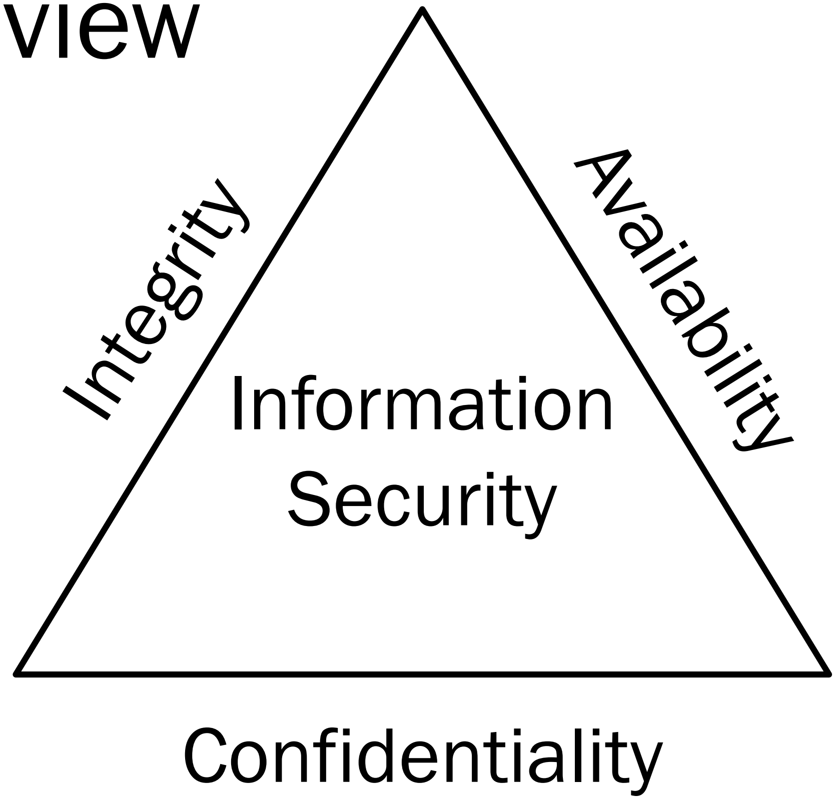
Unit 1 Review



Due Diligence vs. Due Care

- Due Care
- What a reasonable person would do in a given situation.

- Due Diligence
- The management of due care.

3. To prevent any one person from having too much control or power, or performing fraudulent acts, which of the following solutions should NOT be implemented?

A. M of N control
B. Job rotation
C. Multiple key pairs
D. Separation of duties

Answer: B

7. Which item is not a part of the primary security categories?

A. Prevention
B. Encryption
C. Detection
D. Recovery

Answer: B

8. Which of the following is a nontechnical means of enforcing security?

A. Development of a disaster response plan
B. Separation of duties
C. User training
D. Safe testing

Answer: C

15. Which of the following types of controls restricts access based on time?

A. Temporal time restriction
B. Date restriction
C. Time of day restriction
D. Authorized access hours

Answer: C

17. Which of the following is a security program used in many banks to verify the ethics and job performance of a bank manager?

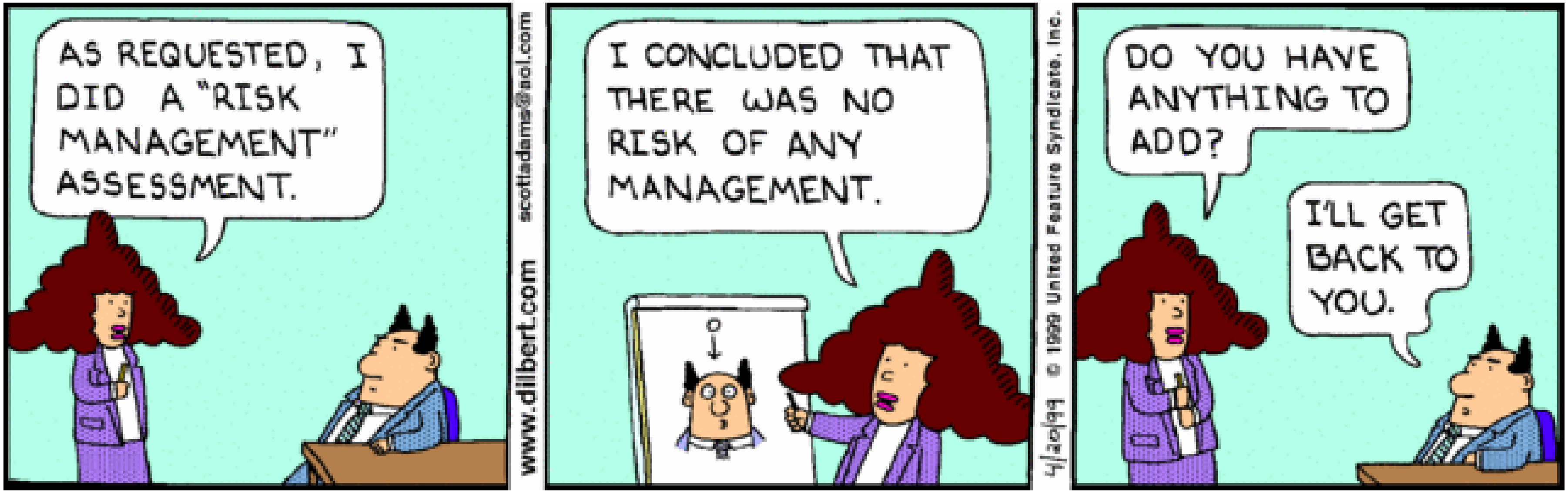
A. Ethical investigation
B. Mandatory vacation
C. Mandatory cruise
D. M of N

