Unit #5a

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

Key Differences Between an Incident and a Disaster

Feature	Incident	Disaster
Impact Scope	Limited, affecting a specific system, user, or process	Widespread, affecting an entire organization or critical infrastructure
Response Time	Can be resolved quickly with normal procedures	Requires long-term recovery efforts
Business Continuity Effect	Minor disruption, normal operations continue	Major disruption, business continuity is threatened
Examples	Phishing, malware infection, minor data breach	Natural disasters, ransomware attack, data center destruction

☁️ SaaS Incident vs. Disaster Scenarios

Category	Incident	Disaster
User Authentication & Identity Management	A single user reports being locked out due to MFA failure.	IAM misconfiguration leads to unauthorized access for all users.
Network Security	A DDoS attack causes temporary slowness.	A large-scale **data breach** due to misconfigured firewall rules exposes customer data.
Application Downtime	A microservice fails due to a coding bug, affecting a specific feature.	A core application service failure due to database corruption renders the entire system unusable.
Data Integrity & Database Issues	An API bug causes minor inconsistencies in customer transaction logs.	A **database failure with no recent backups** results in the loss of critical SaaS user data.
Cloud Infrastructure Issues	A single compute instance crashes, auto-scaling restores it within minutes.	A **cloud region outage** (e.g., AWS US-East-1 failure) takes down the entire application for hours.
Supply Chain & Third-Party Services	A third-party analytics service fails, affecting reporting features.	A **major supply chain attack** compromises dependencies in the SaaS platform, leading to widespread data theft.
Compliance & Regulatory Failures	A compliance check identifies an expired security certificate.	**GDPR violations** due to a massive personal data leak result in heavy fines and legal action.

Virus

Virus: attached to a file

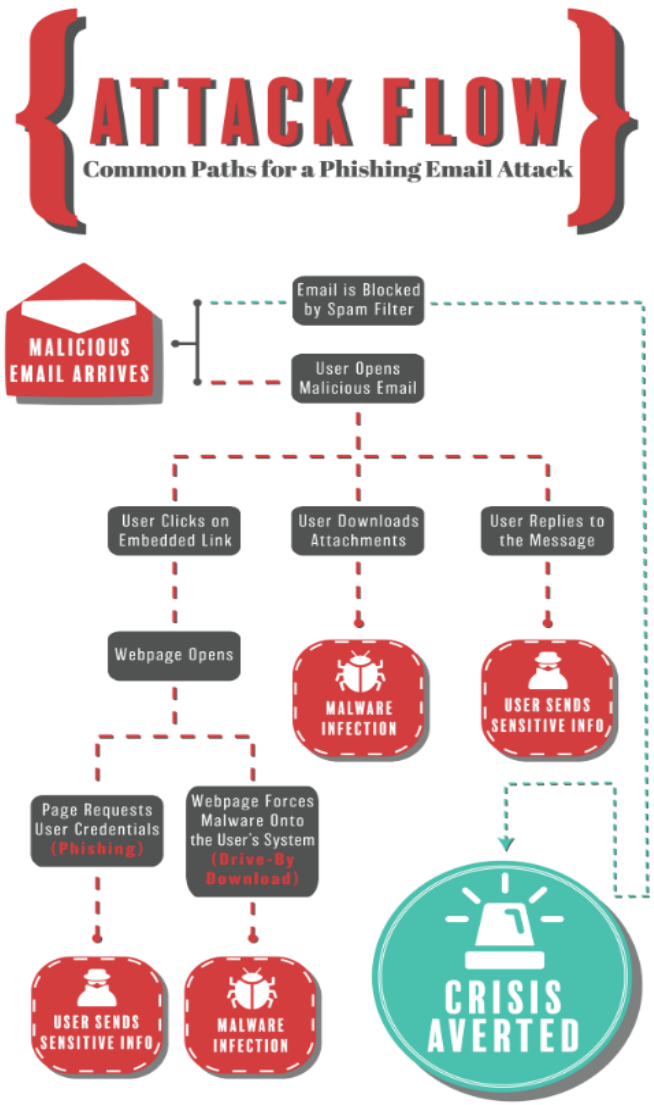
1986

Brain virus


BRAIN
an F-Secure Production

Malware Types, What It Does, and Real-World Examples

Malware Type	What It Does	Real-World Example
Ransomware	Encrypts a victim's files or system, demanding a ransom for decryption. Often spreads via phishing emails, malicious ads, or exploits.	*WannaCry* (2017) - Exploited the EternalBlue vulnerability in Windows to spread rapidly across networks, encrypting files and demanding Bitcoin payments.
Fileless Malware	Operates in memory without leaving traditional files, making it harder to detect. Uses legitimate system tools (e.g., PowerShell, WMI) to execute attacks.	*Astaroth* - A fileless malware campaign using Windows Management Instrumentation (WMI) and PowerShell to steal credentials and install additional payloads.
Spyware	Secretly monitors user activity, stealing sensitive information like credentials, financial data, and browsing habits.	*Pegasus* - A sophisticated spyware used to exploit zero-day vulnerabilities on iOS and Android to gain full device access.
Adware	Delivers unwanted advertisements, often redirecting users to malicious websites or slowing down the system.	*Fireball* - A large-scale adware campaign that hijacked browsers to generate fraudulent ad revenue.
Trojans	Disguised as legitimate software but carries malicious payloads like backdoors, spyware, or ransomware.	*Emotet* - Initially a banking Trojan but evolved into a malware delivery platform for ransomware and other threats.
Worms	Self-replicating malware that spreads across networks without user interaction, often exploiting vulnerabilities.	*Morris Worm* (1988) - One of the first worms to spread via the internet, infecting Unix systems and causing widespread slowdowns.
Rootkits	Grants attackers privileged access while remaining undetected by security software. Often modifies system files and hides processes.	*TDL-4* - A sophisticated rootkit capable of controlling an infected machine while evading detection.
Bots (Botnets)	Infects devices to form a network (botnet) controlled by an attacker for DDoS attacks, spam, or cryptojacking.	*Mirai Botnet* - Used IoT devices to launch large-scale DDoS attacks, including one against Dyn DNS in 2016.
Keyloggers	Records keystrokes to steal passwords, financial information, and other sensitive data.	*Agent Tesla* - A widely used keylogger that also captures clipboard data and screenshots.
Mobile Malware	Targets smartphones and tablets, often spreading through malicious apps or SMS phishing (smishing).	*Triada* - A sophisticated Android malware that granted root access and installed additional malicious apps.




```
+-------------------------------+
|  1. Insertion (Initial Infection)
+-------------------------------+
          |
          v
+-------------------------------+
| Employee receives phishing email
| containing malicious attachment
+-------------------------------+
          |
          v
+-------------------------------+
| Employee opens the attachment,
| executing WannaCry ransomware.
+-------------------------------+
```

```
+-------------------------------+
|  2. Replication (Spreading)  |
+-------------------------------+
          |
          v
+-------------------------------------------------------------+
| Ransomware exploits EternalBlue vulnerability
| and spreads to other unpatched systems in the network.
+-------------------------------------------------------------+
          |
          v
+---------------------------------------+
| Infects hospital servers, workstations |
| patient record databases, and backups. |
+---------------------------------------+
```

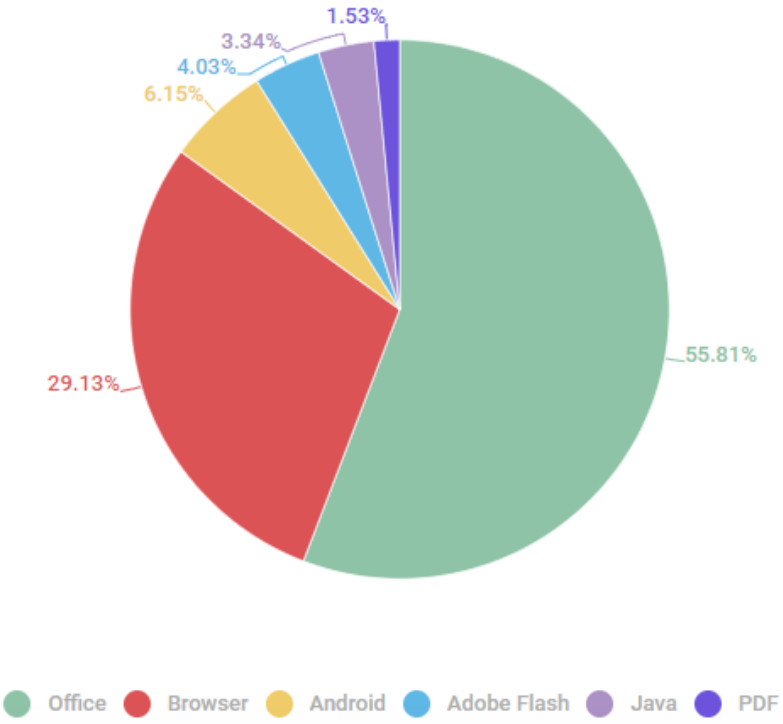
```
|  3. Avoidance (Evasion)       |
+-------------------------------+
          |
          v
+-------------------------------------------------------------+
| Disables Windows Defender and security tools
| Uses process hollowing to hide malicious activity
+-------------------------------+
|  5. Payload (Malicious Action) |
+-------------------------------+
          |
          v
+-------------------------------------------------------------+
Encrypts medical records, financial data, and
other hospital files, rendering systems useless.
```

```
|  4. Trigger (Activation)     |
+-------------------------------+
          |
          v
+-------------------------------------------------------------+
| A countdown timer appears demanding ransom in Bitcoin
| Encrypted files renamed with .WNCRY extension        |
+-------------------------------+
|  6. Eradication (Persistence) |
+-------------------------------+
          |
          v
+-------------------------------------------------------------+
| Ransomware remains on infected devices unless removed.
| Attempts to spread further if not blocked or patched.
| A kill switch domain is later discovered, stopping spread.
```

Vulnerable applications used by cybercriminals during cyberattacks

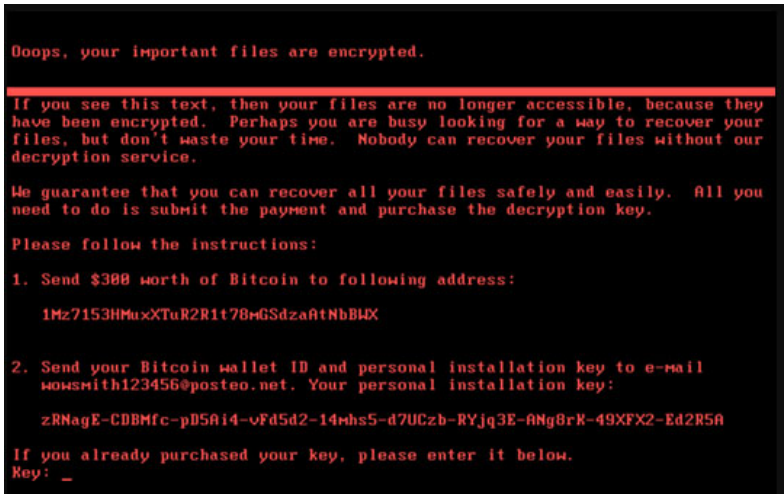
Q2 2021 injected some minor changes into our statistics on exploits used by cybercriminals. In particular, the share of exploits for Microsoft Office dropped to 55.81% of the total number of threats of this type. Conversely, the share of exploits attacking popular browsers rose by roughly 3 p.p. to 29.13%.

- https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/



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



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:

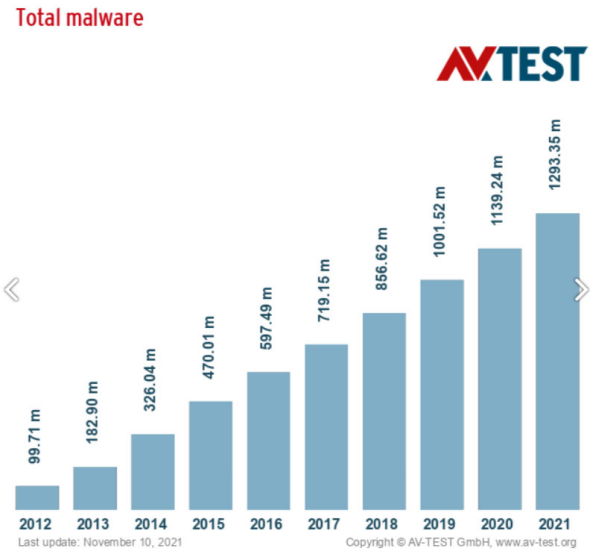
- Compromising systems with botnets for later use in:
  - Distributed denial of service (DDoS) attacks
  - Spam distribution
- Ransomware encrypting users' files with keys that are only given after users pay a ransom
- Spyware collects personal data for resale
- Redirecting web traffic pointing people 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

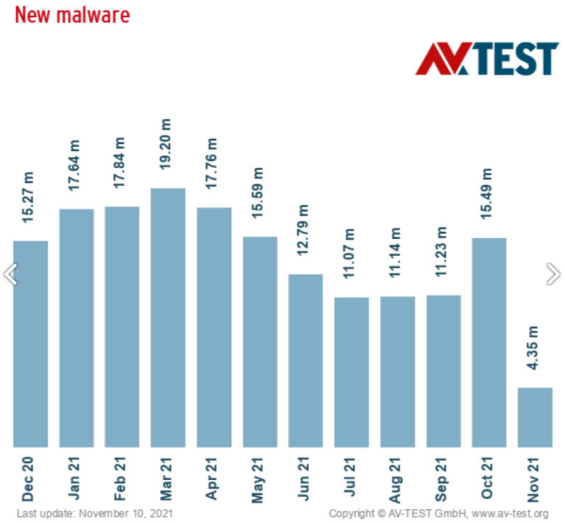
Malware is increasing

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, …)





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

Common Components of Malware

Component	Description
Insertion	Malware installs itself on the victim's system through phishing, drive-by downloads, USB infections, or software vulnerabilities.
Replication	The malware spreads to new victims via network shares, email attachments, removable media, or system exploits.
Avoidance	Uses techniques like polymorphism (changing its code), encryption, rootkits, or anti-analysis techniques to evade detection.
Trigger	A specific event (e.g., a date, user action, or network connection) initiates the execution of the malware's payload.
Payload	Executes its malicious function, such as data theft, system corruption, backdoor installation, file encryption, or botnet recruitment.
Eradication	Some malware self-destructs after execution to avoid detection, while others attempt to persist by modifying system settings.

