CYBERSECURITY AUDITING

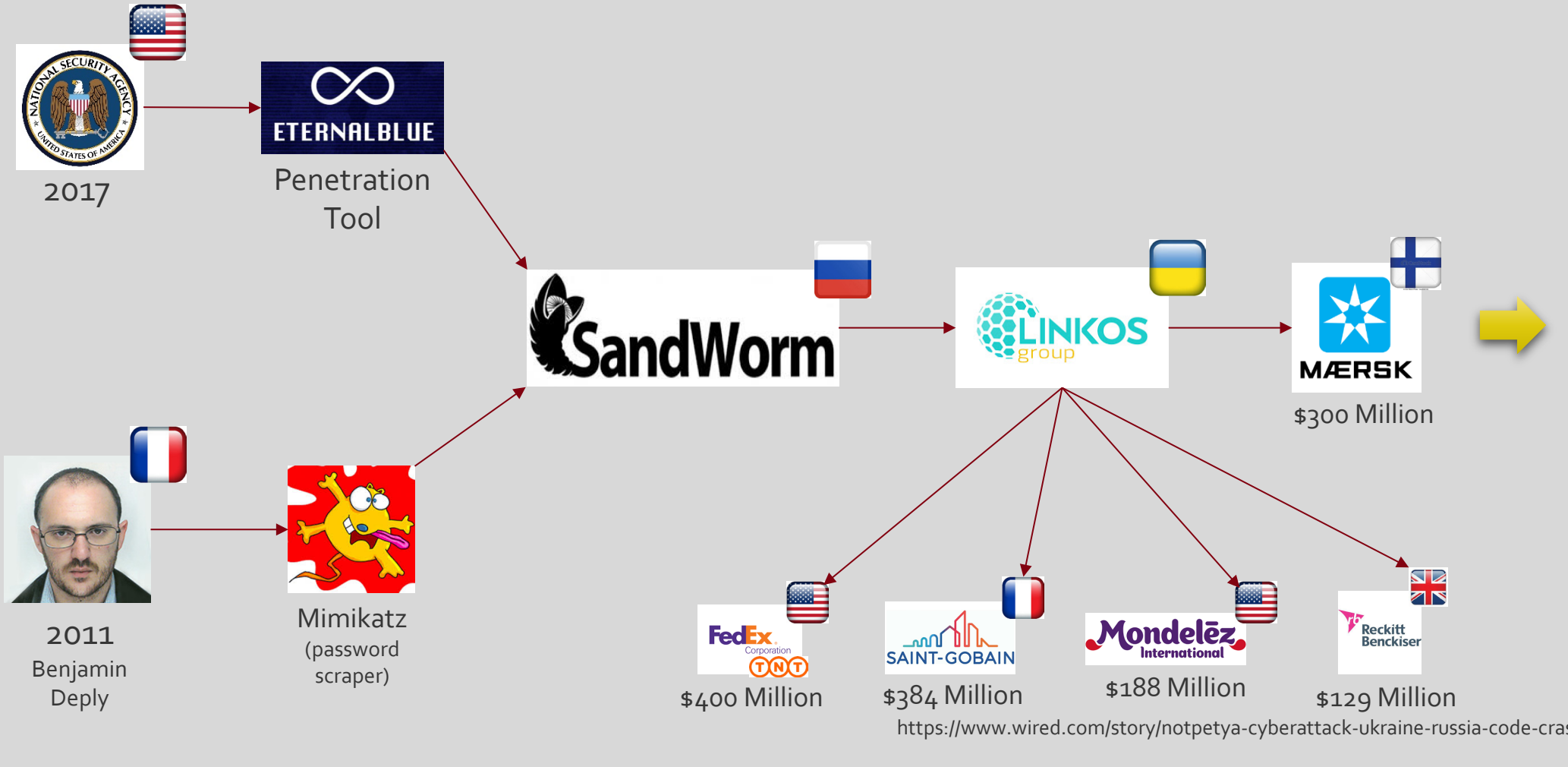
Why it's more important than ever!

STRANDED POTTY-MOUTHED PARROT GREETS FIREFIGHTERS WITH FOUR-LETTER TIRADE

- The efforts by Green Watch from Edmonton station to charm the misbehaving bird went smoothly at first, and she responded positively, telling her would-be rescuer that she loved him back.
- But, Jessie soon launched a foul-mouthed tirade against the fire crew, telling the fighter fighters to “f*** off”.

The Telegraph

NOTPETYA

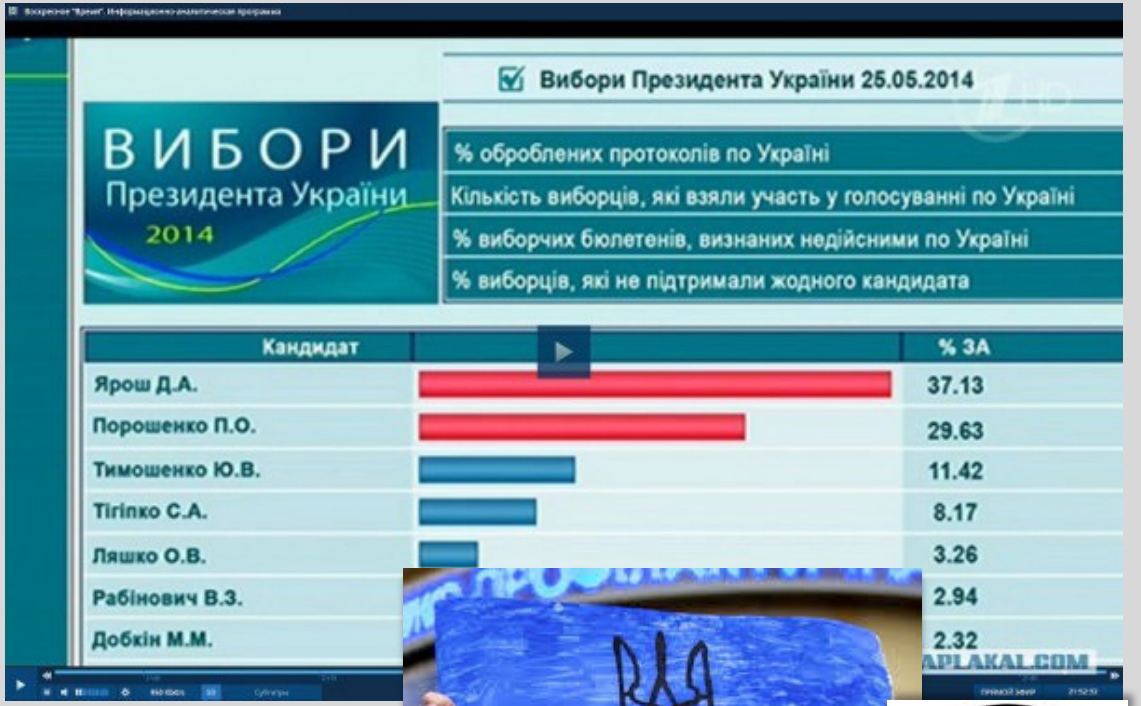


https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

UKRAINE ELECTION 2014

- Election system destruction/disruption
- Displaying of fake election results
- DDoS attack on Ukrainian EC website

- Techniques and Tactics
  - Malware (COTS)
  - Insider Threat
  - Cisco 0-day



https://www.ft.com/content/34177ec8-c7f9-11e6-8f29-9445cac8966f

DEFCON 2018

An 11-year-old hacked a replica of Florida's voting system in 10 minutes

- DEF CON participants discovered:
  - The boy and girl were the quickest of 35 children, ages 6 to 17, who all eventually hacked into copies of the websites of six swing states during the three-day Def Con security convention.
  - Voting systems running on expired SSL certificates, encryption keys that are intended to create secure connections, were the most vulnerable
  - Discovered more vulnerabilities in the system where citizens directly cast their votes.
  - The very real risk that somebody with technical skills and malicious intentions could directly intervene in American elections

https://www.vox.com/policy-and-politics/2018/8/13/17683666/florida-voting-system-hack-children

