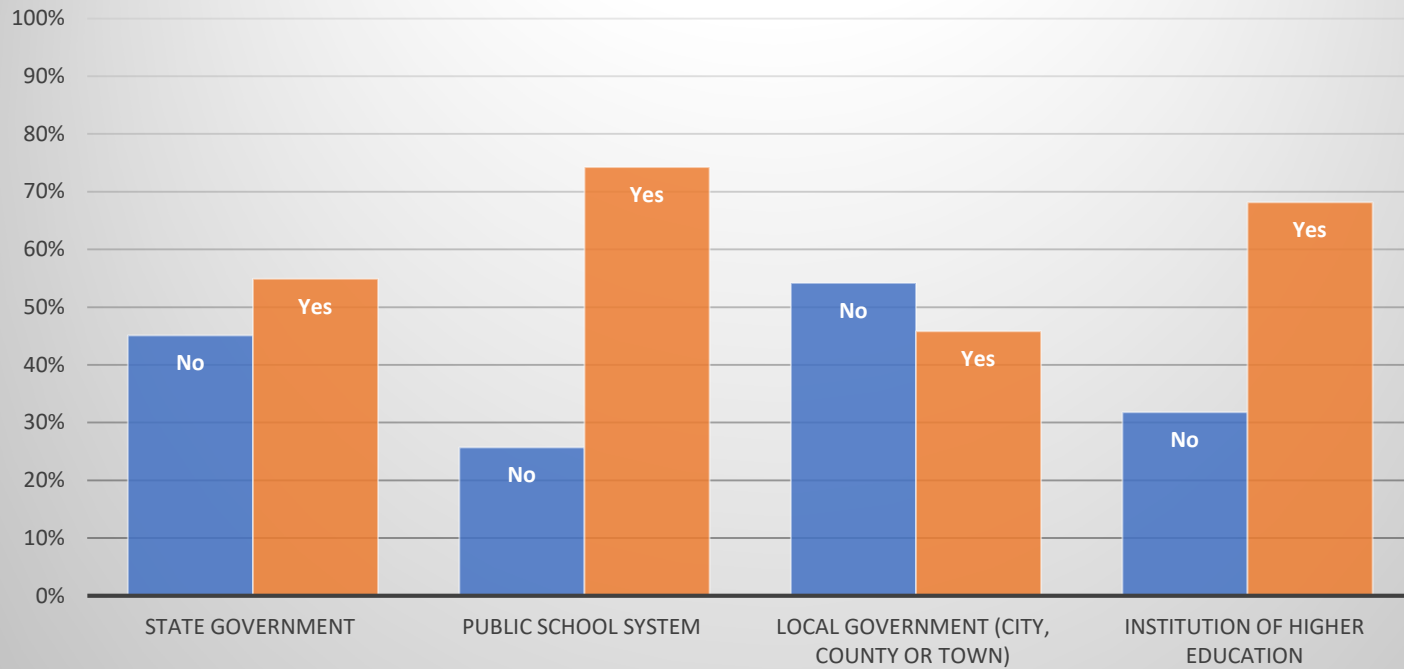
### Does your organization have cybersecurity insurance?