Answer: B

RISK IDENTIFICATION, MONITORING, AND ANALYSIS

SSCP®

Systems Security
Certified Practitioner


AS REQUESTED, I DID A "RISK MANAGEMENT" ASSESSMENT.
scottadams@aol.com
www.dilbert.com
I CONCLUDED THAT THERE WAS NO RISK OF ANY MANAGEMENT.
© 1999 United Feature Syndicate, Inc.
4/20/99
DO YOU HAVE ANYTHING TO ADD?
I'LL GET BACK TO YOU.

Domain Objectives

- Describe the risk management process
- Perform security assessment activities
- Describe processes for operating and maintaining monitoring systems
- Identify events of interest
- Describe the various source systems
- Interpret reporting findings from monitoring results

Risk Management Concepts

The ultimate purpose of information security is to reduce risks to acceptable levels

The cost of controls should never exceed the loss

Key Terms

Risk

Likelihood

Threat source

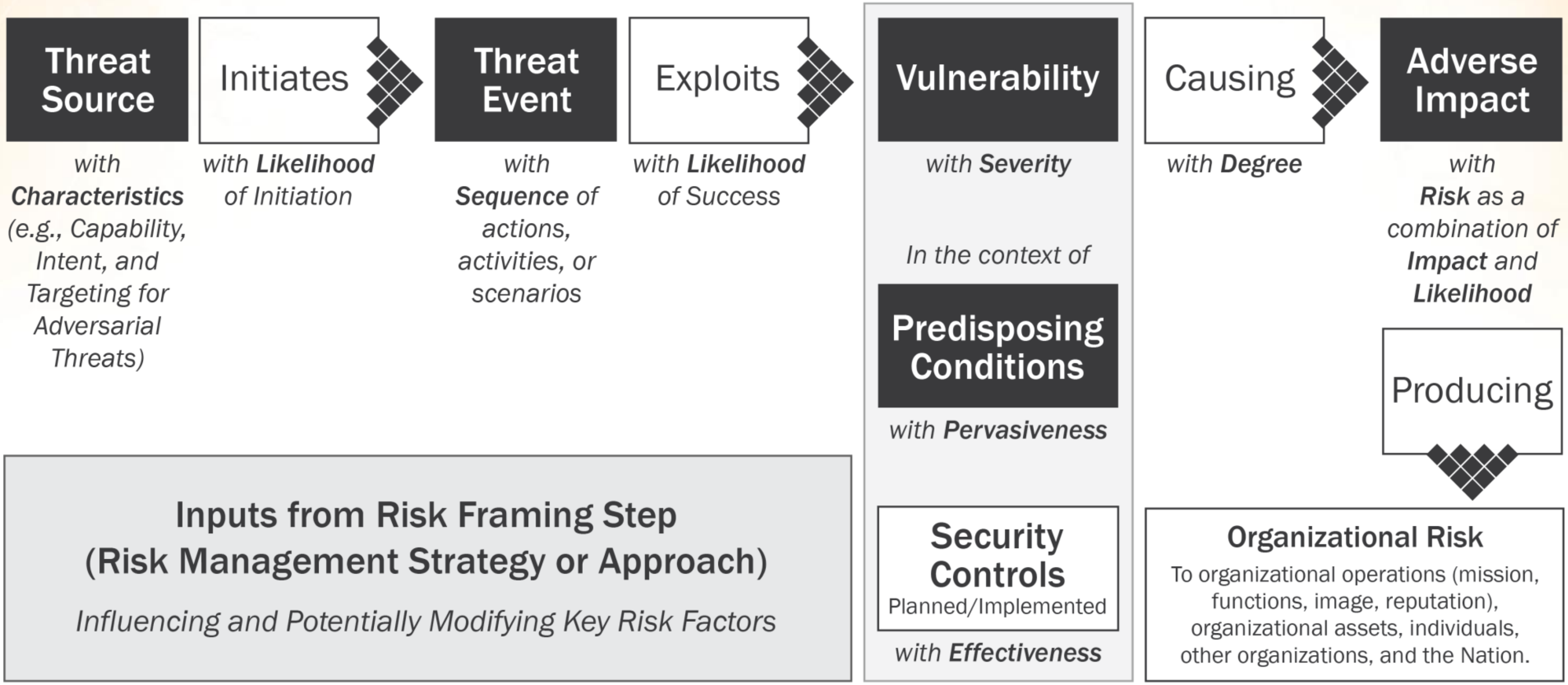
Threat

Vulnerability

Impact

Asset

Generic Risk Model with Key Factors – NIST SP 800-30 R1



Threat Source

with *Characteristics* (e.g., Capability, Intent, and Targeting for Adversarial Threats)