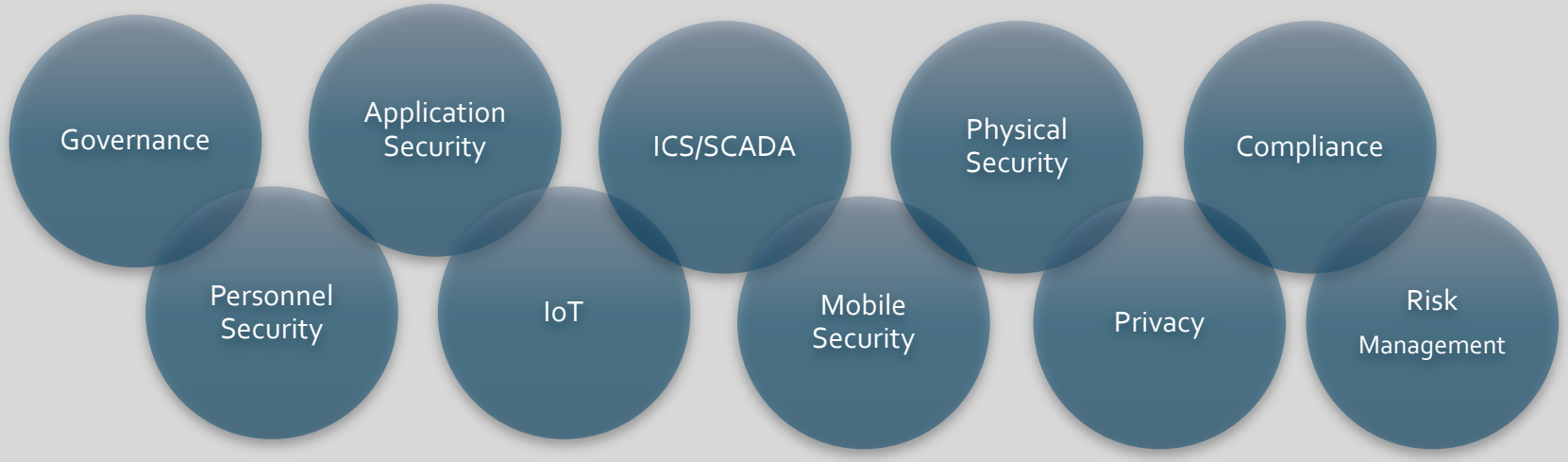
COMPLEXITY OF SECURITY

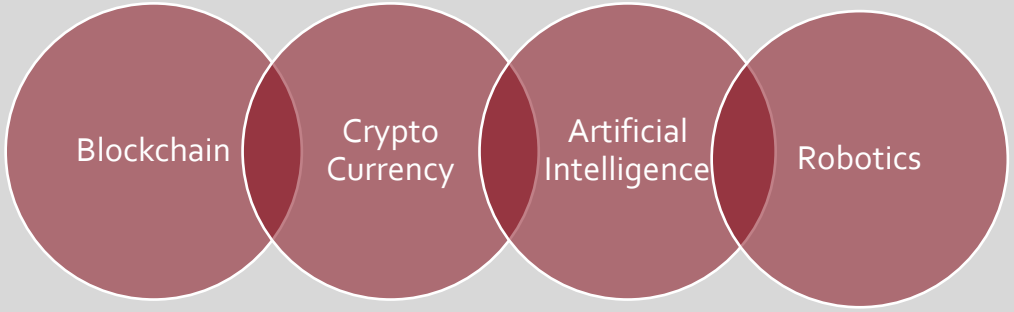
- Conception that they are highly technical
- Multiple conflicting standards
- IT centric vs. business centric
- Responsible stakeholders are often misaligned
- Security is personal
- Almost always met with resistance
- High turnover
- Operations vs. Security
- Rapid evolution of technology and threats
- You never get a fuzzy feeling!

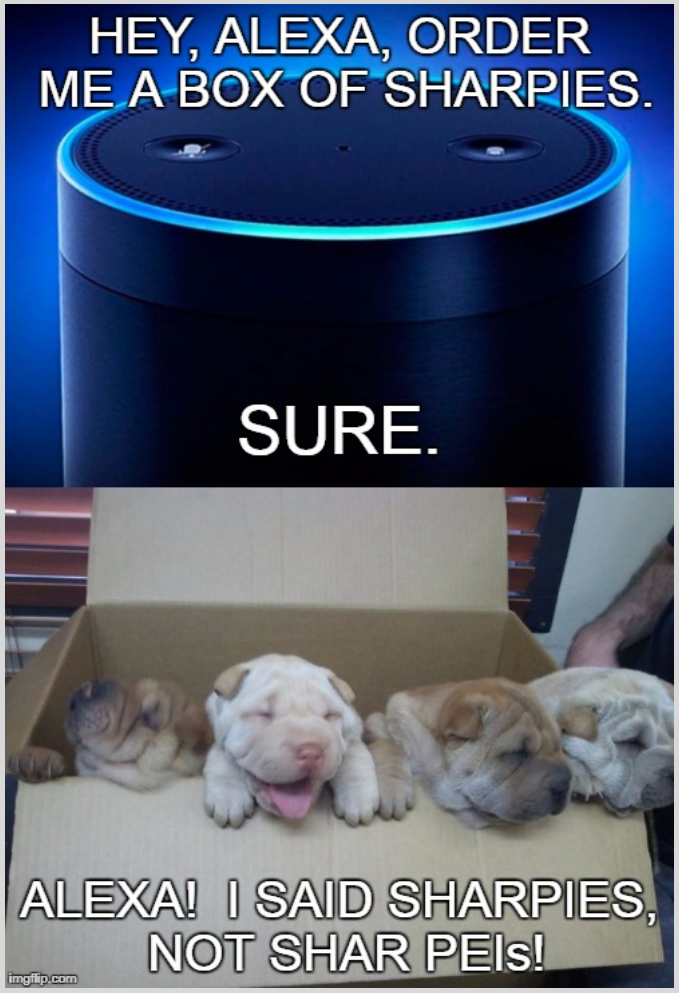
IT VS. SECURITY – COMPARE AND CONTRAST

- A natural conflict between freedom and safety
  - The SOC vs. NOC paradigm
- Differing levels of employee involvement
- Contradicting metrics of success
  - Risk (CIA) vs. "Five Nines"
  - Rapid changes
- Clear lines of leadership
- Steep learning curves and shallow talent pools
- Battle fatigue—chasing the news cycle
- Executive disconnect

