Understanding the Benefits of Risk Management and Information Security

Jobe Beckhom

Brief Overview about me

- Risk Management
- Assets
- Information Security
- Threats
- Vulnerability Assessment
- Network Diagram
- Risk Treatment Strategies
- Risk Management Frameworks
- Incident Response (IR)
- What is an incident
- IR Plan\IR Team
- NIST Life Cycle
- Ways to reduce cybersecurity risks and protect assets
- Ways to prevent and detect an incident
- WIN Audit
- Why it is important to collect data to detect an incident
- Key Takeaways
- Questions

What is Risk Management

- What are risks?
- Program of planning for and managing risks to information assets.

What are Assets

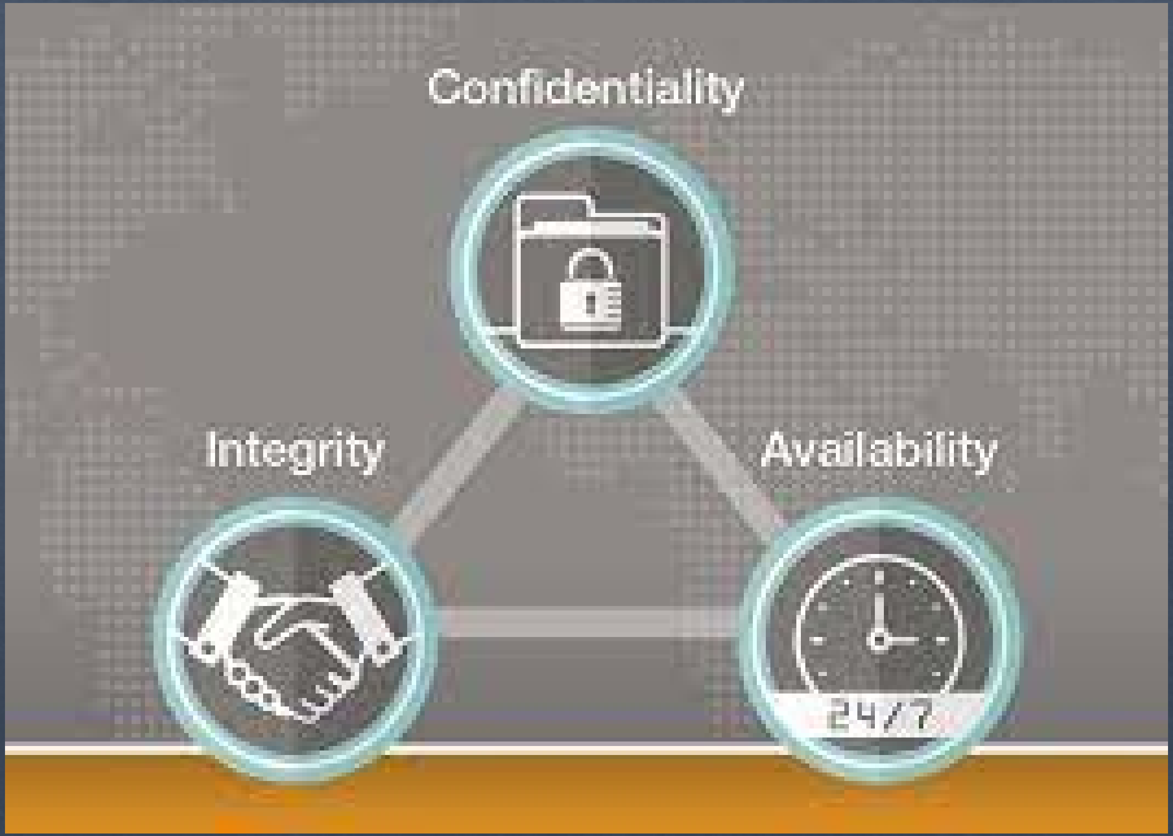
- Organizational resource that is being protected.

Organize your Assets

- Classify your assets
- Prioritize your assets

What is Information Security (InfoSec)

- The protection of the confidentiality, integrity, and availability of information assets.