Initiates

with *Likelihood of Initiation*

Threat Event

with *Sequence of actions, activities, or scenarios*

Exploits

with *Likelihood of Success*

Vulnerability

with *Severity*

In the context of

Predisposing Conditions

with *Pervasiveness*

Security Controls
Planned/Implemented

with *Effectiveness*

Causing

with *Degree*

Adverse Impact

with *Risk as a combination of Impact and Likelihood*

Producing

Organizational Risk

To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

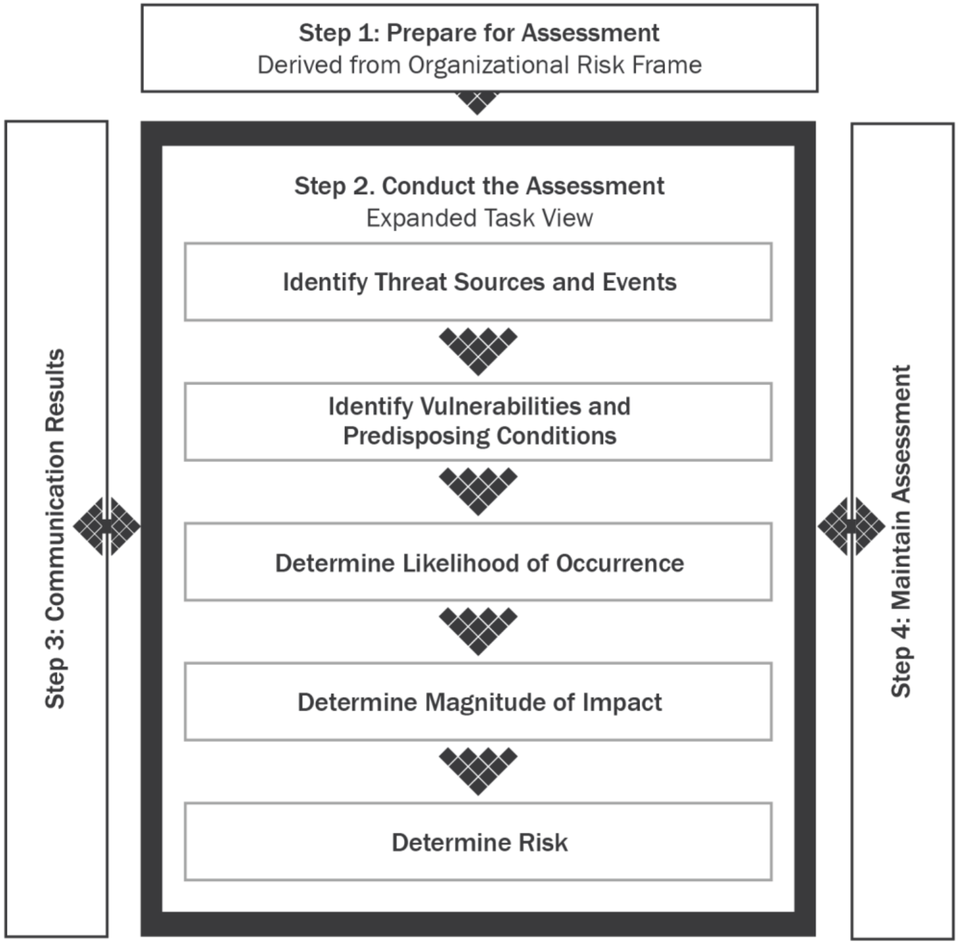
Inputs from Risk Framing Step (Risk Management Strategy or Approach)

Influencing and Potentially Modifying Key Risk Factors

Risk Assessment

Risk assessments evaluate threats to information systems, system vulnerabilities and weaknesses, and the likelihood that threats will exploit these vulnerabilities and weaknesses to cause adverse effects

NIST SP 800-30 R1 Risk Assessment Methodology



Step 1: Prepare for Assessment
Derived from Organizational Risk Frame

Step 2. Conduct the Assessment
Expanded Task View

Identify Threat Sources and Events

Identify Vulnerabilities and Predisposing Conditions

Determine Likelihood of Occurrence

Determine Magnitude of Impact

Determine Risk

Step 3: Communication Results

Step 4: Maintain Assessment

Step 1. Prepare for the Assessment

Objective:

- Establish a context for the risk assessment
- This context is established and informed by the results from the risk-framing step of the risk management process

