Unit #12

Incident and Disaster Response

MIS 5214

Agenda

- Computer virus
- Malicious software
    - Proliferation of malware
    - Malware components
    - Anti-malware components
    - Best practices for protection
- Business Continuity and Disaster Contingency Planning
- Incident Response Planning
- Final Project Schedule

Virus

Virus: attached to a file

1986

Brain virus

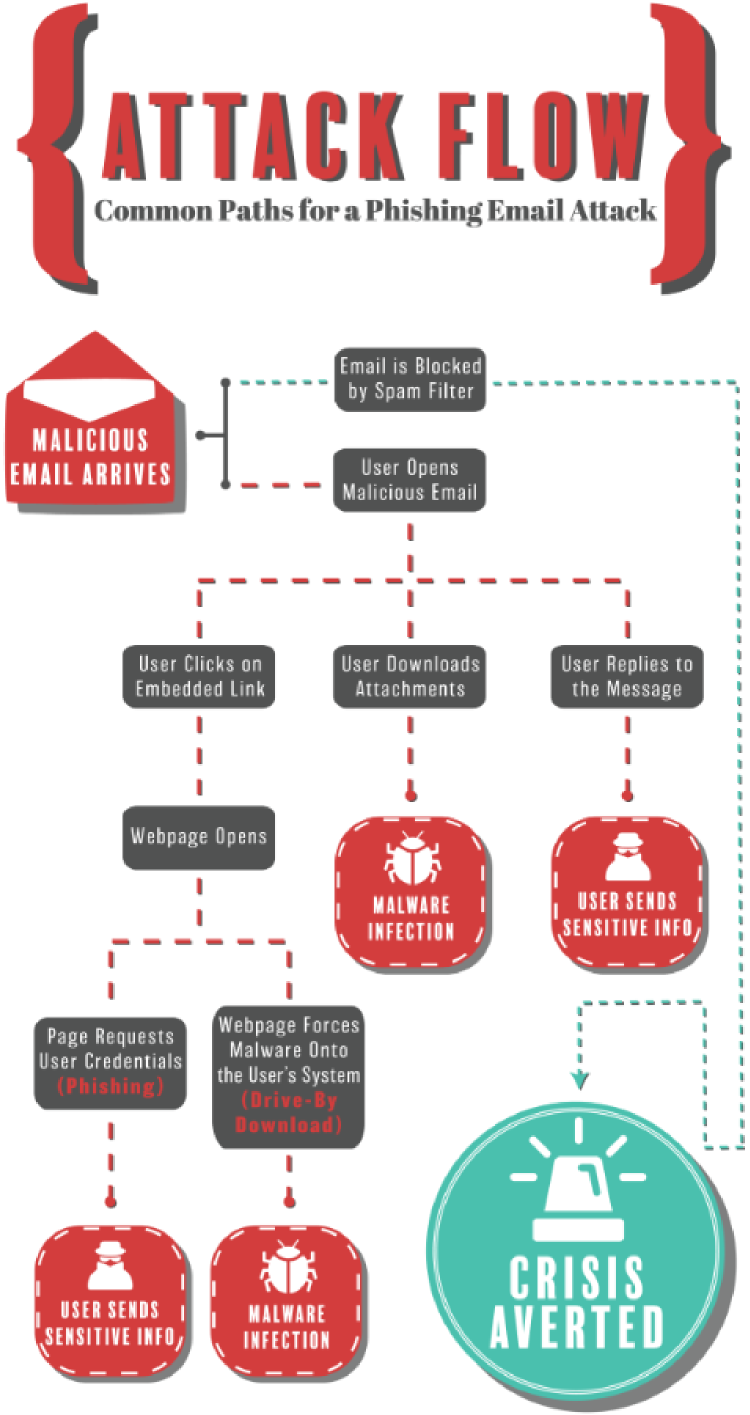
an F-Secure Production

Malicious Software (Malware)

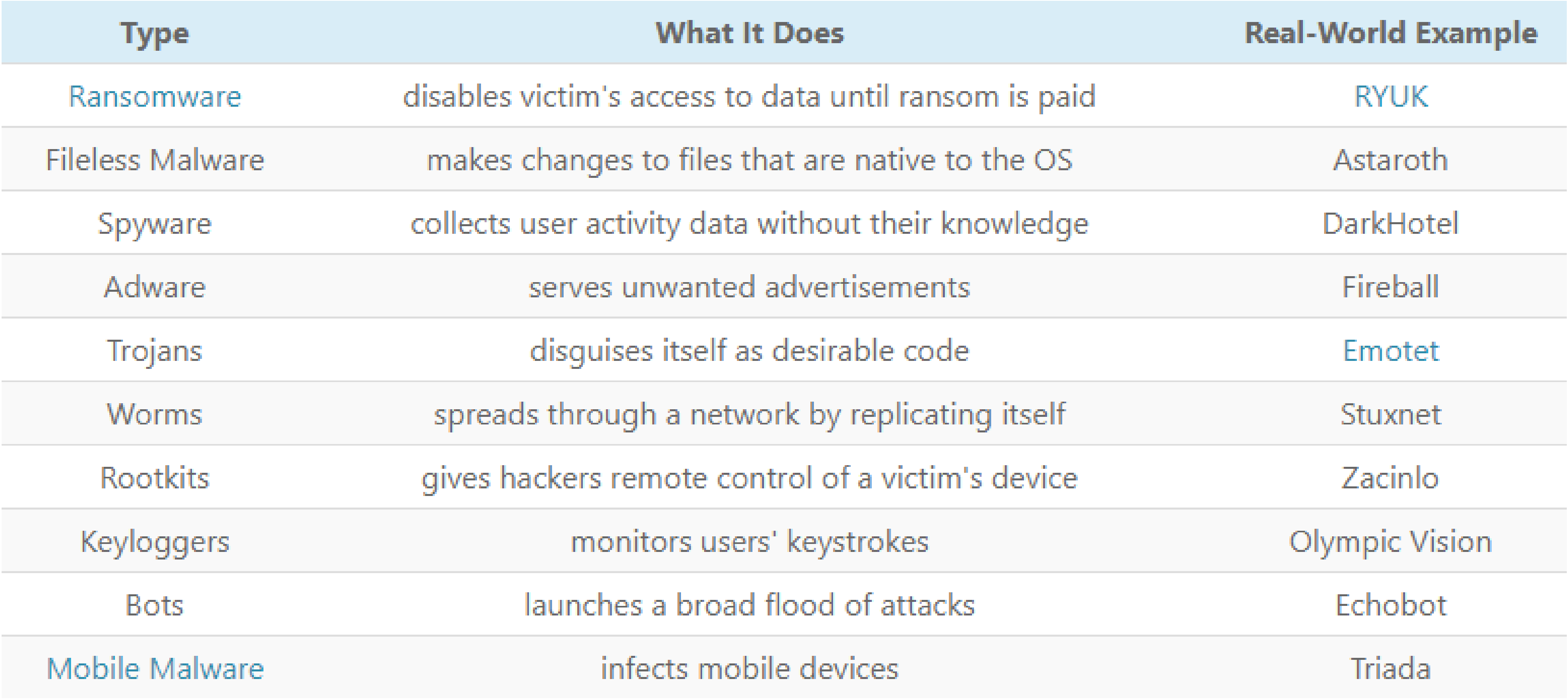
Malware enables unauthorized access to networks for purposes of theft, sabotage, or espionage

- There are many types of malware, many cyberattacks use a combination of several types to achieve their goals
  - Obtain sensitive information (login credentials, credit card data, Social Security numbers, …)
  - Gain unauthorized access to systems
  - Carry out a profit-oriented scheme
- Usually introduced into a network through phishing, attachments, downloads, or may gain access through social engineering or flash drives
- Manual attacks on information systems are less common than the used to be

  >95% of all compromises use email as the main attack vector

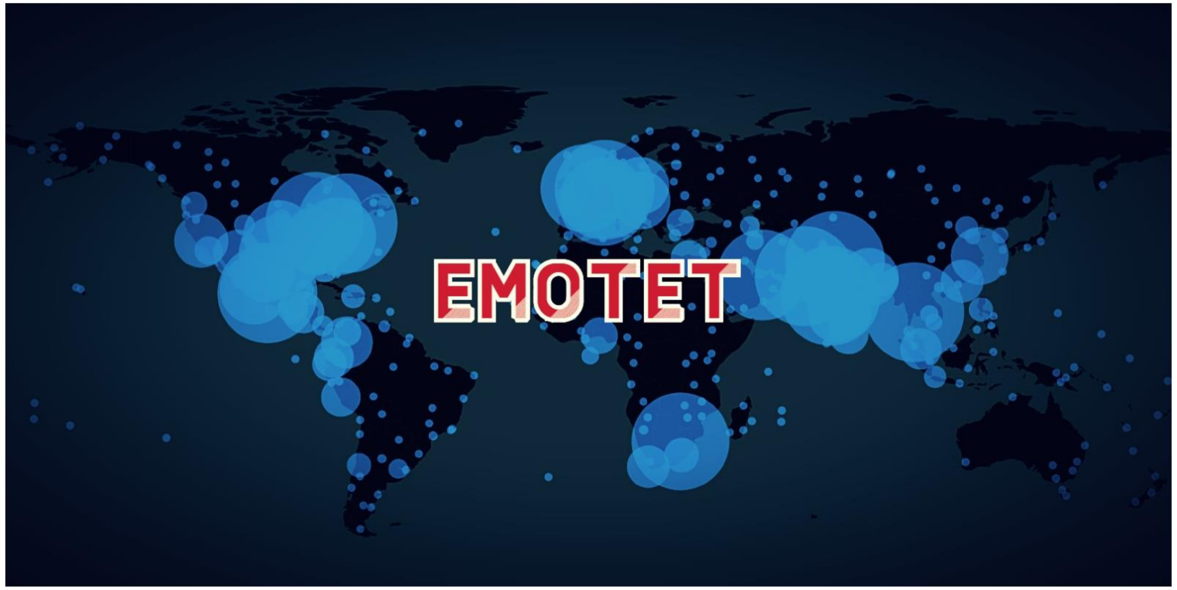

ATTACK FLOW
Common Paths for a Phishing Email Attack
MALICIOUS EMAIL ARRIVES
Email is Blocked by Spam Filter
User Opens Malicious Email
User Clicks on Embedded Link
User Downloads Attachments
User Replies to the Message
Webpage Opens
MALWARE INFECTION
USER SENDS SENSITIVE INFO
Page Requests User Credentials (Phishing)
Webpage Forces Malware Onto the User's System (Drive-By Download)
USER SENDS SENSITIVE INFO
MALWARE INFECTION
CRISIS AVERTED

Common types of malware



Type	What It Does	Real-World Example
Ransomware	disables victim's access to data until ransom is paid	RYUK
Fileless Malware	makes changes to files that are native to the OS	Astaroth
Spyware	collects user activity data without their knowledge	DarkHotel
Adware	serves unwanted advertisements	Fireball
Trojans	disguises itself as desirable code	Emotet
Worms	spreads through a network by replicating itself	Stuxnet
Rootkits	gives hackers remote control of a victim's device	Zacinlo
Keyloggers	monitors users' keystrokes	Olympic Vision
Bots	launches a broad flood of attacks	Echobot
Mobile Malware	infects mobile devices	Triada

https://www.crowdstrike.com/epp-101/types-of-malware/



Emotet is a notorious malware distributed through email containing malicious Microsoft Word and Excel document attachments. When users open these documents and macros are enabled, the Emotet DLL will be downloaded and loaded into memory.

Once Emotet is loaded, the malware will sit quietly, waiting for instructions from a remote command and control server.

Eventually, the malware will steal victims' emails and contacts for use in future Emotet campaigns or download additional payloads such as Cobalt Strike or other malware that commonly leads to ransomware attacks.

While Emotet has been considered the most distributed malware in the past, it has gradually slowed down, with its last spam operation seen in November 2022. However, even then, the spamming only lasted two weeks.

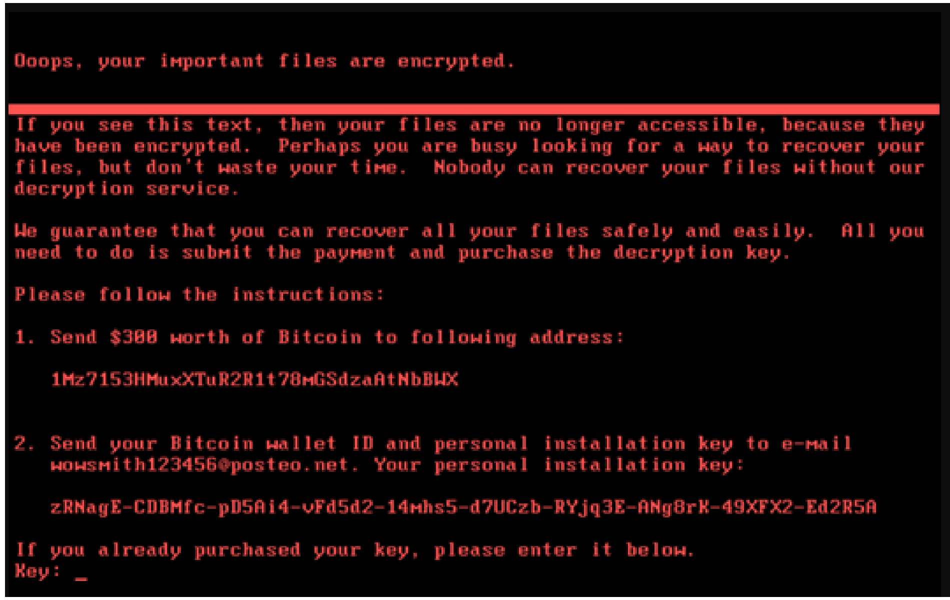
Emotet returns in 2023

Today, cybersecurity firm Cofense and the Emotet-tracking group Cryptolaemus warned that the Emotet botnet had once again resumed sending emails.

Ransomware

Software that uses encryption to disable a target’s access to its data until a ransom is paid

- The victim organization is rendered partially or totally unable to operate until it pays
- There is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

In 2019 the city of Baltimore was hit by a type of ransomware named RobbinHood which was distributed using the National Security Agency’s Eternal Blue hacking tool

- The attack halted all city activities, including tax collection, property transfers, and government email for weeks, and cost the city more than $18 million

- The same type of malware was used against the city of Atlanta in 2018, resulting in costs of $17 million

Fileless Malware

- Does not install anything initially, instead, it makes changes to files that are native to the operating system, such as PowerShell
  - Because the operating system recognizes the edited files as legitimate, a fileless attack is not caught by antivirus software
  - Because these attacks are stealthy, they are up to 10 times more successful than traditional malware attacks

Astaroth is a fileless malware

- When users downloaded the file, a Windows Management Instrumentation (WMI) tool was launched, along with other legitimate Windows tools
- These tools downloaded additional code that was executed only in memory, leaving no evidence that could be detected by vulnerability scanners
- Then the attacker downloaded and ran a Trojan that stole credentials and uploaded them to a remote server

Malware proliferation is directly related to profit hackers can make without being caught

Money making schemes include:

- Compromising systems with botnets for later use in:
  - Distributed denial of service (DDoS) attacks
  - Spam distribution
- Ransomware encrypting users’ files with keys that are only given after users pay a ransom
- Spyware collects personal data for resale
- Redirecting web traffic pointing people to a specific product for purchase
- Installing key loggers, which collect financial information for reuse
- Carrying out phishing attacks, fraudulent activities, identity theft, and information warfare

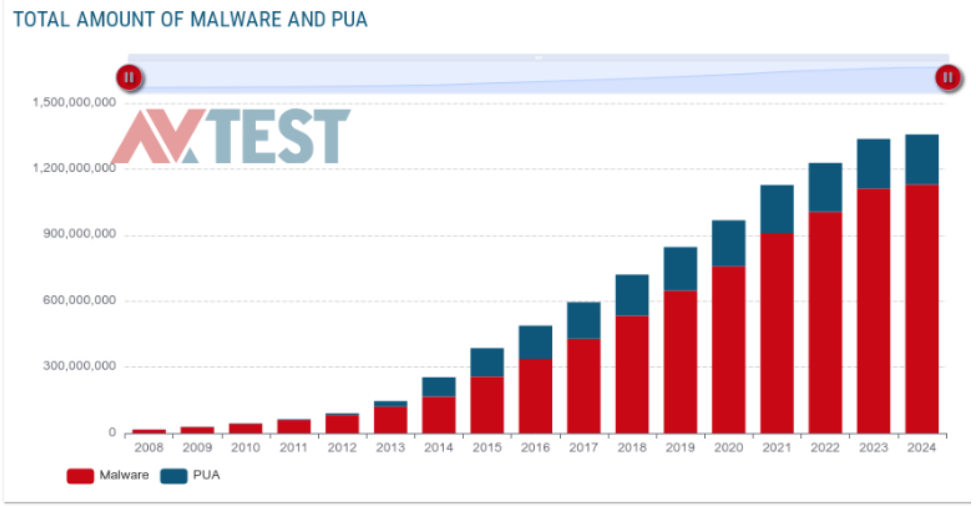
Malware is increasing

AVTest reports over 450,000 new malware and potentially unwanted applications (PUA) identified each day

Main reasons types malware is increasing in quantity and potency:

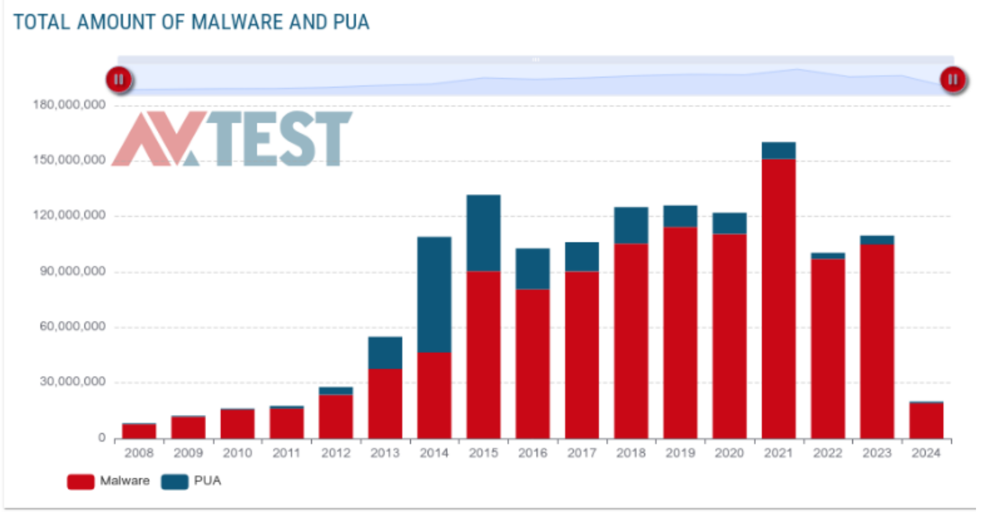
- Homogenous computer environments (Windows, MacOS, Android, iOS) – 1 piece of malware will work on many/most devices
- Everything is becoming a computer capable of being compromised (phones, TVs, game consoles, power grids, medical devices,…)
- More people and companies store all their data in digital format
- Many accounts are configured with too much privilege (i.e. root/administrator access)
- More people who do not understand technology are using it for sensitive purposes (i.e. e-commerce, online banking, …)

Total malware



Source: av-atlas.org

New malware



Source: av-atlas.org

https://www.av-test.org/en/statistics/malware/

Malware Components

Malware typically has 6 common elements

1. **Insertion** – Installs itself on the victim’s computer
2. **Replication** – Copies itself and spreads to other victims
3. **Avoidance** – Uses methods to avoid being detected
4. **Trigger** – An event initiates its payload execution
5. **Payload** - Caries out its function (i.e. exploits a vulnerability to provide access, deletes files, encrypts files, installs a backdoor, …)
6. **Eradication** – Removes itself after its payload is executed

Anti-malware software components

Detection techniques

- Signature-based
- Integrity-based
- Heuristic-based
- Behavior-based

Protection techniques

- Quarantine the file
- Clean the file
- Roll-back to prior version of the file
- Warn the user
- Log the event

Signature-based malware detection

Anti-malware software scans files, e-mail, other data and **compares** them **to a database of signatures** created by the anti-malware vendor

- A malware signature is a sequence of code extracted from the virus that is used to identify the virus
- Can only identify previously identified malware
- Updates to the signatures must be downloaded and applied frequently
- Cannot detect 0-day attacks

Signature-based malware detection avoidance

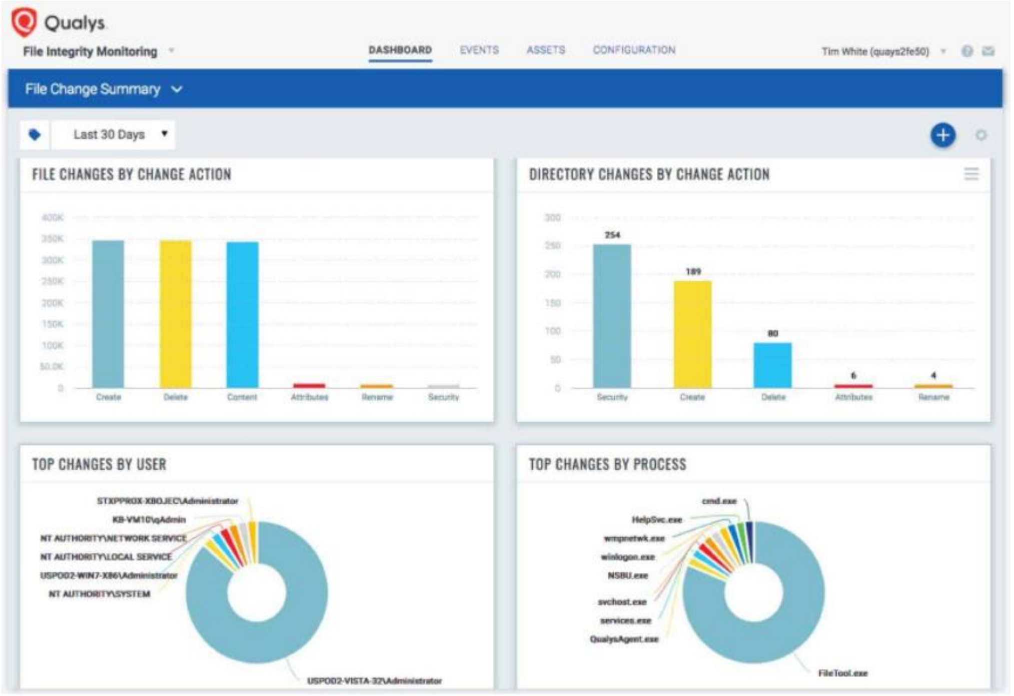
Polymorphic virus has the capability to change its own code to produce thousands of varied operational versions of itself

- Can use different encryption techniques
- Can vary the sequence of their instructions
    - Combining noise or bogus instructions with the useful instructions
    - Using a mutation engine and a random-number generator to change the sequence of their instructions

Multi-part virus distributes its components to different parts of the system

Integrity-based malware detection

- Calculates and stores a hash for each component of the system: operating system files, application files, configuration files, …
- Each new scan of the system calculates a hash for each component and compares it with the stored hash to detect differences
- Detected differences send alters and are flagged as suspect for further analysis



Heuristic-based malware detection

Analyzes the overall structure of the malicious code, evaluating

- Coded logic, instructions, functions and modules
- Data types and structures

Assesses likelihood that the code is malicious by accumulating a scored rating of “suspiciousness”

- Increases as it finds more potentially malicious attributes
- Compared to a threshold, which when crossed the detector identifies the software as malware and the protections are activated

2 types of heuristic malware detection methods

1. Static analysis – Reviewing code without running it
2. Dynamic analysis – Reviewing code’s behavior as it is running

Behavior-based malware detection

Allows suspicious code to execute within the unprotected operating system, and watches its interaction with the operating system components looking for suspicious activities:

- Writing to Run and RunOnce keys in the Windows Registry or startup files
  - These make a program run when a user logs on
    - Run key makes the program run every time the user logs on
    - RunOnce key makes the program run one time, and then the key is deleted
- Opening, deleting, or modifying files
- Modifying executable logic
- Creating or modifying macros and scripts
- Scripting e-mail messages to send executable code
- Connecting to network shares or resources
- Formatting a hard drive or writing to the boot sector

Anti-malware software components

Detection techniques

- Signature-based
- Integrity-based
- Heuristic-based
- Behavior-based

Proactive techniques able to detect new malware (i.e. 0-day attacks)

Protection techniques

- Quarantine the file
- Clean the file
- Roll-back to prior version of the file
- Warn the user
- Log the event

Best practices against malware attacks

User Education

Training users on best practices can go a long way in protecting an organization

- How to avoid malware
  - Don’t download and run unknown software
  - Don’t blindly insert “found media” into your computer
- How to identify potential malware
  - Phishing emails
  - Unexpected applications/processes running on a system

https://www.rapid7.com/fundamentals/malware-attacks/

Best practices against malware attacks

Use Reputable Anti-Virus (A/V) Software

- When installed, a suitable A/V solution will detect (and remove) any existing malware on a system, as well as monitor for and mitigate potential malware installation or activity while the system is running. It'll be important to keep it up-to-date with the vendor's latest definitions/signatures.

Ensure Your Network is Secure

- Control access to systems on the organization's network
- Use of proven technology and methodologies—such as using a firewall, IPS, IDS
- Remote access only through VPN—will help minimize the attack "surface" your organization exposes

Regular Website Security Audits

- Scan the organization's websites regularly for vulnerabilities
  - Software with known bugs and server/service/application misconfiguration
  - Detect if known malware has been installed

Create Regular, Verified Backups

- Have regular (i.e. current and automated) offline backup
- Make sure they are verified to be happening on the expected regular basis and are usable for restore operations
  - Old, outdated backups are less valuable than recent ones
  - Backups that don't restore properly are of no value

https://www.rapid7.com/fundamentals/malware-attacks/

AV-TEST Awards for Anti- Malware, Botnets, Ransomware and APT groups

Criteria:

- Protection
- Performance
- Usability

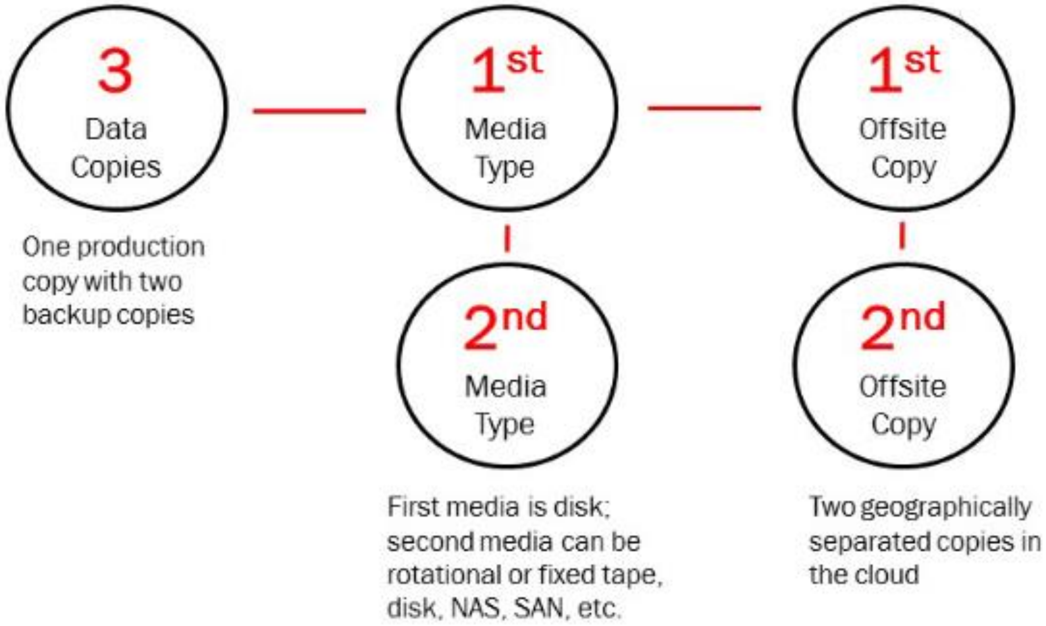
Platforms

- Windows
- Android
- MacOS

Mitigation – Backup Best Practice

Three-Two-One rule

- Make 3 copies of all mission critical software and corresponding data in 2 different formats (to run on Linux and Windows machines), with 1 copy stored off-site not connected to any network

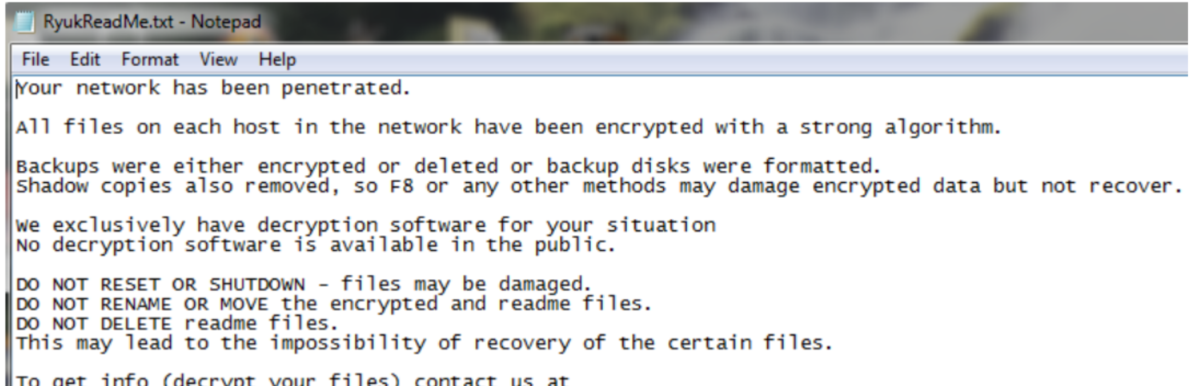

3
Data Copies
One production copy with two backup copies
1st
Media Type
2nd
Media Type
First media is disk; second media can be rotational or fixed tape, disk, NAS, SAN, etc.
1st
Offsite Copy
2nd
Offsite Copy
Two geographically separated copies in the cloud

Agenda

- ✓Computer virus
- ✓Malicious software
  - ✓Proliferation of malware
  - ✓Malware components
  - ✓Anti-malware components
  - ✓Best practices for protection
- Business Continuity and Disaster Contingency Planning
- Incident Response Planning
- Team Project Q&A

Disaster Context

- *Disruptions to operations can occur with or without warning*
- *Results may be predictable or unanticipated*



