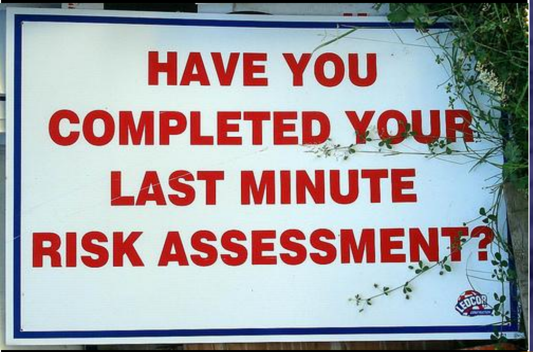


Risk Assessment

The Heart of Information Security

Overview

- Warm-up Quiz
- Why do we perform risk assessments?
- The language of risk - definitions
- The process of risk assessment
- Risk Mitigation Triangle
- Lessons Learned

Ready for a Quiz?

True or False?

1. Conducting a risk assessment is optional for most organizations. False
2. Risk assessment is a decision support aid, not a decision making tool. True
3. Risk assessments should focus on business processes or areas of responsibility, rather than individual assets. True
4. Risk assessment has been used by some enterprises as rationale <u>not</u> to implement security controls. True
5. Risk assessments are plagued by subjectivity which means they simply cannot be relied upon. False
6. The risk assessment process can improve communication between business managers, system support staff, and security/risk specialists. True

True or False?

7. The only acceptable risk assessment is performed by risk assessment experts. False
8. Risk assessments only need to be done once. False
9. Security professionals are ultimately responsible for accepting residual risks. False
10. If you don't have all the data, risk assessments are a waste of time. False
11. A proper risk assessment can help you prioritize security spending. True
12. Risk is the effect of uncertainty on objectives and can include both positive and negative consequences. True

How did you do?

Why do we perform risk assessments?

Not just security, the right security.

Plenty of Assets Needing Protection

Unless we identify our assets, their locations and value, how can we assess the risk and decide the amount of time, money and effort that we should spend on protecting them?

ISO/IEC 27002:2005

Physical assets

- Computer equipment/infrastructure
- Communication equipment
- Storage media
- Non IT equipment
- Furniture and fixtures

Information assets

- Databases
- Data files (Hard & Soft Copies)
- Archived information

Software assets

- Application software
- System software
- Custom Management software

Services

- Outsourced computing services
- Communication services
- Environmental conditioning services

Supporting Documentation

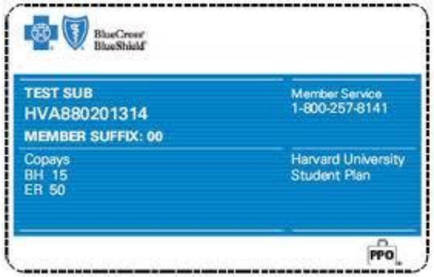
- Compliance Documentation
- Corporate Policies and Procedures
- BC/DR Plans

Intangible assets

- Key employees – Intellectual Property
- Company knowledge - Innovation
- Brand/Corporate culture

Valuable Information is Everywhere

- Medical History/Claims
- Financial Account Numbers
- SS Numbers
- Medical ID Cards
- Credit or Debit Card Numbers
- Drivers License Numbers
- Email Addresses
- User Names
- Intellectual Property
- Client Lists/Contact Information
- PINs & Passwords
- Check Images



BlueCross BlueShield

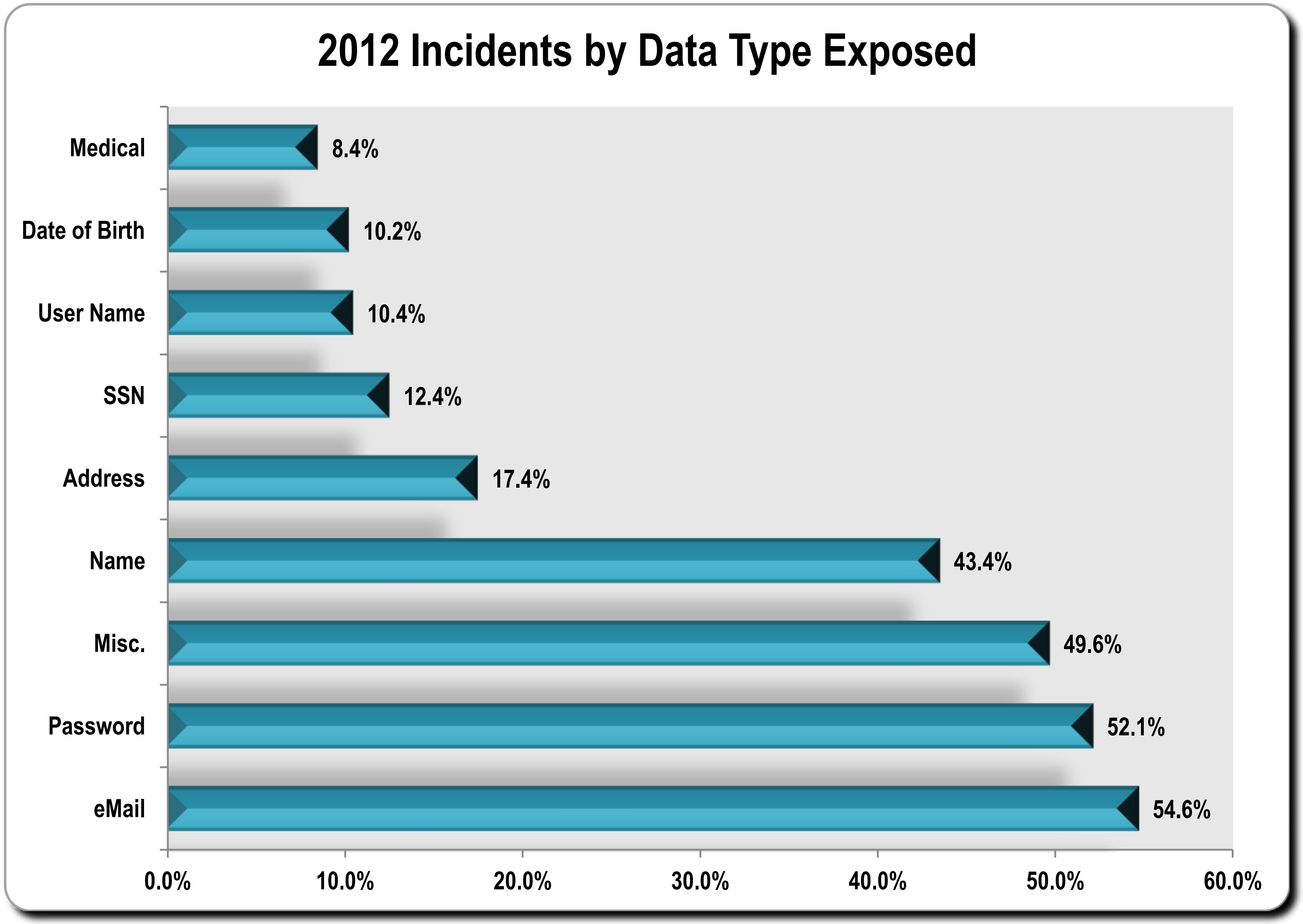
TEST SUB
HVA880201314
MEMBER SUFFIX: 00
Copays
BH 15
ER 50