Preparation Steps

Identify the purpose of the assessment

Identify the scope of the assessment

Identify the assumptions and constraints associated with the assessment

Identify the sources of information to be used as inputs to the assessment

Identify the risk model and analytic approaches

Risk Assessment Steps

Identify threat sources

Identify threat events

Identify vulnerabilities

Determine the likelihood of threats

Determine the adverse impacts

Determine information security risks

Step 2a. Identify Threat Sources

Identify potential threats to information resources

Step 2b. Identify Potential Threat Events

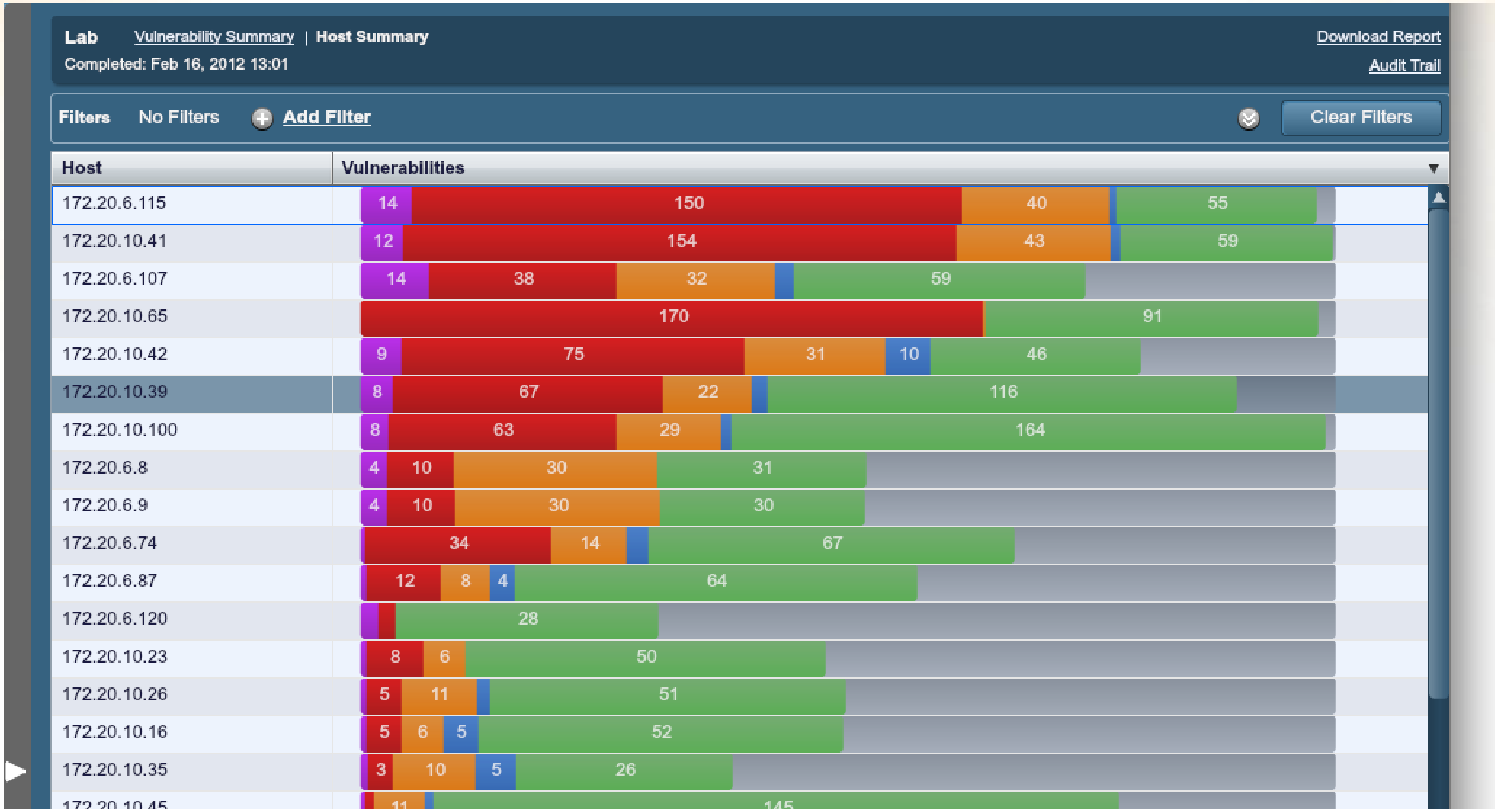
Threat events are characterized by the threat sources that could initiate the events

Define these threat events with sufficient detail to accomplish the purpose of the risk assessment

Step 2c. Identify Vulnerabilities and Predisposing Conditions

Identify technical and nontechnical vulnerabilities that, if exploited, could result in a compromise of system or data confidentiality, integrity, and/or availability

