Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

Oct. 9, 2019

ISOAG Oct. 9, 2019 - Agenda

- Welcome and Opening Remarks - Mike Watson
- Recognition of CTF winner - Mike Watson
- Risk management and Archer Updates - Jon Smith and Mark Martens
- Results of Second Annual Report - Ed
- Upcoming Changes to Policy - Marlon
- 2018 Annual Report - Joy
- ECOS Applications in Archer - Debi
- Threat Update - Kathy/Dean
- New Security Services- Stephanie
- Vulnerability Scanning Update - Bill/Kyle
- Audit Services Update - Mark McCreary
- ISO Services Update - Wes Kleene

Risk management update

Presenters

Jonathan Smith and Mark Martens

ISOAG

Oct. 9, 2019

Agenda

- Incident Response Exercise
- National Cybersecurity Review (NCSR)
- Risk Management Standard
- Quantitative Risk Analysis

Incident response exercise

- Oct. 29, 2019
- MSI tabletop exercise
- Participants:
  - Agencies (voluntary)
  - VITA
  - Suppliers
- Hot wash - Oct. 30, 2019

NCSR

- Self assessment of agency security program maturity
- CSRM has received the 2019 NCSR from MSISAC
- Will be available via Archer after testing and push to production
- Deadline: Dec. 15, 2019
- NCSR completion is a datapoint for the annual report on information security

Risk management standard

- Annual update to SEC 520
- Updates may include:
  - Update to reporting methods, to include the ability to utilize an Archer questionnaire to perform IT risk assessments
  - Additional required fields to support the new quantitative risk analysis methodology
  - Will be posted to ORCA for online review and comment

Quantitative analysis of risk

- CSRM is developing a methodology for quantitatively assessing the information risks to the commonwealth IT systems, data, and agencies
- Quantitative risk analysis enhances leadership ability to make informed risk based decisions
  - Investments
  - Security enhancements
  - Cyberliability insurance

Quantitative analysis of risk

- CSRM is developing the methodology with the risk management committee to ensure that we have agency input
- Based on the factor analysis or information risk (FAIR) framework
- Initially based on existing inputs from application, dataset inventories and BIA's (agency reported)
- Additional inputs will be added to tune the model

Quantitative analysis of risk

- Secretary of Administration has expressed interest in the quantitative risk analysis
  - Potential impacts to commonwealth bond rating due to an incident
  - Investment decisions
  - Reputational risks (under development)
    - Number of users impacted

Quantitative versus qualitative

- Qualitative
  - High impact
- Quantitative
  - X million dollars of impact

If you are an executive faced with a decision on procuring a system, hardening a system or insuring a system, which value would you want?

“High” vs $20,000,000

Quantitative data on loss events

- Ponemon Institute
  - Annual loss expectancy by profile
- Willis Towers Watson
  - Costs per record by industry sector
- Verizon DBIR
  - 16% of data breaches involve public sector entities
- Commonwealth institutional knowledge
  - Incident response gut check on costs

Availability of data

- Ponemon Institute and Verizon both publish publically available reports on cybersecurity loss events and trends
- Willis Towers Watson is a multinational risk management, insurance brokerage and advisory company that has shared similar data with the commonwealth in the past

Quantifying risk with X and Y

- X = Number of target records
- Y = Cost per record
- CSRM derives X from your data set inventory
- CSRM is investigating sources of “Y” (Ponemon, Willis Towers Watson, etc.)

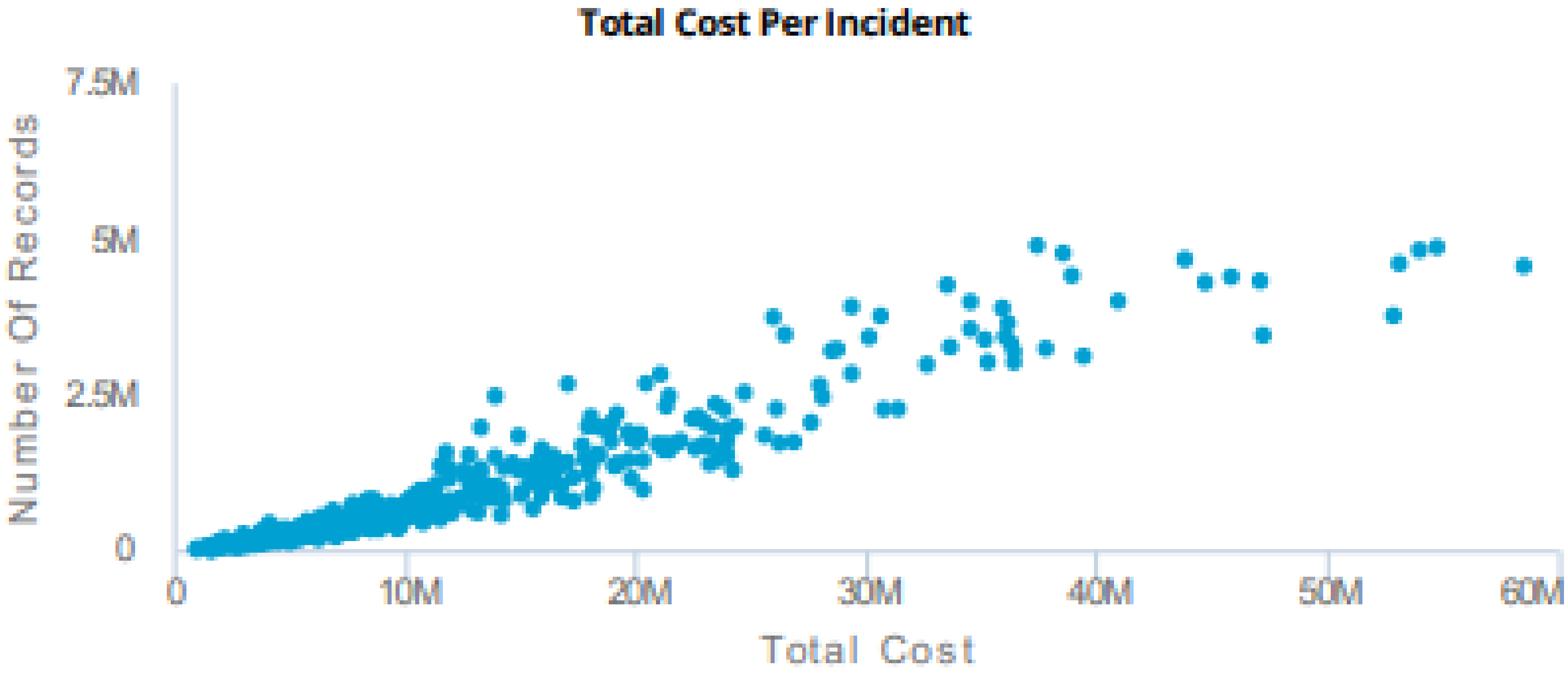
Calculating inherent risk

- Inherent risk = $ per record x record #
- Residual risk = Inherent risk x annualized loss expectancy of a system of that profile
- Other factors for residual risk
  - CIS top 20 control weaknesses
  - Insurance
  - Contracts

Tuning the model

- Currently running several models in parallel using aforementioned sources of data
- Soliciting additional sources of data