### Does your organization continuously monitor network activity?

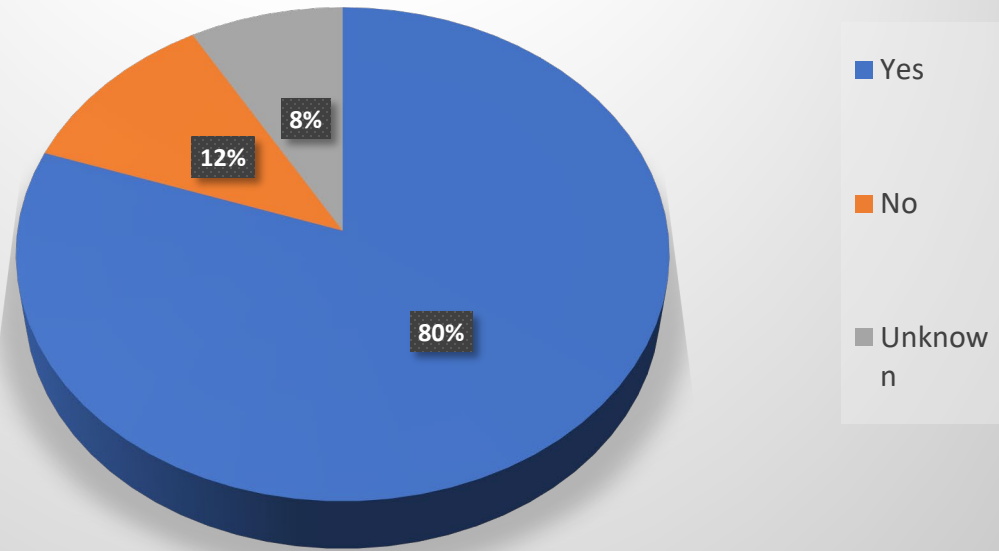


### Does your organization continuously monitor network activity?

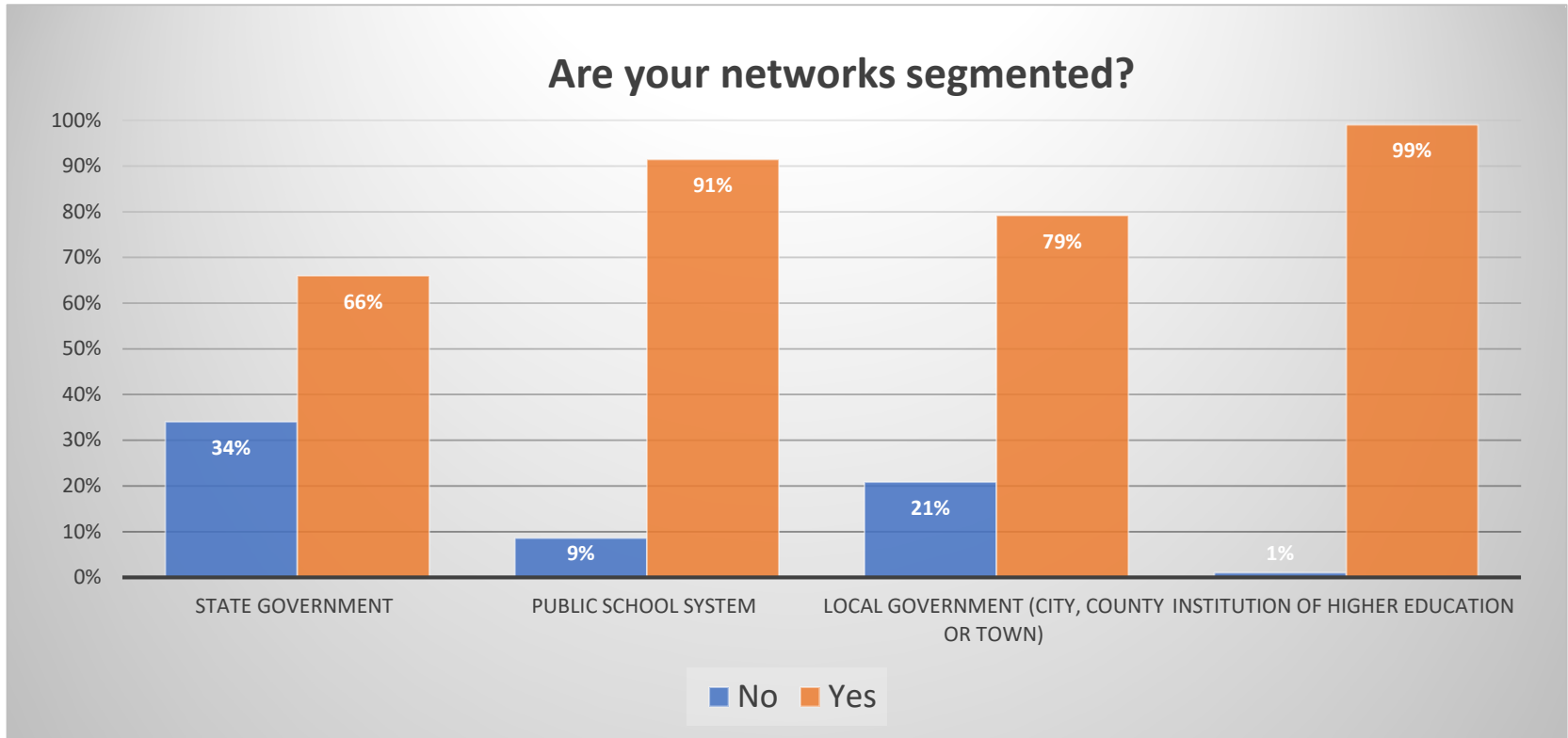




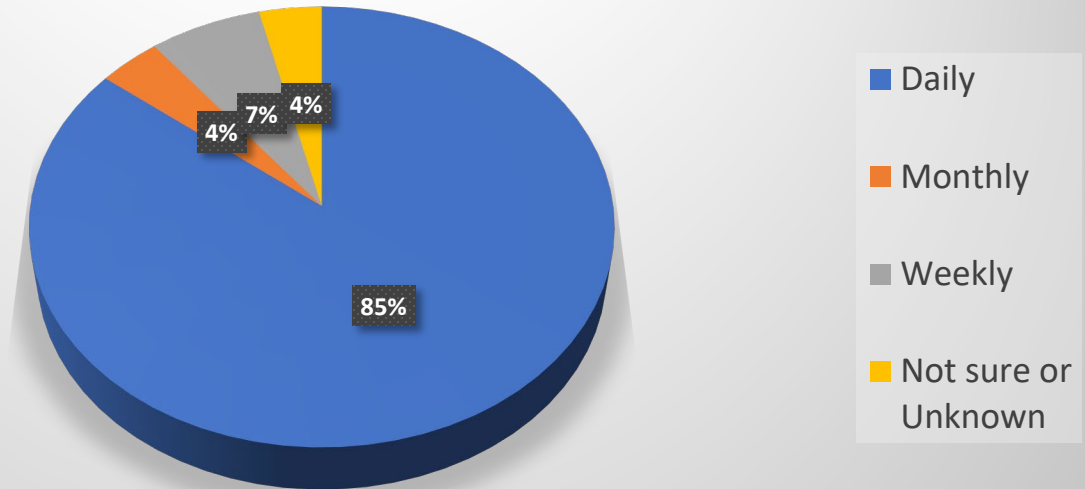
### Are your networks segmented?

