



CIP Enforcement

Jenifer Wallace Farrell

CIP Self Report / Self Log

- Violation description
 - # of devices / facilities / personnel in scope
 - Names/IDs of devices/facilities/personnel
 - Where are the devices located (e.g. ESP, PSP, facility)
 - What are the devices used for
 - What type of access do the personnel have (e.g. cyber, physical, both)

CIP Self Report / Self Log

- Violation description continued
 - How was the noncompliance discovered?
 - Root Cause
 - What control failed or was lacking (can no longer use “Human Error”)
 - Compensating measures
 - Preventative
 - Detective
 - Corrective

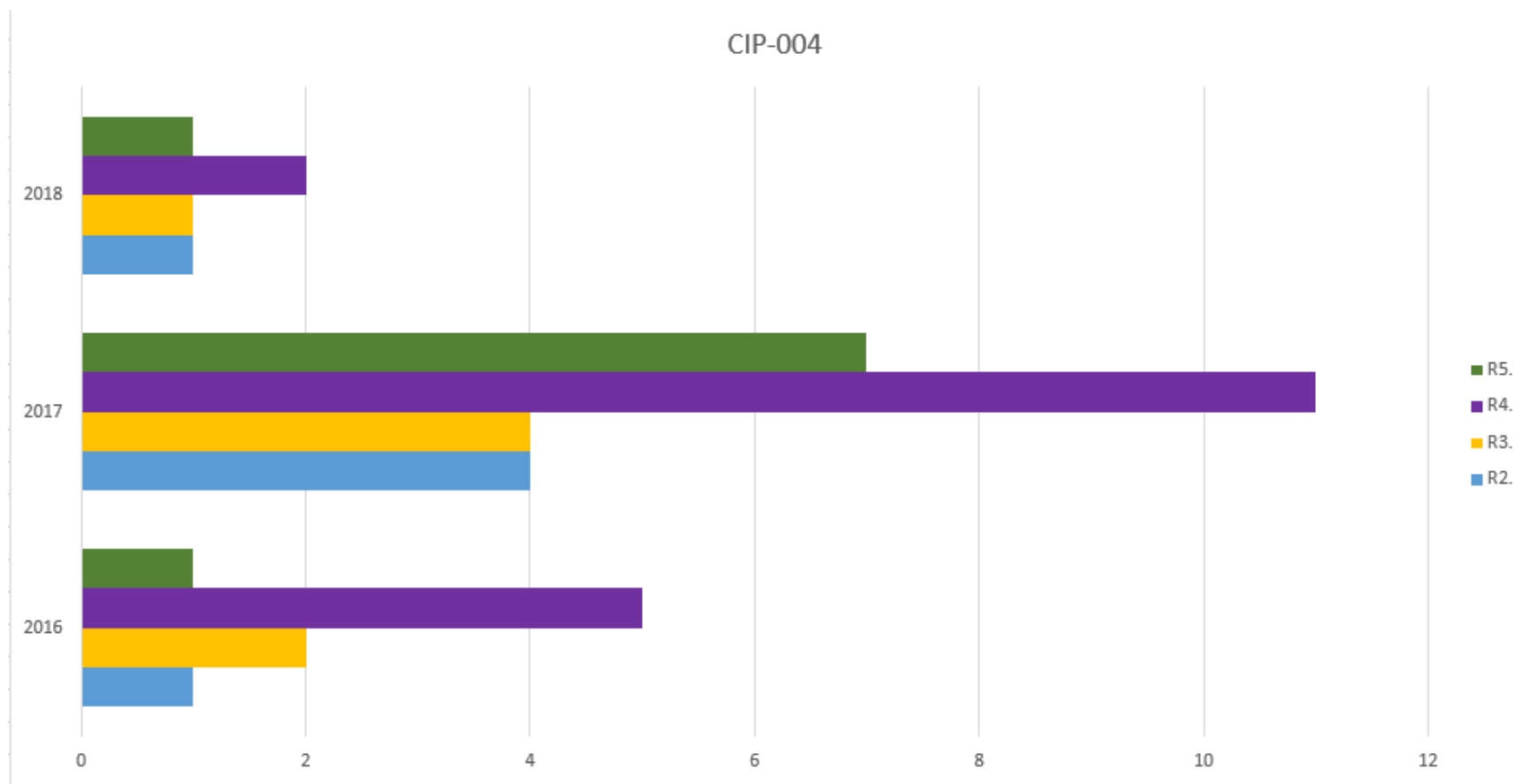
CIP Mitigation Plan

- Is the root cause addressed?
- Future Prevention
 - Identify preventative measures
 - Identify detection measures
 - Training

Violation Trends

- CIP-004 R2, R3, R4, R5
- CIP-006 R1, R2
- CIP-007 R1, R2, R4, R5
- CIP-010 R1, R2, R3, R4

CIP-004



CIP-004

- Common Root Causes
 - R2
 - Out of date procedure
 - Misunderstanding of requirement
 - Tracking system failed to alert
 - R3
 - Miscommunication
 - Tracking system not up to date / gaps for expiring soon

CIP-004

- Common Root Causes
 - R4
 - Failure to follow process when granting
 - Automated Access – system bug
 - R5
 - Management not aware of CIP Procedures
 - Failure to follow documented process
 - Use of outdated lists

CIP-004

- Better Practices
 - R2
 - Computer based training
 - Integrated Workflows
 - Web Application for Access Requests
 - R3
 - Software based tracking
 - Threshold of time since last performed