Costs per record decline with count



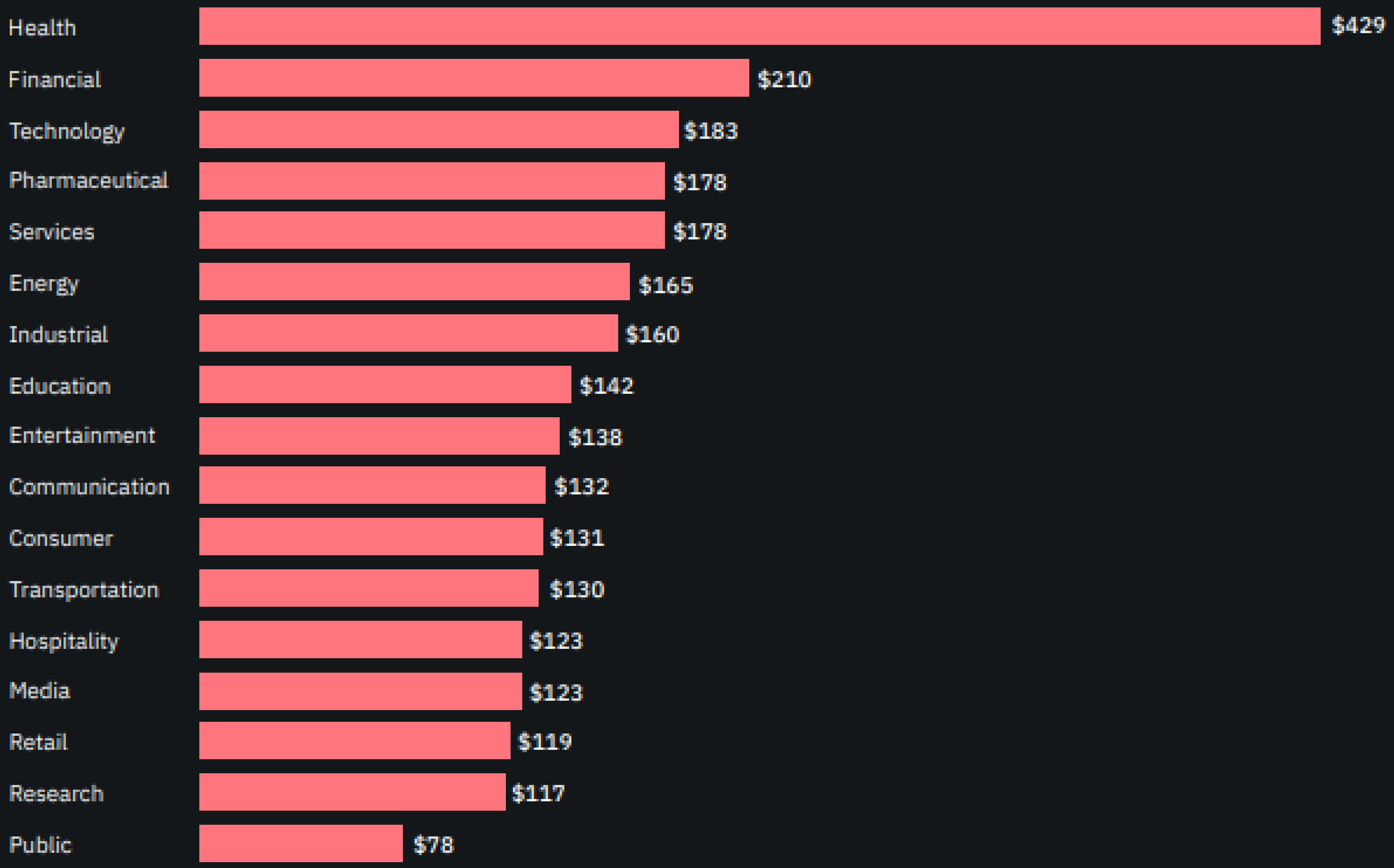
Costs by sector

- Not all systems were created equally and costs vary by industry sector
- Public sector typically has lower costs per record and incident because we are less susceptible to secondary costs such as the loss of customers

Figure 11:

Average cost per record by industry sector

Measured in US$



Primary and secondary costs

- The Ponemon Institute gives the most comprehensive costs
- They include primary and secondary costs in their data

Four cost centers

- Detection and escalation
- Notification costs
- Post data breach response
- Lost business cost
  - In the public sector this is not always as evident. Typically users avoid systems and automation associated with a loss event and these costs are seen through increased use of manual processes and reputational loss.

Detection and escalation

- Activities to detect and report a breach Examples: -
  - – Forensic and investigative activities
  - – Emails, letters, outbound telephone calls, or general notice to data subjects that their personal information was lost or stolen –
  - – Communication with regulators
  - – Determination of all regulatory requirements, engagement of outside experts

Notification costs

- Activities required to notify individuals who had data compromised in the breach (data subjects) as regulatory activities and communications.
    - Examples:
        - Help desk activities / inbound communications
        - Credit report monitoring and identity protection services
        - Issuing new accounts
        - Legal expenditures

Post data breach response

- Processes set up to help individuals or customers affected by the breach to communicate with the company, as well as costs associated with redress activities and reparation with data subjects and regulators. Examples:
  - Help desk activities / inbound communications - credit report monitoring and identity protection services
  - Legal expenditures
  - Regulatory interventions (fines)

Lost business cost

- Activities associated with the cost of lost business, including customer turnover, business disruption, and system downtime.
  - Examples:
    - Cost of business disruption and revenue losses from system downtime
    - Cost of lost customers and acquiring new customers (customer turnover)
    - Reputation losses and diminished goodwill

CIS top 20 critical controls

- These controls are mapped in Archer using the NIST Framework.
- If you have a finding associated with a SEC501/525 policy, that is automatically mapped in Archer to the associated base, foundation or organization control.
- Each CIS group is given a weight and used in calculating the residual risk of a system. Base, foundation and organization are weighted 3,2,1 respectively.
- Remediating and closing your CIS findings will improve your risk scores.

Conclusion

- Methodology is still in development, there will be more to follow
- Accuracy of agency maintained application/dataset inventories and BIA’s will impact the accuracy of the analysis
- Remediation of findings will reduce your risk scores

Second Annual Report

Ed Miller

VITA Virginia Information Technologies Agency

Second Annual Report

Presenter

Ed Miller

ISOAG

Oct. 9, 2019

Code of Virginia § 2.2-2009(C)

“the CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures.’

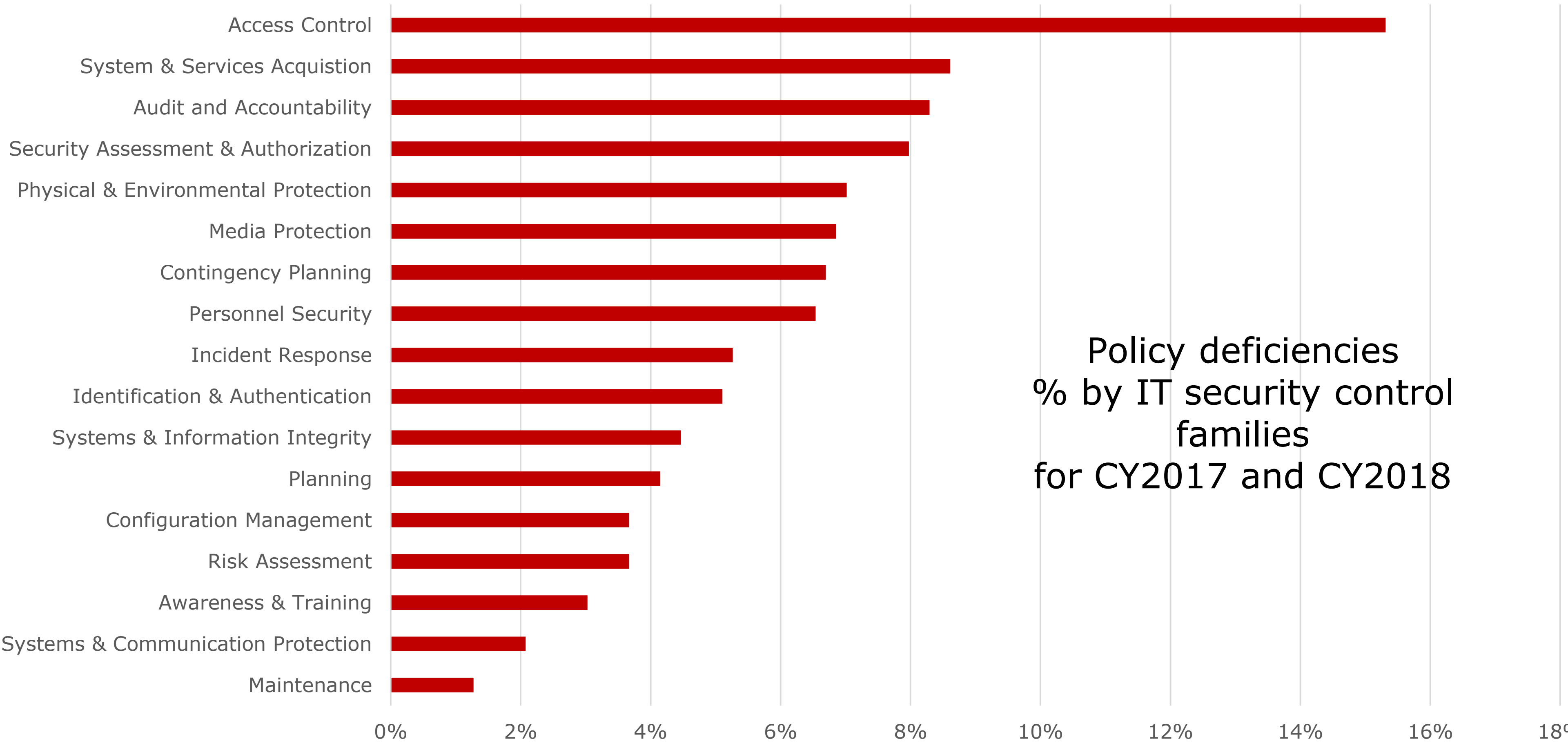
Code of Virginia § 2.2-2009(C)

“Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairman of the House Committee on Appropriations and the Senate Committee on Finance. Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities.”

Methodology

- Review of eGRC (Archer findings data)
- Results of NCSR (National Cybersecurity Rev)
- 2018 Annual Report (the other report)
- IT security incidents (Archer incidents)

Policy related findings (audits and RAs)



Policy deficiencies
% by IT security control
families
for CY2017 and CY2018

Policy related findings (audits and RAs)

- We also looked at what agencies were reporting "policy" related findings
- We also looked at what agencies were not reporting any findings
- Why no findings?

Policy related findings (ORIs)

- We analyzed the type of ORI findings and why

- EOL, or unsupported, hardware and software was the main type of ORI finding reported

National Cybersecurity Review (NCSR)

- How did agencies self-assess how they where doing with “policies”?
- How does that compare with our peer states?
- How does the NCSR self-assessment scoring compare with the COV 2018 report card scoring?

National Cybersecurity Review (NCSR)

- How did agencies self-assess how they where doing with “policies”?
- How does that compare with our peer states?
- How does the NCSR self-assessment scoring compare with the COV 2018 report card scoring?