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
WayneEvenson@protonmail.com
or
WayneEvenson@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe
```

***The first priority is always the safety of the people**:*

- *Employees*
- *Service and Support Staff*
- *Visitors*

Business Continuity

Capability to continue service delivery at acceptable levels following" natural or human-induced disaster

Source: International Standards Organization 22300:2018

Security and resilience - Vocabulary

Resiliency

"Capacity to recover quickly from difficulties

...

Antonyms:

- Vulnerability, weakness…"

Source: https://www.lexico.com/en/synonym/resilience

To assure resilient response

Business Continuity Plan (BCP)

Documented procedures for recovering and resuming critical operational functions following significant disruption

Source: ISO 22301:2012
Societal security – Business continuity management systems - Requirements

…includes a Disaster Recovery Plan (DRP)

Procedures for relocating critical information systems operations to an alternative site following significant disruption

…includes an Incident Recovery Plan (IRP)

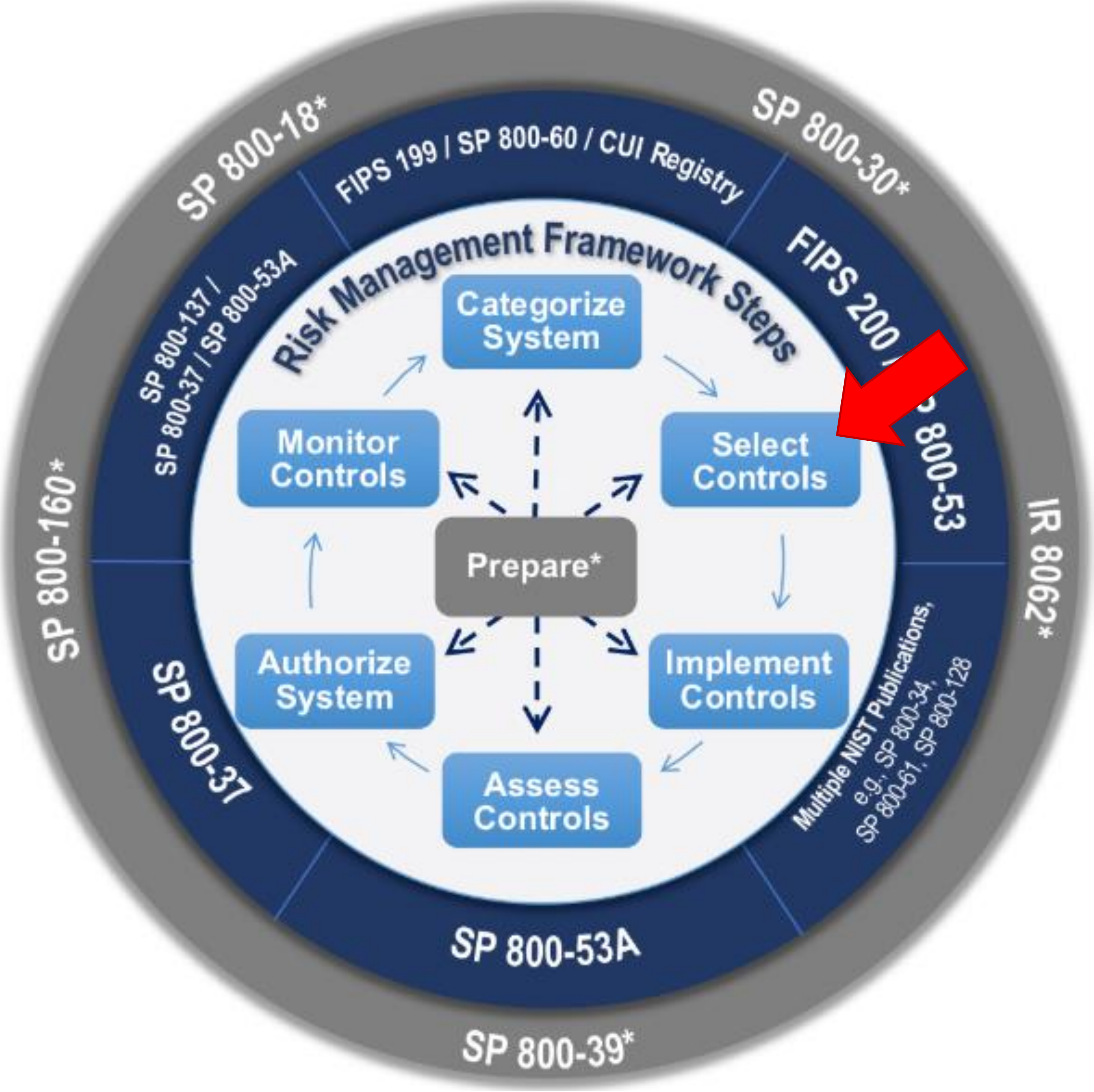
Countermeasures that mitigate the risks of an active data breach

Our Disaster Recovery Plan Goes Something Like This...
HELP! HELP!

NIST

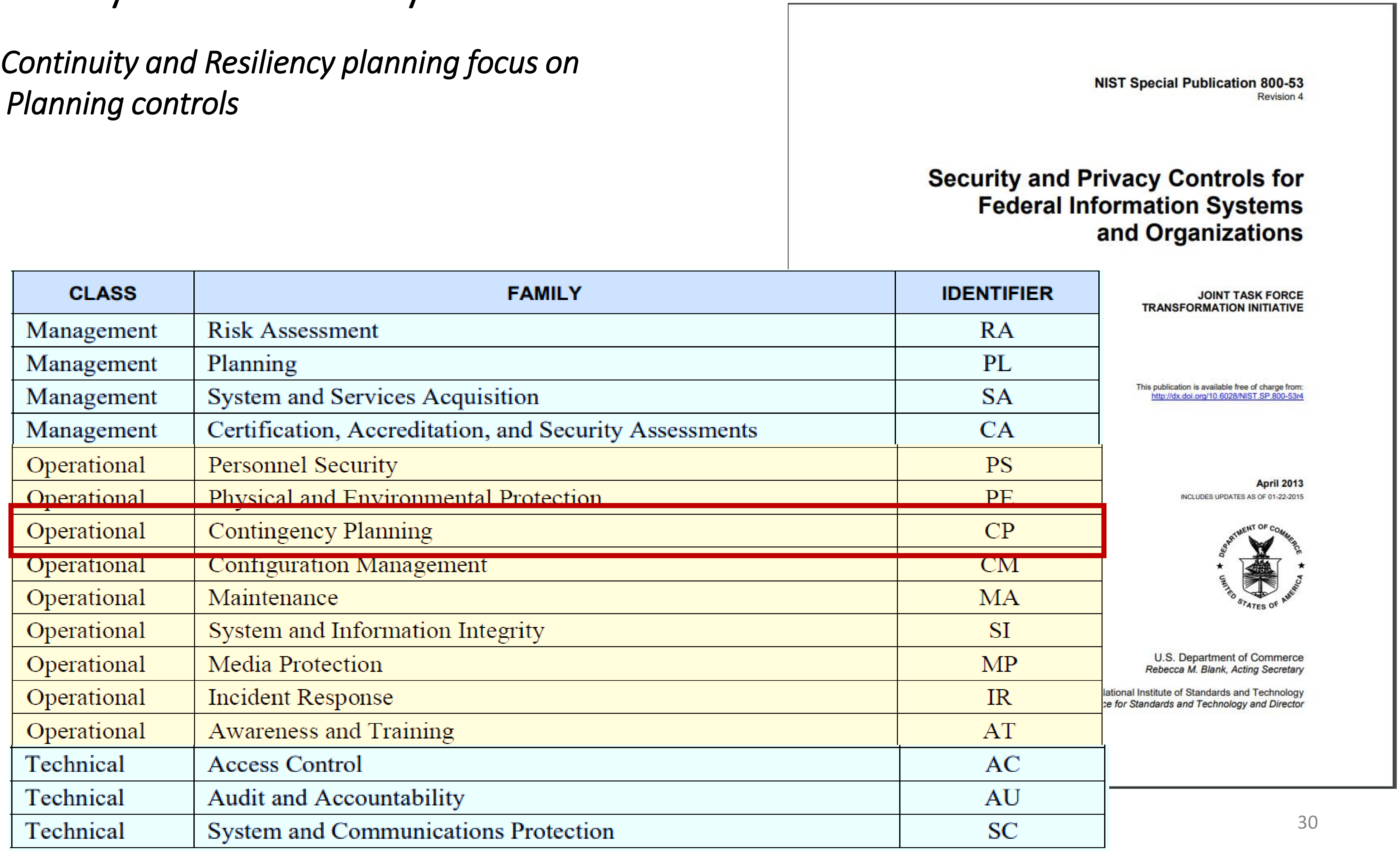
National Institute of Standards and Technology

U.S. Department of Commerce



Catalog of cyber-security controls

for Business Continuity and Resiliency planning focus on Contingency Planning controls



CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

April 2013
INCLUDES UPDATES AS OF 01-22-2015

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

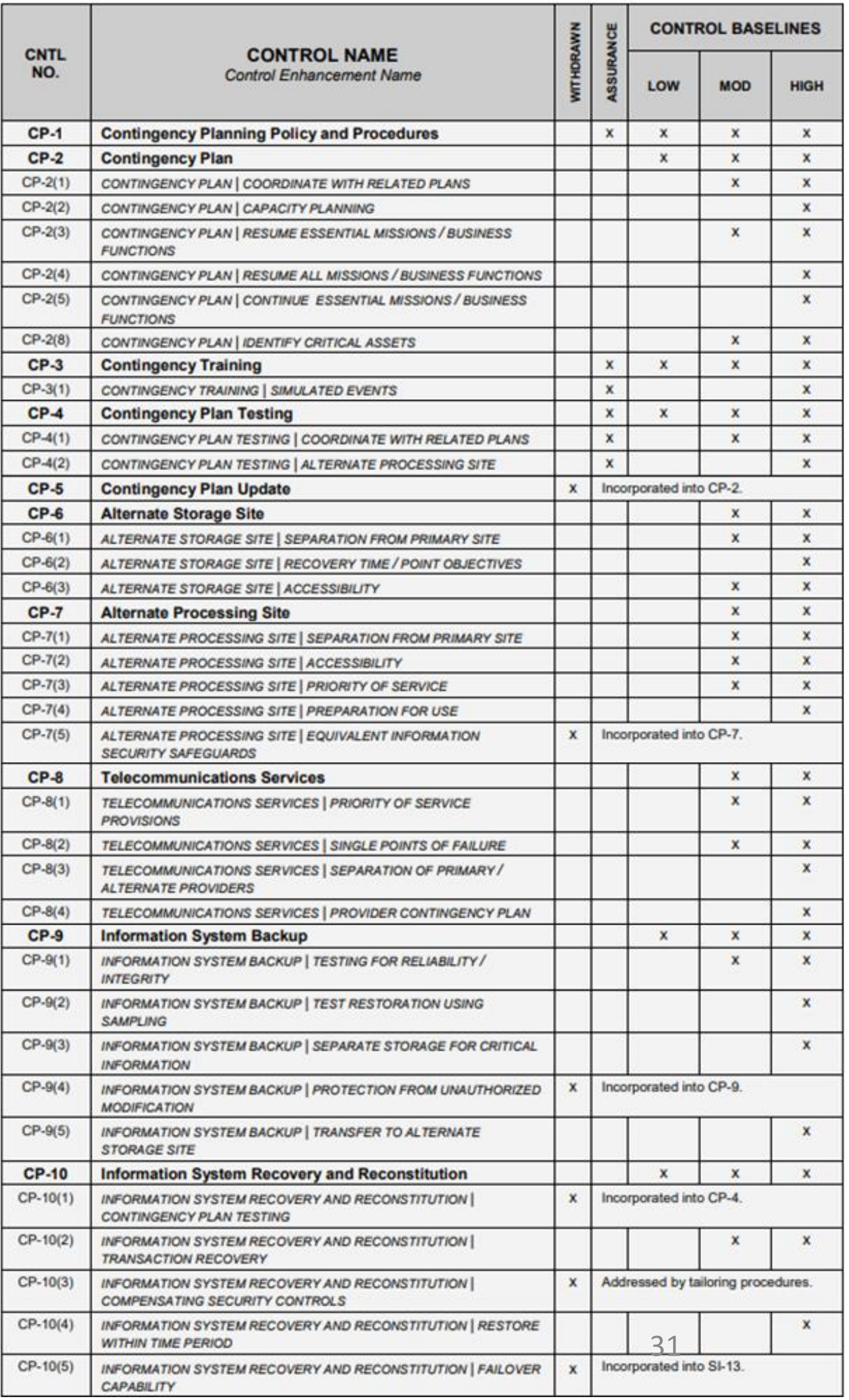
U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

lational Institute of Standards and Technology
ce for Standards and Technology and Director

Contingency Planning Controls

CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information System Recovery and Reconstitution	X	X	X

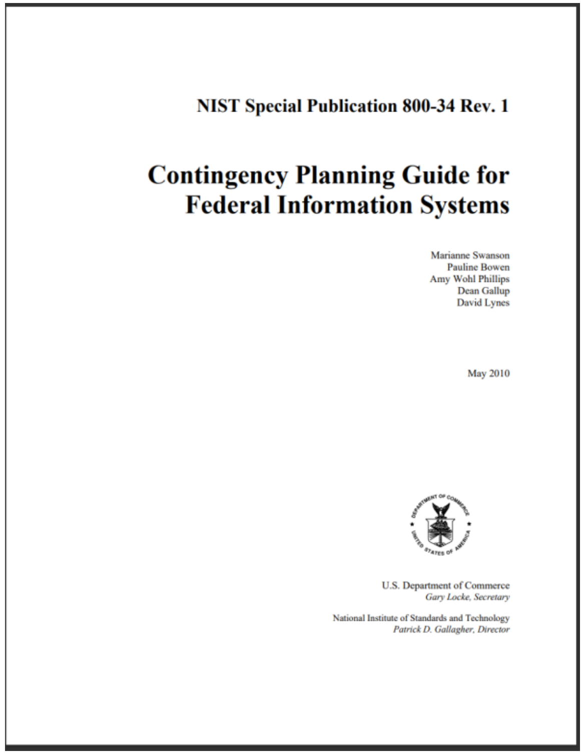
NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations"



CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2(3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2(4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3(1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4(1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4(2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6(2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6(3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7(1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7(2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7(3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7(4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7(5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-8	**Telecommunications Services**				x	x
CP-8(1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8(2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8(3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8(4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-9	**Information System Backup**			x	x	x
CP-9(1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x
CP-9(2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9(3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9(4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9(5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10(1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10(3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10(4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10(5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			

3-Phases in a Contingency Plan

All dependent on a BIA “Business Impact Analysis”



NIST Special Publication 800-34 Rev. 1

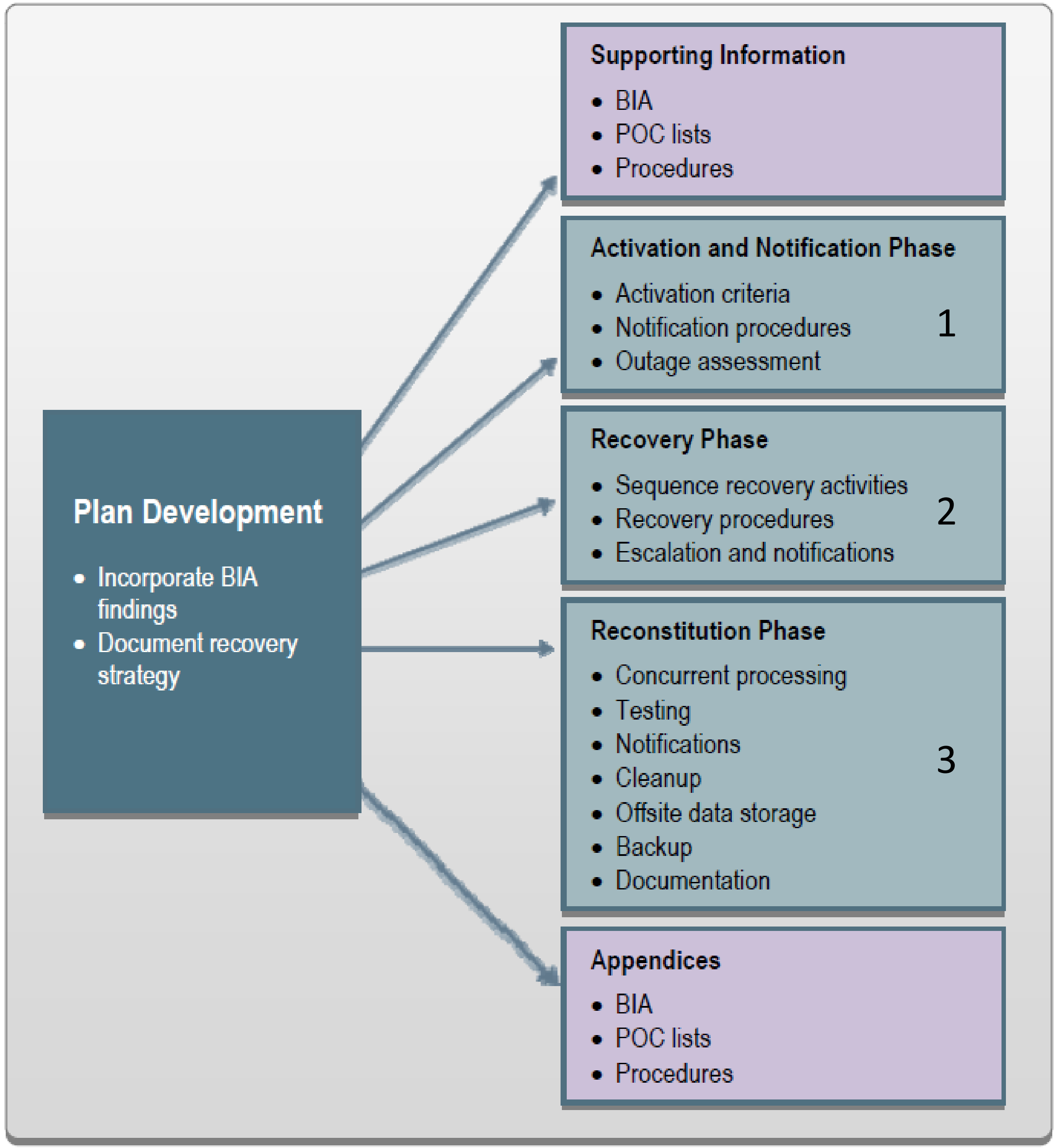
Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

May 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director



Plan Development

- Incorporate BIA findings
- Document recovery strategy

Supporting Information

- BIA
- POC lists
- Procedures

Activation and Notification Phase 1

- Activation criteria
- Notification procedures
- Outage assessment

Recovery Phase 2

- Sequence recovery activities
- Recovery procedures
- Escalation and notifications

Reconstitution Phase 3

- Concurrent processing
- Testing
- Notifications
- Cleanup
- Offsite data storage
- Backup
- Documentation

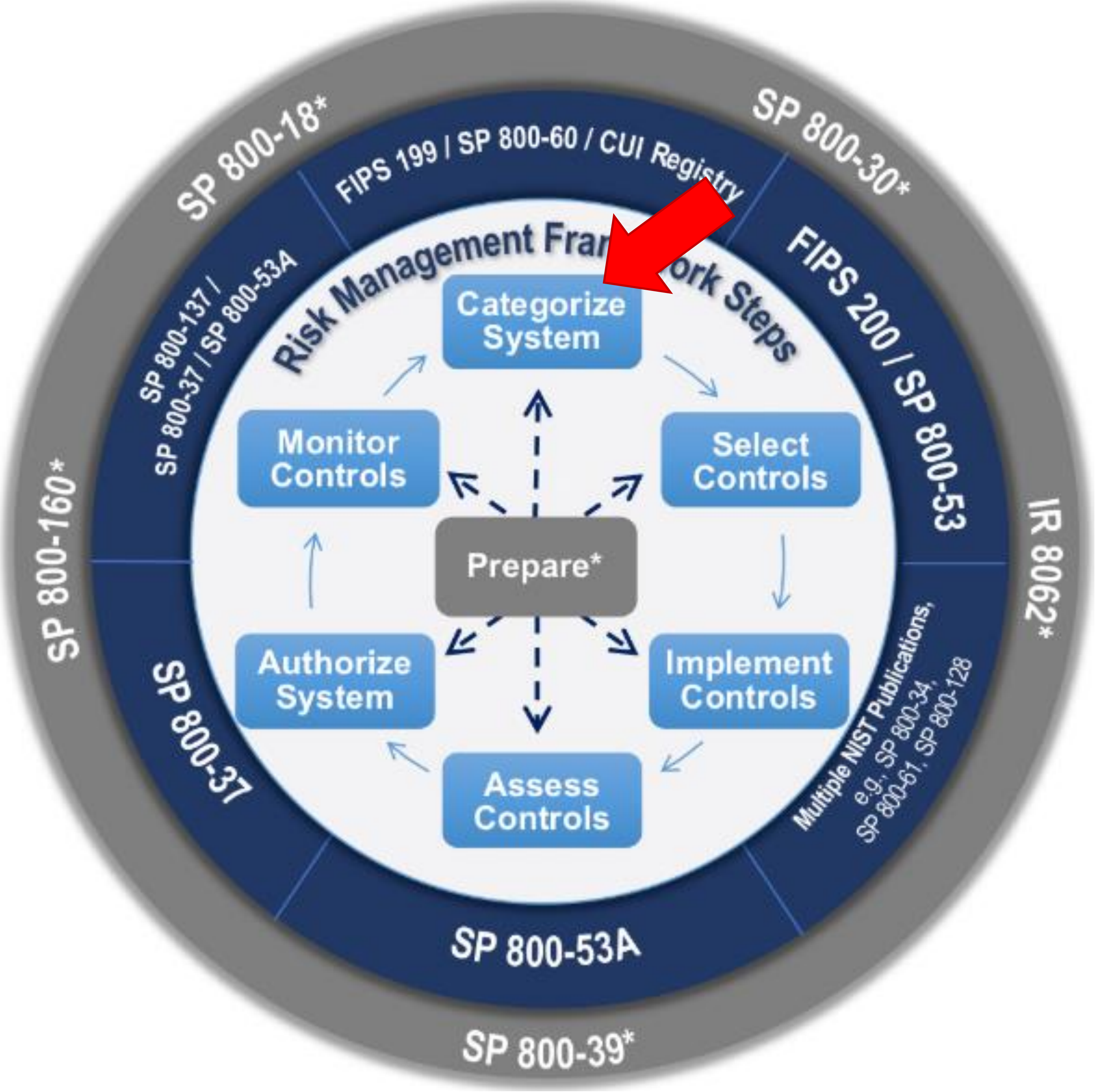
Appendices

- BIA
- POC lists
- Procedures

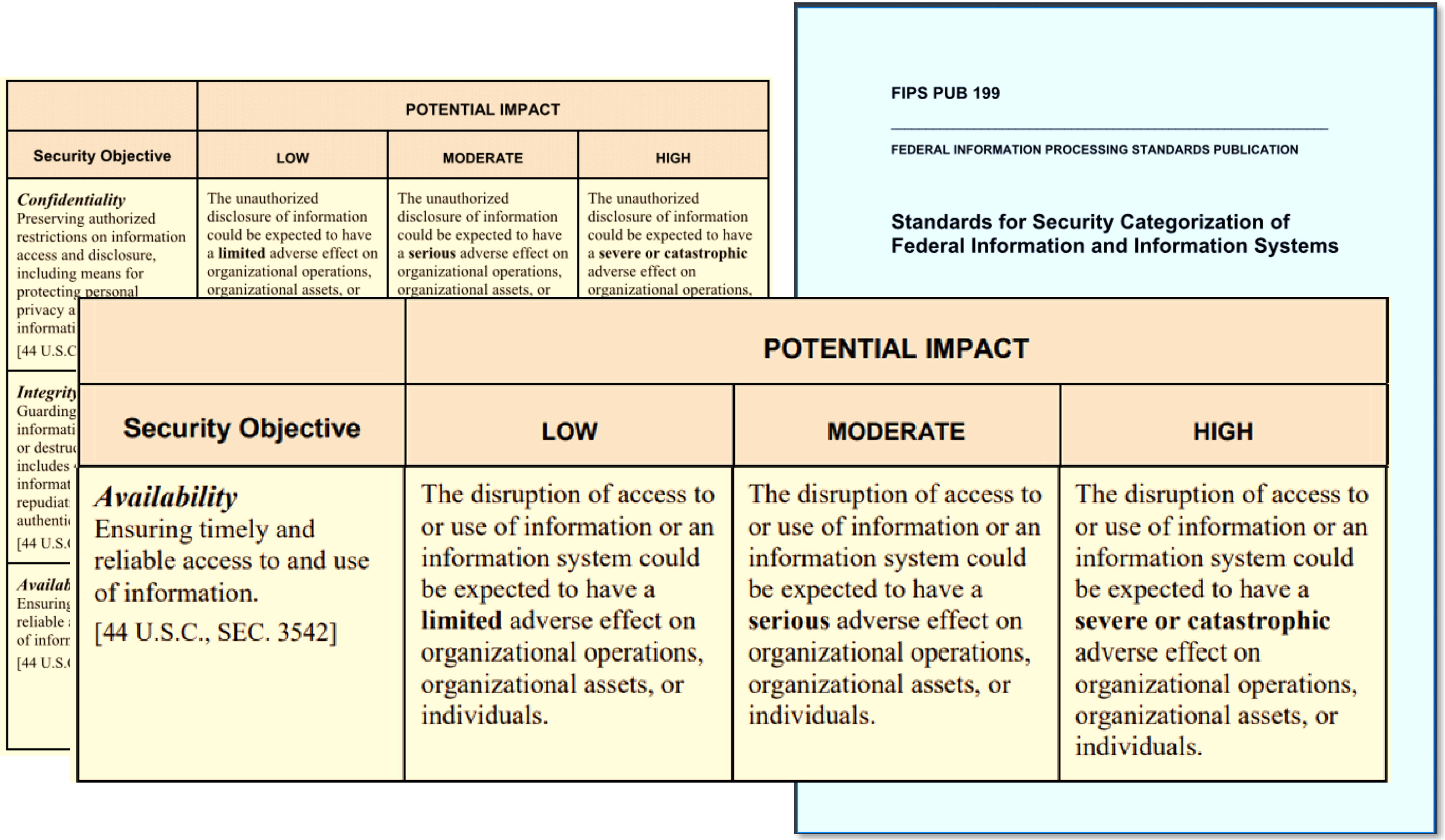
NIST SP 800-34 R1 – Contingency Planning Guide for Federal Information Systems

National Institute of Standards and Technology
U.S. Department of Commerce

Categorizing information systems enables us to understand the priority for recovery…



Impact on which security objective determines priorities for recovery?



	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy a informati [44 U.S.C	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations,
Integrity Guarding informati or destruc includes informat repudiat authenti [44 U.S.(			
Availab Ensuring reliable of inforr [44 U.S.(			

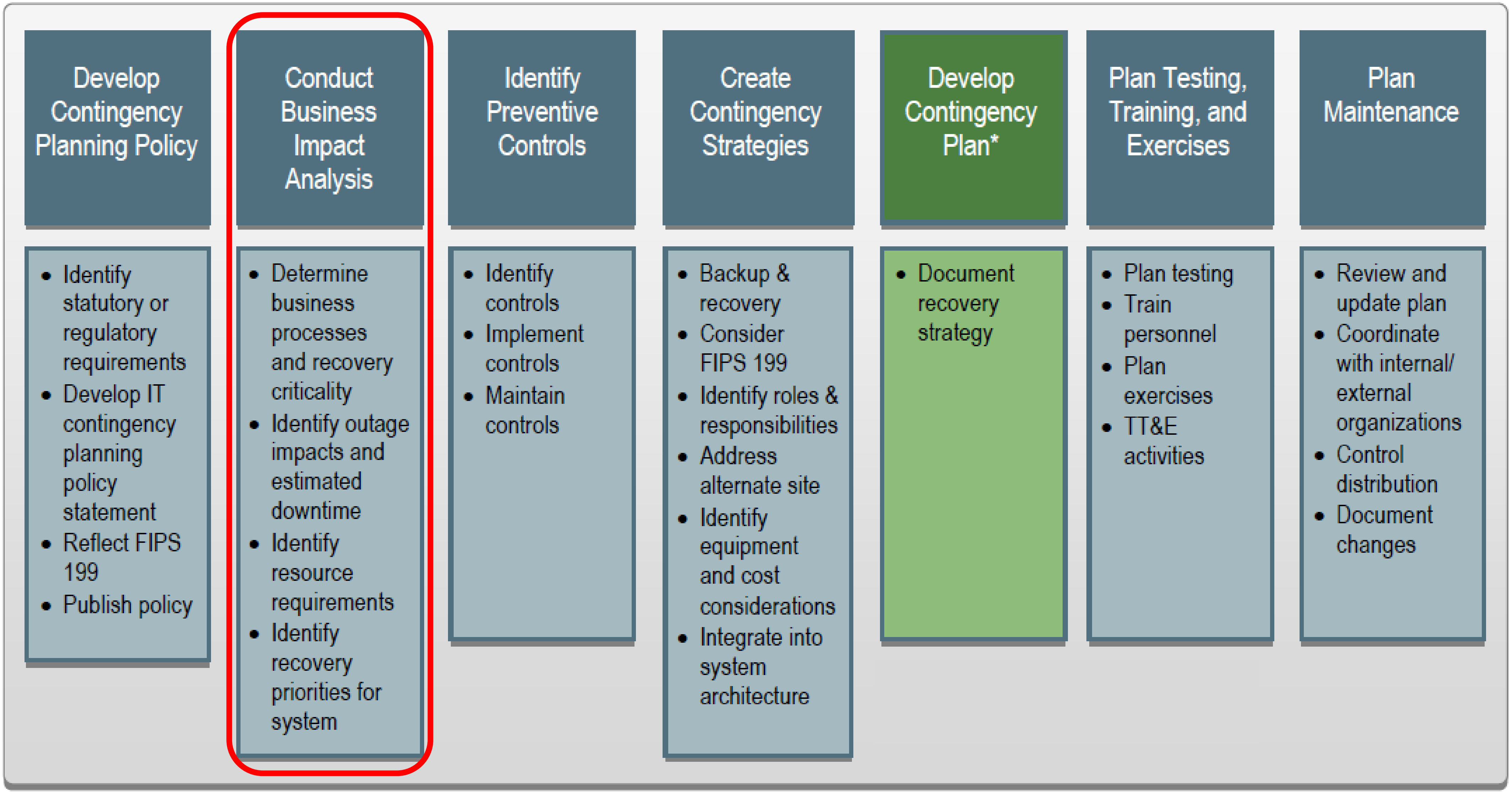
FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Plan is based on “recovery priorities”



Develop Contingency Planning Policy	Conduct Business Impact Analysis	Identify Preventive Controls	Create Contingency Strategies	Develop Contingency Plan*	Plan Testing, Training, and Exercises	Plan Maintenance
• Identify statutory or regulatory requirements • Develop IT contingency planning policy statement • Reflect FIPS 199 • Publish policy	• Determine business processes and recovery criticality • Identify outage impacts and estimated downtime • Identify resource requirements • Identify recovery priorities for system	• Identify controls • Implement controls • Maintain controls	• Backup & recovery • Consider FIPS 199 • Identify roles & responsibilities • Address alternate site • Identify equipment and cost considerations • Integrate into system architecture	• Document recovery strategy	• Plan testing • Train personnel • Plan exercises • TT&E activities	• Review and update plan • Coordinate with internal/ external organizations • Control distribution • Document changes

NIST SP 800-34 R1 – Contingency Planning Guide for Federal Information Systems

Business Impact Analysis (BIA) Answers

1. What are the work processes？
2. How critical is each？
3. What data, applications, and people are needed to run each critical process？
4. What are the priorities for recovering information systems after disruption？

5. For each critical IT resource, what are:
   - **Recover time objective** (RTO):

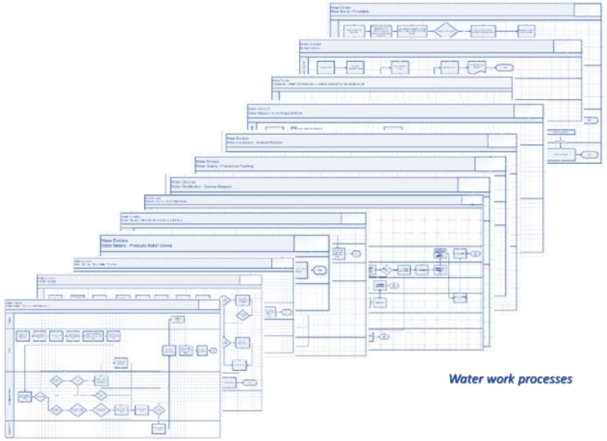
     Maximum acceptable downtime

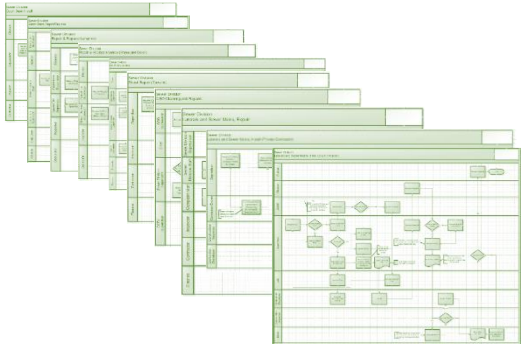
   - **Recovery point objective** (RPO):

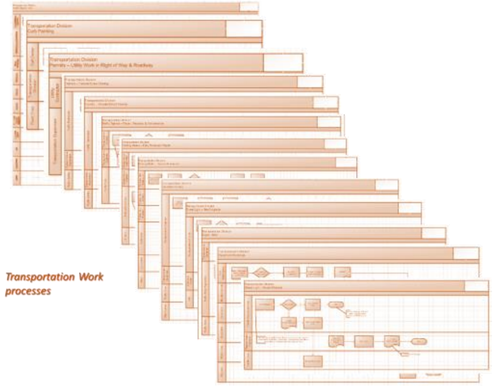