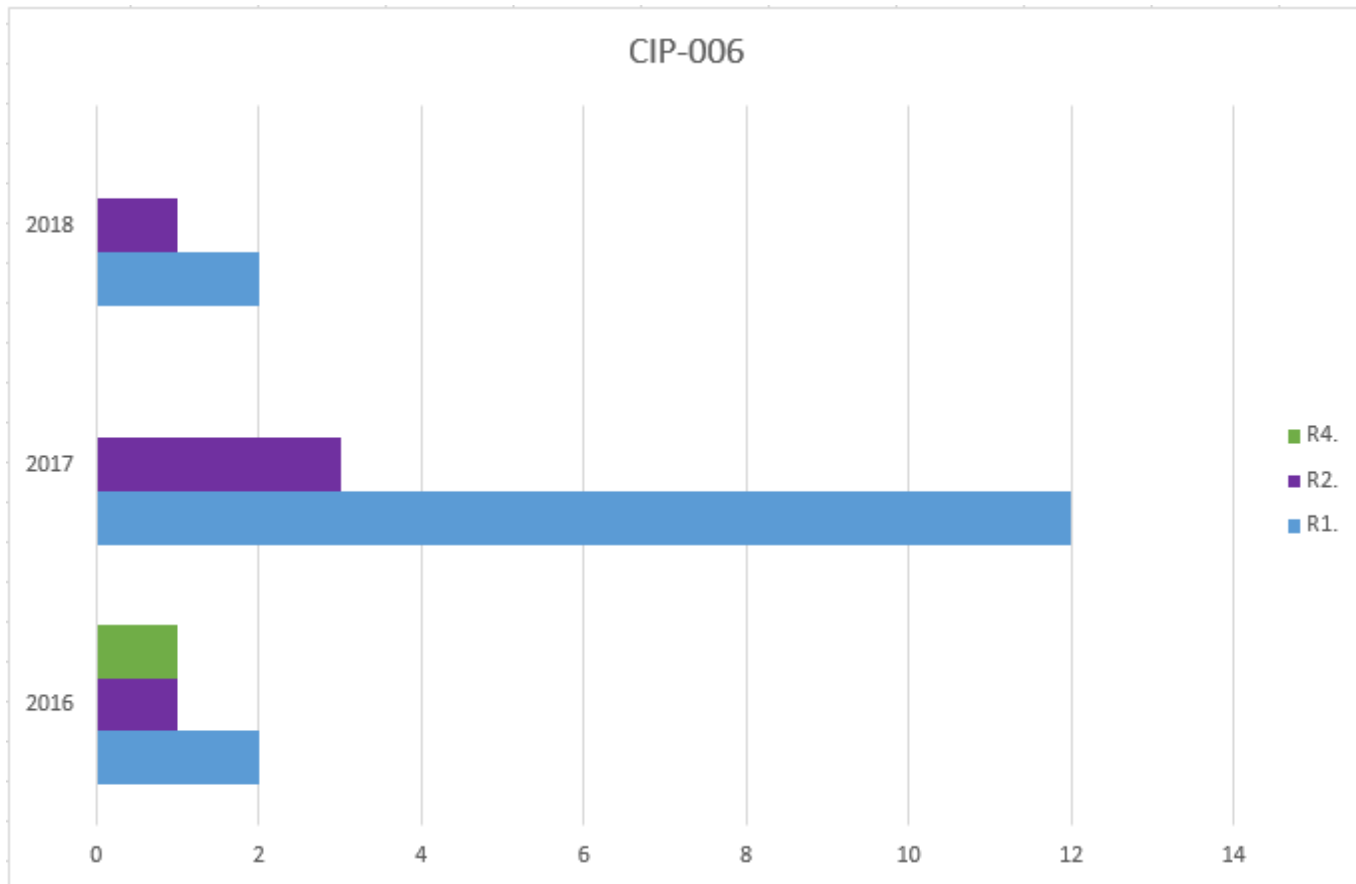
CIP-004

- Better Practices
 - R4
 - Provide scenario based training
 - R5
 - On Demand access

CIP-004

- Things to look for
 - Does your procedure reflect what you do?
 - Do individuals with access understand who is allowed to use the mouse/keyboard and why?
 - Do you have clear communication between departments?
 - Do you test your tracking tool?
 - How often do you check for expiring Training/PRA's?
 - Do personnel know how to respond when they are under pressure to grant access?

CIP-006



CIP-006

- Common Root Causes

- R1

- Door latch malfunction
 - Authorized personnel propping doors / disabling locks
 - Asset list discrepancy
 - Lack of a process to review PSP to PSP connections
 - Failure to follow process / communicate process

- R2

- Misunderstanding of responsibilities
 - Failure to follow process
 - Lack of awareness

CIP-006

- Better Practices
 - Test latches
 - Assign Responsibility
 - Signage
 - Computer based Training
 - Designated visitor escorts

CIP-006

- Things to look for
 - Survey employees
 - Do they know they shouldn't prop open doors?
 - Do they know they shouldn't tape over locks?
 - Do they confirm PSP Doors, Racks and other access points are securely closed when they finish work/leave?
 - Do they know what to do if a door must be propped?
 - Do they know there is a visitor process?