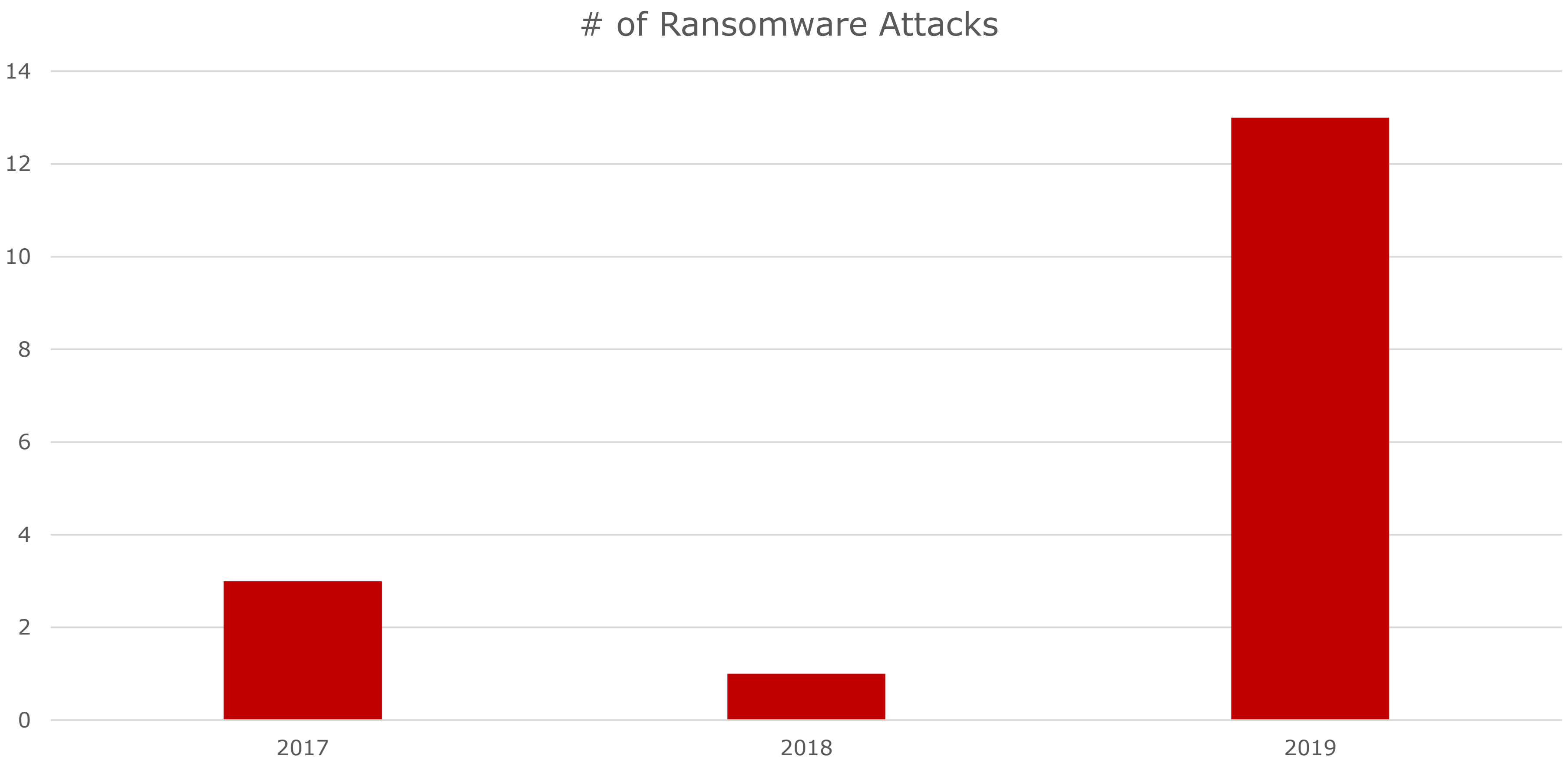
Analysis of cyber incidents

- What were the high priority incidents reports in CY2017 and CY2018?
- What agencies were reporting these types of incidents?
- What data breaches occurred as a result of these incidents?

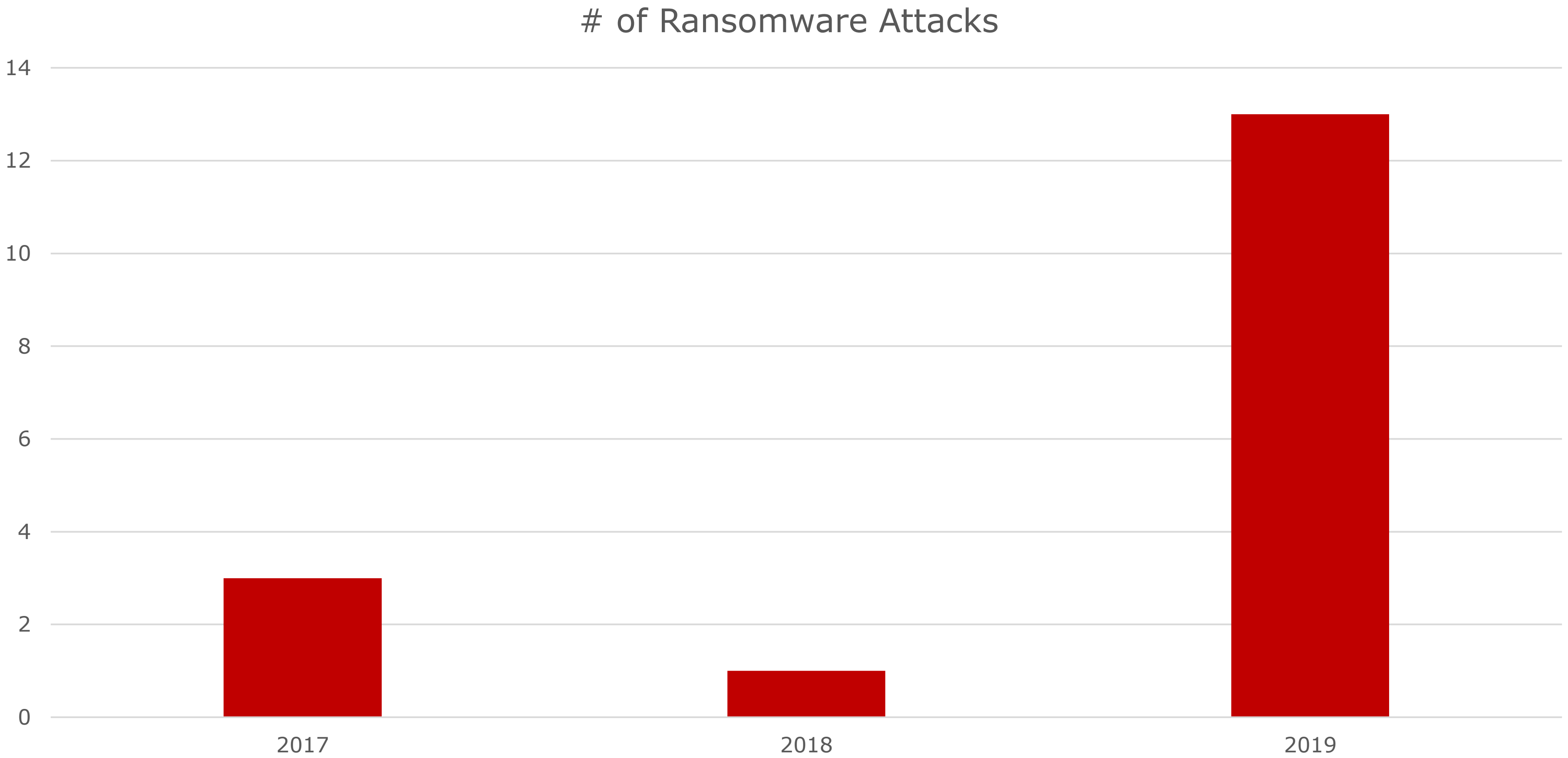
Analysis of cyber incidents

- What types of incidents were most likely to cause a breach?
  - Malware
  - Unauthorized access
    - Social engineering
    - Phishing attacks

Ransomware



Ransomware



Final report

- In final review now
- The end
- QUESTIONS?

Recent and Upcoming Changes to Policies, Standards and Guidelines

Marlon Cole
CSRM Analyst
Commonwealth Security and Risk Management

ISOAG
Oct. 9, 2019

Updated security standards

- SEC501: IT Information Security Standard
- SEC525: Hosted Environment Security Standard
- SEC502: Information Technology Security Audit Standard
- SEC520: IT Risk Management Standard
- SEC514: Removal of Commonwealth Data From Electronic Media Standard

Changes to SEC501 and SEC525

- Section 2.4 now reads "The agency Information Security Officer (ISO) ~~should~~ SHALL report to the agency head"

- Added a new awareness and training control (AT-2 COV)

- Added a new planning control (PL-4-COV)

Changes to SEC502

- Internal audits, as recognized by the Office of the State Inspector General (OSIG), must be based on Red Book (The Institute of Internal Auditors (IIA) framework for the professional practice of internal auditing.

- When performing an external audit, agencies must use an acceptable auditing framework (i.e. Generally Accepted Government Auditing standards (GAGAS) or “Yellow Book”; The use of any other audit standard or framework must be approved by Commonwealth Security and Risk Management (CSRM) prior to the start of the audit.

Changes to SEC520

- Within the Business Impact Analysis section, were two updated requirements.
  - ➢ Mission essential functions
  - ➢ Primary business functions

Changes to SEC514

- Added additional and new information to the Appendix A-Methods for Removal of Commonwealth Data Section.

- To see additional changes to the standards please visit https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

Upcoming changes to SEC509

- IT logical access control guideline will define logical access requirements in the following three areas:
  - Account management
  - Password management
  - Remote access

Upcoming changes to SEC511

- IT standard use of non-commonwealth computing devices to telework will provide further guidance on how to protect COV information technology assets and the data they process and store while assisting to meet the COV’s teleworking objectives.

Upcoming changes to SEC519

- IT information security policy will provide the security framework that each agency will use to establish and maintain their information security program.

Virginia Information Technologies Agency

2018 Commonwealth of Virginia Information Security Report

Joy Young
IT Security Analyst

ISOAG
Oct. 9, 2019

Significant turnover in the ISO community in 2018

ISO resources are available online, including standards and policy. CSRM offers quarterly ISO training.