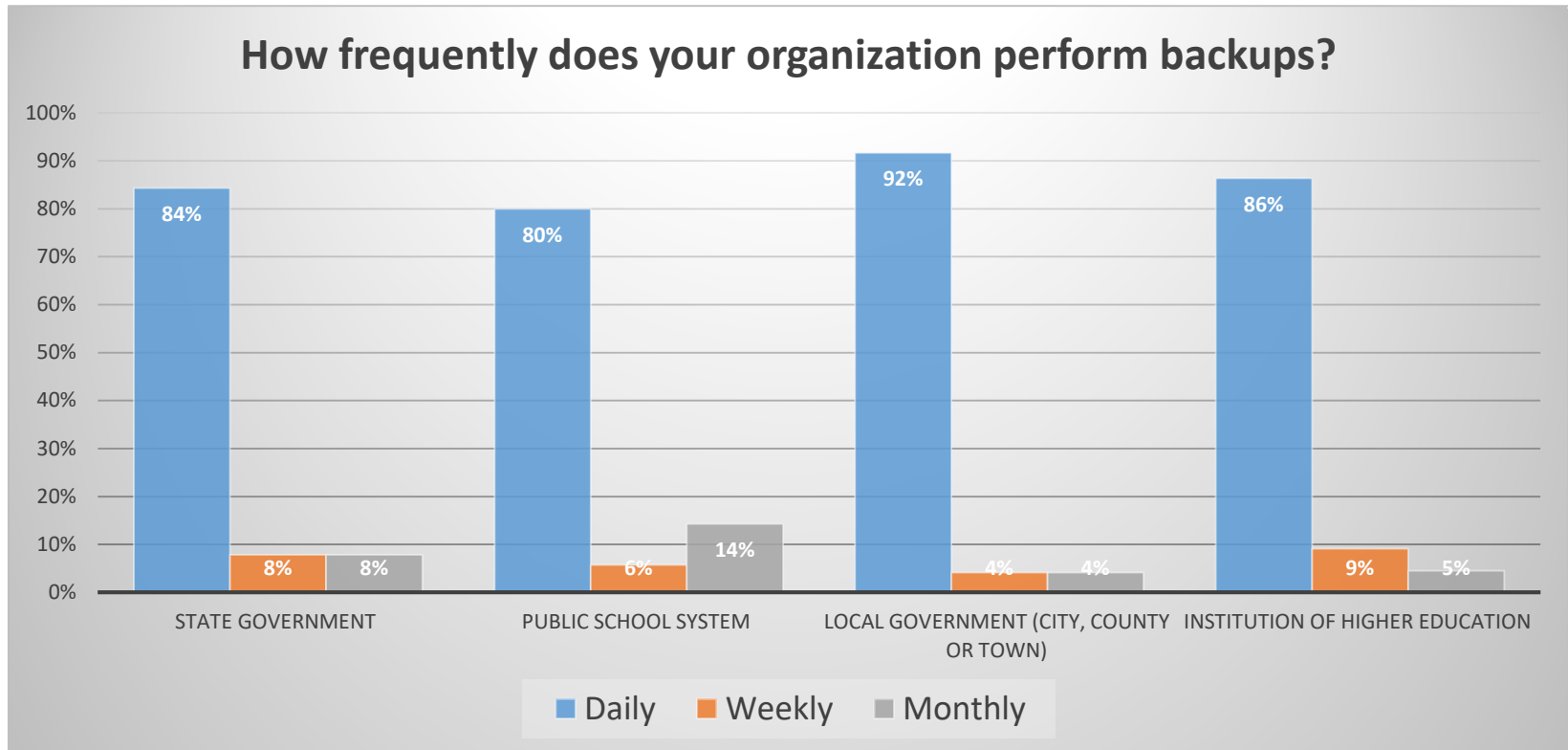




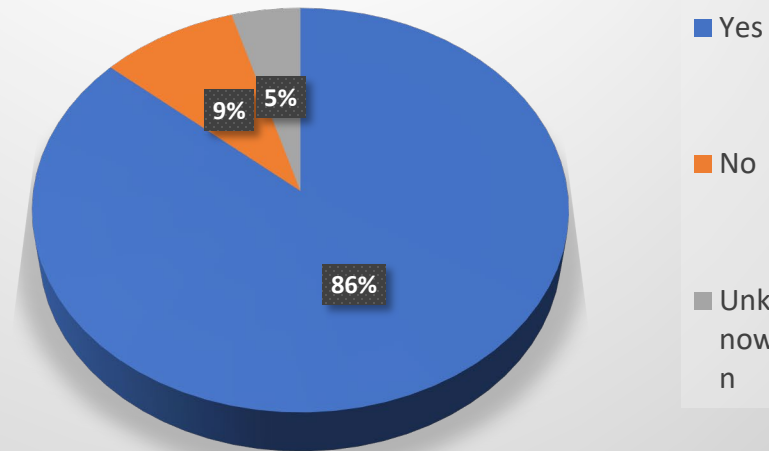


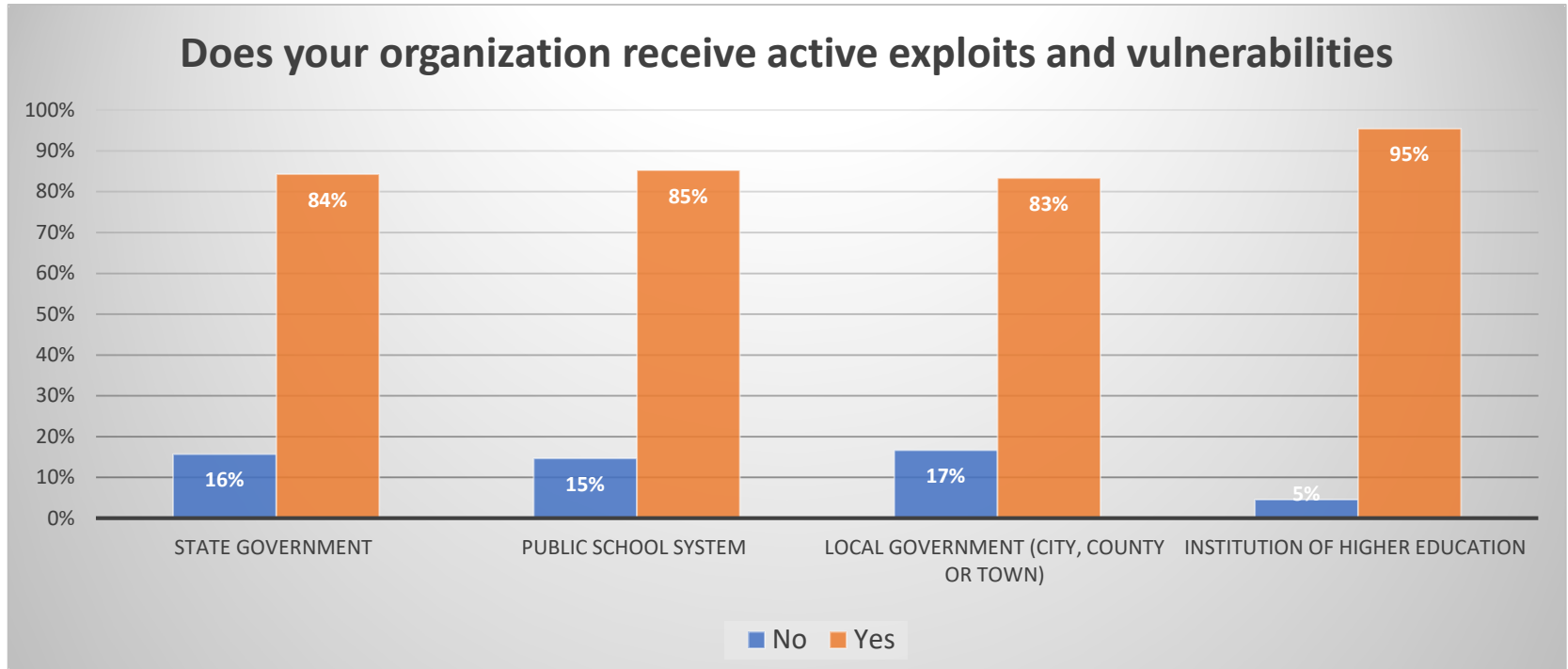
### How frequently does your organization perform backups of its data and computer systems?