Anti-Malware Software Detection Techniques: Comprehensive Comparison

Detection Technique	Definition	How It Works	Pros	Cons	Use Cases	Detection Capability	Effectiveness & Speed	Associated Malware Types
Signature-Based Detection	Matches files against a database of known malware signatures	Compares hash values or specific code patterns to a signature database	✅ Fast and efficient for known malware ✅ Low false positive rate	❌ Cannot detect zero-day threats ❌ Requires frequent updates	Traditional antivirus software Detecting common viruses, worms, trojans	🔹 **Detects:** Known malware 🔹 **Misses:** Zero-day, polymorphic, and fileless malware	🔹 **Speed:** Very fast 🔹 **Effectiveness:** High for known threats, low for unknown threats	**Known Viruses**, **Worms**, **Trojans**, **Ransomware**, **Rootkits**
Integrity-Based Detection	Uses file hashing to detect unauthorized changes in system files	Generates cryptographic hashes of files and monitors changes	✅ Effective in ensuring file integrity ✅ Detects unauthorized modifications	❌ Cannot detect new malware unless a file changes ❌ High resource consumption for constant monitoring	Protecting critical system files Detecting rootkits and unauthorized system modifications	🔹 **Detects:** File tampering, system modifications 🔹 **Misses:** Most standalone malware attacks	🔹 **Speed:** Moderate (depends on file scanning frequency) 🔹 **Effectiveness:** High for integrity violations, low for standalone malware detection	**Rootkits**, **Bootkits**, **Fileless Malware**, **Advanced Persistent Threats (APTs)**
Heuristic-Based Detection	Identifies malware based on code structure analysis and deviation from normal patterns	Uses machine learning and rule-based techniques to flag suspicious code	✅ Can detect zero-day threats ✅ Effective against polymorphic malware	❌ Higher false positive rates ❌ Requires continuous fine-tuning	Identifying new virus strains Scanning for unknown threats	🔹 **Detects:** New malware variants, polymorphic malware 🔹 **Misses:** Highly obfuscated malware	🔹 **Speed:** Moderate (depends on complexity of heuristics) 🔹 **Effectiveness:** Medium to high, especially for unknown threats	**Polymorphic Malware**, **Metamorphic Viruses**, **Obfuscated Malware**, **Encrypted Malware**
Behavior-Based Detection	Monitors program execution and behavior to detect malicious actions	Tracks system calls, memory modifications, and network activity in real-time	✅ Highly effective against fileless malware and ransomware ✅ Does not rely on signature updates	❌ Resource-intensive ❌ Can generate false positives	Detecting ransomware encryption Identifying malicious insider threats	🔹 **Detects:** Fileless malware, ransomware, advanced persistent threats (APTs) 🔹 **Misses:** Subtle malware with minimal system impact	🔹 **Speed:** Slower due to real-time monitoring 🔹 **Effectiveness:** High for detecting evolving threats	**Fileless Malware**, **Ransomware**, **Zero-Day Attacks**, **Trojans**, **Spyware**, **Keyloggers**

Protection and Detection Techniques

Feature	Anti-Malware	Intrusion Prevention System (IPS)	Intrusion Detection System (IDS)
Primary Function	Detects & removes malware from files and systems	Blocks malicious network traffic before it reaches a system	Monitors and logs suspicious network activity
Detection Scope	Files, processes, registry, system memory	Network packets, intrusion attempts	Network packets, logs, host-based intrusion events
Action Taken	Quarantine, delete, or block threats	Blocks threats in real-time	Sends alerts but does not block
Best At	Preventing malware infections	Stopping network-based attacks	Providing visibility into security threats
Detection Capability	Detects malware at the system level (files, processes, memory)	Detects and blocks network-based intrusions	Detects but does not block network-based threats
Challenges	Requires frequent updates, potential false positives	Can disrupt legitimate traffic, high false positives	No prevention, requires human analysis
Associated Malware Types	**Viruses, Worms, Trojans, Rootkits, Ransomware, Fileless Malware**	**DDoS Attacks, Network Worms, Exploits, Botnets, Web-Based Attacks**	**Network-Based Malware, SQL Injection Attacks, Credential Theft, Insider Threats**

Protection and Detection Techniques

Protection Techniques

Protection Technique	Description	Effectiveness
Quarantine the File	Isolates the suspicious file in a secure location to prevent execution.	High (Prevents malware from spreading)
Clean the File	Attempts to remove malicious code from the infected file.	Moderate to High (Success depends on malware complexity)
Roll-Back to Prior Version of the File	Restores the file to a previous clean state using backups or system restore.	High (Best for ransomware recovery)
Warn the User	Notifies the user of suspicious activity and allows manual intervention.	Moderate (Useful for security awareness)
Log the Event	Records malware detection events for forensic analysis and security audits.	High (Crucial for threat hunting and compliance)

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

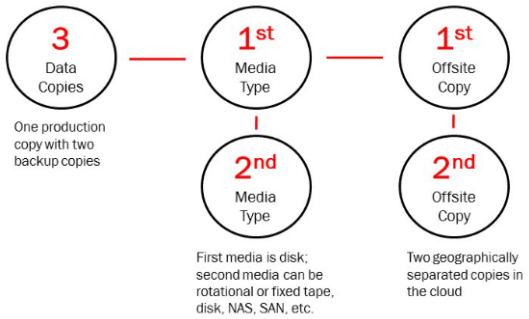
https://www.rapid7.com/fundamentals/malware-attacks/

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



How It Works

3 Copies of Data:

1. One **primary copy** (active data used daily).
2. Two **backup copies** to protect against corruption, loss, or ransomware.

2 Different Storage Types:

1. Backups should be stored on at least two distinct media types, such as:
    1. Internal or external hard drives
    2. Network-attached storage (NAS)
    3. Solid-state drives (SSD)
    4. Cloud storage
    5. Tape backups

1 Copy Stored Offsite:

1. At least one backup should be stored at a remote location to prevent data loss from physical damage, theft, or disasters.
2. Examples:
    1. Cloud backups (Google Drive, AWS S3, Azure, etc.)
    2. Offsite data centers
    3. Physical media stored securely in another location

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

Term	Definition & Explanation	Why It's Important	Responsibilities	Challenges
Business Continuity Plan (BCP)	A strategy ensuring critical business functions continue during and after a disaster. Includes risk assessments, recovery strategies, and testing.	Minimizes downtime and financial loss, ensures compliance, and maintains customer trust.	CIO, Risk Managers, Business Continuity Teams ensure planning, testing, and execution of BCP strategies.	Keeping plans updated, ensuring all departments are aligned, and handling supply chain dependencies.
Resiliency	The ability of an organization to anticipate, withstand, recover, and adapt to adverse conditions while continuing operations.	Reduces impact of disruptions, enhances cybersecurity posture, and ensures business sustainability.	IT and Security Teams, Business Leaders, Risk Management Teams implement security and recovery strategies.	Measuring resilience objectively, balancing cost and feasibility, and keeping up with evolving threats.
Critical Infrastructure	Essential systems like power grids, financial institutions, telecommunications, and healthcare that support national security and economic stability.	Protects against economic collapse, cyberattacks, and physical threats that could cripple society.	Government Agencies (DHS, CISA), Private Sector Leaders, Security Teams ensure protection, monitoring, and emergency response.	Increased cyber threats, supply chain vulnerabilities, and interdependency between sectors.
Disaster Recovery Plan (DRP)	A subset of BCP focusing on IT system restoration after an incident. Includes backup strategies, failover procedures, and testing.	Ensures quick recovery of IT services, reduces data loss, and minimizes disruption.	IT Managers, System Administrators, DR Teams implement data backup, system recovery, and alternative infrastructure.	Complexity in maintaining redundant systems, cyber threats like ransomware, and budget constraints.
Business Impact Analysis (BIA)	Identifies critical business functions, dependencies, and the potential financial and operational impact of disruptions.	Helps prioritize recovery efforts, ensures resource allocation, and supports compliance.	Risk Managers, Business Analysts, IT Leaders assess dependencies, financial loss projections, and downtime impacts.	Difficult to quantify intangible losses, ensuring accuracy, and adapting to changing business models.
Contingency Planning	A comprehensive plan that integrates BCP, DRP, and IRP to prepare for operational failures, cyberattacks, and disasters.	Ensures an organization is prepared for multiple types of threats, minimizing financial and reputational damage.	Executive Management, Security Teams, Business Continuity Officers oversee plan development, drills, and policy enforcement.	Keeping plans adaptable, training employees, and ensuring stakeholder coordination.
Incident Response (IR)	The process of detecting, analyzing, containing, eradicating, recovering, and learning from cybersecurity incidents.	Helps organizations mitigate cyber threats, minimize damage, and improve future security.	CISOs, Security Operations Centers (SOC), Incident Response Teams lead investigations and containment efforts.	Detecting advanced threats, reducing false positives, and ensuring rapid response.
Incident Response Plan (IRP)	A documented approach for responding to cybersecurity incidents, outlining roles, communication protocols, and technical response steps.	Ensures structured and efficient response to threats, helping limit damage and ensure compliance.	Cybersecurity Teams, Legal & Compliance Teams, PR Teams handle communication, forensics, and mitigation.	Keeping IRP updated, coordinating multi-team efforts, and handling regulatory requirements.

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 <u>resilient</u>**"

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

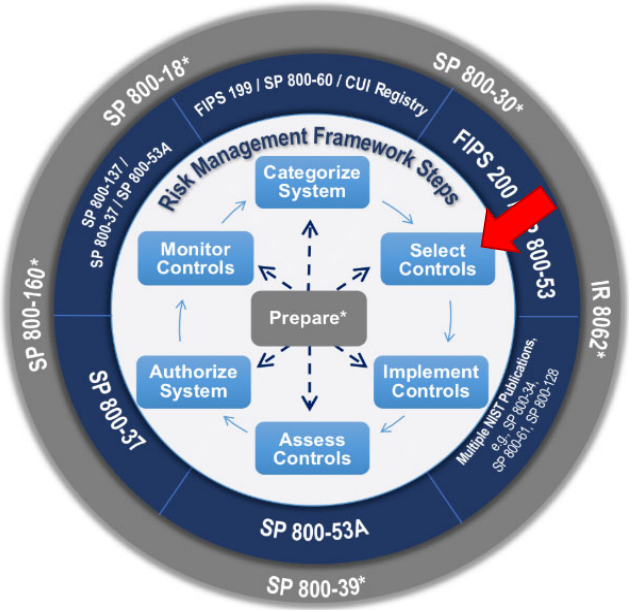
Source: ISO 22301:2012
Societal security – Business continuity management systems - Requirements

…includes a Disaster Recovery Plan (DRP)

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

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

NIST CSF Function	Related Concept	Explanation
Identify	BIA, Critical Infrastructure	Identify business functions, dependencies, and critical assets.
Protect	BCP, Contingency Planning, Resiliency	Implement strategies to maintain operations and mitigate risks.
Detect	Incident Response (IR)	Identify security incidents and threats.
Respond	IRP, DRP	Take appropriate actions to contain and mitigate incidents.
Recover	BCP, DRP, Resiliency	Restore business and IT operations after an incident.

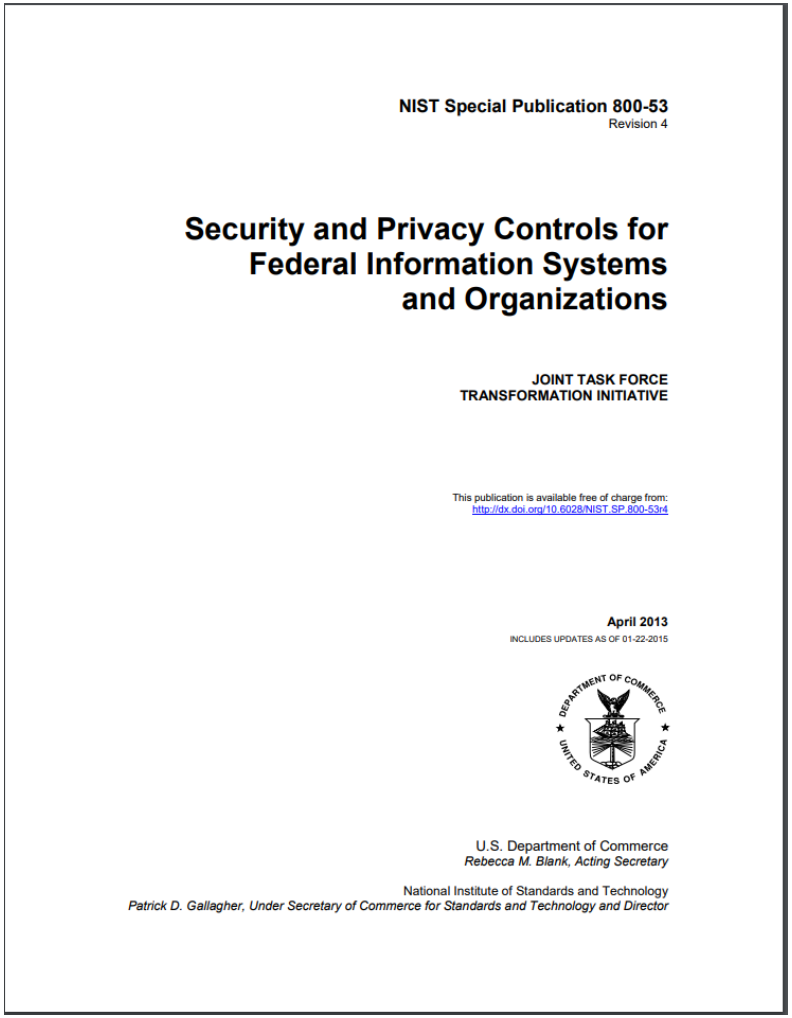


NIST Publication	Related Concept(s)	Description
NIST SP 800-34	BCP, DRP, Contingency Planning	Guide for Contingency Planning for IT systems, including BCP and DRP strategies.
NIST SP 800-61	IR, IRP	Computer Incident Handling Guide, covering incident response planning and execution.
NIST SP 800-160	Resiliency	Focuses on systems security engineering to build resilience.
NIST SP 800-39	BIA, Critical Infrastructure, Risk Management	Enterprise risk management framework addressing impact analysis and security.
NIST CSF	All (BCP, DRP, IR, Resiliency, Contingency, BIA, Critical Infrastructure)	Framework for cybersecurity risk management and resilience.

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

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Contingency Planning Controls

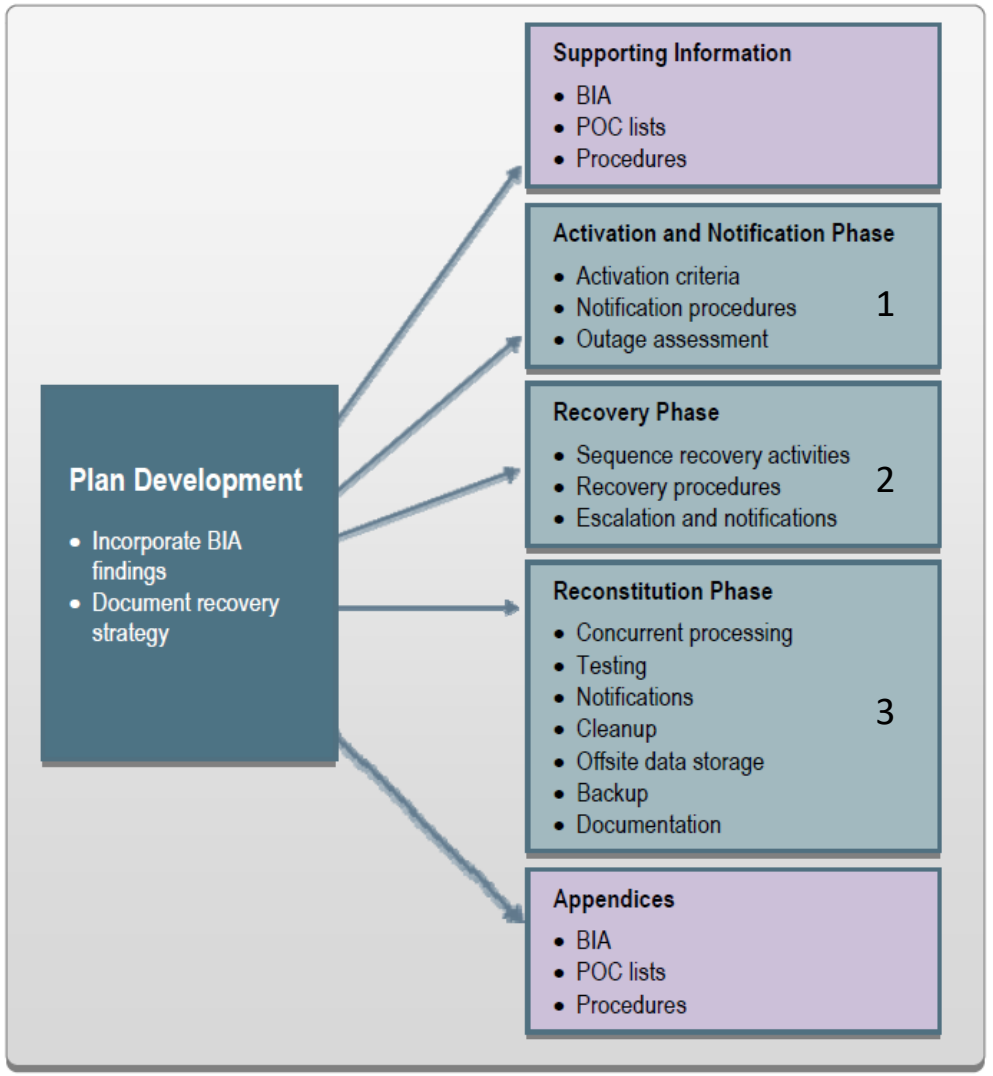
CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information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

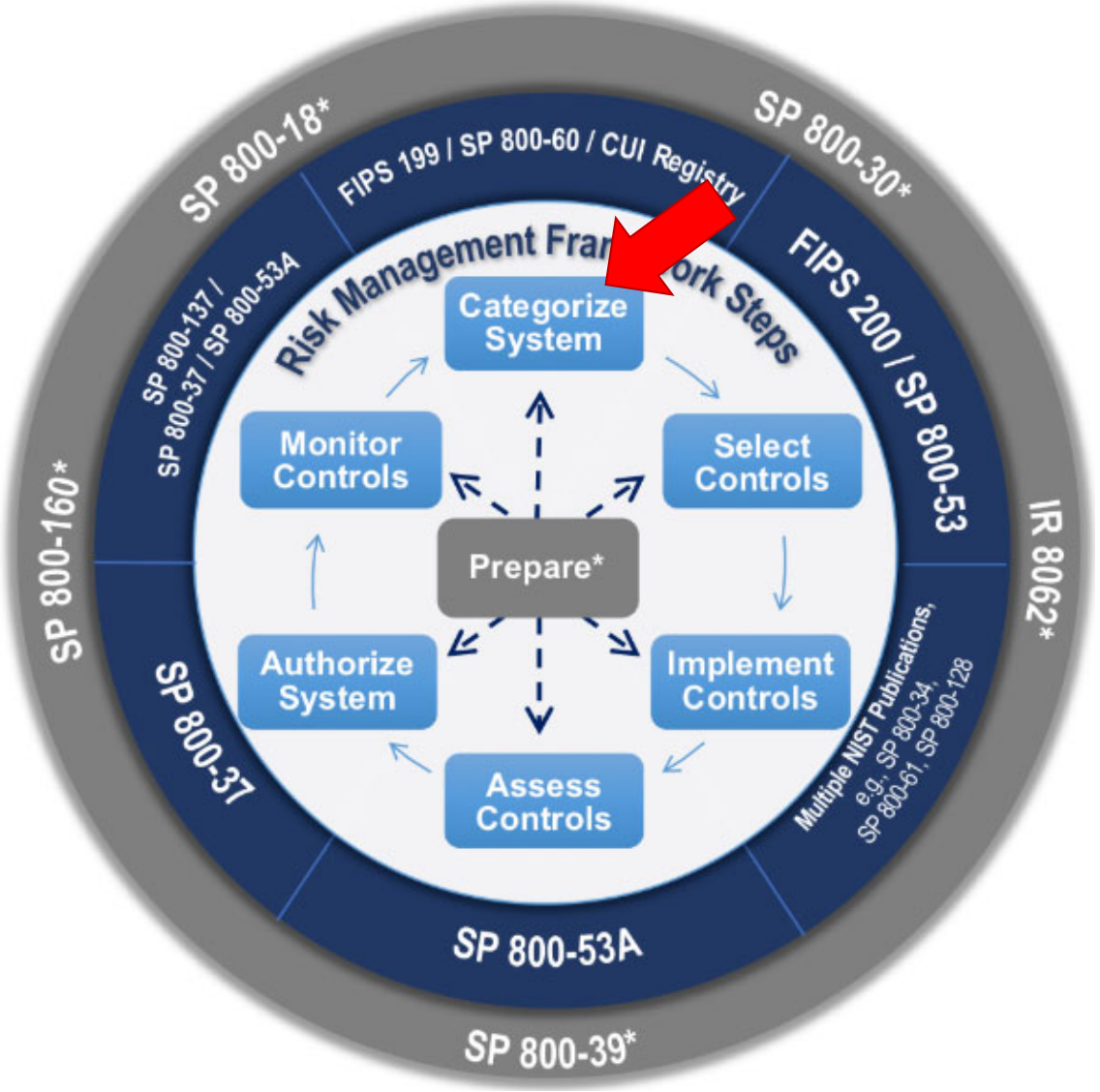
All dependent on a BIA “Business Impact Analysis”



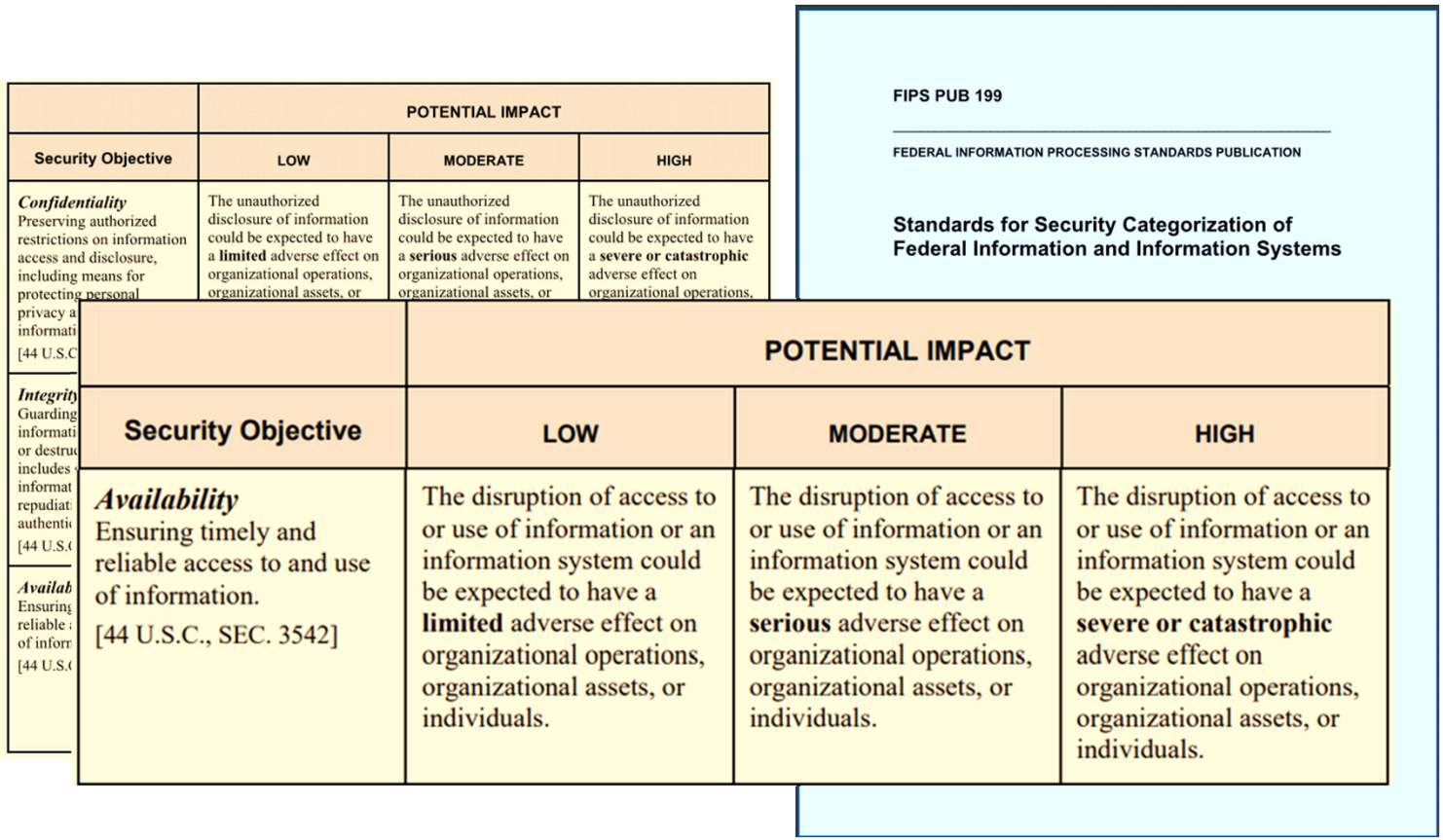
NIST SP 800-34 R1 – Contingency Planning Guide for Federal Information Systems

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?



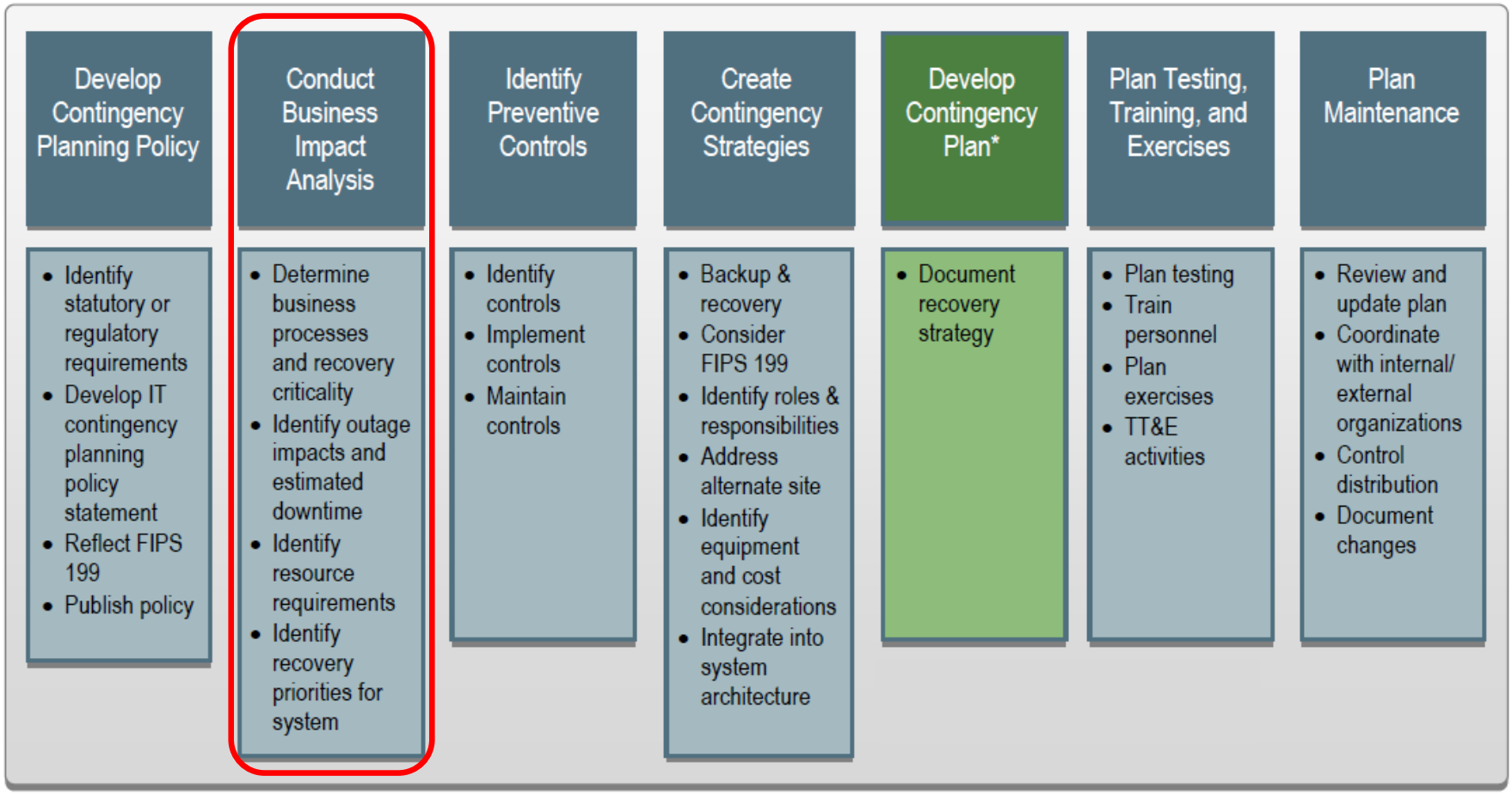
FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Security Objective	POTENTIAL IMPACT		
	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”



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

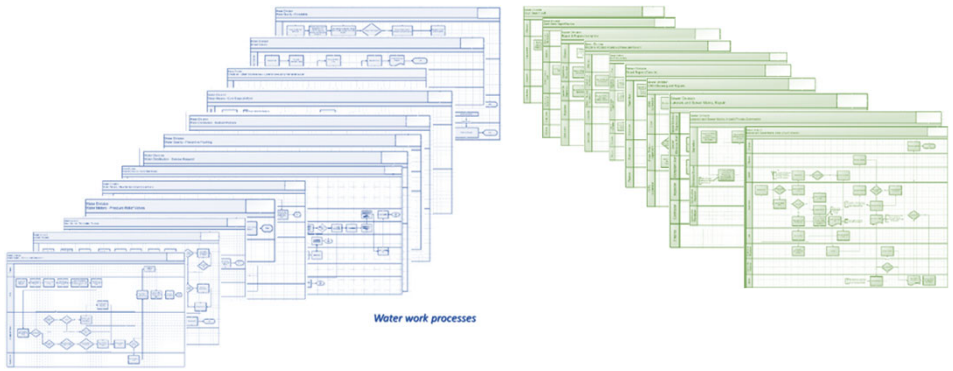
Business Impact Analysis (BIA) Answers

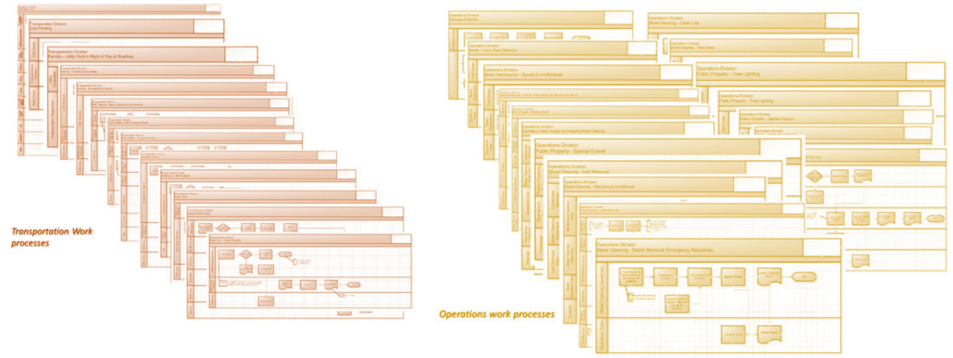
1. What are the work processes ?
2. How critical is each ?
3. What data, applications, and people are needed to run each critical process ?
4. What are the priorities for recovering information systems after disruption ?