Major changes to infrastructure services

CSRM is monitoring the risk introduced with the change, including reviewing system security plans and ensuring audits of supplier IT systems

Standards were updated to address changing threats to information security

IT information security policy and standards are monitored and updates are made where needed keep COV data safe

Agencies using centralized ISO services and audit services saw improved metrics

These services assisted agencies in creating BIAs, risk assessments, and IT security audits to further improve their information security programs

Incident response playbook was adjusted with new VITA service model

CSIRT continues to adjust the incident response playbook as new vendors are added to the program to promote preparedness, consistency, and effectiveness

Virginia colleges and universities continue to be targets of cyberattacks

CSRM recommends additional governance is established to promote information security at Virginia’s colleges and universities

Agency audit program compliance metrics continue to improve

VITA audit services is a driver in the improvements in overall agency audit program compliance

Risk management program results improve

Metrics improved with additional focus on risk management and ISO services provided to agencies

Survey results indicate strengths and opportunities

Agencies should use the survey results from the Nationwide Cybersecurity Review (NCSR) to prioritize agency security efforts

Agencies were a target of a sextortion email campaign

CSRM issues advisories and recommends training to help agencies combat these tactics

New security controls for email access

CSRM worked with the messaging supplier to incorporate security controls. As new attack types developed, CSRIT will work with vendors to block these attacks.

Vulnerability scanning results continue to show progress

Agencies are addressing the vulnerabilities found in the scans. CSRM plans to add application level scanning to build on the successes of the scanning program

Identity and access management (IAM) tools were made available

CSRM is developing additional standards to help improve IAM

Questions?

Email : CommonwealthSecurity@VITA.Virginia.Gov

ISO council

If you are interested in contributing to the strategic direction for commonwealth information security and privacy initiatives?

Consider joining the

ISO council

Contact CSRM @
Commonwealthsecurity@vita.virginia.gov

Virginia Information Technologies Agency

Enterprise Cloud Oversight Services: Exceptions

Debi Smith
Cloud Security Architect

ISOAG
Oct. 9, 2019

ECOS – exceptions

- The ECOS approval…finally!!!
- Now…what is next?
- Cloud T’s and C’s and Exceptions

ECOS – exceptions

- Agency is responsible for submitting any security exceptions within **five** business days after approval…

- It is very important that the exceptions are submitted in a timely fashion
  - Allows time for review
  - Allows time for any modifications
  - Allows time for all signatures
  - Prevents delays in contract signing

ECOS – exceptions

- The exception submission process…
  - Setup your application in Archer
    - (use application name–AGENCY i.e., Splunk Cloud-DSS)
  - Attach that application to the products and services
  - Create new exception
  - Attach your exception for the application to the application you just created
  - Submit for review

ECOS – exceptions

- Link on how to submit security exceptions in Archer…

- https://vccc.service-now.com/vita?id=vita_kb_article&sys_id=62cc2e6bdbd73740f483750e0f961996

Questions

Contact: Debi Smith

Debi.Smith@vita.virginia.gov

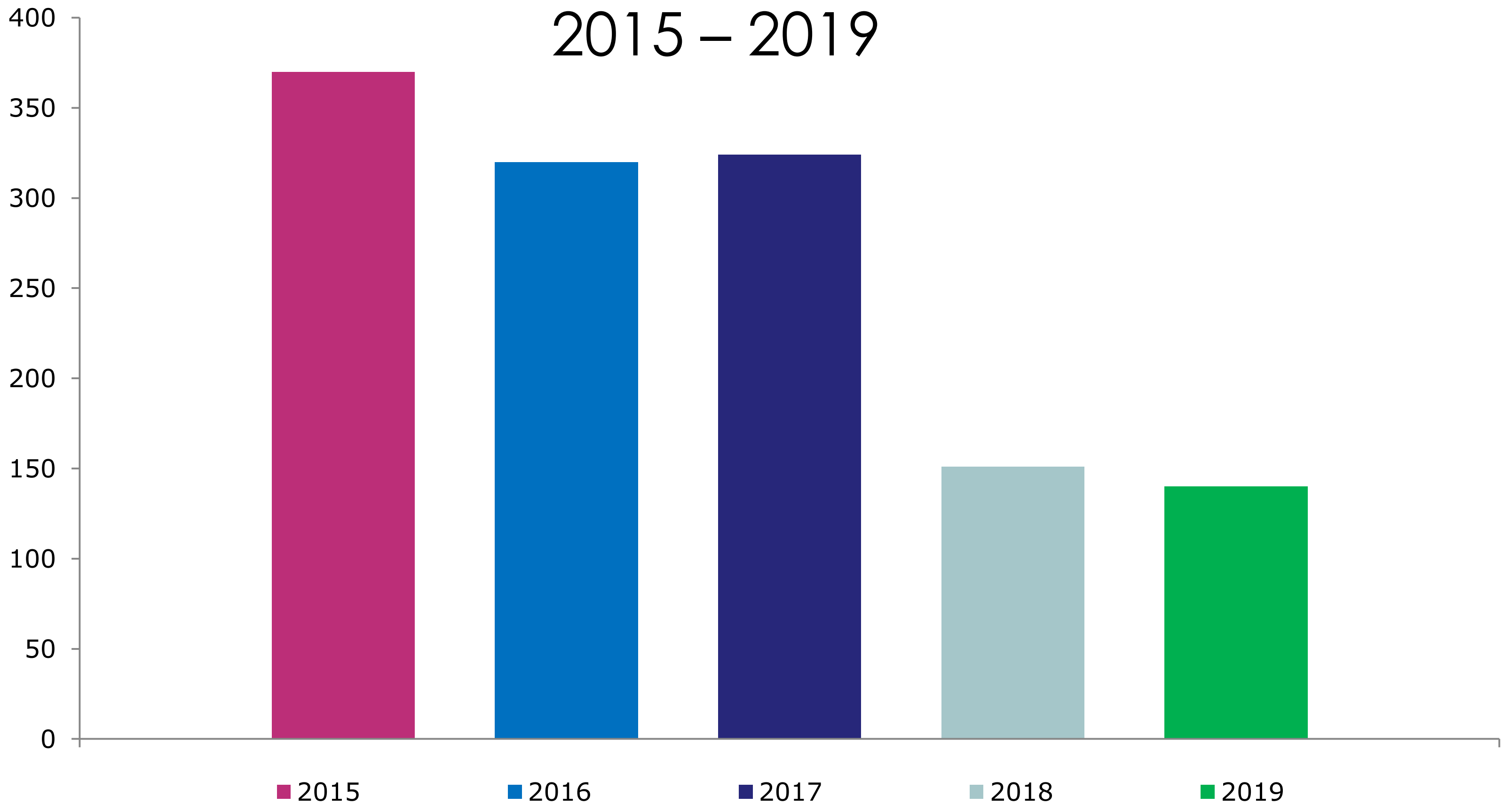
VITA Virginia Information Technologies Agency

Cyber Security Incident Management

Kathy Bortle, CISSP, GCIH, GCIA, GWAPT, GMOB, GPEN, GCFE, PMP
Incident Response Specialist