Member Service
1-800-257-8141

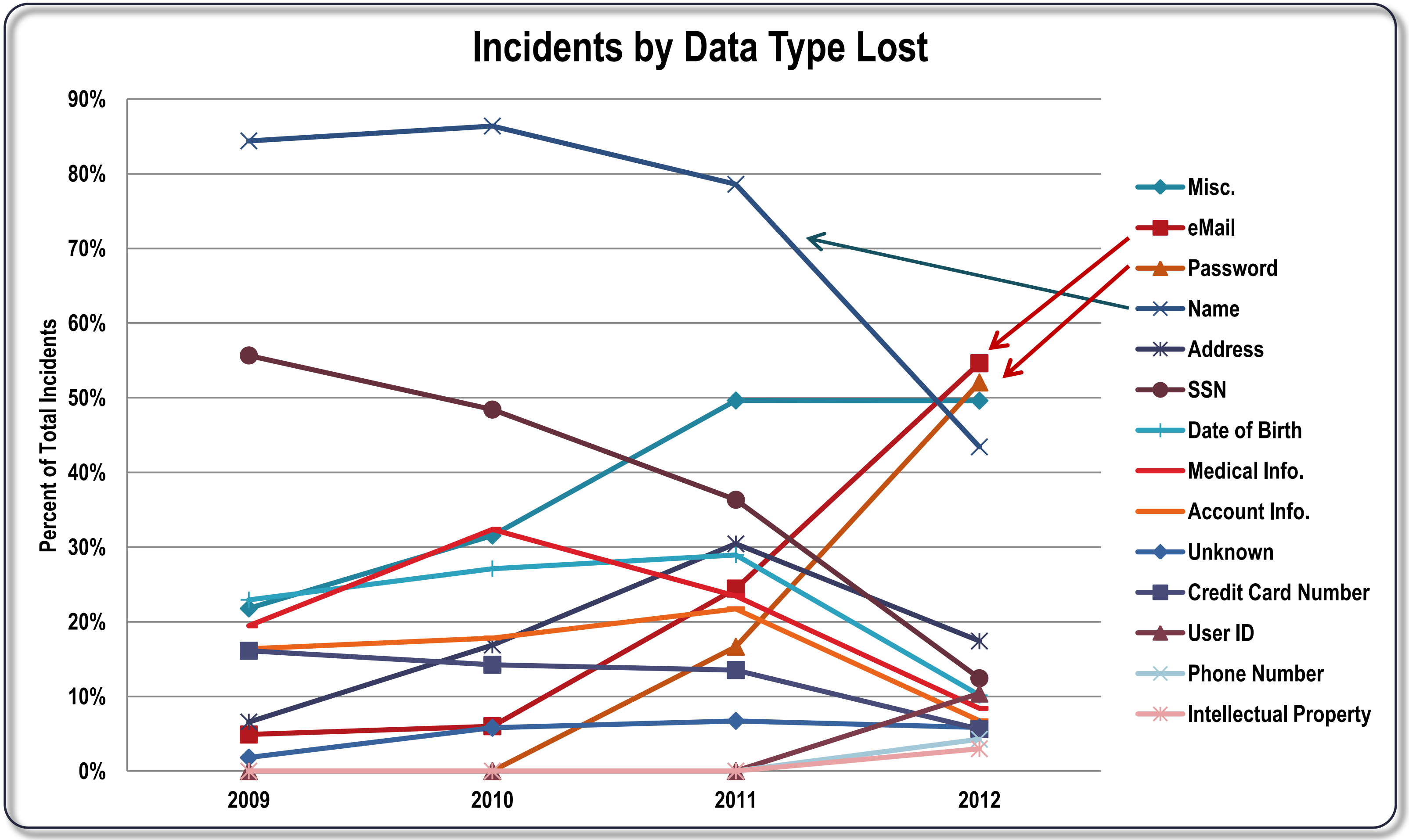
Harvard University
Student Plan

PPO

Top Data Types Exposed in 2012



Change in Top Data Types Exposed



RiskBased SECURITY

Regulations/Standards Demand It

- HIPAA
- HITECH
- GLBA
- FFIEC
- ISO 27001/5
- ISO 31000
- NIST SP 800-30/37/39
- FISMA
- Red Flag Rules

HIPAA HITECH COMPLIANT

Improving Gramm-Leach-Bliley Security Compliance

Security provisions of GLBA are complex and process intensive. Our free guide explains how on-demand security audits make GLBA compliance easier to achieve.