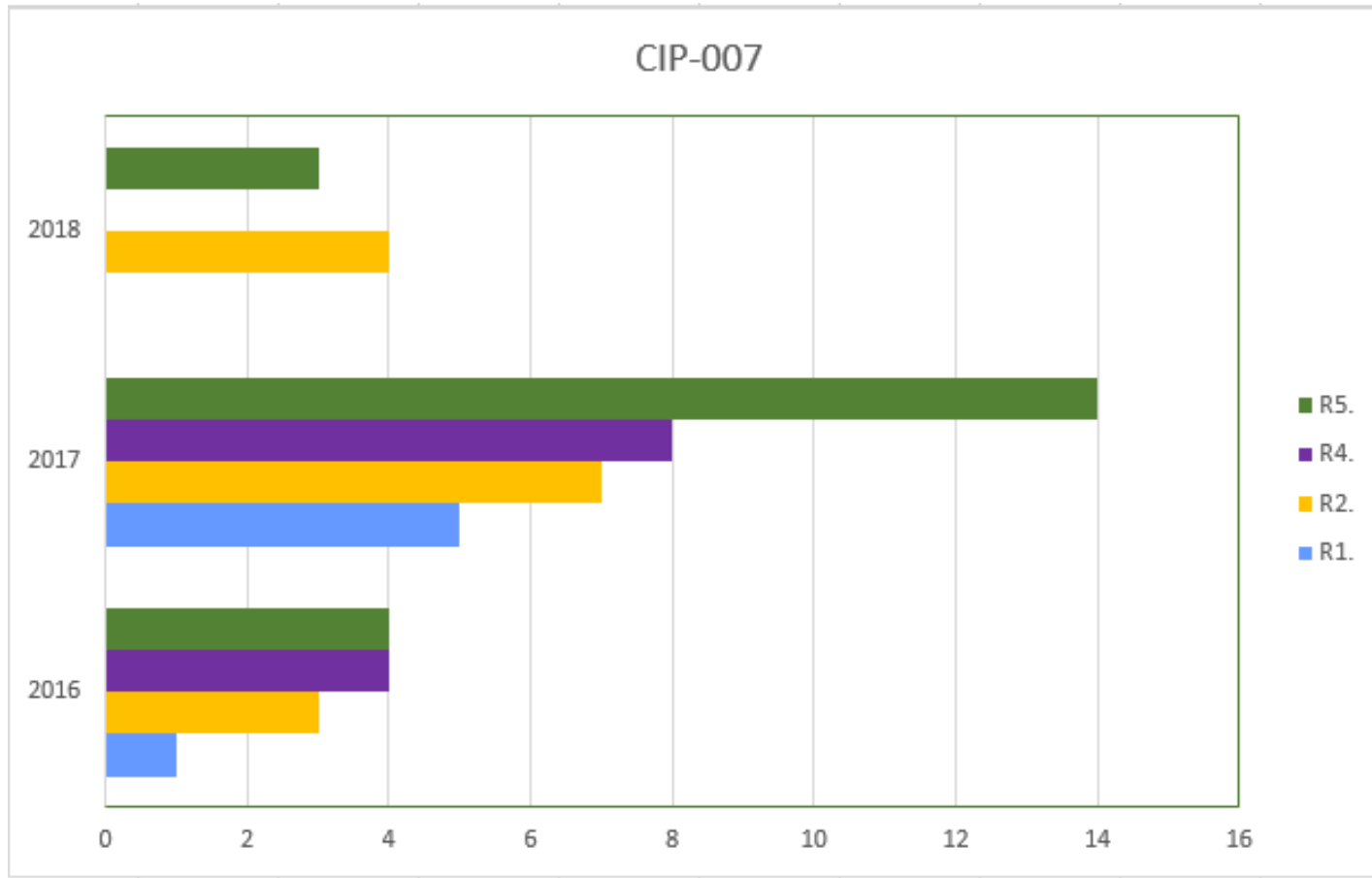
CIP-006

- Things to look for
 - How often are door latches tested?
 - Do door locking mechanisms have a delay?
- Visitors
 - How do personnel know the visitor process applies?
 - What should personnel do if they don't know how to bring a visitor into a facility?

CIP-006

- Visitors continued...
 - Do your personnel know there is a process but choose not to follow it? Why? Is your process too complex?
 - Do personnel know what to do if they can't follow the regular process (off hours – not enough badges, they don't know where to go to get badges)

CIP-007



CIP-007

- Common Root Causes
 - R1
 - Lack of oversight and miscommunication
 - R2
 - Workload constraints / Lack of resources
 - Lack of training on patch tracking system
 - Patch evaluation reminder failure
 - Failure to request a Mitigation Plan extension
 - Failure to assign responsibility upon transfer of personnel

CIP-007

- Common Root Causes

- R4

- Lack of understanding of the requirement
 - lack of process/failure to verify and test logging/alerts
 - Workload constraints / Lack of resources

- R5

- Workload constraints / Lack of resources
 - Password tracking sheet out of date
 - Lack of a process to inventory and track passwords
 - No process to document password changes
 - No method for identifying passwords had been enforced new deployment / upgraded

CIP-007

- Better Practices
 - Asset database control baseline
 - Automation
 - Job aids

CIP-007

- Things to look for
 - When deploying new projects / multiple assets have responsibilities been assigned?
 - Are personnel trained on the use of tools?
 - Do you test your reminder tools to ensure alerts are working?
 - Is your process clear on what to do if a Mitigation Plan date cannot be met?
 - Do you track individual responsibilities and have a method to assign responsibilities to another individual (sick, vacation, transfer)

CIP-007

- Things to look for
 - During times of heavy workload, do personnel have a process for managing workload, setting priorities and escalating issues (Daily/weekly scrum)?
 - Do you have a clear process for identifying what devices need CIP-007 controls?
 - Do you have a method for verifying and testing that logging and alerting are functional (initial deployments and after baseline changes)?