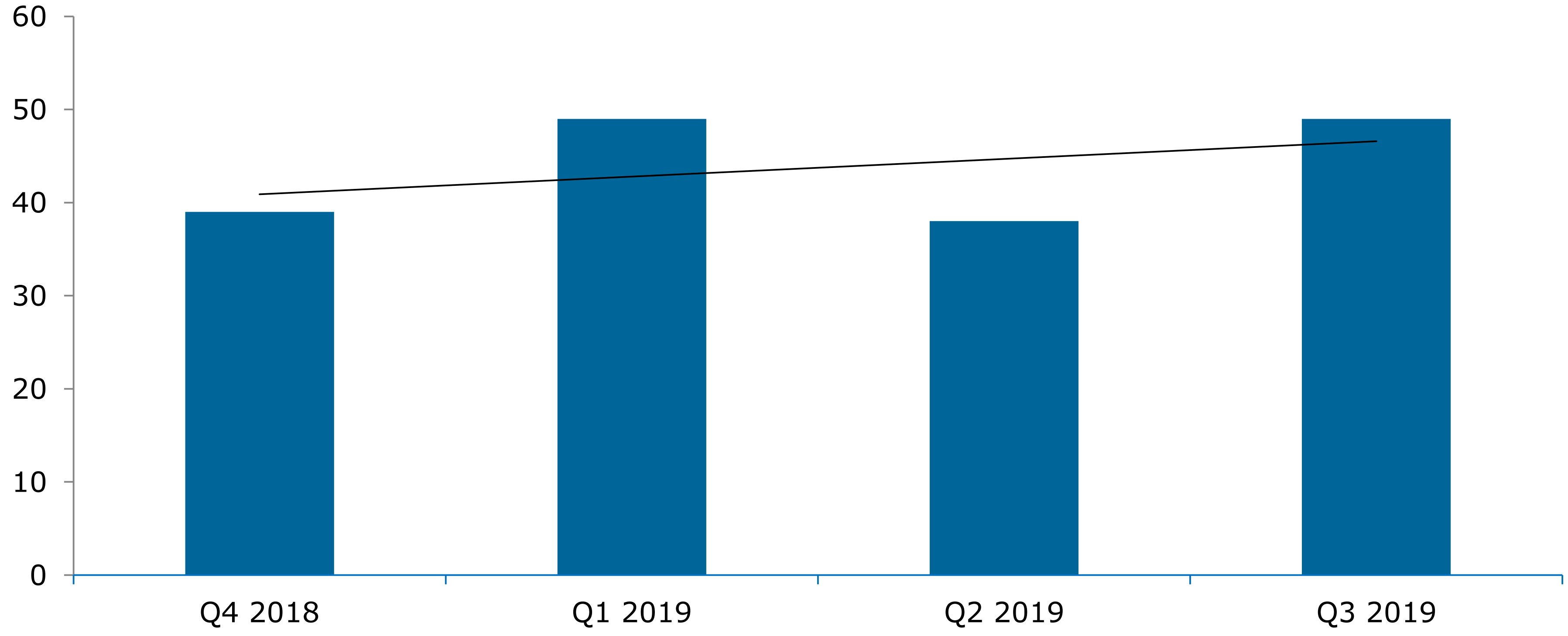
Oct. 9, 2019

Cyber security incidents by year

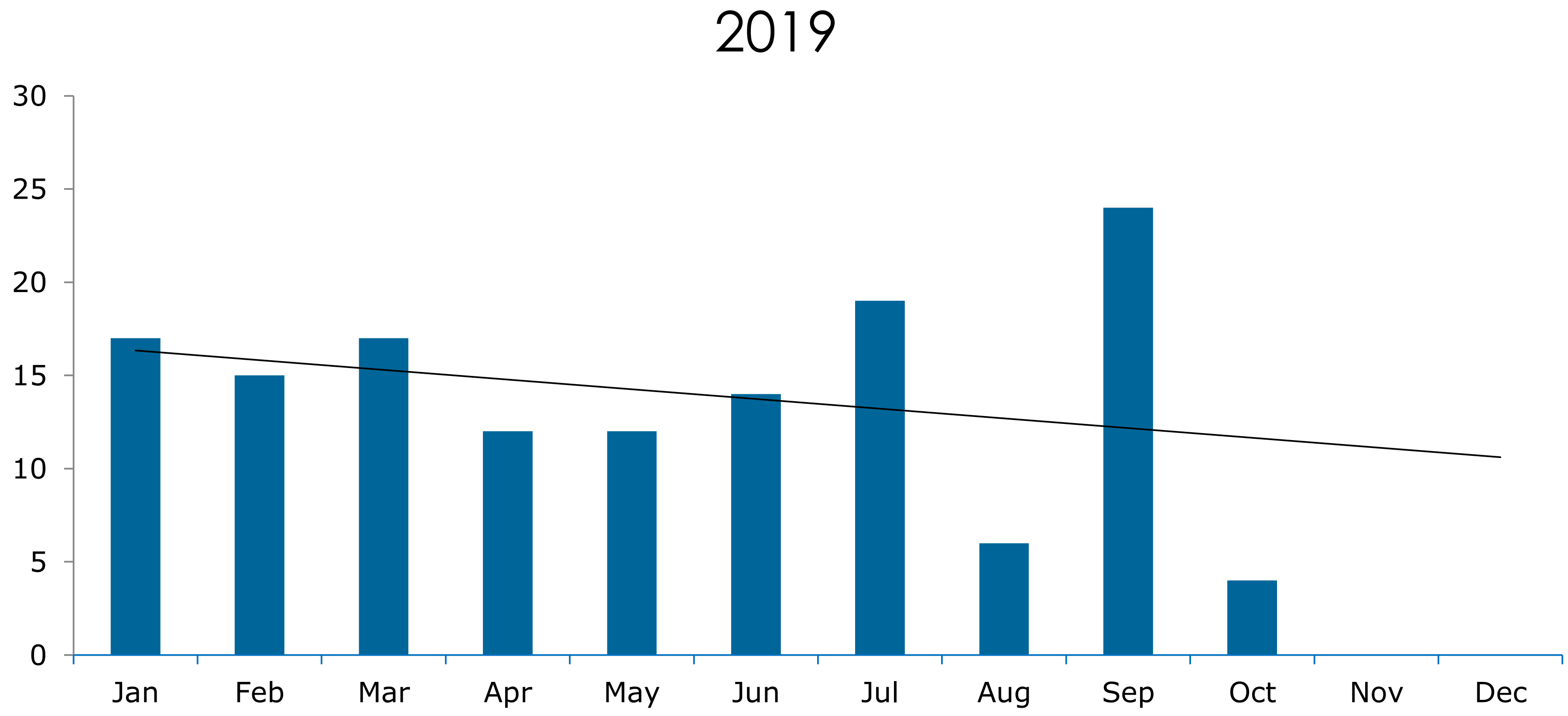


Trend of Cybersecurity incidents by quarter

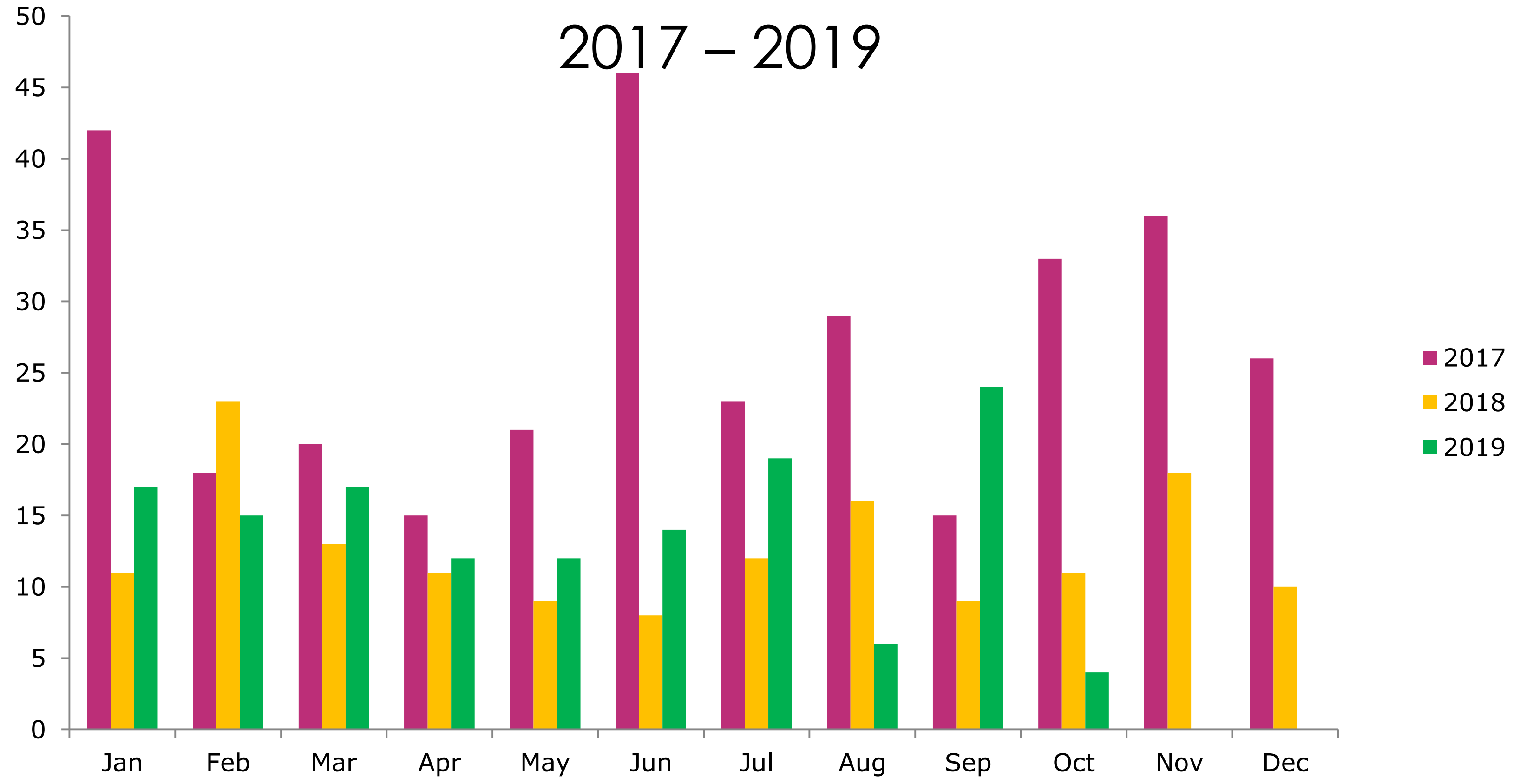
Q4 2018 – Q3 2019



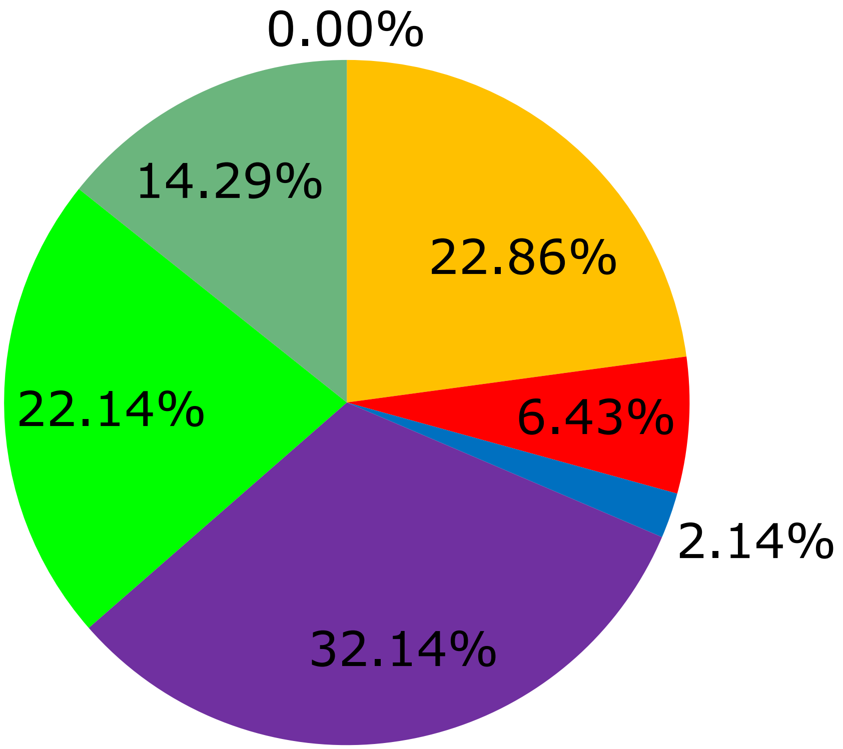
Trend of cybersecurity incidents



Cybersecurity incidents by month



Security incidents by category 2019



■ Denial of Service

🟨 Malware

🟥 Inappropriate Use

🟦 Social Engineering

🟪 Informatino Disclosure

🟩 Physical Loss

🟩 Unauthorized Access

Total Incidents for COV = 140
Estimated Cleanup Costs $ 84,000

How to mitigate information disclosure

- Verify recipient and their address before sending the information (both mail and email)
- Use email encryption for all sensitive data
- When sending information via mail, verify that the correct information is inserted into the package before sending