     Maximum acceptable data loss (measured in time, but implies # of data records)

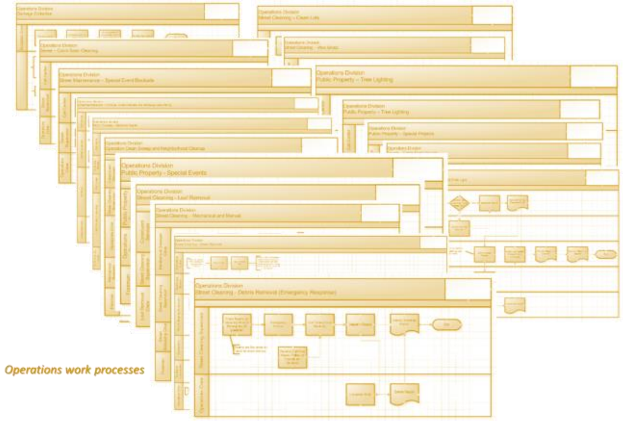
Prerequisite for BIA and contingency planning…

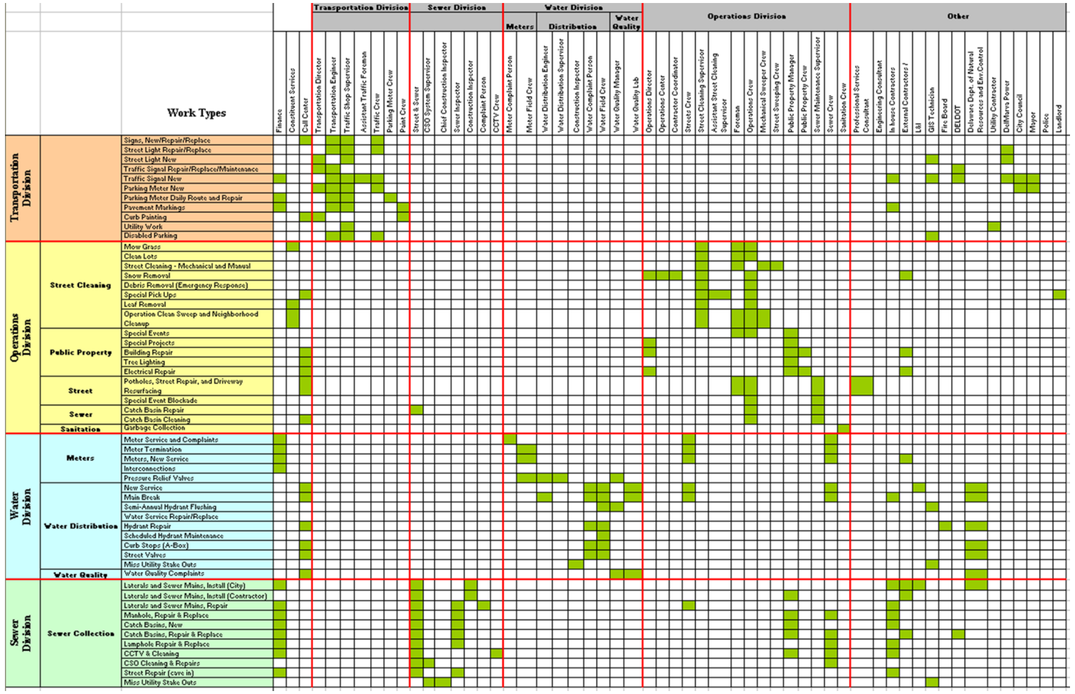
Good work process documentation identifies all people, data, applications, communications and information technologies needed to restore operations


Water work processes

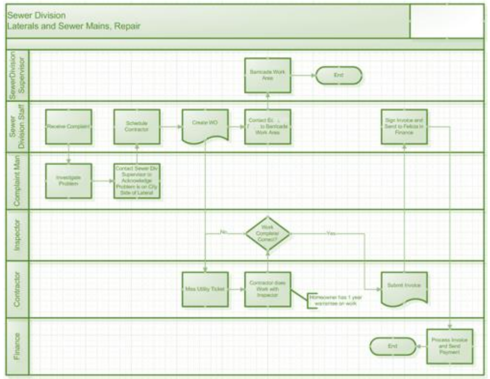



Transportation Work processes


Operations work processes

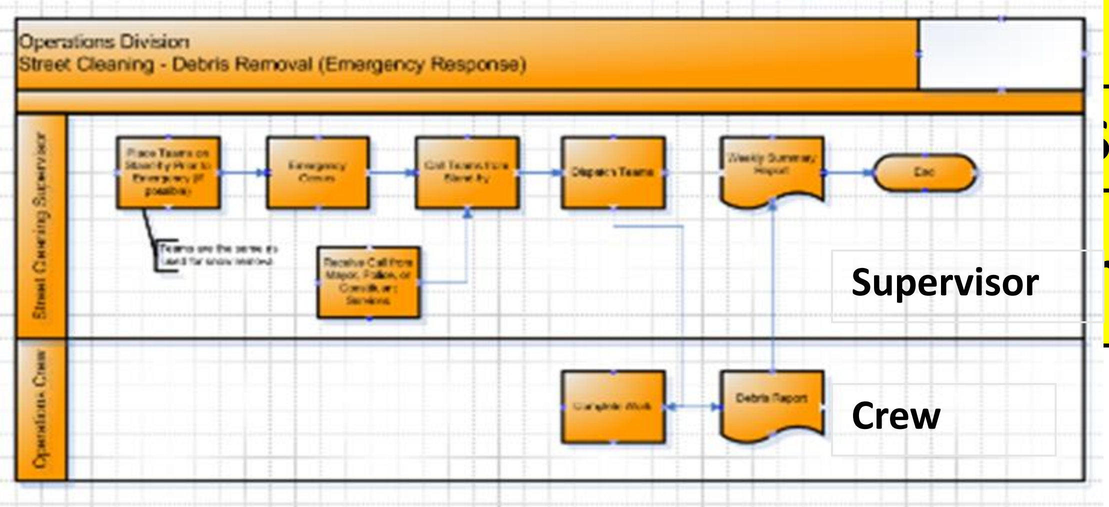


						Transportation Division							Sewer Division							Water Division									Operations Division															Other														
																				Meters		Distribution					Water Quality																															
		Work Types	Finance	Constituent Services	Call Center	Transportation Director	Transportation Engineer	Traffic Shop Supervisor	Assistant Traffic Foreman	Traffic Crew	Parking Meter Crew	Paint Crew	Street & Sewer	CSO System Supervisor	Chief Construction Inspector	Sewer Inspector	Construction Inspector	Complaint Person	CCTV Crew	Meter Complaint Person	Meter Field Crew	Water Distribution Engineer	Water Distribution Supervisor	Construction Inspector	Water Complaint Person	Water Field Crew	Water Quality Manager	Water Quality Lab	Operations Director	Operations Center	Contractor Coordinator	Streets Crew	Street Cleaning Supervisor	Assistant Street Cleaning Supervisor	Foreman	Operations Crew	Mechanical Sweeper Crew	Street Sweeping Crew	Public Property Manager	Public Property Crew	Sewer Maintenance Supervisor	Sewer Crew	Sanitation Crew	Professional Services Consultant	Engineering Consultant	In house Contractors	External Contractors /	I&I	GIS Technician	Fire Board	DELDOT	Delaware Dept. of Natural Resources and Env.Control	Utility Contractor	DelMarva Power	City Council	Mayor	Police	Landlord
Transportation Division		Signs, New/Repair/Replace			🟩		🟩	🟩		🟩																																													🟩				
		Street Light Repair/Replace					🟩	🟩		🟩																																							🟩					🟩				
		Street Light New				🟩		🟩																																									🟩					🟩				
		Traffic Signal Repair/Replace/Maintenance				🟩	🟩																																												🟩							
		Traffic Signal New	🟩				🟩	🟩	🟩	🟩																																					🟩			🟩		🟩			🟩	🟩	🟩		
		Parking Meter New				🟩	🟩	🟩		🟩																																													🟩	🟩		
		Parking Meter Daily Route and Repair	🟩				🟩	🟩			🟩																																															
		Pavement Markings	🟩				🟩	🟩				🟩																																			🟩													
		Curb Painting			🟩	🟩						🟩																																														
		Utility Work						🟩																																													🟩					
		Disabled Parking					🟩	🟩		🟩																																							🟩									
Operations Division	Street Cleaning	Mow Grass		🟩																													🟩		🟩	🟩																							
		Clean Lots																															🟩		🟩	🟩																							
		Street Cleaning - Mechanical and Manual																															🟩		🟩		🟩	🟩																				
		Snow Removal																											🟩	🟩	🟩		🟩			🟩											🟩											
		Debris Removal (Emergency Response)																															🟩			🟩																							
		Special Pick Ups			🟩																												🟩	🟩		🟩																						🟩
		Leaf Removal		🟩																													🟩			🟩																							
		Operation Clean Sweep and Neighborhood Cleanup		🟩																													🟩		🟩	🟩	🟩																						
	Public Property	Special Events																																	🟩	🟩			🟩																				
		Special Projects																											🟩										🟩																				
		Building Repair			🟩																								🟩										🟩	🟩							🟩											
		Tree Lighting			🟩																																		🟩																				
		Electrical Repair			🟩																								🟩										🟩	🟩							🟩											
	Street	Potholes, Street Repair, and Driveway Resurfacing			🟩																														🟩	🟩					🟩			🟩														
		Special Event Blockade																																		🟩					🟩																	
	Sewer	Catch Basin Repair											🟩																							🟩					🟩																	
		Catch Basin Cleaning			🟩																															🟩					🟩																	
	Sanitation	Garbage Collection																																									🟩														
Water Division	Meters	Meter Service and Complaints	🟩																	🟩												🟩										🟩																
		Meter Termination	🟩																		🟩											🟩										🟩																
		Meters, New Service	🟩																		🟩											🟩										🟩					🟩											
		Interconnections	🟩																																																							
		Pressure Relief Valves																			🟩	🟩	🟩				🟩																															
	Water Distribution	New Service			🟩																				🟩	🟩		🟩				🟩										🟩						🟩				🟩						
		Main Break			🟩																	🟩			🟩	🟩		🟩				🟩										🟩				🟩						🟩						
		Semi-Annual Hydrant Flushing																								🟩	🟩																						🟩									
		Water Service Repair/Replace																																																								
		Hydrant Repair			🟩																				🟩	🟩																								🟩		🟩						
		Scheduled Hydrant Maintenance																								🟩																																
		Curb Stops (A-Box)			🟩																				🟩	🟩																										🟩						
		Street Valves			🟩																				🟩	🟩																										🟩						
		Miss Utility Stake Outs																						🟩																									🟩									
	Water Quality	Water Quality Complaints			🟩																						🟩	🟩																								🟩						
Sewer Division	Sewer Collection	Laterals and Sewer Mains, Install (City)	🟩										🟩				🟩																													🟩	🟩	🟩				🟩						
		Laterals and Sewer Mains, Install (Contractor)											🟩				🟩																						🟩								🟩											
		Laterals and Sewer Mains, Repair	🟩										🟩			🟩		🟩														🟩														🟩												
		Manhole, Repair & Replace	🟩										🟩			🟩																							🟩			🟩				🟩												
		Catch Basins, New	🟩										🟩			🟩																							🟩							🟩												
		Catch Basins, Repair & Replace	🟩										🟩			🟩																							🟩			🟩					🟩				🟩							
		Lamphole Repair & Replace	🟩										🟩			🟩																										🟩				🟩												
		CCTV & Cleaning	🟩										🟩						🟩																				🟩			🟩				🟩												
		CSO Cleaning & Repairs											🟩	🟩																												🟩																
		Street Repair (cave in)	🟩										🟩			🟩																														🟩												
		Miss Utility Stake Outs												🟩	🟩																																		🟩									


Sewer Division
Laterals and Sewer Mains, Repair
SewerDivision Supervisor
Sewer Division Staff
Complaint Man
Inspector
Contractor
Finance
Barricade Work Area
End
Receive Complaint
Schedule Contractor
Create WO
Contact to Barricade Work Area
Sign Invoice and Send to Felicia in Finance