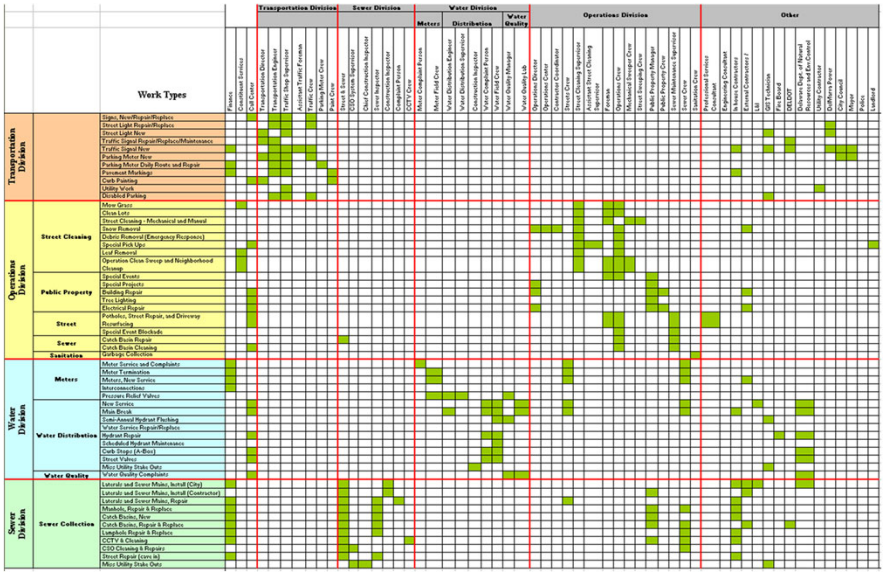
5. For each critical IT resource, what are:
   - **Recover time objective** (RTO):
     Maximum acceptable downtime
   - **Recovery point objective** (RPO):
     Maximum acceptable data loss (measured in time, but implies # of data records)

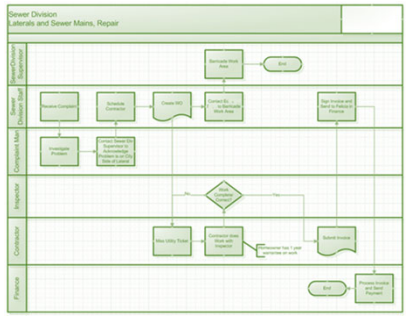
Prerequisite for BIA and contingency planning…

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



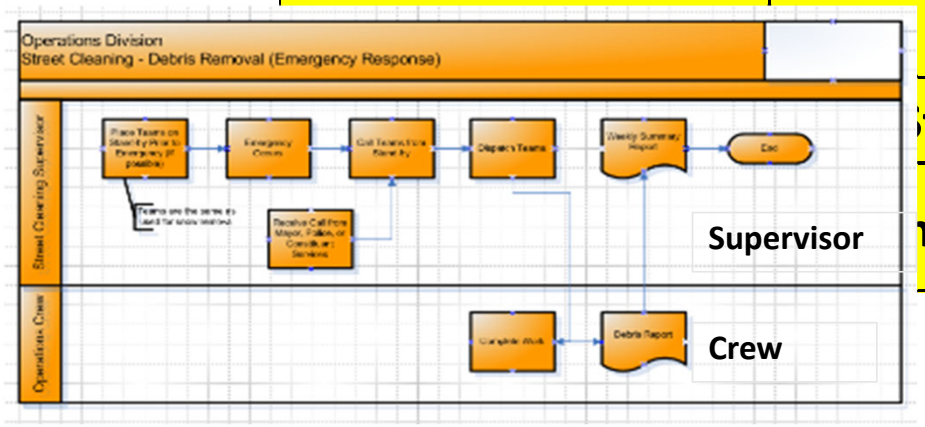






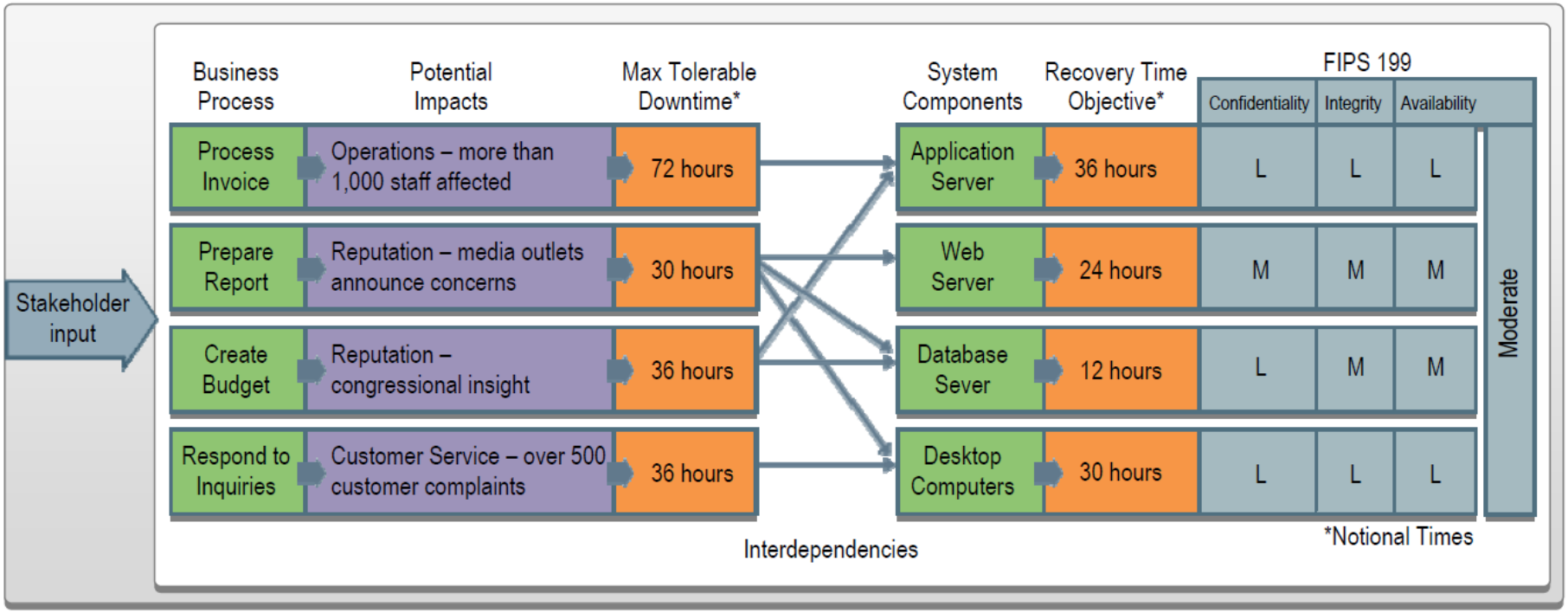
Priorities for recovery example

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
	treet	**Potholes, Street Repair, and Resurfacing**
		Special Event Blockade
	itation	**Catch Basin Repair**
		Catch Basin Cleaning
		Garbage Collection



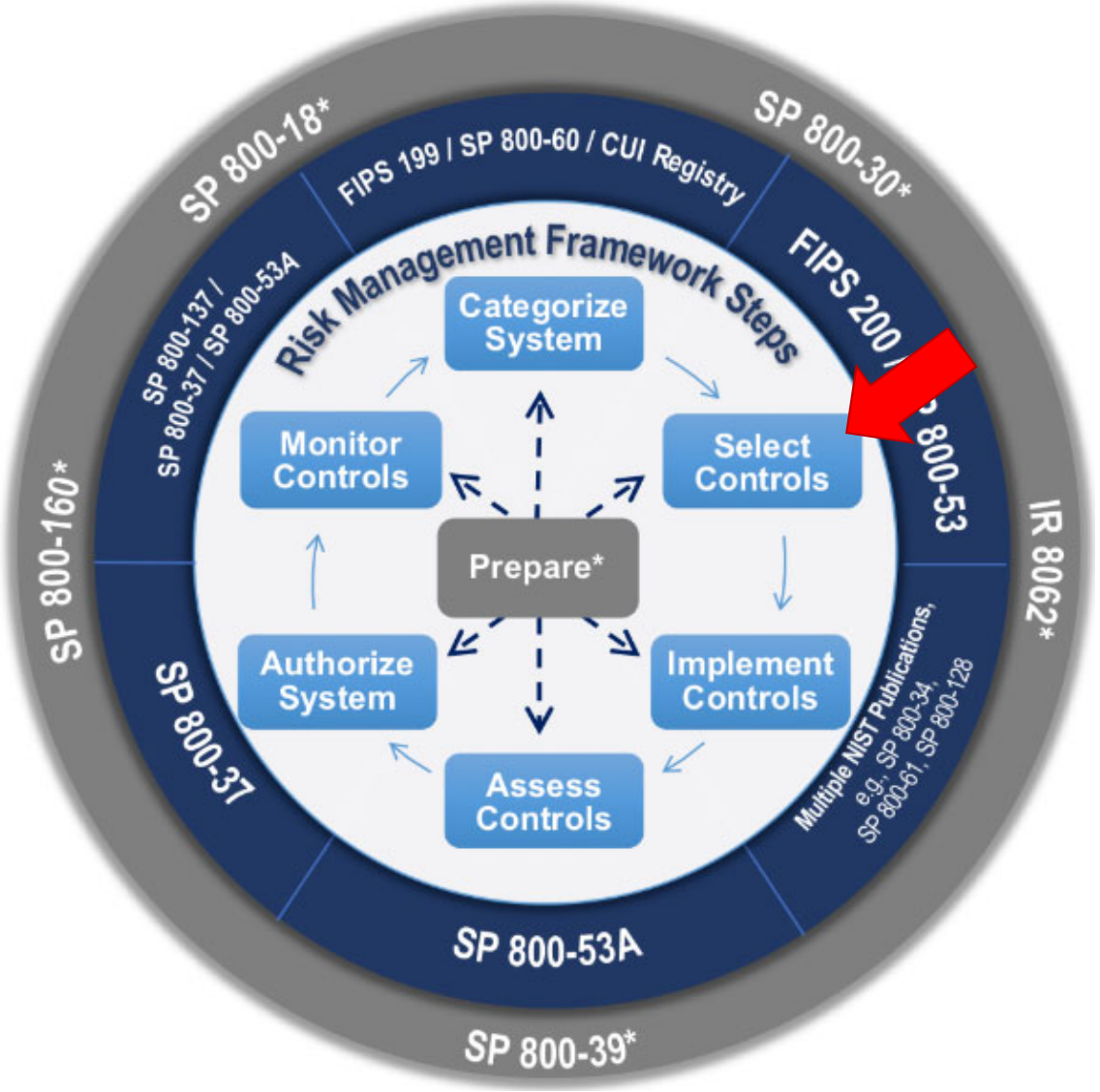
Business Impact Analysis (BIA) example…

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



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

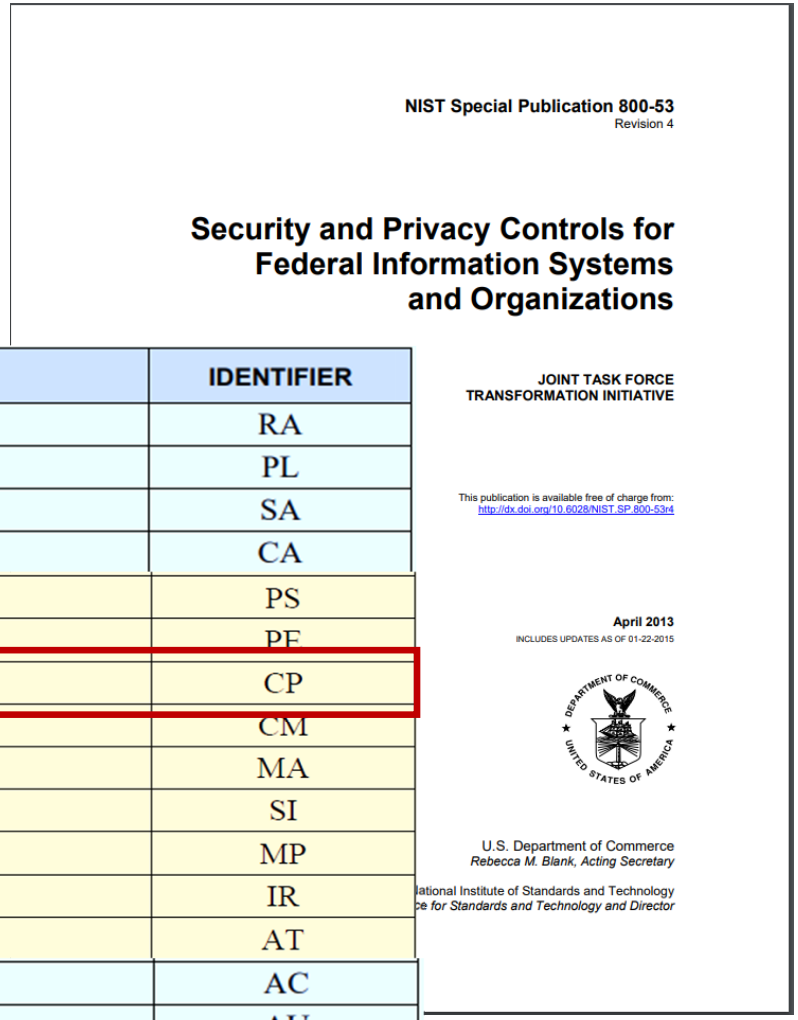
National Institute of Standards and Technology
U.S. Department of Commerce



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

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

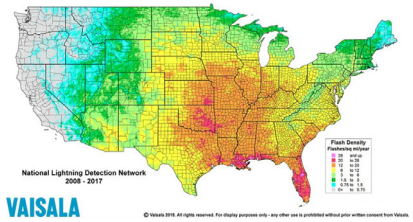
Cold site: Provides only the basic environment that can be outfitted with communication, utilities and computers

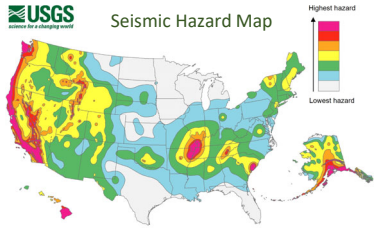
Site	Cost	Hardware Equipment	Telecommunications	Setup Time
Hot Site	High	Full	Full	Short
Warm Site	Medium	Partial	Full / Partial	Medium
Cold Site	Low	None	None	Long

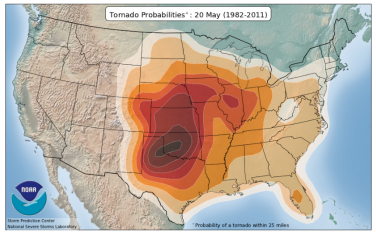
Location of Alternate site

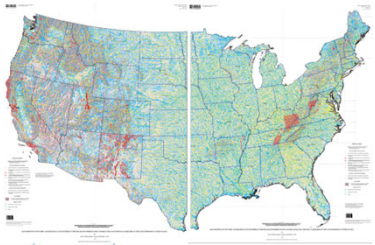
Disaster recovery site should be in a different geophysical area not susceptible to same disaster as the primary operations facility

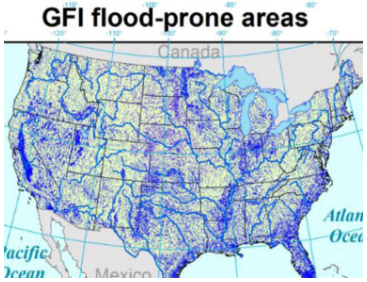
Note: even the cloud is located somewhere…



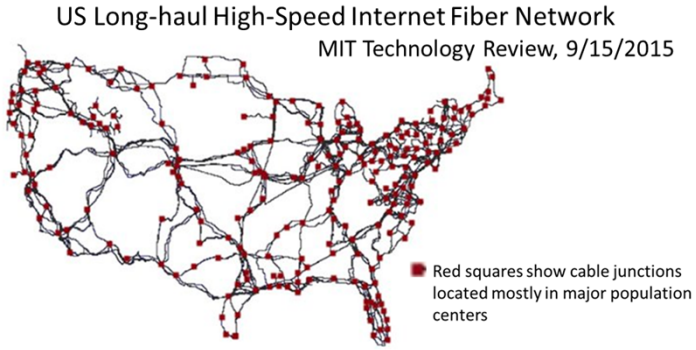








With multiple providers of:



- 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

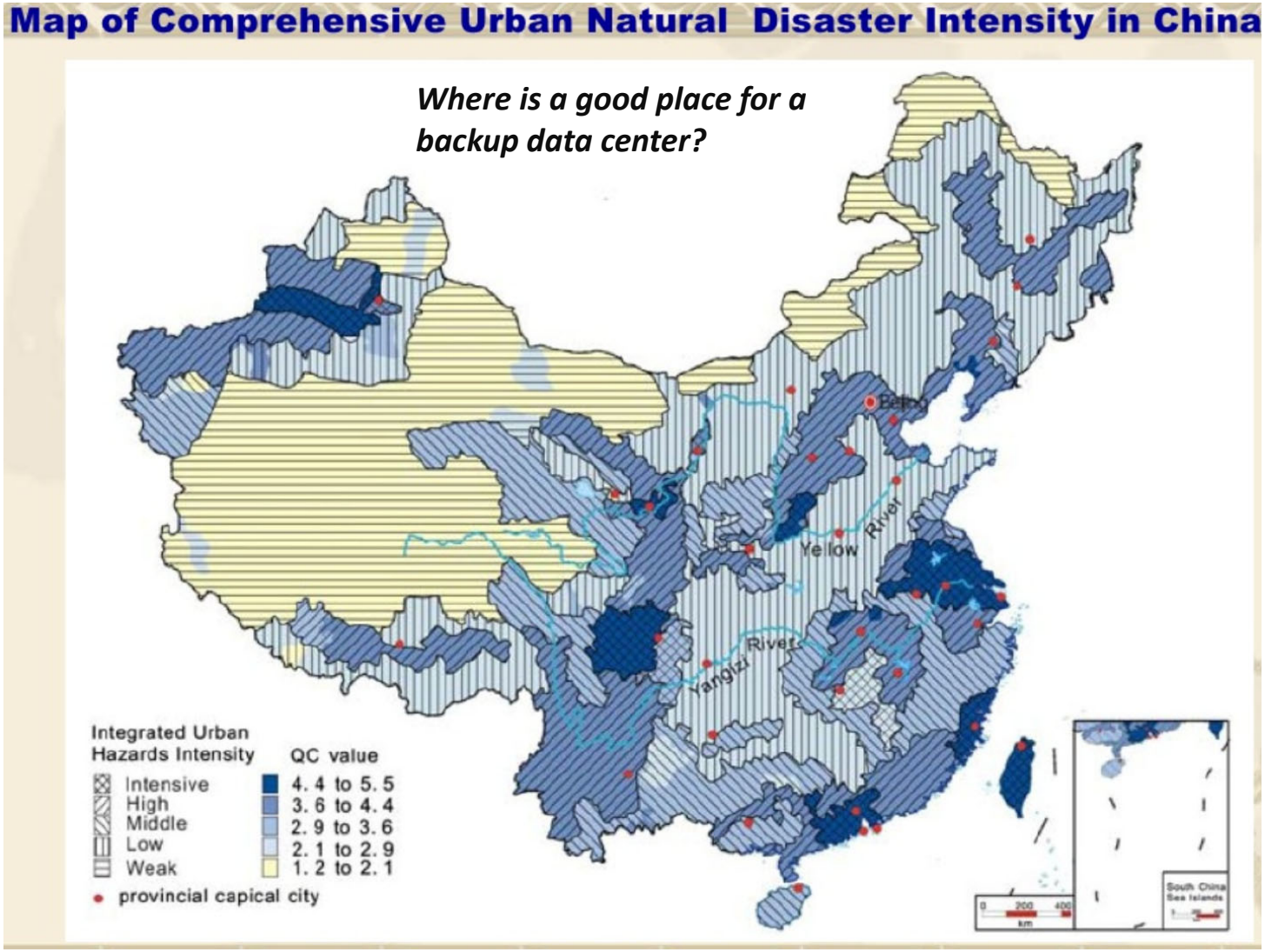
Washington, D.C. 1991

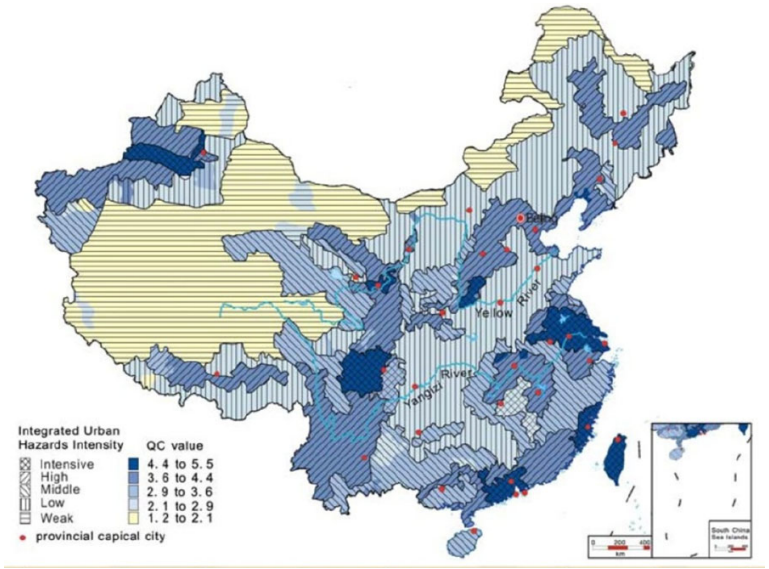
Figure 6-1 EXAMPLES OF NATURAL PHENOMENA WHICH MAY BE HAZARDOUS

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 lateral blasts	Erosion	Submarine slides	Liquefaction	Urban conflagration
Tornadoes	Pyroclastic flows	River floods	Subsidence	Seiches	
Tropical storms	Tephra (ashes, cinders, lapilli)	Storm surges		Tsunamis	

CHAPTER 6 - MULTIPLE HAZARD MAPPING

Map of Comprehensive Urban Natural Disaster Intensity in China





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

Contingency Planning Controls

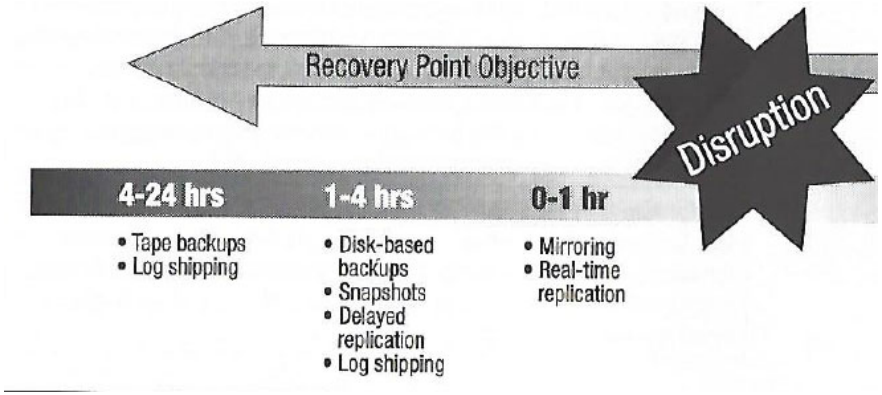
CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information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

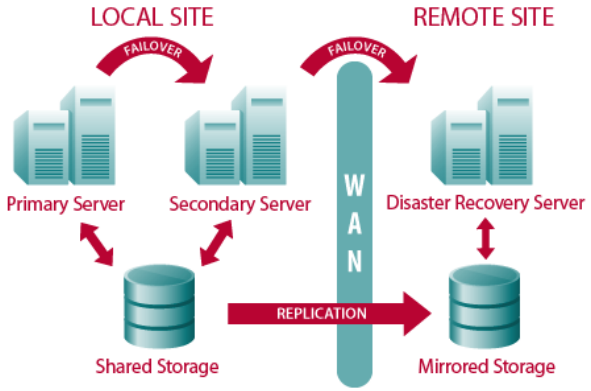
NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations"

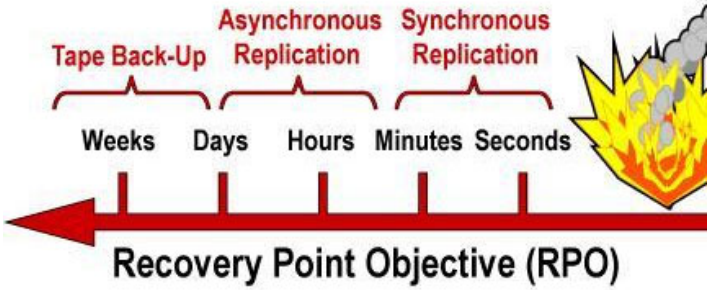
CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY 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**



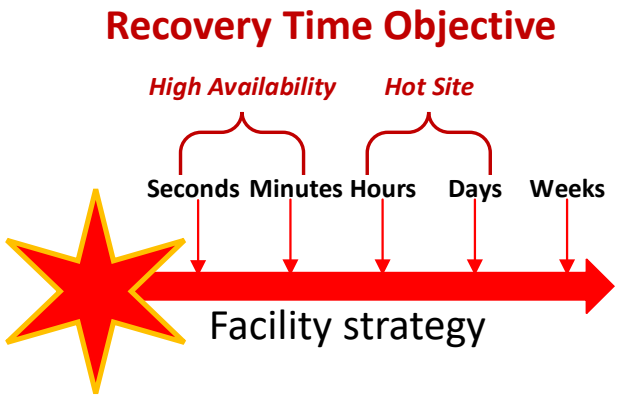


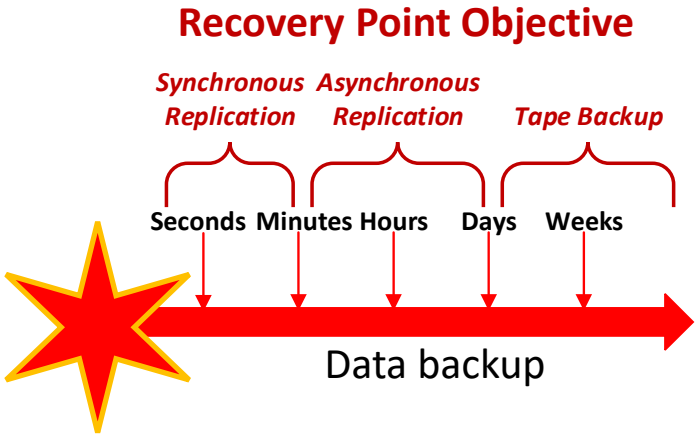


Recovery Options: Location & Backup

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]

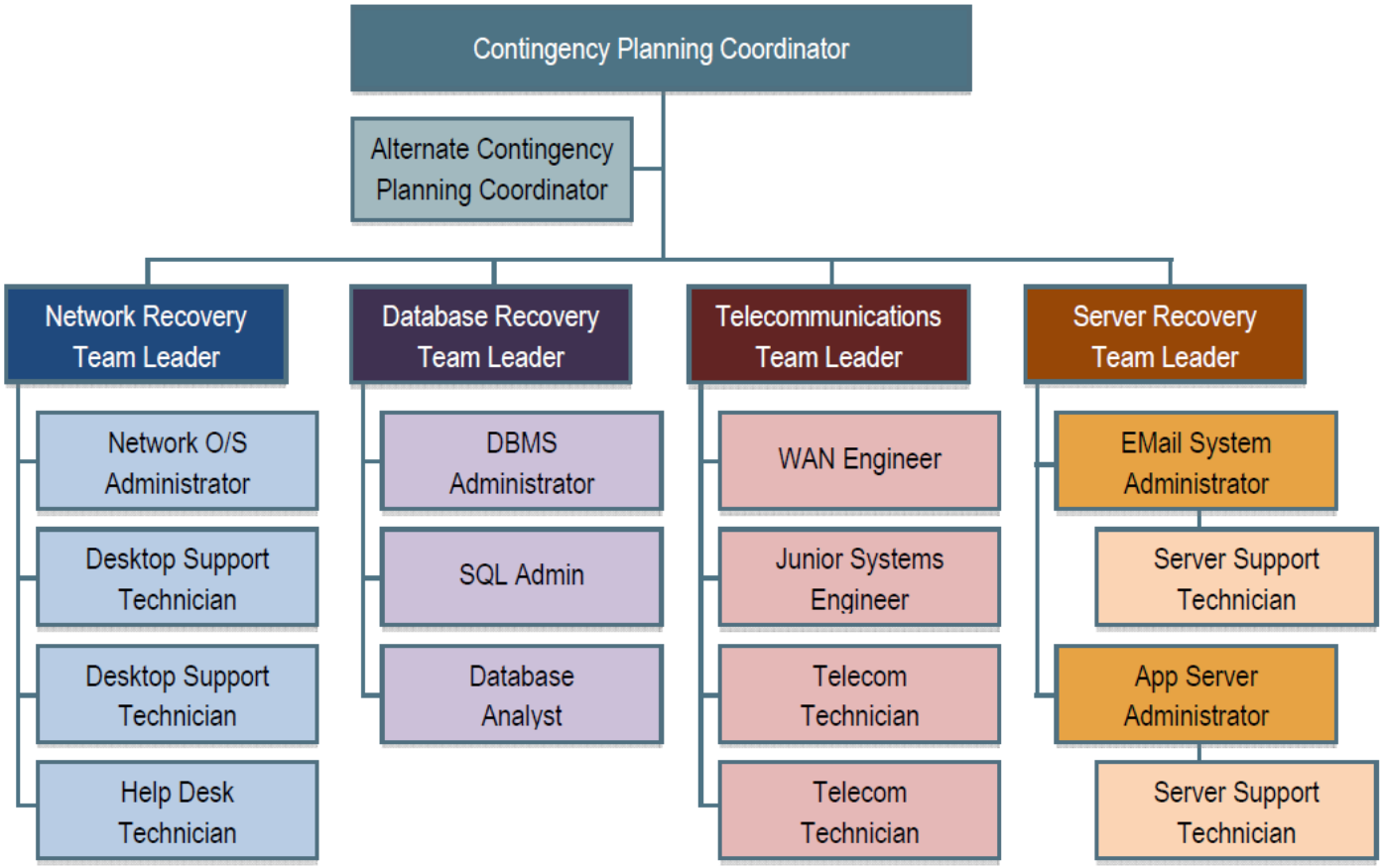




Considerations - Budget

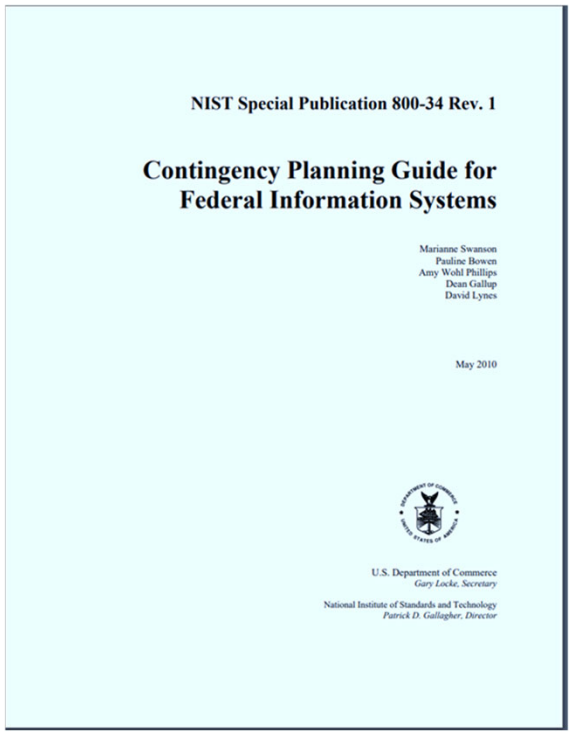
Contingency Resources	Strategies	Vendor Costs	Hardware Costs	Software Costs	Travel / Shipping Costs	Labor / Contractor Costs	Testing Costs	Supply Costs
Alternate Site	Cold Site							
	Warm Site							
	Hot Site							
Offsite Storage	Commercial							
	Internal							
Equipment Replace-ment	SLA				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

Response Roles and Responsibilities example



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

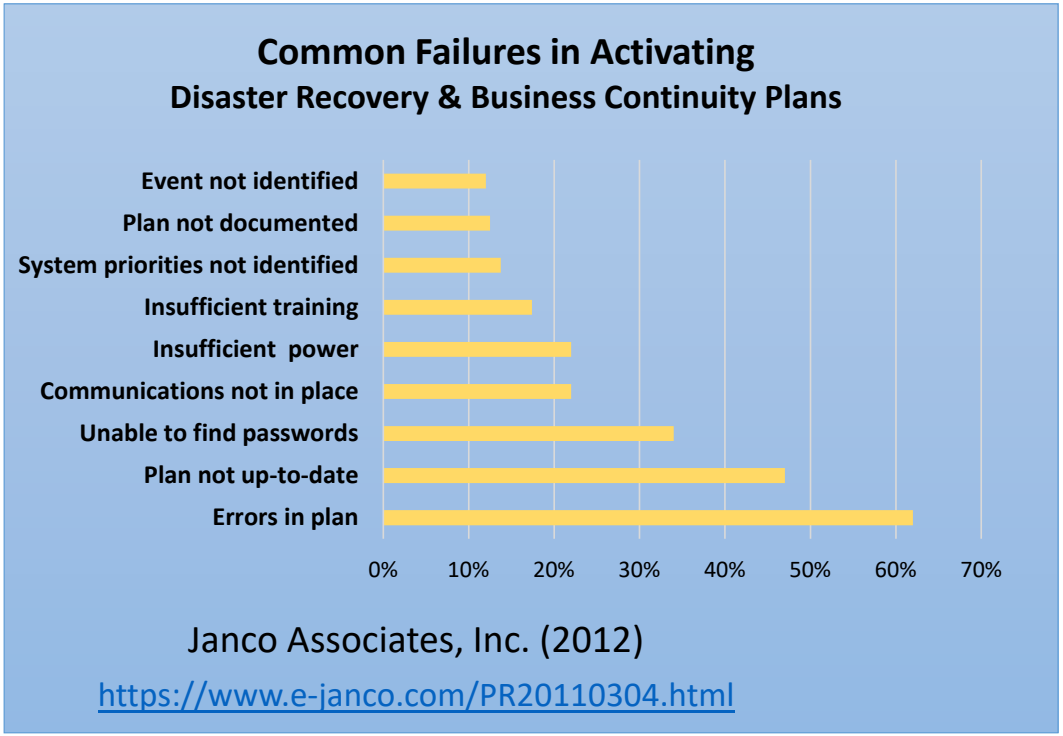
TABLE OF CONTENTS

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*



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

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.

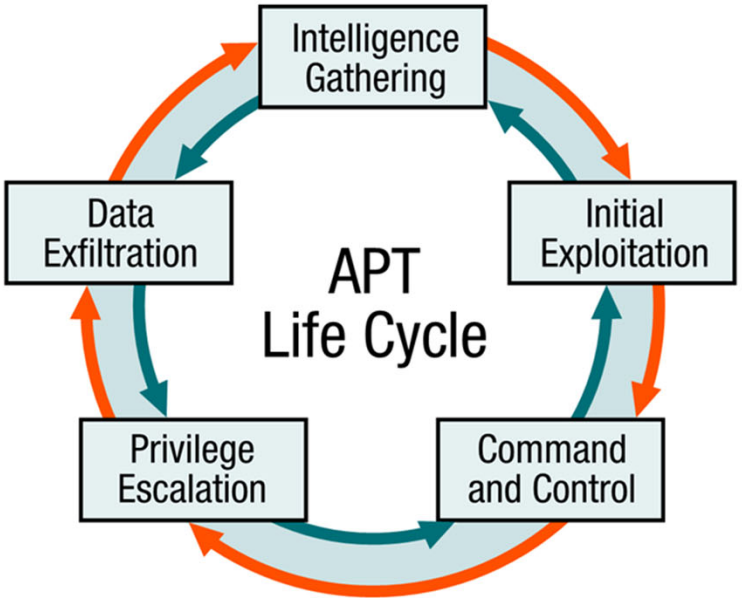
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization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

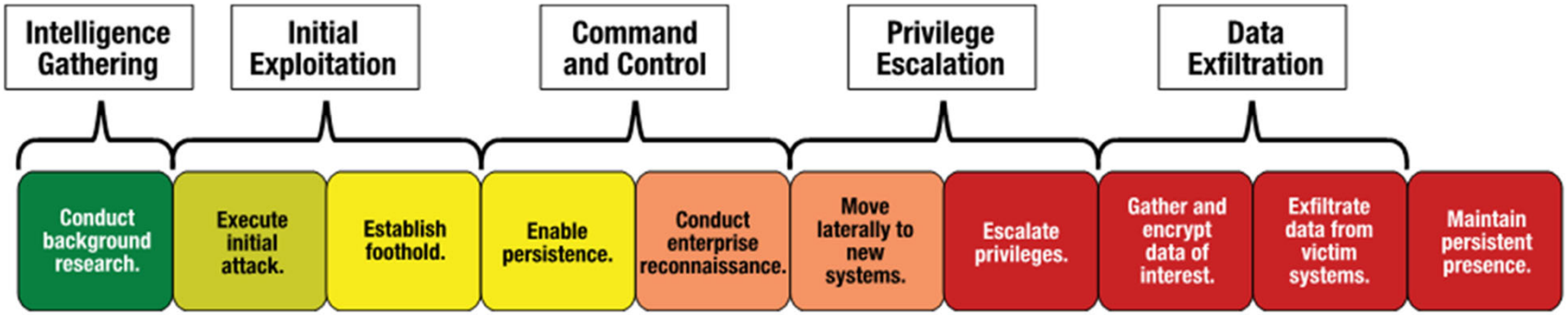
Computer security incident response

Is necessary because…

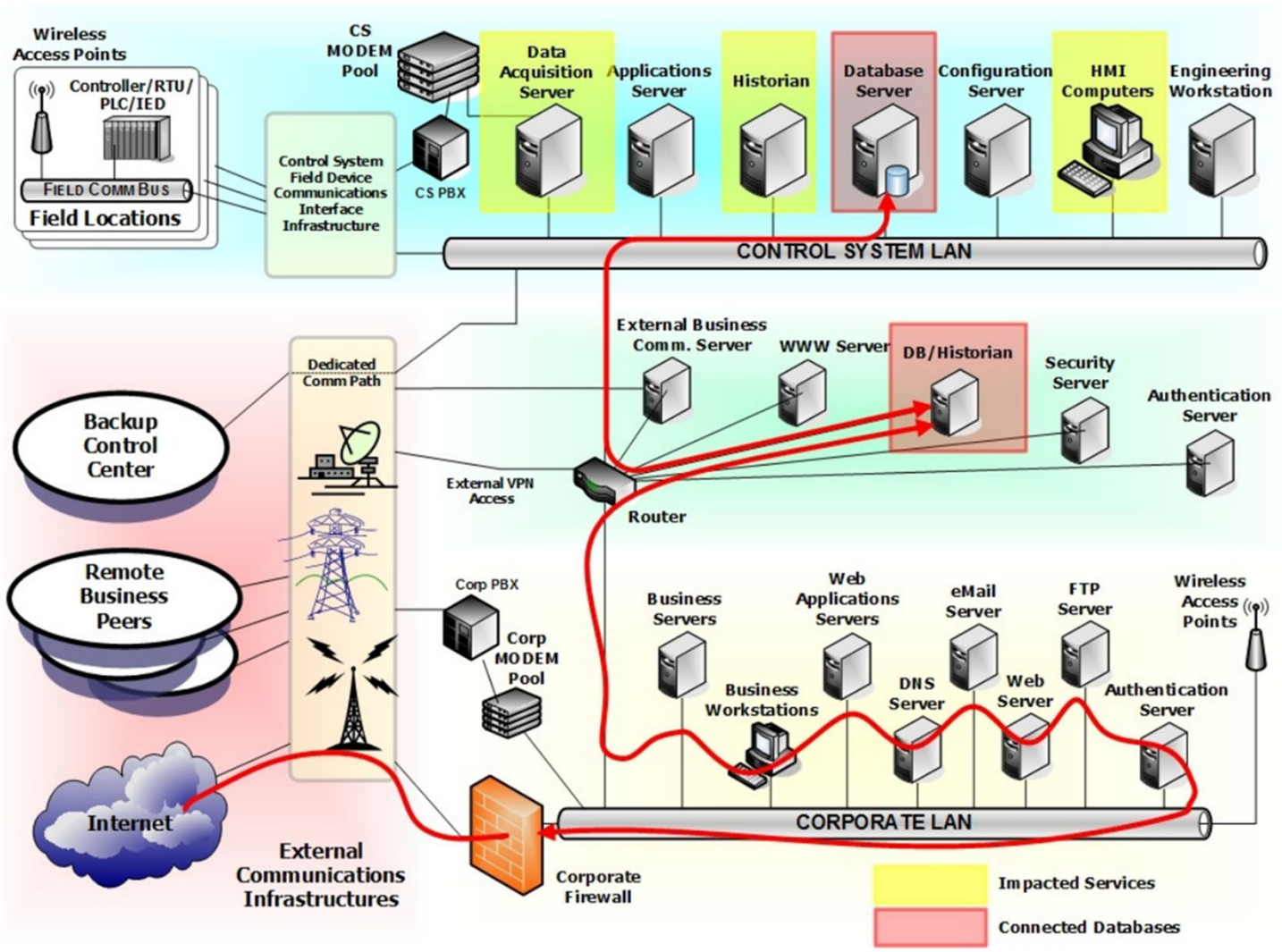
- Computer security controls, systems, and processes are not perfect
- Protections designed to protect information and information systems eventually fail
- Security breaches are inevitable

Anatomy of Advanced Persistent Threats





Example of Network Intrusion



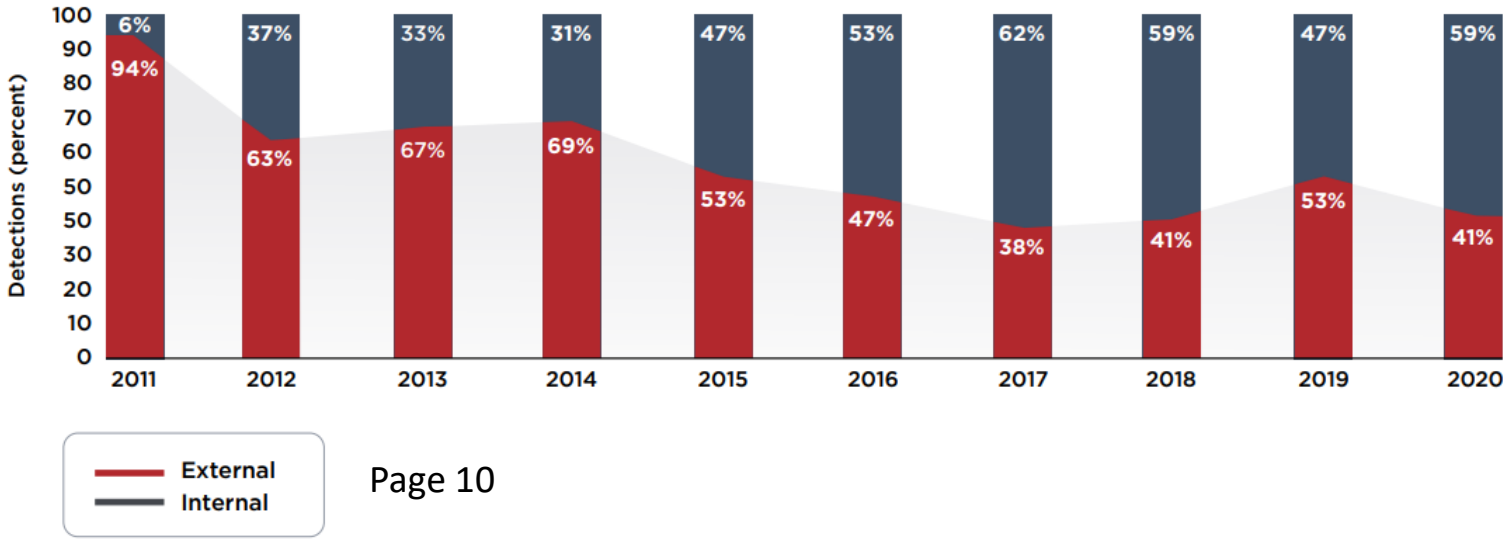
Industry Targeting

"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."

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

FIREEYE | MANDIANT

Median Dwell Time

416 ➤ **24**

DAYS IN 2011 **DAYS IN 2020**

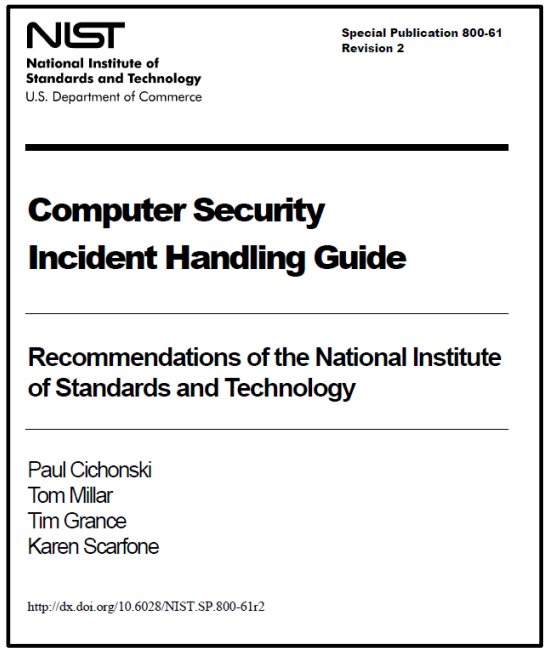
"Dwell time is calculated as the number of days an attacker is present in a victim environment before they are detected."

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

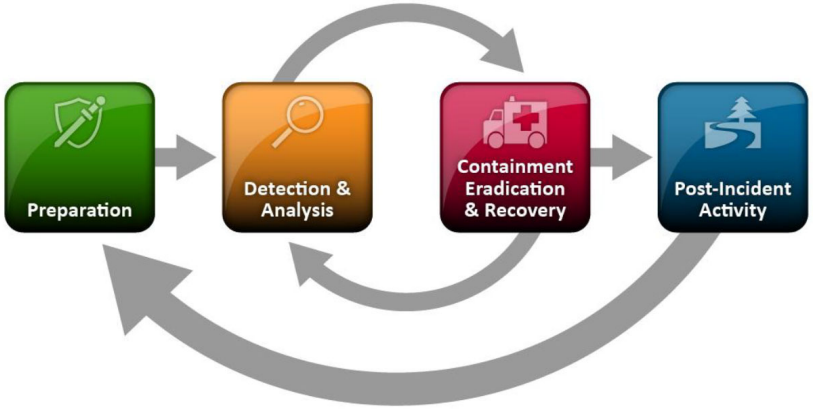
Handling an Incident - Preparation

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



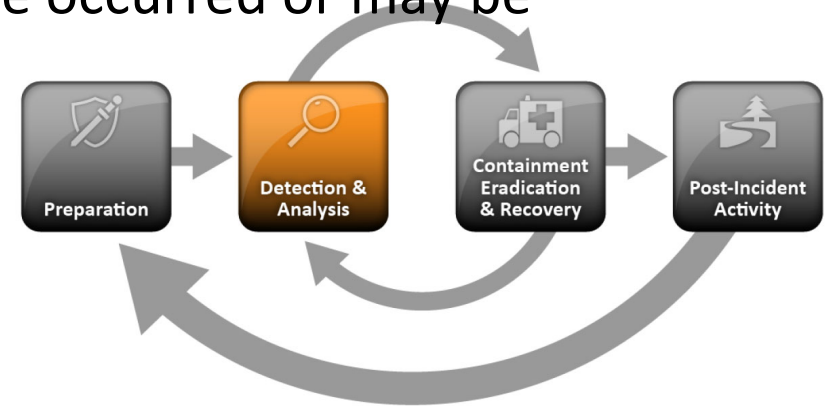
Handling an Incident – Detection and Analysis

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

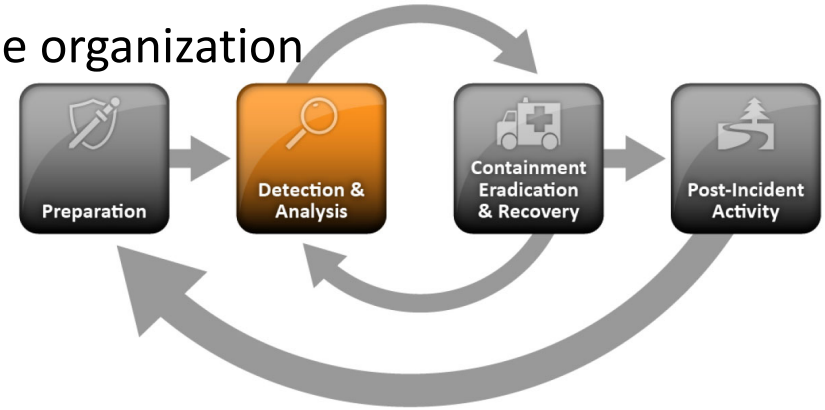


Handling an Incident – Detection and Analysis

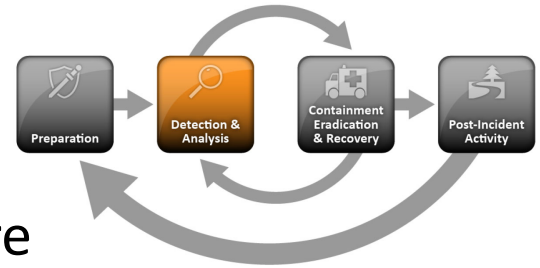
Precursors – While rare, if precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.

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

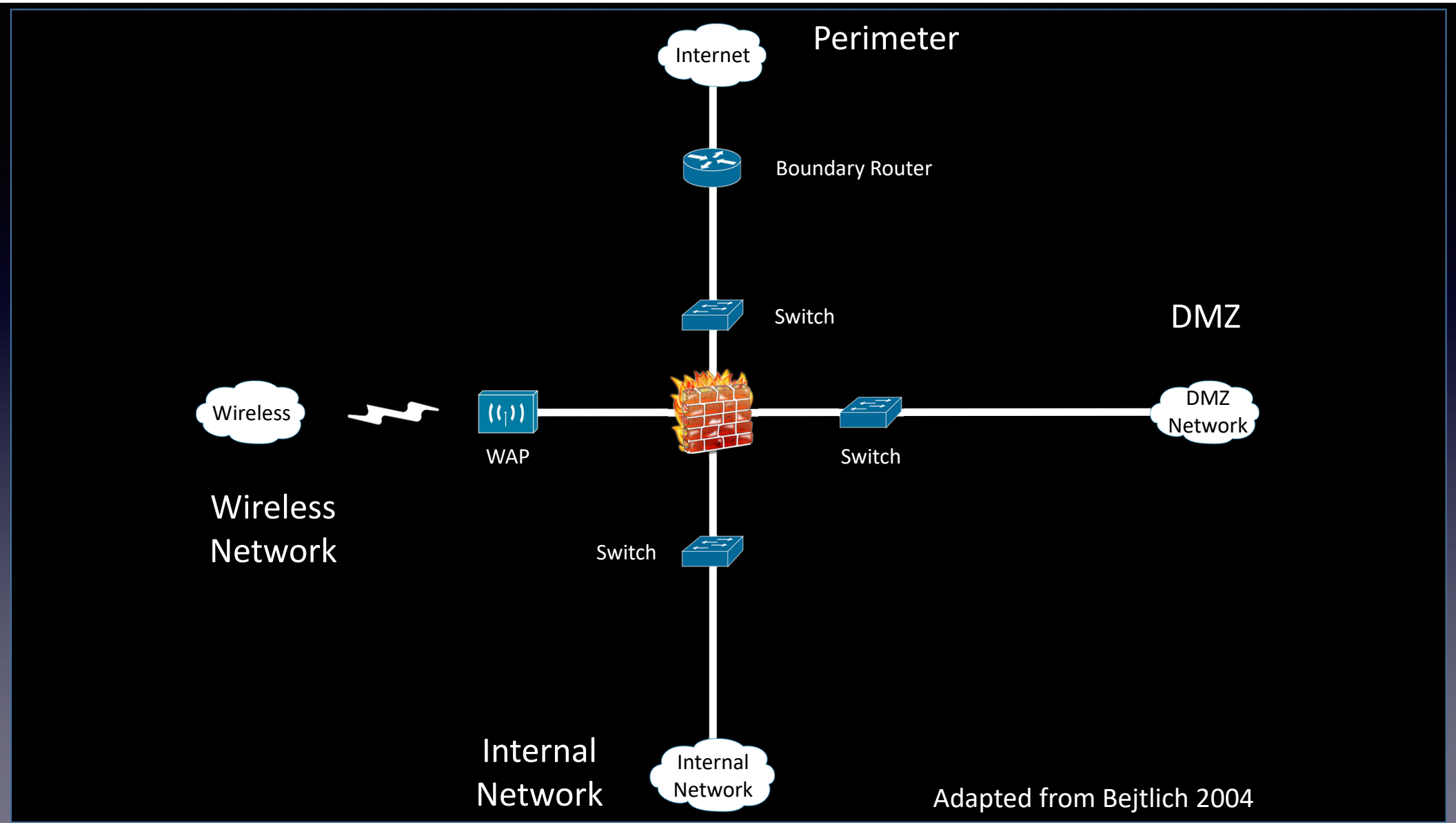


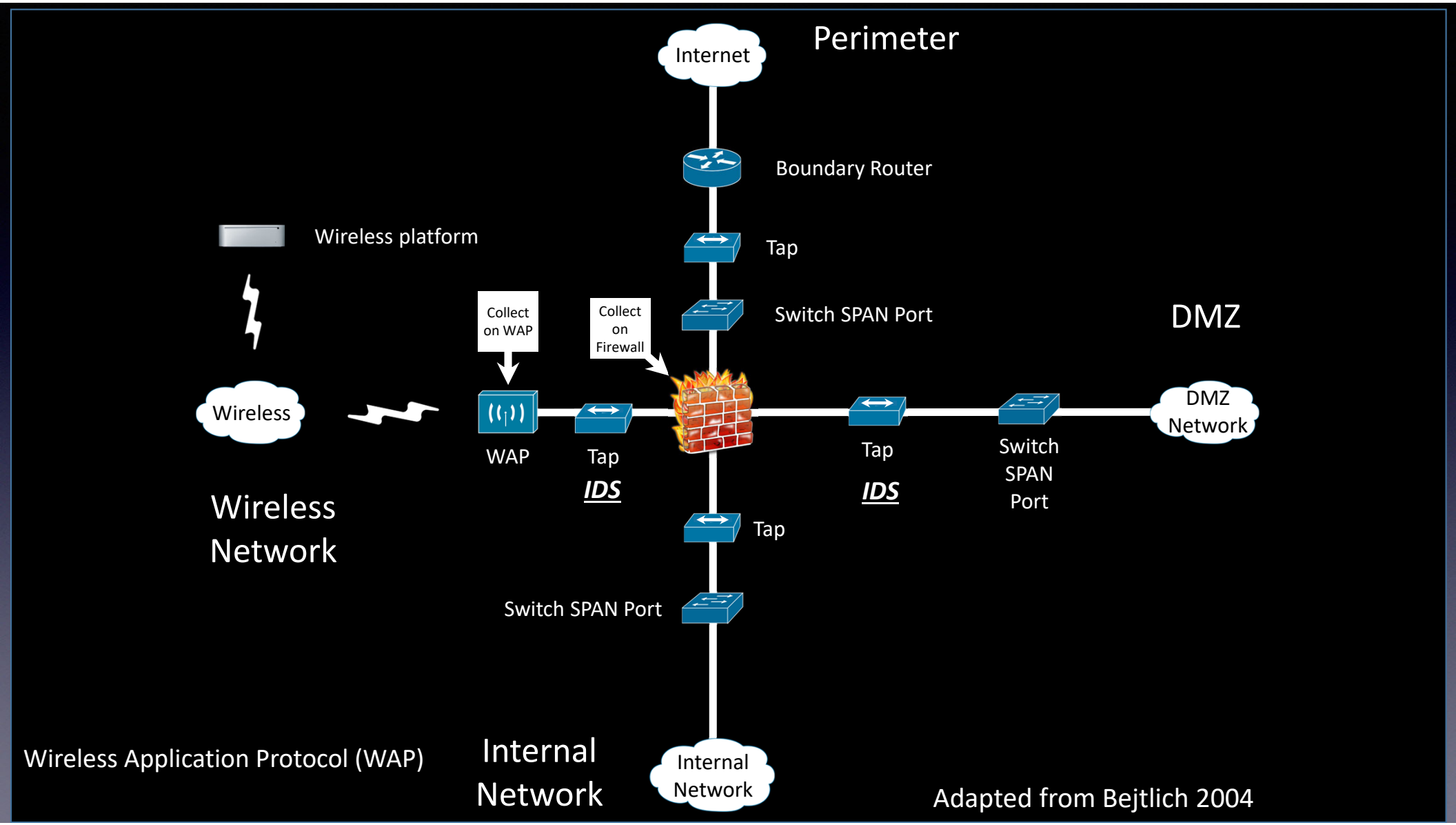
Detection and Analysis



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


Perimeter
Internet
Boundary Router
Switch
DMZ
Wireless
WAP
Switch
DMZ Network
Wireless Network
Switch
Internal Network
Internal Network
Adapted from Bejtlich 2004

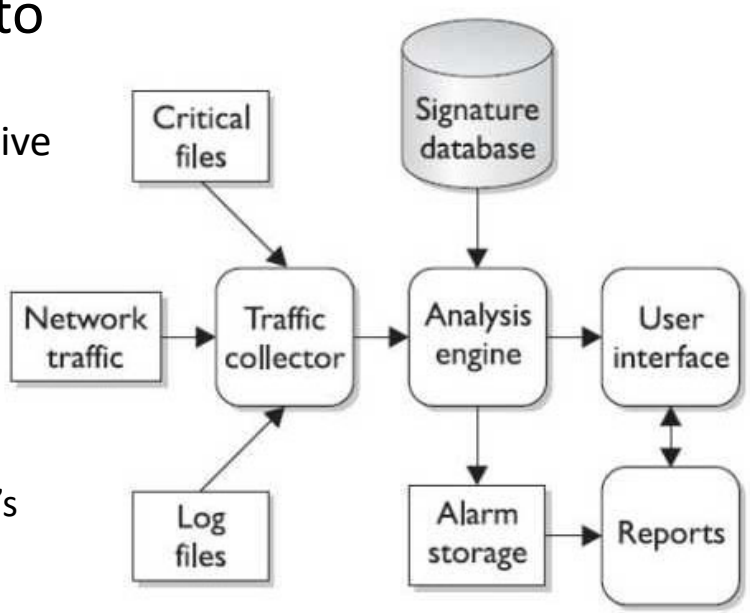

Perimeter
Internet
Boundary Router
Wireless platform
Tap
Switch SPAN Port
DMZ
Collect on WAP
Collect on Firewall
Wireless
WAP
Tap
IDS
Tap
IDS
Switch SPAN Port
DMZ Network
Wireless Network
Tap
Switch SPAN Port
Wireless Application Protocol (WAP)
Internal Network
Internal Network
Adapted from Bejtlich 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



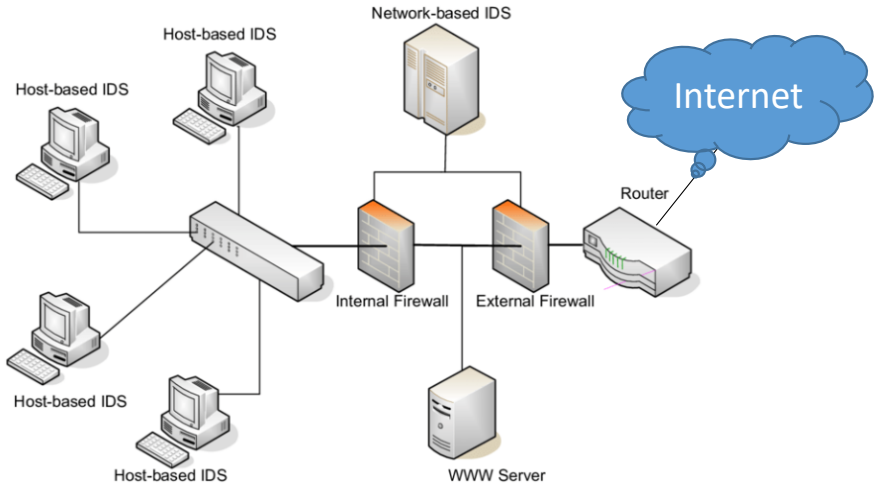
Intrusion Detection Systems (IDSs)

Two main types of IDS

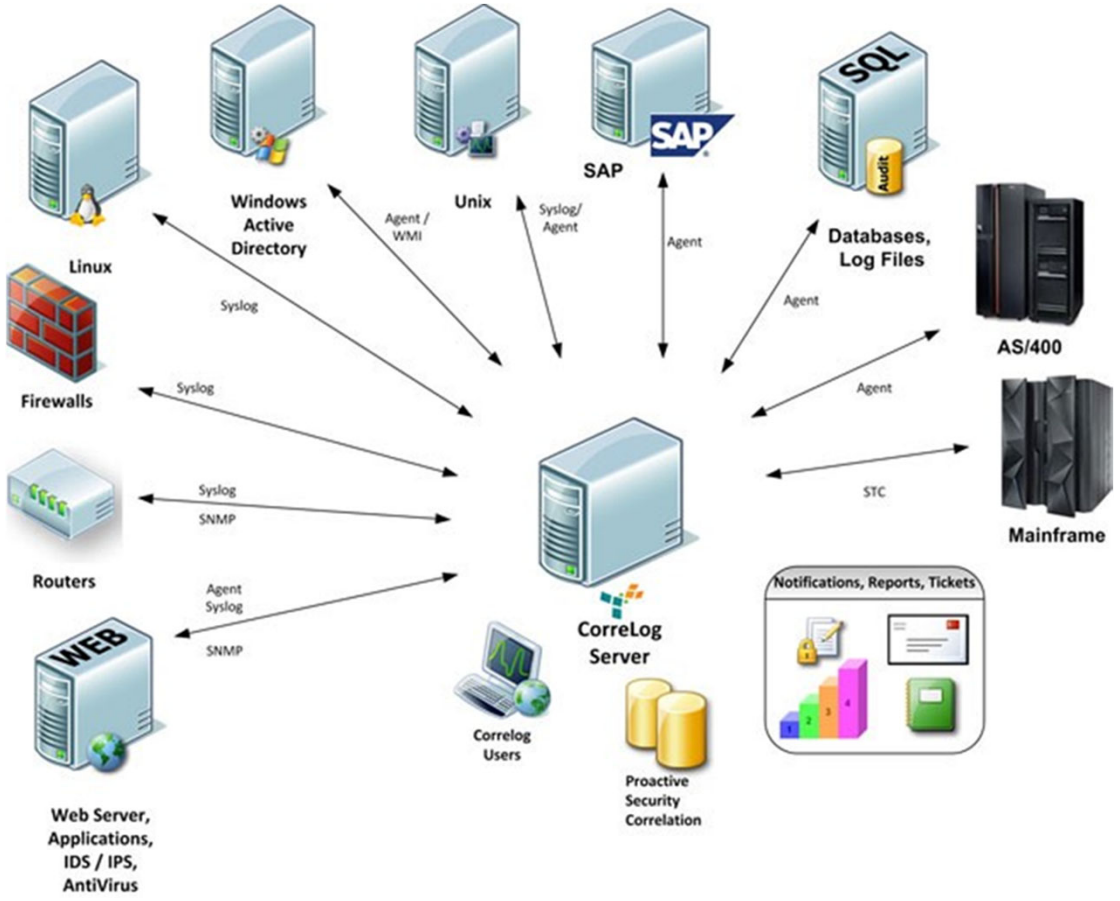
1. **Host-based** for analyzing activity within a particular computer system
2. **Network-based** for monitoring network communications

IDS can be configured to:

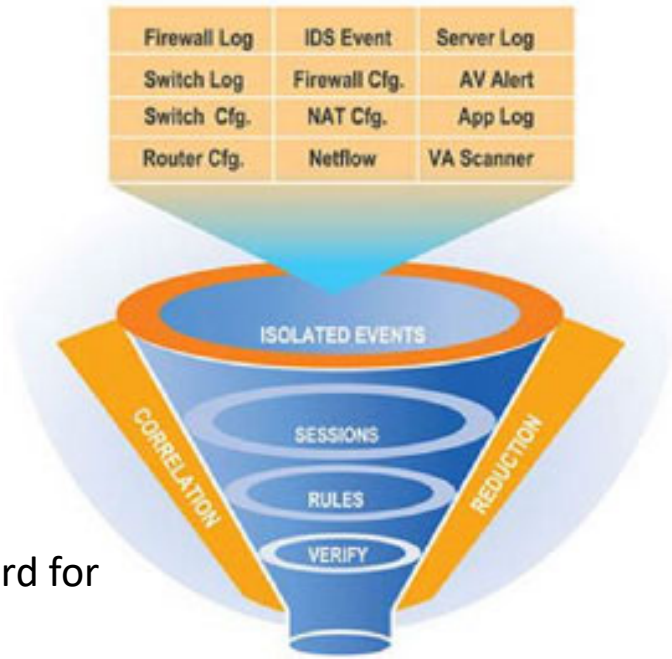
- Watch for attacks
- Alert administrator as attacks happen
- Expose a hacker & her/his techniques
- Work with firewalls to terminate a connection



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



SIEM's help with Data Analysis and Correlation

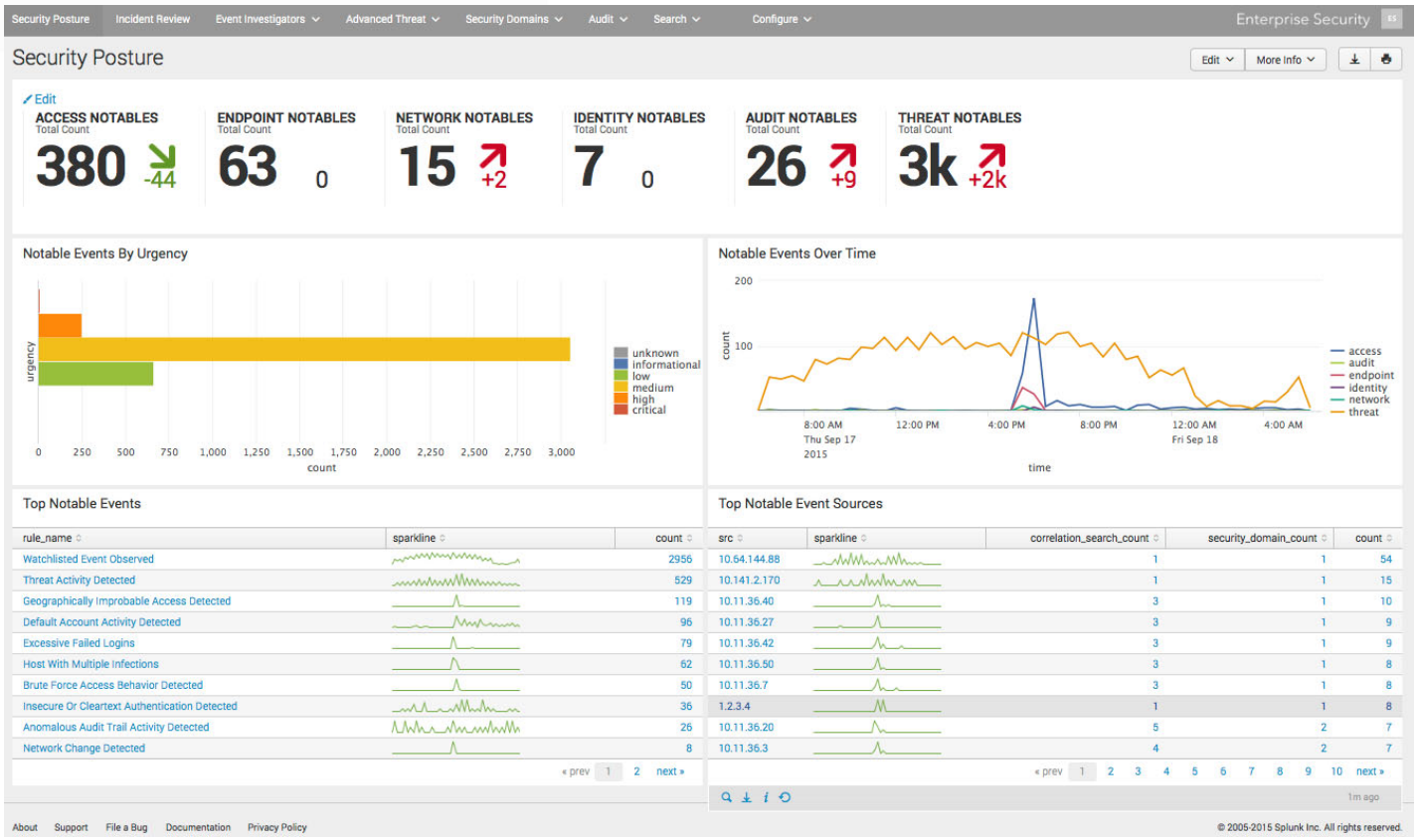


- Bring raw data events into one database
- Database software is programmed to look for "Notable events" or correlations
- Correlations will take seemingly isolated events and bring them forward for review/action:
  - **Windows Log:** Employee denied windows login (unknown user account)
  - **Identity Management System:** notes the user account was deleted because employee was terminated last month.
- Security Domains: Access, Endpoints, Networks, Identity

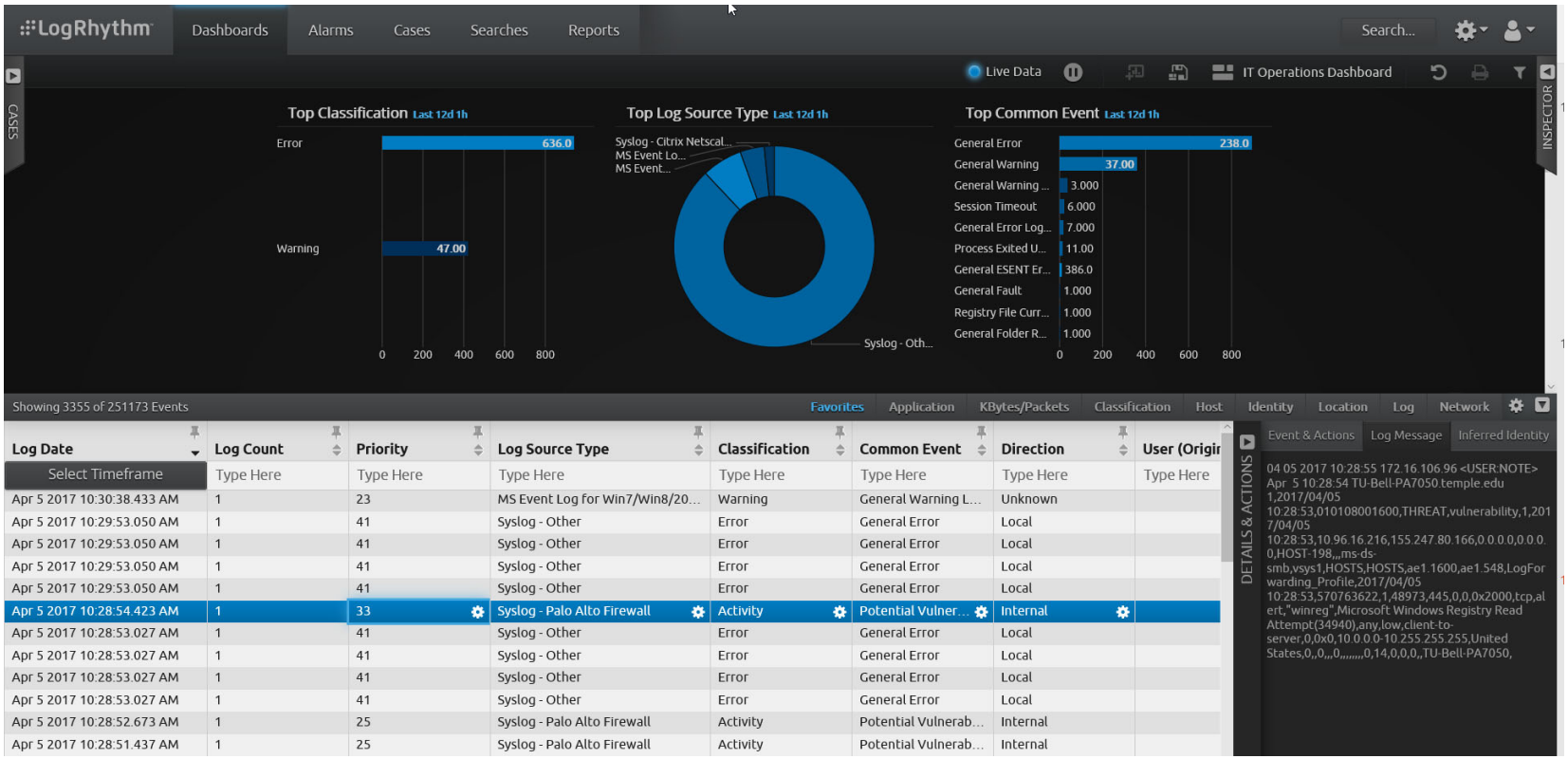
SIEM

- ***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.

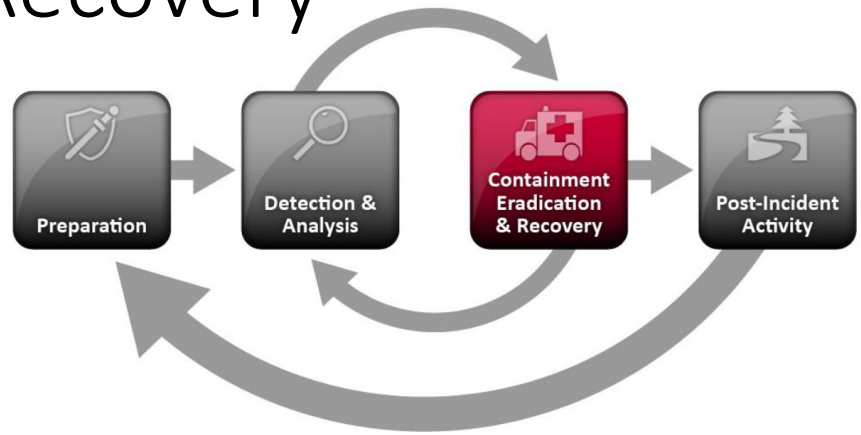
splunk>


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Security Posture
Edit
More Info
Edit
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
urgency
unknown
informational
low
medium
high
critical
0
250
500
750
1,000
1,250
1,500
1,750
2,000
2,250
2,500
2,750
3,000
count
Notable Events Over Time
200
100
count
access
audit
endpoint
identity
network
threat
8:00 AM
Thu Sep 17
2015
12:00 PM
4:00 PM
8:00 PM
12:00 AM
Fri Sep 18
4:00 AM
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
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.

LogRhythm™


LogRhythm
Dashboards
Alarms
Cases
Searches
Reports
Search...
Live Data
IT Operations Dashboard
CASES
INSPECTOR
Top Classification Last 12d 1h
Error
636.0
Warning
47.00
0
200
400
600
800
Top Log Source Type Last 12d 1h
Syslog - Citrix Netscal...
MS Event Lo...
MS Event...
Syslog - Oth...
Top Common Event Last 12d 1h
General Error
238.0
General Warning
37.00
General Warning ...
3.000
Session Timeout
6.000
General Error Log...
7.000
Process Exited U...
11.00
General ESENT Er...
386.0
General Fault
1.000
Registry File Curr...
1.000
General Folder R...
1.000
0
200
400
600
800
Showing 3355 of 251173 Events
Favorites
Application
KBytes/Packets
Classification
Host
Identity
Location
Log
Network
Log Date
Log Count
Priority
Log Source Type
Classification
Common Event
Direction
User (Origi
Select Timeframe
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
DETAILS & ACTIONS
Event & Actions
Log Message
Inferred Identity
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,1,2017/04/05 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,LogForwarding_Profile,2017/04/05 10:28:53,570763622,1,48973,445,0,0,0x2000,tcp,alert,"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,

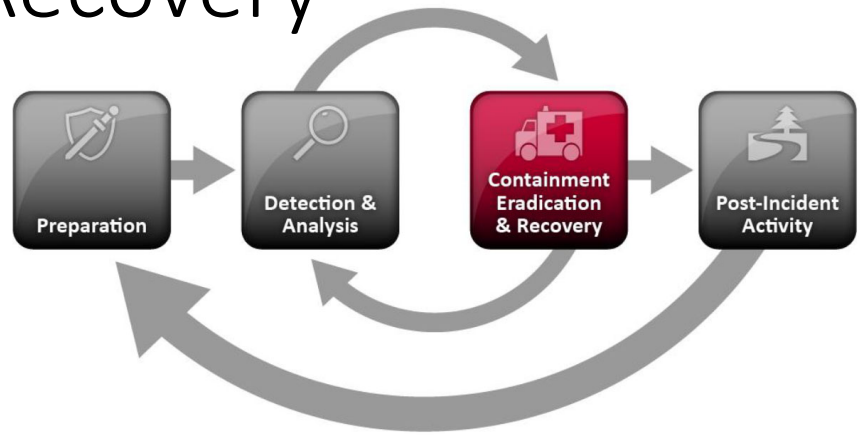
Containment, Eradication, and Recovery



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

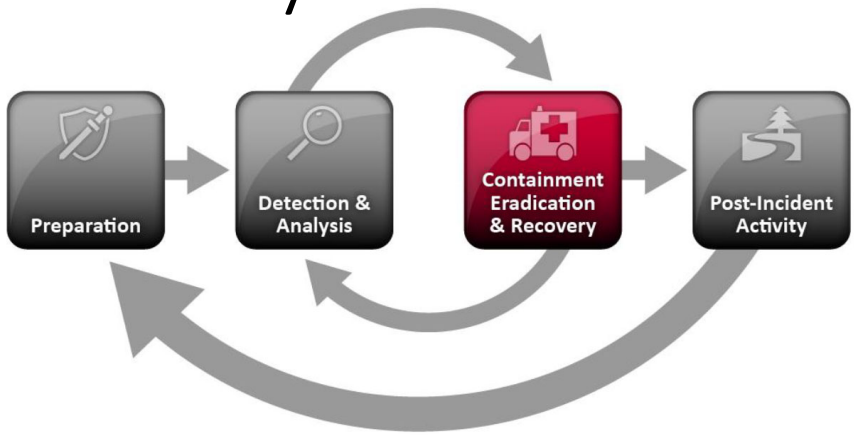


Eradication - After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as:

- 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:

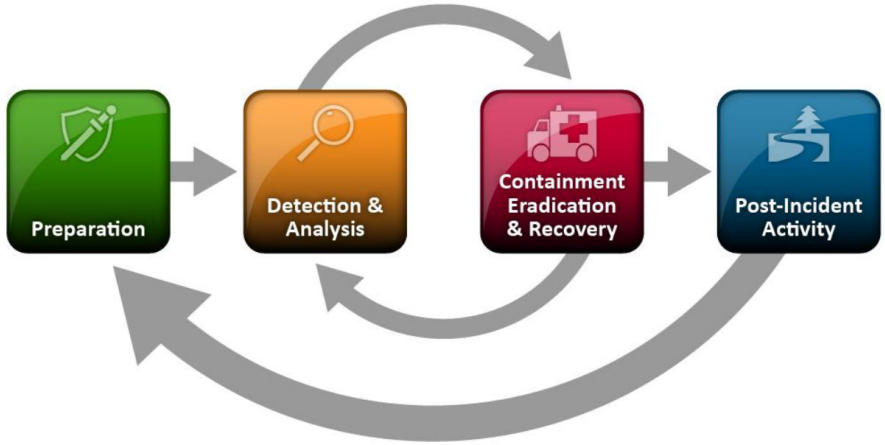
- Restoring systems from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security (e.g. firewall rules, boundary router access control lists, …)

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