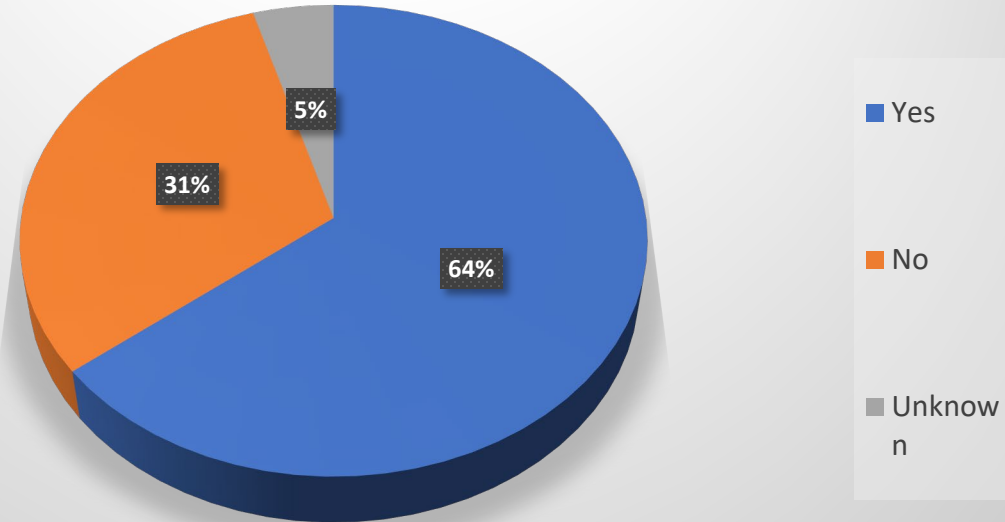
### Does your organization receive reporting on active exploits and vulnerabilities that may impact your environment?