Commercial Tools

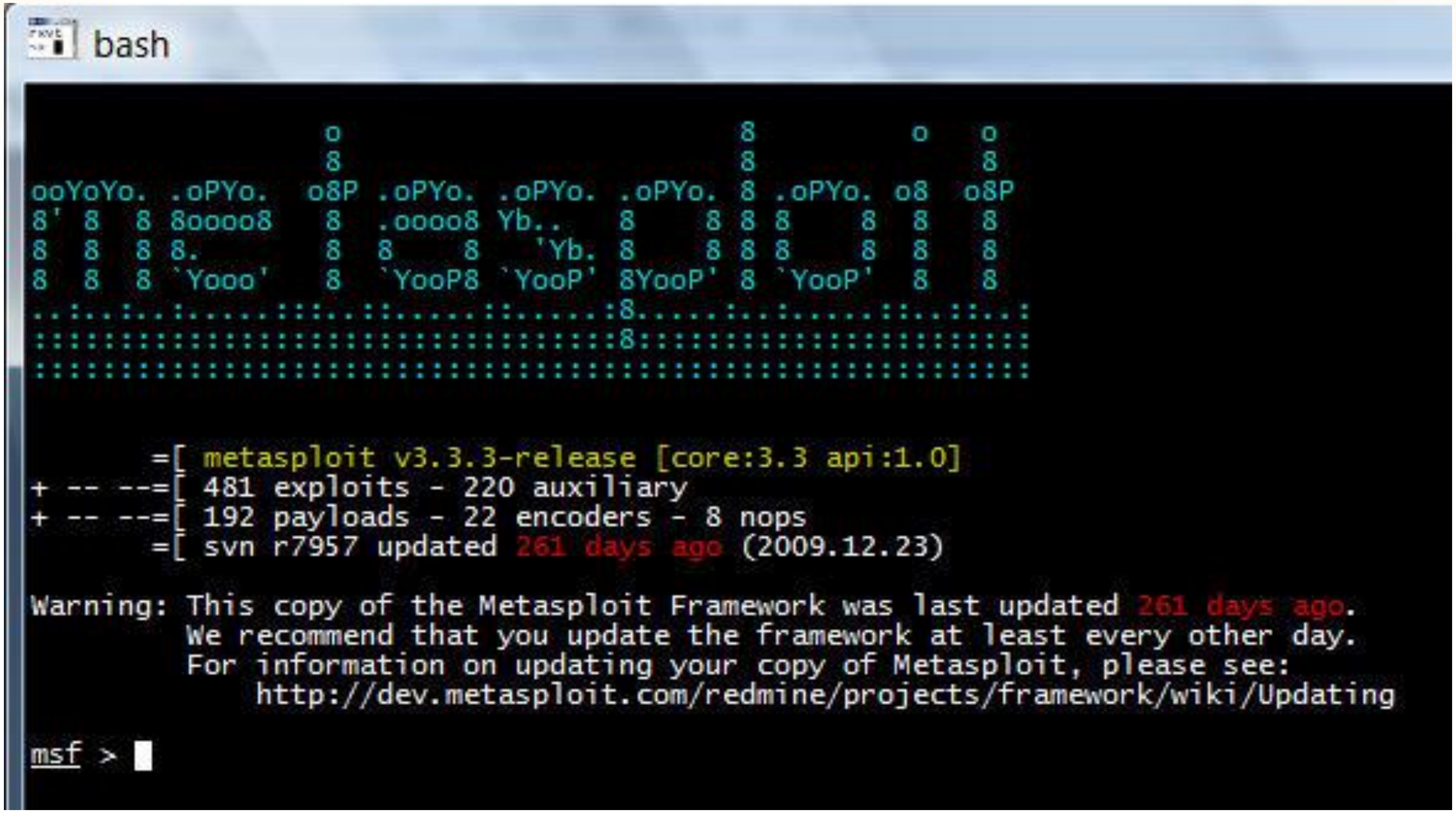


Lab Vulnerability Summary | **Host Summary**

Completed: Feb 16, 2012 13:01

Host	Vulnerabilities
172.20.6.115	14 150 40 55
172.20.10.41	12 154 43 59
172.20.6.107	14 38 32 59
172.20.10.65	170 91
172.20.10.42	9 75 31 10 46
172.20.10.39	8 67 22 116
172.20.10.100	8 63 29 164
172.20.6.8	4 10 30 31
172.20.6.9	4 10 30 30
172.20.6.74	34 14 67
172.20.6.87	12 8 4 64
172.20.6.120	28
172.20.10.23	8 6 50
172.20.10.26	5 11 51
172.20.10.16	5 6 5 52
172.20.10.35	3 10 5 26
172.20.10.45	11 145

Metasploit Console



```
                 o                       8         o   o
                 8                       8             8
ooYoYo. .oPYo.  o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8  8 8oooo8   8  .oooo8 Yb..   8    8 8 8    8  8   8
8  8  8 8.       8  8    8   'Yb. 8    8 8 8    8  8   8
8  8  8 `Yooo'   8  `YooP8 `YooP' 8YooP' 8 `YooP'  8   8
..:..:..:.....:::..::.....::.....:8.....:..:.....::..::..:
::::::::::::::::::::::::::::::::::8:::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --=[ 481 exploits - 220 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 nops
       =[ svn r7957 updated 261 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 261 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf >
```