Three simple questions regarding Organizational Assets

- Where are our assets located?
- Who has access to those assets?
- How are we securing those assets?

Threat Assessment

- An evaluation of threats to organizational assets.

The twelve categories of Threats

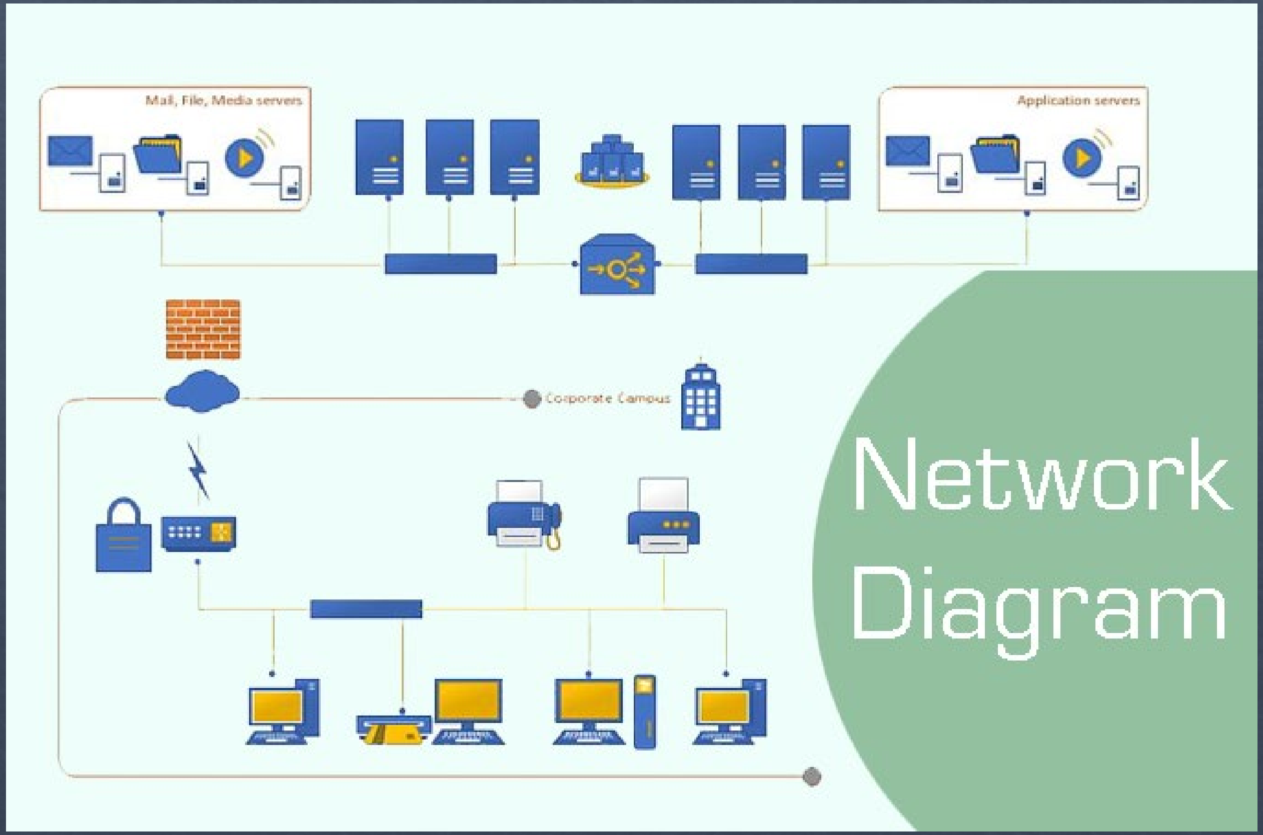
Category of Threats
Compromise of intellectual property
Deviations in quality of service
Espionage or trespass
Forces of nature
Human error or failure
Information extortion
Sabotage or vandalism
Software attacks
Technical hardware failures or errors
Technical software failures or errors
Technological obsolescence
Theft

Vulnerability Assessment

- A review of security weaknesses in an information system.

Network Diagram

- A visual representation of a computer network.