Investigate Problem
Contact Sewer Div Supervisor to Acknowledge Problem is on City Side of Lateral
Work Complete/ Correct?
No
Yes
Miss Utility Ticket
Contractor does Work with Inspector
Homeowner has 1 year warrantee on work
Submit Invoice
End
Process Invoice and Send Payment

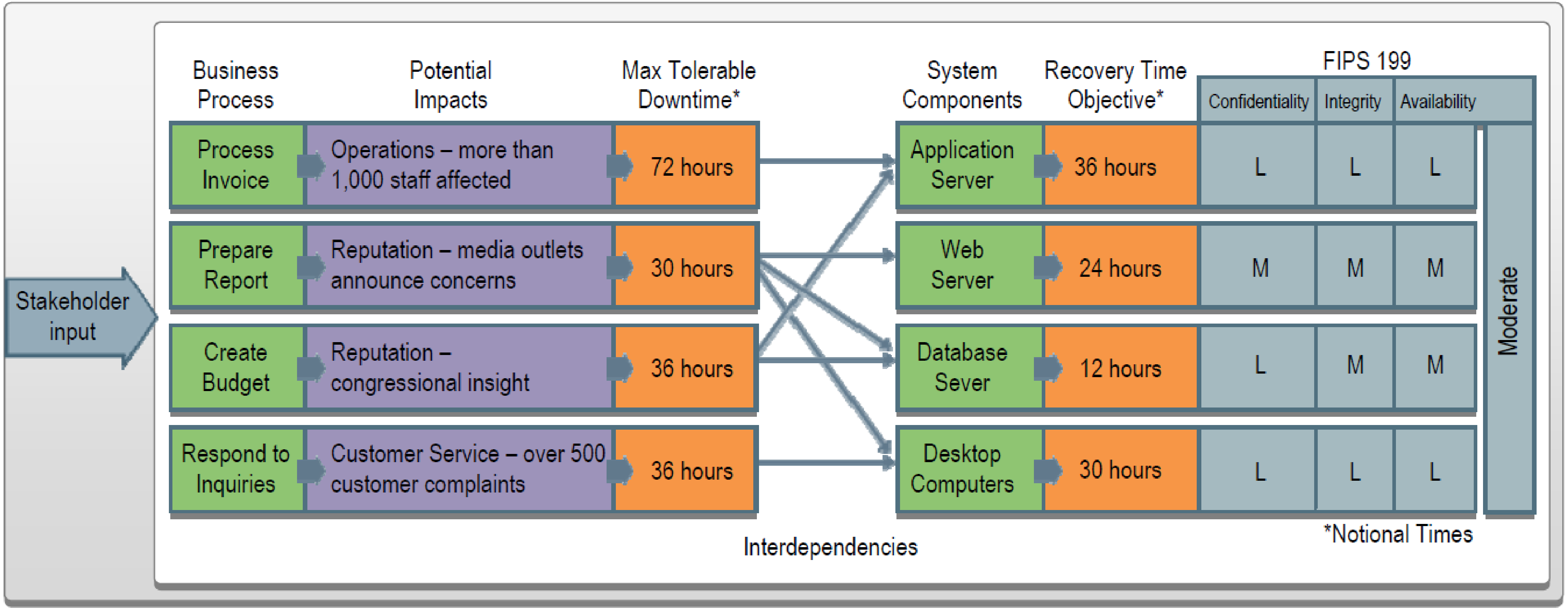
Priorities for recovery example

Public Works Dept Operations Division	**Street Cleaning**	**Mow Grass**
		Clean Lots
		Street Cleaning - Mechanical and Manual
		Snow Removal
		Debris Removal (Emergency Response)
		Special Pick Ups
		Leaf Removal
		Neighborhood Cleanup
	Public Property	**Special Events**
		Special Projects
		Building Repair
		Tree Lighting
		Electrical Repair
	Street	**Potholes, Street Repair, and Resurfacing**
		Special Event Blockade
	nitation	**Catch Basin Repair**
		Catch Basin Cleaning
		Garbage Collection


Operations Division
Street Cleaning - Debris Removal (Emergency Response)
Street Cleaning Supervisor
Place Teams on Standby Prior to Emergency (if possible)
Emergency Occurs
Call Teams into Stand-by
Dispatch Teams
Weekly Summary Report
End
Teams are the same as used for snow removal
Receive Call from Mayor, Police, or Constituent Services
Operations Crew
Complete Work
Debris Report
Supervisor
Crew

Business Impact Analysis (BIA) example…

- Determine Business Processes and Recovery Criticality
- Identify Information and IT Resource Requirements
- Identify Information System Resource Recovery Priorities

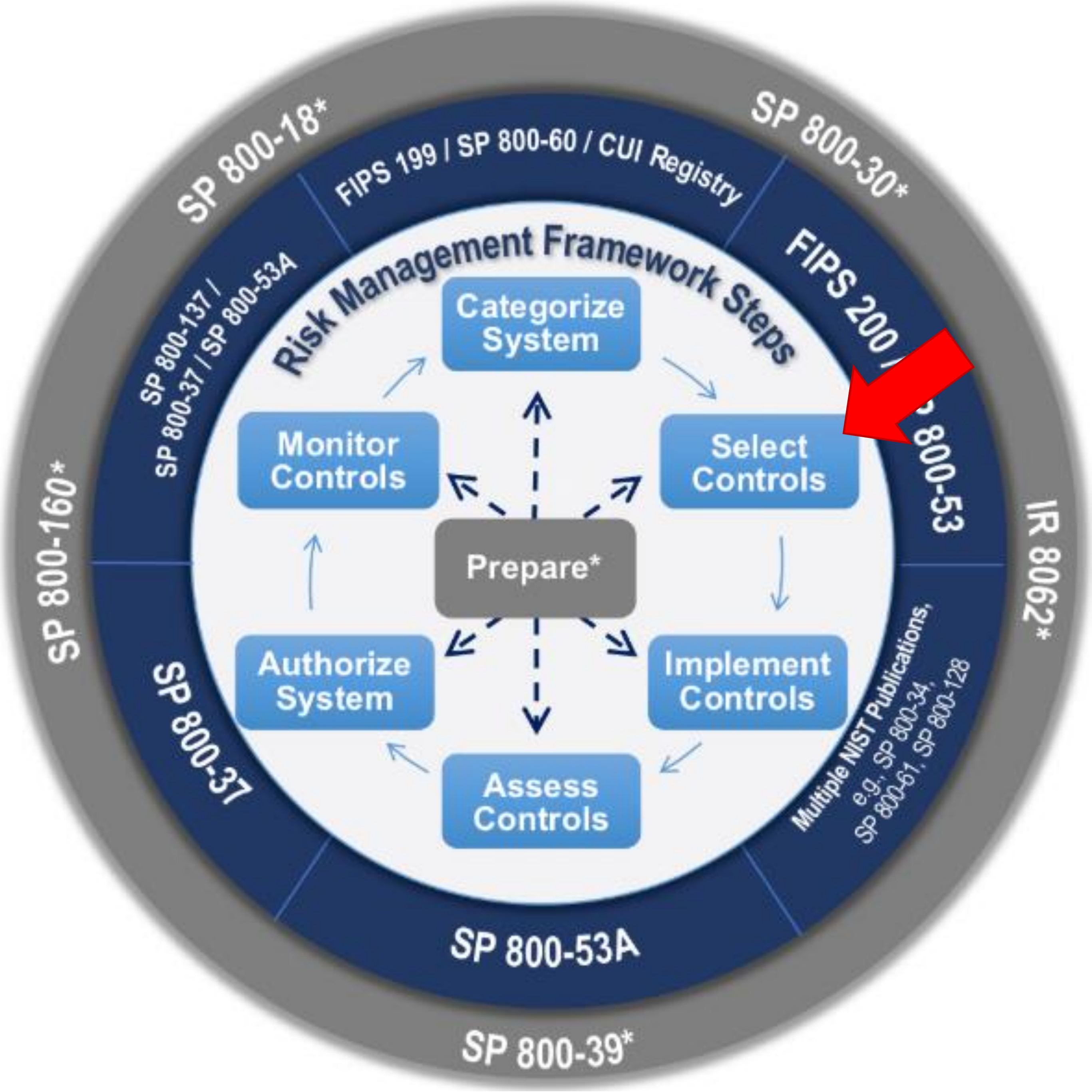


Stakeholder input

Business Process	Potential Impacts	Max Tolerable Downtime*	System Components	Recovery Time Objective*	FIPS 199		
					Confidentiality	Integrity	Availability
Process Invoice	Operations – more than 1,000 staff affected	72 hours	Application Server	36 hours	L	L	L
Prepare Report	Reputation – media outlets announce concerns	30 hours	Web Server	24 hours	M	M	M
Create Budget	Reputation – congressional insight	36 hours	Database Sever	12 hours	L	M	M
Respond to Inquiries	Customer Service – over 500 customer complaints	36 hours	Desktop Computers	30 hours	L	L	L

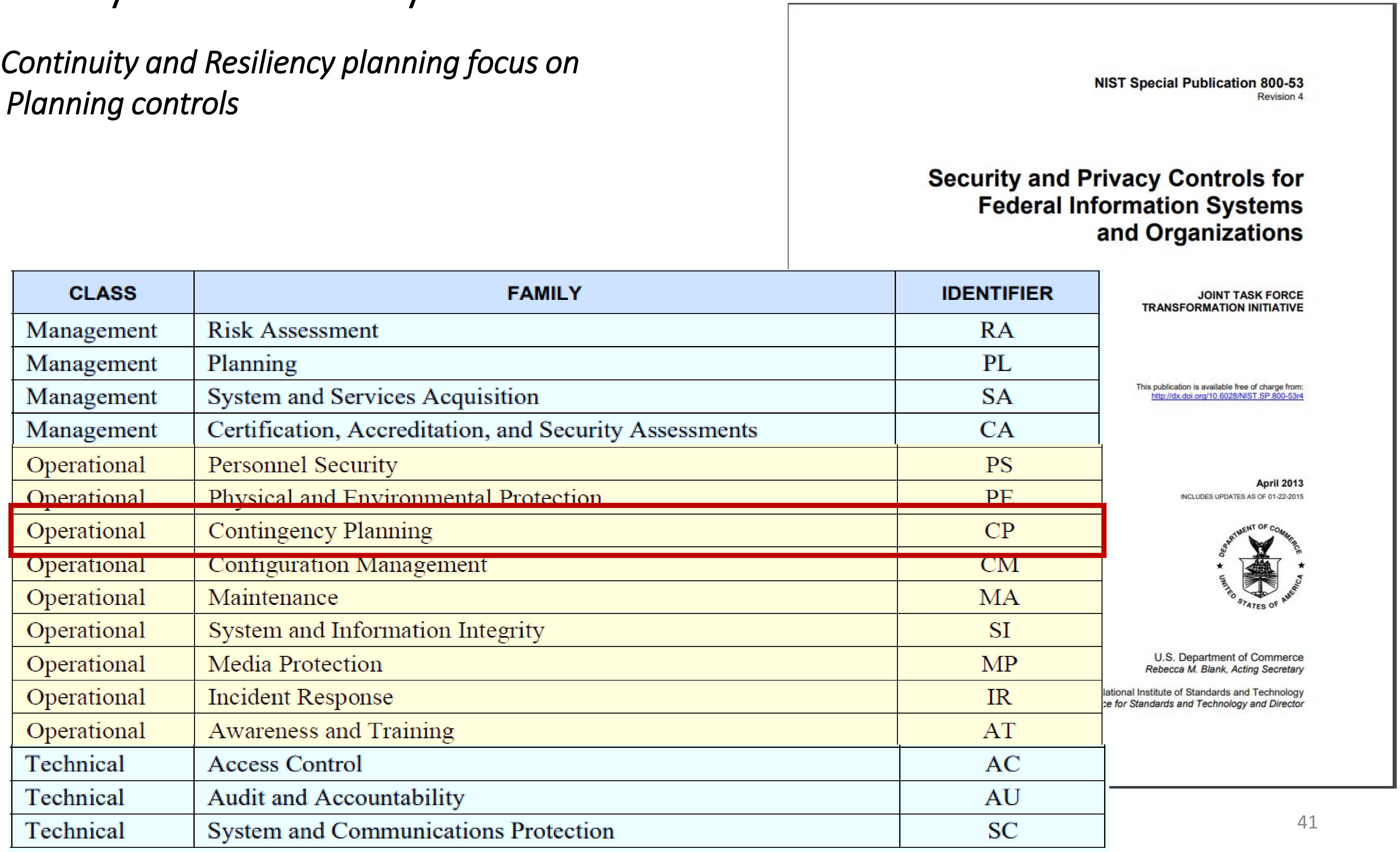
*Notional Times

NIST SP 800-34 R1 – Contingency Planning Guide for Federal Information Systems


SP 800-18*
FIPS 199 / SP 800-60 / CUI Registry
SP 800-30*
FIPS 200 /
800-53
IR 8062*
Multiple NIST Publications, e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A
SP 800-39*
SP 800-37
SP 800-160*
SP 800-137 / SP 800-37 / SP 800-53A
Risk Management Framework Steps
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Prepare*

Catalog of cyber-security controls

for Business Continuity and Resiliency planning focus on Contingency Planning controls



CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

April 2013
INCLUDES UPDATES AS OF 01-22-2015

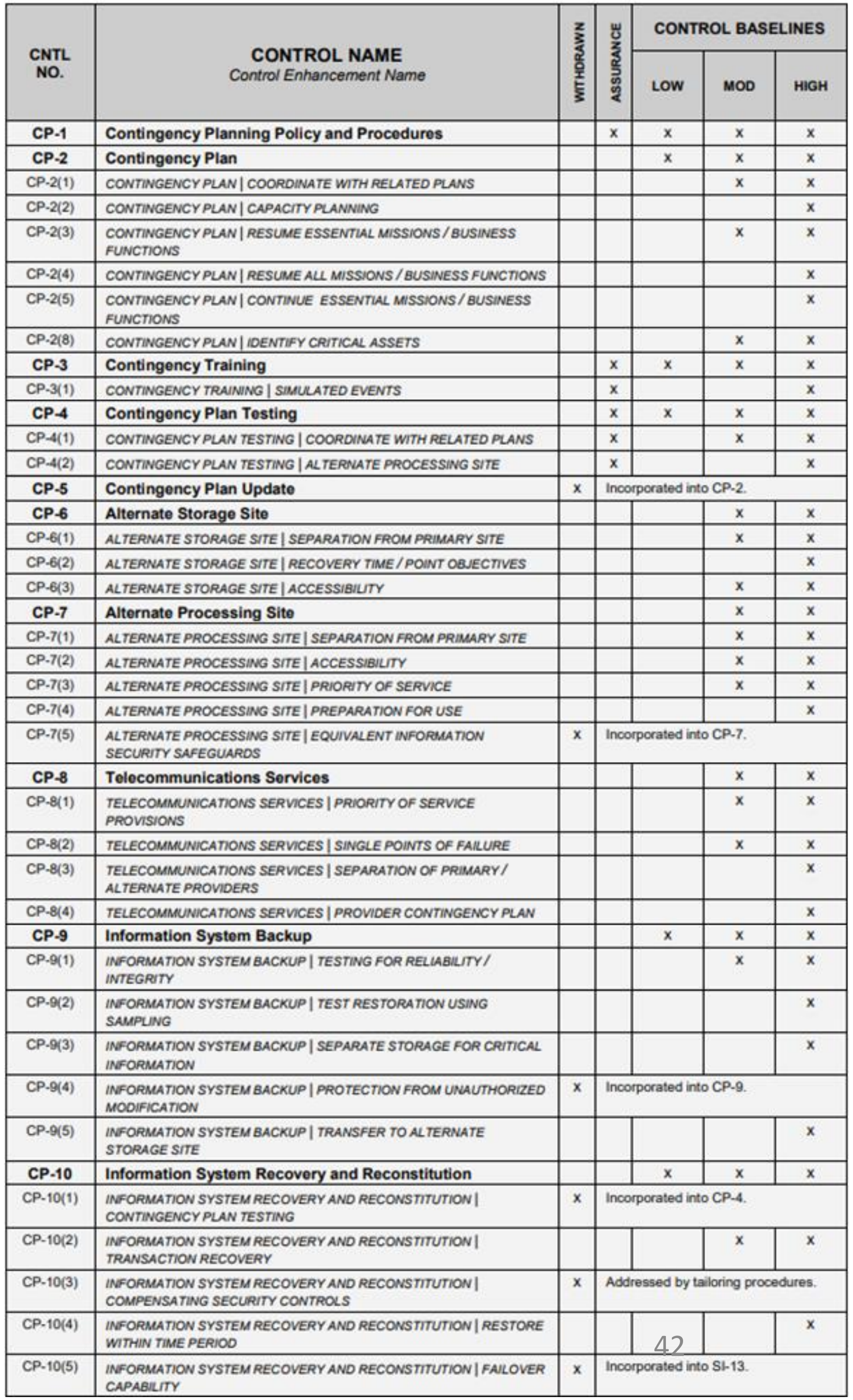
U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

lational Institute of Standards and Technology
ce for Standards and Technology and Director

Contingency Planning Controls

CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information System Recovery and Reconstitution	X	X	X

NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations"



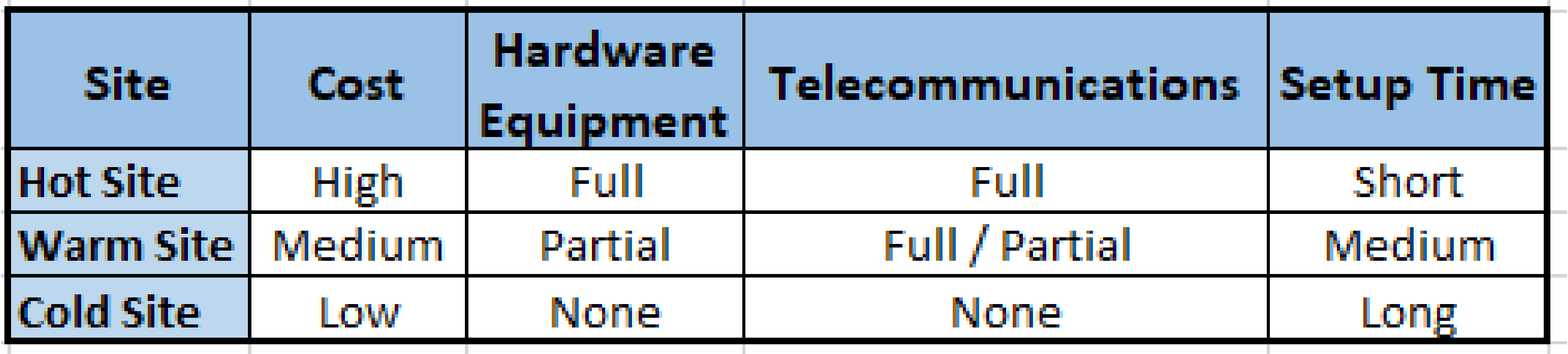
CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2(3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2(4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3(1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4(1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4(2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6(2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6(3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7(1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7(2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7(3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7(4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7(5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-8	**Telecommunications Services**				x	x
CP-8(1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8(2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8(3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8(4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-9	**Information System Backup**			x	x	x
CP-9(1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x
CP-9(2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9(3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9(4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9(5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10(1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10(3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10(4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10(5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			

Options for alternate Data Processing Site

Hot site: A geographically remote facility, fully equipped and ready to power up at a moments notice

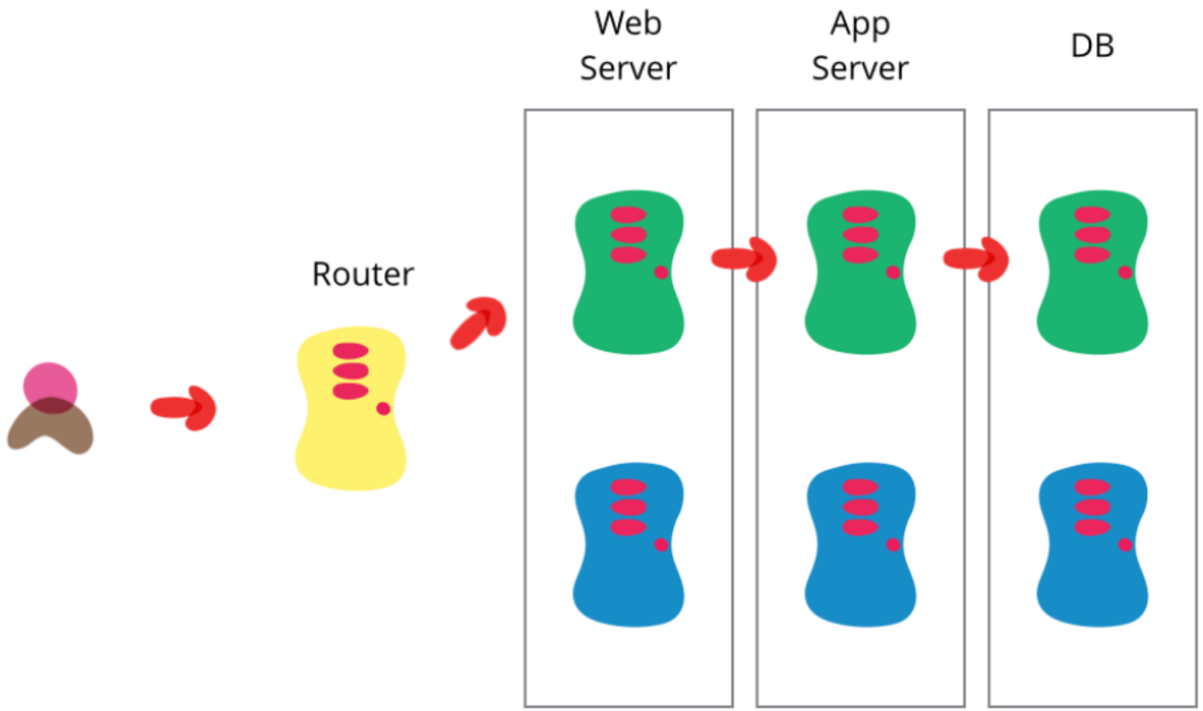
Warm site: Includes communications components but computers are not installed – will need to be delivered and setup

Cold site: Provides only the basic environment that can be outfitted with communication, utilities and computers



Site	Cost	Hardware Equipment	Telecommunications	Setup Time
Hot Site	High	Full	Full	Short
Warm Site	Medium	Partial	Full / Partial	Medium
Cold Site	Low	None	None	Long

BlueGreen Deployment



“As you prepare a new release of your software you do your final stage of testing in the green environment. Once the software is working in the green environment, you switch the router so that all incoming requests go to the green environment - the blue one is now idle.

Blue-green deployment also gives you a rapid way to rollback - if anything goes wrong you switch the router back to your blue environment. …

Once you've put your green environment live and you're happy with its stability, you then use the blue environment as your staging environment for the final testing step for your next deployment.

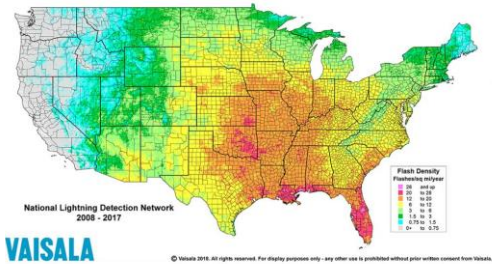
When you are ready for your next release, you switch from green to blue in the same way that you did from blue to green earlier. That way both green and blue environments are regularly cycling between live, previous version (for rollback) and staging the next version.”

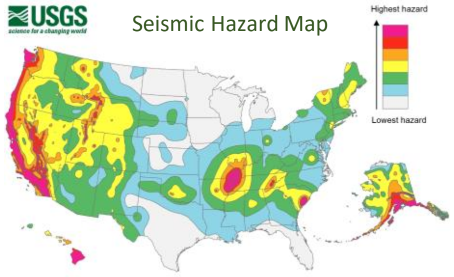
https://www.martinfowler.com/bliki/BlueGreenDeployment.html

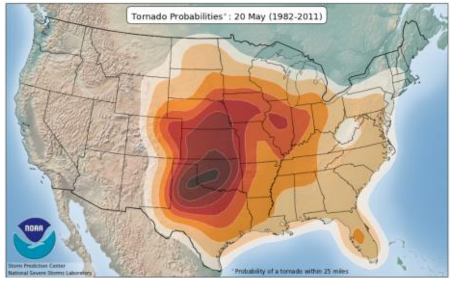
Location of Alternate site

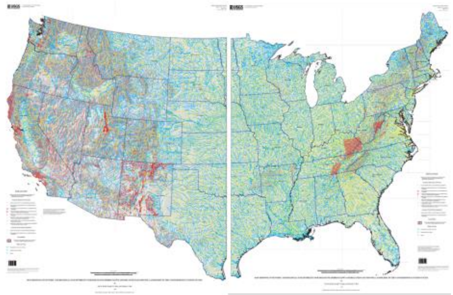
Disaster recovery site should be in a different geophysical area not susceptible to same disaster as the primary operations facility

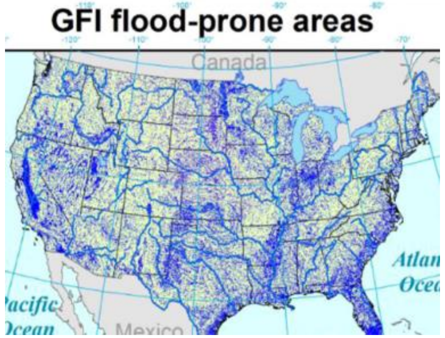
Note: even the cloud is located somewhere…



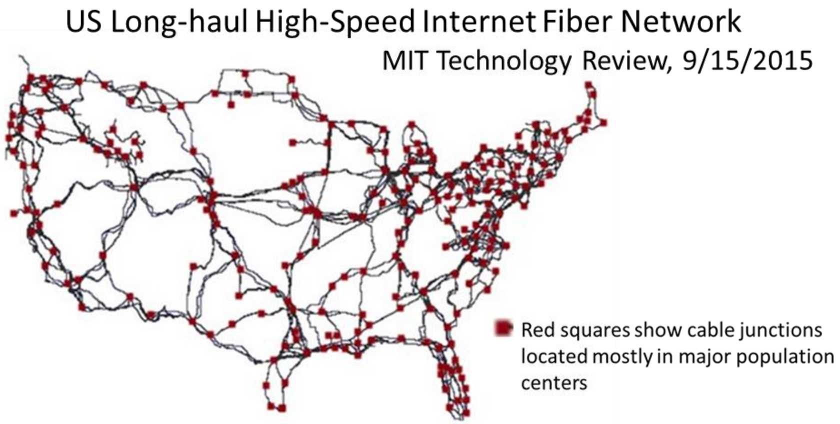



Tornado Probabilities : 20 May (1982-2011)
NOAA
Probability of a tornado within 25 miles





With multiple providers of:



US Long-haul High-Speed Internet Fiber Network
MIT Technology Review, 9/15/2015

Red squares show cable junctions located mostly in major population centers

- Telecommunications
- Stable power supply
- Redundant utilities

Multi-hazard mapping

Primer on Natural Hazard Management in Integrated Regional Development Planning

Department of Regional Development and Environment Executive Secretariat for Economic and Social Affairs Organization of American States

With support from the Office of Foreign Disaster Assistance United States Agency for International Development

Washington, D.C. 1991

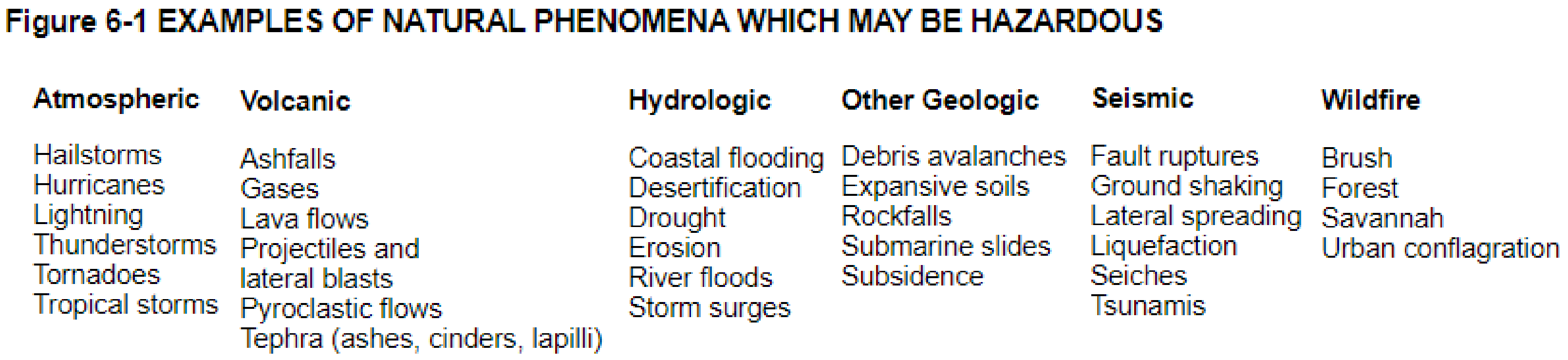
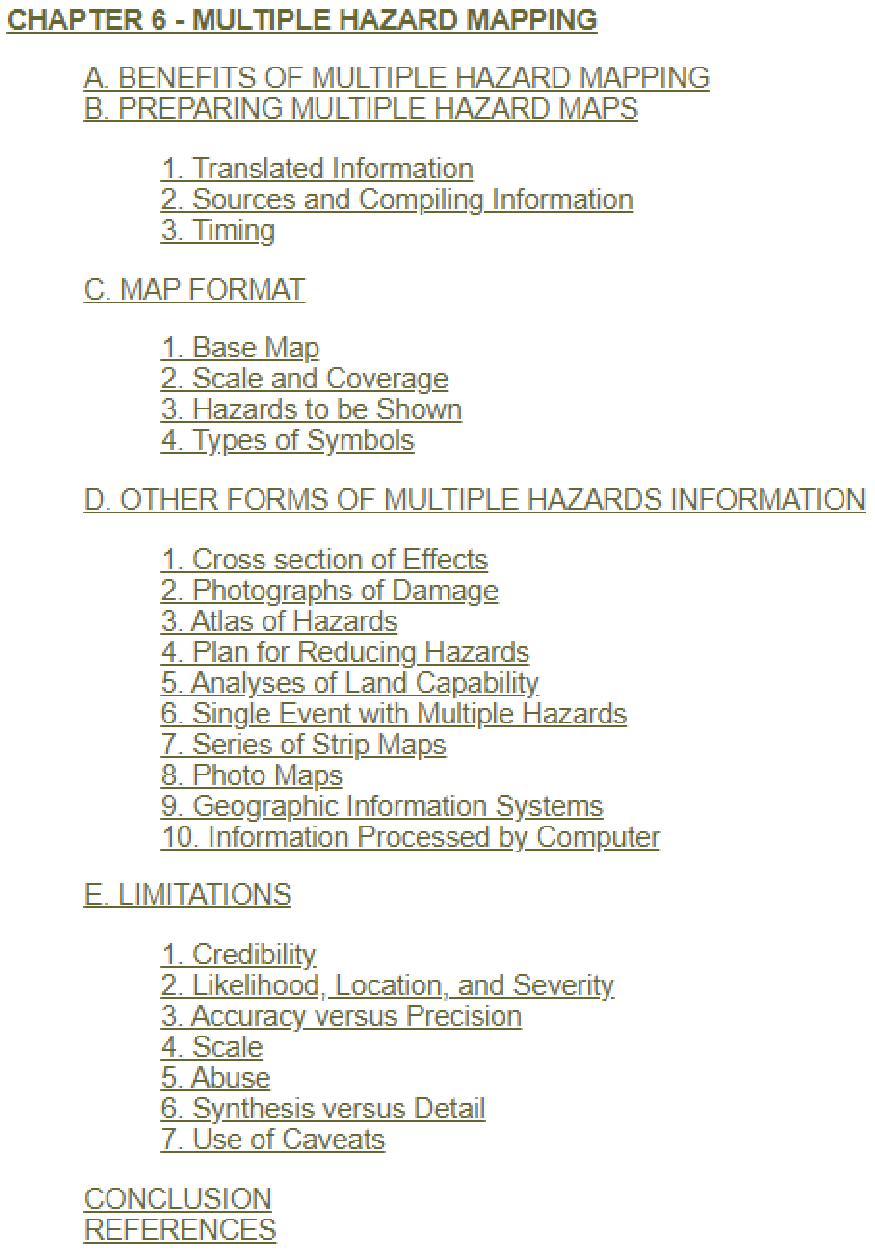


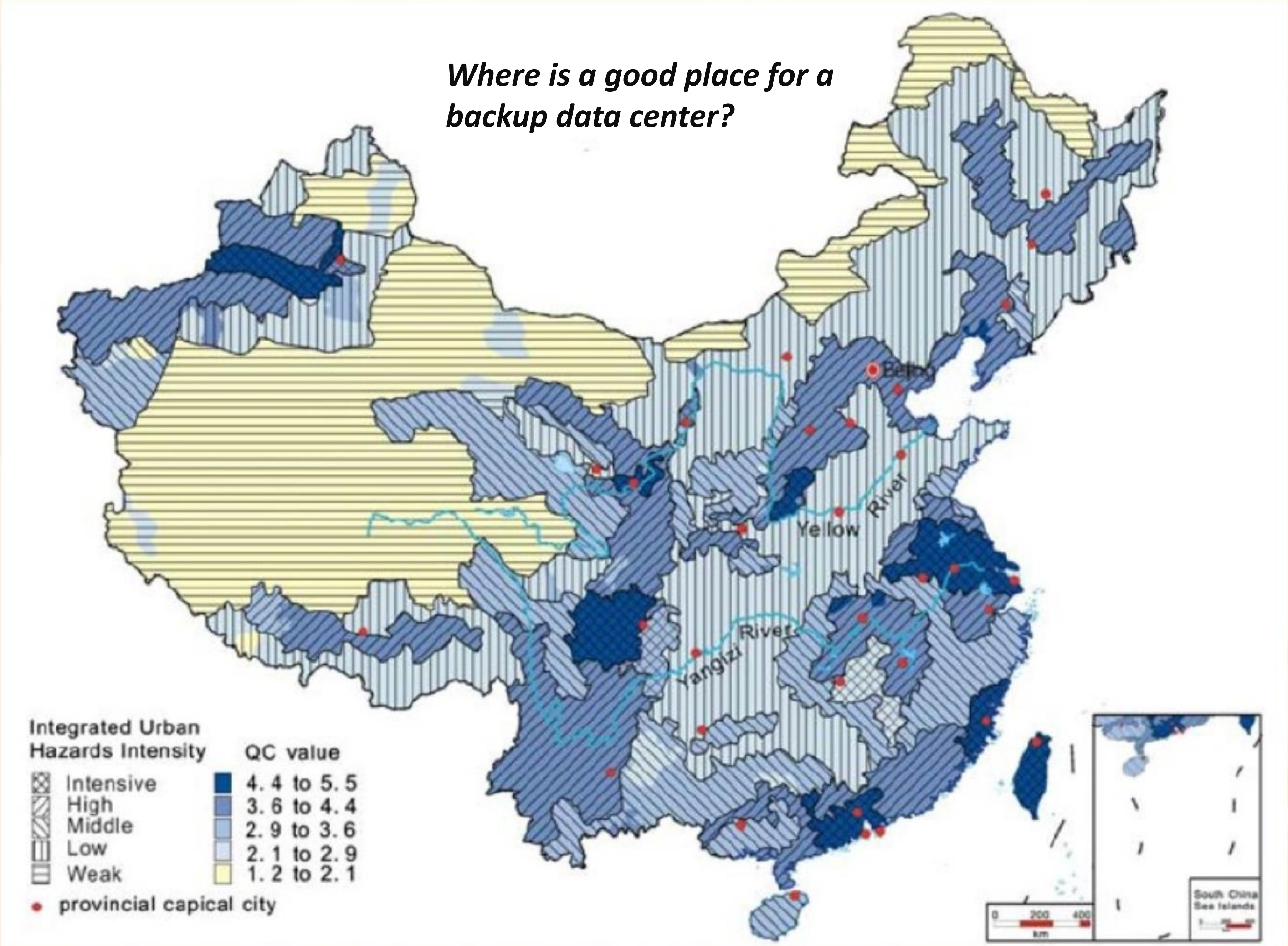
Figure 6-1 EXAMPLES OF NATURAL PHENOMENA WHICH MAY BE HAZARDOUS

Atmospheric	Volcanic	Hydrologic	Other Geologic	Seismic	Wildfire
Hailstorms	Ashfalls	Coastal flooding	Debris avalanches	Fault ruptures	Brush
Hurricanes	Gases	Desertification	Expansive soils	Ground shaking	Forest
Lightning	Lava flows	Drought	Rockfalls	Lateral spreading	Savannah
Thunderstorms	Projectiles and	Erosion	Submarine slides	Liquefaction	Urban conflagration
Tornadoes	lateral blasts	River floods	Subsidence	Seiches	
Tropical storms	Pyroclastic flows	Storm surges		Tsunamis	
	Tephra (ashes, cinders, lapilli)				

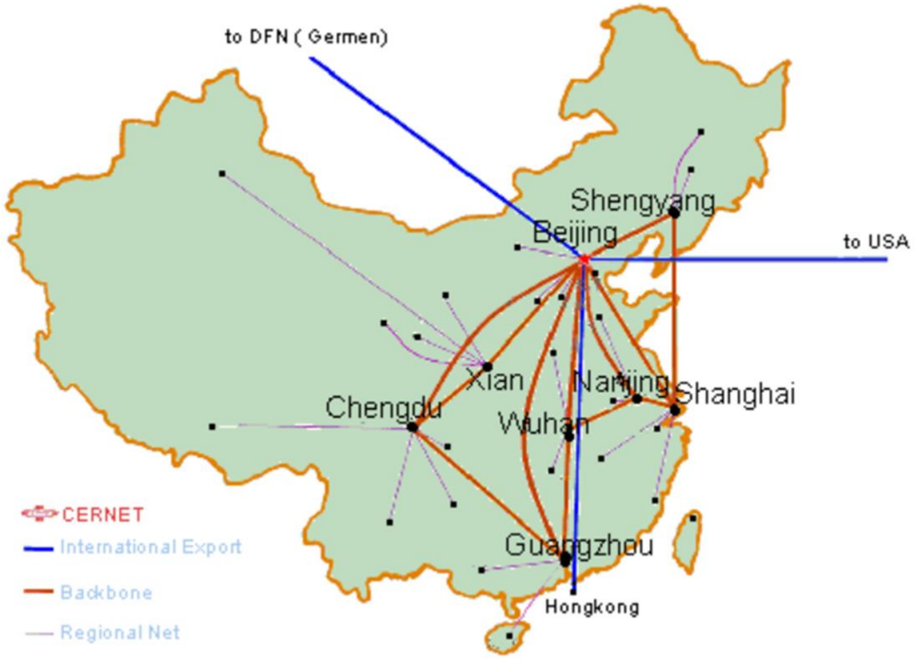


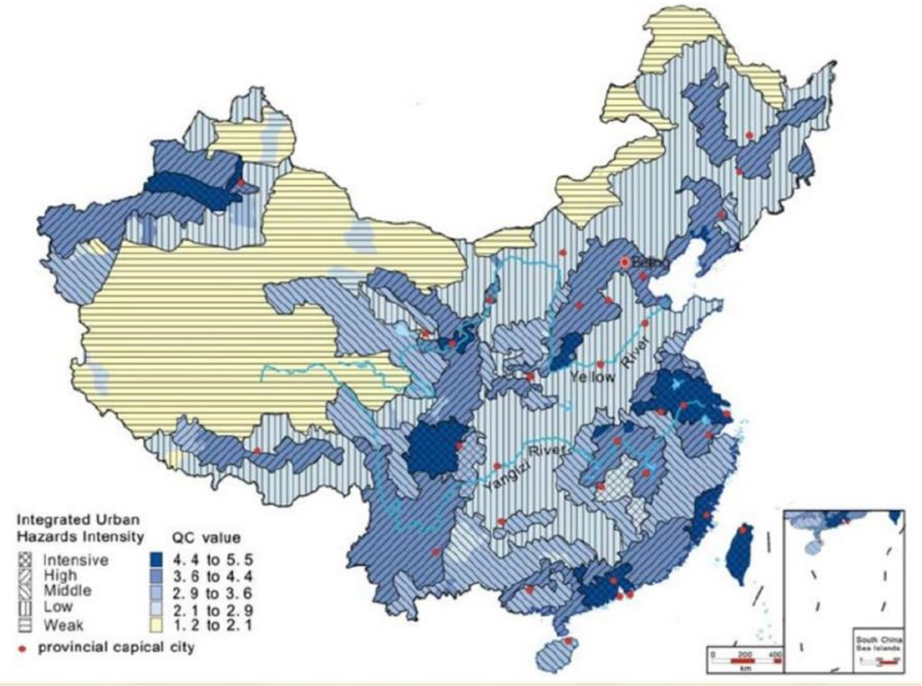
CHAPTER 6 - MULTIPLE HAZARD MAPPING

Map of Comprehensive Urban Natural Disaster Intensity in China



Where is a good place for a backup data center?





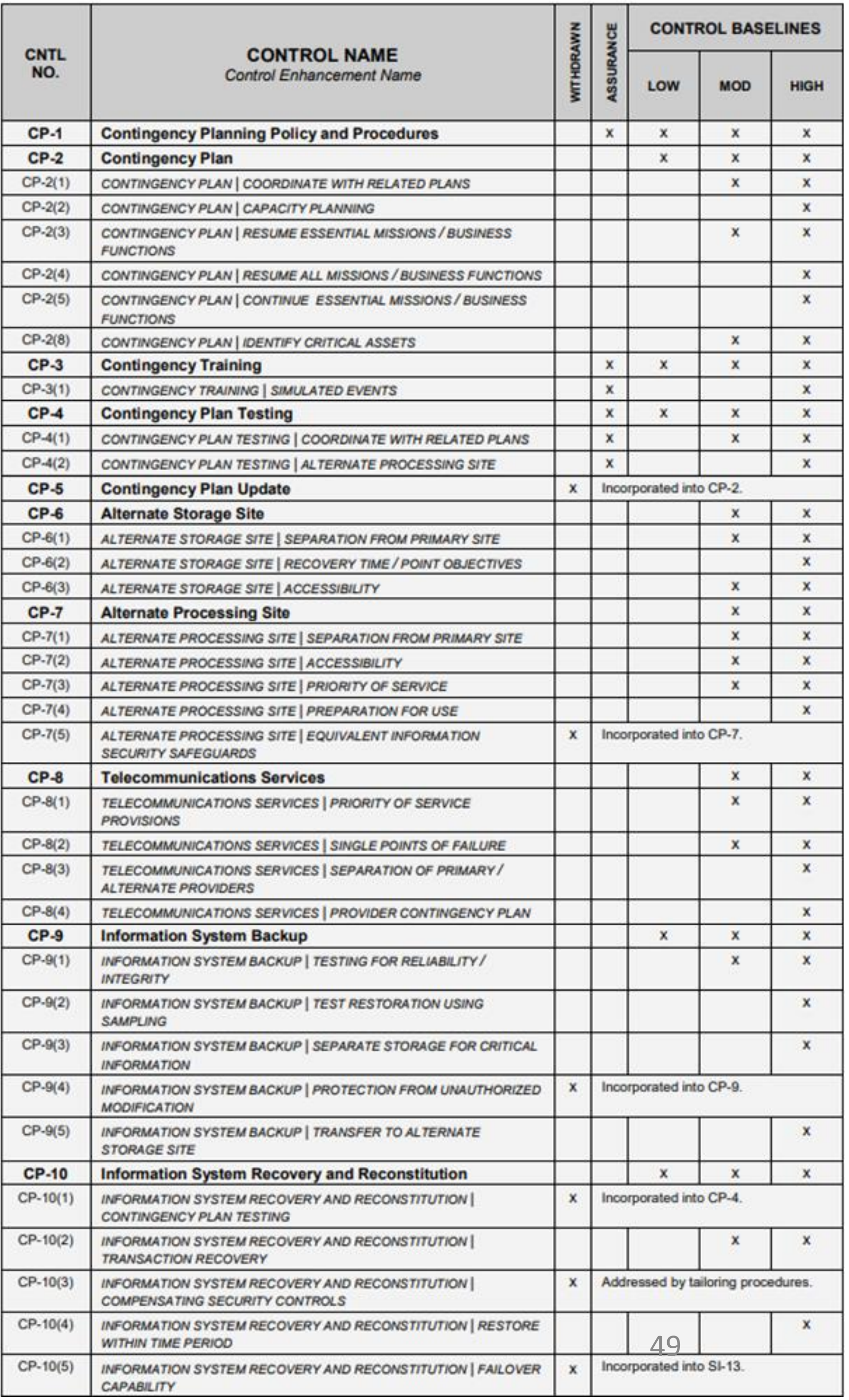
中国教育和科研计算机网
China Education and Research Network

Example is an outdated internet infrastructure map intended to illustrate what is needed to plan data center disaster recovery site

Contingency Planning Controls

CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information System Recovery and Reconstitution	X	X	X

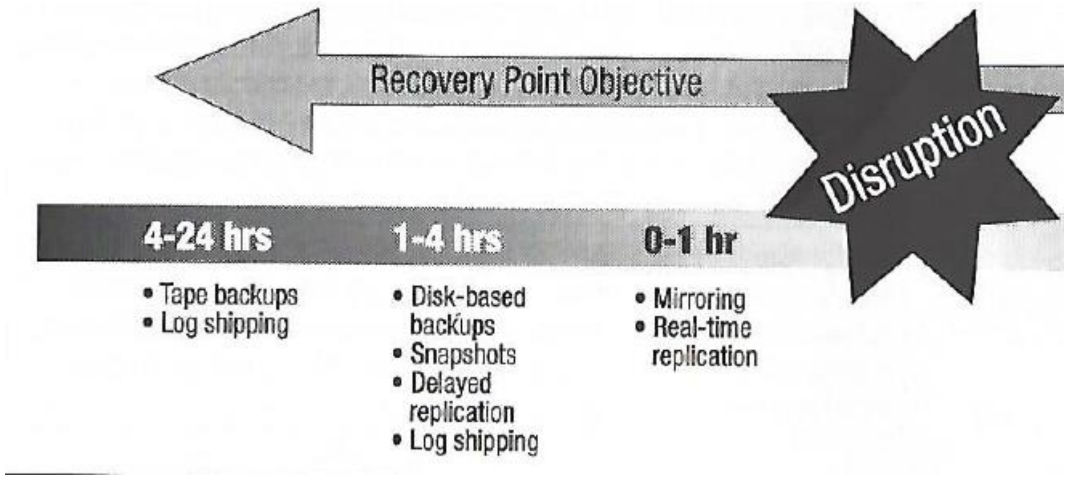
NIST SP 800-53r4 “Security and Privacy Controls for Federal Information Systems and Organizations”

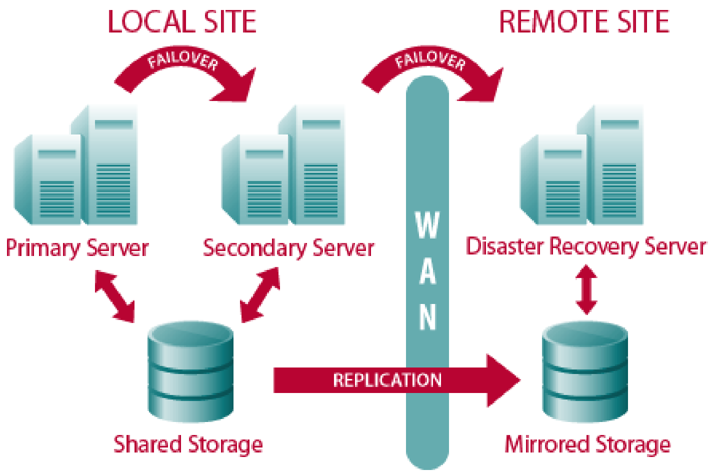


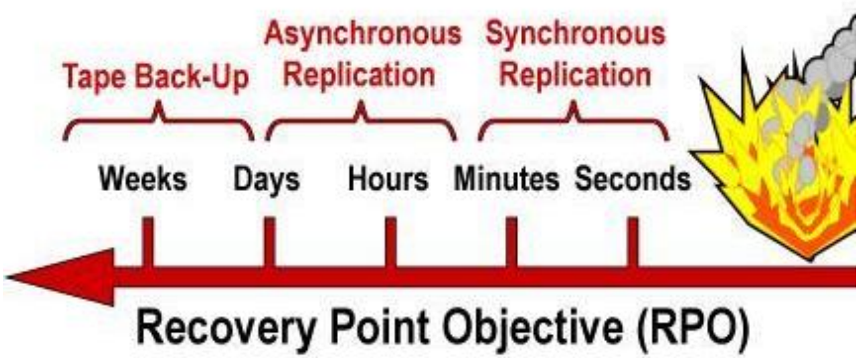
CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2(3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2(4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3(1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4(1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4(2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6(2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6(3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7(1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7(2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7(3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7(4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7(5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-8	**Telecommunications Services**				x	x
CP-8(1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8(2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8(3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8(4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-9	**Information System Backup**			x	x	x
CP-9(1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x
CP-9(2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9(3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9(4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9(5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10(1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10(3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10(4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10(5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			

Data backup systems and redundancies

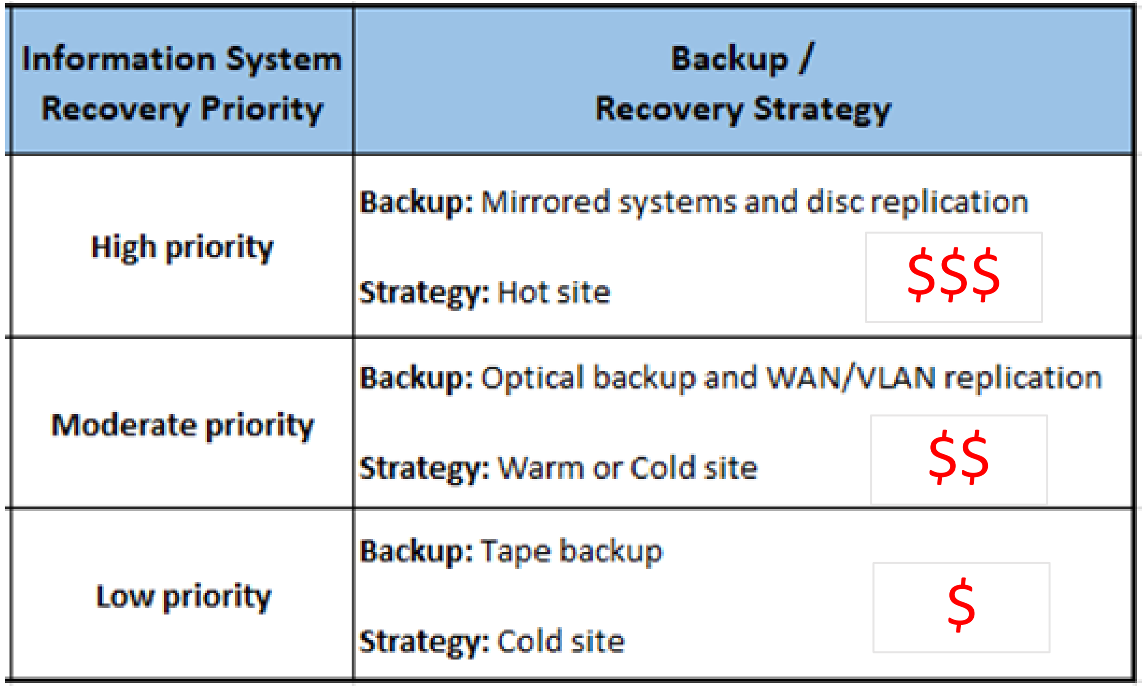
- **Database shadowing**
- **Electronic vaulting**
- **Remote journaling**
- **Storage area network and hierarchical storage management**
- **Shared storage**
- **RAID**
- **Failover clustering**







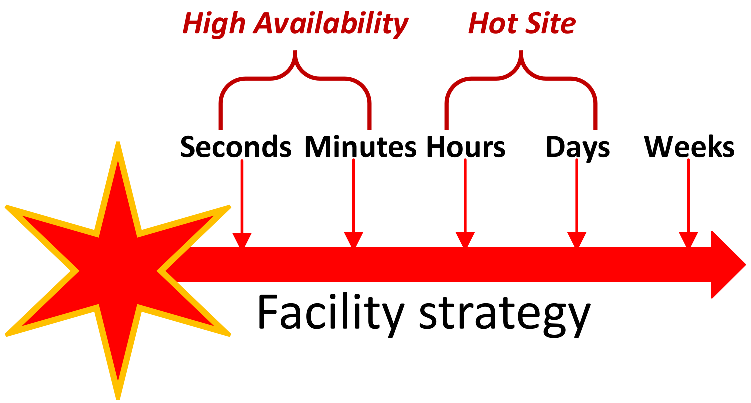
Recovery Options: Location & Backup



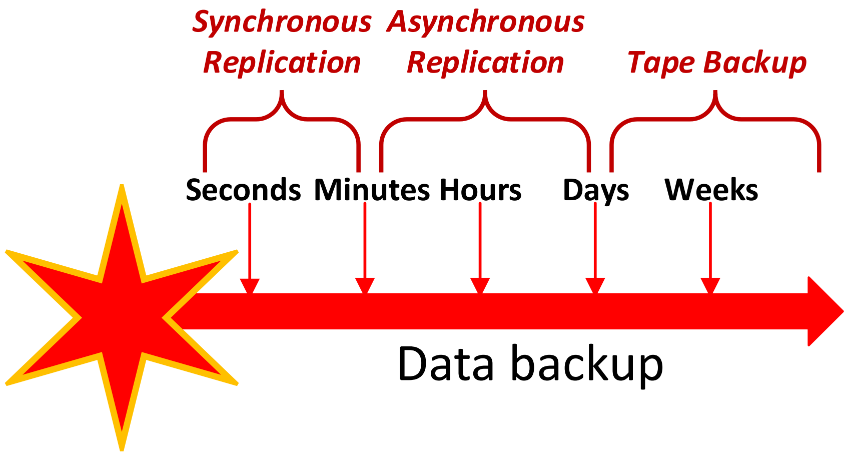
Information System Recovery Priority	Backup / Recovery Strategy
High priority	**Backup:** Mirrored systems and disc replication **Strategy:** Hot site $$$
Moderate priority	**Backup:** Optical backup and WAN/VLAN replication **Strategy:** Warm or Cold site $$
Low priority	**Backup:** Tape backup **Strategy:** Cold site $

[NIST SP 800-34 R1](#)
[Planning Guide for Federal Information Systems](#)

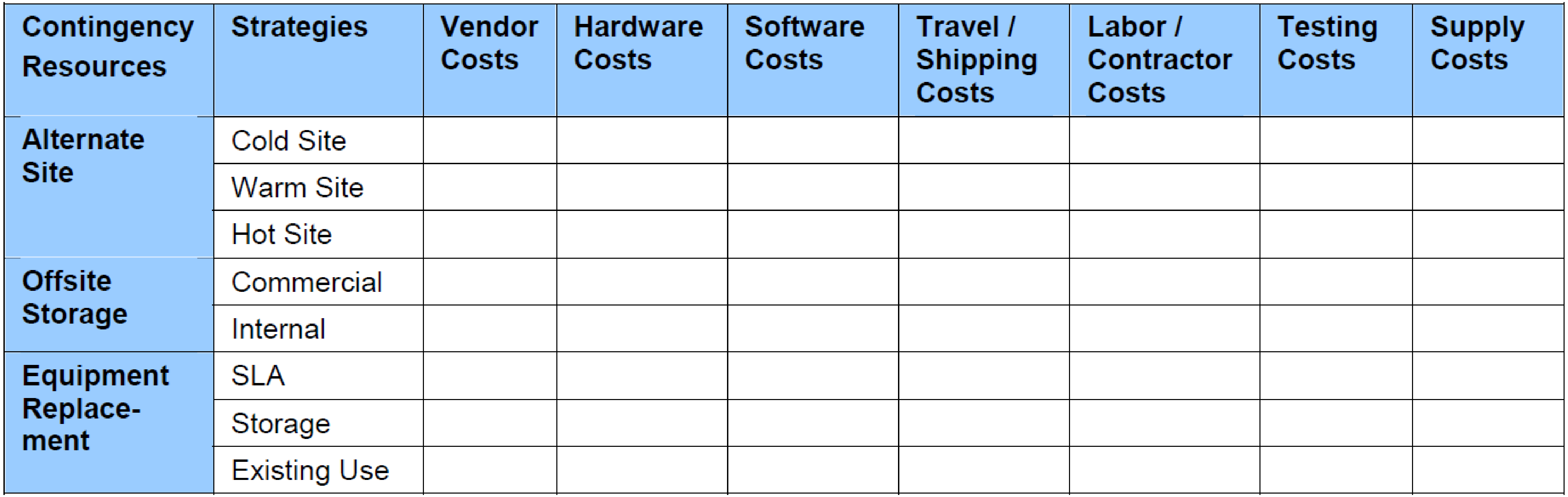
Recovery Time Objective



Recovery Point Objective

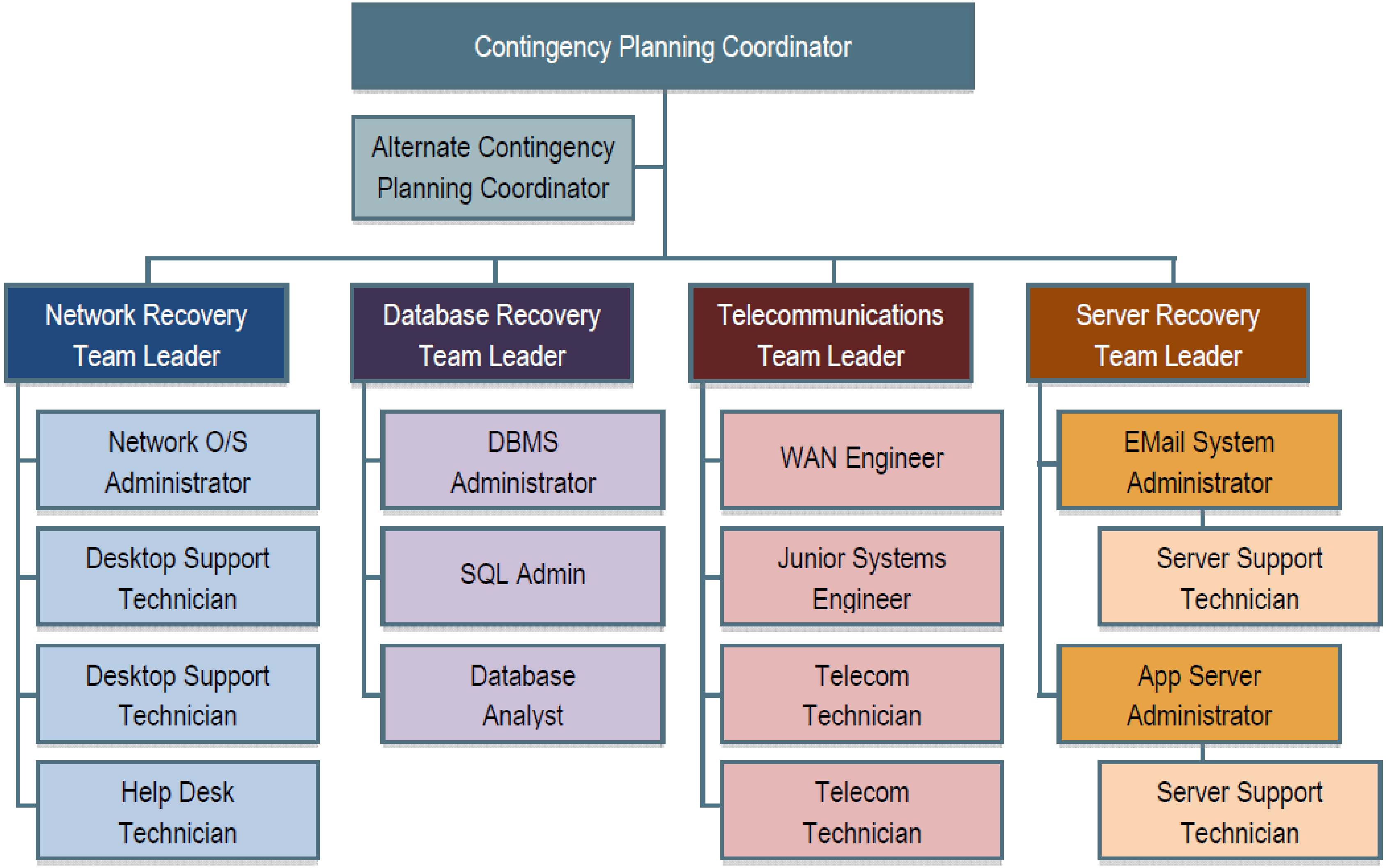


Considerations - Budget



Contingency Resources	Strategies	Vendor Costs	Hardware Costs	Software Costs	Travel / Shipping Costs	Labor / Contractor Costs	Testing Costs	Supply Costs
Alternate Site	Cold Site							
	Warm Site							
	Hot Site							
Offsite Storage	Commercial							
	Internal							
Equipment Replacement	SLA							
	Storage							
	Existing Use							

Response Roles and Responsibilities example



Contingency Planning Coordinator

Alternate Contingency Planning Coordinator

Network Recovery Team Leader

- Network O/S Administrator
- Desktop Support Technician
- Desktop Support Technician
- Help Desk Technician

Database Recovery Team Leader

- DBMS Administrator
- SQL Admin
- Database Analyst

Telecommunications Team Leader

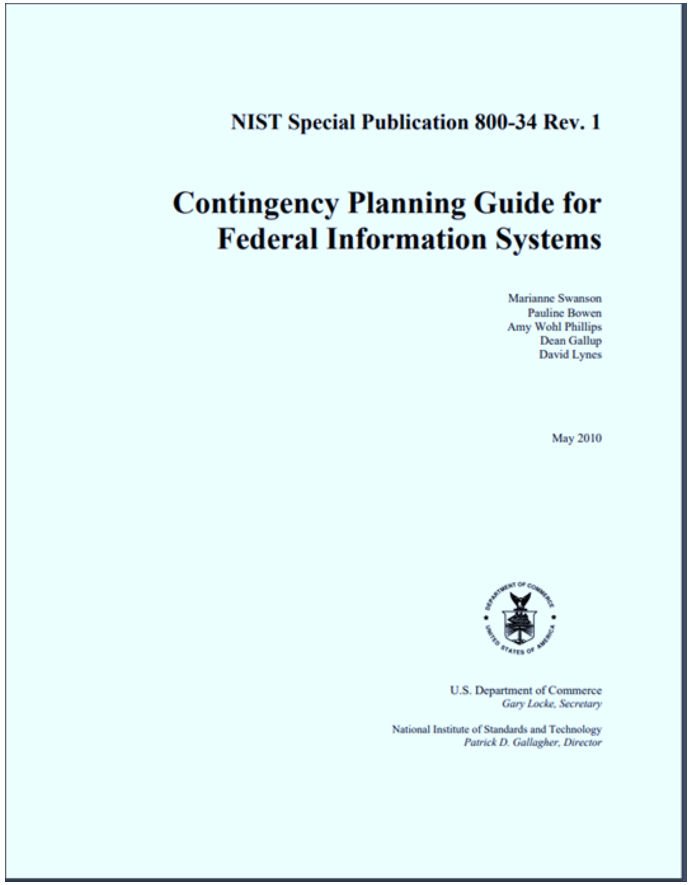
- WAN Engineer
- Junior Systems Engineer
- Telecom Technician
- Telecom Technician

Server Recovery Team Leader

- EMail System Administrator
  - Server Support Technician
- App Server Administrator
  - Server Support Technician

NIST SP 800-34 R1 – Contingency Planning Guide for Federal Information Systems

Contingency Plan



NIST Special Publication 800-34 Rev. 1

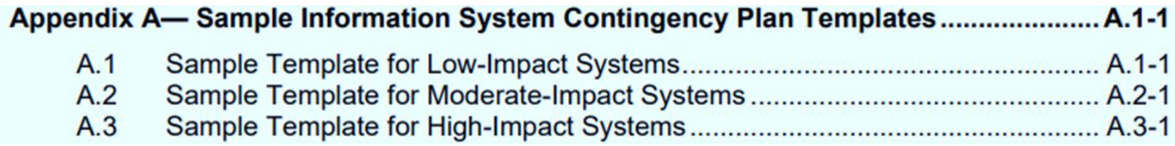
Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

May 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director



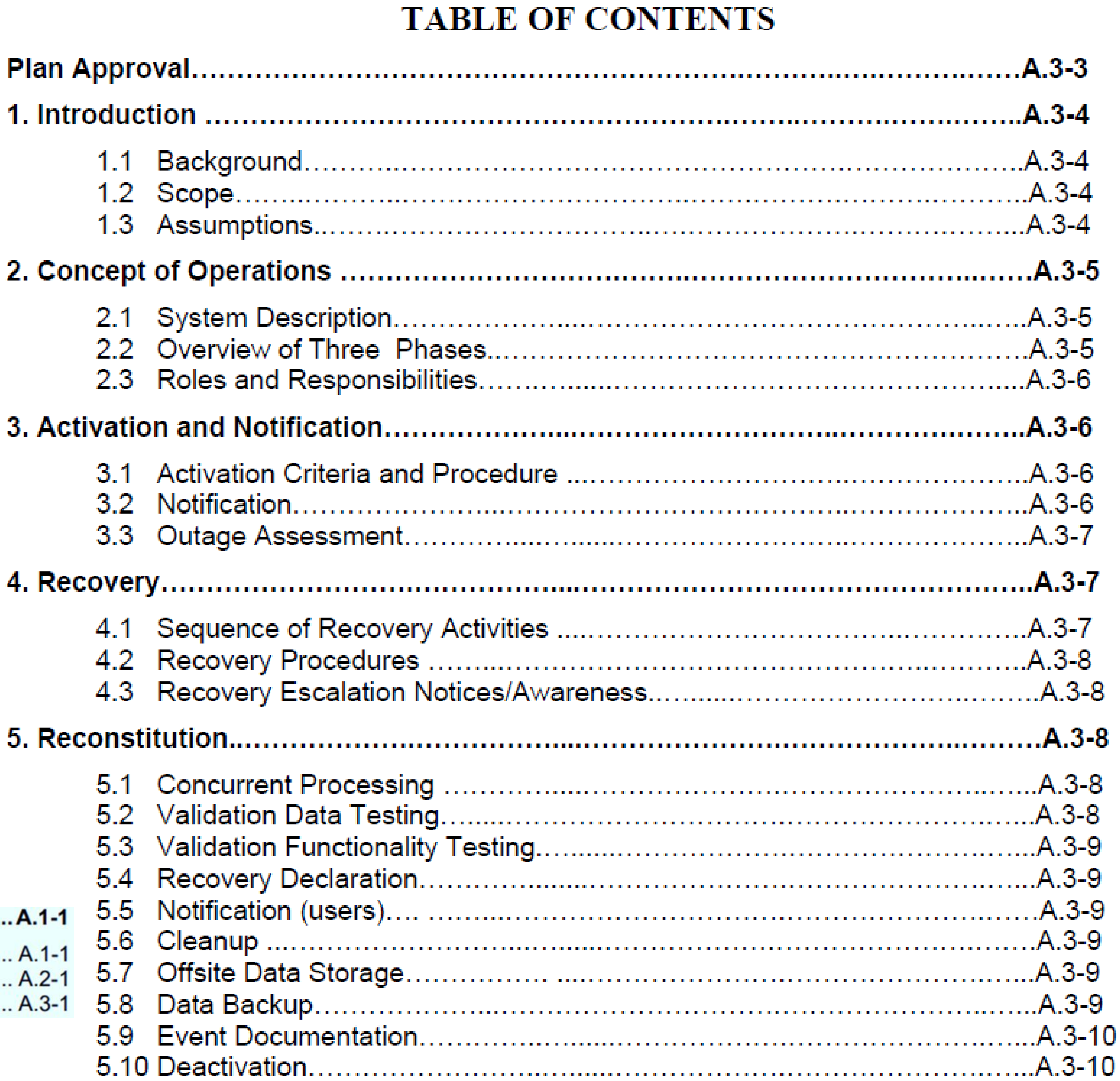


TABLE OF CONTENTS

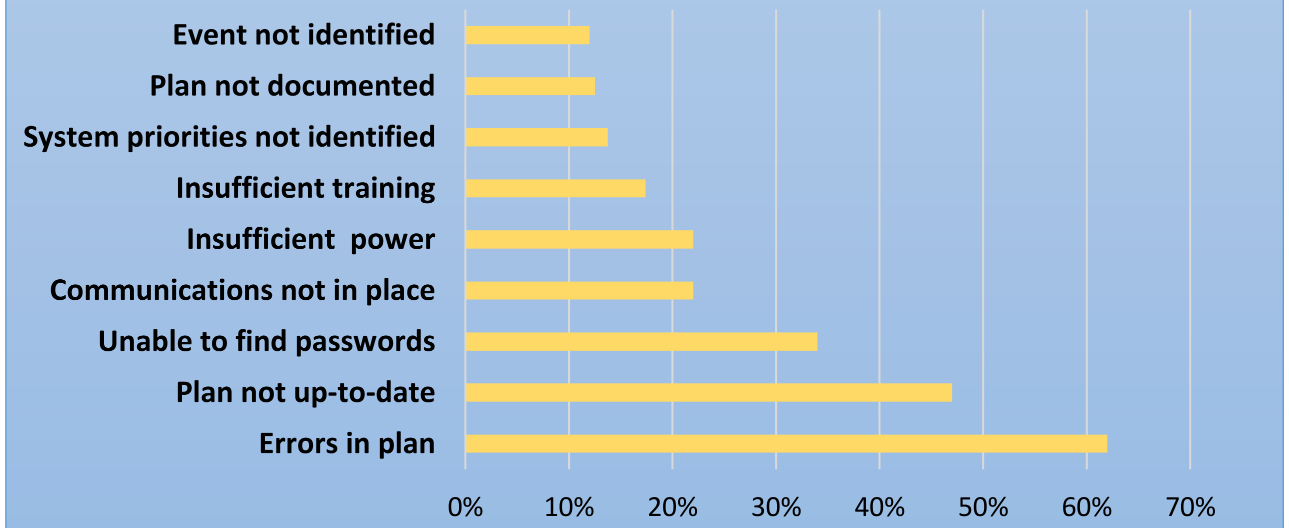
Contingency plans must be practiced and tested

…to be sure the plan is good, everyone is prepared and knows what to do

Can range from:

- *Checklist review*
- *Tabletop exercise*
- *Structured walk-through*
- *Dry-Run tests*

Common Failures in Activating
Disaster Recovery & Business Continuity Plans



Janco Associates, Inc. (2012)

https://www.e-janco.com/PR20110304.html

Agenda

- ✓Computer virus
- ✓Malicious software
  - ✓Proliferation of malware
  - ✓Malware components
  - ✓Anti-malware components
  - ✓Best practices for protection
- ✓Business Continuity and Disaster Contingency Planning
- Incident Response Planning
- Team Project Q&A

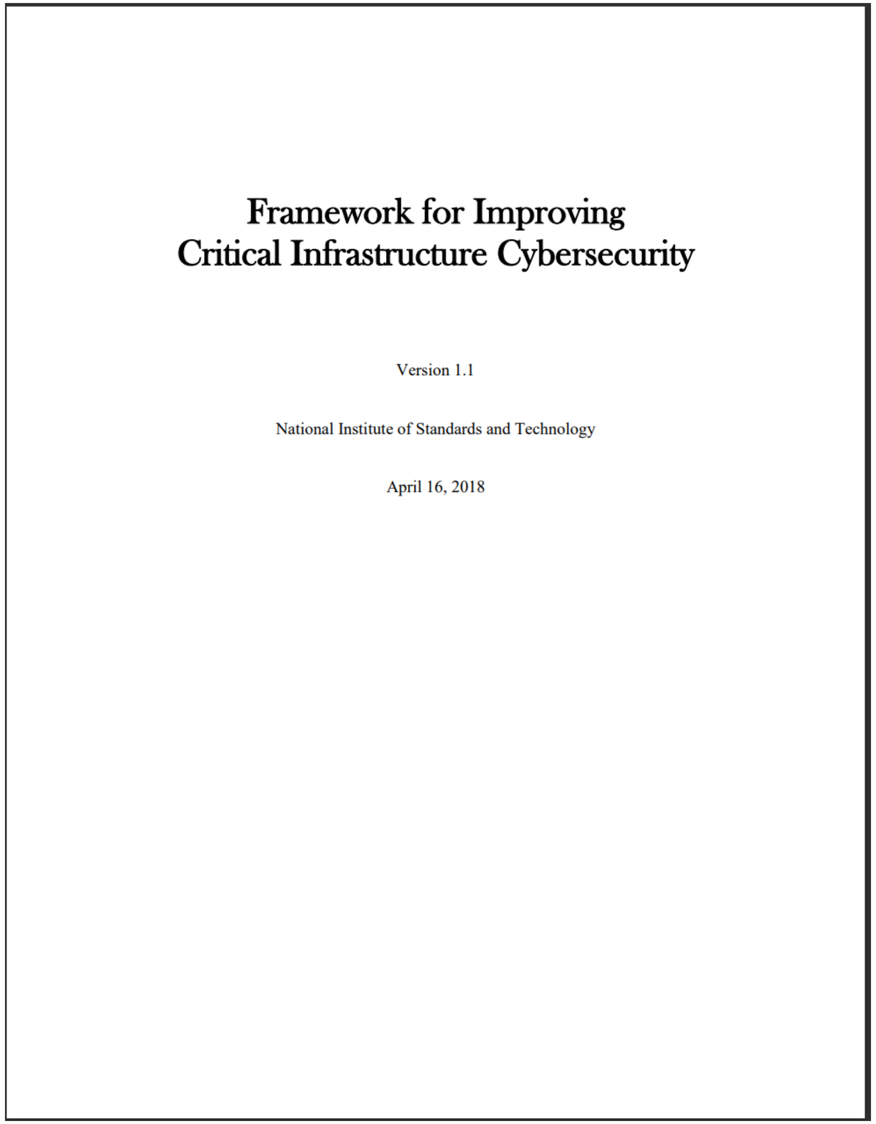
Disaster Recovery Versus Incident Response

The key difference in the principles of incident response and disaster recovery is the **focus of their response**

  - **Disaster recovery plans** reduce risks and damage caused by unexpected disasters like weather events, equipment damage, or human errors that have negative business impacts
  - **Incident response** handles countermeasures that mitigate the risks of an active data breach

- Incident response plans ensure that the right personnel and procedures are in place to effectively deal with a network security incident as it occurs
  - Having an incident response plan in place provides a targeted response to contain and remove the threat

NIST “Cybersecurity Framework”

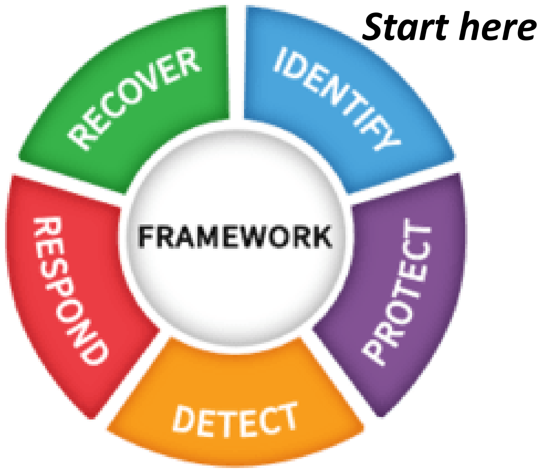


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



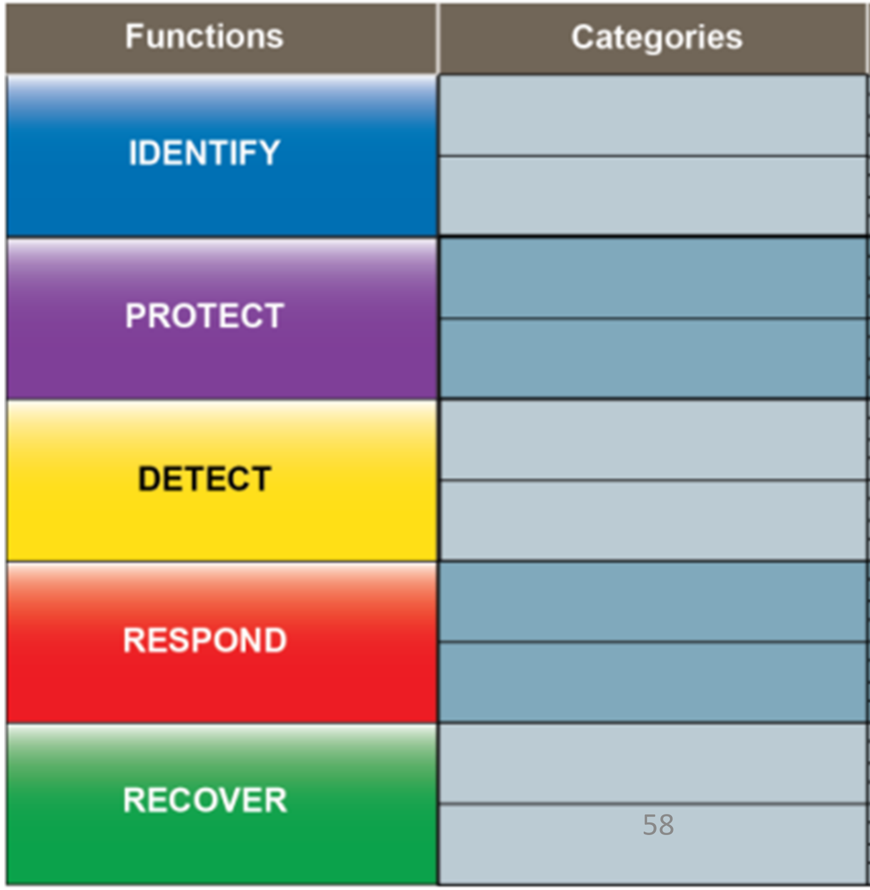
What assets need protection?

What safeguards are available ?

What techniques can identify incidents ?

What techniques can contain impacts of incidents ?

What techniques can restore capabilities?



Functions	Categories
IDENTIFY	
PROTECT	
DETECT	
RESPOND	
RECOVER	

NIST Cybersecurity Framework

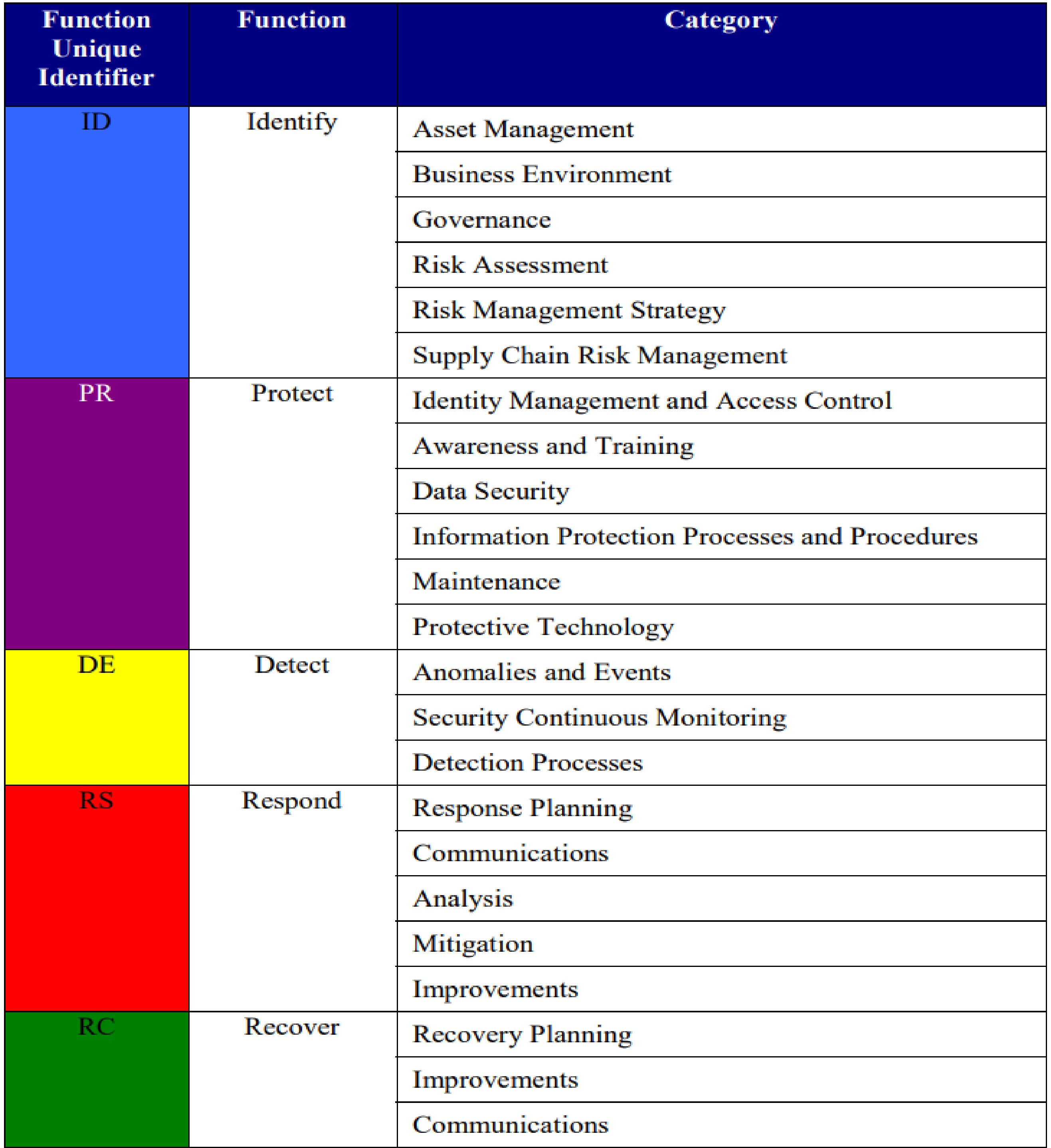
What assets need protection?

What safeguards are available ?

What techniques can identify incidents ?

What techniques can contain impacts of incidents ?

What techniques can restore capabilities ?



Function Unique Identifier	Function	Category
ID	Identify	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management
PR	Protect	Identity Management and Access Control
		Awareness and Training
		Data Security
		Information Protection Processes and Procedures
		Maintenance
		Protective Technology
DE	Detect	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
RS	Respond	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
RC	Recover	Recovery Planning
		Improvements
		Communications

Computer security incident response - vocabulary

Event – any observable occurrence in a system or a network, e.g.

- User sending an email
- User connecting to a file share (i.e. file folder on another computer)
- Server receiving a request for a web page
- Firewall blocking a connection attempt

Adverse event – is an event with a negative consequence, e.g.

- System crash
- Execution of malware that destroys data
- Unauthorized use of system privileges

Computer security incident response - vocabulary

Computer security incident – is a violation (or imminent threat) of computer security policies, acceptable use policies, or standard practices, e.g.

- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money
- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash
- A user provides or exposes sensitive information to others by mistake or on purpose

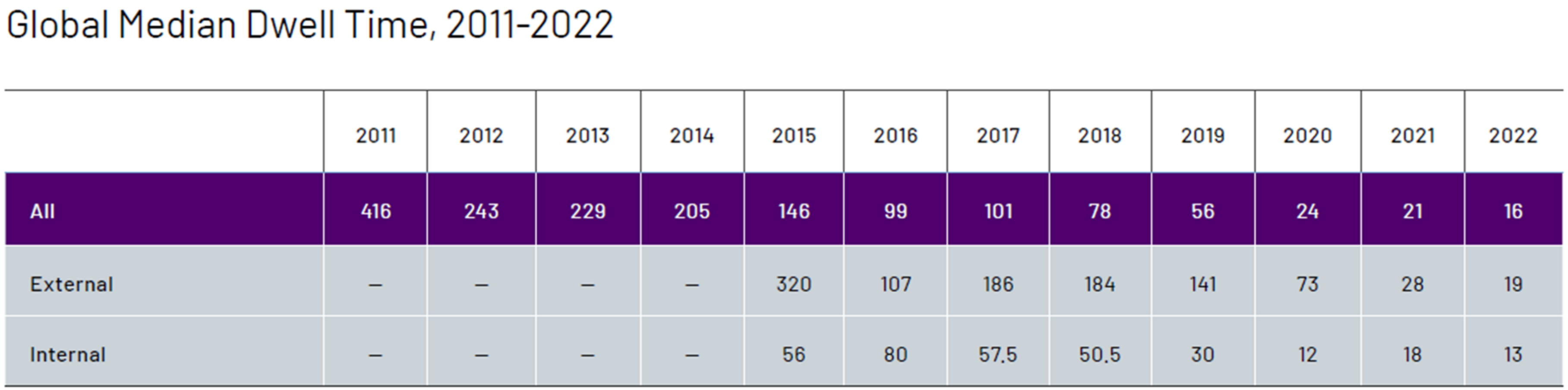
Computer security incident response

Is necessary because…

- Computer security controls, systems, and processes are not perfect
- Protections designed to protect information and information systems eventually fail
- Security breaches are inevitable

- An incident response plan ensures that in the event of a security breach:
  - The right personnel and procedures are in place to effectively deal with a network security incident as it occurs
  - A targeted response is provided to contain and remove the threat

How long are attackers in compromised networks?



Global Median Dwell Time, 2011-2022

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
All	416	243	229	205	146	99	101	78	56	24	21	16
External	–	–	–	–	320	107	186	184	141	73	28	19
Internal	–	–	–	–	56	80	57.5	50.5	30	12	18	13

*“**Dwell time** is calculated as the number of days an attacker is present in a victim environment before they are detected.”*

https://www.mandiant.com/m-trends

Handling an Incident

Incident response process has several phases:

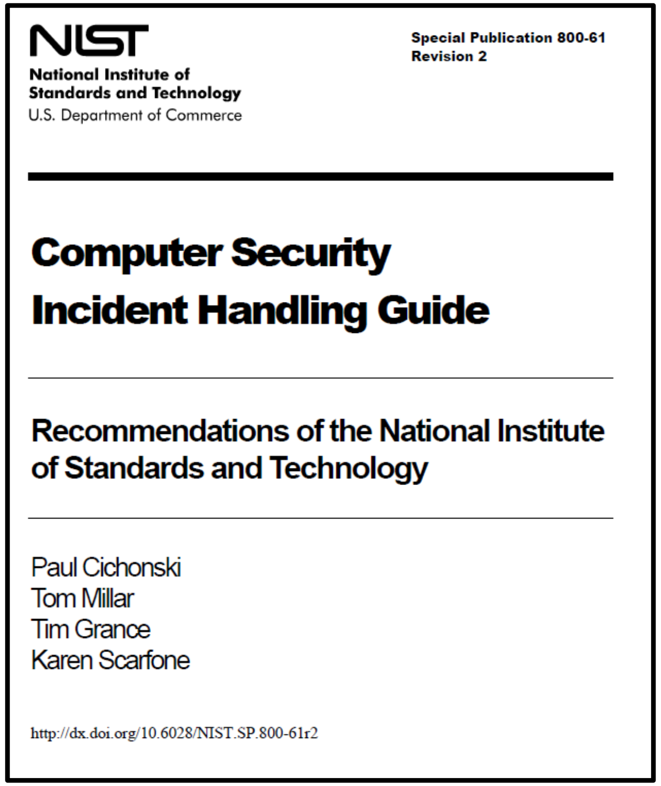
1. **Preparation** - the business attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments
   - o **Residual risk** will inevitably persist after controls are implemented

2. **Detection and analysis** - of security breaches is necessary to alert the organization when incidents occur

3. **Containment, Eradication & Recovery** - the organization works to mitigate the impact of the incident by containing it and ultimately recovering from it
   - o Activity often cycles back to detection and analysis

     E.g., to see if additional hosts are infected by malware while eradicating malware

4. **Post-Incident Activity** - After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

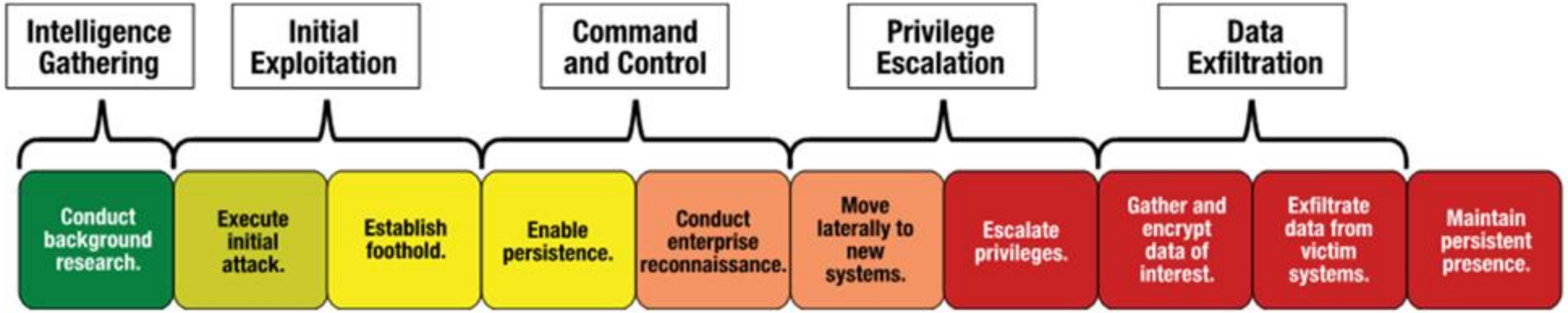
Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

What might attackers be doing in compromised networks during incidents?



Intelligence Gathering

- Conduct background research.

Initial Exploitation

- Execute initial attack.
- Establish foothold.

Command and Control

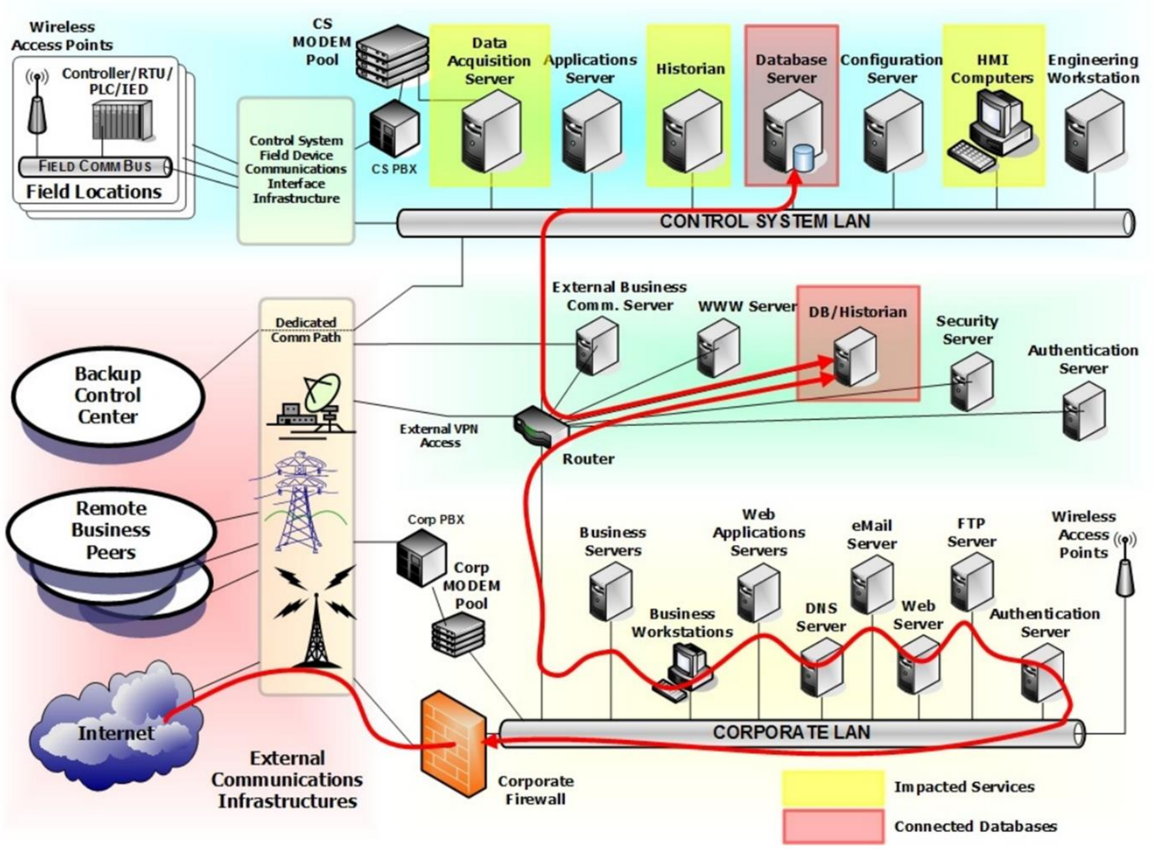
- Enable persistence.
- Conduct enterprise reconnaissance.

Privilege Escalation

- Move laterally to new systems.
- Escalate privileges.

Data Exfiltration

- Gather and encrypt data of interest.
- Exfiltrate data from victim systems.
- Maintain persistent presence.



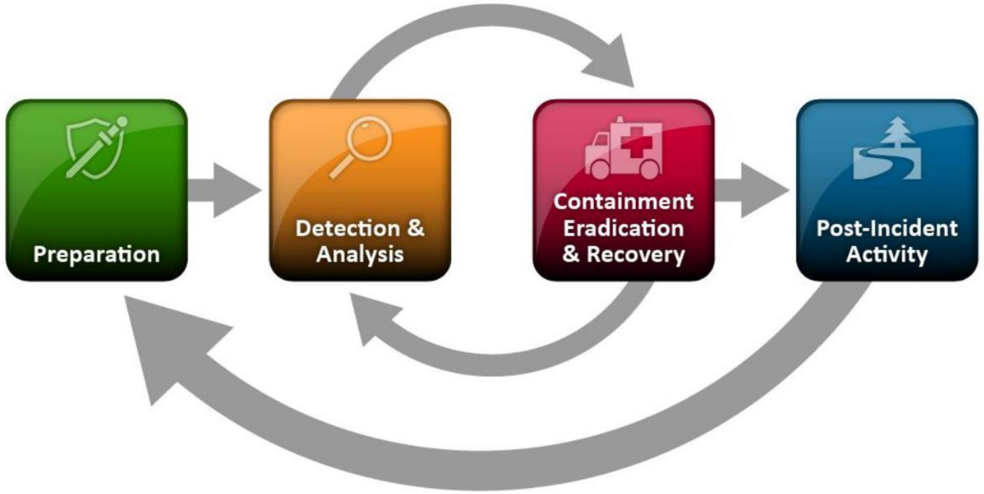
Handling an Incident - Preparation

Preventing Incidents – Keeping the number of incidents reasonably low is very important to protect the business processes of the organization

- If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team
- This can lead to slow and incomplete responses, which translate to a larger negative business impact (e.g., more extensive damage, longer periods of service and data unavailability)

Incident response preparation includes preventing incidents by ensuring that systems, networks, and applications are sufficiently secure

- Risk Assessments
- Host Security
- Network Security
- Malware Prevention
- User Awareness and Training



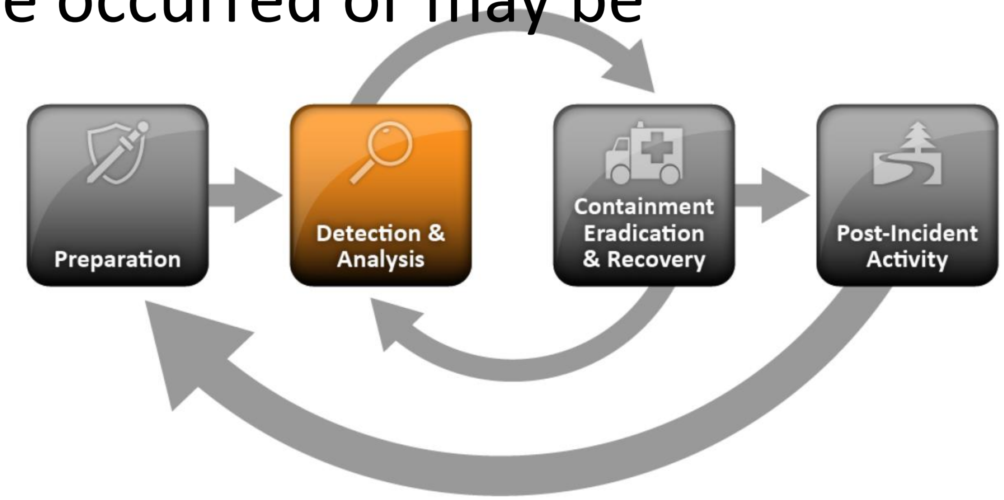
Handling an Incident – Detection and Analysis

Signs of an incident

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem

Signs of an incident fall into one of two categories:

1. **Precursors** – a sign that an incident may occur in the future
2. **Indicators** - a sign that an incident may have occurred or may be occurring now

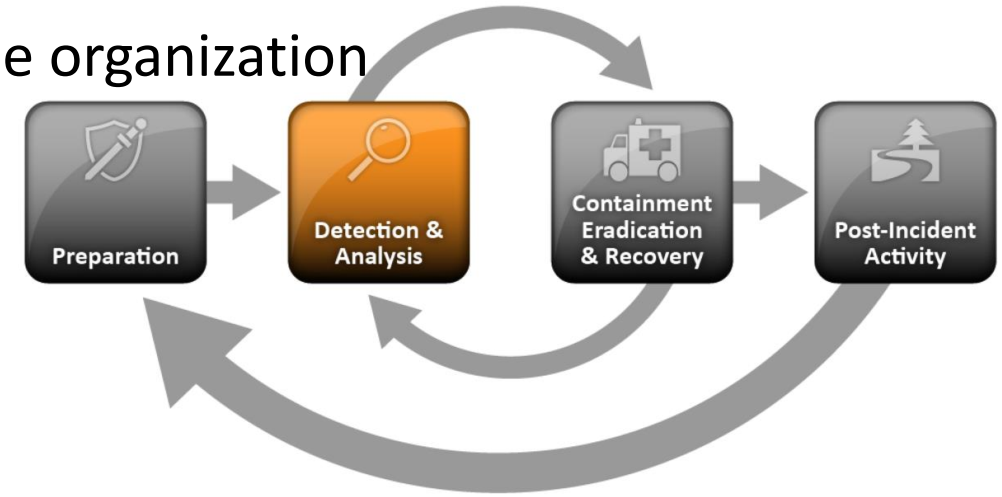


Handling an Incident – Detection and Analysis

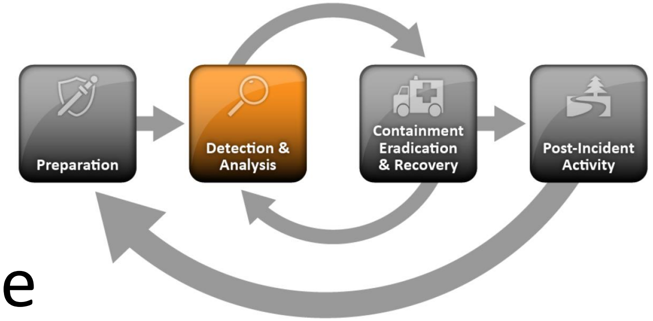
Precursors – While rare, if precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.

Examples of precursors are:

- Web server log entries that show the usage of a vulnerability scanner
- NIST National Vulnerability Database (NVD) Announcement of a new exploit targeting a vulnerability of the organization’s mail server
- A threat from a group stating the group will attack the organization

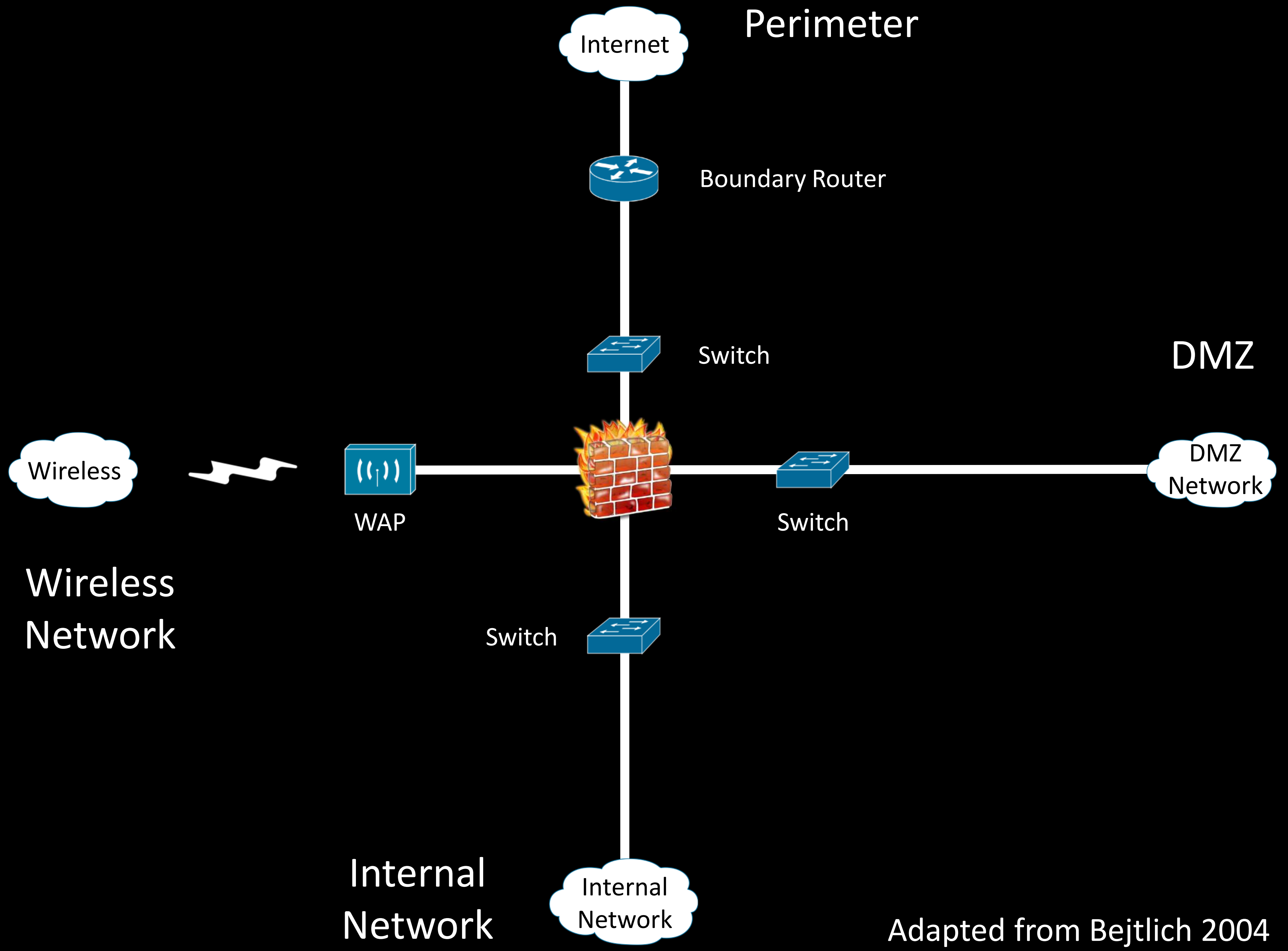


Detection and Analysis

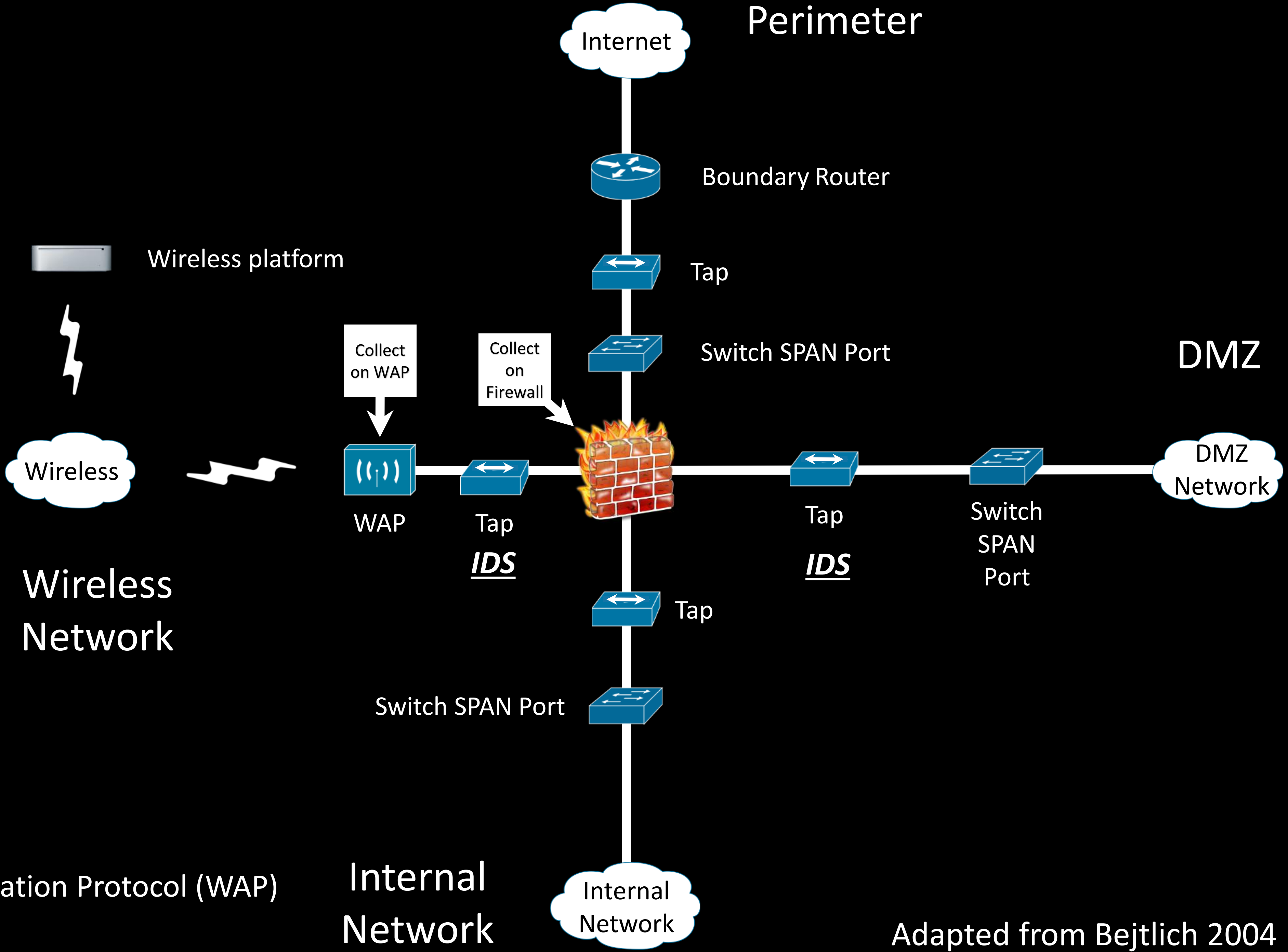


Indicators - While precursors are relatively rare, indicators are all too common. Too many types of indicators exist to exhaustively list them, but some examples are listed below:

- An application logs multiple failed login attempts from an unfamiliar remote system
- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server
- A system administrator sees a filename with unusual characters
- Antivirus software alerts when it detects that a host is infected with malware
- A host records a configuration change in its log
- An email administrator sees a large number of bounced emails with suspicious content
- A network administrator notices an unusual deviation from typical network traffic flows



Adapted from Bejtlich 2004



Perimeter

Internet

Boundary Router

Tap

Switch SPAN Port

Wireless platform

Collect on WAP

Collect on Firewall

DMZ

Wireless

WAP

Tap

IDS

Tap

IDS

Switch SPAN Port

DMZ Network

Wireless Network

Tap

Switch SPAN Port

Internal Network

Internal Network

Wireless Application Protocol (WAP)

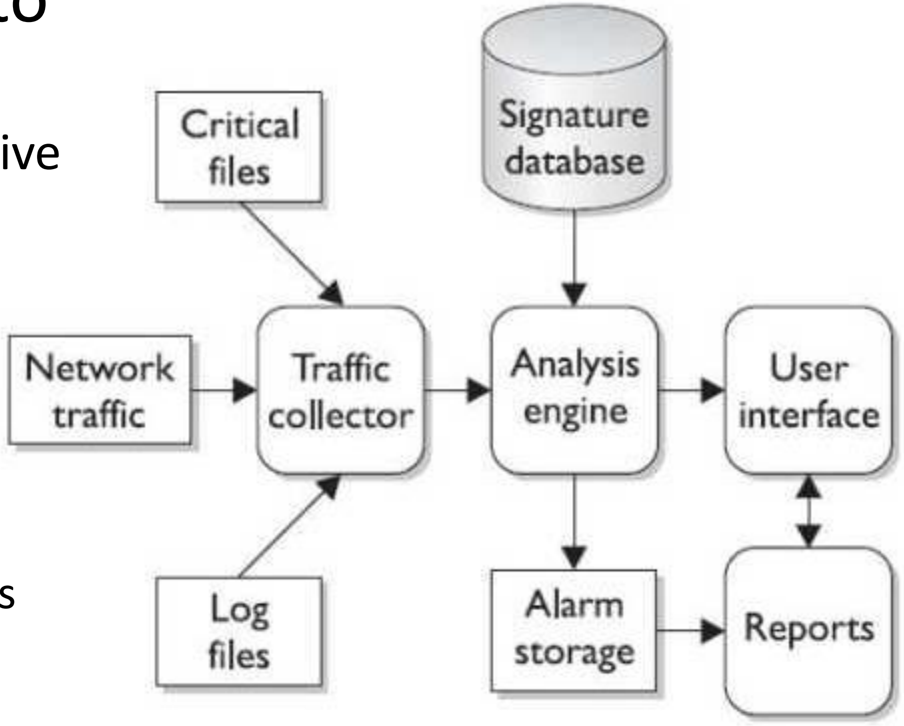
Adapted from Bejtlich 2004

Intrusion Detection Systems (IDSs)

While firewalls and antivirus are preventive controls, IDS are access control monitoring devices designed to

1. Detect a security breach
2. Aid in mitigating damage caused by hackers breaking into sensitive computer and network systems

- IDS' components
  1. Sensors
     - Collect and send traffic and user activity data to analyzers
  2. Analyzers
     - Look for suspicious activity and if found sends alert to administrator's interface
  3. Administrative interfaces



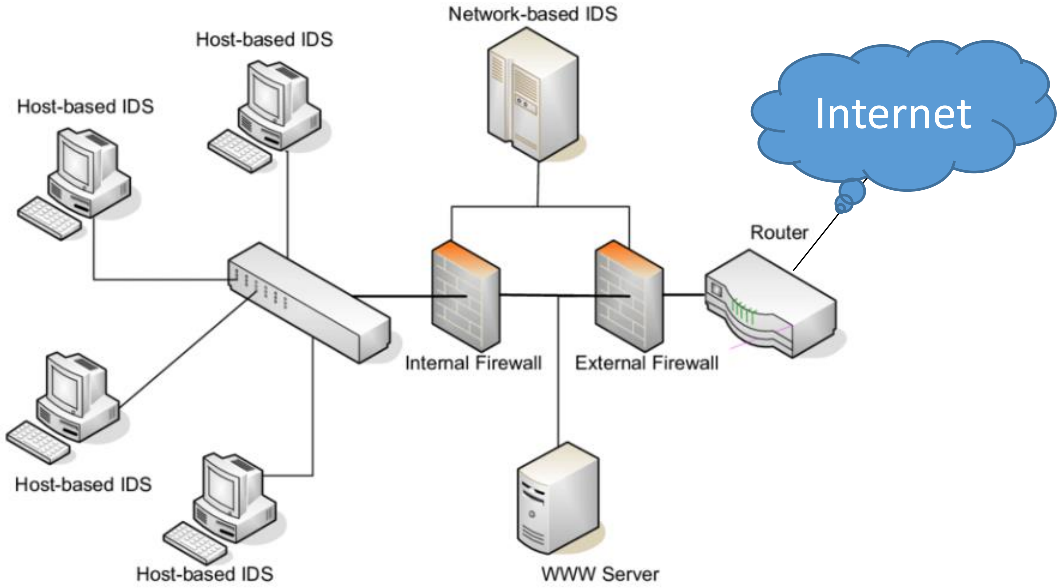
Intrusion Detection Systems (IDSs)

Two main types of IDS

1. **Host-based** for analyzing activity within a particular computer system
2. **Network-based** for monitoring network communications

IDS can be configured to:

- Watch for attacks
- Alert administrator as attacks happen
- Expose a hacker & her/his techniques
- Work with firewalls to terminate a connection



Intrusion Prevention Systems (IPS)

IDS – Detect something bad may be taking place and send an alert

Detective and "after the fact" response

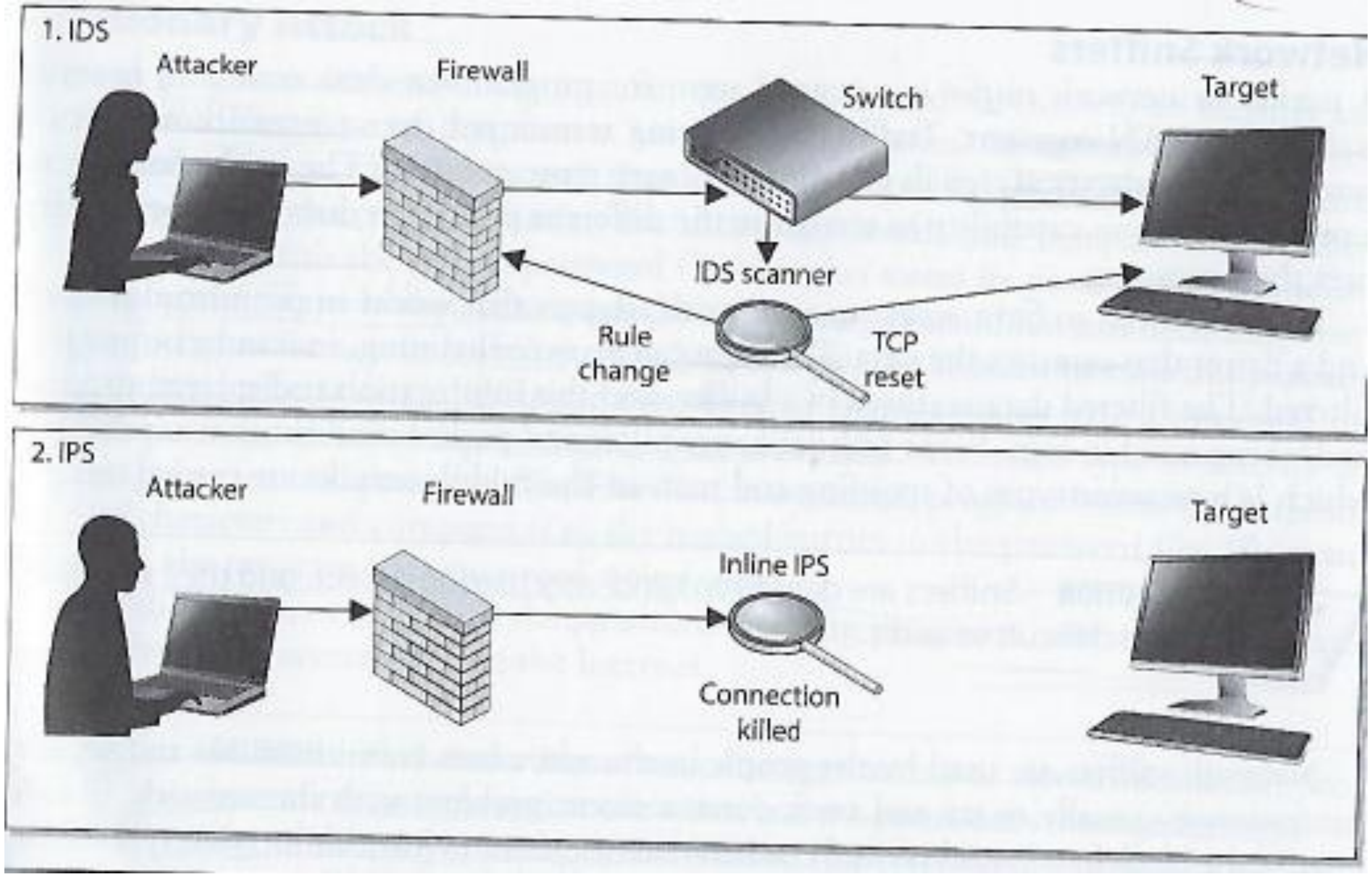
- IPS – Detect something bad may be taking place and block traffic from gaining access to target
    - *Preventive and proactive response*

    - *IPS can be host-based or network-based (like IDS)*
    - *Can be content-based (looking deep into packets), conduct protocol analysis or be signature matching*
    - *Also can use rate-based metrics to identify suspicious increases in volumes of traffic*
        - *E.g. DoS – flood attack*
        - *Traffic flow anomalies – "slow and low" stealth attack attempting to be undetected*

IDS versus IPS

Possible responses to a triggered event:

- Disconnect communications and block transmission of traffic
- Block a user from accessing a resource
- Send alerts of an event trigger to other hosts, IDS monitors and administrators



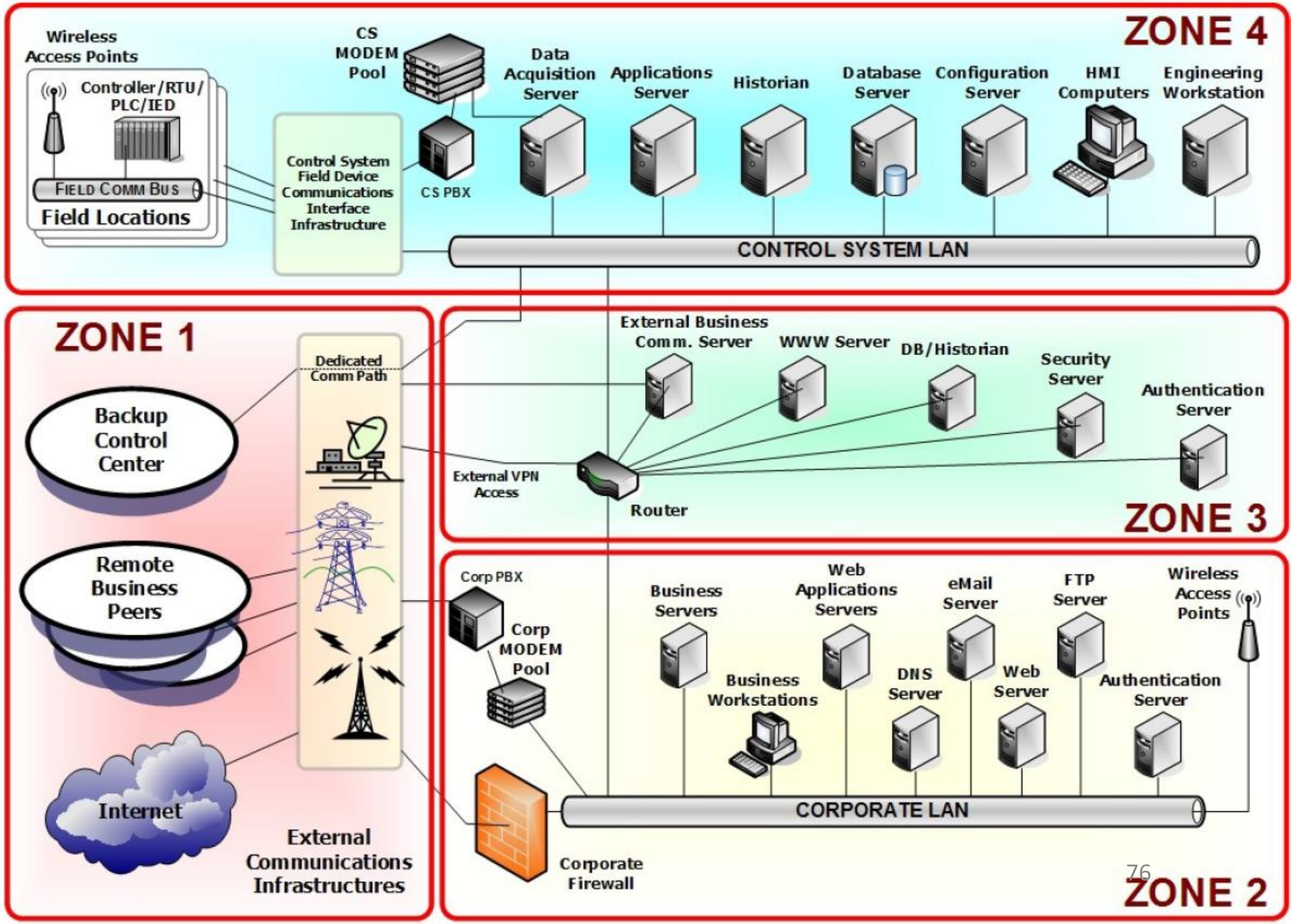
Network Security: Begins with understanding roles of assets in the topology of the network, and moves onto partitioning resources into distinct security zones…

Zone 1: External connectivity to the Internet, peer locations, and back- up facilities

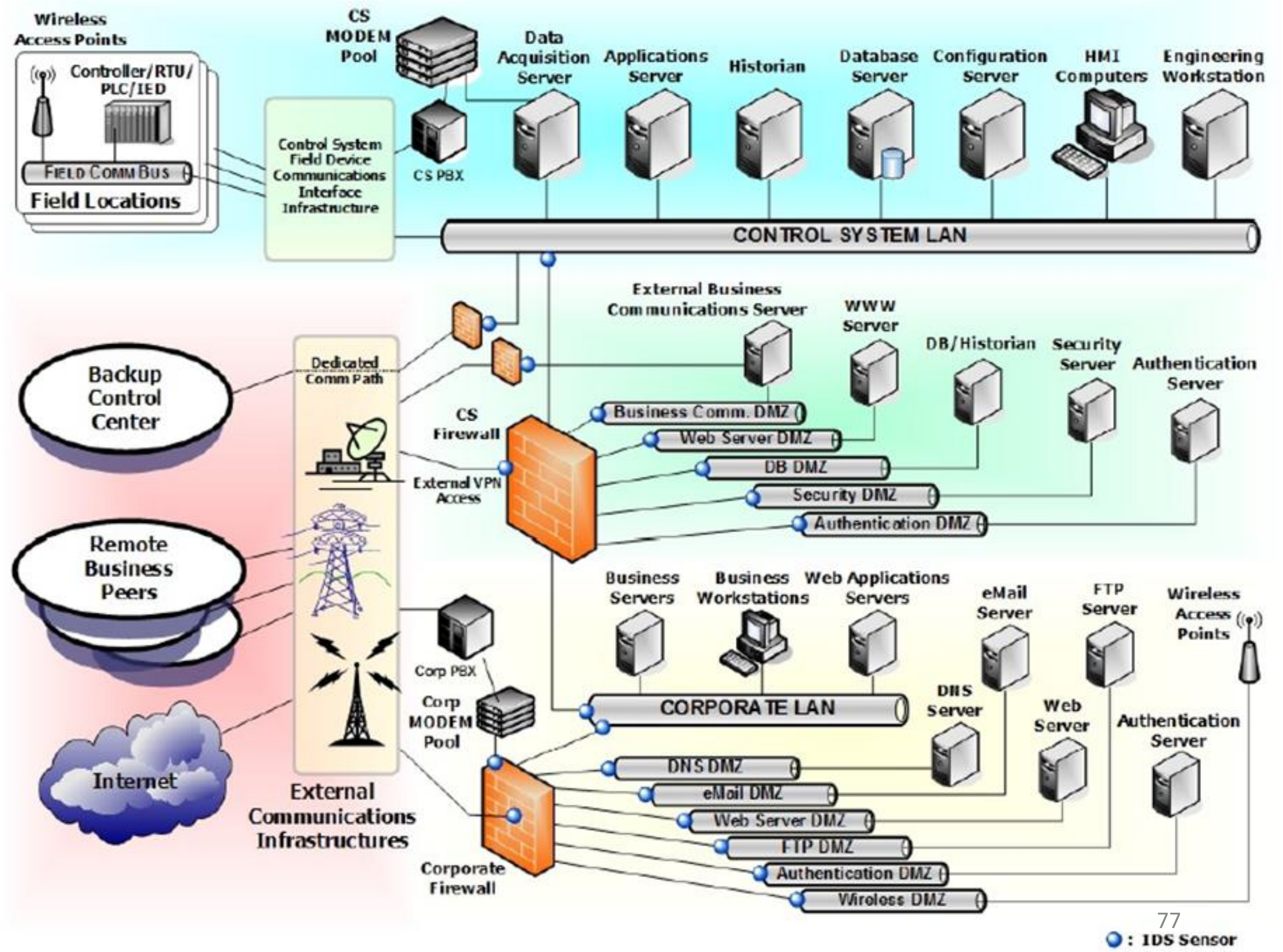
Zone 2: External connectivity and corporate communications

Zone 3: Control systems (in Zone 4) sending and receiving communications to/from external services

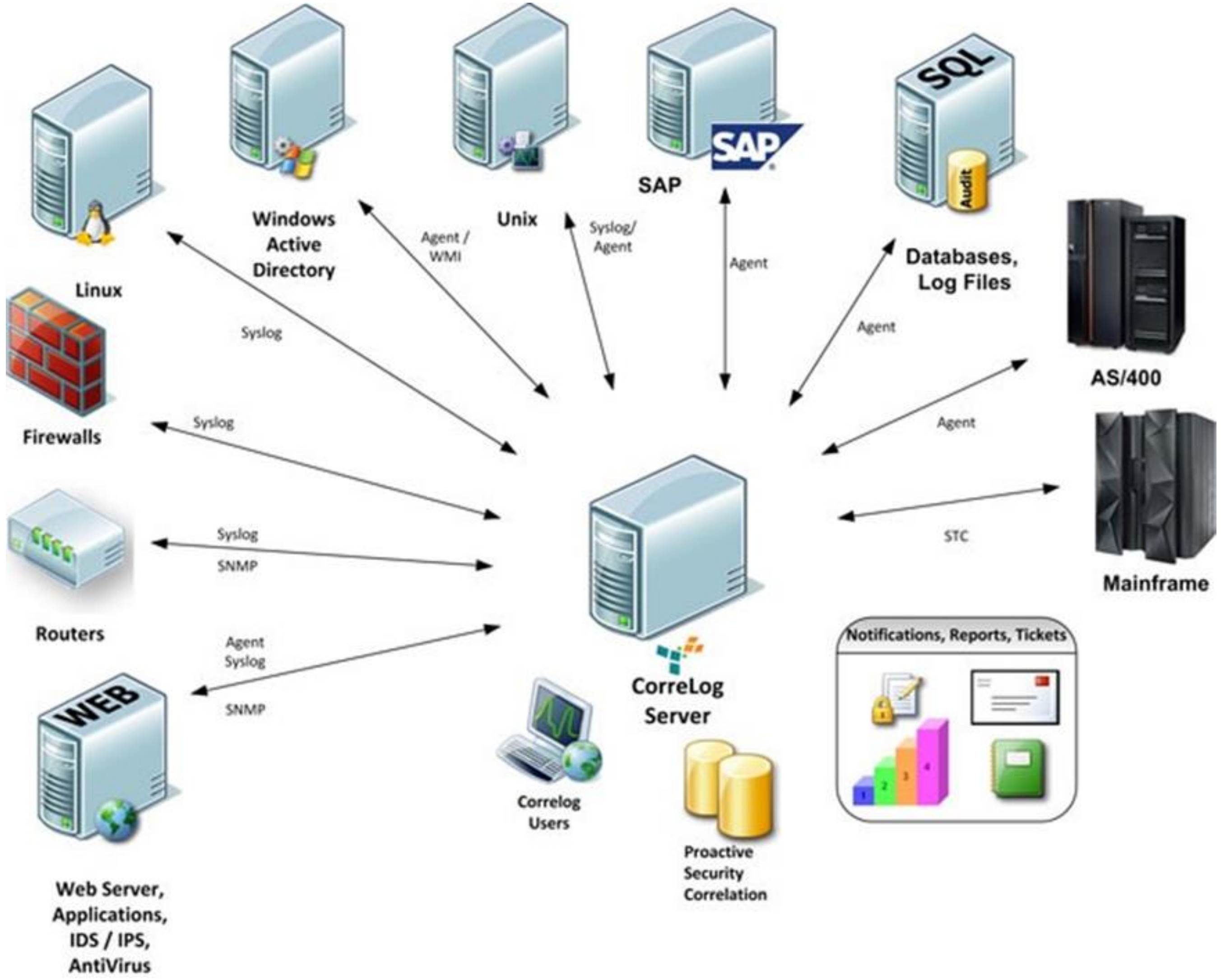
Zone 4: Control systems operations – process based or SCADA



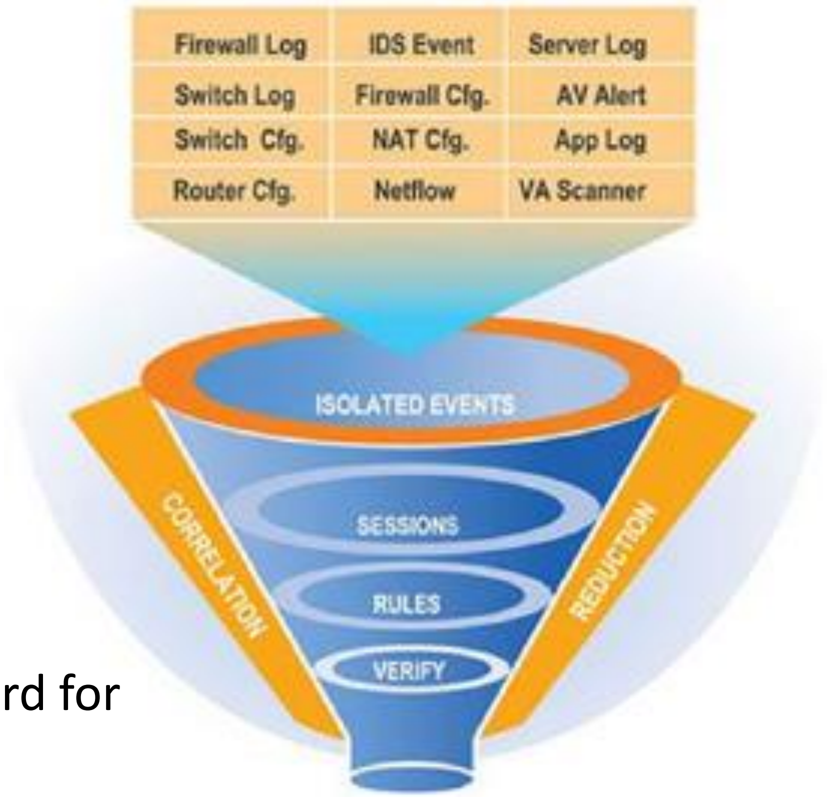
Intrusion Detection System sensors and firewalls located throughout the network



Continuous monitoring with a Security Information and Event Management (SIEM) system



SIEM’s help with Data Analysis and Correlation



- Bring raw data events into one database

- Database software is programmed to look for “Notable events” or correlations

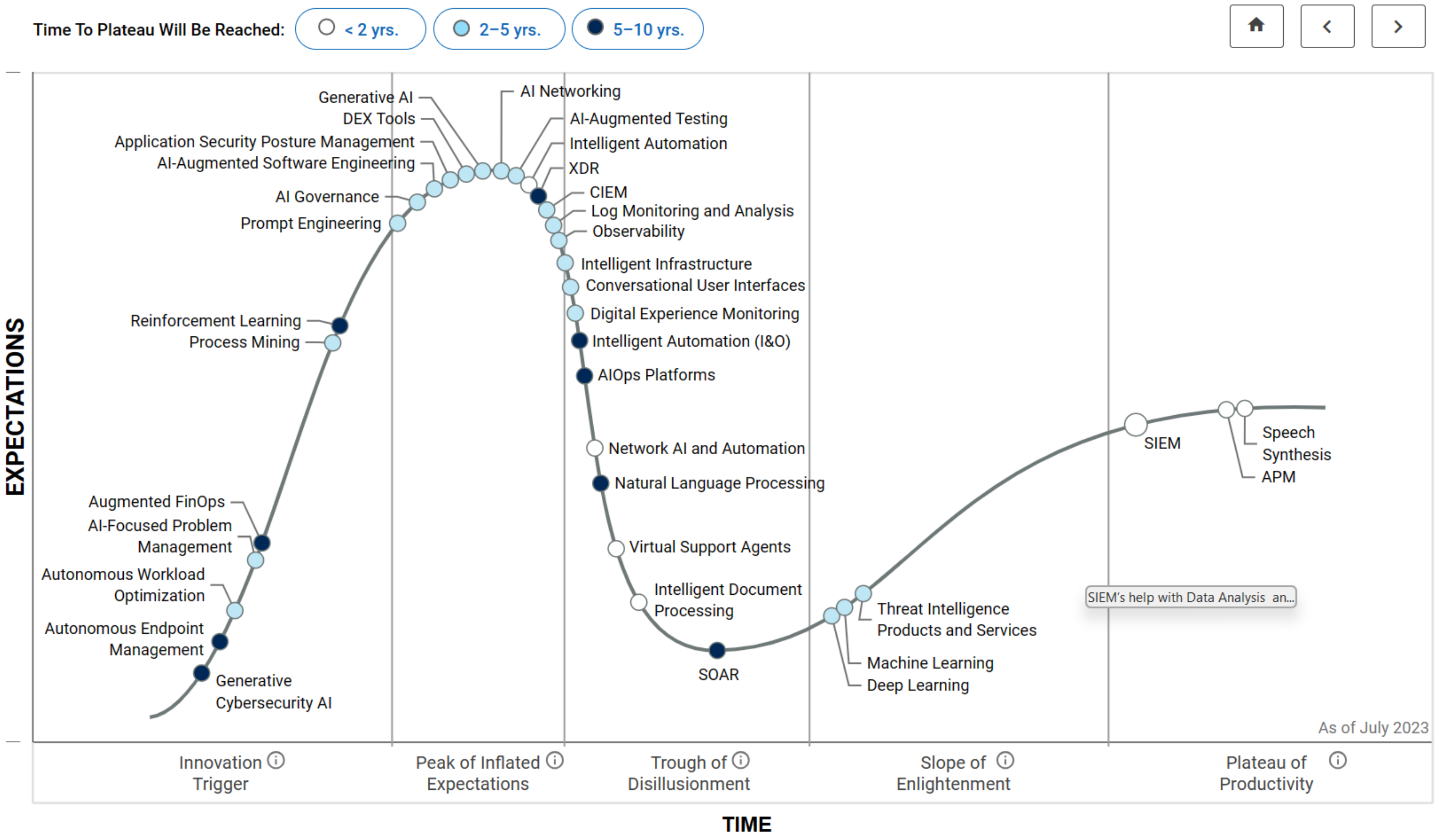
- Correlations will take seemingly isolated events and bring them forward for review/action:
  - **Windows Log:** Employee denied windows login (unknown user account)

  - **Identity Management System:** notes the user account was deleted because employee was terminated last month.

- Security Domains: Access, Endpoints, Networks, Identity

Hype Cycle for IT Management Intelligence, 2023

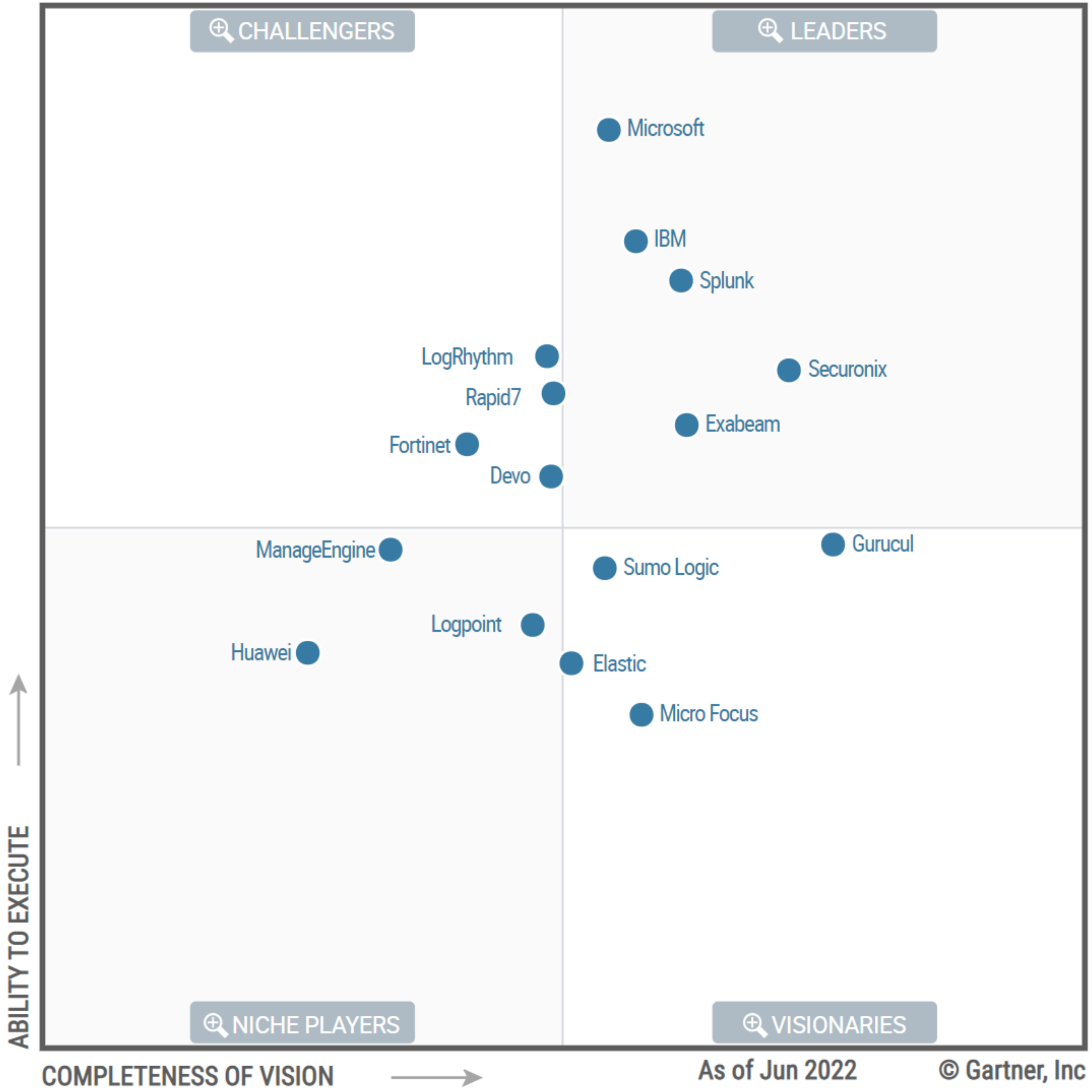
Published 20 July 2023 • ID G00792530
By Cameron Haight, Gartner



SIEM

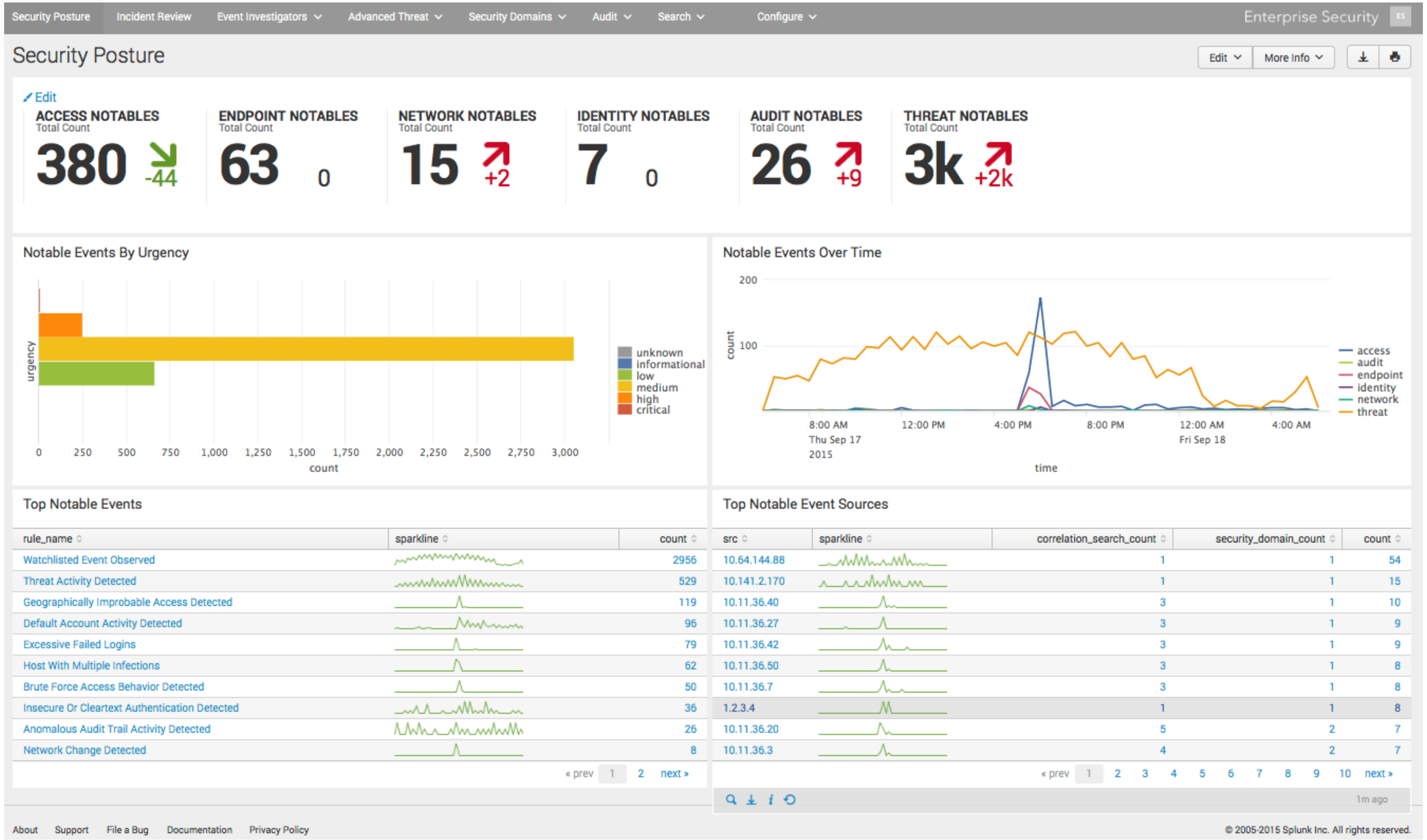
- ***Security Information and Event Management (SIEM)*** market is defined by the customer's need to analyze event data in real time
- Allows for the early detection of targeted attacks and data breaches
- Collect, store, investigate and report on log data for incident response, forensics and regulatory compliance.
- Aggregates event data (logs) produced by security devices, network infrastructure, systems and applications

2022 Magic Quadrant



As of Jun 2022 © Gartner, Inc

splunk>



Security Posture

Edit

ACCESS NOTABLES Total Count	ENDPOINT NOTABLES Total Count	NETWORK NOTABLES Total Count	IDENTITY NOTABLES Total Count	AUDIT NOTABLES Total Count	THREAT NOTABLES Total Count
380 ↘ -44	63 0	15 ↗ +2	7 0	26 ↗ +9	3k ↗ +2k

Notable Events By Urgency

Notable Events Over Time

Top Notable Events

rule_name	sparkline	count
Watchlisted Event Observed		2956
Threat Activity Detected		529
Geographically Improbable Access Detected		119
Default Account Activity Detected		96
Excessive Failed Logins		79
Host With Multiple Infections		62
Brute Force Access Behavior Detected		50
Insecure Or Cleartext Authentication Detected		36
Anomalous Audit Trail Activity Detected		26
Network Change Detected		8

« prev 1 2 next »

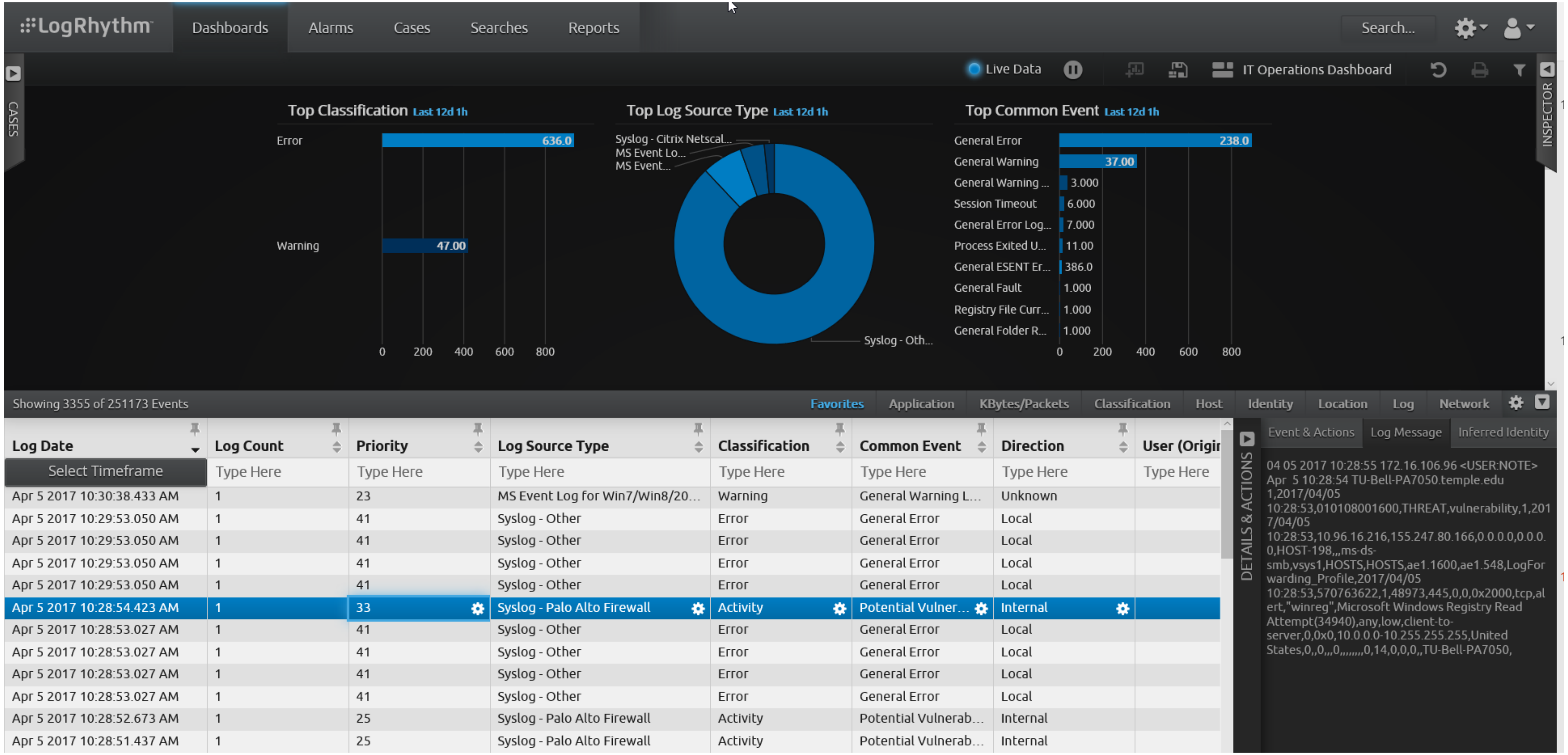
Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
10.64.144.88		1	1	54
10.141.2.170		1	1	15
10.11.36.40		3	1	10
10.11.36.27		3	1	9
10.11.36.42		3	1	9
10.11.36.50		3	1	8
10.11.36.7		3	1	8
1.2.3.4		1	1	8
10.11.36.20		5	2	7
10.11.36.3		4	2	7

« prev 1 2 3 4 5 6 7 8 9 10 next »

1m ago

LogRhythm™



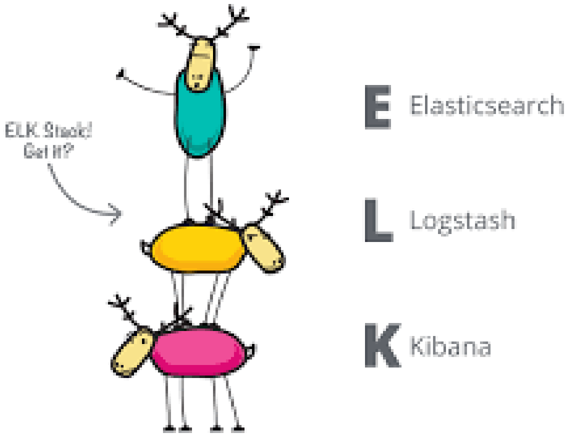
Showing 3355 of 251173 Events

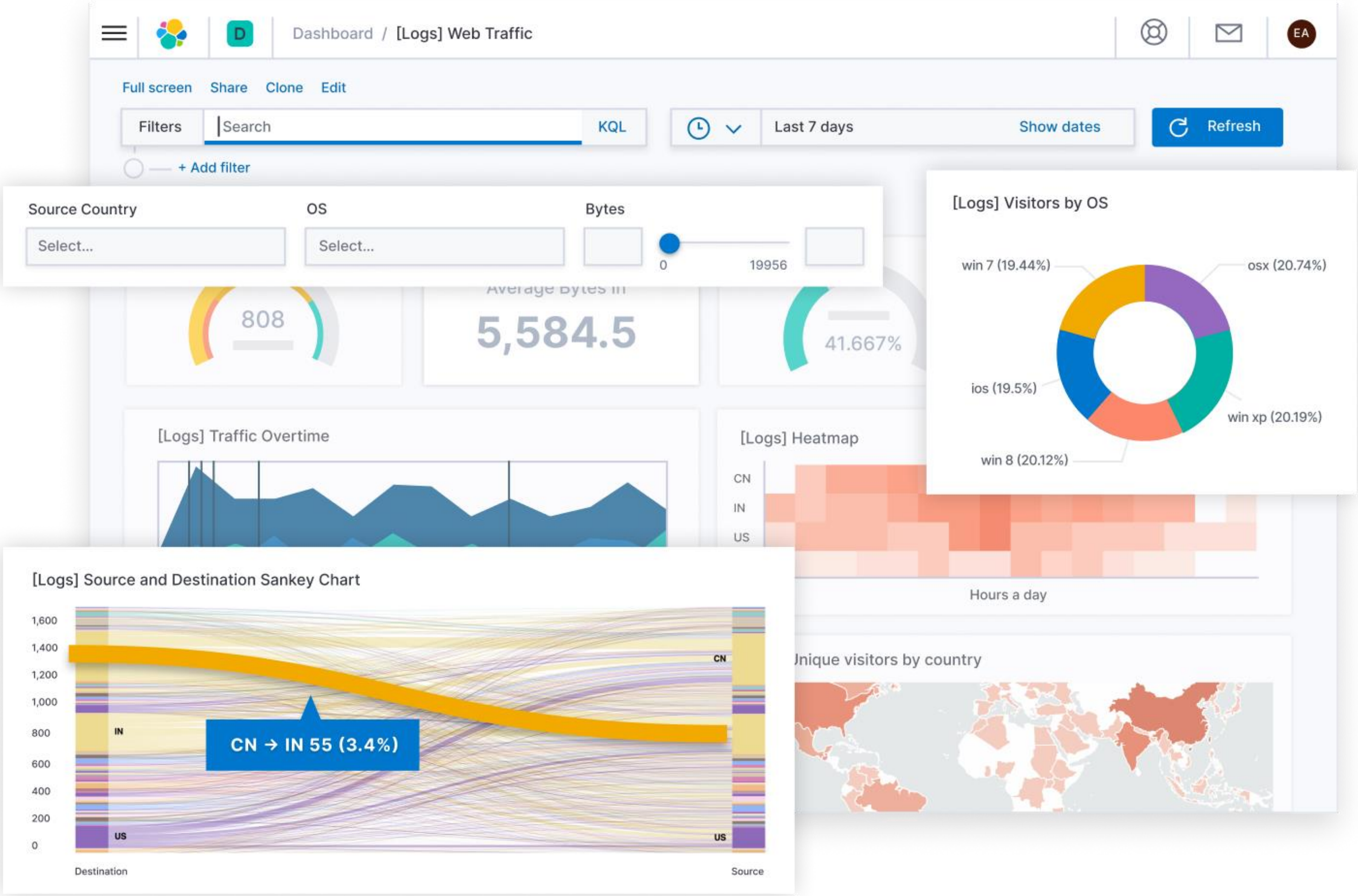
Log Date	Log Count	Priority	Log Source Type	Classification	Common Event	Direction	User (Origir
Select Timeframe	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here
Apr 5 2017 10:30:38.433 AM	1	23	MS Event Log for Win7/Win8/20...	Warning	General Warning L...	Unknown	
Apr 5 2017 10:29:53.050 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:29:53.050 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:29:53.050 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:29:53.050 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:54.423 AM	1	33	Syslog - Palo Alto Firewall	Activity	Potential Vulner...	Internal	
Apr 5 2017 10:28:53.027 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:53.027 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:53.027 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:53.027 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:52.673 AM	1	25	Syslog - Palo Alto Firewall	Activity	Potential Vulnerab...	Internal	
Apr 5 2017 10:28:51.437 AM	1	25	Syslog - Palo Alto Firewall	Activity	Potential Vulnerab...	Internal	

```
04 05 2017 10:28:55 172.16.106.96 <USER:NOTE>
Apr  5 10:28:54 TU-Bell-PA7050.temple.edu
1,2017/04/05
10:28:53,010108001600,THREAT,vulnerability,1,201
7/04/05
10:28:53,10.96.16.216,155.247.80.166,0.0.0.0,0.0.0.
0,HOST-198,,,ms-ds-
smb,vsys1,HOSTS,HOSTS,ae1.1600,ae1.548,LogFor
warding_Profile,2017/04/05
10:28:53,570763622,1,48973,445,0,0,0x2000,tcp,al
ert,"winreg",Microsoft Windows Registry Read
Attempt(34940),any,low,client-to-
server,0,0x0,10.0.0.0-10.255.255.255,United
States,0,,0,,,0,,,,,,,,0,14,0,0,0,,TU-Bell-PA7050,
```

Hybrid – “ELK Stack”

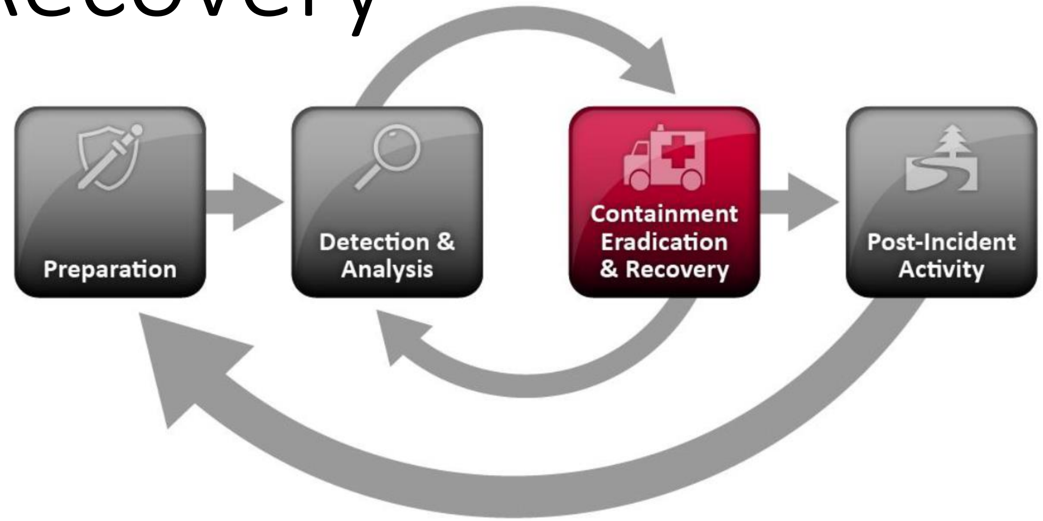
- On-Premises, or…
- Cloud (hosted)





Note: Sankey charts are a type of flow diagram in which the width of the arrows is proportional to the flow rate

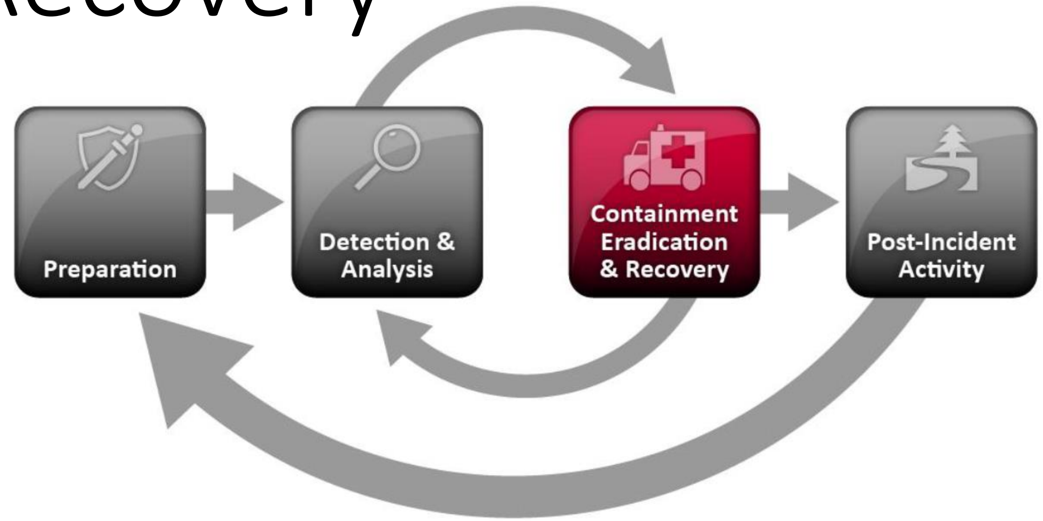
Containment, Eradication, and Recovery



Containment - is important before an incident overwhelms resources or increases damage

- Most incidents require containment, which provides time for developing a tailored remediation strategy
- An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions)
- Criteria for selecting among containment strategies are based on type of incident:
  - Potential damage & theft of resources
  - Need for evidence preservation
  - Service availability requirements (e.g., network connectivity, services provided to external parties)
  - Time & resources needed to implement
  - Effectiveness (e.g., partial containment, full containment)

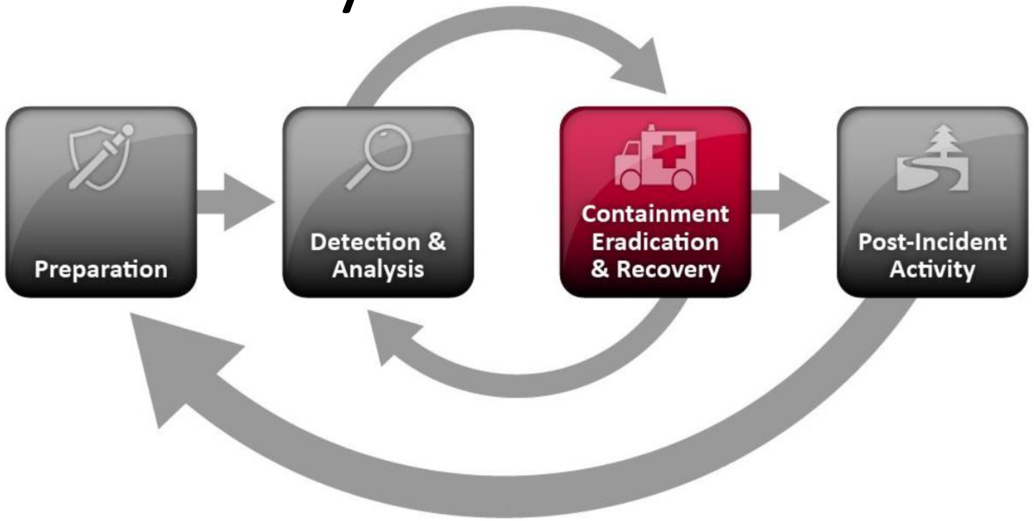
Containment, Eradication, and Recovery



Eradication - After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as:

- Deleting malware
- Disabling breached user accounts
- Identifying and mitigating all vulnerabilities that were exploited
  - *During eradication, it is important to identify all affected hosts within the organization so that they can be remediated*

Containment, Eradication, and Recovery



Recovery - In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents

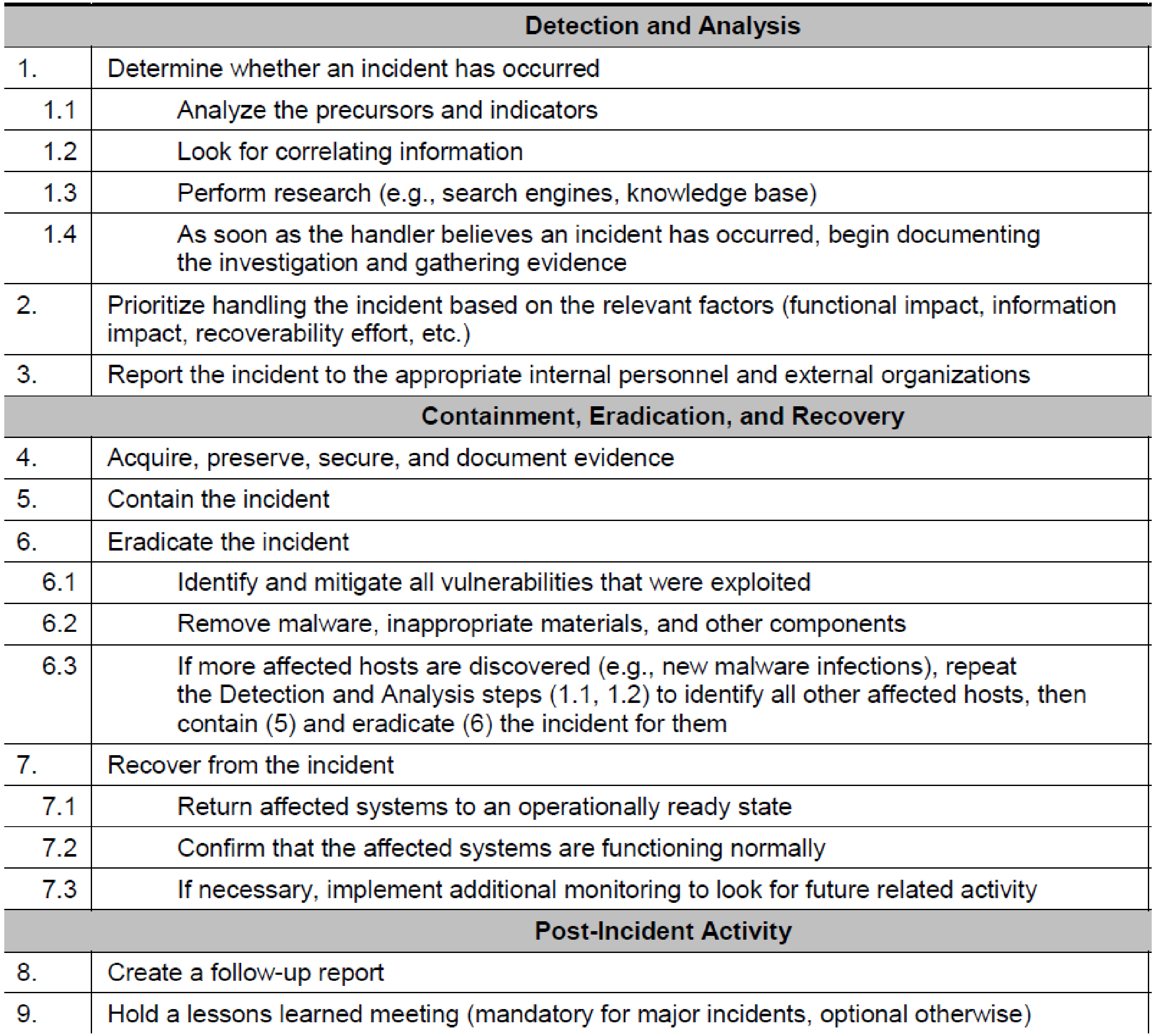
May involve such actions as:

- Restoring systems from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security (e.g. firewall rules, boundary router access control lists, …)

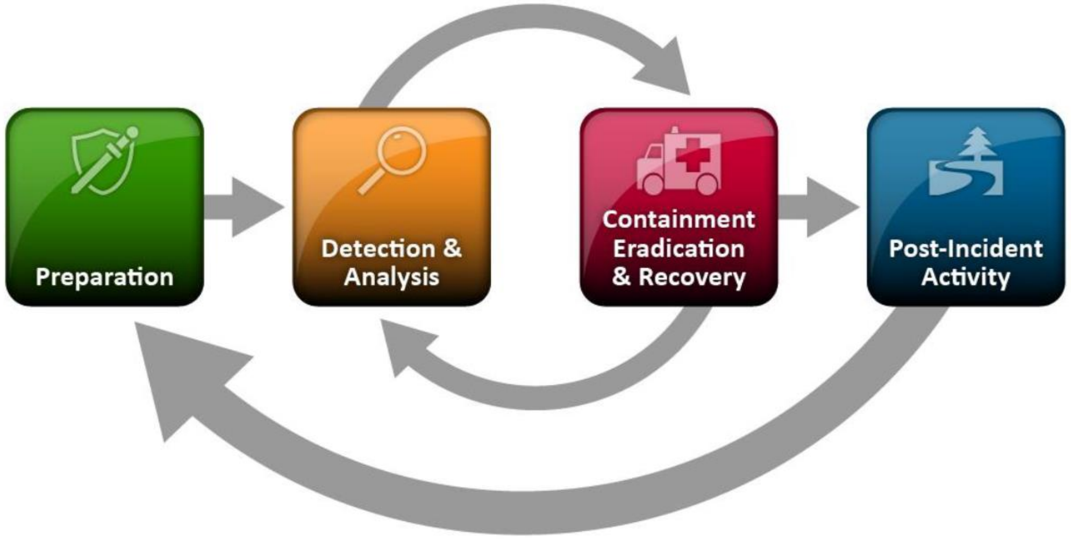
Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner

- As a result, higher levels of system logging or network monitoring are often part of the recovery process

Incident Response Workflow



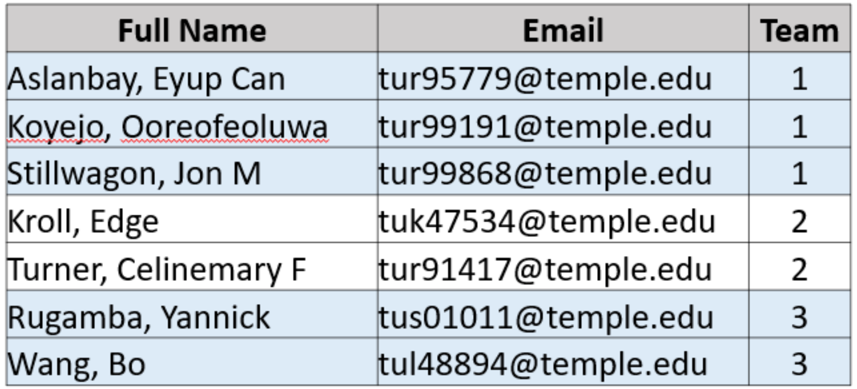
	Detection and Analysis
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators
1.2	Look for correlating information
1.3	Perform research (e.g., search engines, knowledge base)
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3.	Report the incident to the appropriate internal personnel and external organizations
	Containment, Eradication, and Recovery
4.	Acquire, preserve, secure, and document evidence
5.	Contain the incident
6.	Eradicate the incident
6.1	Identify and mitigate all vulnerabilities that were exploited
6.2	Remove malware, inappropriate materials, and other components
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
7.	Recover from the incident
7.1	Return affected systems to an operationally ready state
7.2	Confirm that the affected systems are functioning normally
7.3	If necessary, implement additional monitoring to look for future related activity
	Post-Incident Activity
8.	Create a follow-up report
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)



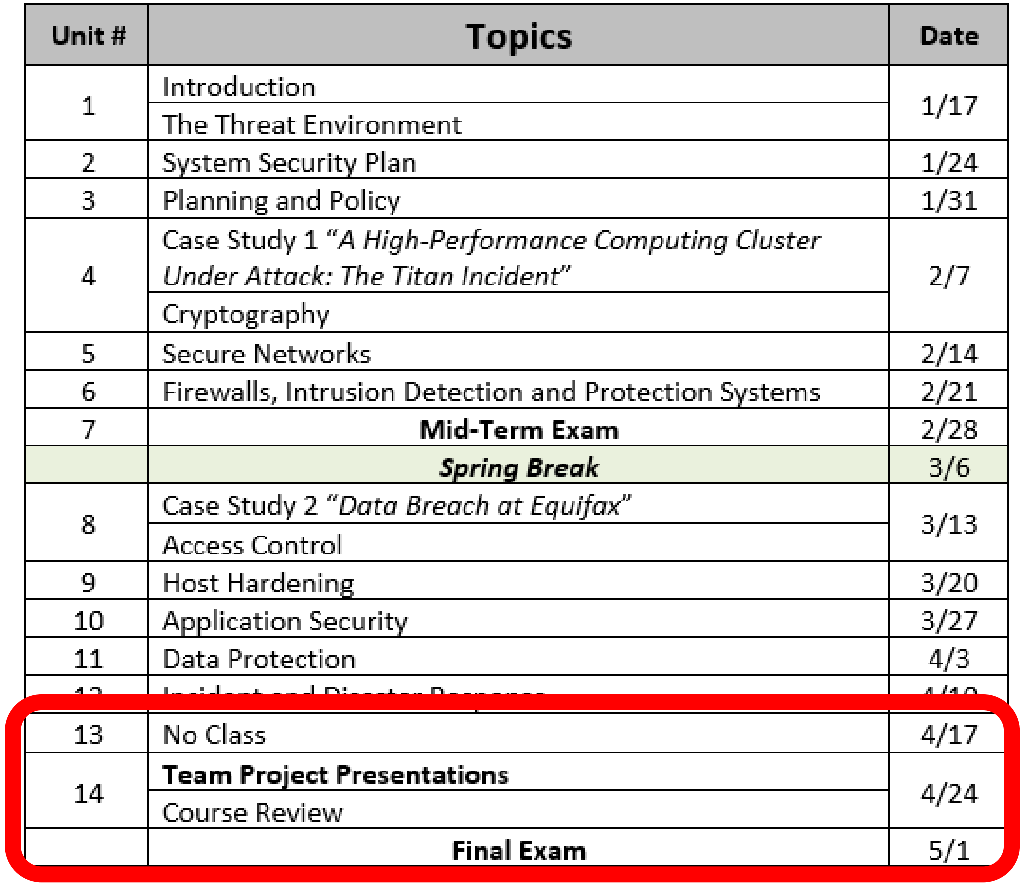
Agenda

- ✓In the News
- ✓Computer virus
- ✓Malicious software
  - ✓Proliferation of malware
  - ✓Malware components
  - ✓Anti-malware components
  - ✓Best practices for protection
- ✓Business Continuity and Disaster Contingency Planning
- ✓Incident Response Planning
- Final Project – Presentation Schedule

Final Project - Presentation Schedule

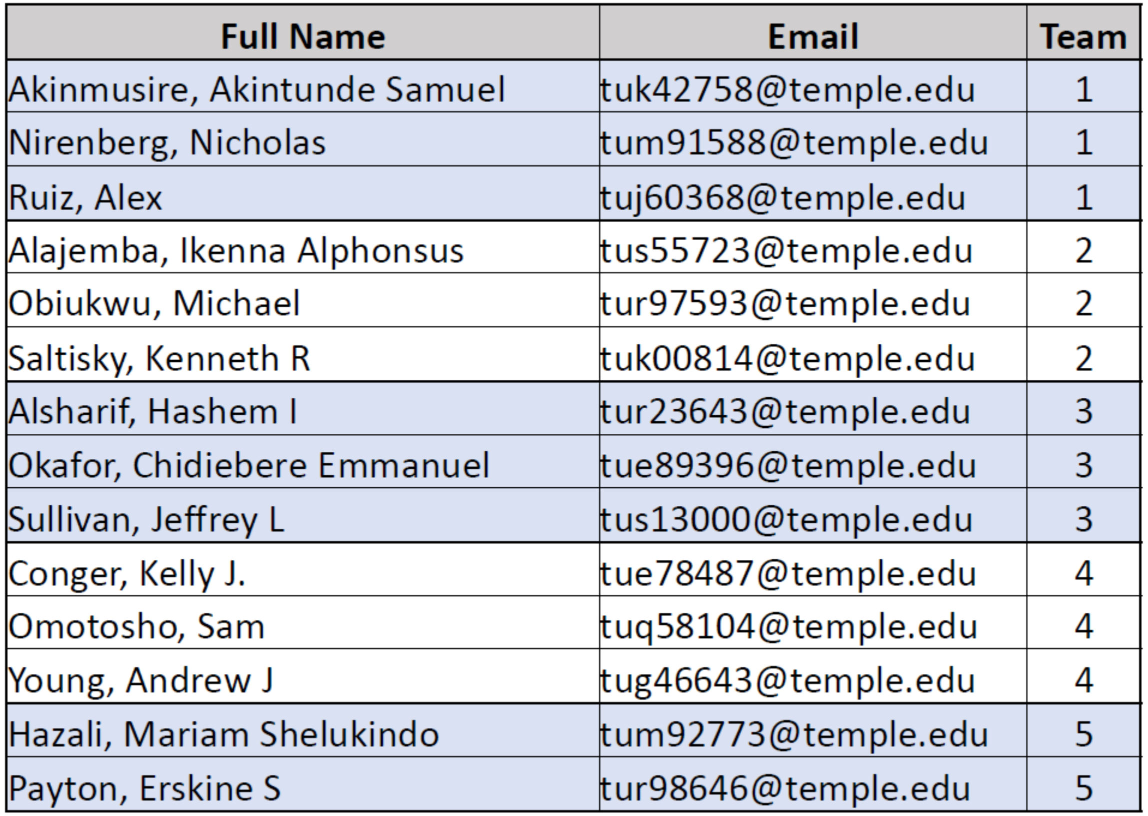


Full Name	Email	Team
Aslanbay, Eyup Can	tur95779@temple.edu	1
Koyejo, Ooreofeoluwa	tur99191@temple.edu	1
Stillwagon, Jon M	tur99868@temple.edu	1
Kroll, Edge	tuk47534@temple.edu	2
Turner, Celinemary F	tur91417@temple.edu	2
Rugamba, Yannick	tus01011@temple.edu	3
Wang, Bo	tul48894@temple.edu	3

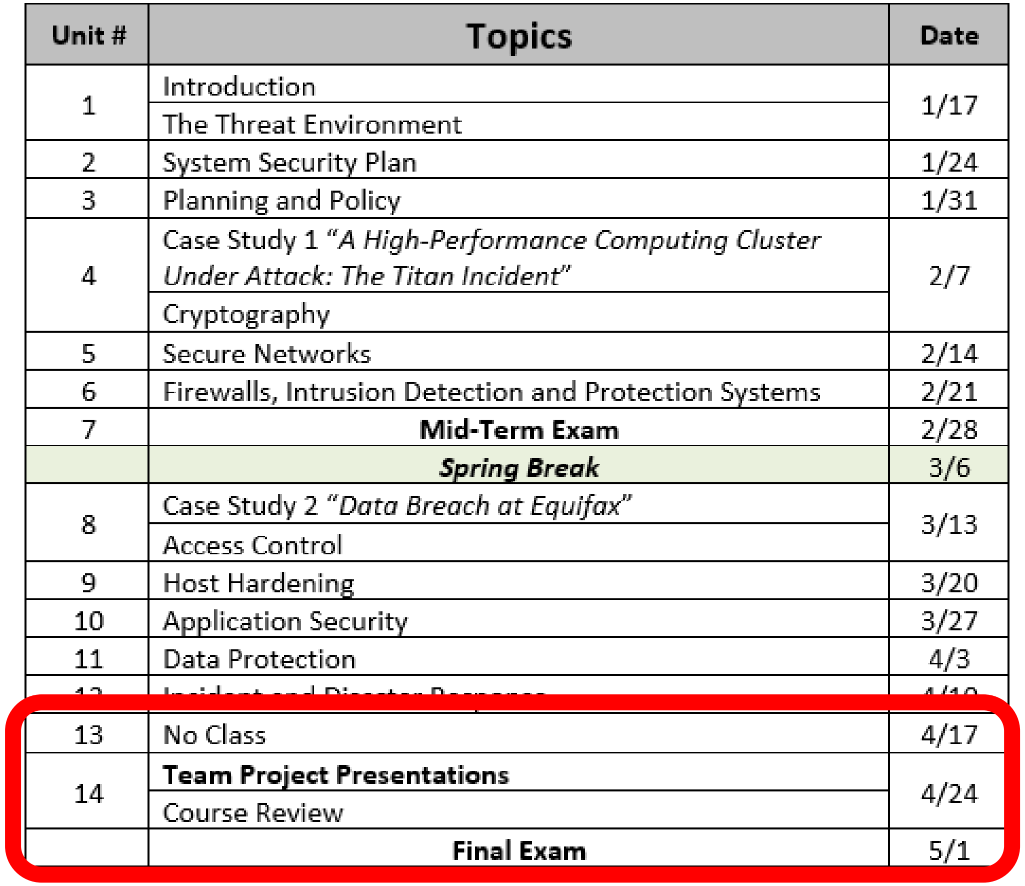


Unit #	Topics	Date
1	Introduction	1/17
	The Threat Environment	
2	System Security Plan	1/24
3	Planning and Policy	1/31
4	Case Study 1 *"A High-Performance Computing Cluster Under Attack: The Titan Incident"*	2/7
	Cryptography	
5	Secure Networks	2/14
6	Firewalls, Intrusion Detection and Protection Systems	2/21
7	**Mid-Term Exam**	2/28
	Spring Break	3/6
8	Case Study 2 *"Data Breach at Equifax"*	3/13
	Access Control	
9	Host Hardening	3/20
10	Application Security	3/27
11	Data Protection	4/3
12	Incident and Disaster Response	4/10
13	No Class	4/17
14	**Team Project Presentations**	4/24
	Course Review	
	Final Exam	5/1

Final Project - Presentation Schedule



Full Name	Email	Team
Akinmusire, Akintunde Samuel	tuk42758@temple.edu	1
Nirenberg, Nicholas	tum91588@temple.edu	1
Ruiz, Alex	tuj60368@temple.edu	1
Alajemba, Ikenna Alphonsus	tus55723@temple.edu	2
Obiukwu, Michael	tur97593@temple.edu	2
Saltisky, Kenneth R	tuk00814@temple.edu	2
Alsharif, Hashem I	tur23643@temple.edu	3
Okafor, Chidiebere Emmanuel	tue89396@temple.edu	3
Sullivan, Jeffrey L	tus13000@temple.edu	3
Conger, Kelly J.	tue78487@temple.edu	4
Omotosho, Sam	tuq58104@temple.edu	4
Young, Andrew J	tug46643@temple.edu	4
Hazali, Mariam Shelukindo	tum92773@temple.edu	5
Payton, Erskine S	tur98646@temple.edu	5



Unit #	Topics	Date
1	Introduction The Threat Environment	1/17
2	System Security Plan	1/24
3	Planning and Policy	1/31
4	Case Study 1 *"A High-Performance Computing Cluster Under Attack: The Titan Incident"* Cryptography	2/7
5	Secure Networks	2/14
6	Firewalls, Intrusion Detection and Protection Systems	2/21
7	**Mid-Term Exam**	2/28
	Spring Break	3/6
8	Case Study 2 *"Data Breach at Equifax"* Access Control	3/13
9	Host Hardening	3/20
10	Application Security	3/27
11	Data Protection	4/3
12	Incident and Disaster Response	4/10
13	No Class	4/17
14	**Team Project Presentations** Course Review	4/24
	Final Exam	5/1

Agenda

- ✓Computer virus
- ✓Malicious software
  - ✓Proliferation of malware
  - ✓Malware components
  - ✓Anti-malware components
  - ✓Best practices for protection
- ✓Business Continuity and Disaster Contingency Planning
- ✓Incident Response Planning
- ✓Final Project Schedule