THE SECURITY FOOTPRINT



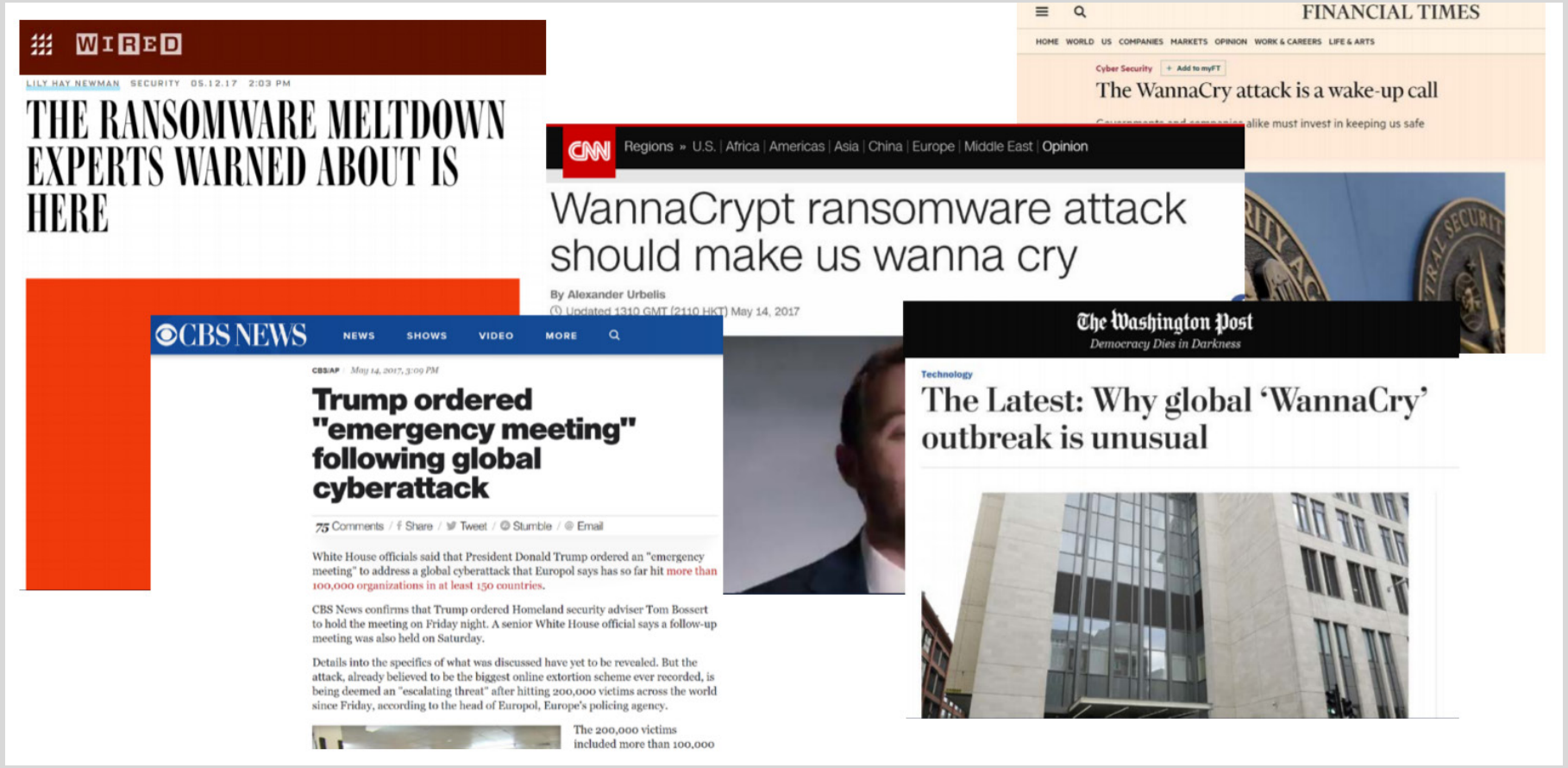




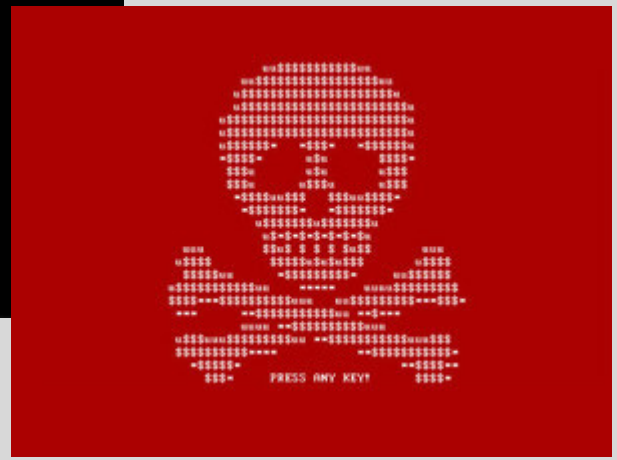
WHAT KEEPS THE CISO UP AT NIGHT?

Platform Attacks	Data Leakage	Fraud	Client Attacks	Intangible Assets	Physical
• Hack • DDoS • HW/SW Vulnerabilities	• Device Loss/Theft • Wrongful Disclosure • Theft	• Social Network Abuse • Credit Card Fraud • 3rd Party/Employee Fraud	• Credential Theft • Malware • Phishing	• Politically Exposed Persons (CEO…) • Brand Reputation	• VoIP • Video • ICS/SCADA • Credit Card Fraud • Active Shooter