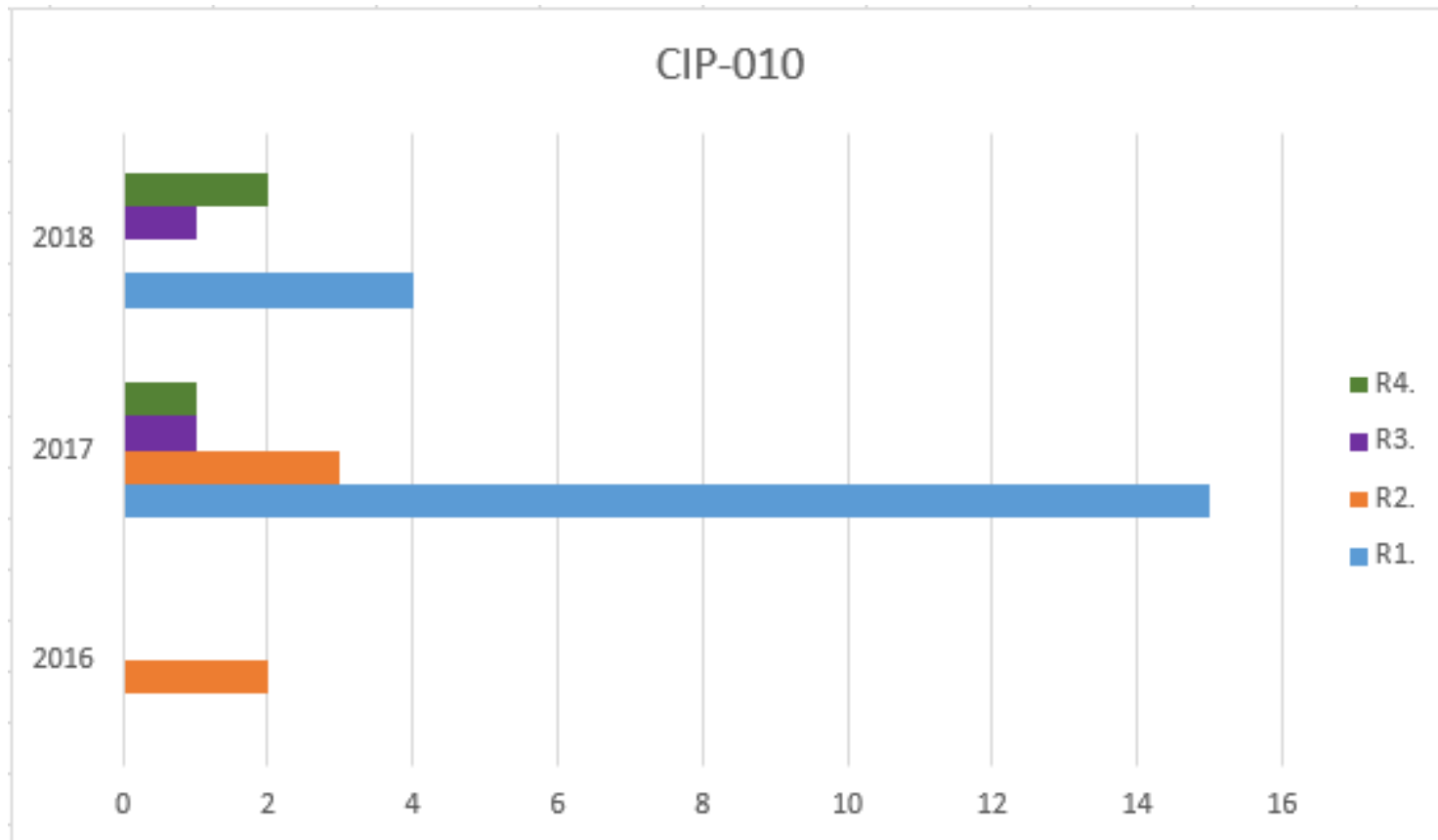
CIP-007

- Things to look for
 - Do you have a job aid for all applicable device types that describes how to enable logging / adjust settings?
 - Do you have a method to alert for detected failure of event logging?
 - Do you have a method to identify all application accounts and default shared accounts within applications?

CIP-007

- Things to look for
 - Do you have a method for checking the timeframes for password changes that are enforced procedurally?
 - Do personnel know what requirements need to be implemented when installing new/replacement devices (What if the replacement device has more functionality than the prior TFE'd device)?

CIP-010



CIP-010

- Common Root Causes

- R1

- Lack of understanding what should be a PACS, EACMS, PCA
 - Insufficient training on new technology
 - Lack of awareness, communication and oversight
 - Lack of a process for requiring CIP compliance evaluations prior to performing system restoration or troubleshooting tasks.
 - Failure to follow documented procedures
 - Workload constraints / Lack of resources

CIP-010

- Common Root Causes

- R2

- Individuals responsible for monitoring forgot
 - Failure to follow documented procedures
 - Lack of a process for identifying communication failures

- R3

- Lack of a process and controls to ensure vulnerability scans and mitigation plans were coordinated and completed.

- R4

- Lack of a control to identify patch failures
 - Lack of awareness and contractor training

CIP-010

- Better Practices
 - Asset Management Database
 - Assign Responsibility
 - Automated reminders
 - Job aids

CIP-010

- Things to look for
 - 36 calendar month active vulnerability assessment due by 07/01/2018
 - Do your personnel have a clear understanding or have job aid or process for identifying PACS, EACMS, and PCAs?
 - Does someone have assigned responsibility for completing a baseline for new/updated assets?
 - Do you have a process to identify new substation projects?

CIP-010

- Things to look for
 - For manual baseline collection, do personnel have a clear understanding or job aid for what they should be collecting and documenting?
 - Have personnel been trained on how to use new technology and how to identify errors?
 - Have personnel been trained on what job tasks require authorization?
 - Do personnel have a job aid for identifying changes that deviate from the baseline?

CIP-010

- Things to look for
 - Raise awareness that system restoration and troubleshooting tasks can lead to baseline changes
 - Do personnel know what adequate evidence is when it comes to demonstrating testing?
 - During times of heavy workload, do personnel have a process for managing workload, setting priorities and escalating issues (Daily/weekly scrum)?

CIP-010

- Things to look for
 - Do you have methods for reminding and escalating incomplete work tasks before you are in noncompliance?
 - Do you have a process for identifying device communication failures before you are in noncompliance with the 35 calendar days monitoring?
 - Do you have a process to ensure vulnerability scans and mitigations plans are coordinated and completed?

CIP-010

- Things to look for
 - Do you have a method for identifying control failures on TCA's?
 - Have contractors been trained on your TCA and Removable media processes?
 - Do personnel have a way to identify who is authorized to use a TCA?

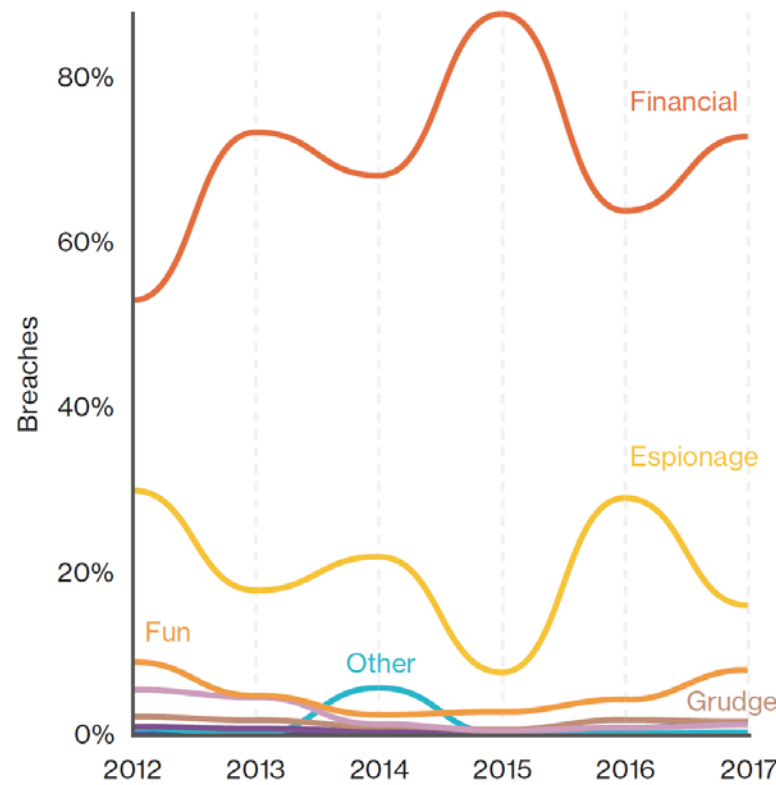
Verizon Data Breach Investigations Report

Reference

- Verizon. (2018, May 16). Verizon 2018 Data Breach Investigations Report. Retrieved from Verizon:
<http://www.verizonenterprise.com/verizon-insights-lab/dbir/>

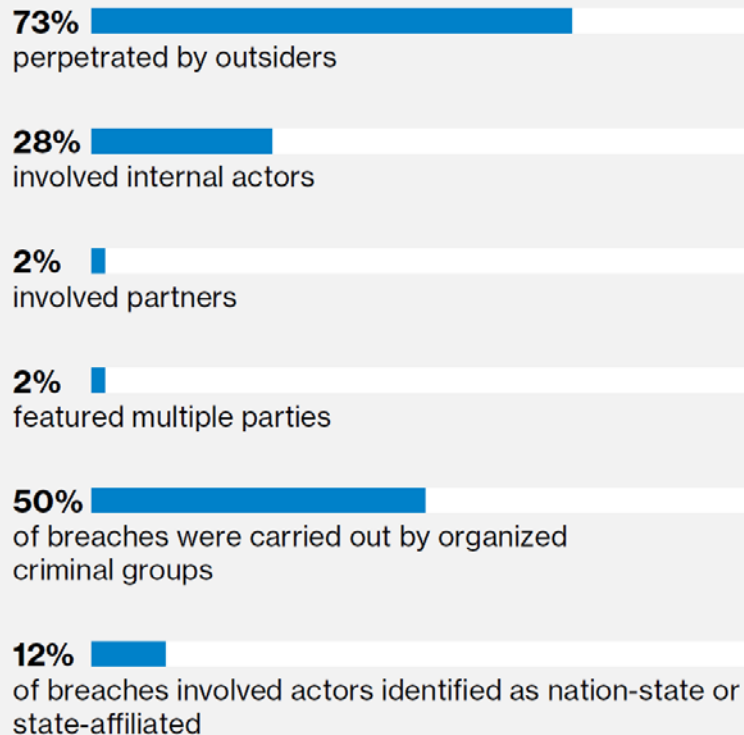
Verizon Data Breach Investigations Report

Actor motives in breaches



Verizon Data Breach Investigations Report

Who's behind the breaches?

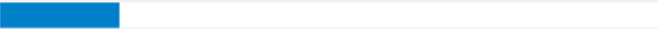


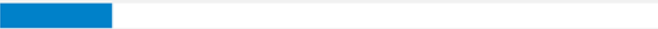
Verizon Data Breach Investigations Report

What tactics are utilized?

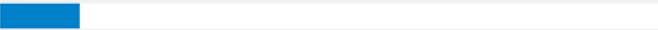
48% 
of breaches featured hacking

30% 
included malware

17% 
of breaches had errors as causal events

17% 
were social attacks

12% 
involved privilege misuse

11% 
of breaches involved physical actions

Verizon Data Breach Investigations Report

What are other commonalities?

49% 
of non-POS malware was installed via malicious email¹

76% 
of breaches were financially motivated

13% 
of breaches were motivated by the gain of strategic advantage (espionage)

68% 
of breaches took months or longer to discover

Verizon Data Breach Investigations Report

Top 20 action varieties in breaches

Use of stolen credentials (hacking)

399

RAM scraper (malware)

312

Phishing (social)

236

Privilege abuse (misuse)

201

Misdelivery (error)

187

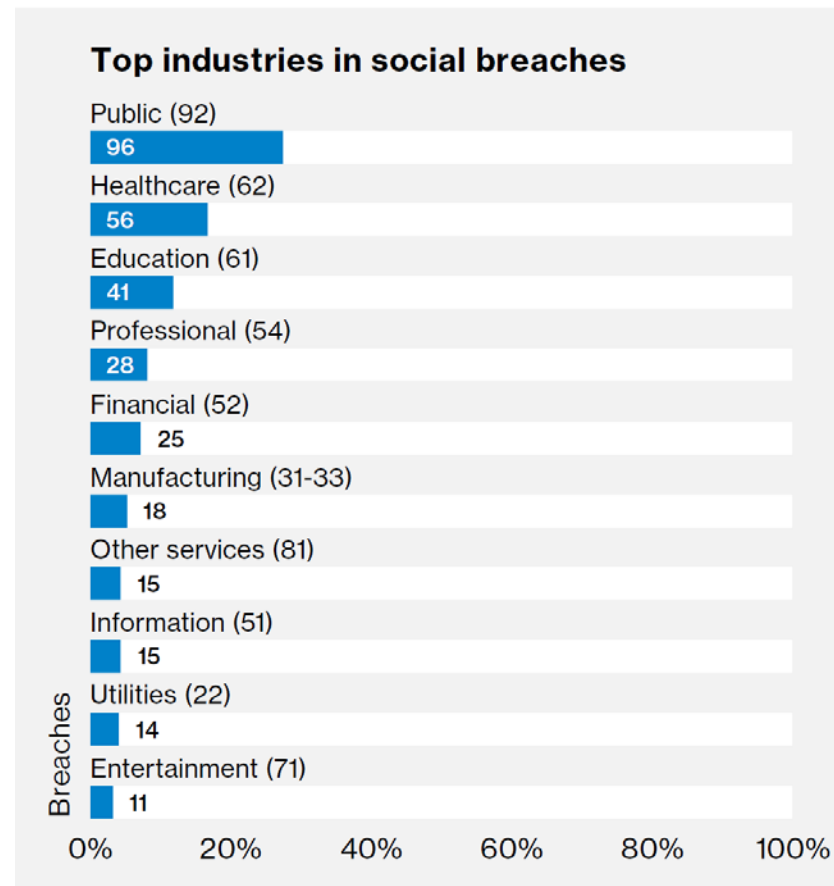
Use of backdoor or C2 (hacking)

148

Theft (physical)

123

Verizon Data Breach Investigations Report



Phishing

- Training / Awareness
 - Test your ability to detect a campaign, identify infected hosts, look for existence of data exfiltration.
- Identify the clickers
 - Give them a tablet or sandboxed OS
 - Segment clients from critical assets
 - Use strong authentication (i.e., more than a keylogger is needed to compromise)

Information Handling

- What information is provided to Vendors
 - Full databases (troubleshooting)
 - Obfuscate data where possible or use test data
 - Ensure vendor knows if data is sensitive
 - Logs
 - Redact usernames and passwords
 - Passwords
 - Have secure method, don't keep a full spreadsheet of unencrypted passwords within your vendor's portal

Questions?

Jenifer Wallace Farrell, CISSP, CISA

Senior CIP Analyst

jwallace@npcc.org