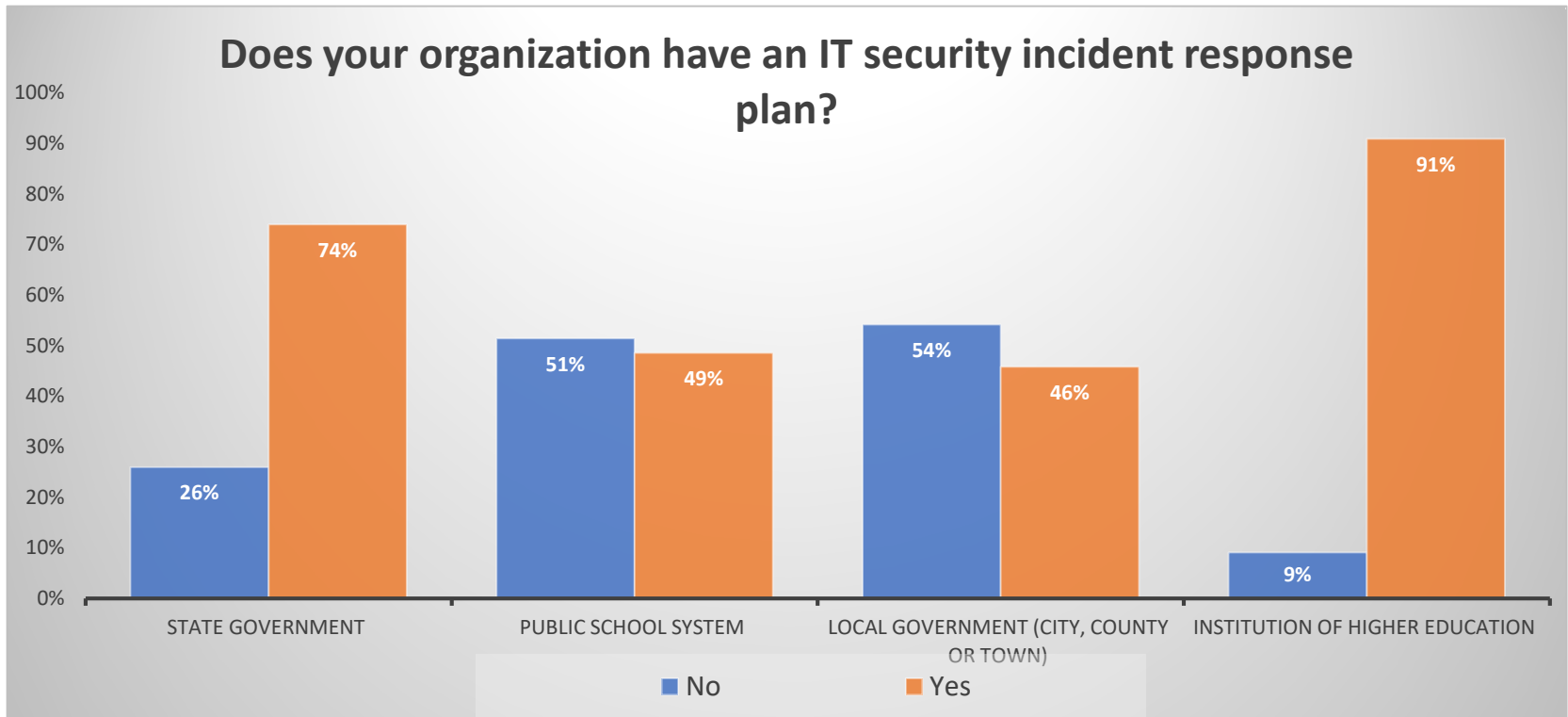




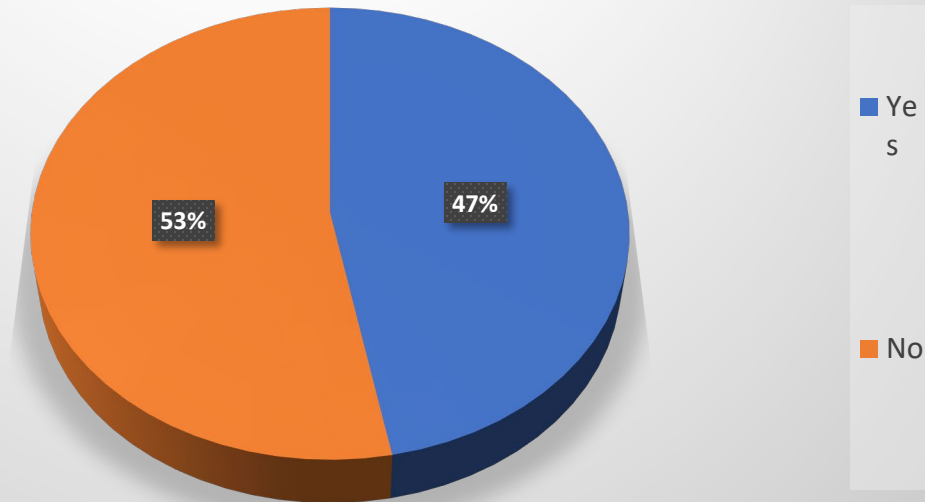


### Does your organization have an IT security incident response plan?



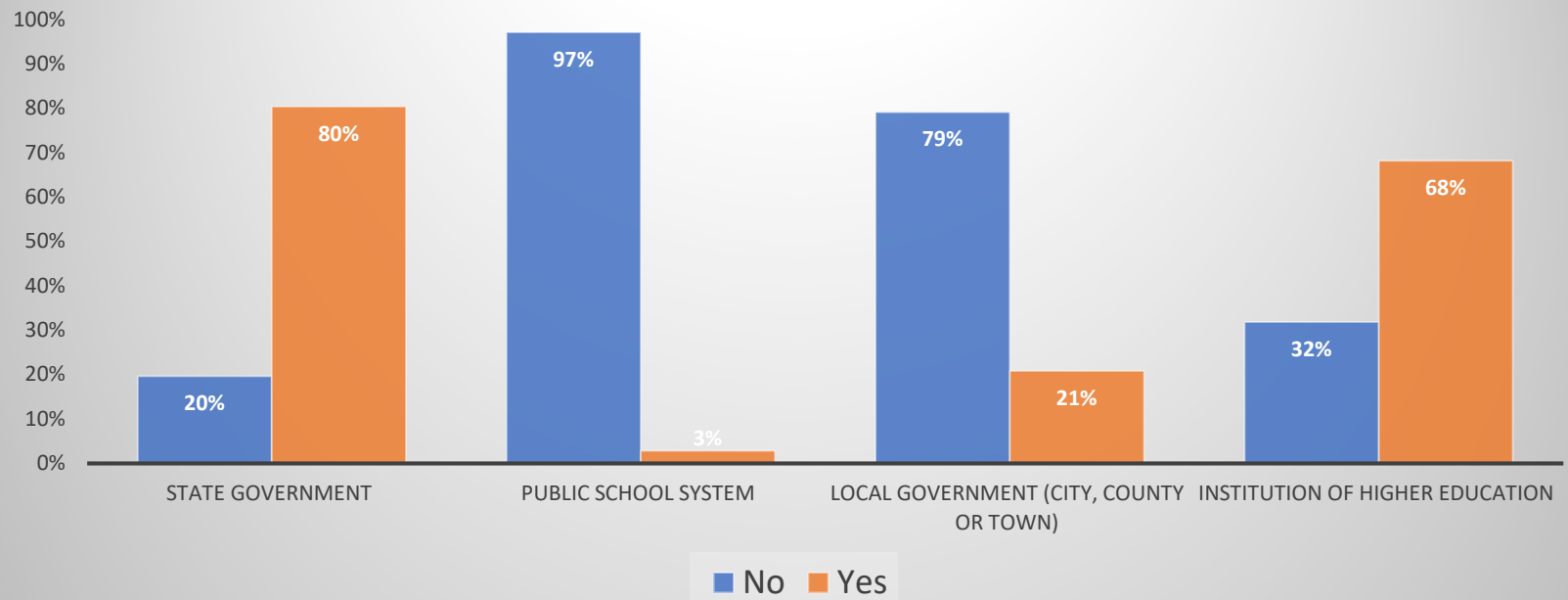


### Are all consultants/contractors required to take IT security awareness training?





## Are contractors required to take IT security awareness training?





**The requirement is to have the report completed before the end of the year in preparation for presentation to the General Assembly in 2021.**