FOLLOWING THE NEWS CYCLE



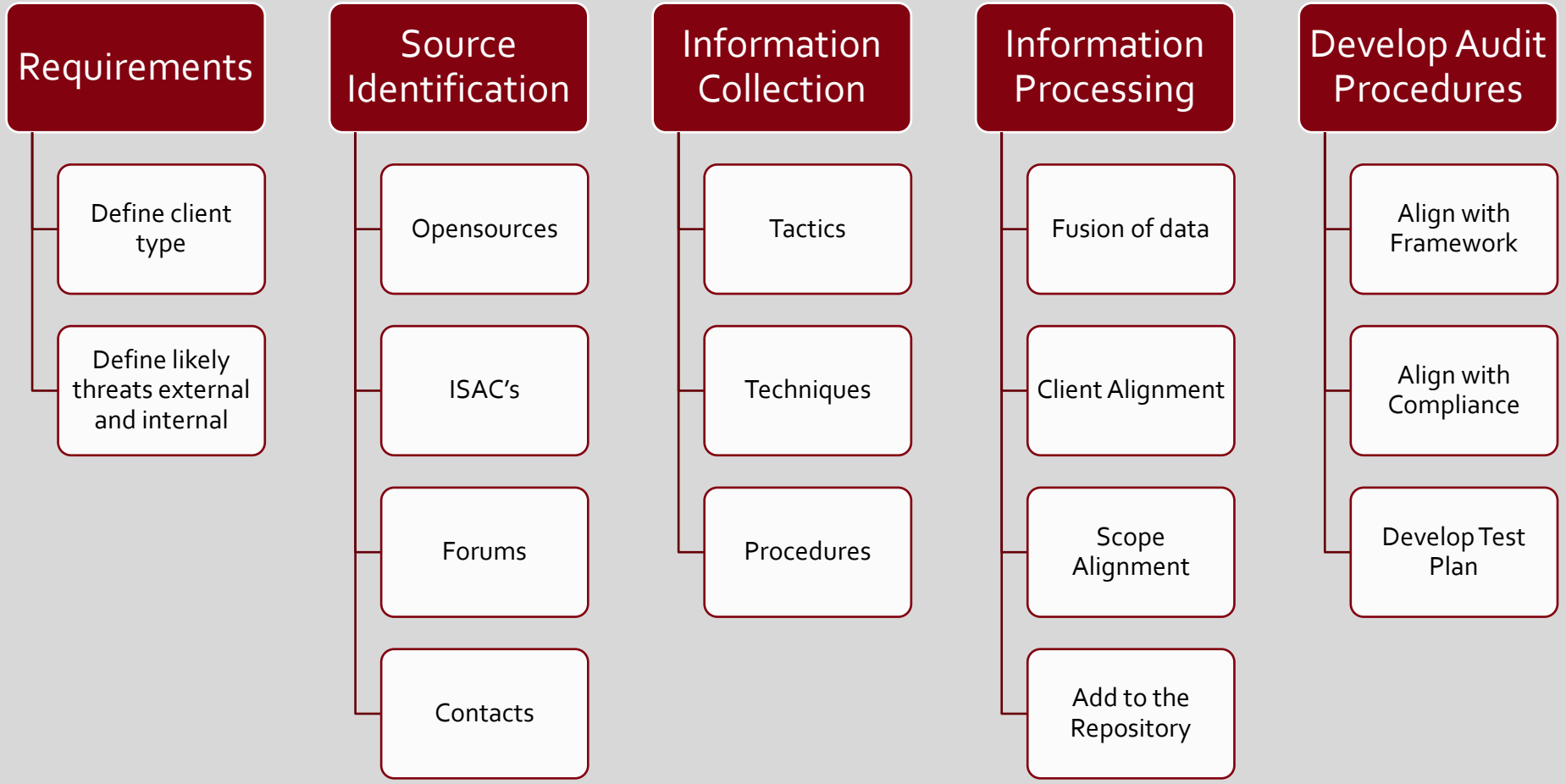
WHEN SECURITY GETS PERSONAL



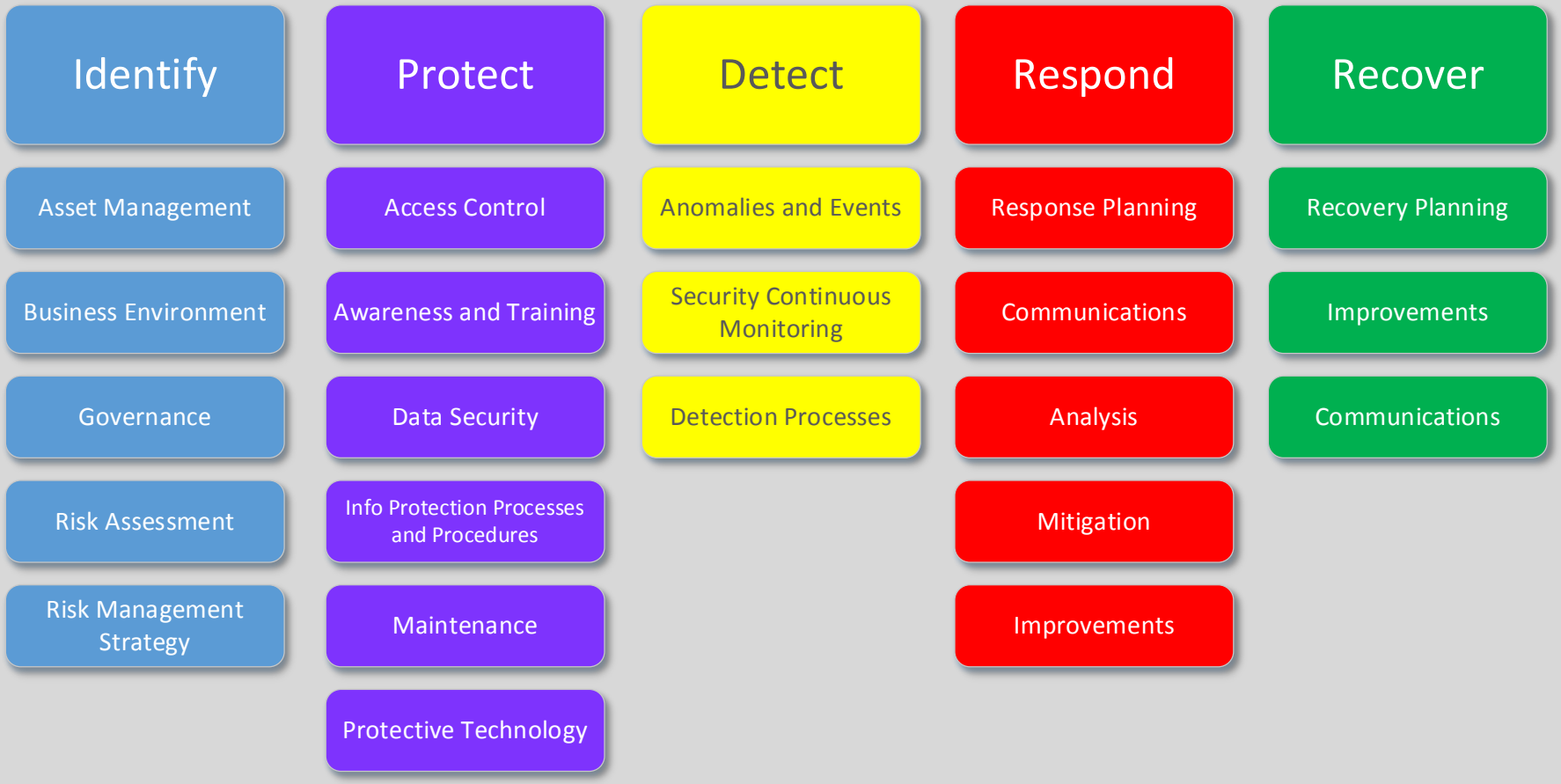
THE CYBER THREAT INTELLIGENCE LOOP

- Cumbersome
- Very technical
- Difficult to establish – buy in
- Brain drain
- Infrastructure intensive

SIMPLIFY THE PROCESS



NIST'S RISK MANAGEMENT FRAMEWORK

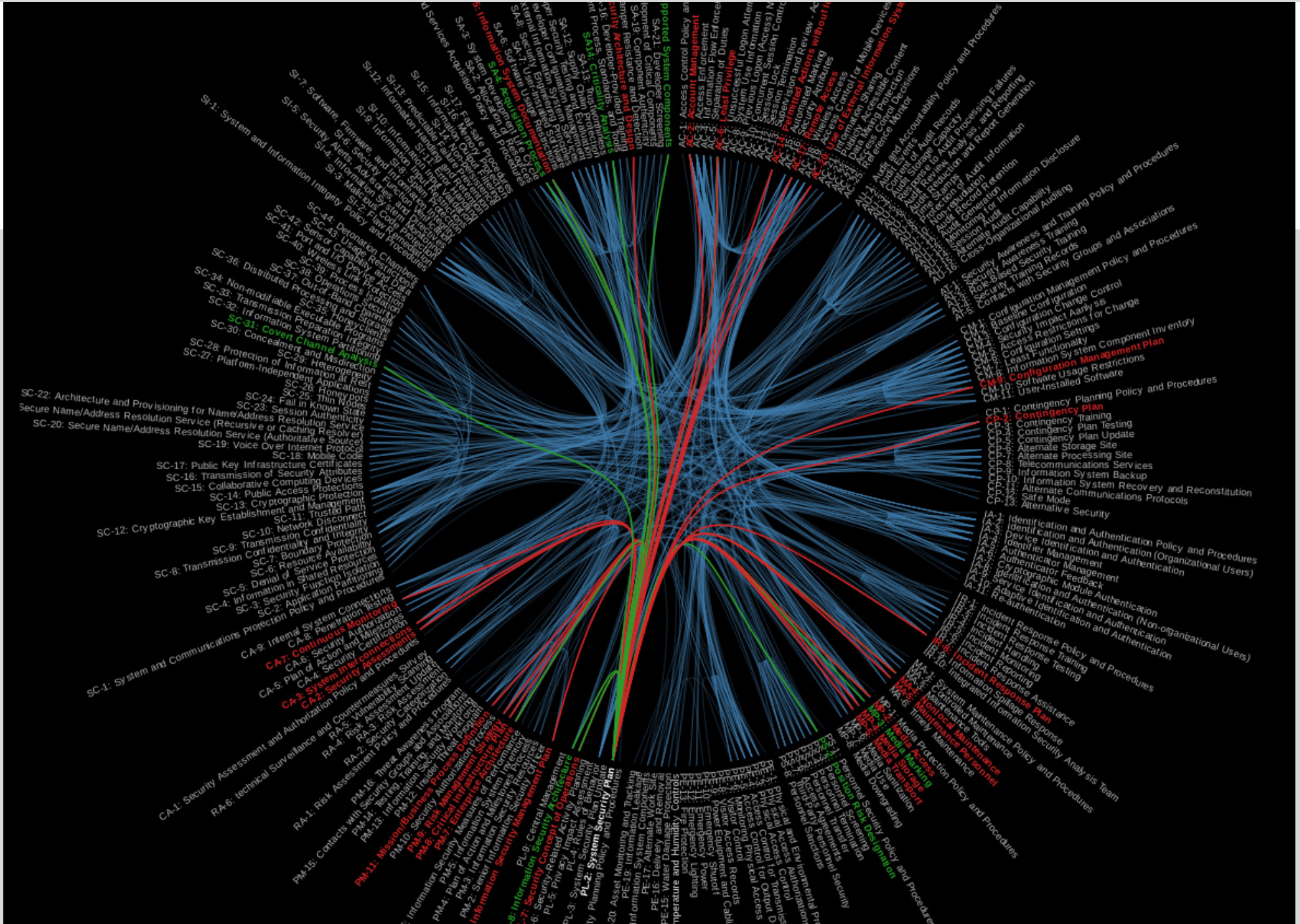


THREAT ANALYSIS IN CONTEXT?

- Integrity - An assurance that data cannot be modified in an unauthorized manner.
- Availability – Information is readily available for authorized users.
- Confidentiality – Prevention of unauthorized disclosure of information.

CHANGE IS NEEDED

How can Cyber Threat Analysis Help?