Systems Security
Certified Practitioner

Step 2d. Determine Likelihood

Factors that must be considered:

- The nature of the vulnerability
- The threat source's motivation and capability
- The effectiveness of controls

Step 2e. Determine Impact

An impact analysis cannot be performed until system mission, system and data criticality, and system and data sensitivity have been obtained and assessed

Step 2f. Risk Determination

Risk determination results from the combination of:

- The likelihood of a threat source attempting to exploit a specific vulnerability
- The magnitude of the impact that would result if an attempted exploit were successful
- The effectiveness of existing and planned security controls in reducing risk

Step 3. Communicating and Sharing Risk Assessment Information

Communicating and sharing information consists of:

- Communicate the risk assessment results
- Share information developed in the execution of the risk assessment to support other risk management activities

Step 4. Maintaining the Risk Assessment

Maintaining risk assessments includes the following specific tasks:

- Monitor risk factors identified in risk assessments
- Update the components of risk assessments

"We've considered every potential risk except the risks of avoiding all risks."

Important Formulas

Single Loss Expectancy = Asset Value X Exposure Factor

Annual Loss Expectancy = Single Loss Expectancy X Annualized Rate of Occurrence

Annualized Rate of Occurrence

Quantitative Analysis

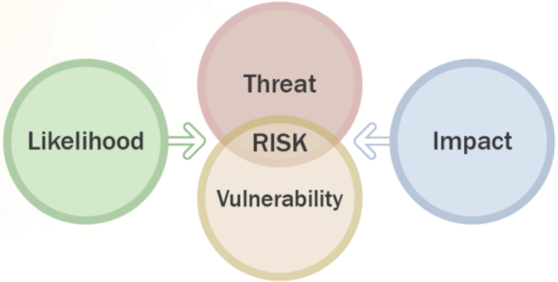
A quantitative impact analysis assigns a dollar value to the impact

Qualitative Analysis

A qualitative impact analysis assesses impact in relative terms such as high impact, medium impact, and low impact without assigning a dollar value to the impact

Risk-Level Matrix

A risk-level matrix can be created that analyzes the combined impact of these factors to assess the overall risk to a given IT system



IMPACT

Threat Likelihood	Low (10)	Moderate (50)	High (100)
High (1.0)	10 x 1.0 = 10	50 x 1.0 = 50	100 x 1.0 = 100
Moderate (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

Risk Scale: High (>50 to 100)   Moderate (>10-50)   Low (1 to 10)

Risk Treatment

- Risk mitigation
- Risk transference
- Risk avoidance
- Risk acceptance

Risk Mitigation

Risk mitigation reduces risks to the organization by implementing technical, managerial, and operational controls

Controls should be selected and implemented to reduce risk to acceptable levels

Control Selection

The key to control selection is to implement cost-effective controls that reduce or mitigate risks to levels that are acceptable to the organization

Managerial

Technical

Operational

Residual Risk

- Residual risk:
  - The risk that remains after risk reduction and mitigation efforts are complete

- Organizations must determine how to treat this residual risk

Risk Transference

Risk transference transfers risk from an organization to a third party

Most common method is insurance

Some risk cannot be transferred

Risk Avoidance

Risk can be avoided by eliminating the entire situation causing the risk

- Disabling system functionality
- Preventing risky activities when risk cannot be adequately reduced

Risk Acceptance

A risk acceptance strategy indicates that an organization is willing to accept the risk associated with the potential occurrence of a specific event

Audit Methodologies

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- NIST SP 800-37 R1
- COBIT

Auditor Responsibilities

Provide independent assurance to management that security systems are effective

Analyze the appropriateness of organizational security objectives

Analyze the appropriateness of policies, standards, baselines, procedures, and guidelines that support security objectives

Analyze the effectiveness of the controls that support security policies

State and explain the scope of the systems to be audited

PERFORM SECURITY ASSESSMENT ACTIVITIES

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

Vulnerability Scanning and Analysis

Vulnerability scanning is simply the process of checking a system for weaknesses

- **Benefits:**
  - Identifies system vulnerabilities
  - Allows for the prioritization of mitigation tasks
  - Useful tool for comparing security posture over time
- **Disadvantages:**
  - It may not effectively focus efforts
  - Potential to crash the network

Potential Problems

False positives

Weeding out false positives

Crash exposure

Temporal information

Security Gateway Types

Antivirus gateways

Java/ActiveX filters

Web traffic screening

Penetration Testing

Phase 1: Preparation

Phase 2: Information gathering

Phase 3: Information evaluation and risk analysis

Phase 4: Active penetration

Phase 5: Analysis and reporting

Penetration Testing Modes

- White box
- Gray box
- Black box

Social Engineering and Low-Tech Reconnaissance

- Social engineering involves the manipulation of people or physical reconnaissance to get information
- Low-tech reconnaissance uses simple technical means to obtain information

Basic Built-in Tools

Traceroute (Windows calls this tracert)

Ping

Telnet

Whois

System Fingerprinting

Understanding Network Behavior

Source address allows the understanding of who is originating the traffic

Destination address tells who is receiving the traffic

Ports characterize the application utilizing the traffic

Class of service examines the priority of the traffic

The device interface tells how traffic is being utilized by the network device

Tallied packets and bytes show the amount of traffic

Monitoring Terminology

- Safeguard
- Countermeasure
- Vulnerability
- Exploit
- Signature
- False positive
- False negative
- True positive
- True negative
- Tuning
- Promiscuous interface

Types of IDS/IPS Devices

Network-based IDS (NIDS)

Host-based IDS (HIDS)

Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS)

Intrusion detection

- Detection of malicious activity in a computer related system
- These malicious activities or intrusions are interesting from a computer security perspective

Everyone who works here
Everyone who doesn't work here
klossner

" WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

Attackers

Attackers are threats generally thought of as people who perform overt and covert intrusions or attacks on systems

Attacker Motivations

- Notoriety, ego, or sport
- Greed and profit
- Political agenda
- Revenge
- Curiosity

Intrusions

Intrusions are acts by persons, organizations, or systems that violate the security framework of the recipient

- Overt
- Covert

Logging

Tune to what is relevant.

What devices and hosts might contain critical log data

What information gets logged

Where and how the log files are going to be stored

Retention schedule for log files

What security measures are going to be employed to ensure the integrity of the log files in storage and in transit

Who has access to modify or delete log files

Big Red-flag!

Reviewing Host Logs

- Auditors are going to want to review host logs as part of the audit process
- Review host log files regularly as part of your organization’s security program

Reviewing Incident Logs

- Any time an incident occurs, save the log files of all devices that have been affected or are along the network path the intruder took
- These files need to be saved differently than your standard log retention policy

Clipping Levels

Clipping levels:

- Are a predefined criteria or threshold that sets off an event entry
- Usually have a time property associated with them
- Great for reducing the amount of data accumulating in log files

Log Retention

- Automation is one of the keys to successful log file management
- There are many different tools both commercial and open source that can automate different phases of log file retention

Distributed Log Collectors

- Scribe
- Flume
- Logstash
- Chukwa
- Graylog2
- splunk

Event Correlation Systems

SIEM technology is used in many enterprise organizations to provide real-time reporting and long-term analysis of security events

- Security event management (SEM)
- Security information management (SIM)

Comprehensive Application, Middleware, OS, and Infrastructure Monitoring

Auto-discover

Complete run-book deployment automation

Comprehensive monitoring for performance

Understand availability, performance, utilization, events, logs

Log Management Recommendations

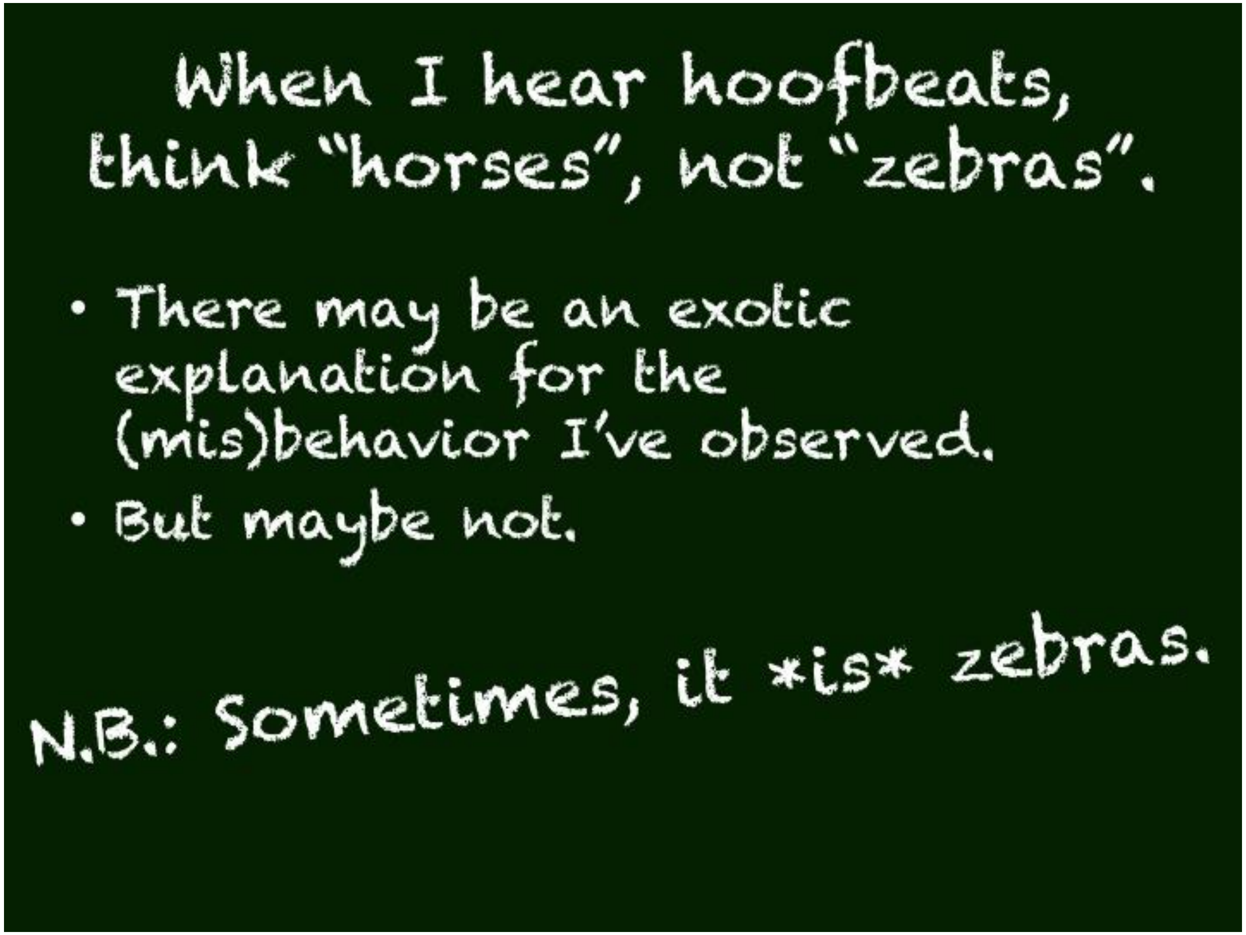
Establish policies and procedures for log management

Prioritize log management appropriately throughout the organization

Create and maintain a log management infrastructure

Provide proper support for all staff with log management responsibilities

Establish standard log management operational processes



When I hear hoofbeats, think "horses", not "zebras".

- There may be an exotic explanation for the (mis)behavior I've observed.
- But maybe not.

N.B.: Sometimes, it *is* zebras.

Assignment #1

Risk Register

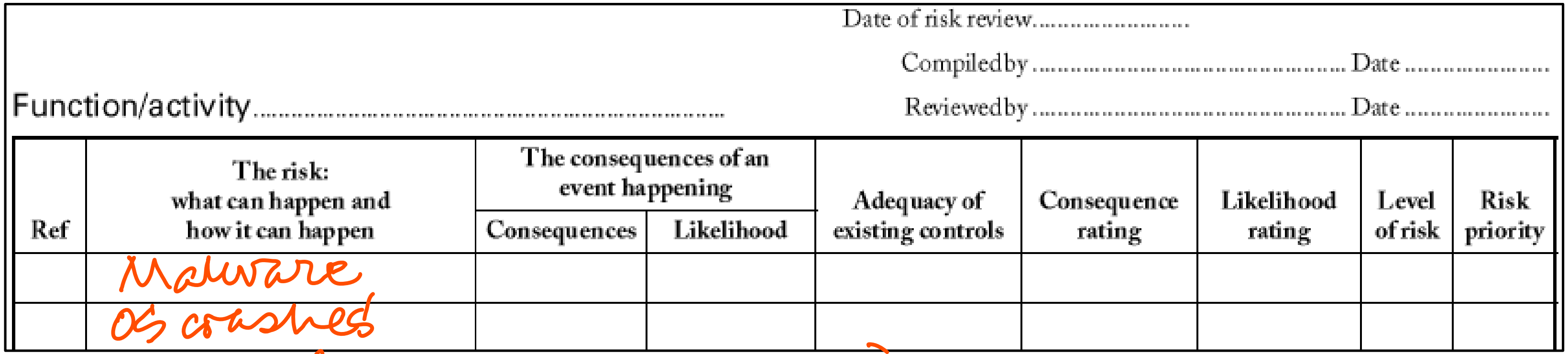
A way for the organization to know its possible exposure at a given time

Keeps stakeholders aware of issues

Tracks the response to issues

Creating a Risk Register

1. Create the Risk Register
2. Record active risks
3. Assign a unique number to each risk element



Date of risk review........................

Compiled by .... Date ....

Function/activity .... Reviewed by .... Date ....

Ref	The risk: what can happen and how it can happen	The consequences of an event happening		Adequacy of existing controls	Consequence rating	Likelihood rating	Level of risk	Risk priority
		Consequences	Likelihood					
	Malware							
	OS crashed							

Tornado

etc

↑ For which system

Risk Register Risk Management Steps

1. Identifying the risk
2. Evaluating the severity of any identified risks
3. Applying possible solutions to those risks
4. Monitoring and analyzing the effectiveness of any subsequent steps taken

Examples of Risks

Botnets
DDoS
Hacking
Malware
Pharming
Phishing
Ransomware
Spam
Spoofing
Spyware
Trojan Horses
Viruses
WiFi Eavesdropping
Worms