**QUESTIONS???**



# CENTRALIZED IT SECURITY AUDIT SERVICE

Mark McCreary, CISA, CISSP, CISM

Director

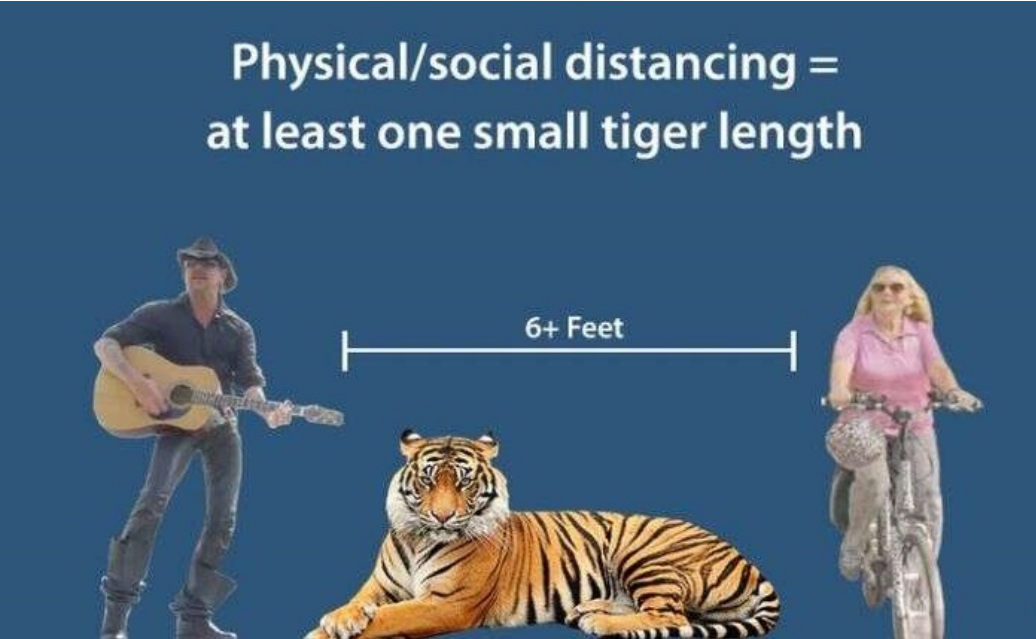
ISOAG

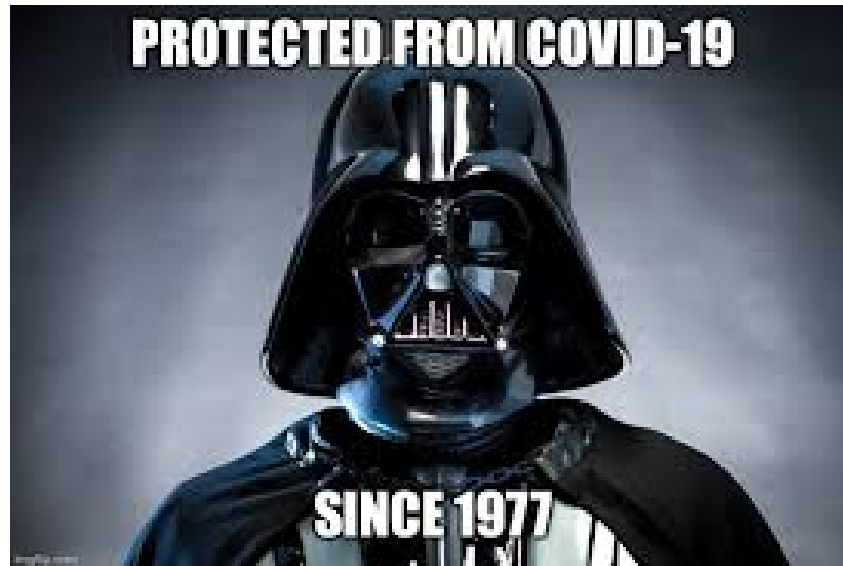
Oct. 7, 2020



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ Risk-Based Audits
- ❖ Benefits from Using the Service
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding











➤ Current version is 502.3

➤ Found on VITA's website:

<https://www.vita.virginia.gov/it-governance/itrm-policies-standards/>



- IT Security Audit Standard (SEC502) requires audits of each Sensitive System every three-years.
- Measures compliance with the applicable requirements of IT Security Standard 501.
- Also includes other Federal regulations or COV Standards as applicable.



- ❖ IT Security Audit Standard
- ❖ **Centralized IT Security Audit Service**
- ❖ Risk-Based Audits
- ❖ Benefits from Using the Service
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding



## Our Team

Mike Dorris, Sr. IT Security Auditor

Nat Chusing, IT Security Auditor

Matt Steinbach, IT Security Auditor

Autumn Mashore, IT Security Auditor

### The Information Technology Auditor's Toolkit

- **people skills**
  - to work as a team
  - to interact with clients and other auditors,
  - to interview many people constantly for evaluation
  - can't just be a technical nerd!



- Conducts Risk-Based IT Security Audits
- Helps identify appropriate Corrective Action Plans
- Helps with annual Audit Plan Submission



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ **Risk-Based Audits**
- ❖ Benefits from Using the Service
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding





- 1 = Account Management
  - 2 = Awareness and Training
  - 3 = Contingency Planning
  - 4 = Risk Assessment
- Bulls Eye = Pick any Family



## Determine High-Risk Areas By:

- Evaluating *Pre-Audit Internal Control Questionnaire(s)*
  
- Evaluating results of other audits or reviews
  - System and Organization Controls (SOC) Reports
  - Prior Audit Reports, Outstanding Findings





- Reviewing Security Exceptions
- Evaluating additional controls for Hosted Applications
  - Uses SEC525, some controls more restrictive than SEC501
  - Emphasis placed primarily on areas the agency controls, for example, Access Controls and Contingency Planning
  - ECOS Assessments/Oversight



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ Risk-Based Audits
- ❖ **Benefits from Using the Service**
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding





- Familiar with Commonwealth Security Standards and VITA Operations
- More cost-effective than private firms as DPB sets rates
- Knowledge retention
- Helps provide awareness to Agency Heads of IT security control weaknesses





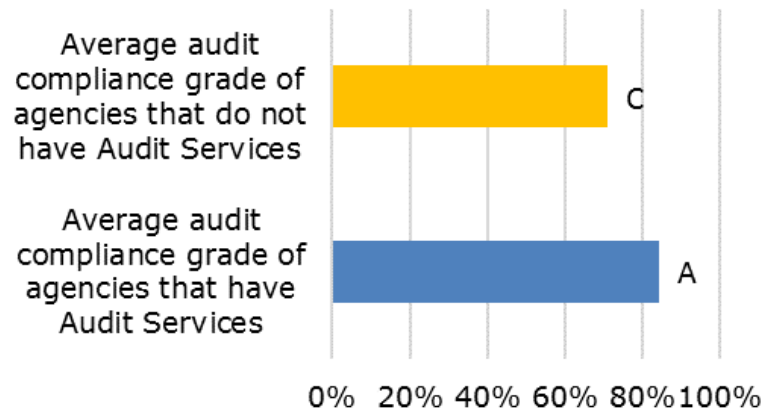
## *Audit Compliance Grade*

- 1) Sensitive System Audits conducted at least once every three-years +
- 2) Audit Plan Updated and Submitted +
- 3) Quarterly Finding Updates Submitted =

