Understanding the Benefits of Risk Management and Information Security

Jobe Beckhom

Brief Overview about me

- Risk Management
- What are Assets
- What are Threats
- Vulnerability Assessment
- Network Diagram
- Risk Management Frameworks
- Risk Treatment Strategies
- Information Security
- Incident Response
- 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

- The entire program of planning for and managing risk to information assets in an organization.

What are Assets

- Organizational resource that is being protected.

Organize your assets

- Classify your assets
- Categorize your 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

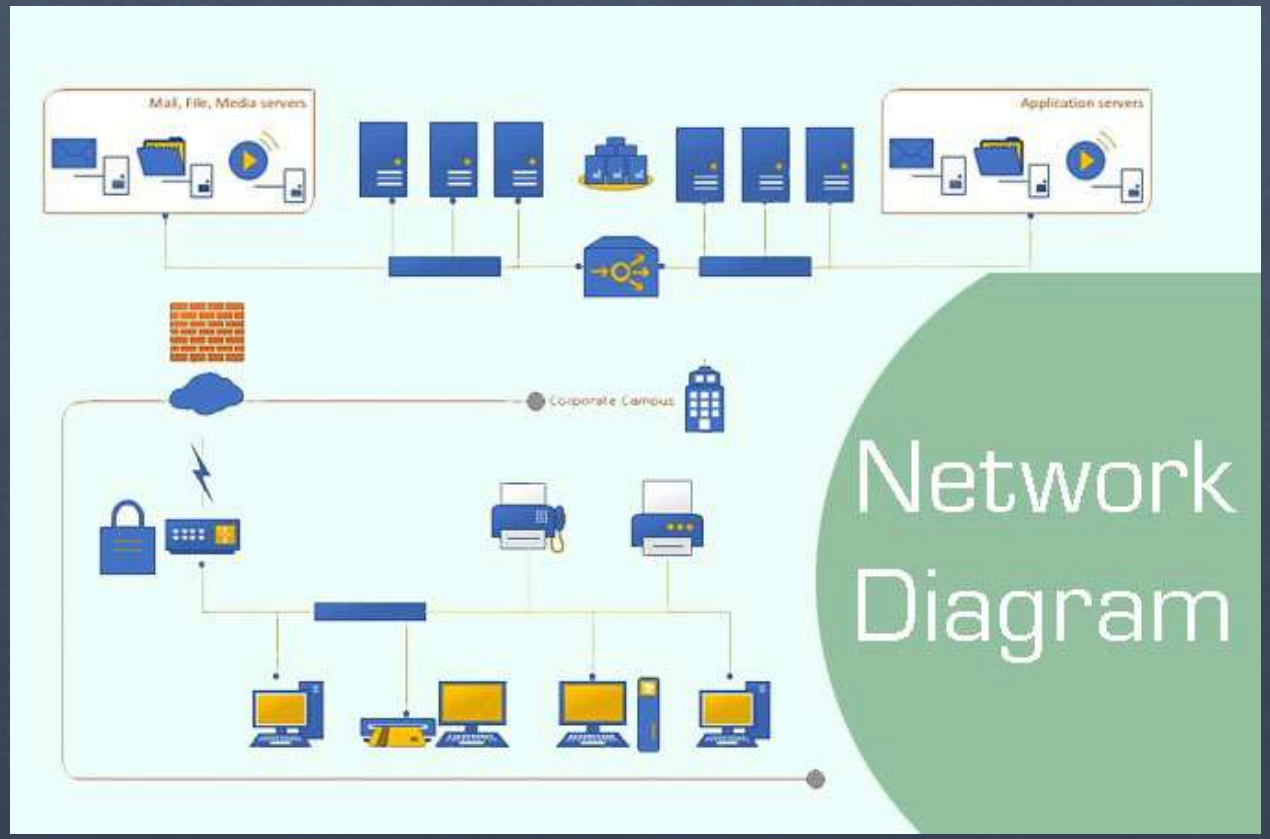
Category of Threat
Compromise of intellectual property
Deviations in quality of service
Espionage or trespass
Forces of nature
Human error or failure
Information extortion
Sabotage or vandalism
Software attacks
Technical hardware failures or errors
Technical software failures or errors
Technological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

Vulnerability Assessment

- A systematic review of security weaknesses in an information system.

Network Diagram

- A visual representation of a computer network.

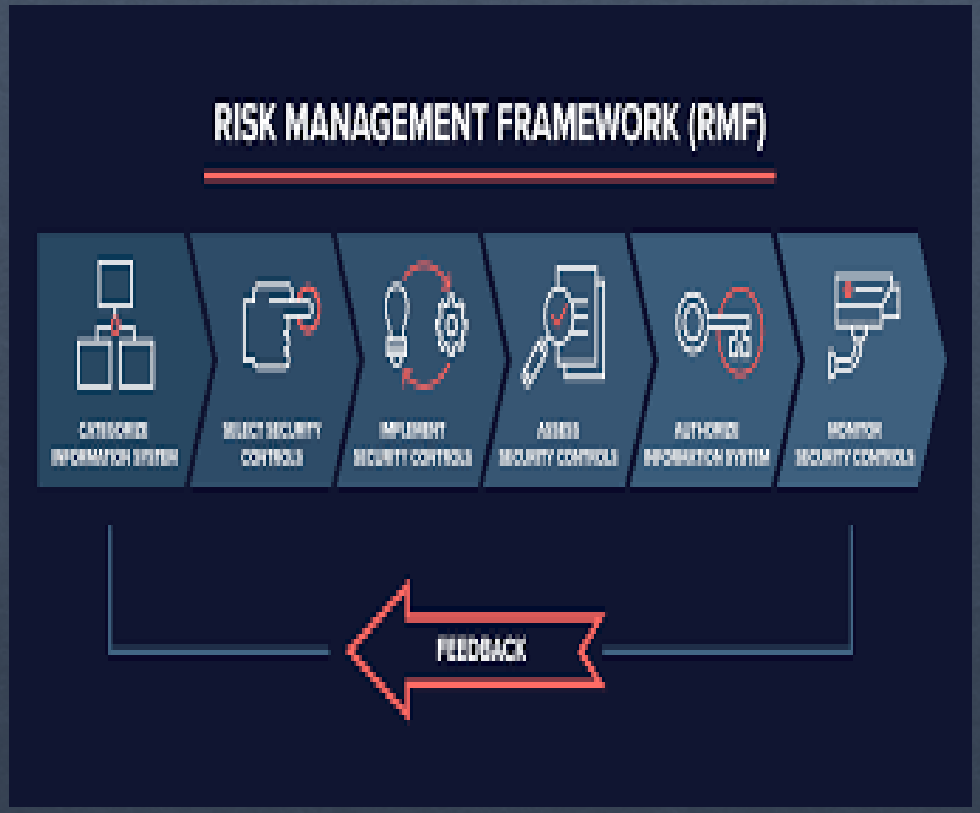


Risk Questions every Organization should be asking

- 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 Management Frameworks

- National Institute of Standards and Technology (NIST)



Risk treatment strategies

- Defense
- Transference
- Mitigate
- Termination

Knowledge

- Know yourself
- Know your enemy

What is Information Security (InfoSec)

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

What is Incident Response (IR)

- Organization's planning and preparation for detecting, reacting and recovering from an indecent

What is an Incident

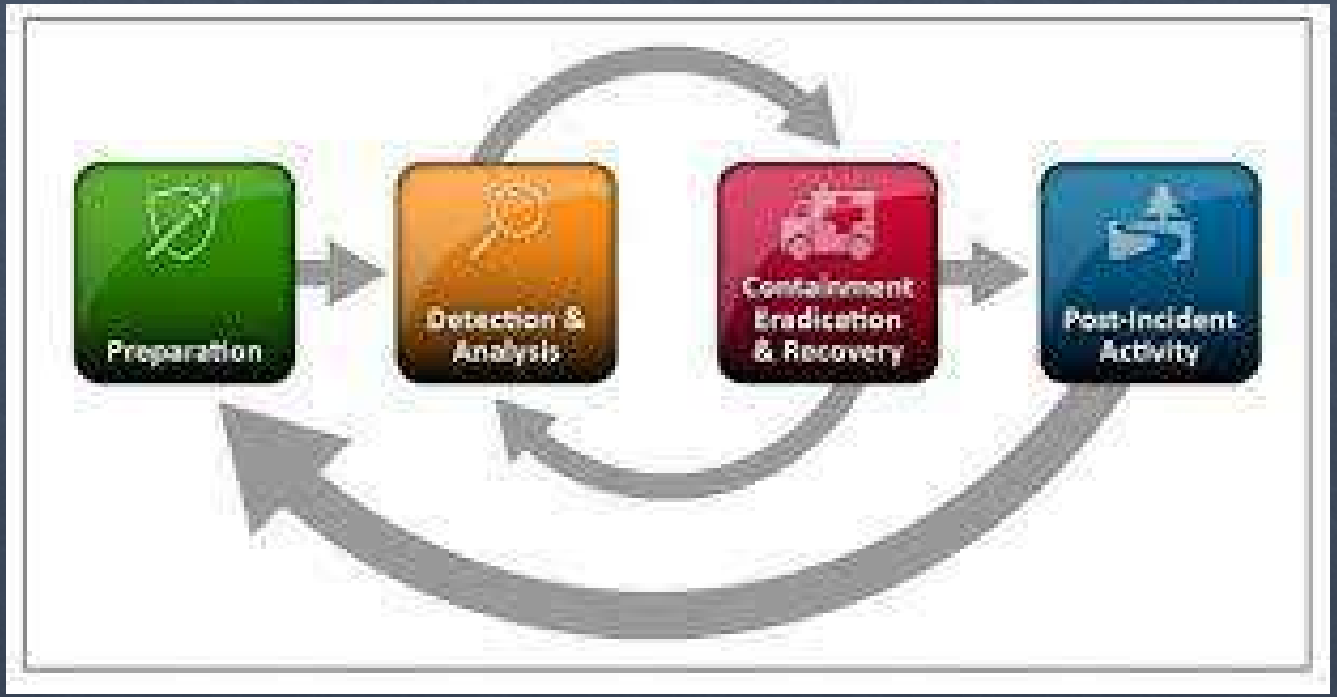
- An adverse event that violates the security of an organization and represents a potential risk of loss of the confidentiality, integrity, or availability of its assets.

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

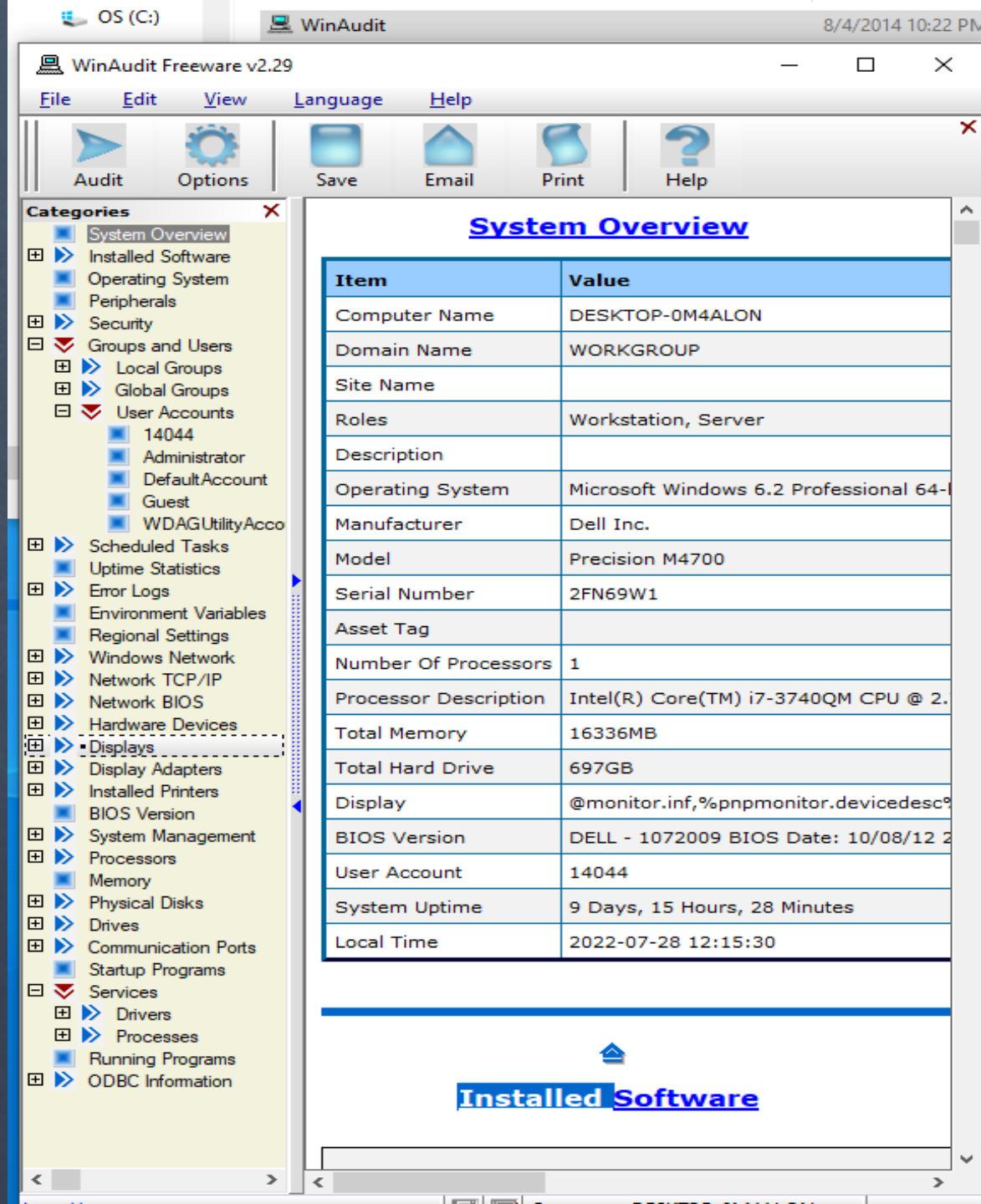
Ways to reduce cybersecurity Risks and protect assets
Implement backups and understand your retention policy
Multi-Factor Authentication (MFA)
Anti-Virus
Encrypt in rest and in transit
Conduct Risk Management Training
Update systems and install patches
Use strong password and have it as a policy
Have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

Ways to prevent and detect an incident (Collect Data)

Data Category
Network performance
Other network data
System data
Process performance
Other process data
Files and directories
Users
Applications
Log files

WinAudit

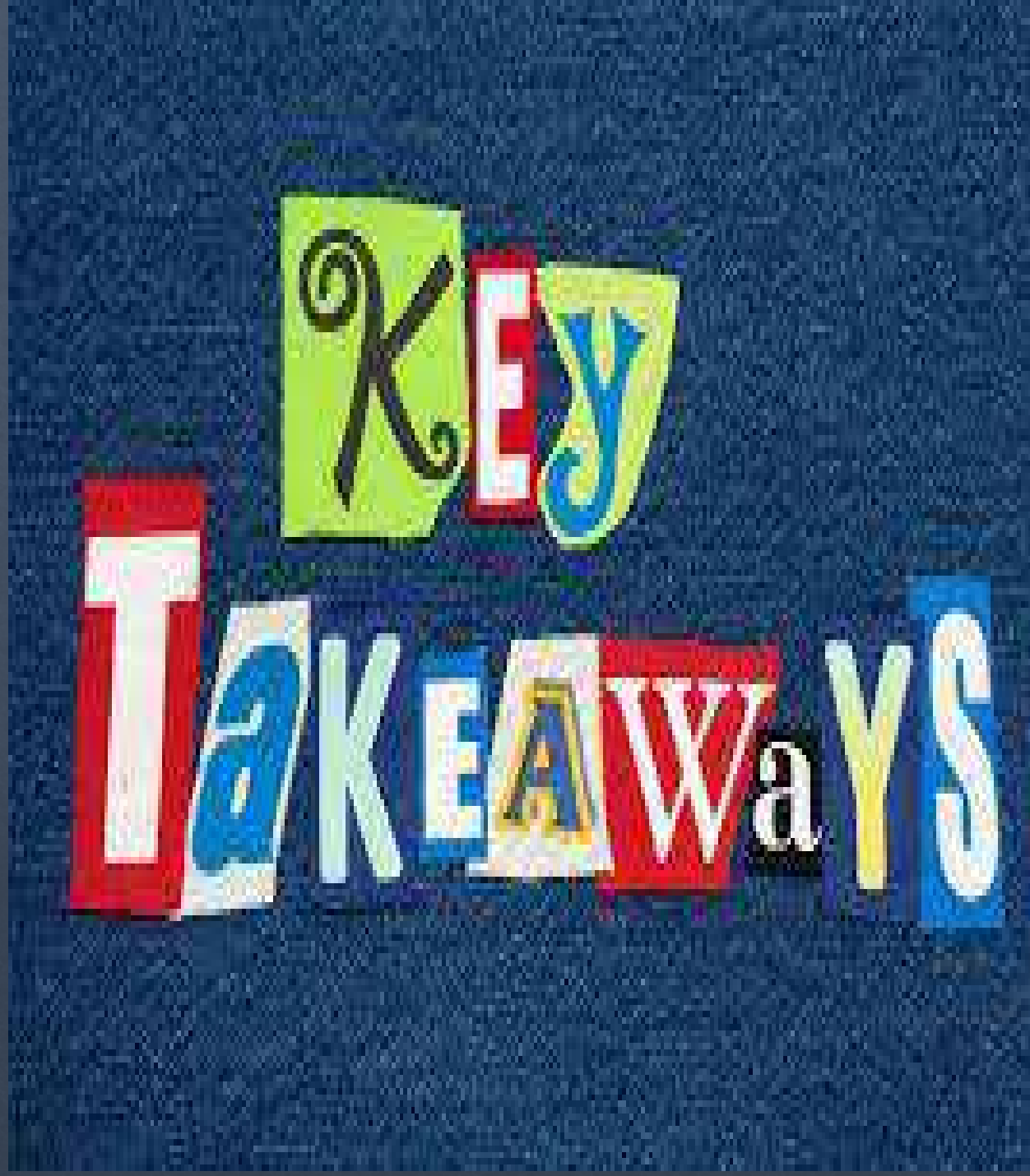
- WinAudit: Inventory GUI for Windows computers.



Why is it Important to collect Data to detect an Incident

- Understand organization normal and routine operations.

- What is Risk Management
- Information Security
- Incident Response
- Ways to reduce cybersecurity risks and protect assess
- Ways to prevent and detect an incident




ANY
QUESTIONS