CERTIFIED ISO 27001

NIST National Institute of Standards and Technology

FISMA

- PIPEDA
- GDPR
- SOX
- PCI DSS
- COBIT
- ITIL
- State Privacy Laws

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS

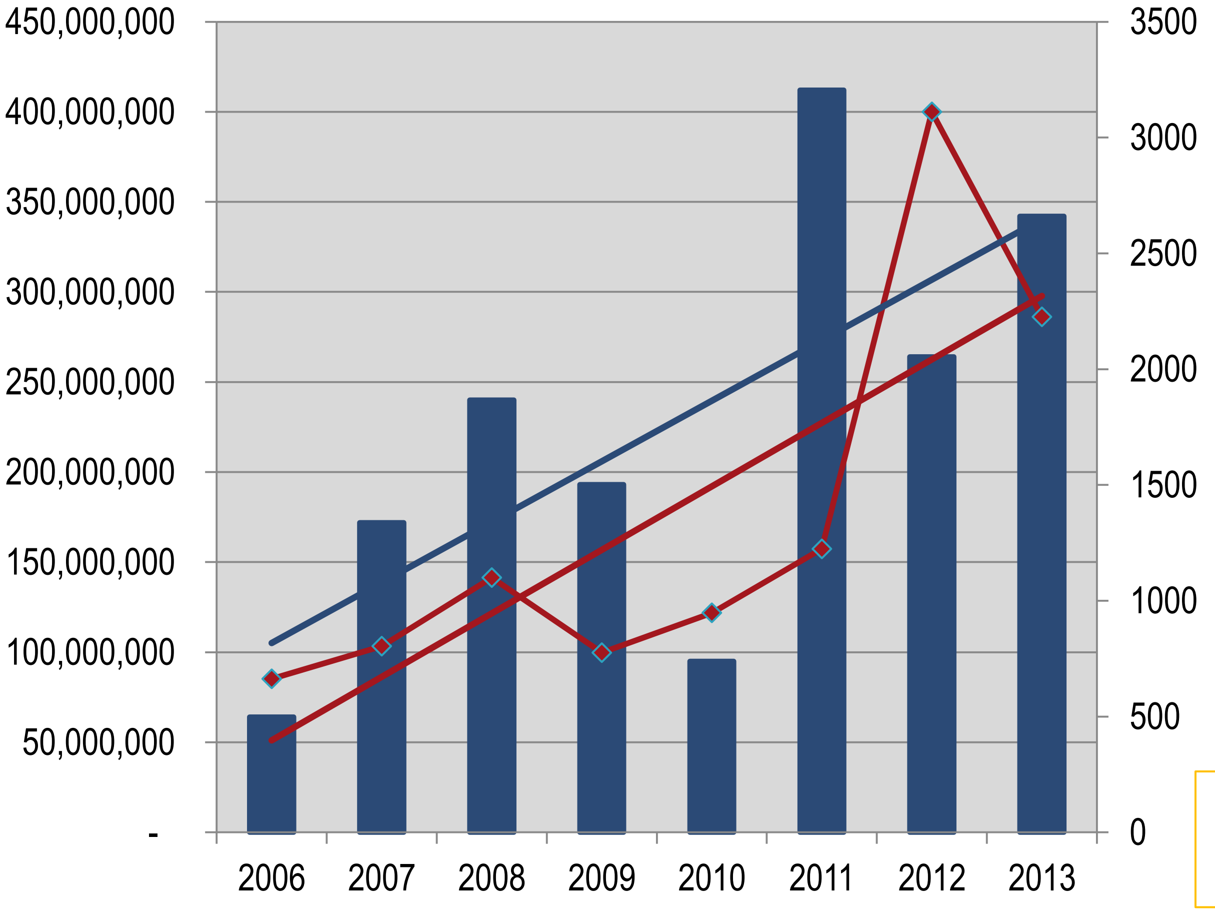
SARBANES-OXLEY DO IT OR ELSE

PCI Compliance

Privacy Policy

RiskBased SECURITY

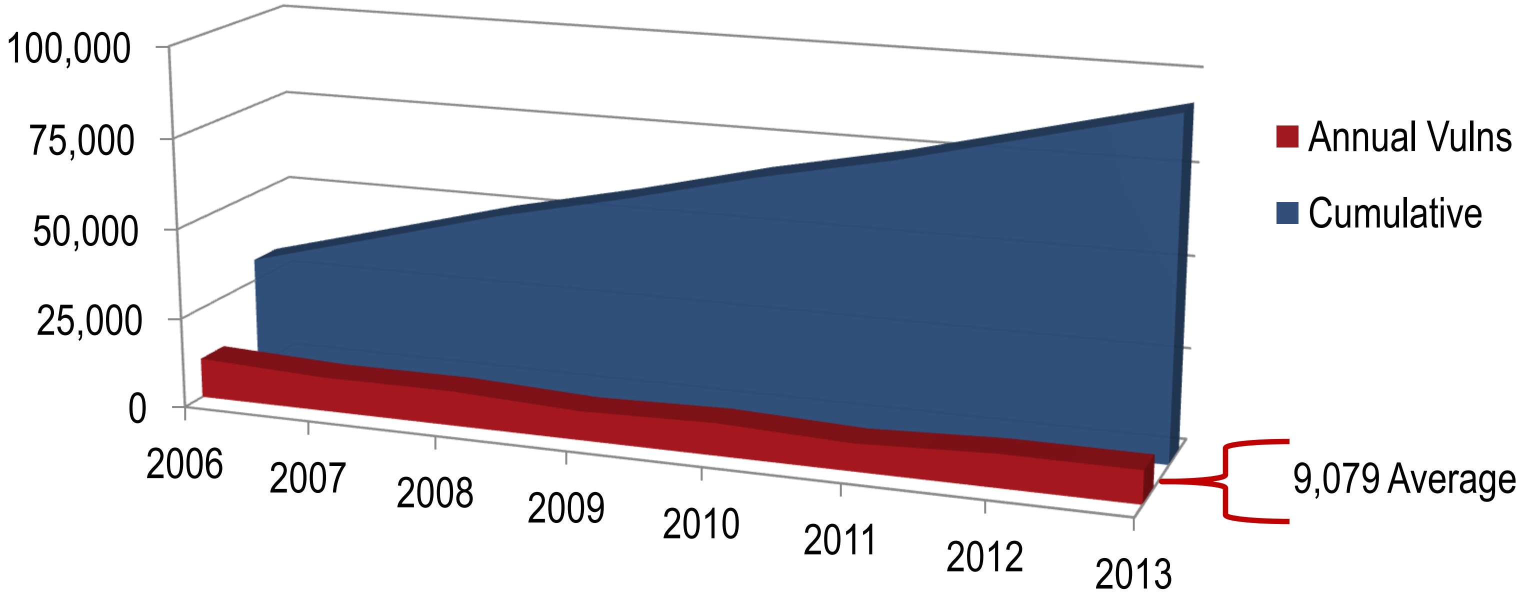
Today's Reality – Data Breaches



2013 Estimates

- Incidents April 30th x 3
- Records April 30th x 2

Today's Reality – New Exploits



2013 Estimate April 30th x 3

The Need has Never Been Higher

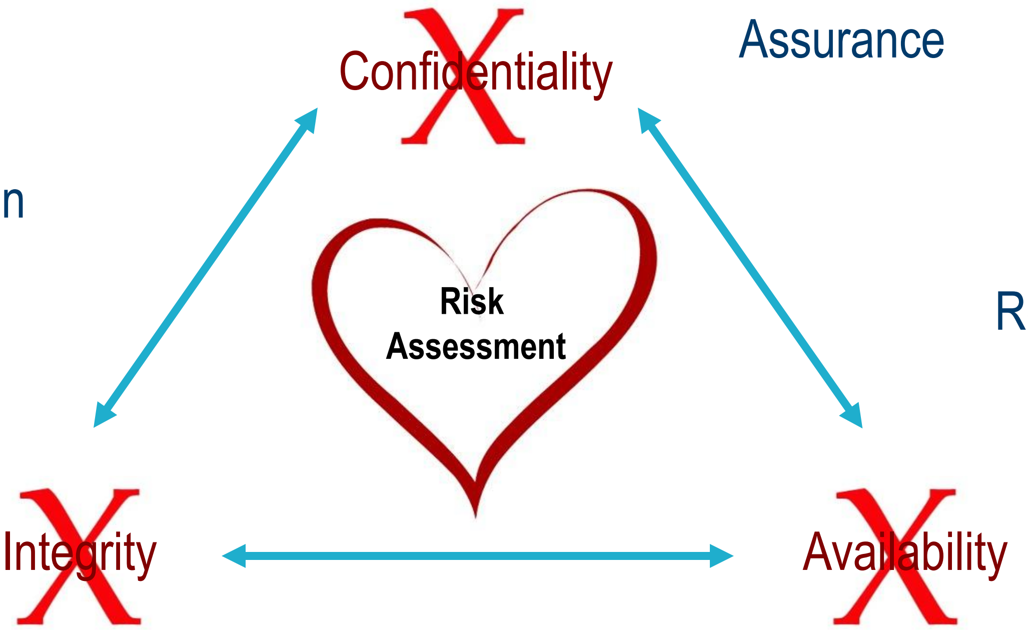
- Anyone who captures, stores or transmits sensitive information or processes financial transactions is actively being targeted.
- Organizations need a way to properly focus limited resources to deal directly with potential impacts and existing vulnerabilities.
- Organizations need justification for security recommendations in business terms.
- In a highly competitive business environment, organizations cannot afford to have costly or inappropriate security.
- An effective risk assessment program can be thought of as the first line of defense of an organization’s profitability.

The Language of Risk Assessments

Not just security, the right security.

Information Security

ISO/IEC 27002:2005 defines Information Security as the preservation of:



Assurance

Non-repudiation

Reliability

Authenticity

Accountability

First, Some Definitions

- Risk can be defined as…
  - a combination of the consequence of an event and the probability of the event
  - Impact x Threat x Vulnerability
  - Impact to the organization when a threat exploits a vulnerability
  - the “effect of uncertainty on objectives” (positive or negative)
- A threat is any potential danger to an asset or business objective
- A vulnerability is a weakness that provides an open door to exploit
- Risk Score is the potential impact to the business based on the likelihood of a threat agent taking advantage of a vulnerability

Chinese Definition of Risk

风 险

Danger + Opportunity

Risk Assessment

- Risk assessment is made up of three processes:
  - Risk identification is used to find, recognize, and describe the risks that could affect the achievement of objectives.
  - Risk analysis is used to understand the risks that you have identified, study impacts and consequences, and to estimate the level of risk based on the controls that currently exist.
  - Risk evaluation compares the risk analysis results with risk criteria to determine the appropriate risk treatment.
- Risk treatment options include: avoidance, transfer, implementing safeguards (controls), or knowingly accepting the risk.
- Residual risk is the risk left over after you've implemented risk treatment.

My Personal Risk Definition

- *Risk* – a combination of the consequence of an event and the probability of the event happening

Consequence – The impact to the organization of a potential breach to an asset's confidentiality, integrity or availability. [Asset Value (AV) or Security Impact (SI)]

Probability – The probability of the threat occurring. [Threat Likelihood (TL)]

X

The probability of exposure to the threat considering the existing security controls. [Vulnerability Exposure (VE)]

Consequence X Probability

Risk = AV x (TL x VE)

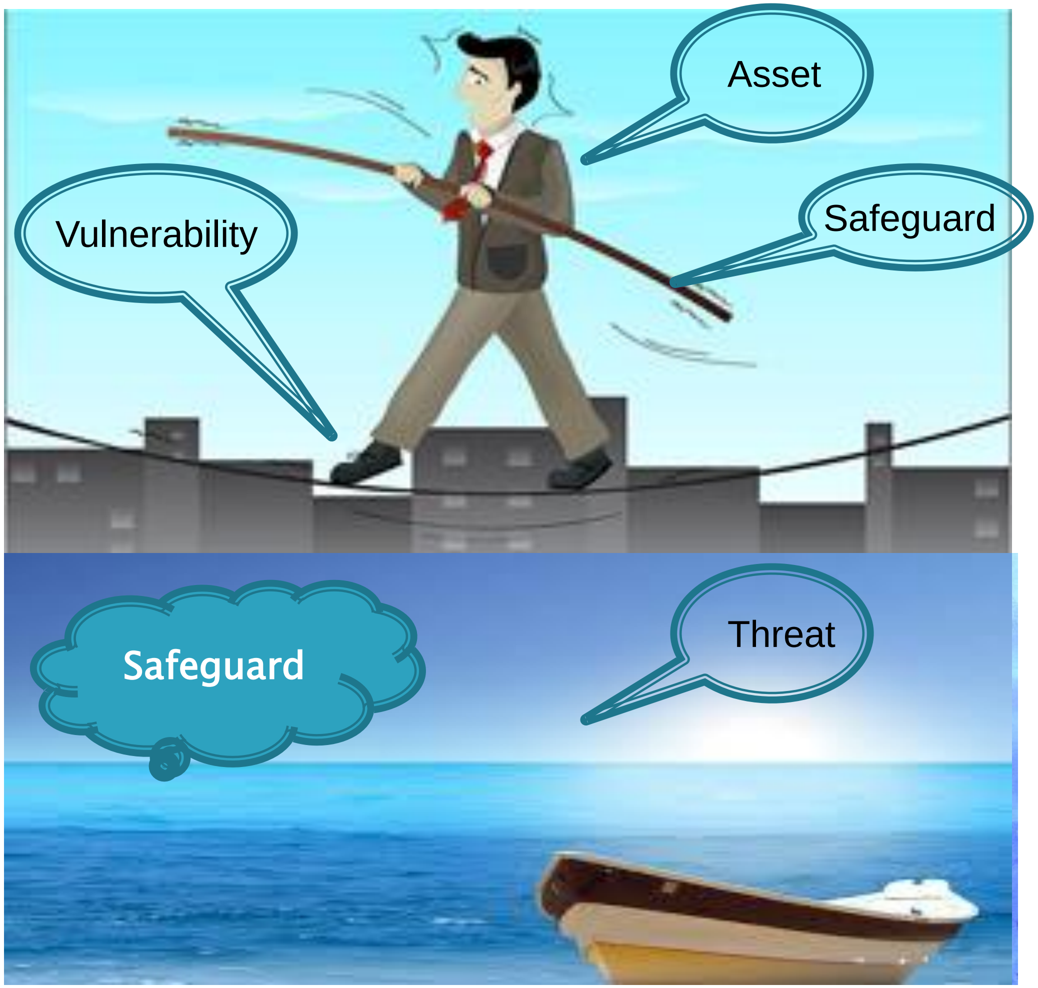
RiskBased SECURITY

Where Do We Get The Numbers?

- Quantitative Analysis – uses 'real' numbers in the calculation of probability and consequence, not rankings (1st, 2nd, 3rd); and is used in industries with years of documented historical data. [Any industries come to mind?]

- Qualitative Analysis – uses common terms to describe the magnitude of potential consequences and probability and is useful when reliable data for more quantitative approaches is not available or too costly to obtain.

What Can You Spot?

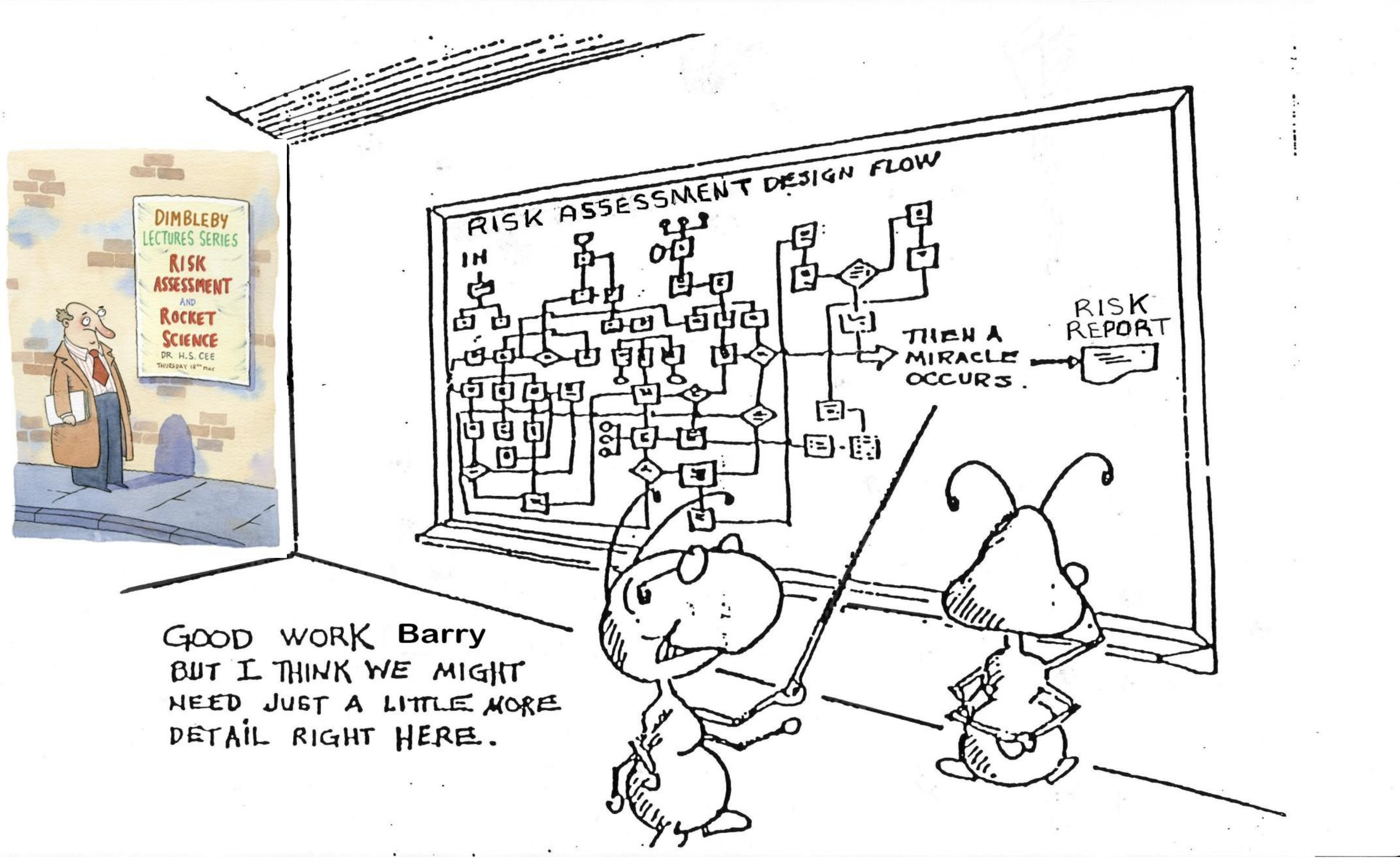


The Process of Risk Assessments

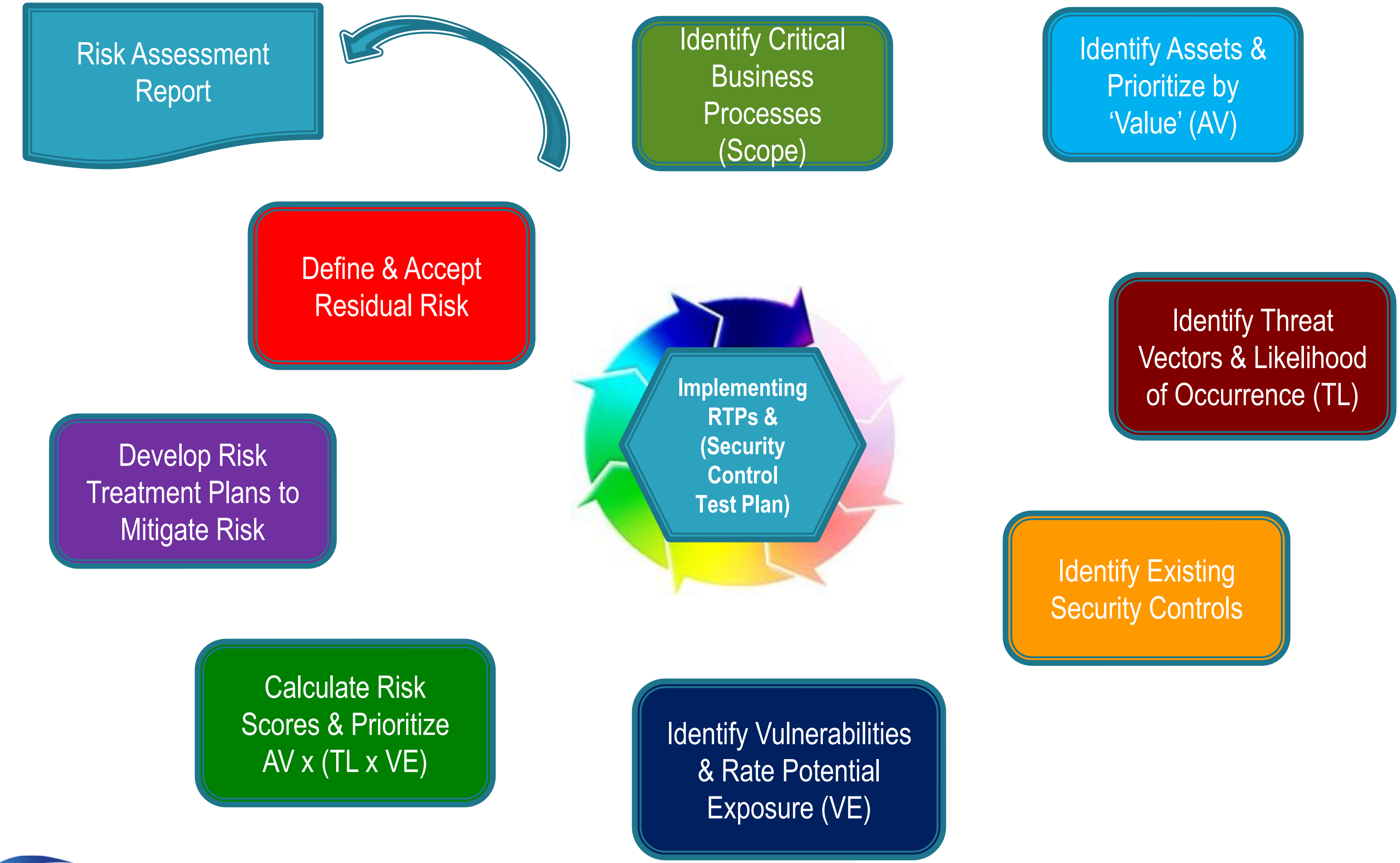
Not just security, the right security.

The Best Method of Accomplishing an Accidental Result

Ambrose Bierce


DIMBLEBY
LECTURES SERIES
RISK ASSESSMENT AND ROCKET SCIENCE
DR H.S. CEE
THURSDAY 18TH MAY
RISK ASSESSMENT DESIGN FLOW
IN
THEN A MIRACLE OCCURS.
RISK REPORT
GOOD WORK Barry BUT I THINK WE MIGHT NEED JUST A LITTLE MORE DETAIL RIGHT HERE.

The Risk Assessment Process



Identify Critical Business Processes (Scope)

Identify Assets & Prioritize by 'Value' (AV)

Identify Threat Vectors & Likelihood of Occurrence (TL)

Identify Existing Security Controls

Identify Vulnerabilities & Rate Potential Exposure (VE)

Calculate Risk Scores & Prioritize AV x (TL x VE)

Develop Risk Treatment Plans to Mitigate Risk

Define & Accept Residual Risk

Risk Assessment Report

Implementing RTPs & (Security Control Test Plan)

The Risk Assessment Scope

Identify Critical Business Processes (Scope)

System Characterization (Scope)

- Business Process/ Department Mission Description
- Information Flow
- Security Requirements
- People & Users
- Physical & Logical Perimeters
- Network Diagram
- Critical Information Asset Inventory

RiskBased SECURITY

Calculating Asset Values (AV)

Identify Assets & Prioritize by 'Value' (AV)

Asset Name	Data Classification	Impact to the Asset from a Breach in **Confidentiality**
		5.0 Very High;
		4.0 High;
		3.0 Medium;
		2.0 Low;
		1.0 Very Low
			Impact to the Asset from a Breach in **Integrity**
			5.0 Very High;
			4.0 High;
			3.0 Medium;
			2.0 Low;
			1.0 Very Low
				Impact to the Asset from a Breach in **Availability**
				5.0 Very High;
				4.0 High;
				3.0 Medium;
				2.0 Low;
				1.0 Very Low
					Asset Value SCORE **(AV)**

Web Server	Sensitive	3.0	4.0	5.0	4.0
On-line Banking Application	Confidential	5.0	5.0	5.0	5.0
Marketing Material	Public	1.0	2.0	3.0	2.0

Asset Value (AV) Severity Descriptions

Value (AV)	Severity Description
Catastrophic (5.0)	Severe impact to operations, extended outage, permanent loss of resource, triggers business continuity and/or public relations procedures, complete compromise of information, damage to reputation and/or significant cost to repair with continuity of business in jeopardy
Major (4.0)	Serious impact to operations, considerable system outage, compromise of a large amount of information, loss of connected customers, lost client confidence with significant expenditure of resources required to repair
Moderate (3.0)	Some impact to operations, tarnished image and loss of member confidence with significant effort to repair
Minor (2.0)	Small but tangible harm, may be noticeable by a limited audience, some embarrassment, with repair efforts absorbed into normal operations
Insignificant (1.0)	Insignificant impact to operations with minimal effort required to repair, restore or reconfigure

Threats & Threat Likelihood

Identify Threat Vectors & Likelihood of Occurrence (TL)

Threat – a potential cause of an unwanted incident, which may result in harm to an organization's asset.

- Natural/Manmade Disaster
- Equip./Service Failures
- Acts of Terrorism
- Hackers
- Corporate Espionage
- Theft, Loss, or Fraud
- Accidental Human Action
- Malicious Human Action
- Software Errors
- Non Compliance
- External Parties
- Unauthorized Access
- Emerging Threats

RiskBased SECURITY

Threat Likelihood (TL) Descriptions

Threat Likelihood (TL)	Description
Very High (5.0)	There are incidents, statistics or other information that indicate that this threat is very likely to occur or there are very strong reasons or motives for an attacker to carry out such an action. (Likely to occur multiple times per week)
High (4.0)	Likely to occur two - three times per month
Medium (3.0)	There are past incidents, or statistics that indicate this or similar threats have occurred before, or there is an indication that there may be some reasons for an attacker to carry out such an action. (Likely to occur once per month)
Low (2.0)	Likely to occur once or twice every year
Very Low (1.0)	Few previous incidents, statistics or motives to indicate that this is a threat to the organization (Likely to occur two/three times every five years)

Existing Controls Inventory

Identify Existing Security Controls

Security Controls – administrative, technical, and physical safeguards intended to ensure the confidentiality, integrity, and availability of an organization’s information assets.

Access Enforcement
Separation Of Duties
Least Privilege
Unsuccessful Login Attempts
System Use Notification
Previous Logon Notification
Concurrent Session Control
Session Lock
Session Termination
Supervision And Review — Access Control
Remote Access
Auditable Events

Content Of Audit Records
Audit Storage Capacity
Response To Audit Processing Failures
Audit Monitoring, Analysis, And Reporting
Audit Reduction And Report Generation
Time Stamps
Protection Of Audit Information
Audit Record Retention
Security Assessments
Security Certification
Baseline Configuration
Access Restrictions For Change

Vulnerabilities & Exposures

Identify Vulnerabilities & Rate Potential Exposure (VE)

Vulnerability – a weakness that can be exploited by one or more threats that could impact an asset. Vulnerabilities are paired with specific threats.

- Inadequate fire prevention
- Disposal/re-use of storage media
- Excessive authority
- Inadequate asset classification
- Inadequate/insufficient testing
- Inadequate access control
- Lack of security awareness
- Poor segregation of duties
- Lack of third party contracts
- Lack of protection from viruses
- Lack of information back-up
- Inadequate control of visitors
- Lack of termination procedures
- Insufficient security controls testing
- Inadequate physical protection
- Located in Flood/tornado zone

RiskBased SECURITY

Vulnerability Exposure (VE) Descriptions

Vulnerability Exposure (VE)	Description
Very High (5.0)	The vulnerability is very easy to exploit and the asset is completely exposed to external and internal threats with few if any security controls in place; (Requires drastic action to safeguard the asset and immediate attention to implementing security controls.)
High (4.0)	The vulnerability is easy to exploit and the asset is highly exposed to external and internal threats with only minimal security controls in place; (Requires immediate action to safeguard the asset and near-term implementation of security controls.)
Medium (3.0)	The vulnerability is moderately exposed to both internal and external threats and the security controls in place to protect the asset are limited and/or are not regularly tested. (Requires immediate attention and safeguard consideration in the near future)
Low (2.0)	The vulnerability is easy to exploit and the asset is highly exposed to external and internal threats with only minimal security controls in place; (Requires immediate action to safeguard the asset and near-term implementation of security controls.)
Very Low (1.0)	The vulnerability is very hard to exploit or the security controls in place to protect the asset are very strong

RiskBased SECURITY

Calculating Risk Scores

Calculate Risk Scores & Prioritize AV x (TL x VE)

$$\text{Risk} = AV \times (TL \times VE)$$

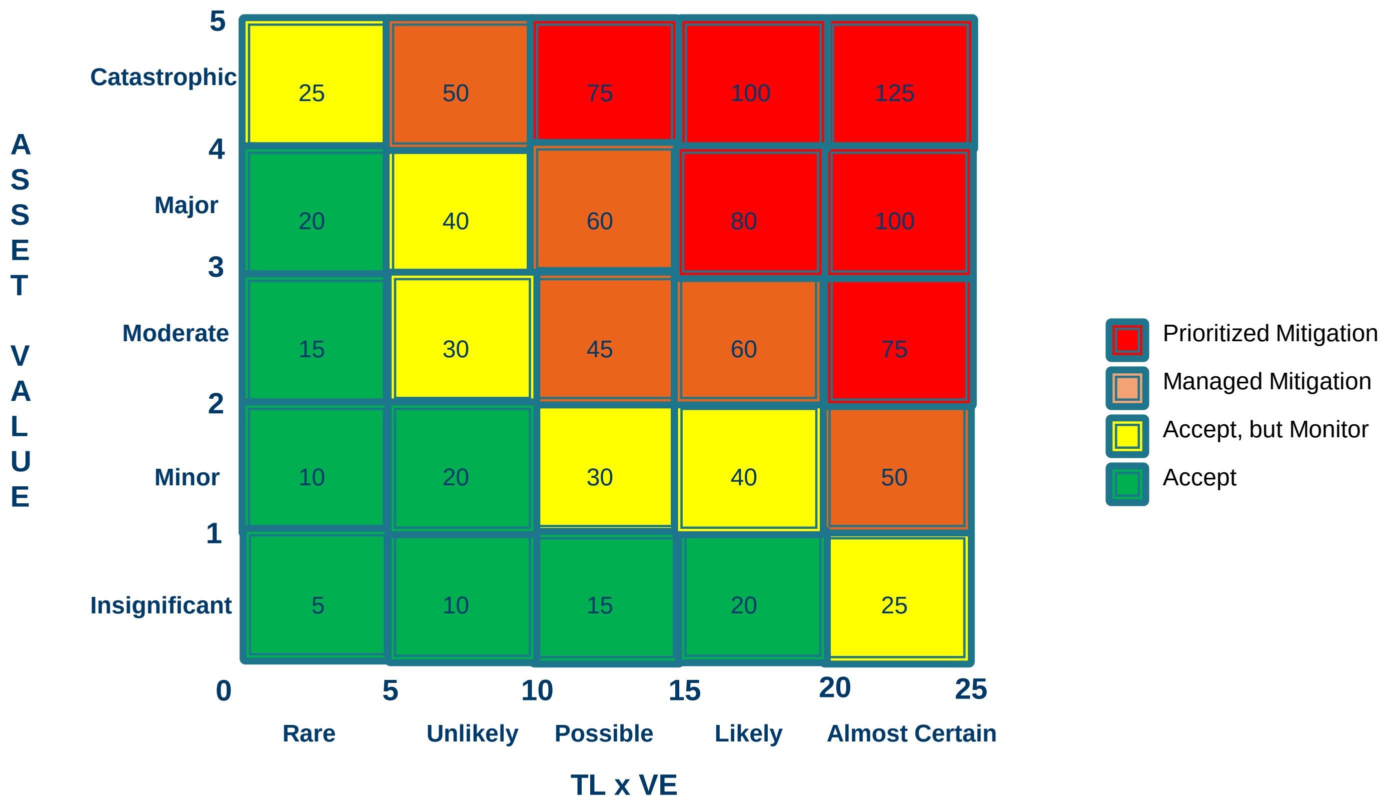
Asset ID#	Asset Description	Asset Value (AV)	Threat	Threat Likelihood (TL)
				5 Very High;
				4 High;
				3 Medium;
				2 Low;
				1 Very Low
					Vulnerability	Vulnerability Exposure (VE)
						5 Very High;
						4 High;
						3 Medium;
						2 Low;
						1 Very Low
							Risk Score
							AV x TL x VE

Calculating Risk Scores

Calculate Risk Scores & Prioritize AV x (TL x VE)

$$\text{Risk} = AV \times (TL \times VE)$$

$$(1\text{-}5) \times [(1\text{-}5) \times (1\text{-}5)]$$



ASSET VALUE	Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic	🟨 25	🟧 50	🟥 75	🟥 100	🟥 125
Major	🟩 20	🟨 40	🟧 60	🟥 80	🟥 100
Moderate	🟩 15	🟨 30	🟧 45	🟧 60	🟥 75
Minor	🟩 10	🟩 20	🟨 30	🟨 40	🟧 50
Insignificant	🟩 5	🟩 10	🟩 15	🟩 20	🟨 25

- 🟥 Prioritized Mitigation
- 🟧 Managed Mitigation
- 🟨 Accept, but Monitor
- 🟩 Accept

Calculating Risk Scores

Calculate Risk Scores & Prioritize AV x (TL x VE)

Risk = AV x (TL x VE)

Threats & Vulnerabilities		Asset Value [Security Impact]				
Threat Likelihood	Vulnerability Exposure	Very Low	Low	Medium	High	Very High
High	High	M	M	H	H	H
	Medium	L	M	M	H	H
	Low	L	L	M	M	H
Medium	High	L	L	M	M	H
	Medium	L	L	L	M	M
	Low	L	L	L	L	M
Low	High	L	L	L	L	M
	Medium	L	L	L	L	M
	Low	L	L	L	L	L

Developing Risk Treatment

Develop Risk Treatment Plans to Mitigate Risk

Risk Treatment Plan

Risk Calculation	Risk Treatment:
	• Avoid,
	•Transfer,
	•Accept or
	•Control
		Rationale if Avoiding, Transferring or Accepting Risk	Control to Mitigate Risk	New Vulnerability Exposure (NVE) after Controls
				5 Very High;
				4 High;
				3 Medium;
				2 Low;
				1 Very Low
					New Risk Calculation with Additional Control	Mitigation Action	Action/ Control Owner	Target Implementation Date

Reviewing Residual Risk

Define & Accept Residual Risk

The quantity of risk left over at the end of a risk treatment process.

- It is management's responsibility to set their company's acceptable risk level.
- As a security professional, it is our responsibility to work with management and help them understand what it means to define an acceptable level of risk.
- Each company’s acceptable risk level is derived from its legal and regulatory compliance responsibilities, its threat profile, and its business drivers and impacts.

RiskBased SECURITY

Risk Assessment Report

Risk Assessment Report

EXECUTIVE SUMMARY

I. INTRODUCTION

– Purpose
– Scope of Risk Assessment

II. SYSTEM CHARACTERIZATION

– Mission Description
– Security Requirements
– People & Users
– Physical Perimeters
– Logical Perimeters
– Network Diagram
– Critical Information Assets

III. RISK ASSESSMENT APPROACH

– Introduction
– Methodology
– Project Participants
– Information Gathering Techniques
– Information Assets Impact Analysis
– Threat Identification & Likelihood Determination
– Control Analysis & Vulnerability Exposure Determination
– Risk Calculations
– Prioritized Mitigation Actions

RiskBased SECURITY

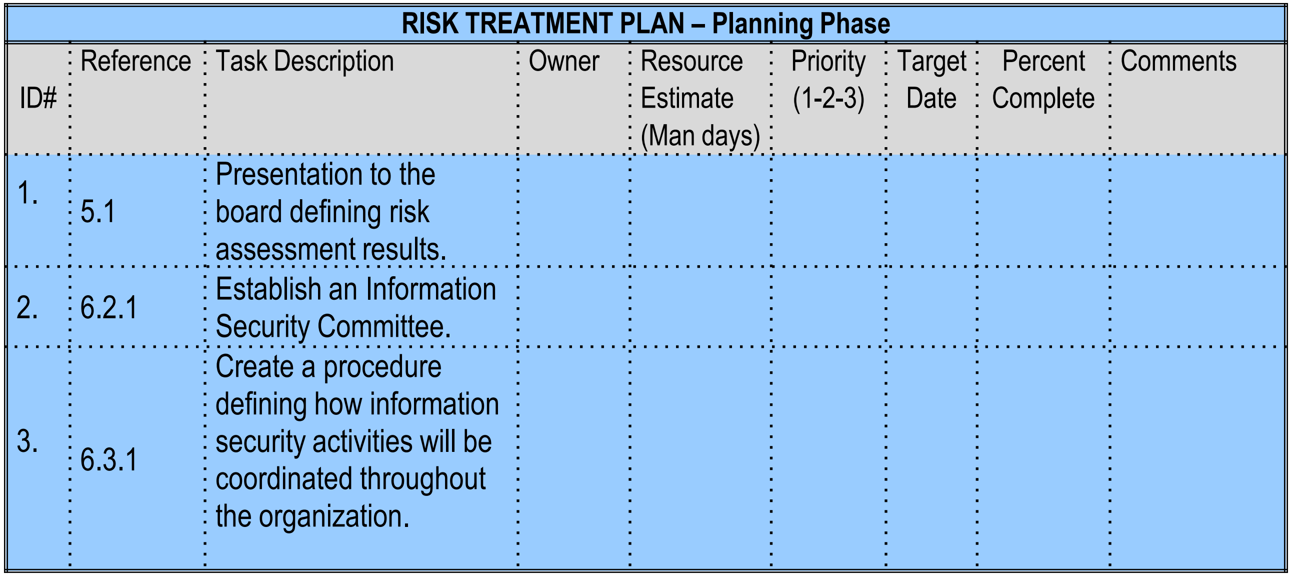
Risk Assessment Report

IV. RISK ASSESSMENT RESULTS

- – Business Owner Threat Analysis
- – Previous Risk Assessment Mitigation Actions
- – Policy and Procedure Review
- – Security Control Test Plan Review
- – Vulnerability Scan Results
- – Mitigation Actions Summary
- – Overall Level of Risk
- – Acceptable Level of Risk
- – Conclusions

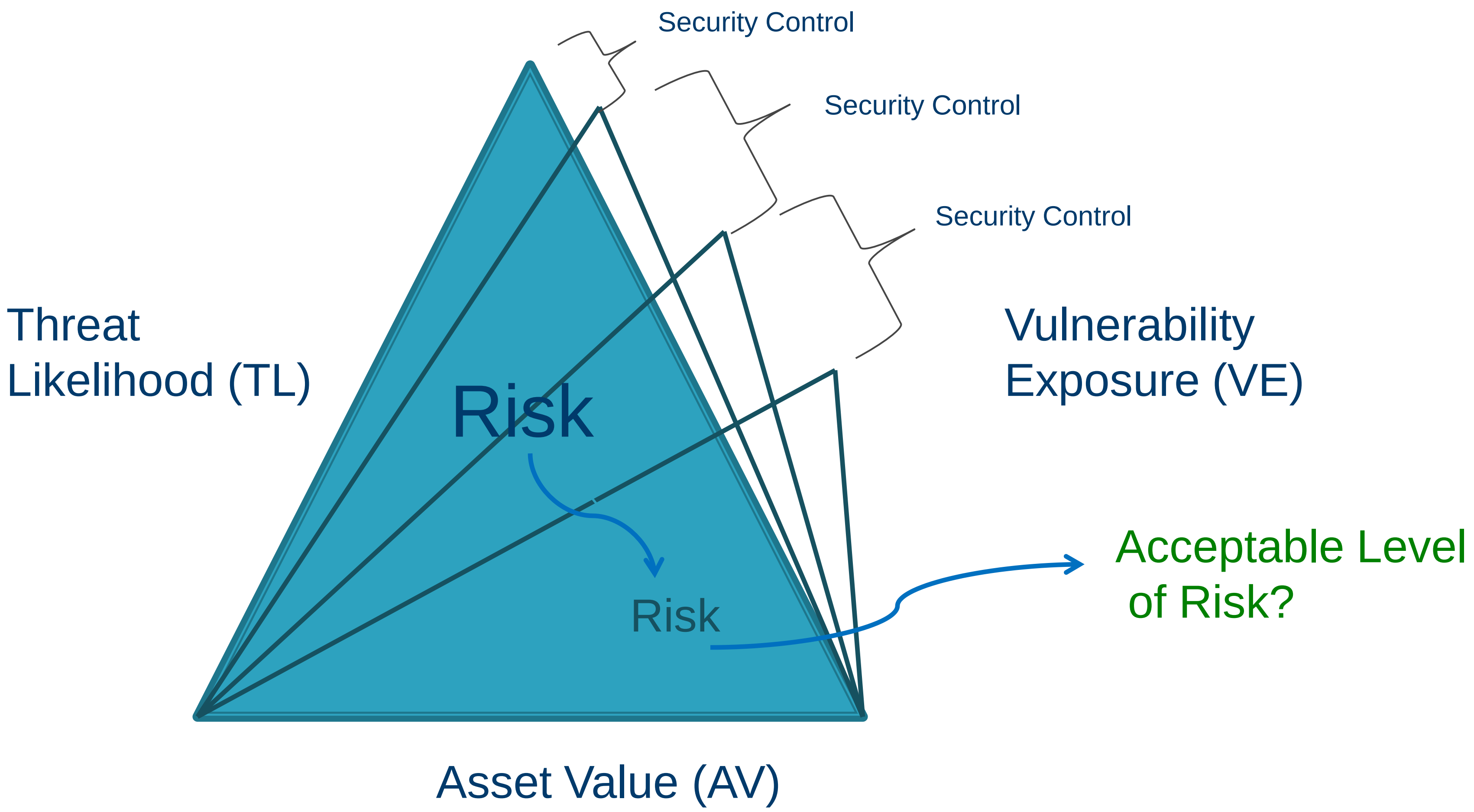
RiskBased SECURITY

Implementing RTPs



RISK TREATMENT PLAN – Planning Phase								
ID#	Reference	Task Description	Owner	Resource Estimate (Man days)	Priority (1-2-3)	Target Date	Percent Complete	Comments
1.	5.1	Presentation to the board defining risk assessment results.						
2.	6.2.1	Establish an Information Security Committee.						
3.	6.3.1	Create a procedure defining how information security activities will be coordinated throughout the organization.						

Risk Mitigation Triangle



Lessons Learned

- All business processes do not have the same impact;
- Critical information assets include more than just the IT assets;
- All information assets are not ‘valued’ the same;
- Risk scores help to prioritize control decisions;
- Lowering risk scores is a cost – benefit exercise;
- It is important for business and IT to acknowledge the responsibility for risk ownership;
- Risk requires consistent terminology to discuss and measure; and
- Risk assessment is the foundation to better decision making.

Remember …

- Risk assessment is about Direction and NOT Perfection.

“There is no perfect risk assessment. We don’t have enough time or money to consider every threat and vulnerability and even if we did the assessment is still obsolete as soon as the report is published.”

Thank you for your attention

Not just security, the right security.

For more information …

Contact:

Barry L. Kouns
Risk Based Security, Inc.
Email: barry@riskbasedsecurity.com