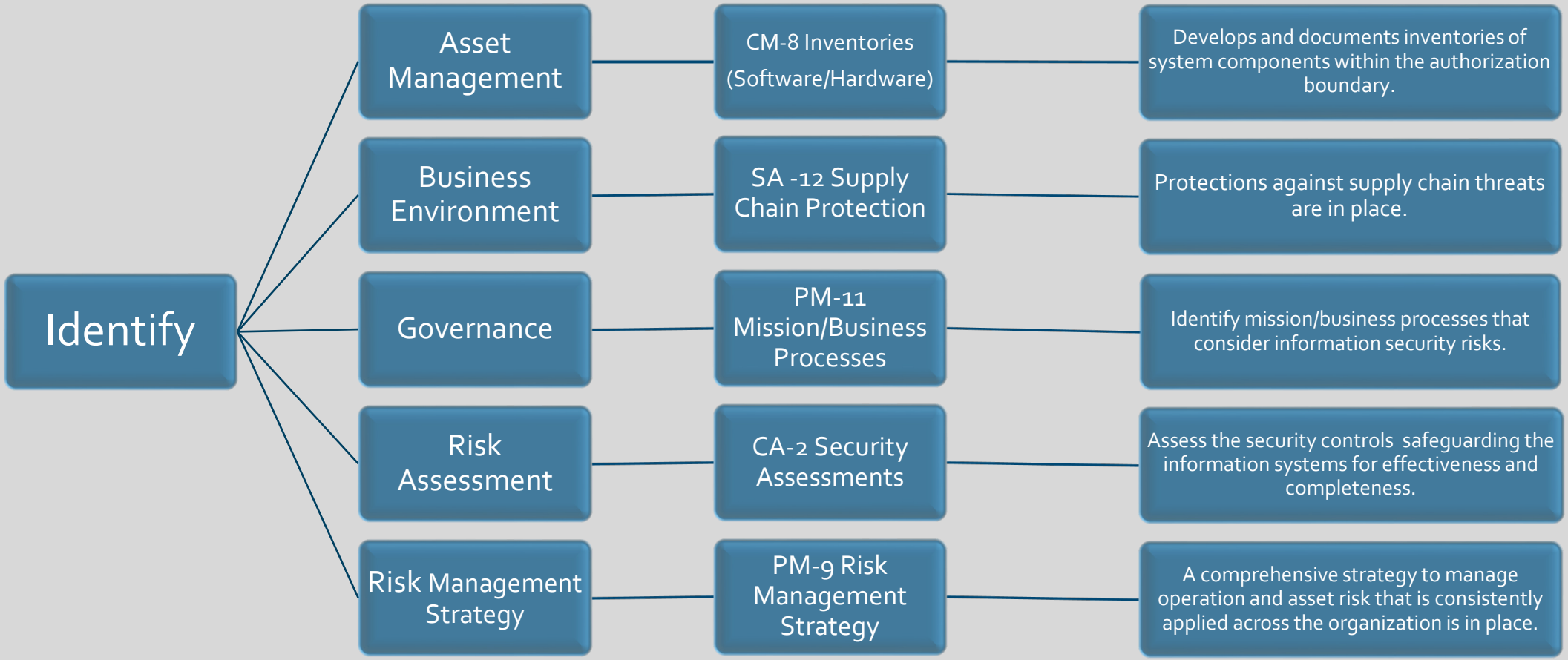

AC-1: Access Control Policy and
AC-2: Account Management
Access Enforcement
Information Flow Enforcement
Separation of Duties
Least Privilege
AC-6: Unsuccessful Logon Attempts
System Use Information
Previous Logon (Access) Notification
Concurrent Session Control
Session Lock
Supervision and Review - Access Control
Automated Marking
Security Attributes
Wireless Access
Access Control for Mobile Devices
Use of External Information Systems
Information Sharing
Publicly Accessible Content
Data Mining Protection
Access Control Decisions
Reference Monitor
AU-1: Audit and Accountability Policy and Procedures
Audit Events
Content of Audit Records
Audit Storage Capacity
Response to Audit Processing Failures
Audit Review, Analysis, and Reporting
Audit Reduction and Report Generation
Time Stamps
Protection of Audit Information
Non-repudiation
Audit Record Retention
Audit Generation
Monitoring for Information Disclosure
Session Audit
Alternate Audit Capability
Cross-Organizational Auditing
AT-1: Security Awareness and Training Policy and Procedures
Security Awareness Training
Role-Based Security Training
Security Training Records
Contacts with Security Groups and Associations
CM-1: Configuration Management Policy and Procedures
Baseline Configuration
Configuration Change Control
Security Impact Analysis
Access Restrictions for Change
Configuration Settings
Least Functionality
Information System Component Inventory
CM-9: Configuration Management Plan
Software Usage Restrictions
User-Installed Software
CP-1: Contingency Planning Policy and Procedures
CP-2: Contingency Plan
Contingency Training
Contingency Plan Testing
Contingency Plan Update
Alternate Storage Site
Alternate Processing Site
Telecommunications Services
Information System Backup
Information System Recovery and Reconstitution
Alternate Communications Protocols
Safe Mode
Alternative Security
IA-1: Identification and Authentication Policy and Procedures
Identification and Authentication (Organizational Users)
Device Identification and Authentication
Identifier Management
Authenticator Management
Authenticator Feedback
Cryptographic Module Authentication
Identification and Authentication (Non-organizational Users)
Service Identification and Authentication
Adaptive Identification and Authentication
Re-authentication
IR-1: Incident Response Policy and Procedures
Incident Response Training
Incident Response Testing
Incident Handling
Incident Monitoring
Incident Reporting
Incident Response Assistance
IR-9: Incident Response Plan
Information Spillage Response
Integrated Information Security Analysis Team
MA-1: System Maintenance Policy and Procedures
MP-1: Media Protection Policy and Procedures
MP-2: Media Access
MP-3: Media Marking
MP-4: Media Storage
MP-5: Media Transport
MP-6: Media Sanitization
Media Use
Media Downgrading
Nonlocal Maintenance
Maintenance Personnel
Timely Maintenance
Controlled Maintenance
Maintenance Tools
PS-1: Personnel Security Policy and Procedures
Position Risk Designation
Personnel Screening
Personnel Termination
Personnel Transfer
Access Agreements
Third-Party Personnel Security
Personnel Sanctions
PE-1: Physical and Environmental Protection Policy and Procedures
Physical Access Authorizations
Physical Access Control
Access Control for Transmission Medium
Access Control for Output Devices
Monitoring Physical Access
Visitor Access Records
Power Equipment and Cabling
Emergency Shutoff
Emergency Power
Emergency Lighting
Fire Protection
Temperature and Humidity Controls
Water Damage Protection
Delivery and Removal
Alternate Work Site
Location of Information System Components
Information Leakage
Asset Monitoring and Tracking
PL-1: Security Planning Policy and Procedures
PL-2: System Security Plan
PL-3: System Security Plan Update
PL-4: Rules of Behavior
PL-5: Privacy Impact Assessment
PL-6: Security-Related Activity Planning
PL-7: Security Concept of Operations
PL-8: Information Security Architecture
PL-9: Central Management
PM-1: Information Security Program Plan
PM-2: Senior Information Security Officer
PM-3: Information Security Resources
PM-4: Plan of Action and Milestones Process
PM-5: Information System Inventory
PM-6: Information Security Measures of Performance
PM-7: Enterprise Architecture
PM-8: Critical Infrastructure Plan
PM-9: Risk Management Strategy
PM-10: Security Authorization Process
PM-11: Mission/Business Process Definition
PM-12: Insider Threat Program
PM-13: Information Security Workforce
PM-14: Testing, Training, and Monitoring
PM-15: Contacts with Security Groups and Associations
PM-16: Threat Awareness Program
RA-1: Risk Assessment Policy and Procedures
RA-2: Security Categorization
RA-3: Risk Assessment
RA-4: Risk Assessment Update
RA-5: Vulnerability Scanning
RA-6: Technical Surveillance and Countermeasures Survey
CA-1: Security Assessment and Authorization Policy and Procedures
CA-2: Security Assessments
CA-3: System Interconnections
CA-4: Security Certification
CA-5: Plan of Action and Milestones
CA-6: Security Authorization
CA-7: Continuous Monitoring
CA-8: Penetration Testing
CA-9: Internal System Connections
SC-1: System and Communications Protection Policy and Procedures
SC-2: Application Partitioning
SC-3: Security Function Isolation
SC-4: Information in Shared Resources
SC-5: Denial of Service Protection
SC-6: Resource Availability
SC-7: Boundary Protection
SC-8: Transmission Confidentiality and Integrity
SC-9: Transmission Confidentiality
SC-10: Network Disconnect
SC-11: Trusted Path
SC-12: Cryptographic Key Establishment and Management
SC-13: Cryptographic Protection
SC-14: Public Access Protections
SC-15: Collaborative Computing Devices
SC-16: Transmission of Security Attributes
SC-17: Public Key Infrastructure Certificates
SC-18: Mobile Code
SC-19: Voice Over Internet Protocol
SC-20: Secure Name/Address Resolution Service (Authoritative Source)
SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22: Architecture and Provisioning for Name/Address Resolution Service
SC-23: Session Authenticity
SC-24: Fail in Known State
SC-25: Thin Nodes
SC-26: Honeypots
SC-27: Platform-Independent Applications
SC-28: Protection of Information at Rest
SC-29: Heterogeneity
SC-30: Concealment and Misdirection
SC-31: Covert Channel Analysis
SC-32: Information System Partitioning
SC-33: Transmission Preparation Integrity
SC-34: Non-modifiable Executable Programs
SC-35: Honeyclients
SC-36: Distributed Processing and Storage
SC-37: Out-of-Band Channels
SC-38: Operations Security
SC-39: Process Isolation
SC-40: Wireless Link Protection
SC-41: Port and I/O Device Access
SC-42: Sensor Capability and Data
SC-43: Usage Restrictions
SC-44: Detonation Chambers
SI-1: System and Information Integrity Policy and Procedures
SI-2: Flaw Remediation
SI-3: Malicious Code Protection
SI-4: Information System Monitoring
SI-5: Security Alerts, Advisories, and Directives
SI-6: Security Functionality Verification
SI-7: Software, Firmware, and Information Integrity
SI-8: Spam Protection
SI-9: Information Input Restrictions
SI-10: Information Input Validation
SI-11: Error Handling
SI-12: Information Handling and Retention
SI-13: Predictable Failure Prevention
SI-14: Non-Persistence
SI-15: Information Output Filtering
SI-16: Memory Protection
SI-17: Fail-safe Procedures
SA-1: System and Services Acquisition Policy and Procedures
SA-2: Allocation of Resources
SA-3: System Development Life Cycle
SA-4: Acquisition Process
SA-5: Information System Documentation
SA-6: Software Usage Restrictions
SA-7: User-Installed Software
SA-8: Security Engineering Principles
SA-9: External Information System Services
SA-10: Developer Configuration Management
SA-11: Developer Security Testing and Evaluation
SA-12: Supply Chain Protection
SA-13: Trustworthiness
SA-14: Criticality Analysis
SA-15: Development Process, Standards, and Tools
SA-16: Developer-Provided Training
SA-17: Developer Security Architecture and Design
SA-18: Tamper Resistance and Detection
SA-19: Component Authenticity
SA-20: Customized Development of Critical Components
SA-21: Developer Screening
SA-22: Unsupported System Components