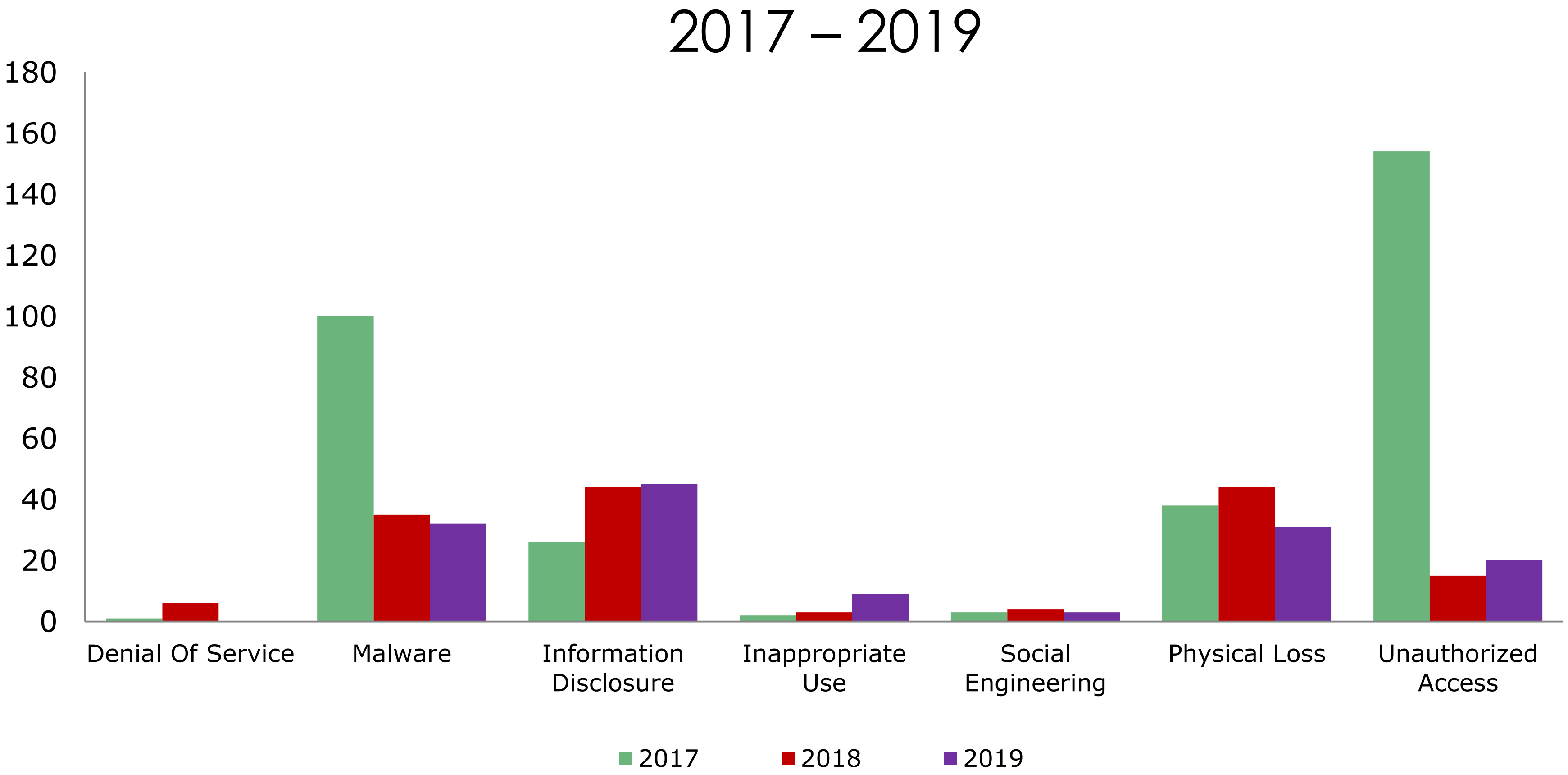
How to mitigate malware infections

- Don’t install any unnecessary software on devices
- Keep virus protection up to date
- Login to the COV network at least every two weeks so patches can be applied to your device
- Patch systems as soon as possible after appropriate testing

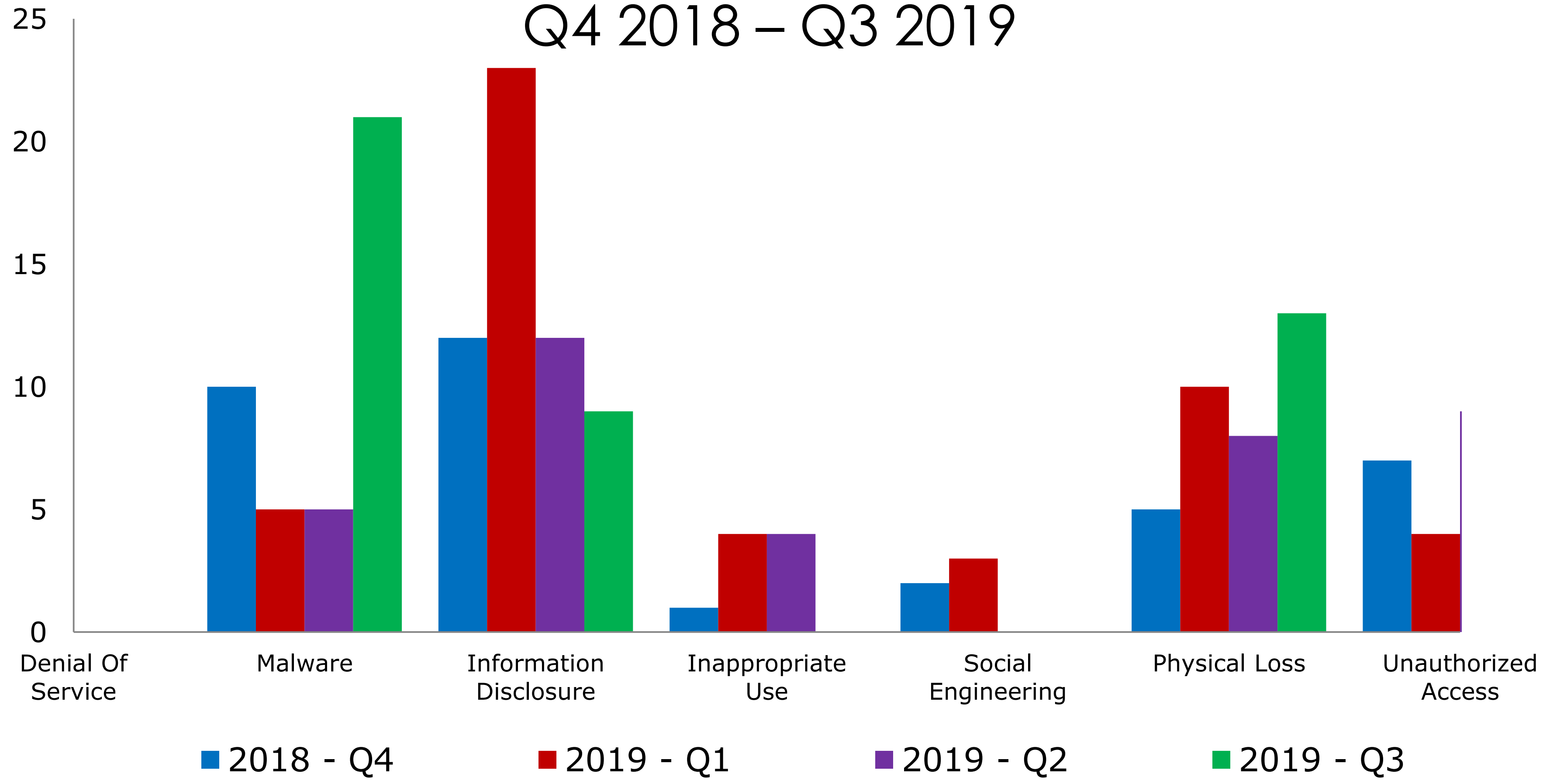
How to mitigate physical loss

- Encrypt data on all devices (laptops, tablets, cell phones) to prevent data loss if a device is lost or stolen
- When traveling with your devices, keep them with you or lock them up in the car or hotel safe. Keep them out of sight.