Risk Questions every Organization should be asking

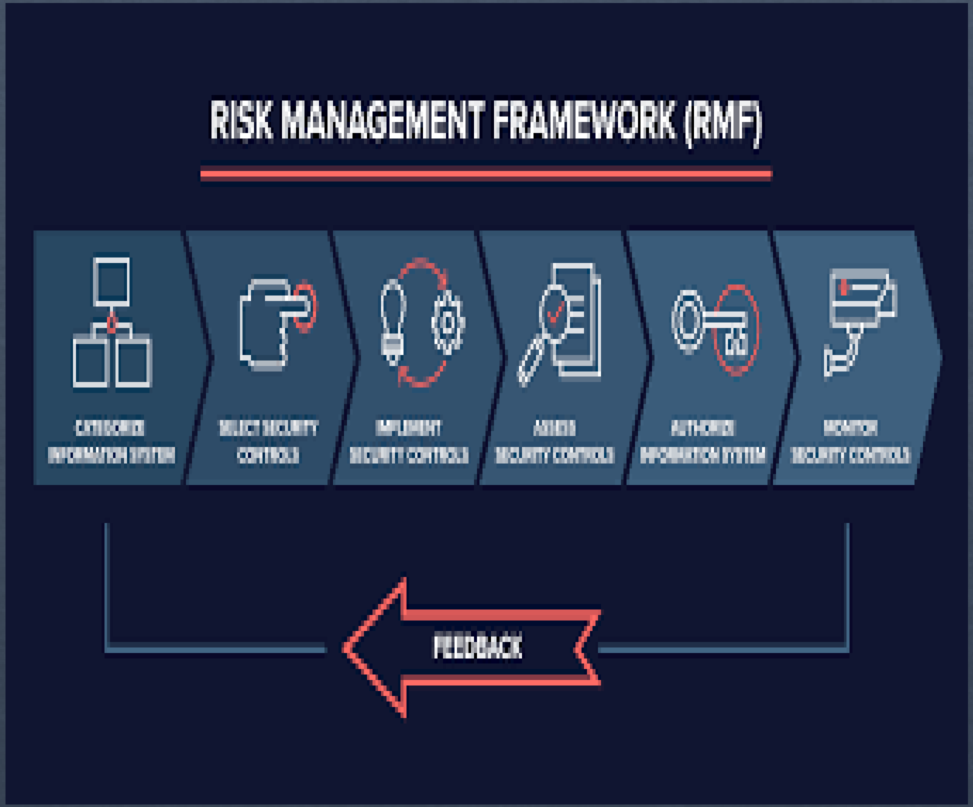
- Where and what are our risks (risk identification)?
- How severe is our current level of risk (risk analysis)
- Is our current level of risk acceptable (risk evaluation)
- What do we need to do our risk to an acceptable level (risk treatment)

Risk treatment strategies

- Defense
- Transference
- Mitigate
- Acceptance
- Termination

Risk Management Frameworks

- What is the National Institute of Standards and Technology (NIST)
- What is NIST 800-39


RISK MANAGEMENT FRAMEWORK (RMF)
CATEGORIZE INFORMATION SYSTEM
SELECT SECURITY CONTROLS
IMPLEMENT SECURITY CONTROLS
ASSESS SECURITY CONTROLS
AUTHORIZE INFORMATION SYSTEM
MONITOR SECURITY CONTROLS
FEEDBACK

Knowledge

- Know yourself
- Know your enemy

What is Incident Response (IR)

- Planning, preparation, detecting, reacting and recovering from an indecent.