ORANGE WORM

- Trojan, dubbed **Kwampirs**,
- Active since 2015
- Origin unknown
- Top 3 targets - US, Saudi Arabia, India
- Targets X-Ray and MRI Machines
- Consent form processing
- Valuable target?

https://thehackernews.com/search/label/Orangeworm

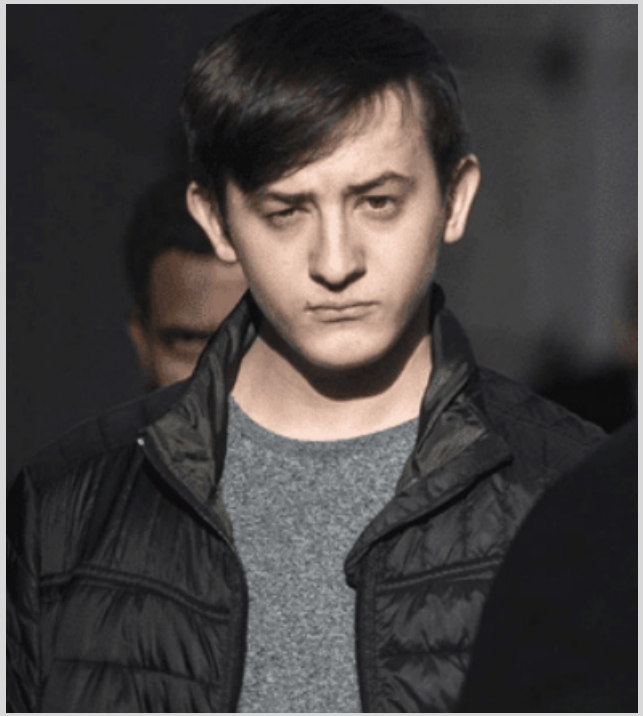
IDENTIFY


Identify
Asset Management
CM-8 Inventories (Software/Hardware)
Develops and documents inventories of system components within the authorization boundary.
Business Environment
SA -12 Supply Chain Protection
Protections against supply chain threats are in place.
Governance
PM-11 Mission/Business Processes
Identify mission/business processes that consider information security risks.
Risk Assessment
CA-2 Security Assessments
Assess the security controls safeguarding the information systems for effectiveness and completeness.
Risk Management Strategy
PM-9 Risk Management Strategy
A comprehensive strategy to manage operation and asset risk that is consistently applied across the organization is in place.

HACKING THE CIA DIRECTOR

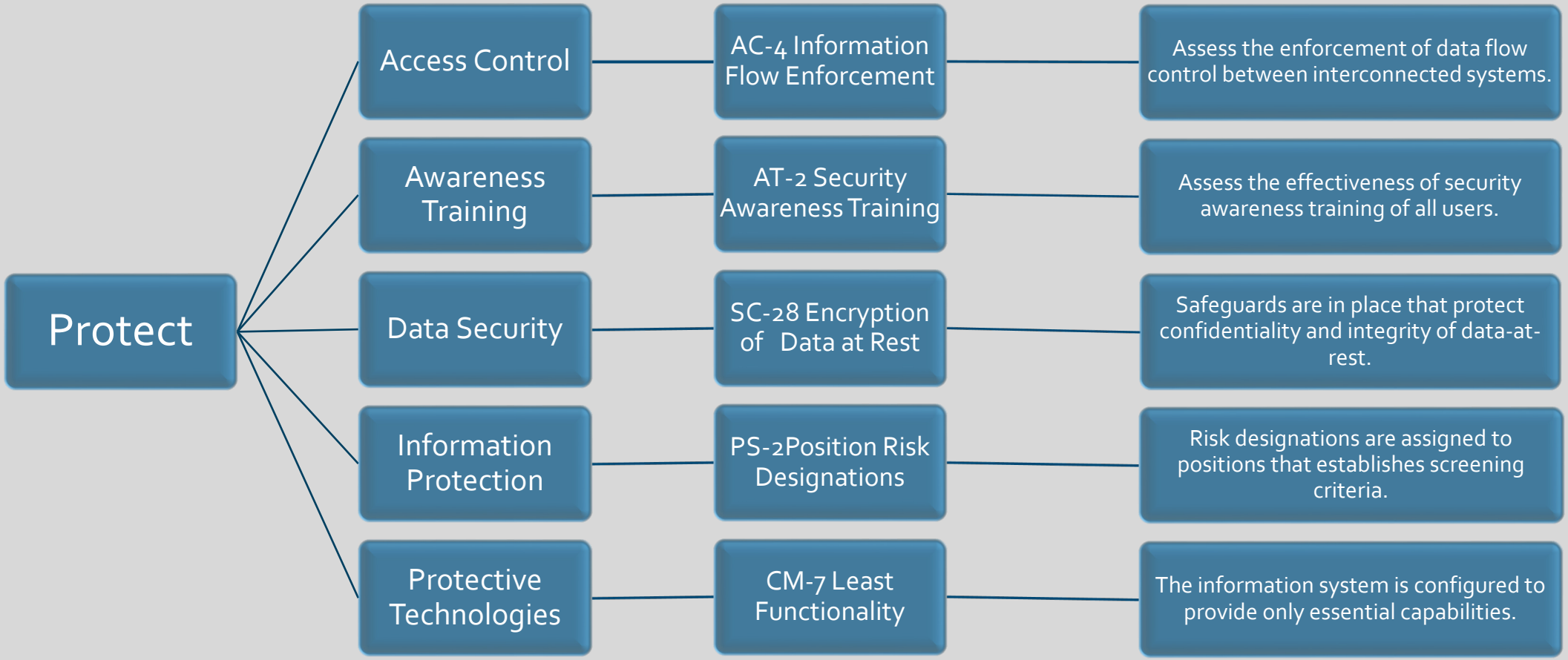
HACKING THE CIA DIRECTOR

- British teenage, Kane Gamble a.k.a. "Cracka"
- Founder of Crackas With Attitude @ 15
- Hacked email accounts of CIA Director John Brennan & Director of National Intelligence James Clapper
- Leaked the personal details of 20,000 FBI agents and 9,000 DHS personnel
- Taunted families with messages on their televisions
- 2 years in prison