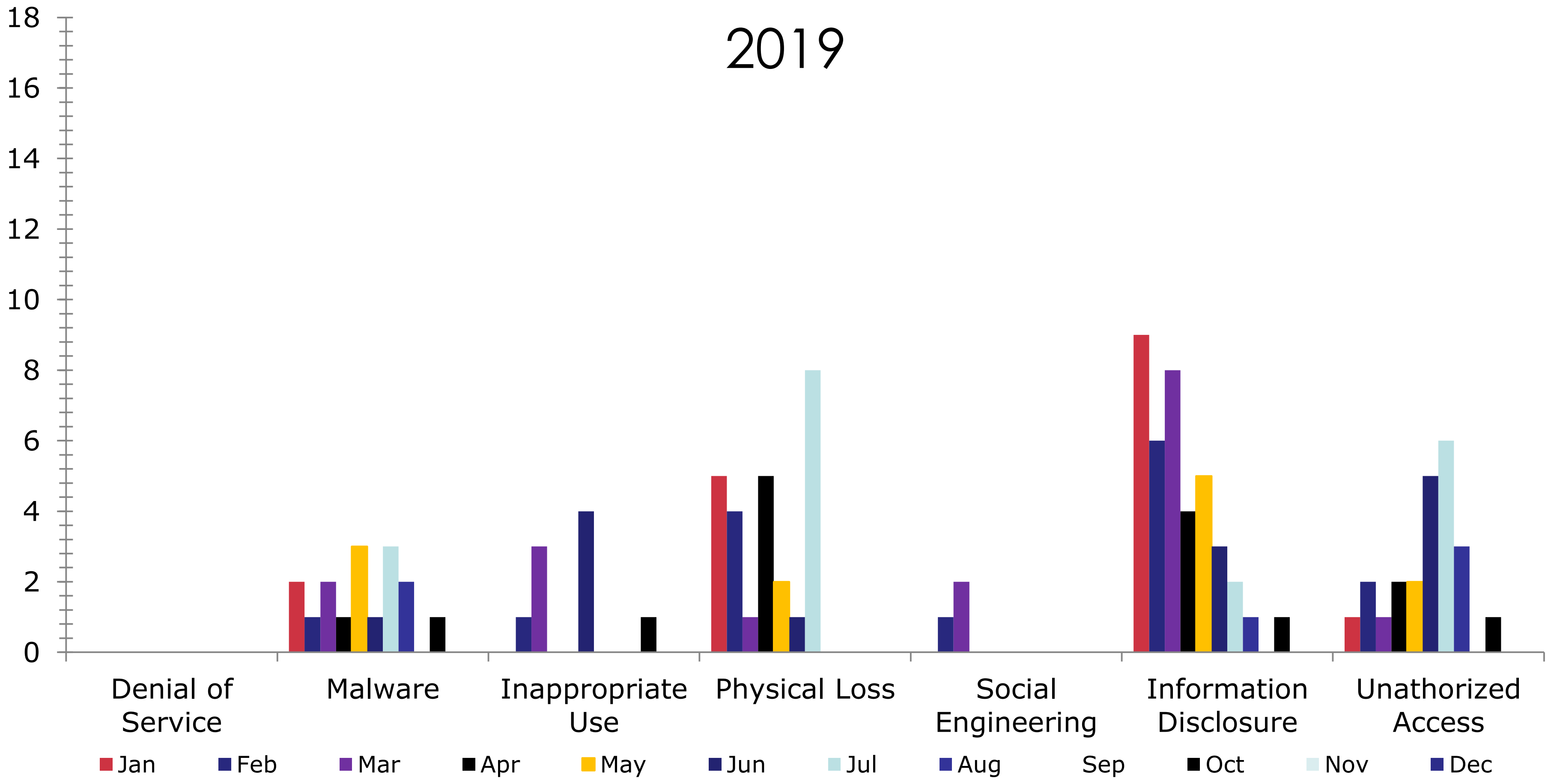
Cybersecurity incident trends by category



Cybersecurity incident trends by category



CoVA Cybersecurity incidents by category



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

VITA Virginia Information Technologies Agency

Web Application Vulnerability Scanning Update

VITA

Commonwealth Security and Risk Management

Oct. 9, 2019

COV web application vulnerability scanning program

- History
  - Evolved from incident scans in 2009 to paid service to legislative support for all systems in FY2017
- Status
  - The trend fluctuates and is trending down in severity, but appears to be flattening out
- Future
  - Integrating internal sensitive applications into the program
  - Reporting repeat high alerts to the risk management team
- How you can help
  - Review reports and remediate, ask for assistance if needed

Alert trends and alert reduction

- We scan 1500 unique URLs per quarter
  - Alerts are being remediated across the board, but….
  - Repeat high and medium alerts are very visible
  - Low's are not always low risk
- Application developers and web masters should strive for a culture that creates secure resilient applications to reduce alerts

Thank you and welcome

- To agencies for cooperating with the program. Including, whitelisting and remediation!
- Tyrone Williams
  - Great help, shifted to the governance group
- Welcome to Kyle Linsday
  - Recent JMU grad
  - Interned with the incident team
  - Strong networking and skills

Internal sensitive applications

- 2020 goal to increase our coverage on internal sensitive browser applications
  - – Discovery via Tenable.SC
  - – URL’s in Archer
    - Sensitive applications with a browser interface must include the URL in Archer
  - – Independents and higher education
    - Archer update

Survey

- 2020 survey
  - Would agencies like to run their own scans?
    - We would still run quarterly scans, but agencies could rerun scans and test alerts.
  - Would agencies like to run their own reports?
    - We would still import alerts into Archer
  - Would agencies like the ability to scan development systems and test systems?

Repeat high and medium alerts

- We will report high and medium alerts to the CSRM risk management group on a periodic basis
- The risk management people will alert agencies based on the severity of the alerts and sensitivity of the applications

Summary

- Read your quarterly reports. Test and remediate vulnerabilities. Review each alert. Ask for help.
- Look out for the survey
- Remediate high and medium vulnerabilities in a timely manner

Questions?

FY20 New and Enhanced Security Services Update
ISOAG Meeting

VITA Bill Stewart
Atos - Darrell Raymond

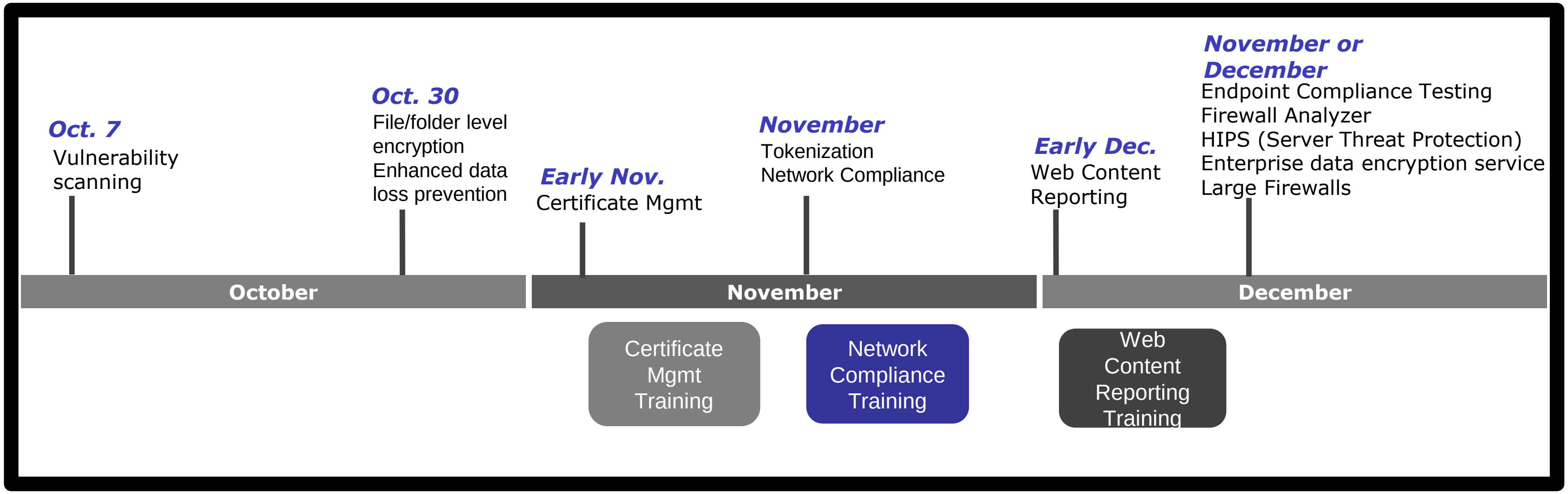
Oct. 9, 2019

Agenda

- New and Enhanced Services Rollout Schedule Update
- Network Compliance (NAC)
- Enhanced Data Loss Prevention Service
- Endpoint File/Folder Level Encryption

FY20 new and enhanced security services

VITA and it's managed security supplier, Atos, are rolling out new and enhanced security services to enhance the security of the entire COV environment and provide agencies with more choice.



Oct. 7
Vulnerability scanning

Oct. 30
File/folder level encryption
Enhanced data loss prevention

Early Nov.
Certificate Mgmt

November
Tokenization
Network Compliance

Early Dec.
Web Content Reporting

November or December
Endpoint Compliance Testing
Firewall Analyzer
HIPS (Server Threat Protection)
Enterprise data encryption service
Large Firewalls

October | **November** | **December**

Certificate Mgmt Training

Network Compliance Training

Web Content Reporting Training

*Schedule is tentative and subject to changes

FY20 new and enhanced security services

New/Enhanced Service	Catalog or Enterprise Service	Expected Launch	Training?	Rollout strategy
Application and source code security	Catalog	Launched Sept. 4	Provided after purchase	Catalog addition
Vulnerability Scanning and Management	Enterprise	Agency rollouts begin Oct. 7		Rolling release
Endpoint file/folder level encryption service	Catalog	Oct. 30	Job aid	Catalog addition
Enhanced Data Loss Prevention service	Catalog	Oct. 30		Catalog addition
Certificate Management	Enterprise	Early November	Yes – Early November	All agencies
Network Compliance	Enterprise	Mid-November	Yes – Mid-November	Rolling releases
Tokenization	Catalog	November	Provided after purchase	
Web Content Reporting	Enterprise	Early December	Yes – Early December	All agencies
Endpoint Compliance Testing	Enterprise	November or December		Rolling releases
Firewall Analyzer	Catalog	November or December		Catalog addition
HIPS (Server Threat Protection)	Enterprise	November or December		Rolling releases
Enterprise data encryption service	Catalog	November or December	Provided after purchase	Catalog addition
Large Firewalls	Catalog	November or December		Catalog addition

*Schedule is tentative and subject to changes

Network compliance (NAC)

- **Rollout type:** Enterprise required service
- **Expected launch:** Discovery mode in Mid-November
- **Overview:**

Network compliance monitors the network infrastructure to discover devices as they connect to the network.