What is an Incident

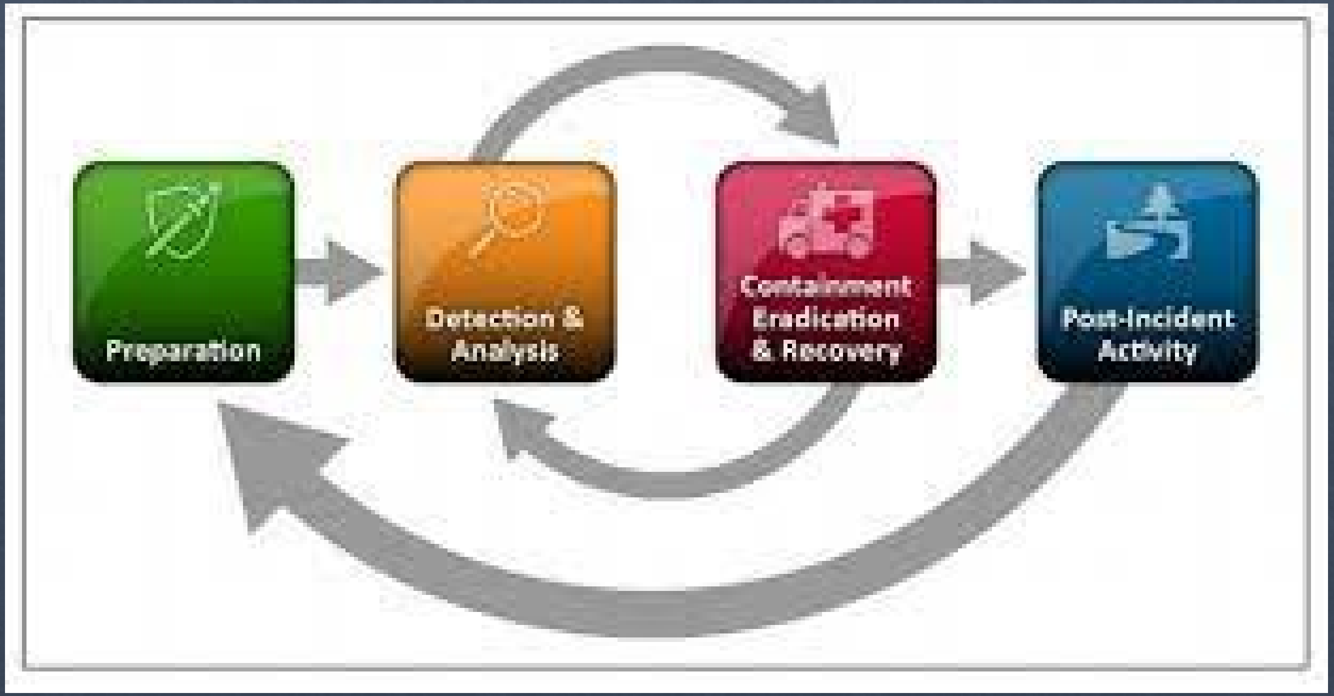
- Event that violates the security of an organization and represents a potential risk to confidentiality, integrity, or availability of its assets.

What is an Incident Response (IR)Plan and an Incident Response (IR) team

- Plan that shows the organization’s intended efforts in the event of an incident.
- IR team is a group of IT professionals in charge of preparing for and reacting to an organizational emergency

NIST Incident Response Life Cycle

- Prepare
- Detect & Analyze
- Contain, eradicate and recover
- Post-Incident Activity