https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/

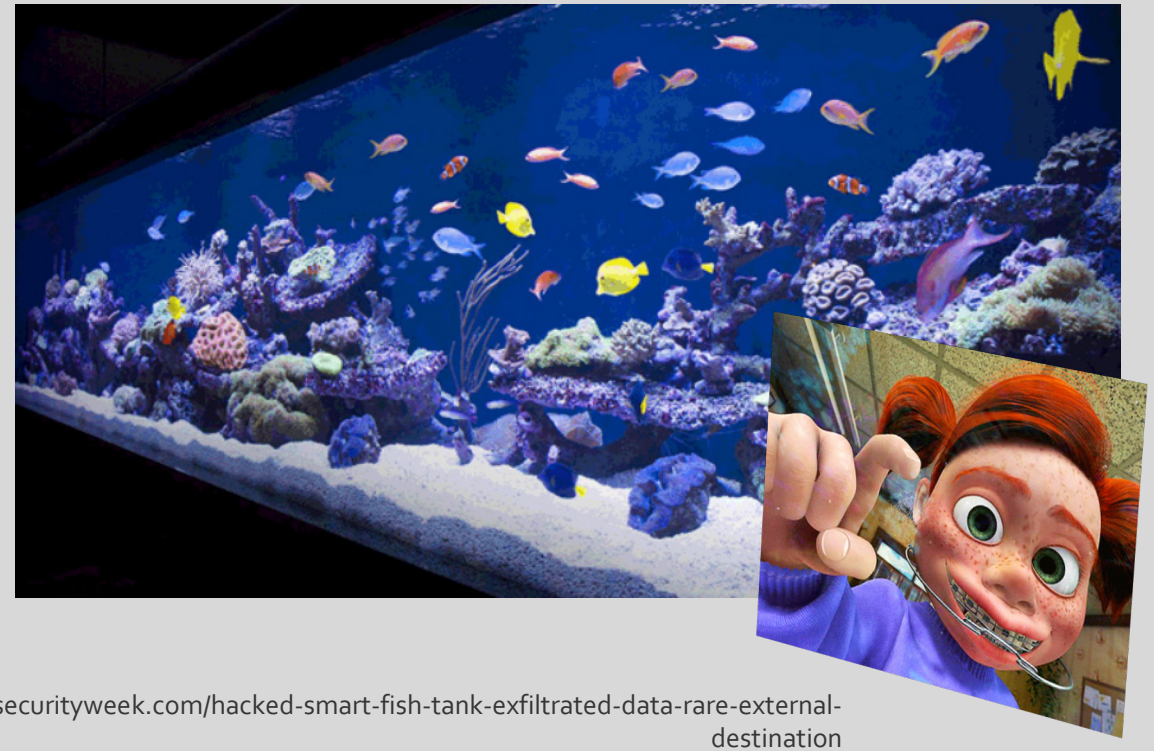
PROTECT


Protect
Access Control
AC-4 Information Flow Enforcement
Assess the enforcement of data flow control between interconnected systems.
Awareness Training
AT-2 Security Awareness Training
Assess the effectiveness of security awareness training of all users.
Data Security
SC-28 Encryption of Data at Rest
Safeguards are in place that protect confidentiality and integrity of data-at-rest.
Information Protection
PS-2Position Risk Designations
Risk designations are assigned to positions that establishes screening criteria.
Protective Technologies
CM-7 Least Functionality
The information system is configured to provide only essential capabilities.

MALICIOUS FISH TANKS AND IOT

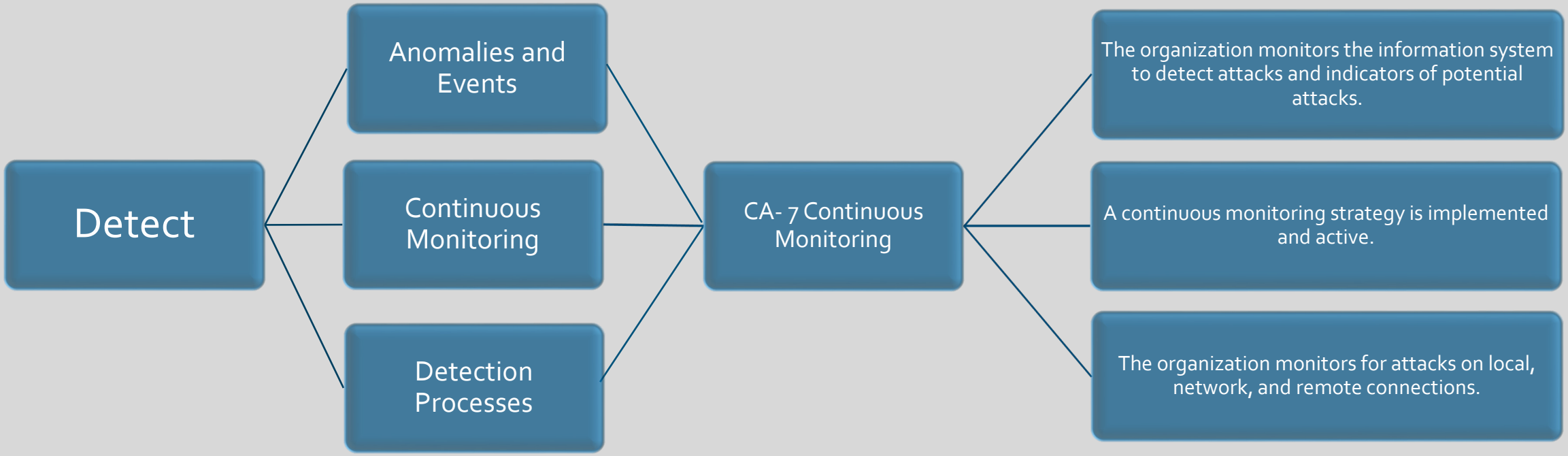
MALICIOUS FISH TANKS AND IoT

- North American Casino
- Thermostat Isolated from the network
- Transfer of 10GB outside the network to Finland (high-roller database)
- No other company device had communicated with this external location
- No other company device was sending a comparable amount of outbound data
- Communications took place on a protocol normally associated with audio and video



https://www.securityweek.com/hacked-smart-fish-tank-exfiltrated-data-rare-external-destination

DETECT


Detect
Anomalies and Events
Continuous Monitoring
Detection Processes
CA- 7 Continuous Monitoring
The organization monitors the information system to detect attacks and indicators of potential attacks.
A continuous monitoring strategy is implemented and active.
The organization monitors for attacks on local, network, and remote connections.

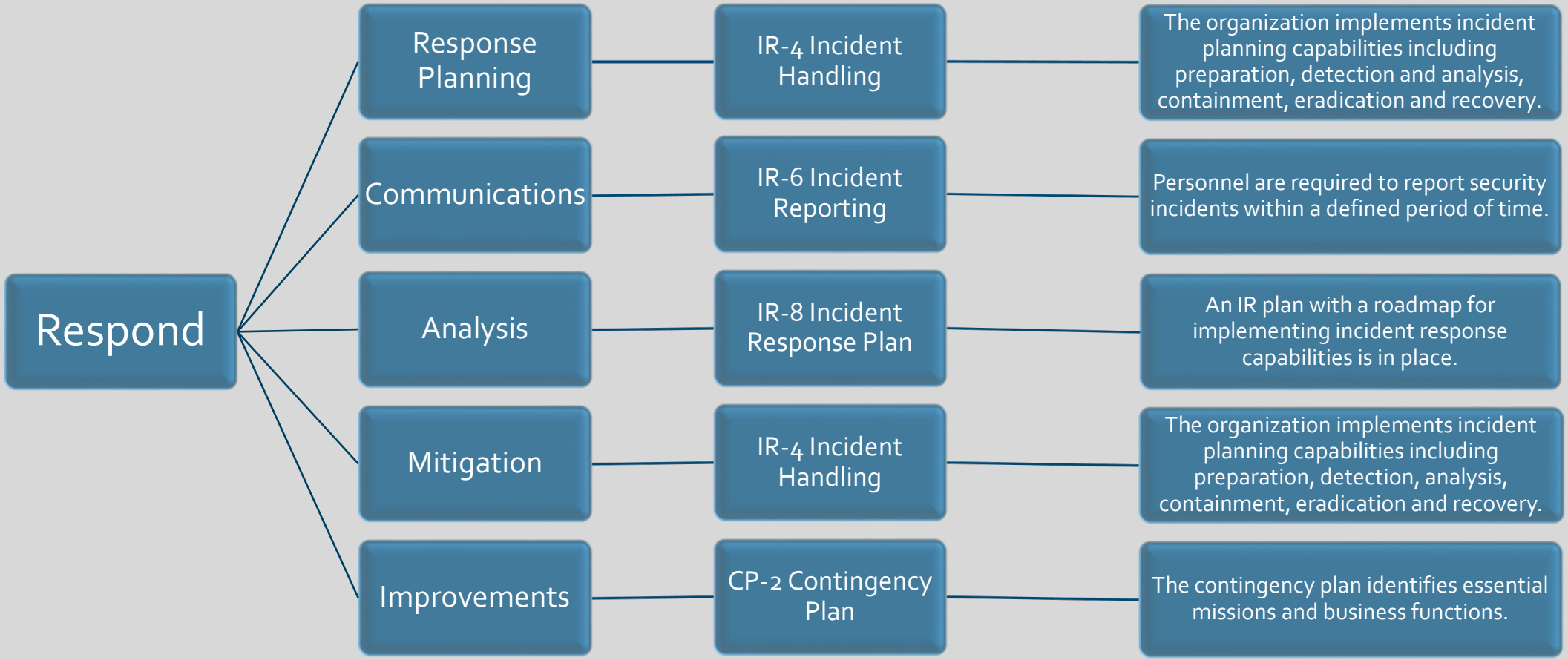
A BOTCHED RESPONSE

A BOTCHED RESPONSE

- Originally reported 500 million user accounts – underreported by another 500 million
- State-sponsored attack
- Knew of the attack in 2014 but occurred in 2013
- *"As a result, the 2014 security Incident was not properly investigated and analyzed at the time,"* Yahoo's SEC filing
- Hacker forged browser cookies
- Cost the company $350 million in its acquisition by Verizon

https://www.theverge.com/2018/4/24/17275994/yahoo-sec-fine-2014-data-breach-35-million

RESPOND


Respond
Response Planning
IR-4 Incident Handling
The organization implements incident planning capabilities including preparation, detection and analysis, containment, eradication and recovery.
Communications
IR-6 Incident Reporting
Personnel are required to report security incidents within a defined period of time.
Analysis
IR-8 Incident Response Plan
An IR plan with a roadmap for implementing incident response capabilities is in place.
Mitigation
IR-4 Incident Handling
The organization implements incident planning capabilities including preparation, detection, analysis, containment, eradication and recovery.
Improvements
CP-2 Contingency Plan
The contingency plan identifies essential missions and business functions.

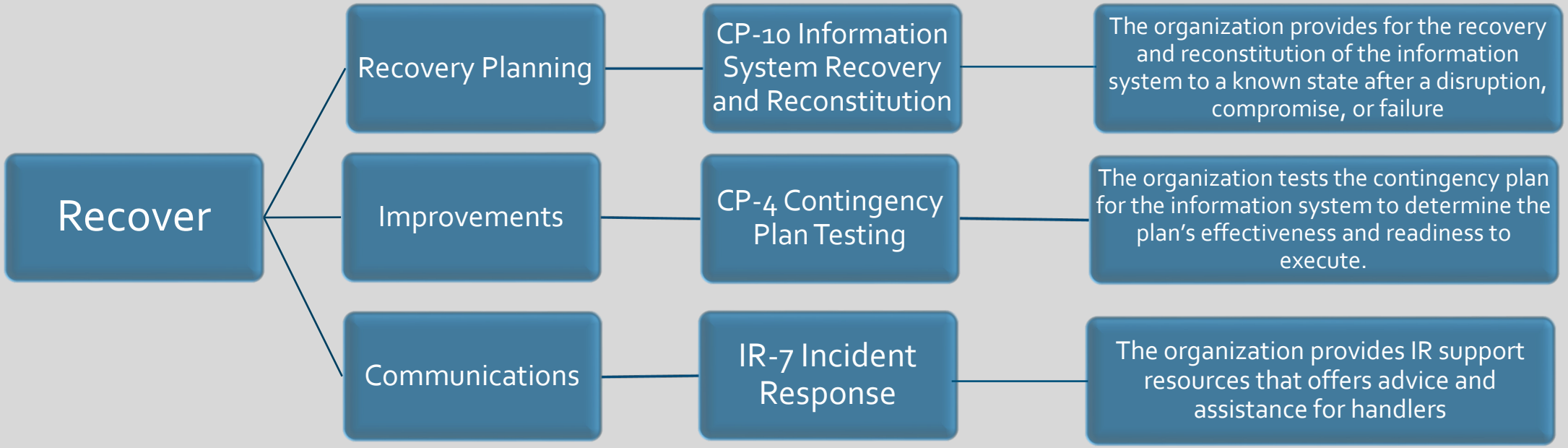
SONY PICTURES

SONY PICTURES

- Reddit post appeared stating that Sony Pictures
- had been breached
- Was carried out by a group calling themselves "The GOP", or "The Guardians Of Peace"
- A few days after the initial breach four torrent links were published that contained unreleased movies from Sony
- First leaked data summary:
  - 26.4 GB in size, containing 33,880 files and 4,864 folders
  - Includes 47,426 unique Social Security Numbers (SSN)
  - 15,232 SSN belonged to current or former Sony employees
  - 18 files contained between 10,860 and 22,533 SSN each
- Second leak data summary:
  - Photocopies and scans of driver licenses, passports and other tax related documents exposing a bunch of personal credentials, home addresses, full names, date of births, social security numbers and more.
  - Federal Tax Returns

https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

RECOVER

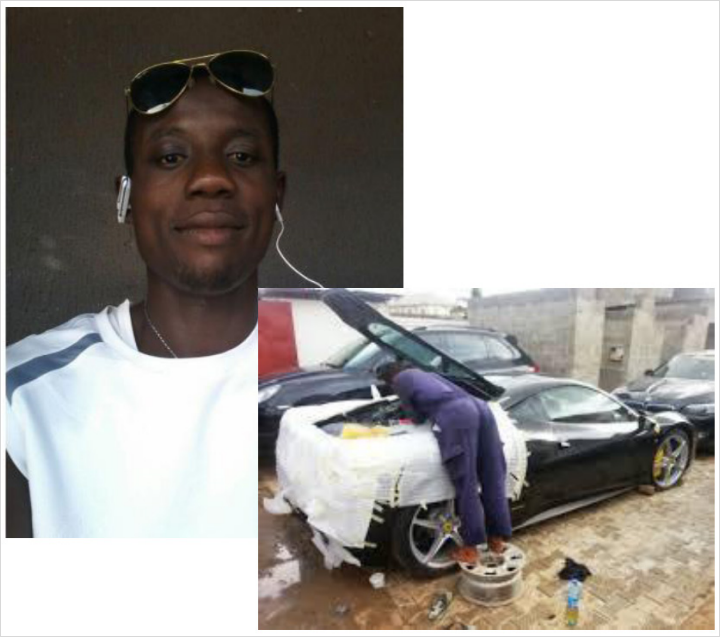

Recover
Recovery Planning
CP-10 Information System Recovery and Reconstitution
The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure
Improvements
CP-4 Contingency Plan Testing
The organization tests the contingency plan for the information system to determine the plan's effectiveness and readiness to execute.
Communications
IR-7 Incident Response
The organization provides IR support resources that offers advice and assistance for handlers

OUR RESULTS

- More executive cooperation
- Actionable remediation recommendations
- Better prioritization of remediation recommendations
- Better understanding of the client environment
- More focused audits with narrowing boundaries
- Increased client awareness
- More collaborative audit process
- More knowledgeable audit staff

NEXT STEPS

- **Ignore marketing - We're not "at war"**
- Develop an intellectual curiosity
- Develop sources of information
- Be willing to build relationships
- Obtain a basic understand of computing principals
- Don't become overwhelmed
- Don't forget the human factor!



Name:	Mike Gab
Age:	30 yo
Gender:	Male
POB:	Nnewi, Nigeria
Current:	Satellite Town, Lagos, Nigeria