Allows VITA and agencies to set policies that establish which devices can connect to the network and the specific behavior the device can have while connected to a network.

Network compliance (NAC)

- **Overview continued:**
  - Enforces VITA’s and agency’s security standards and policies
  - Unsupported devices without an approved exception are not permitted access to the network
  - Devices that do not meet security posture standards are quarantined until remediated
  - Controls the specific behavior devices are allowed to have while connected to the network

Network compliance modes

Discovery mode

- Data collection of all devices connected to network and domain
- Monitor your agencies level of policy compliance
- Preparing for enforcement mode
  - The first phase of discovery mode will confirm devices are known in the CMDB.
  - The second phase of discovery mode will confirm devices meet VITA and agency security postures

Enforcement mode

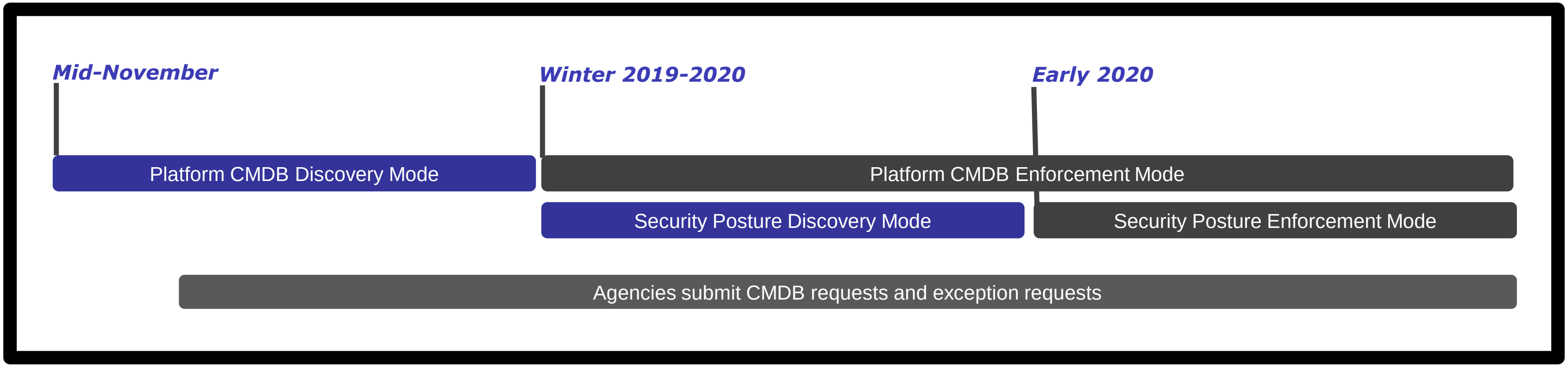
- Pre-connect compliance check to ensure only authorized devices connect to COV networks
- Once the device has passed the pre-connect check the service puts the user on the right network segment according to their role when the service configured for enforcement
- Post-connect compliance check to identify any persistent threats

Network compliance (NAC)

Rollout overview:

Discovery mode has no effect on the agency's network or devices. Agencies will receive reports during discovery mode with devices that need to be remediated.

To remediate, devices will need to be added to the CMDB or receive an exception.


Mid-November
Winter 2019-2020
Early 2020
Platform CMDB Discovery Mode
Platform CMDB Enforcement Mode
Security Posture Discovery Mode
Security Posture Enforcement Mode
Agencies submit CMDB requests and exception requests

Network compliance (NAC)

Training:

- Coming in mid-November
- How to review the reports and remediate out-of-compliance devices

NAC Report information:

- Segment that the device was discovered on
- IP address for the device
- Function of the device (server, workstation, etc.)
- Operating system on the device
- Compliance status

Enhanced data loss prevention service

- **Rollout type:** VITA Service Catalog item
- **Expected launch:** Oct. 29
- **Overview:**
  - Monitors and prevents confidential data loss by controlling how employees use and transfer sensitive data
  - Automatically detects or blocks transmissions containing sensitive data
  - Automatically quarantines messages that may need approval to exit COV network
  - Prevents data loss and leakage when data is modified, copied, pasted, printed, or transmitted
  - Generates detailed forensics reports
  - Ability to add additional scanning categories and content filters (e.g., adult content, credit card information, backdoors, key logger, P2P, personal information, Social Security numbers, violent acts)

Enhanced data loss prevention service

- **What content types are supported by EDLP?**
  - DLP supports more than 300 content type classifications including:
    - Microsoft documents
    - Adobe files
    - Multimedia files
    - Source code
    - Design files
    - Archives
    - Encrypted files

Endpoint file/folder level encryption

- **Rollout type:** VITA Service Catalog item
- **Expected launch:** Oct. 29
- **Overview:**
  - **File and Folder Encryption (FRP):**
    - Encryption software that helps protect data stored on file shares, removable media, and cloud storage services such as Google Drive
    - It uses policy-enforced, transparent encryption to prevent unauthorized access to your information across removable media, network servers, and computer hard drives
  - **Drive Encryption (DE):**
    - Full disk encryption software that protects data especially from lost or stolen equipment
    - Makes all data on a system drive unintelligible to unauthorized persons
    - Drive Encryption is compatible with traditional hard drives (spinning media AKA HDD), solid-state drives (SSD), and self-encrypting drives (SED and OPAL)

Endpoint file/folder level encryption

- **What are the broad use cases that FRP addresses?**
  - FRP protects data on local drives, network shares, and removable media devices. Specifically, it offers options to:
    - Encrypt files/folders on local drives
    - Encrypt files/folders on network shares
    - Encrypt files/folders synced to cloud storage services
    - Encrypt removable media devices
    - Restricts usage of encrypted removable media devices to just within the company's environment (onsite access only)

Virginia Information Technologies Agency

Centralized IT Security Audit Service

Mark McCreary, CISA, CISSP, CISM
Director

ISOAG
Oct. 9,2019

Agenda

- Audit Requirements
- Centralized IT Security Audit Service
- Risk-Based Audits
- Benefits of Using the Service
- Common Issues Identified During Audits
- Memorandum of Understanding/Ordering the Service

IT Security audits

IT Security Audit Standard (SEC502) requires:

- Annual audit plan submission for upcoming three-year period
- Audit of each sensitive system every three-years

IT'S AUDIT BUSY SEASON, SO I'M GOING TO NEED YOU
TO GO AHEAD AND COME IN ON SATURDAY

Centralized IT security audit service

- Assists with audit plan development

- Conducts risk-based sensitive system IT security audits

- Helps with management responses/corrective action plans

Risk-based audits

Focus on high-risk areas

Leverage results of other audits or reviews:

- System and organization controls (SOC) reports
- Prior audit reports

ECOS

- Emphasis placed on access controls and contingency Planning (primarily areas where you have control)
- ECOS assessments/oversight

Benefits of using the service

- Familiar with commonwealth security standards and VITA operations

- More cost effective than private firms

- Knowledge retention

"You're *sure* you've conducted an internal audit before?"

Benefits of using the service

- Sensitive system audit compliance rose from 54% in 2017 to 92% in 2018

- Completed IT security audits of 50 sensitive systems at 11 agencies in 2018

- Helps to provide assurance that agencies are aware of any IT security issues related to their sensitive systems and are able to develop corrective action plans to address deficiencies

Common Issues

Common issues

- ❑ No formally documented and approved IT security policies and procedures
- ❑ ISO does not report to the agency head
- ❑ No 42-day password change frequency for:
  - Sensitive system authenticators
  - Administrative authenticators

Common issues

- ❑ Using end-of-life software
- ❑ Account management
  - Inappropriate privileges for regular COV accounts

    We find many cases where regular COV accounts have been made members of administrator security groups on servers and workstations
  - Not disabling inactive accounts
- ❑ Tier III data center requirements not met

Common issues

- ❑ Lack of two-factor authentication for:
  - Remote network connections for accessing sensitive systems
  - Network connections for accessing development environments or performing administrative functions on servers or multi-user systems. Two-factor is required for all network-based administrative access to servers and multi-use systems.
- ❑ Few security exceptions submitted

Memorandum of understanding

- Identifies the in-scope sensitive IT systems
- Cost for each fiscal year
- One-year lead time for opting out

Questions/ordering the service

- Contact me at:

Mark.McCreary@Vita.Virginia.Gov

or

(804) 416-5174

ISO Service Update
Wes Kleene

Upcoming Events

IS Orientation

Dec. 10, 2019

1 – 3 p.m.

Room 1221

Register @:
http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

Cybersecurity summit

ISACA VA Cybersecurity Summit

Nov. 7, 2019

8:30 AM-5:30 PM

Delta Hotel

555 Canal Street, Richmond, VA

https://web.cvent.com/event/65f94887-0bbb-4a97-8064-b8c92e1137b7/summary?environment=P2

Future ISOAG

Nov. 6, 2019 @ CESC 1-4 p.m.

Speakers: Brandon Lapetina- Varonis Systems

Marlon Cole - VITA

ISOAG meets the first Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk