

# Unit #7a

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
- Team Project Q&A

Virus

Virus: attached to a file

**1986**

**Brain virus**

an F-Secure Production

BRAIN

# 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

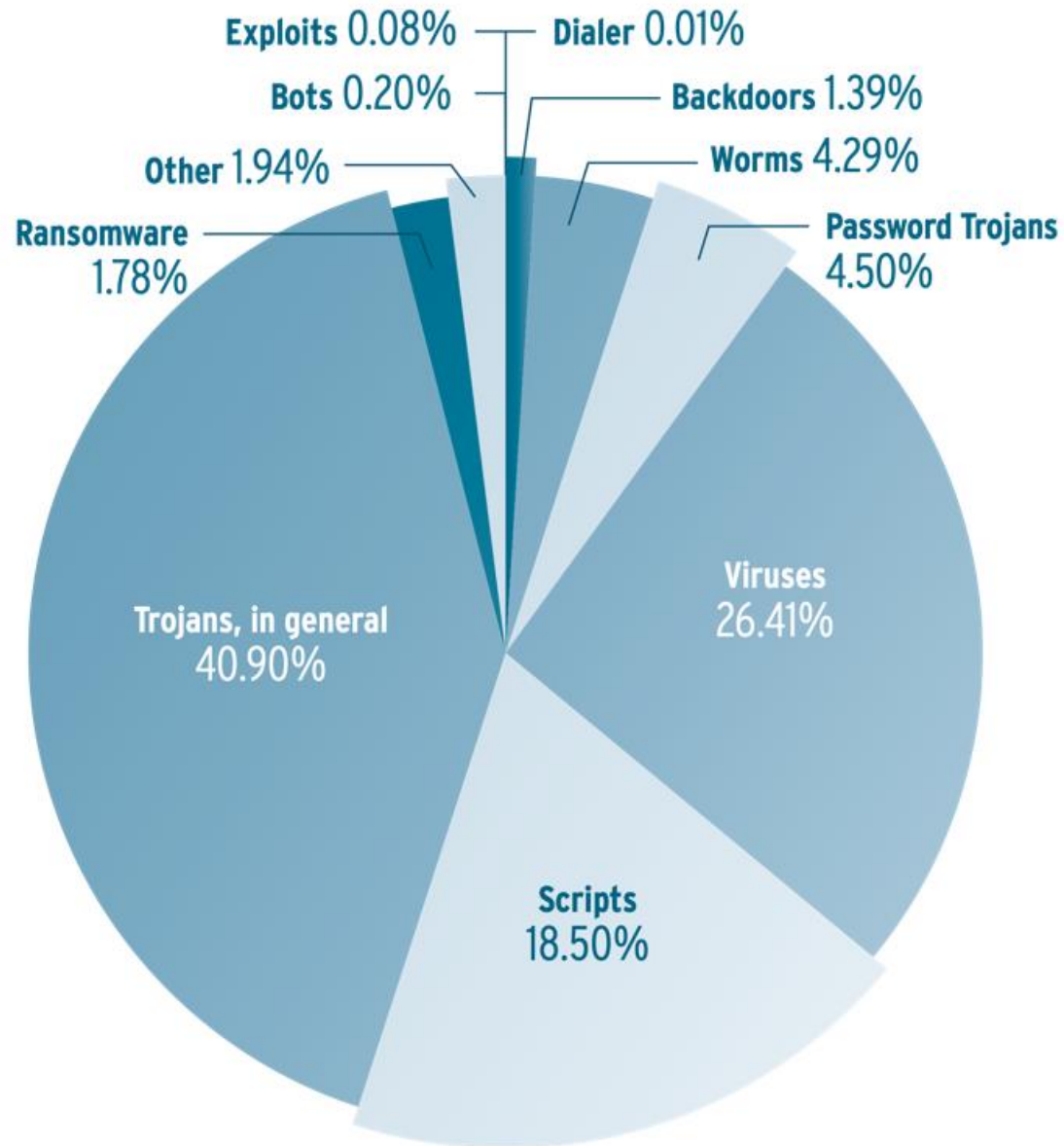


# Types of malware

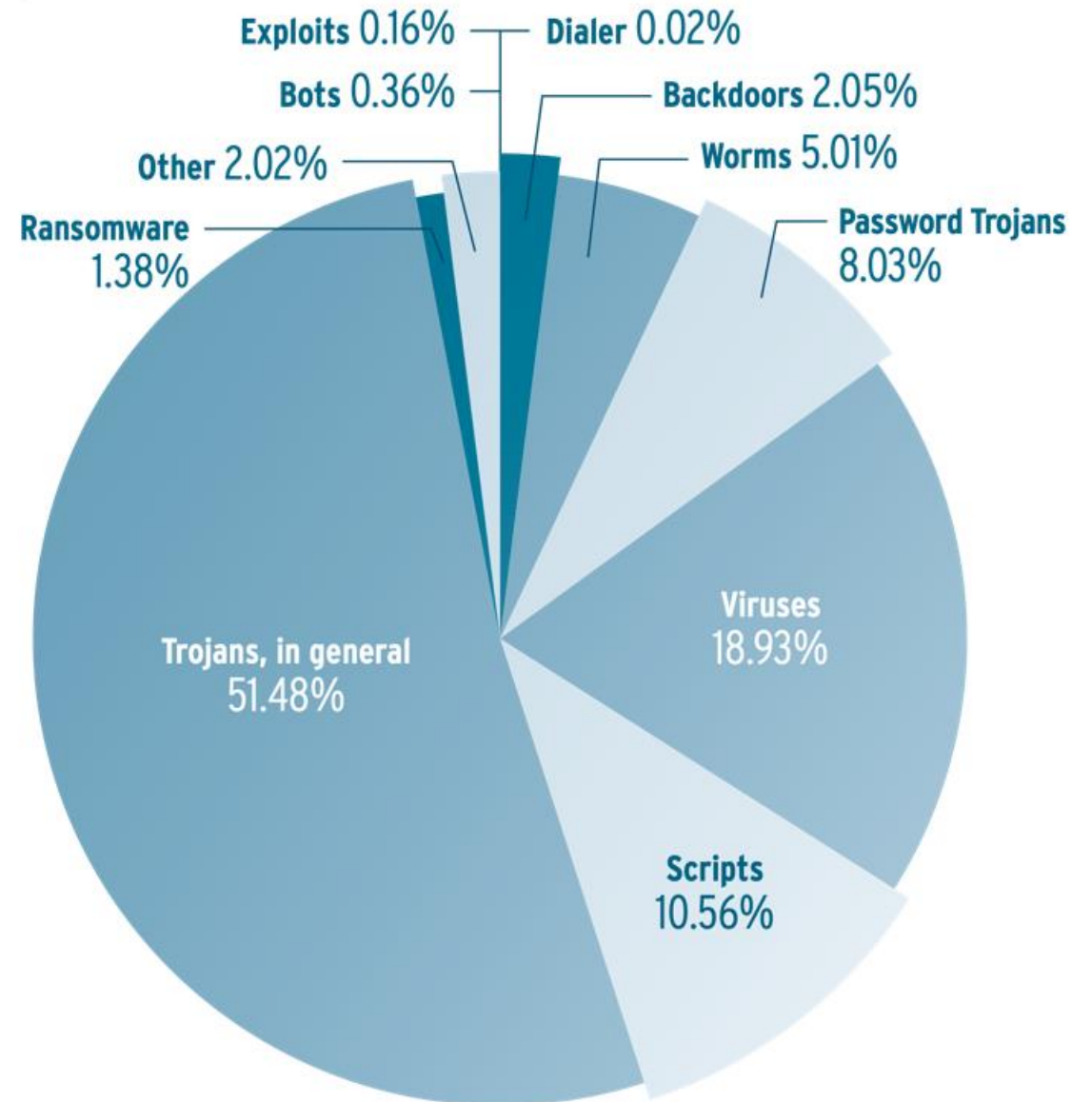
Type	What It Does	Real-World Example
Ransomware	disables victim's access to data until ransom is paid	RYUK
Fileless Malware	makes changes to files that are native to the OS	Astaroth
Spyware	collects user activity data without their knowledge	DarkHotel
Adware	serves unwanted advertisements	Fireball
Trojans	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/>

## Distribution of malware under Windows 2017



## Q1 2018



# 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

```
Oops, 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-pD5A14-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

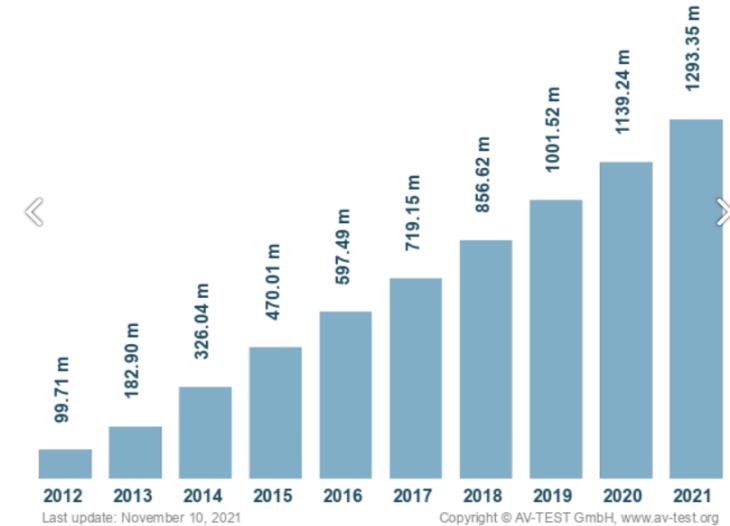
# Malware is increasing

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

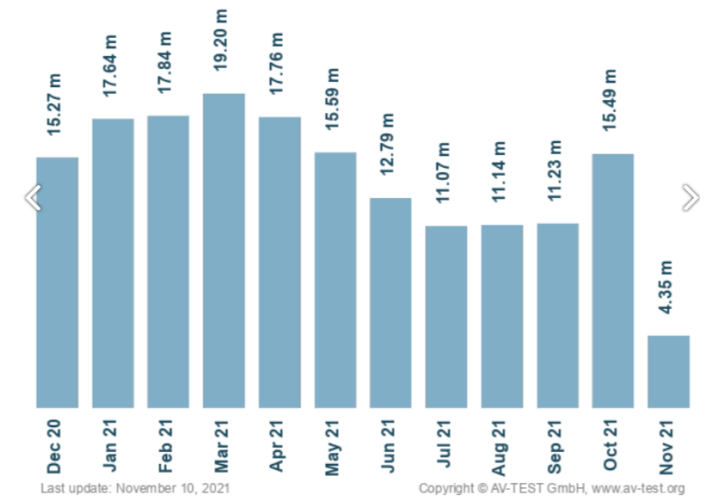
Main reasons types malware is increasing in quantity and potency:

- 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



New 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 - Carries 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 alerts 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 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 keys in the Windows Registry or startup files
- 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**

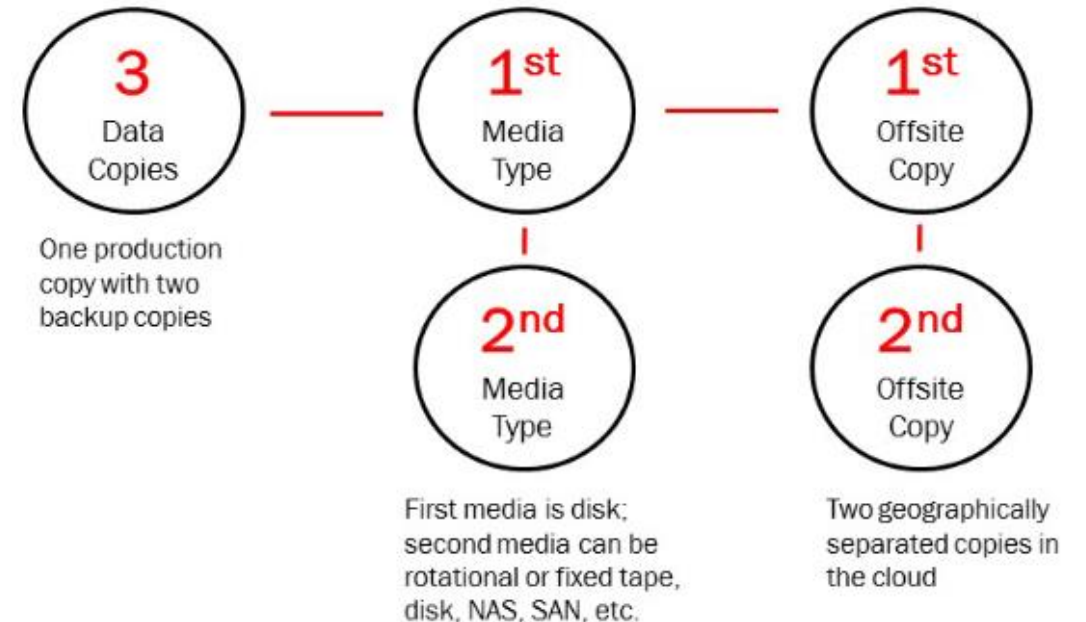
- Have regular (i.e. current and automated) offline backup
- Make sure they are verified to be happening on the expected regular basis and are usable for restore operations
  - Old, outdated backups are less valuable than recent ones
  - Backups that don't restore properly are of no value

# 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

Maersk had 50 copies of their mission critical software and corresponding data – all in the same format, all on the network



# 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

# 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>



# Critical Infrastructure

“Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. ...As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks.”

Presidential Decision Directive/NSC 63, 1998



## Critical Infrastructure Security and Resilience

“Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to **determine effective strategies to make them more secure and resilient**”

Presidential Policy Directive/  
PPD-21, 2013

# America's Water Infrastructure Act of 2018

Defines 'resilience' as

*“The ability of a community water system or an asset of a community water system to adapt to or withstand the effects of a malevolent act or natural hazard without interruption to the asset's or system's function, or if the function is interrupted, to rapidly return to a normal operating condition”*



# To assure resilient response

## Business Continuity Plan (BCP)

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

Source: ISO 22301:2012

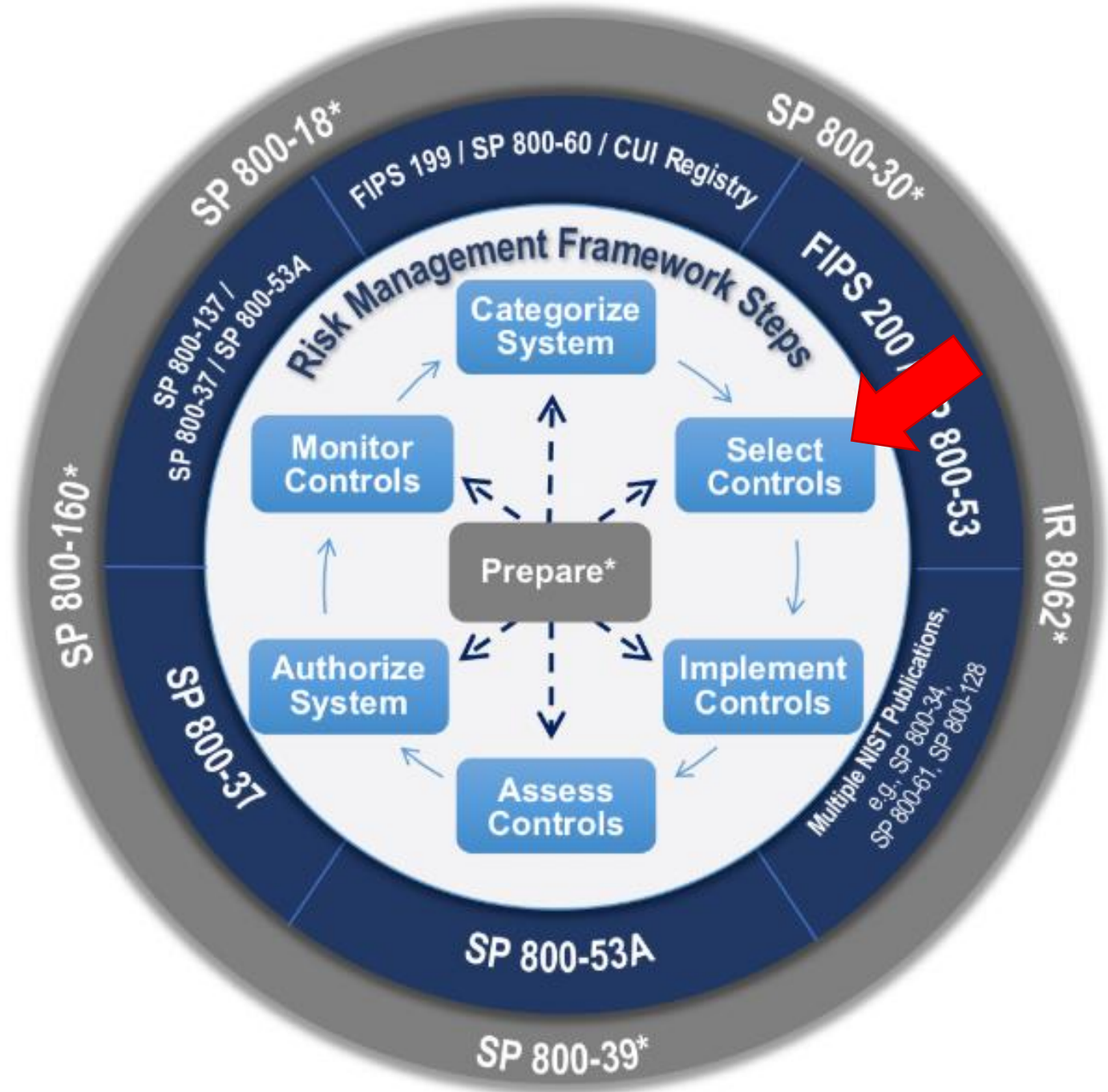
Societal security – Business continuity management systems - Requirements

## ...includes a Disaster Recovery Plan (DRP)

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

# Our Disaster Recovery Plan Goes Something Like This...





# Catalog of cyber-security controls

*for Business Continuity and Resiliency planning focus on  
Contingency Planning controls*

NIST Special Publication 800-53  
Revision 4

## Security and Privacy Controls for Federal Information Systems and Organizations

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

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

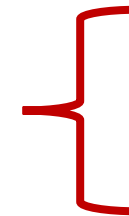


U.S. Department of Commerce  
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology  
Director

# Contingency Planning Controls

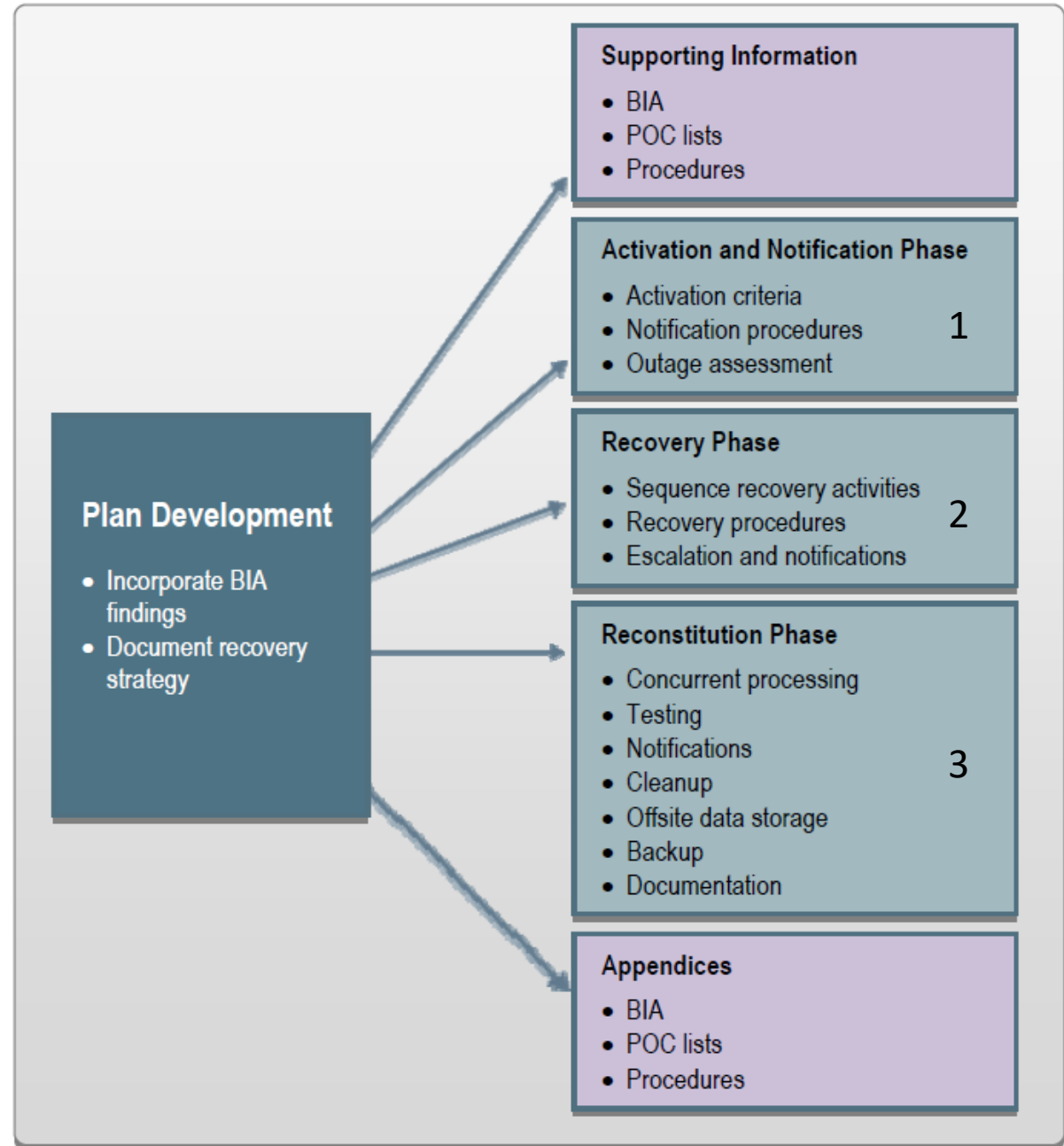
CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information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



CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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.			

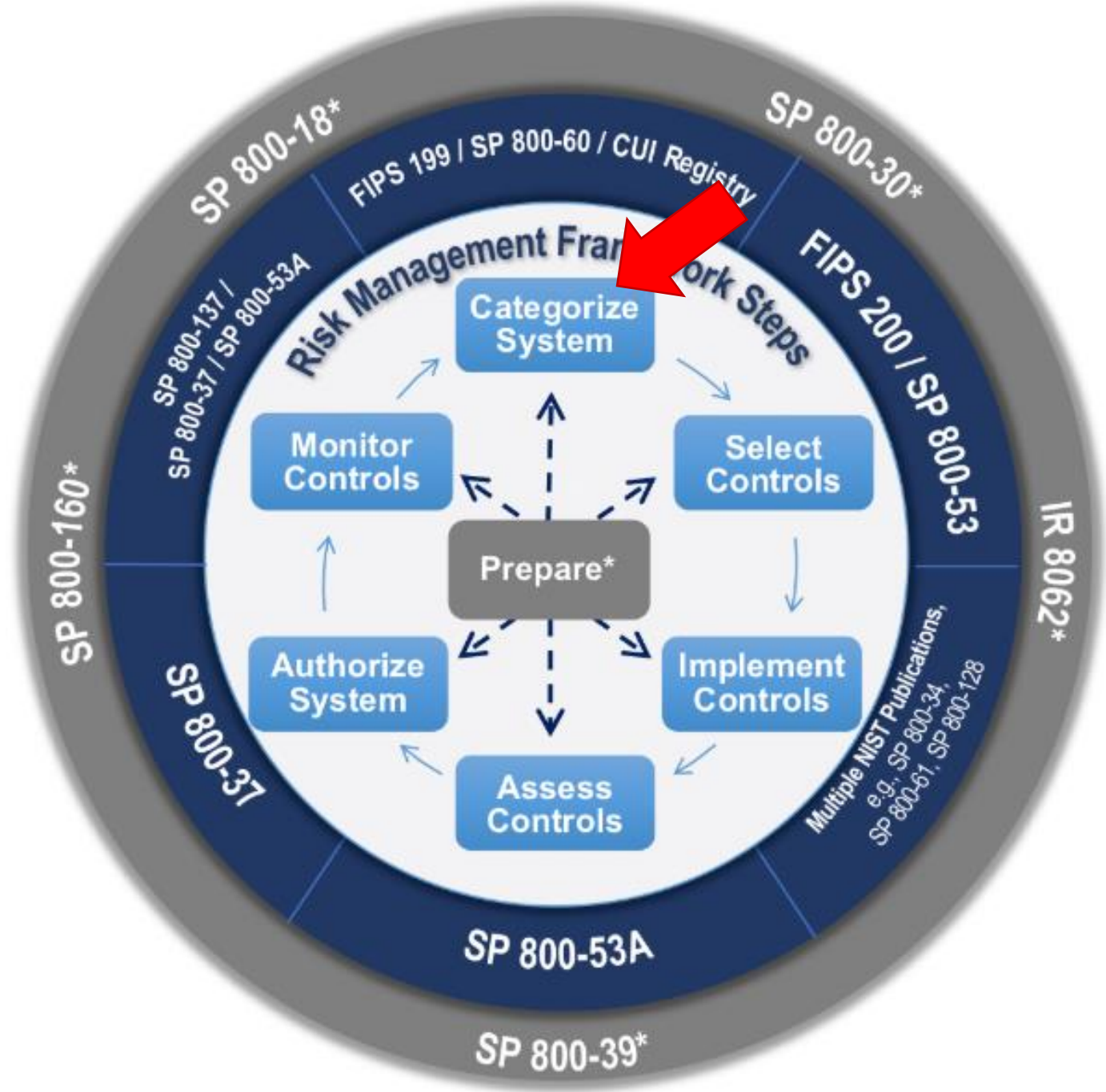
# 3-Phases in a Contingency Plan

All dependent on a BIA “Business Impact Analysis”





*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	
<p><b>Confidentiality</b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and information.</p> <p>[44 U.S.C.]</p>	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.	
		POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH	
<p><b>Availability</b> Ensuring timely and reliable access to and use of information.</p> <p>[44 U.S.C., SEC. 3542]</p>	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> 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 <b>serious</b> 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 <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.	

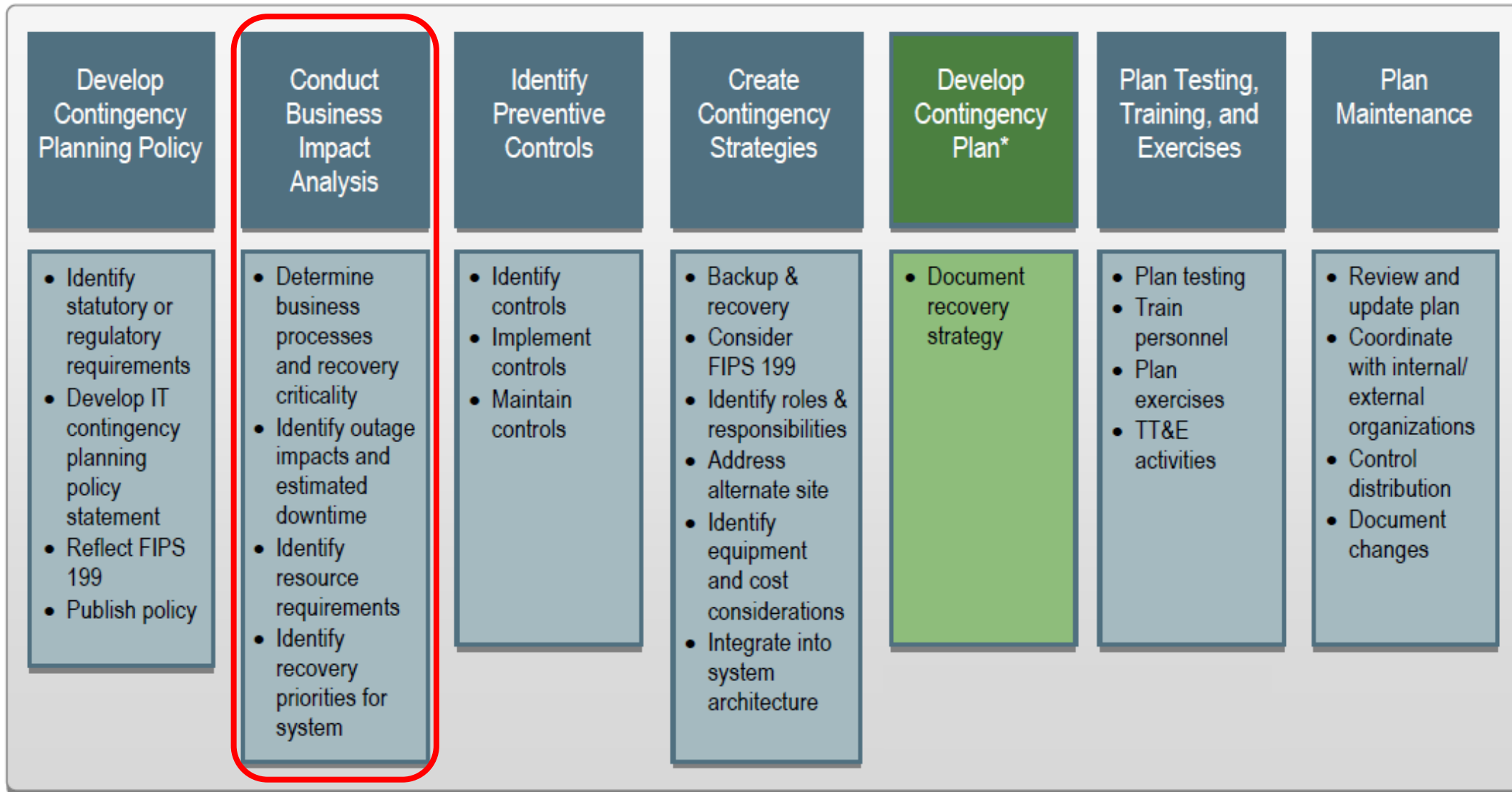
FIPS PUB 199

---

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

**Standards for Security Categorization of Federal Information and Information Systems**

# Plan is based on “recovery priorities”

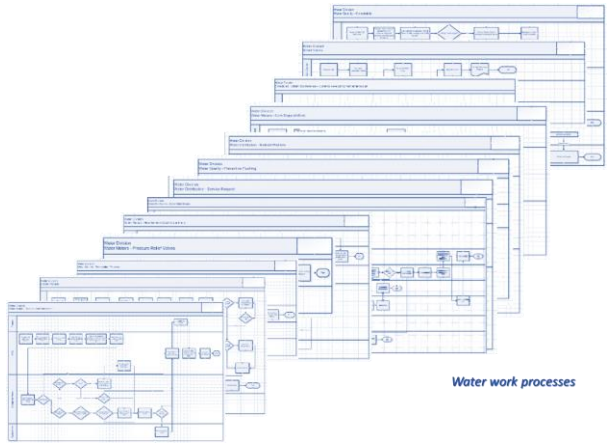


# Business Impact Analysis (BIA) Answers

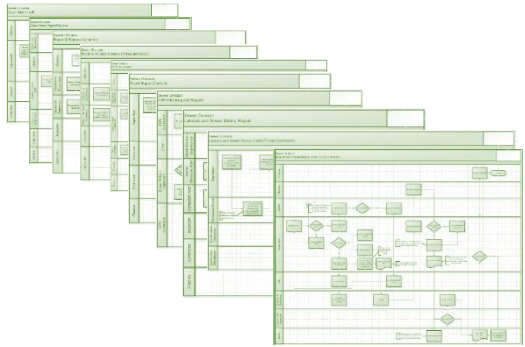
1. What are the work processes ?
2. How critical is each ?
3. What data, applications, and people are needed to run each critical process ?
4. What are the priorities for recovering information systems after disruption ?
5. For each critical IT resource, what are:
  - **Recover time objective (RTO):**  
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...

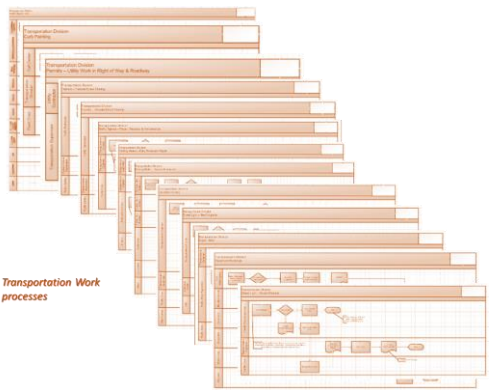
*Good work process documentation identifies all people, data, applications, communications and information technologies needed to restore operations*



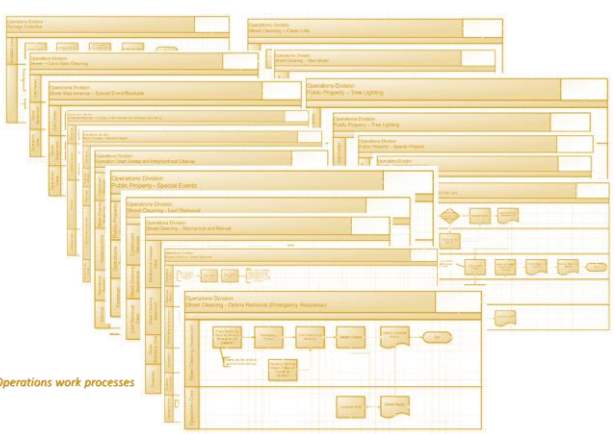
Water work processes



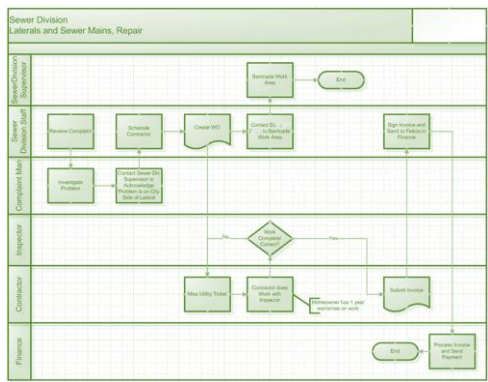
Operations work processes



Transportation Work processes

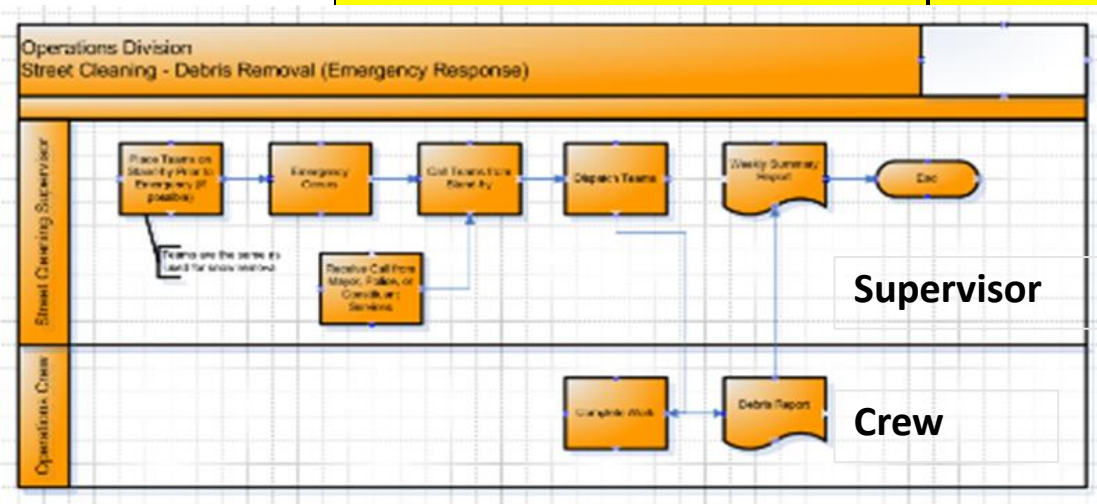
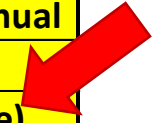


		Transportation Division	Sewer Division	Water Division	Water Quality	Operations Division	Other
Transportation Division	Signs, New/Repair/Replace						
	Street Light Repair/Replace						
	Street Light New						
	Traffic Signal Repair/Replace/Maintenance						
	Traffic Signal New						
	Painting Meter Base						
	Parking Meter Daily Route and Repair						
	Emergency Maintenance						
	Carb Painting						
	Utility Work						
Operations Division	Mow Grass						
	Chow Litter						
	Street Cleaning - Mechanical and Manual						
	Debris Removal						
	Debris Removal (Emergency Response)						
	Special Pick Up						
	Litter Removal						
	Operation Clean Sweep and Neighborhood Cleanup						
	Special Events						
	Special Projects						
Water Division	Meter Services and Complaints						
	Meter Terminations						
	Meter, New Service						
	Interconnections						
	Pressure Balok Valves						
	New Service						
	Water Break						
	Event Annual Hydrant Flushing						
	Water Services Repair/Replace						
	Hydrant Repair						
Sewer Division	Laterals and Sewer Mains, Install (City)						
	Laterals and Sewer Mains, Install (Contractor)						
	Laterals and Sewer Mains, Repair						
	Maintenance, Repair & Replace						
	Catch Basins, New						
	Catch Basins, Repair & Replace						
	Landscape Repair & Replace						
	CCTV & Cleaning						
	Street Repair (Crews on)						
	Meter Utility Shuts, Out						



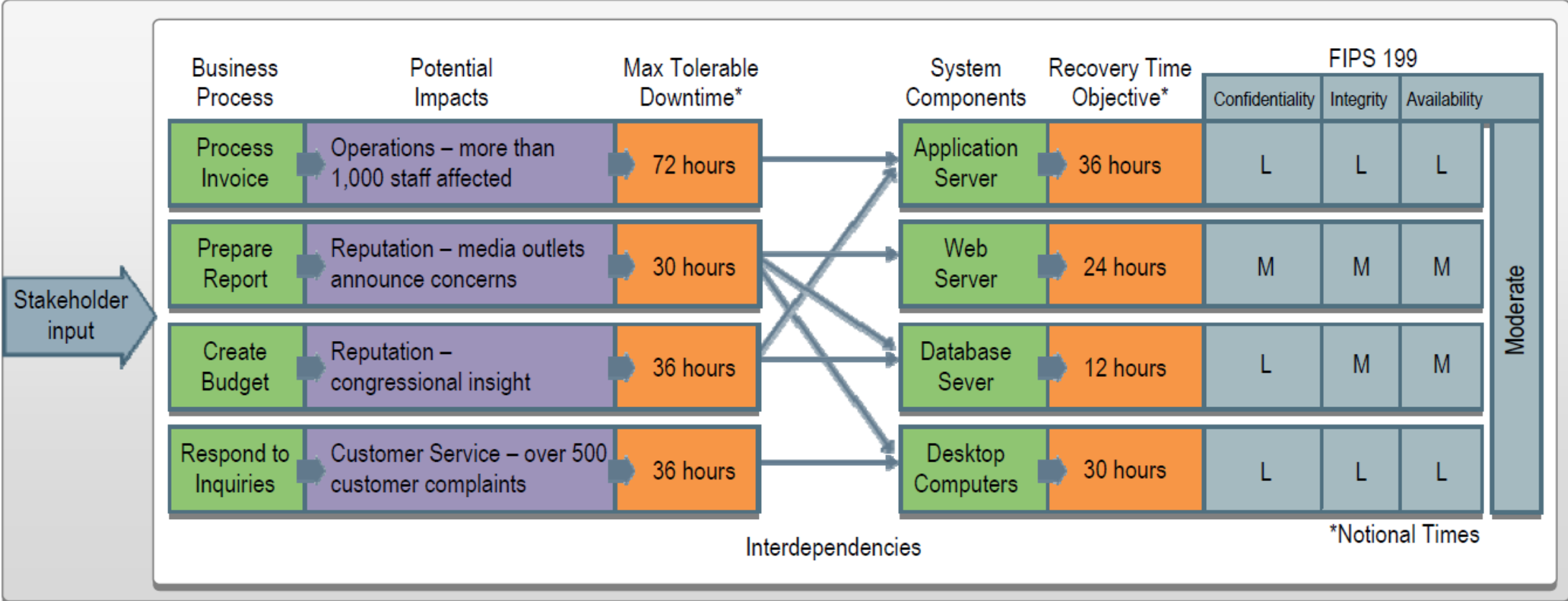
# Priorities for recovery example

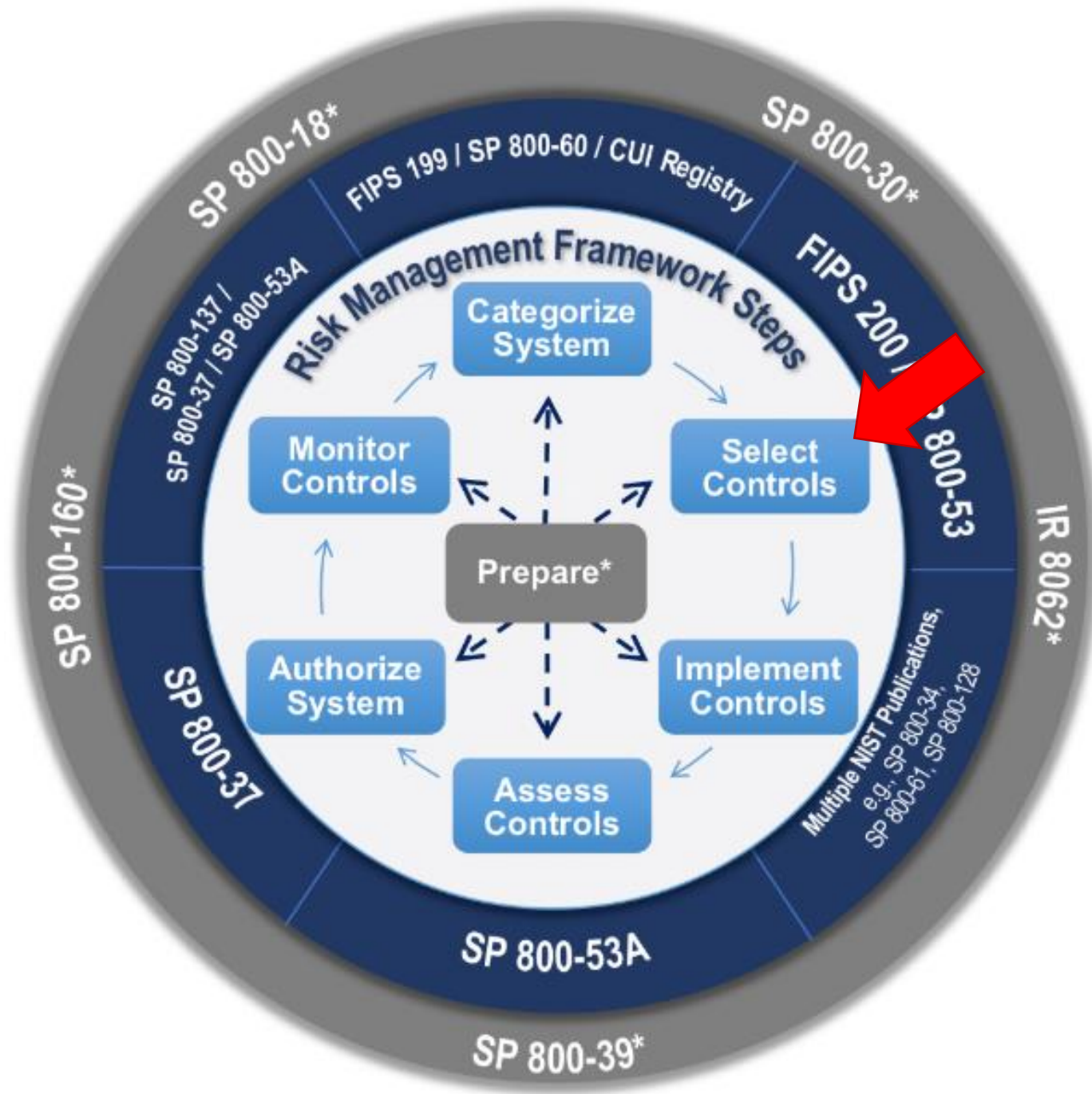
<b>Public Works Dept Operations Division</b>	<b>Street Cleaning</b>	Mow Grass
		Clean Lots
		Street Cleaning - Mechanical and Manual
		Snow Removal
		Debris Removal (Emergency Response)
		Special Pick Ups
		Leaf Removal
		Neighborhood Cleanup
	<b>Public Property</b>	Special Events
		Special Projects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



# Business Impact Analysis (BIA) example...

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







# Catalog of cyber-security controls

*for Business Continuity and Resiliency planning focus on  
Contingency Planning controls*

NIST Special Publication 800-53  
Revision 4

## Security and Privacy Controls for Federal Information Systems and Organizations

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

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

National Institute of Standards and Technology  
Director

# Contingency Planning Controls

CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
	Contingency Planning Policy and Procedures	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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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	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	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

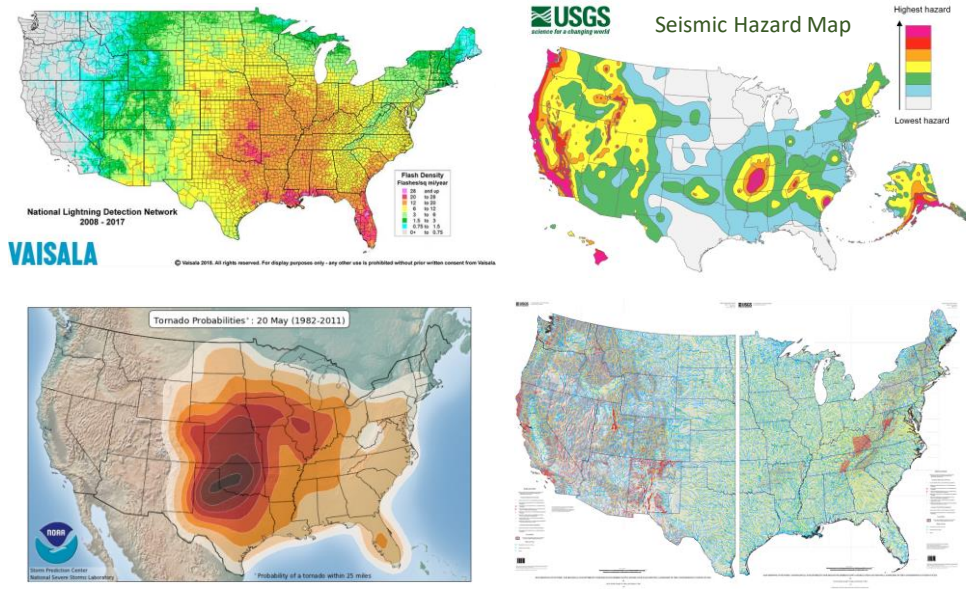
**Cold site:** Provides only the basic environment that can be outfitted with communication, utilities and computers

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

# Location of Alternate site

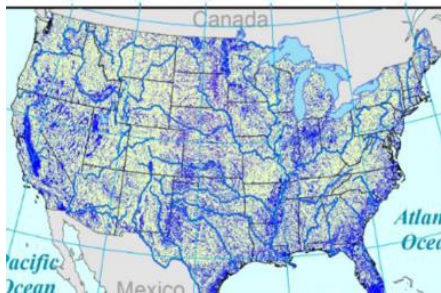
Disaster recovery site should be in a different geophysical area not susceptible to same disaster as the primary operations facility

*Note: even the cloud is located somewhere...*



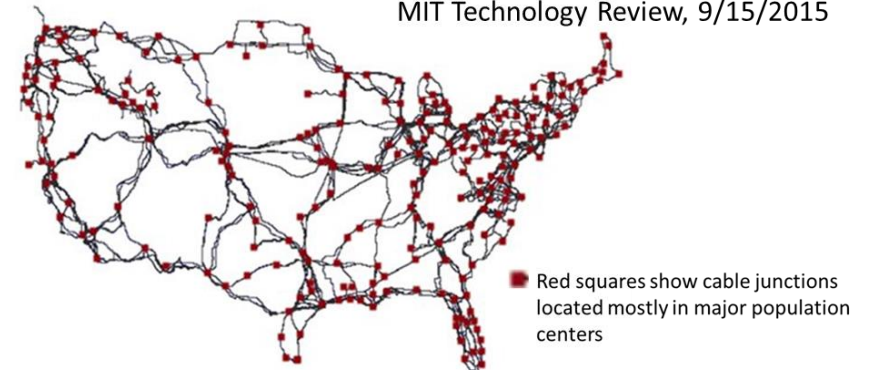
VAISALA

GFI flood-prone areas



With multiple providers of:

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



- 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**

<b>Atmospheric</b>	<b>Volcanic</b>	<b>Hydrologic</b>	<b>Other Geologic</b>	<b>Seismic</b>	<b>Wildfire</b>
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

### A. BENEFITS OF MULTIPLE HAZARD MAPPING

### B. PREPARING MULTIPLE HAZARD MAPS

1. Translated Information
2. Sources and Compiling Information
3. Timing

### C. MAP FORMAT

1. Base Map
2. Scale and Coverage
3. Hazards to be Shown
4. Types of Symbols

### D. OTHER FORMS OF MULTIPLE HAZARDS INFORMATION

1. Cross section of Effects
2. Photographs of Damage
3. Atlas of Hazards
4. Plan for Reducing Hazards
5. Analyses of Land Capability
6. Single Event with Multiple Hazards
7. Series of Strip Maps
8. Photo Maps
9. Geographic Information Systems
10. Information Processed by Computer

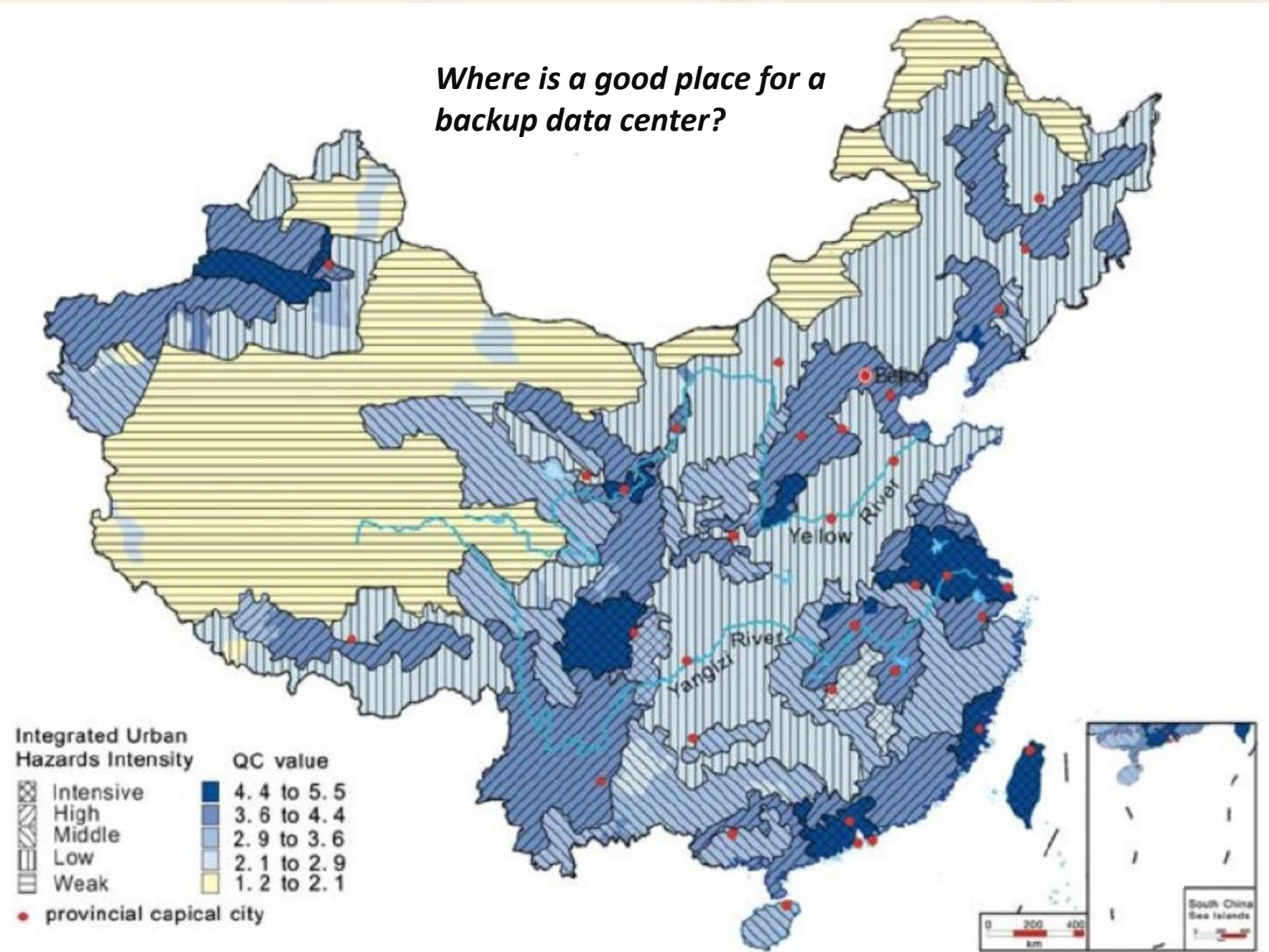
### E. LIMITATIONS

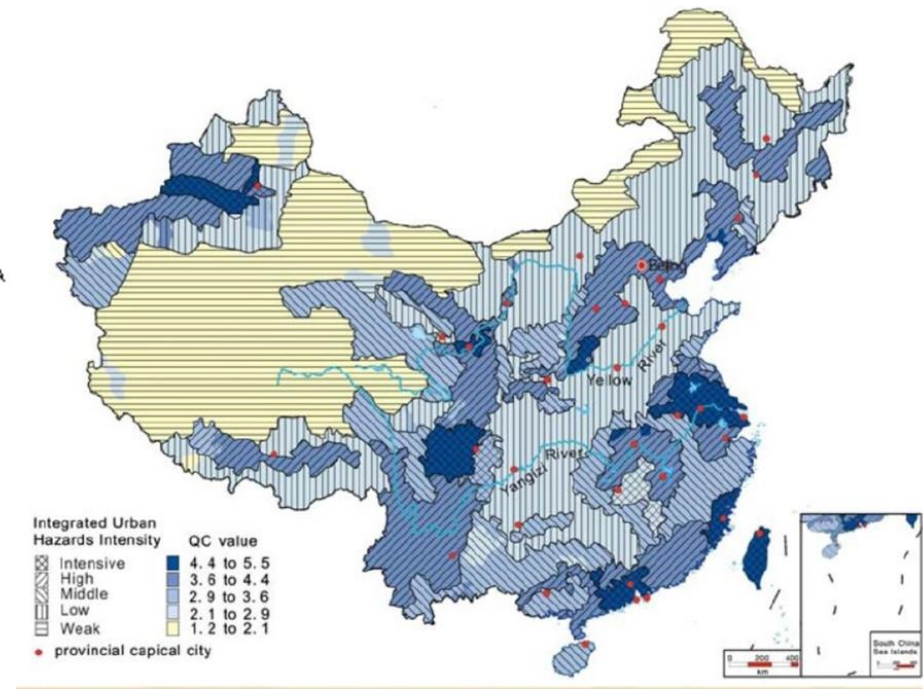
1. Credibility
2. Likelihood, Location, and Severity
3. Accuracy versus Precision
4. Scale
5. Abuse
6. Synthesis versus Detail
7. Use of Caveats

### CONCLUSION REFERENCES

# Map of Comprehensive Urban Natural Disaster Intensity in China

*Where is a good place for a backup data center?*





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
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

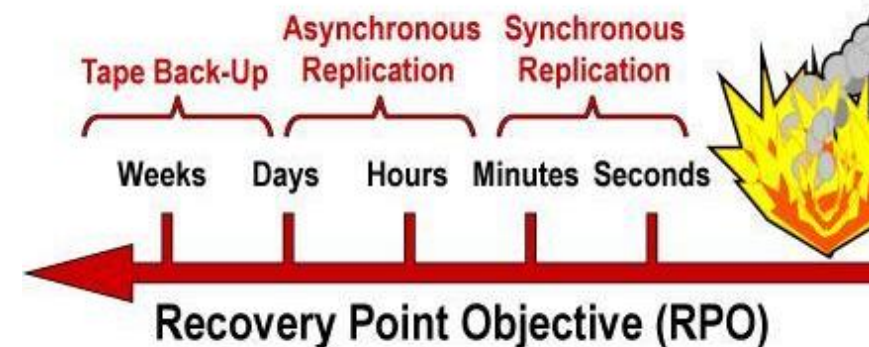
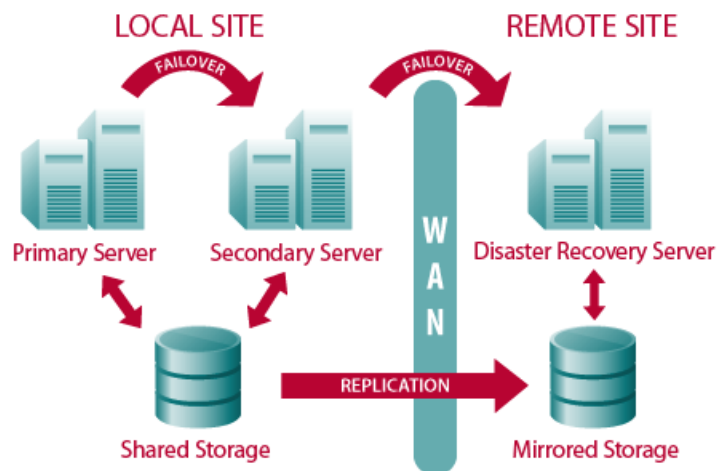
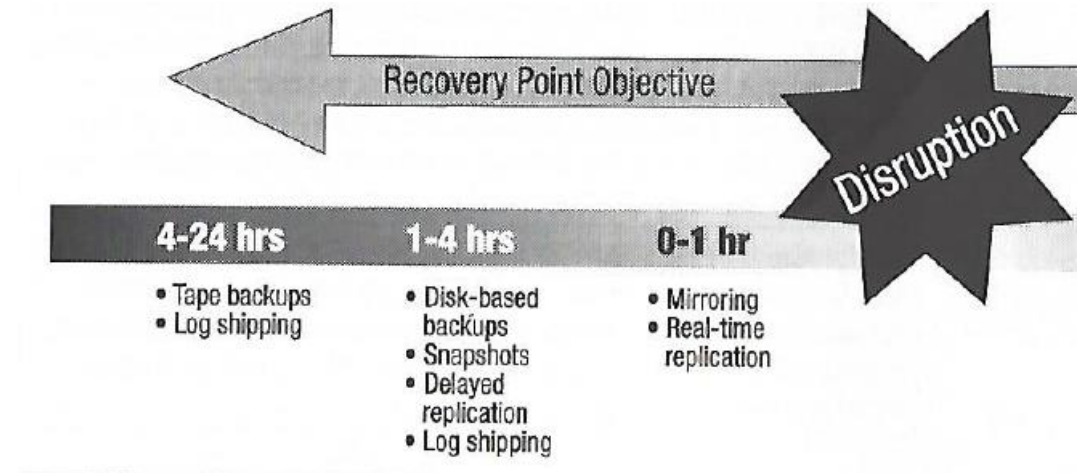
CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	Contingency Planning Policy and Procedures		X	X	X	X
CP-2	Contingency Plan			X	X	X
CP-2(1)	CONTINGENCY PLAN   COORDINATE WITH RELATED PLANS				X	X
CP-2(2)	CONTINGENCY PLAN   CAPACITY PLANNING					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	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	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.			

NIST SP 800-53r4 “[Security and Privacy Controls for Federal Information Systems and Organizations](#)”



# Data backup systems and redundancies

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

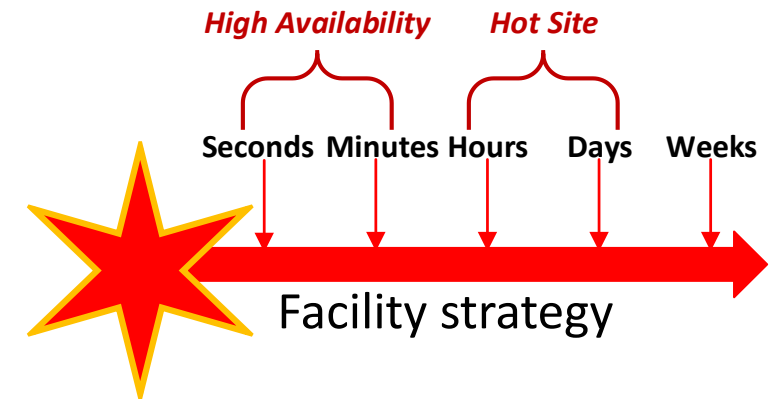


# Recovery Options: Location & Backup

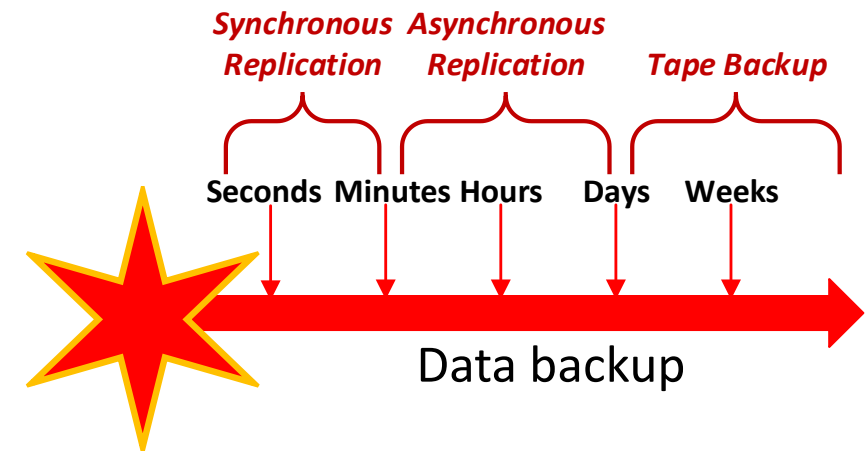
Information System Recovery Priority	Backup / Recovery Strategy
High priority	Backup: Mirrored systems and disc replication Strategy: Hot site <span style="float: right;">\$\$\$</span>
Moderate priority	Backup: Optical backup and WAN/VLAN replication Strategy: Warm or Cold site <span style="float: right;">\$\$</span>
Low priority	Backup: Tape backup Strategy: Cold site <span style="float: right;">\$</span>

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

## Recovery Time Objective



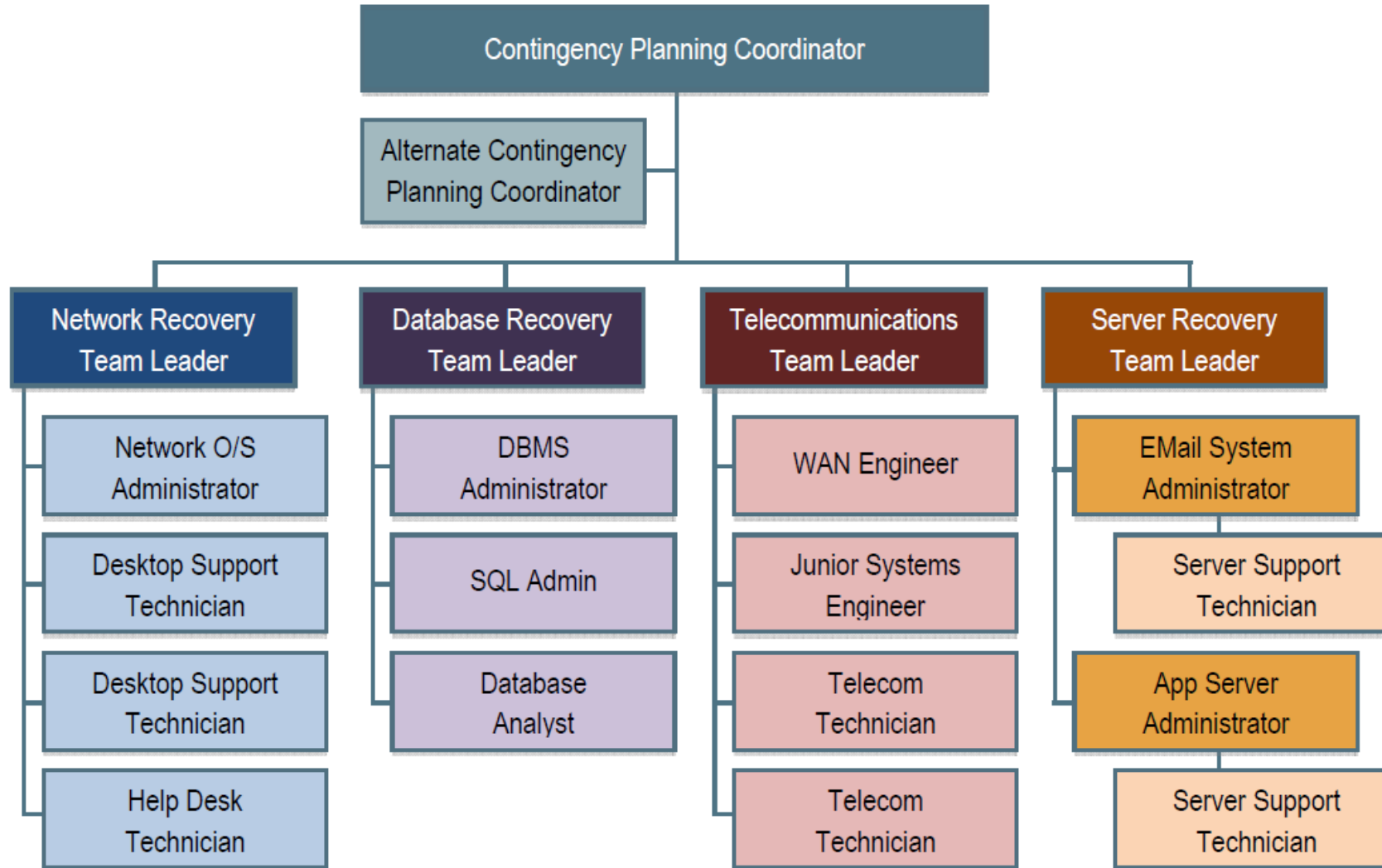
## Recovery Point Objective



# Considerations - Budget

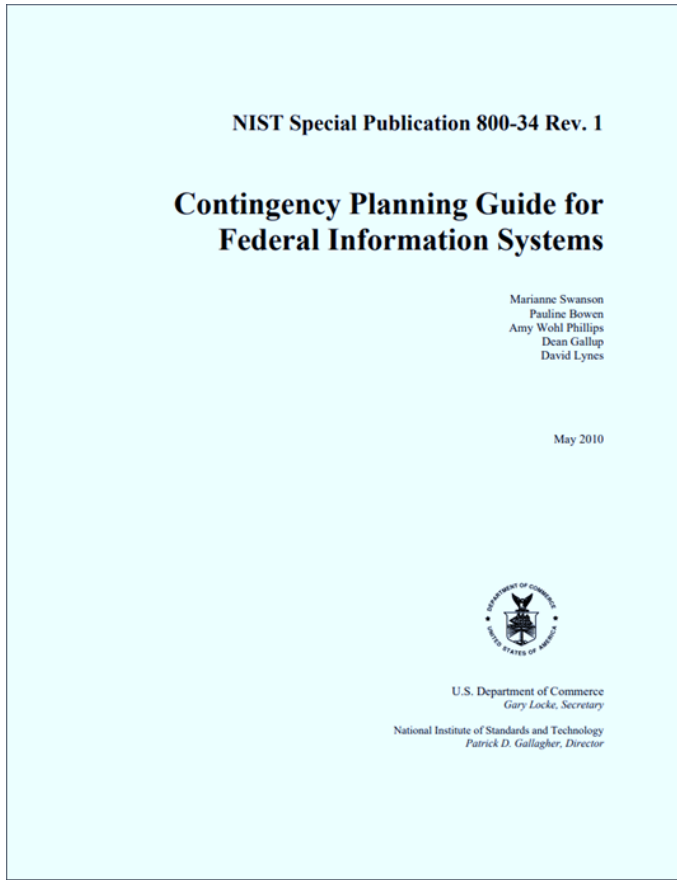
Contingency Resources	Strategies	Vendor Costs	Hardware Costs	Software Costs	Travel / Shipping Costs	Labor / Contractor Costs	Testing Costs	Supply Costs
Alternate Site	Cold Site							
	Warm Site							
	Hot Site							
Offsite Storage	Commercial							
	Internal							
Equipment Replacement	SLA					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

# Response Roles and Responsibilities example



# Contingency Plan

Plan Approval.....	A.3-3
1. Introduction .....	A.3-4
1.1 Background.....	A.3-4
1.2 Scope.....	A.3-4
1.3 Assumptions.....	A.3-4
2. Concept of Operations .....	A.3-5
2.1 System Description.....	A.3-5
2.2 Overview of Three Phases.....	A.3-5
2.3 Roles and Responsibilities.....	A.3-6
3. Activation and Notification.....	A.3-6
3.1 Activation Criteria and Procedure .....	A.3-6
3.2 Notification.....	A.3-6
3.3 Outage Assessment.....	A.3-7
4. Recovery.....	A.3-7
4.1 Sequence of Recovery Activities .....	A.3-7
4.2 Recovery Procedures .....	A.3-8
4.3 Recovery Escalation Notices/Awareness.....	A.3-8
5. Reconstitution.....	A.3-8
5.1 Concurrent Processing .....	A.3-8
5.2 Validation Data Testing.....	A.3-8
5.3 Validation Functionality Testing.....	A.3-9
5.4 Recovery Declaration.....	A.3-9
5.5 Notification (users).....	A.3-9
5.6 Cleanup .....	A.3-9
5.7 Offsite Data Storage.....	A.3-9
5.8 Data Backup.....	A.3-9
5.9 Event Documentation.....	A.3-10
5.10 Deactivation.....	A.3-10



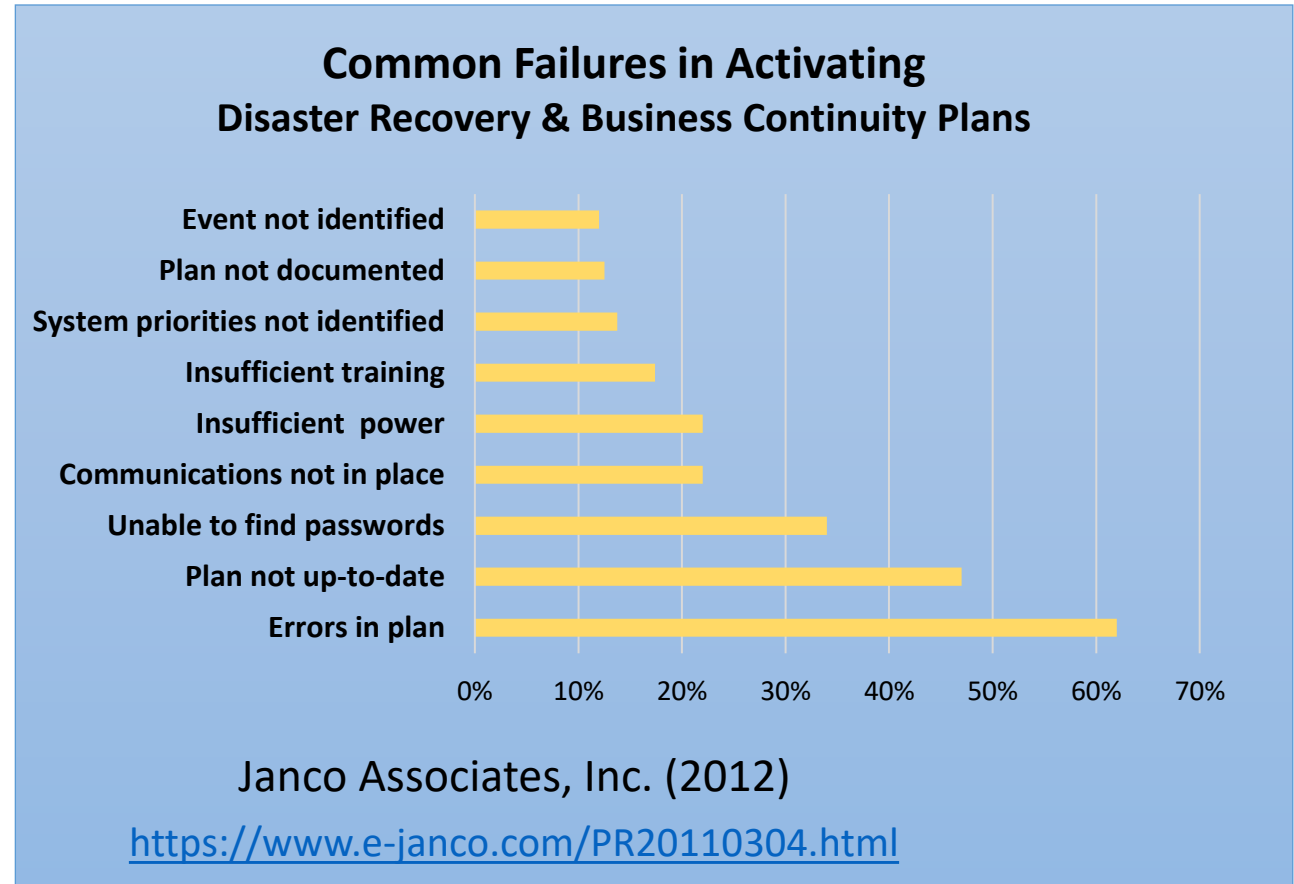
<b>Appendix A— Sample Information System Contingency Plan Templates .....</b>	<b>A.1-1</b>
A.1 Sample Template for Low-Impact Systems.....	A.1-1
A.2 Sample Template for Moderate-Impact Systems .....	A.2-1
A.3 Sample Template for High-Impact Systems.....	A.3-1

# 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:*

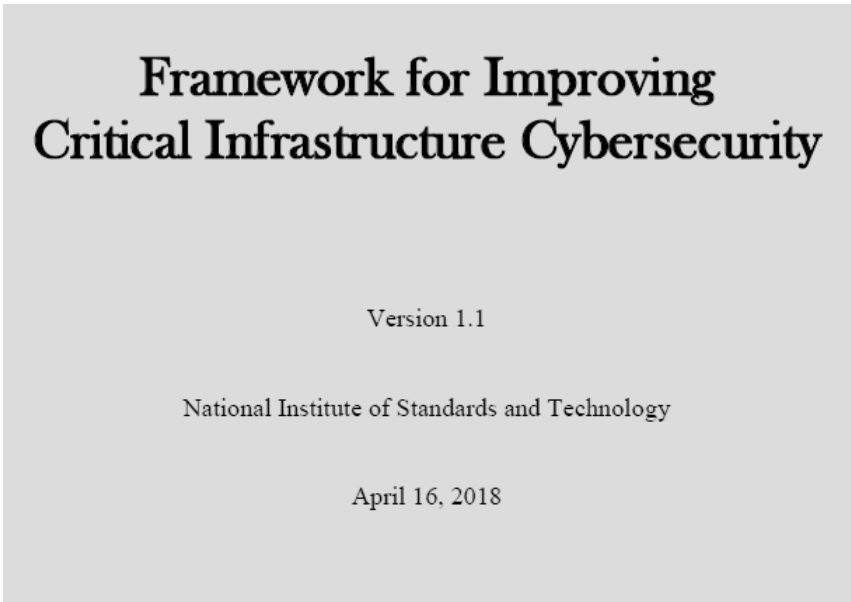
- *Checklist review*
- *Tabletop exercise*
- *Structured walk-through*
- *Dry-Run tests*



# 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

# 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?

Functions	Categories
IDENTIFY	
PROTECT	
DETECT	
RESPOND	
RECOVER	
	56



# 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.

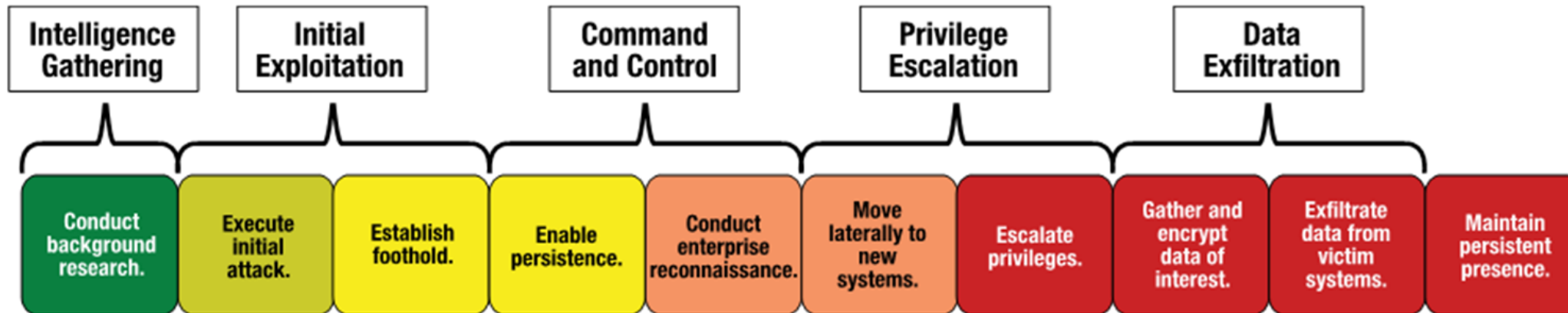
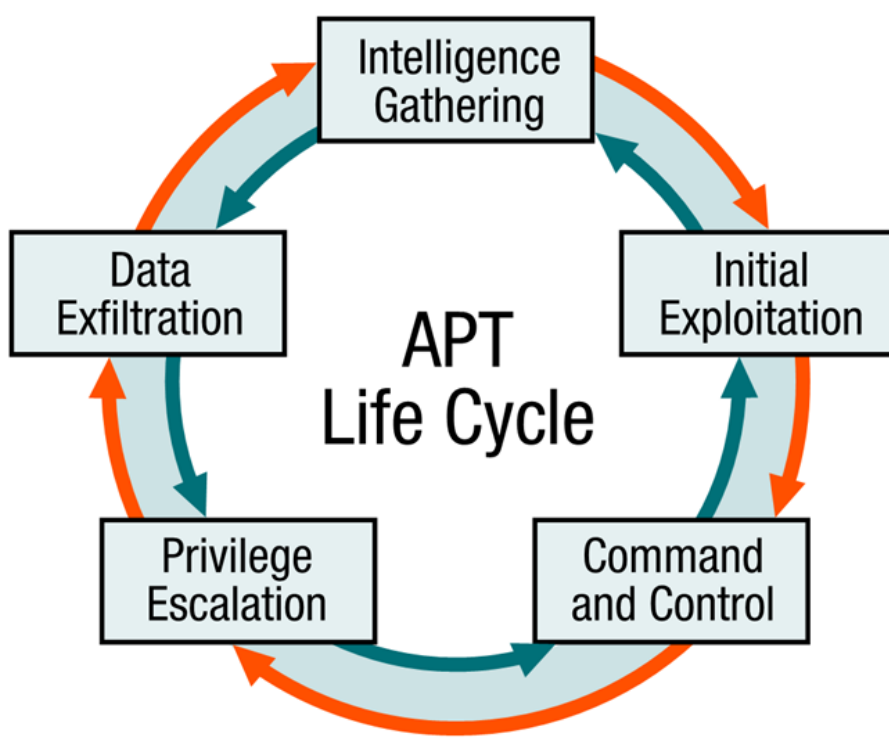
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization 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

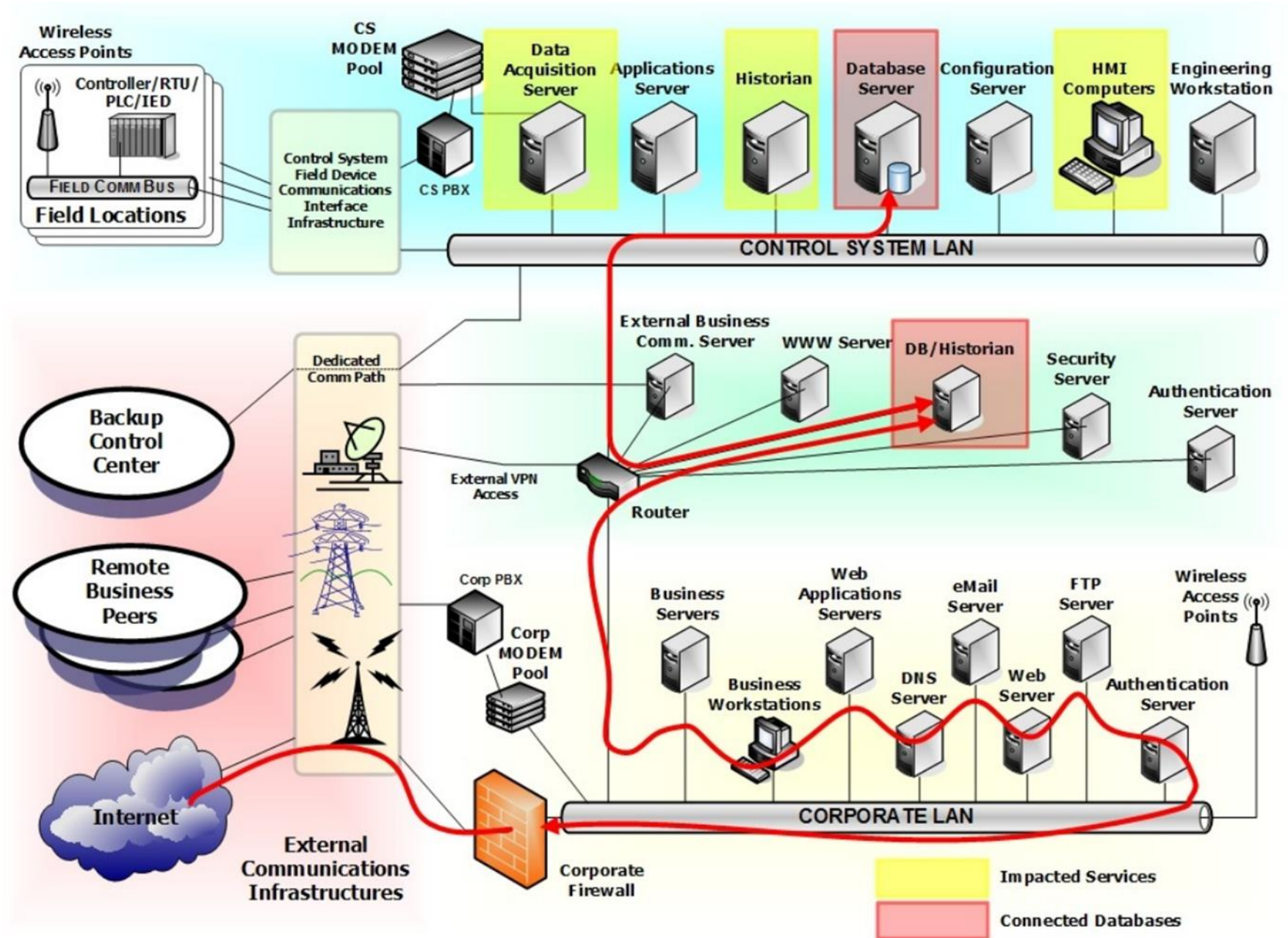
Is necessary because...

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

# Anatomy of Advanced Persistent Threats



# Example of Network Intrusion



# Industry Targeting

*“The top five most targeted industries in 2020 were:*

- business and professional services,*
- retail and hospitality,*
- financial,*
- healthcare, and*
- high technology.*

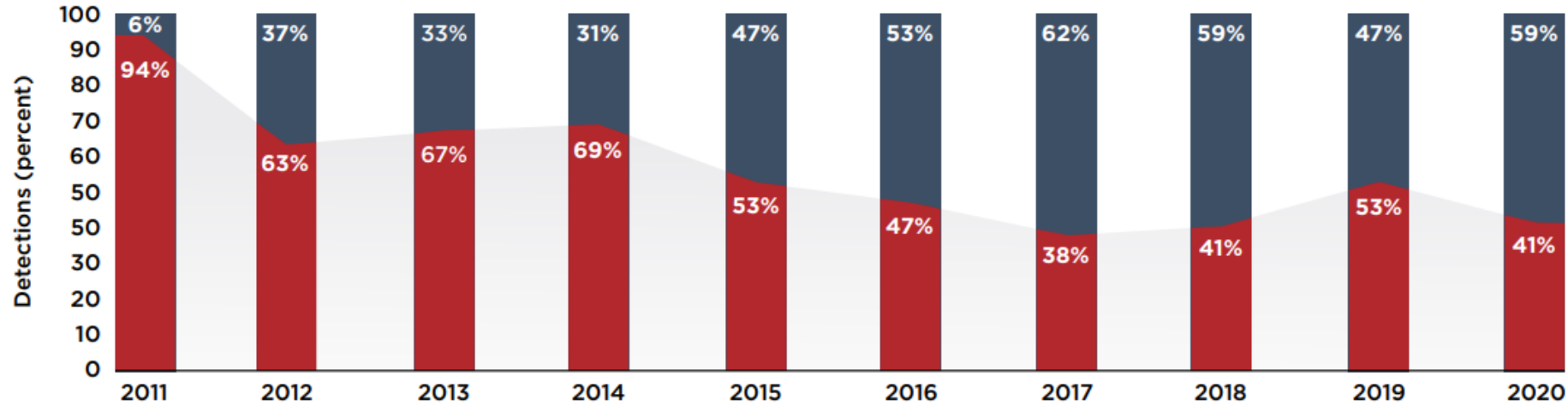
*Over the past decade, business and professional services and financial have consistently placed in the top five most targeted industries.”*

Page 17



<b>Ransomware</b>	<b>36</b>	<b>UNC2452</b>	<b>62</b>
Ransomware Evolves Into Multifaceted Extortion	37	Mapping UNC2452 Activity to the Targeted Attack Lifecycle Framework	63
Steps toward Proactive Hardening Against Ransomware in Multiple Environments	41	<b>Case Studies</b>	<b>72</b>
Recovery and Reconstitution Challenges in Post-Ransomware Scenarios	45	Insider Threat Risks to Flat Environments	73
<b>Newly Named Threat Groups</b>	<b>49</b>	Red Team Makes the Most of Social Engineering and System Misconfigurations	76
FIN11	50	<b>Conclusion</b>	<b>80</b>
<b>Pandemic-Related Threats</b>	<b>56</b>	More Security Awareness to Build Best Practices	81
Threats Against Organizations Working with COVID-19 Information and Research	57		

# Who is detecting intrusions by attackers?



Page 10

FIREEYE | MANDIANT





# How long are attackers remaining in compromised systems?

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24
External Notification	—	—	—	—	320	107	186	184	141	73
Internal Detection	—	—	—	—	56	80	57.5	50.5	30	12

## Median Dwell Time

**416** > **24**  
DAYS IN 2011      DAYS IN 2020

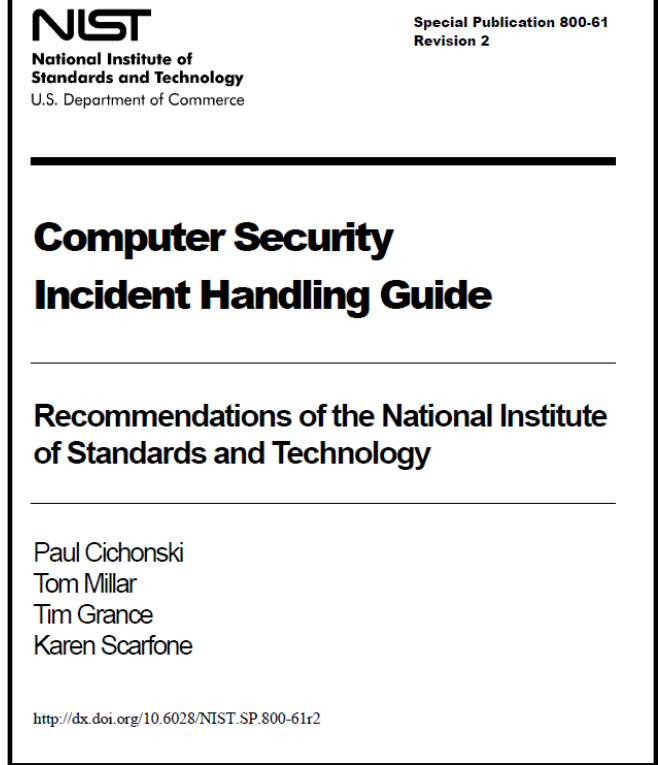
“**Dwell time** is calculated as the number of days an attacker is present in a victim environment before they are detected.”



# 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
  - **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
  - 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



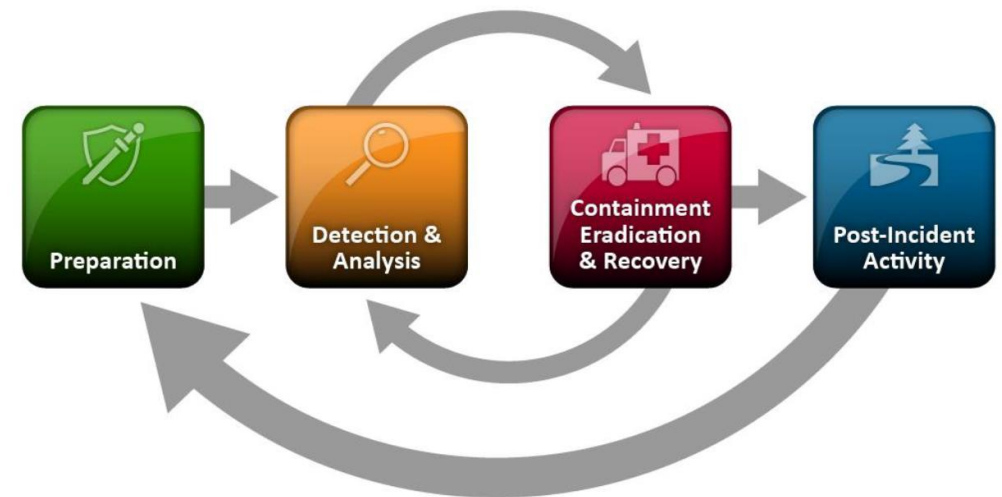
# Handling an Incident - Preparation

**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



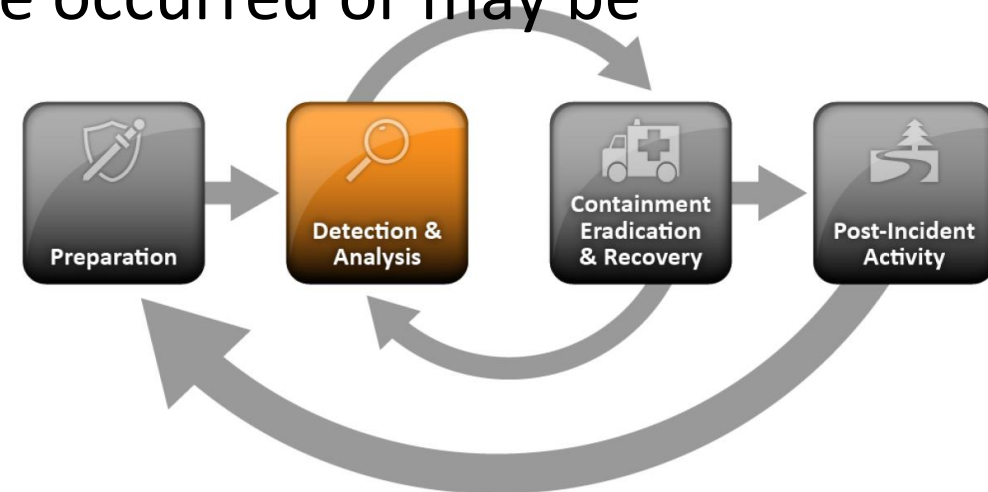
# Handling an Incident – Detection and Analysis

## 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

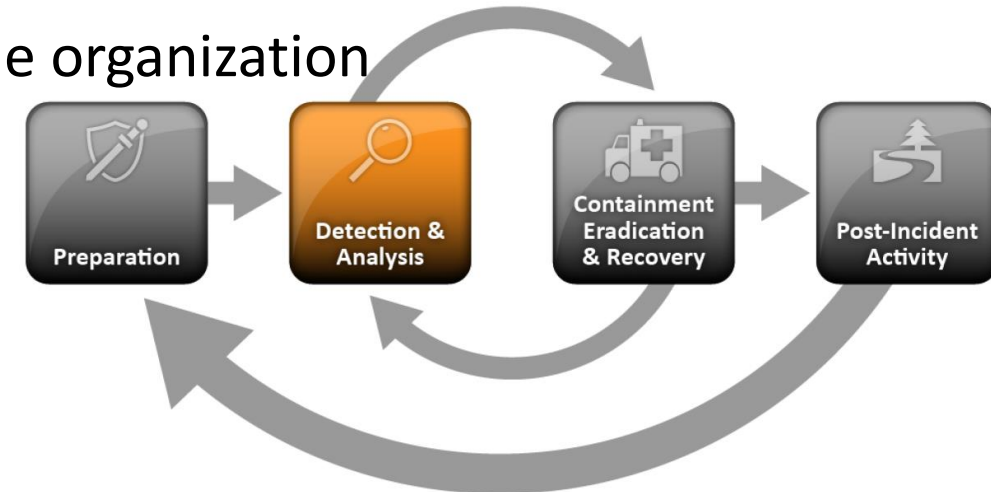


# Handling an Incident – Detection and Analysis

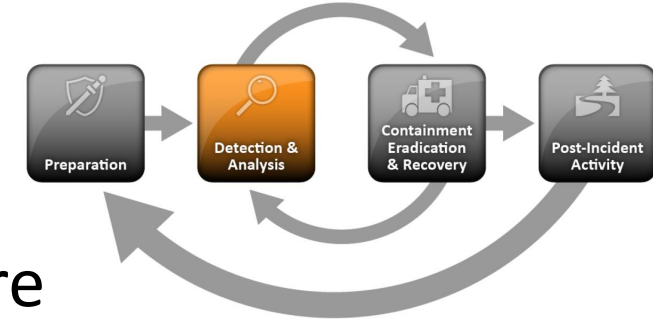
**Precursors** – While rare, if precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.

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

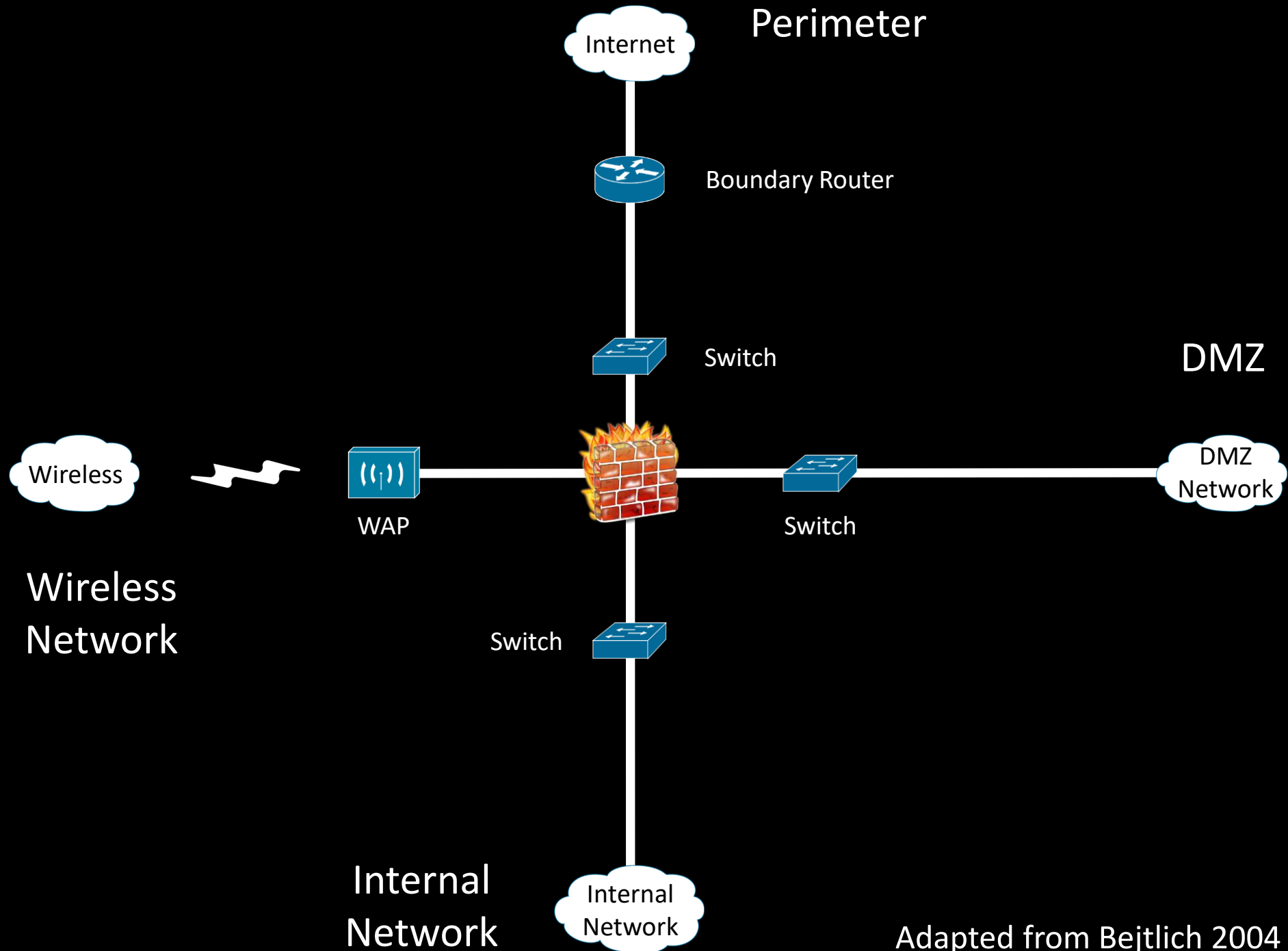


# Detection and Analysis

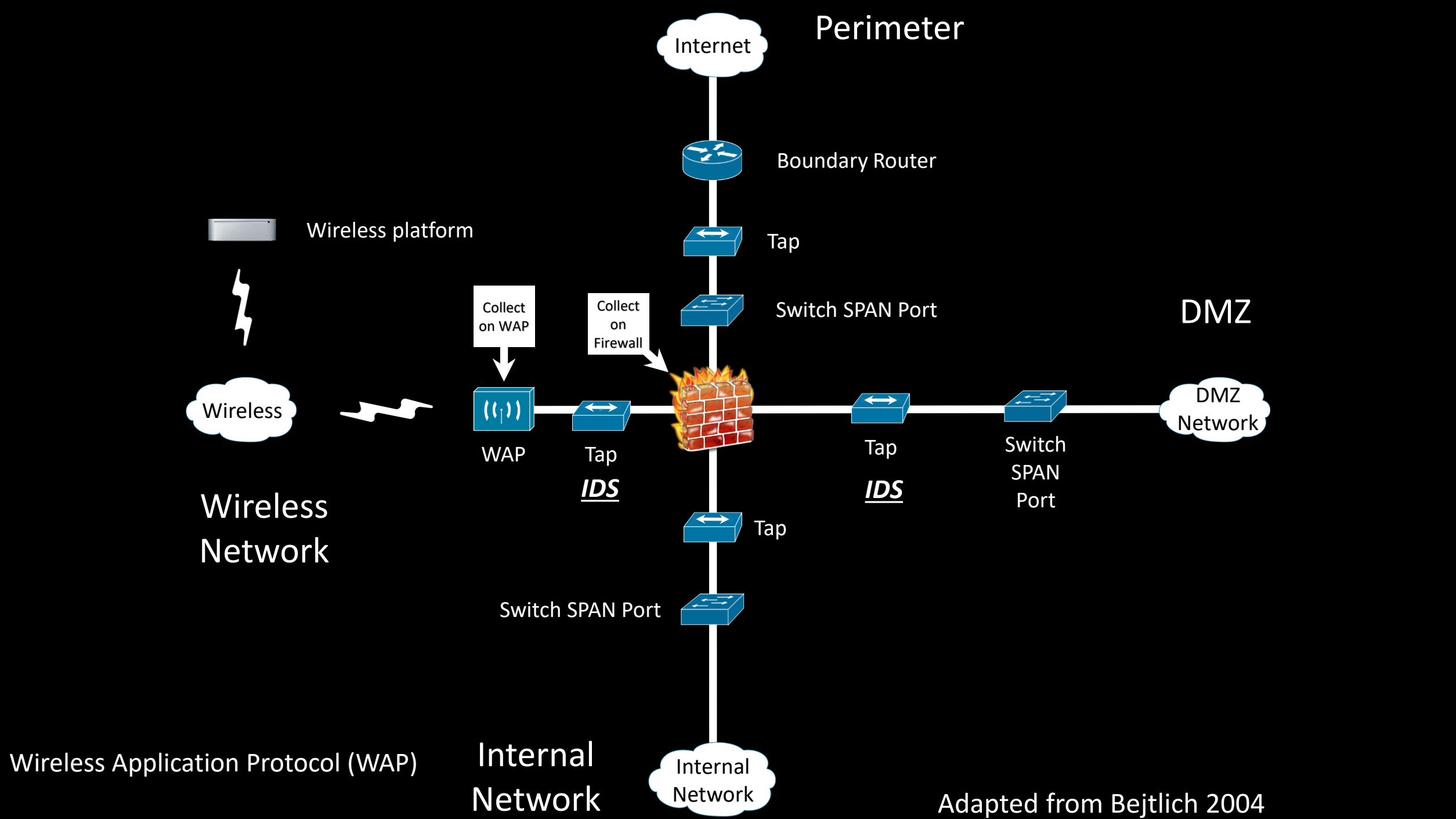


**Indicators** - While precursors are relatively rare, indicators are all too common. Too many types of indicators exist to exhaustively list them, but some examples are listed below:

- 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



Wireless Application Protocol (WAP)

Internal Network

Adapted from Bejtlich 2004



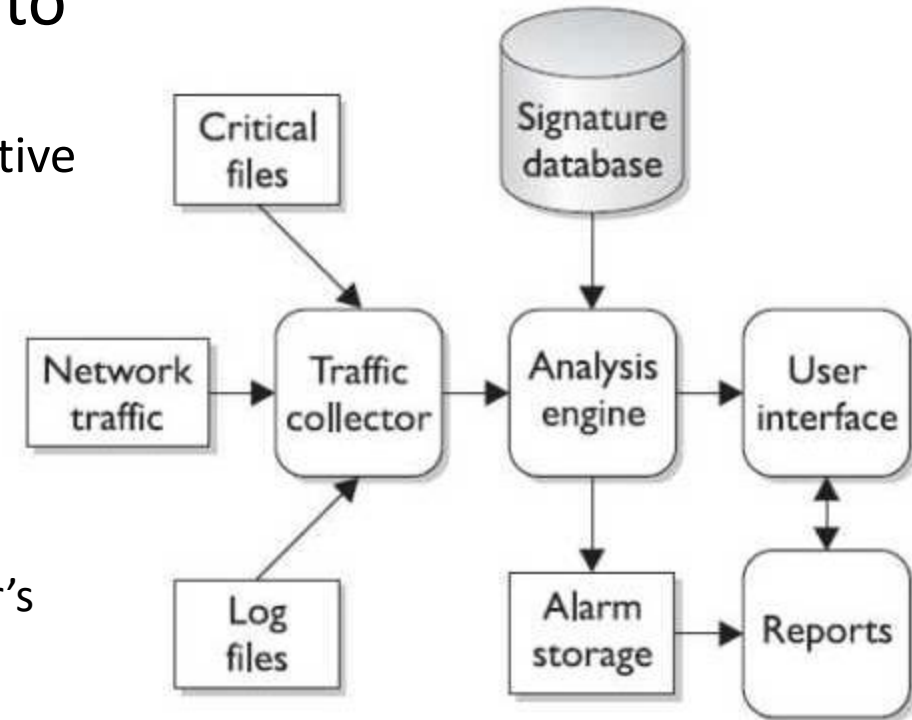
# Intrusion Detection Systems (IDSs)

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



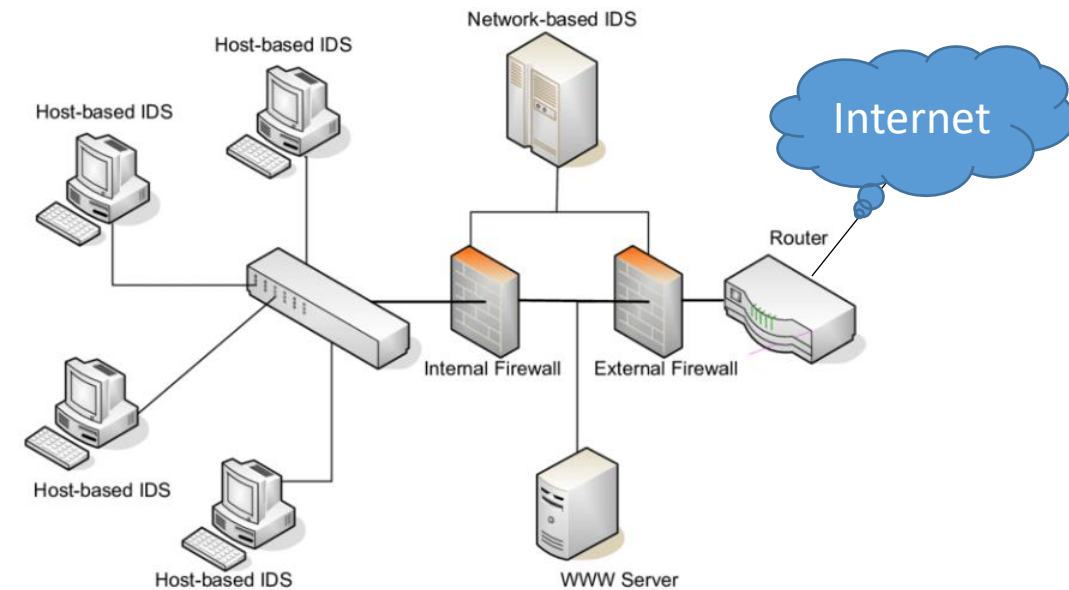
# Intrusion Detection Systems (IDSs)

Two main types of IDS

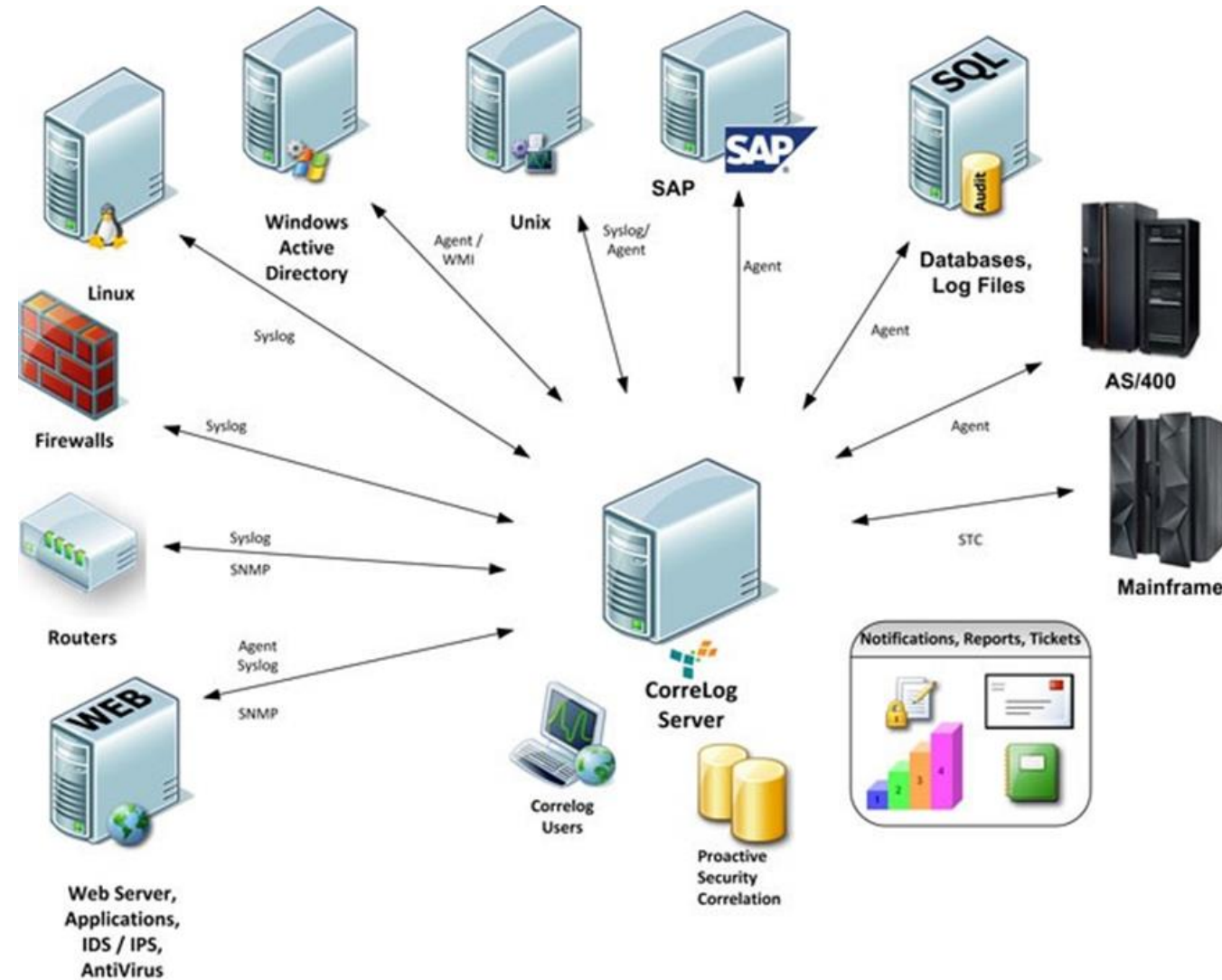
1. **Host-based** for analyzing activity within a particular computer system
2. **Network-based** for monitoring network communications

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

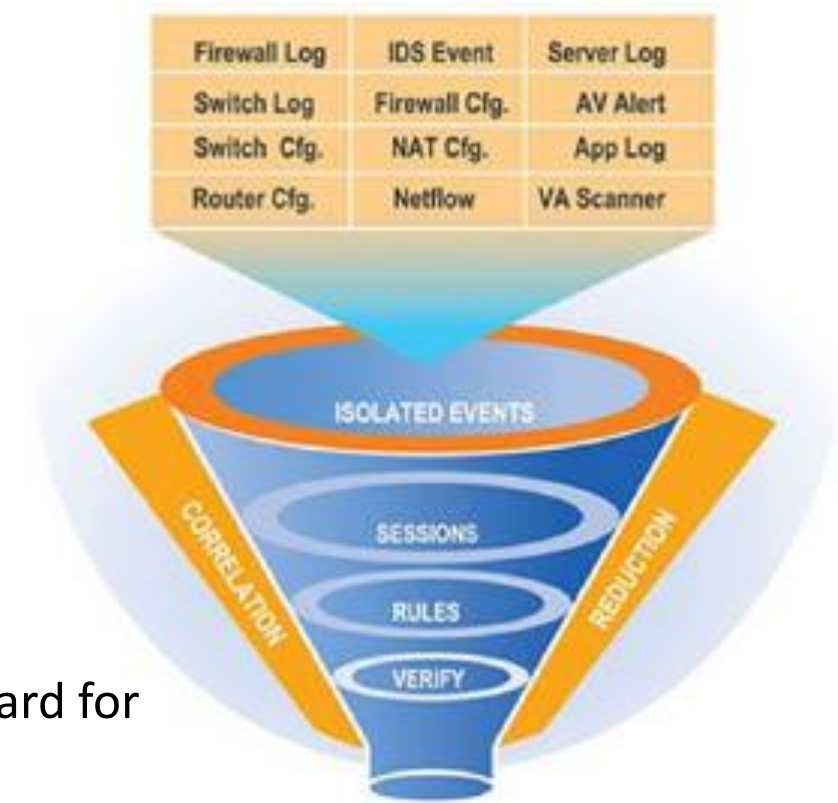


# Continuous monitoring with a Security Information and Event Management (SIEM) system



# 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



# 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 produced by security devices, network infrastructure, systems and applications. The primary data source is log data.





Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure Enterprise Security ES

Security Posture Edit More Info Download Print

**ACCESS NOTABLES**  
Total Count

**380** ↓ -44

**ENDPOINT NOTABLES**  
Total Count

**63** 0

**NETWORK NOTABLES**  
Total Count

**15** ↑ +2

**IDENTITY NOTABLES**  
Total Count

**7** 0

**AUDIT NOTABLES**  
Total Count

**26** ↑ +9

**THREAT NOTABLES**  
Total Count

**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

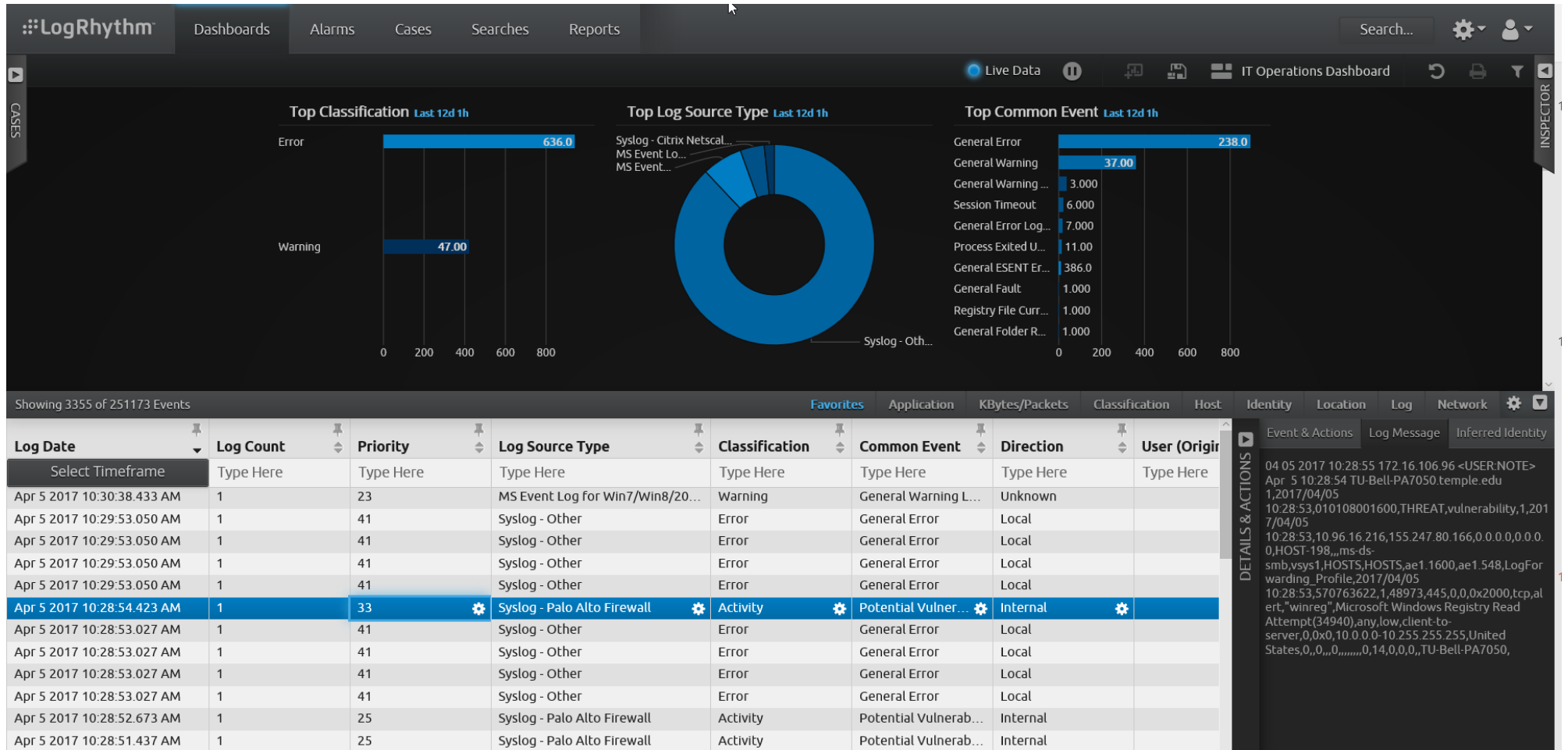
**Top Notable Event Sources**

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

1m ago

About Support File a Bug Documentation Privacy Policy © 2005-2015 Splunk Inc. All rights reserved.

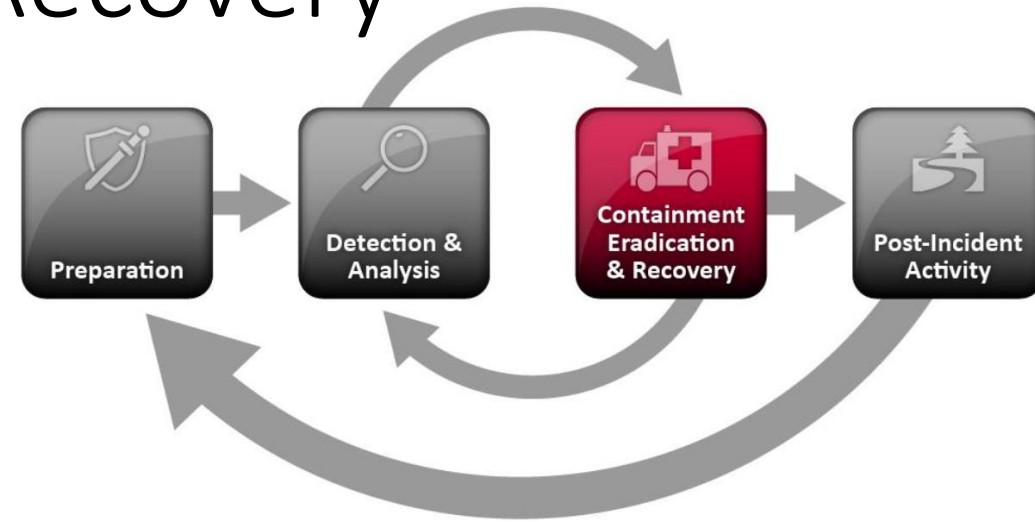
# LogRhythm™



# 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)

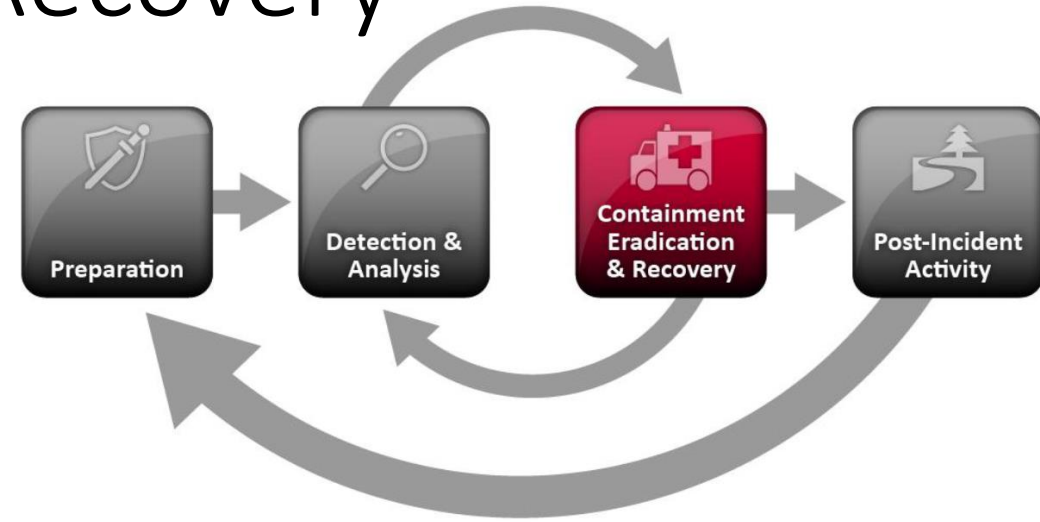




# Containment, Eradication, and Recovery

**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

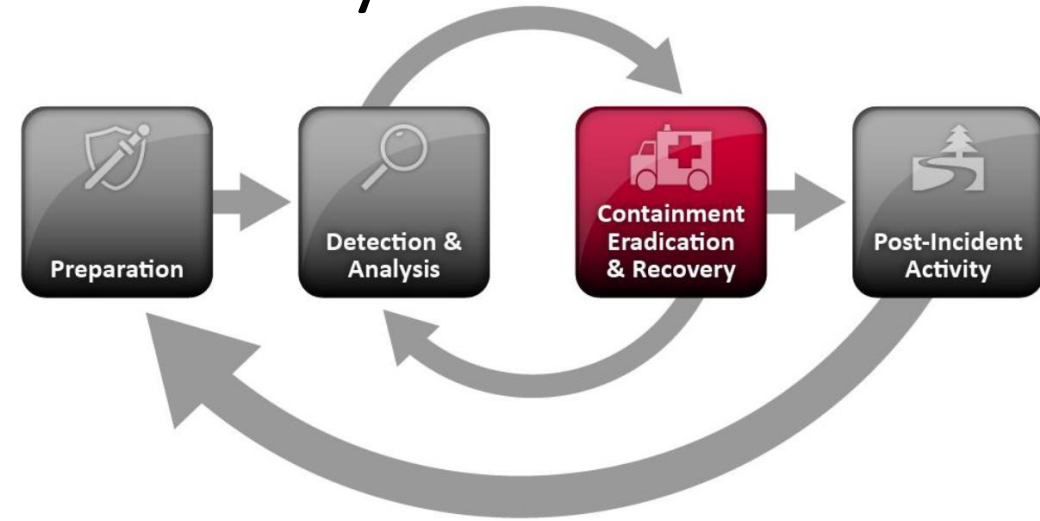
**Recovery** - In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents

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, ...)

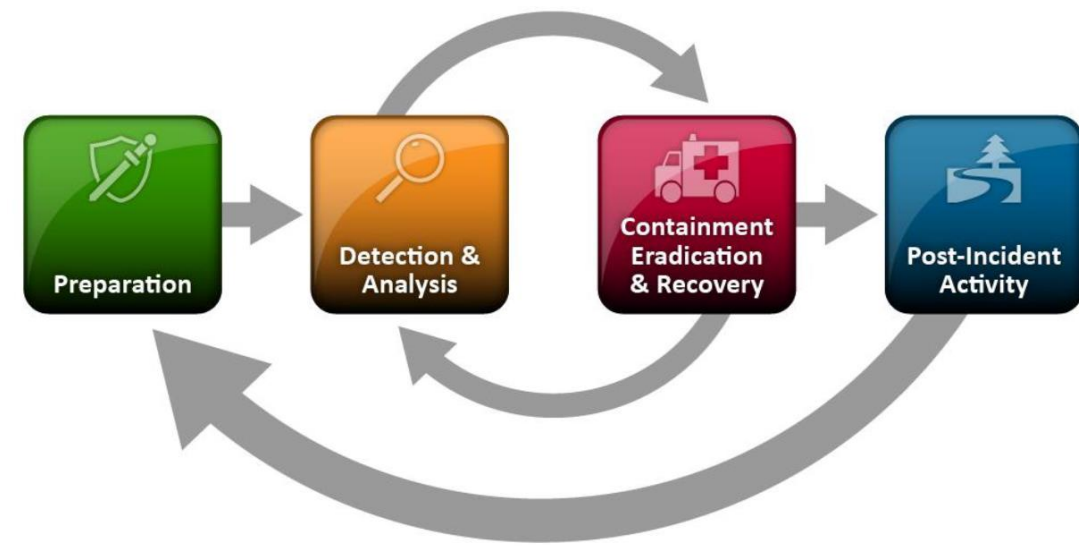
Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner

- 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

- ✓ 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

# Team Project Q&A