Ways to reduce cybersecurity risks and protect assets in your organization

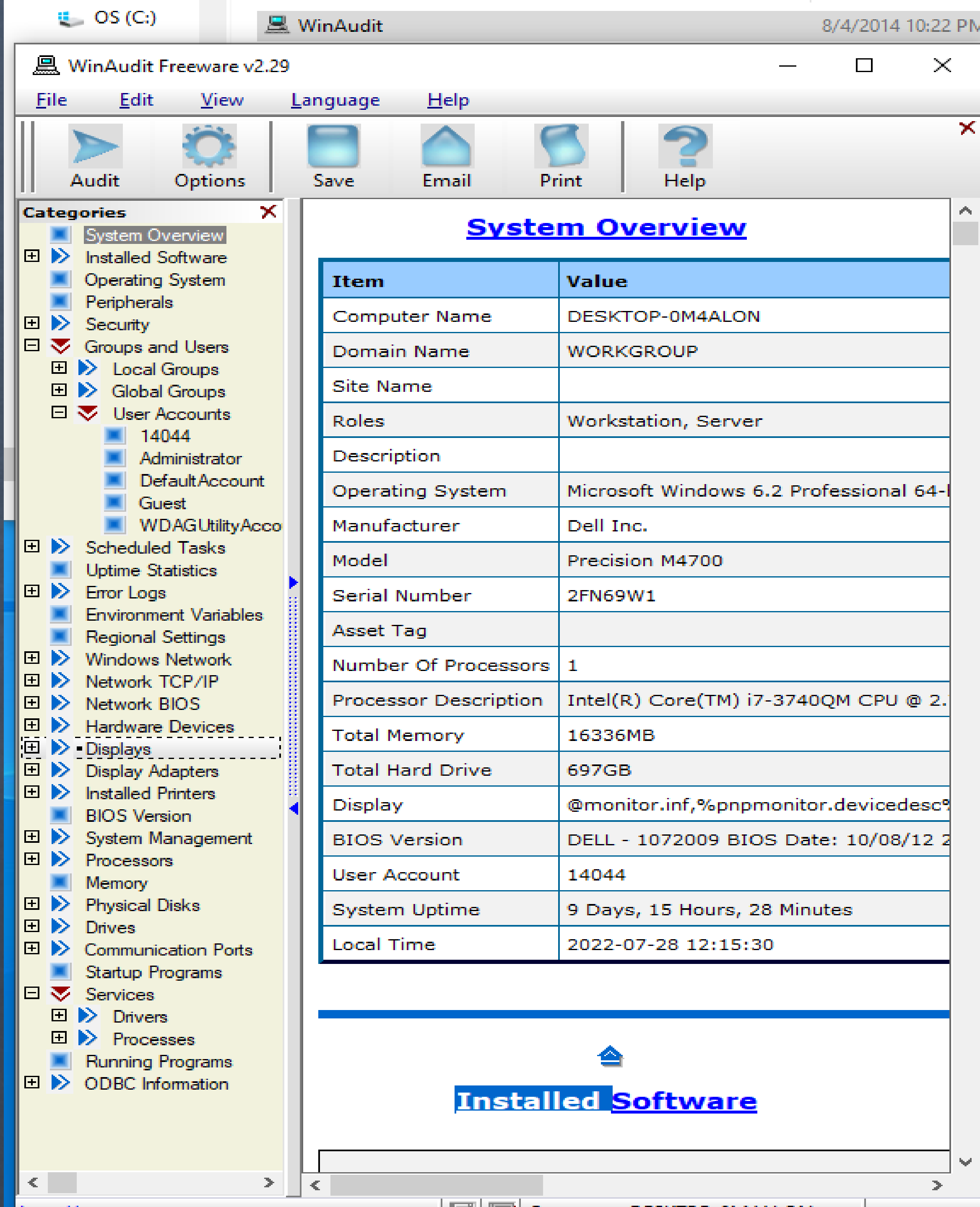
Ways to reduce cybersecurity Risks and protect assets
Implement backups and understand your retention policy
Multi-Factor Authentication (MFA)
Anti-Virus
Encrypt in rest and in transit
Conduct Risk Management Training
Update systems and install patches
Use strong password and have it as a policy
Have good physical security
Monitor third party vendors
Install Firewalls

Ways to prevent and detect an incident (Collect Data)

Data Category
Network Data
System Data
Process Data
Files and Directories
Users
Log Files
Vulnerabilities

WinAudit

- WinAudit: Inventory GUI for Windows computers.