A

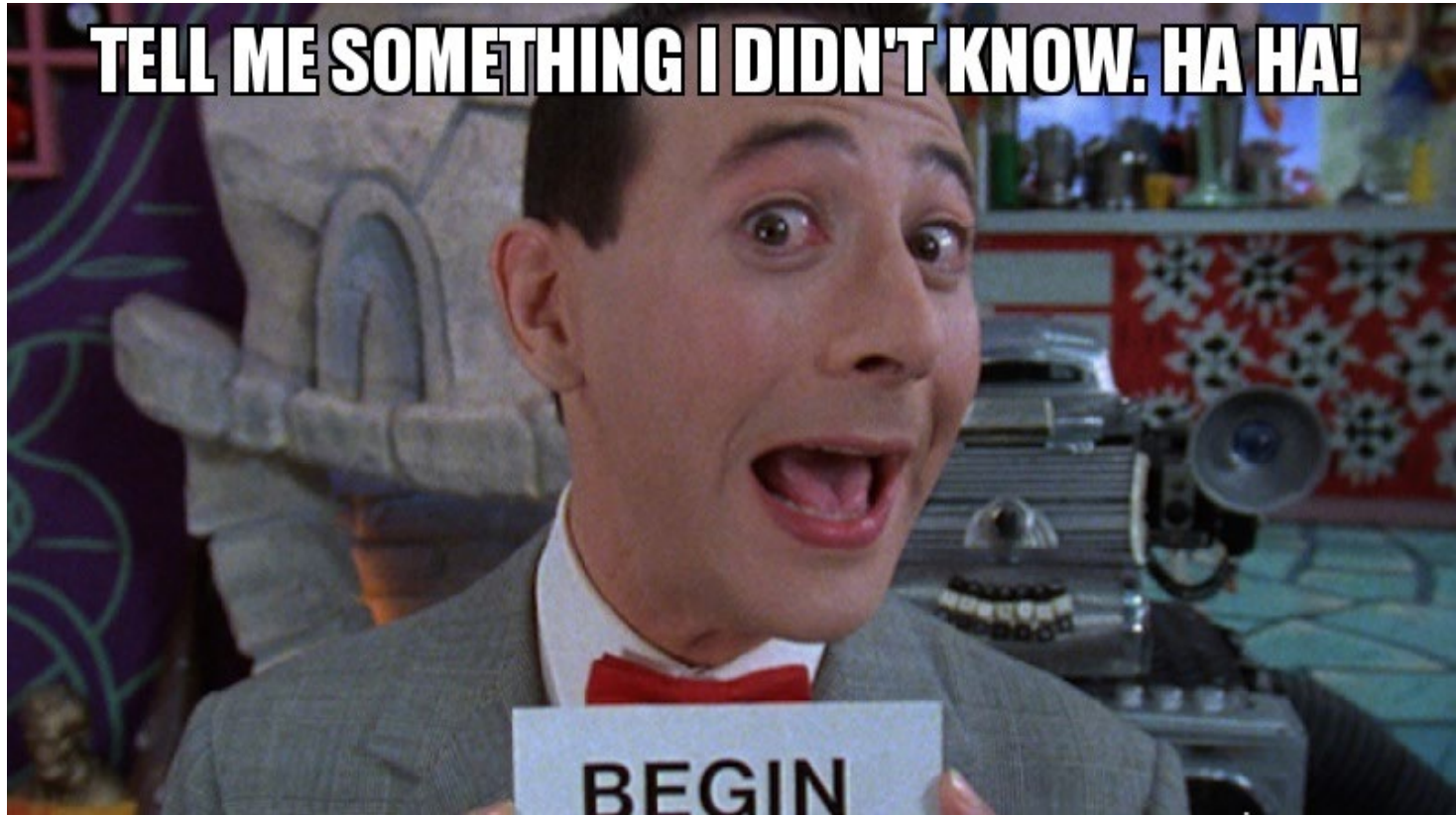


### Average Audit Compliance Grades Audit Services Agencies vs. Non- Audit Services Agencies



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ Risk-Based Audits
- ❖ Benefits from Using the Service
- ❖ **Common Issues Found During Audits**
- ❖ Memorandum of Understanding







- No Formally Documented and Approved IT Security Policies and Procedures
- ISO does not report to the Agency Head
- Agency Head not formally designating System Owners, System Owners not designating Data Owners and/or System Admins
- Not documenting how the impacts resulting from a compromise of data confidentiality, integrity, or availability were determined



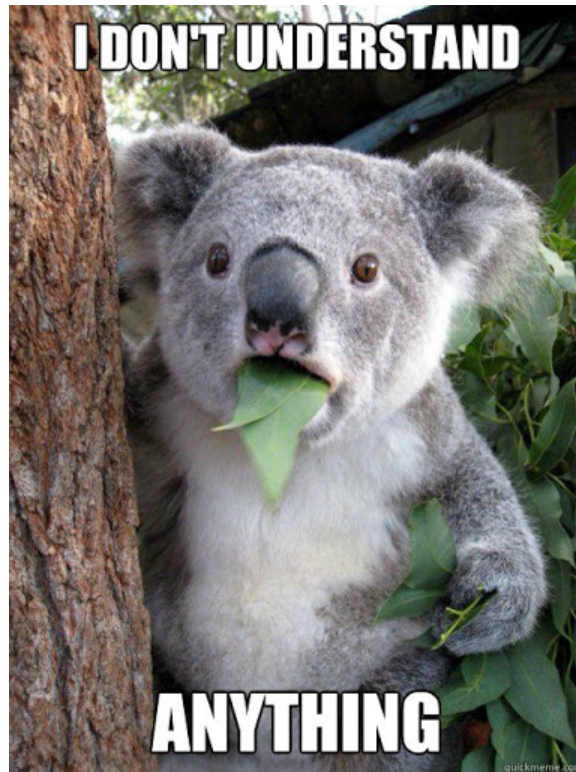
- Account Management
  - Inappropriate privileges, separation of duties
  - Not Disabling Inactive Accounts
  - Not using a 42-day password change frequency for sensitive system authenticators or for Admin accounts
  
- Not using Two-Factor Authentication
  - When accessing sensitive systems over the Internet
  - When using a network connection to access development environments or perform administrative functions on servers or multi-user systems



- Hosting agreements do not contain current information security terms and conditions or are inappropriate for type of service
- Limited review and analysis of audit logs
- Few approved Security Exceptions on file for known control failures







- Identifies the in-scope sensitive IT systems
- Audit cycle is three-years
- Deliverable = One Audit Report per cycle covering the in-scope systems
- Total charge is split into three installment payments



- Every two-years, Planning and Budget uses the sensitive systems in Archer to determine funding and charges for Audit Services
  
- Funding and charges may be adjusted by DPB during the term of the three-year MOU



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ Risk-Based Audits
- ❖ Benefits from Using the Service
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding





Contact me at (804) 416-5174

or

[Mark.McCreary@VITA.VIRGINIA.GOV](mailto:Mark.McCreary@VITA.VIRGINIA.GOV)



## Be like DARTH VADER



- Wears a mask
- Doesn't visit his son and daughter
- Socially and emotionally distant
- Follows orders



# Web Server Vulnerabilities and Remediation



## WEB SERVER VULNERABILITIES LEAD TO WEB SERVER COMPROMISE

The Commonwealth has suffered eleven P1 incidents in 2020

Six incidents were compromised web servers due to vulnerable software

The average time for resolution and restoration of services is 26 days

The total number of days of incident response activities related to P1 server incidents for 2020 stands at 158 (58% of the calendar days)

For each incident the critical files required to restore service only existed on the compromised server



## TRENDS IN WEB SERVER COMPROMISES

The current popular targets for compromising web servers are Content Management Systems (CMS) and the supporting libraries (PHP and Telerik)

Additional avenues of web server compromise include code vulnerabilities, encryption errors, encryption vulnerabilities, and site configuration issues.

Old school attacks still target the Remote Desktop Protocol (RDP) service if exposed to the Internet



## WEB SERVERS REQUIRE CONSTANT MONITORING AND MAINTENANCE

The last quarterly web service vulnerability scan indicated 550 unresolved High vulnerabilities on COV websites

The last quarterly web service vulnerability scan indicated 2460 unresolved Medium vulnerabilities on COV websites

A malicious individual only requires one vulnerability to compromise a web server and take complete control



## WEB SERVERS REQUIRE CONSTANT MONITORING AND MAINTENANCE

Review the monthly Nessus scans for operating system and supporting library vulnerabilities

Review the quarterly Acunetix web application vulnerability scans for vulnerabilities with the web services and supporting libraries

Work with the agency system admins and developers to update website software and support libraries



## RECOMMENDATIONS TO MITIGATE THE CHANCE OF SERVER COMPROMISE

Stop using end-of-life software

Ensure that agency system admins and developers consistently review vendor publications for vulnerability announcements and software updates

Work with the agency system admins and developers to update website software and support libraries





## RECOMMENDATIONS TO MITIGATE THE CHANCE OF SERVER COMPROMISE

Contact the CAM and BRM to escalate software updates from Unisys for server operating system software

Ensure all website content is stored in a location other than the production web server

Establish a test and development environment to test website changes prior to promotion to production



## COMPROMISED SERVER CONTAINMENT AND REMEDIATION

Once a web server is compromised it becomes a threat to the Commonwealth

The two remediation options available to the agency are:

Take the server offline and build a replacement server

Place the server behind the Enterprise Web Application Firewall and build a replacement server



## COMPROMISED SERVER CONTAINMENT AND REMEDIATION

The reconstruction of the web server will be complicated if:

The source code for the web service or the supporting configuration files only exist on the compromised server

The web service uses end-of-life software that is not compatible with the current, vendor supported version

No documentation exists that stipulates the website architecture or the requirements to make the website function



# QUESTIONS



# Cybersecurity Awareness Month

# DO YOUR PART. #BECYBERSMART

October is  
Cybersecurity  
Awareness Month



# CYBERSECURITY AWARENESS MONTH 2020



**DO YOUR PART.**  
**#BECYBERSMART**

NATIONAL  
**CYBERSECURITY**  
ALLIANCE



## 2020 THEME

Do Your Part. #BeCyberSmart

Helping to empower individuals and organizations to own their role in protecting their part of cyberspace.



## WEEKLY THEMES

October 1 and 2: Official NCSAM Kick-off

Week of October 5 (Week 1): If You Connect It, Protect It

Week of October 12 (Week 2): Securing Devices at Home and Work

Week of October 19 (Week 3): Securing Internet-Connected Devices in Healthcare

Week of October 26 (Week 4): The Future of Connected Devices

## RESOURCES

<https://staysafeonline.org/cybersecurity-awareness-month/theme/>

<https://www.vita.virginia.gov/commonwealth-security/awareness-toolkit/agency-awareness/>

<https://www.cisa.gov/national-cyber-security-awareness-month>

<https://www.dhs.gov/publication/dhs-speaker-request-form>

<https://www.knowbe4.com/ncsam-resource-kit>

<https://www.cisa.gov/cisa-cybersecurity-resources>

<https://www.cisa.gov/national-cybersecurity-awareness-month-sample-social-media-posts-and-graphics>

[Mike Watson's intro to Cybersecurity Awareness Month 2020 video](#)

# Upcoming Events

## NOVEMBER 2020 ISOAG

November ISOAG Meeting  
November 4 from 1 to 4  
Webex

- David Ihrie / Center for Innovative Technologies
- Eric Paxton / Risk Based Security
- Brandon Lapetina / Varonis

## DECEMBER 2020 ISOAG

December ISOAG Meeting  
December 2 from 1 to 4  
Webex

- Benjamin Gilbert / Cyber Security & Infrastructure Agency (CISA)
- Michale P. French / Federal Bureau of Investigation
- Chris Jensen / Tenable

## IS ORIENTATION

IS Orientation

December 9 at 1pm

Presenter: Marlon Cole

Registration Link:

<https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e376010e5a8341c8fd6133acaaddeaf2d>

# ADJOURN

## THANK YOU FOR ATTENDING