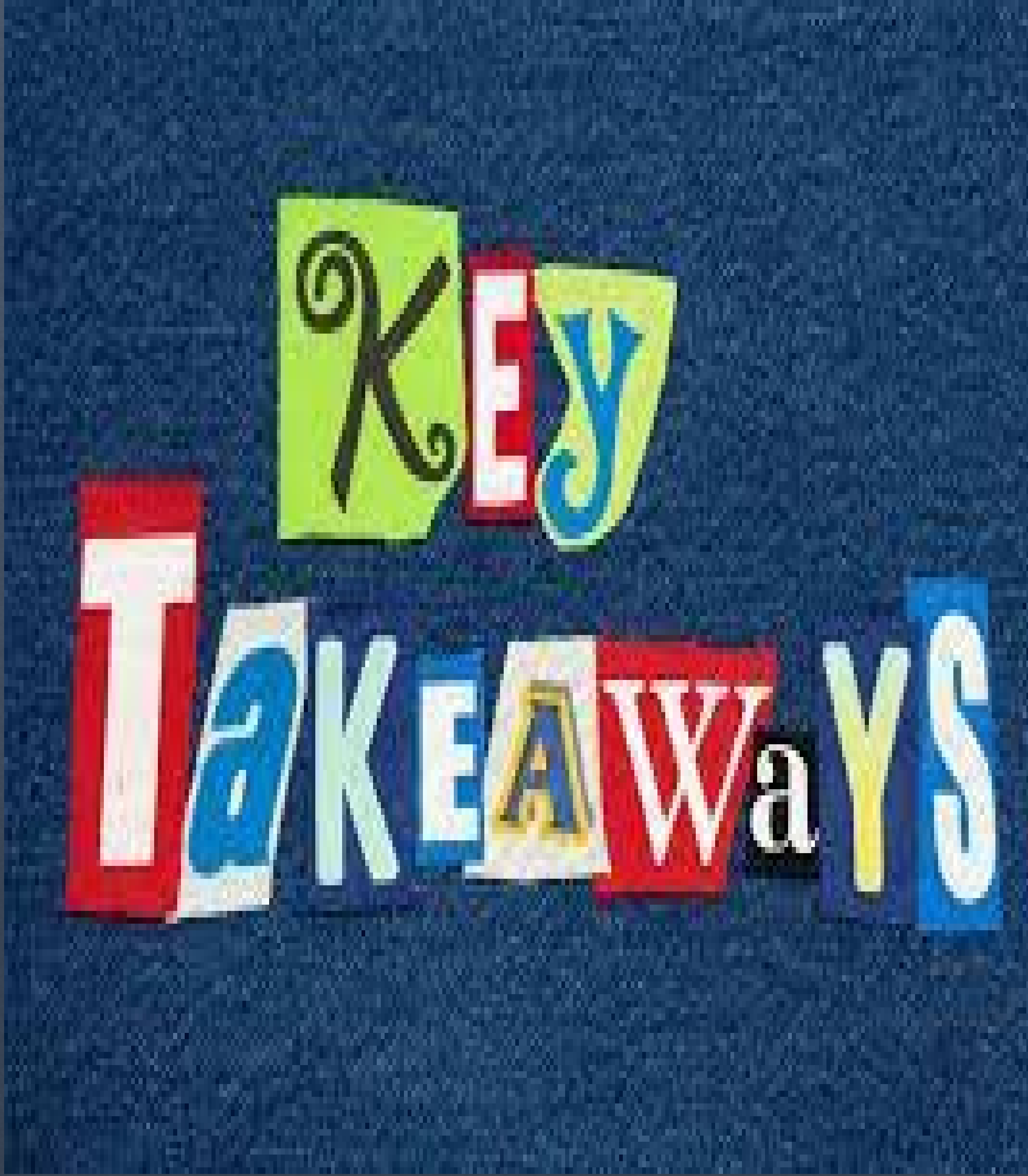
System Overview

Item	Value
Computer Name	DESKTOP-0M4ALON
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server
Description	
Operating System	Microsoft Windows 6.2 Professional 64-
Manufacturer	Dell Inc.
Model	Precision M4700
Serial Number	2FN69W1
Asset Tag	
Number Of Processors	1
Processor Description	Intel(R) Core(TM) i7-3740QM CPU @ 2.
Total Memory	16336MB
Total Hard Drive	697GB
Display	@monitor.inf,%pnpmonitor.devicedesc%
BIOS Version	DELL - 1072009 BIOS Date: 10/08/12 2
User Account	14044
System Uptime	9 Days, 15 Hours, 28 Minutes
Local Time	2022-07-28 12:15:30

Why is it Important to collect Data to detect an Incident

- Understand organization normal and routine operations.

- What is Risk Management
- Assets
- Ways to reduce cybersecurity risks and protect assess



ANY
QUESTIONS