Risk Assessment – the Heart of Risk-based Security

BARRY KOUNS
CEO AT RISK BASED SECURITY

RiskBased SECURITY

Session Overview

- Warm-up Quiz
- Introduction to our security challenge
- What is Risk-based Security?
- The language of risk – some definitions
- What role does a risk assessment play?
- Risk Mitigation Triangle
- The process of risk assessment
- Lessons Learned

Ready for a Quiz?

True or False?

1. Conducting a risk assessment is optional for most organizations. **False**
2. As long as we "check-the-box" and are compliant with legal, regulatory and contractual requirements, we should be good. **False**
3. Risk assessments can often focus on business processes, or groups of assets rather than individual assets. **True**
4. A risk-based approach to information security works best if it involves stakeholders from throughout an organization. **True**
5. Risk assessments are plagued by subjectivity which means they simply cannot be relied upon. **False**
6. A risk-based security program should be closely aligned with the goals of the organization. **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 both positive and negative. **True**
13. A risk-based strategy applies more security resources to your most sensitive assets. **True**

How did you do?

Introduction to our Challenge

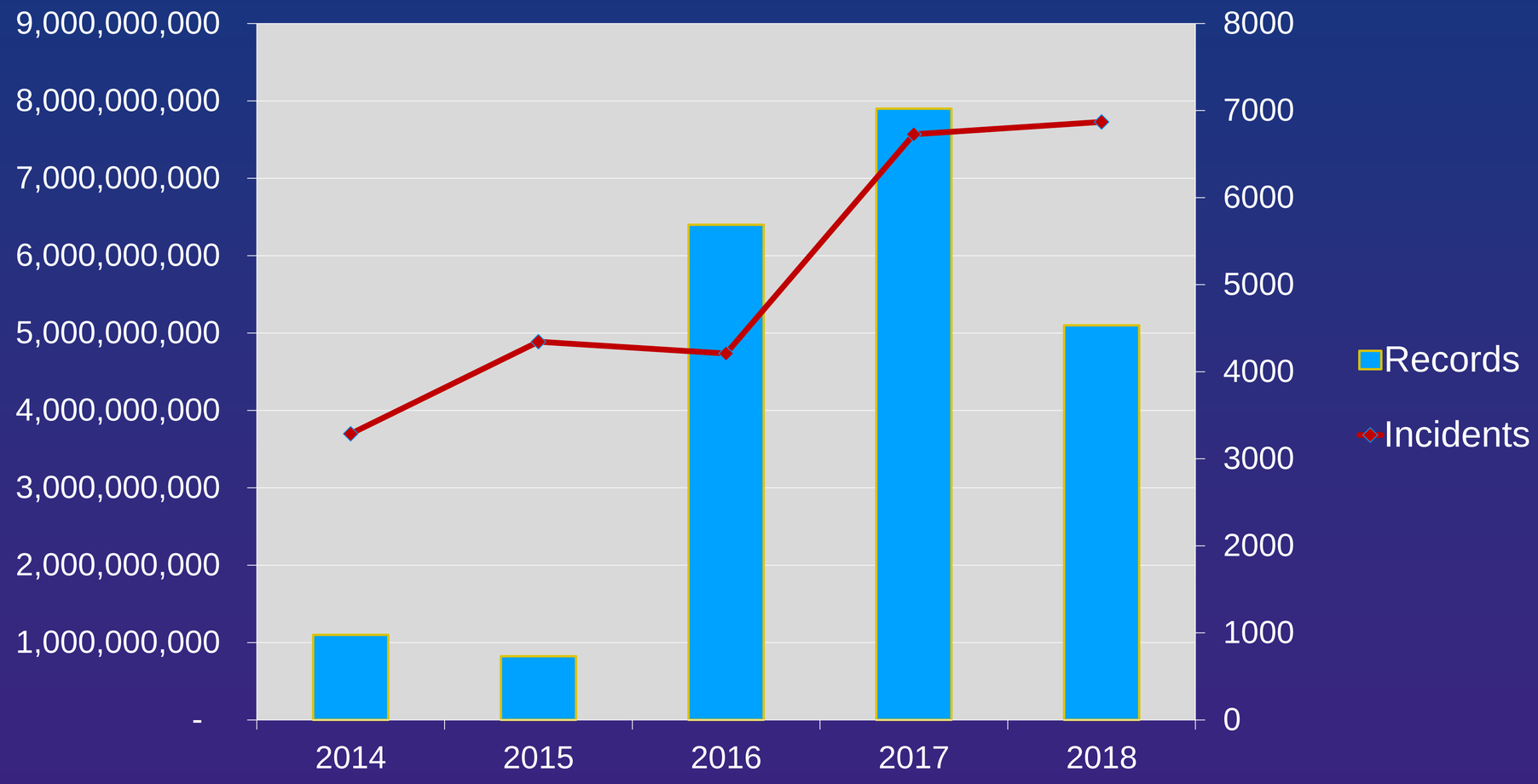
Everyone has information security risk.

But the risk is even bigger than we think.

RiskBased SECURITY

RISKBASEDSECURITY.COM

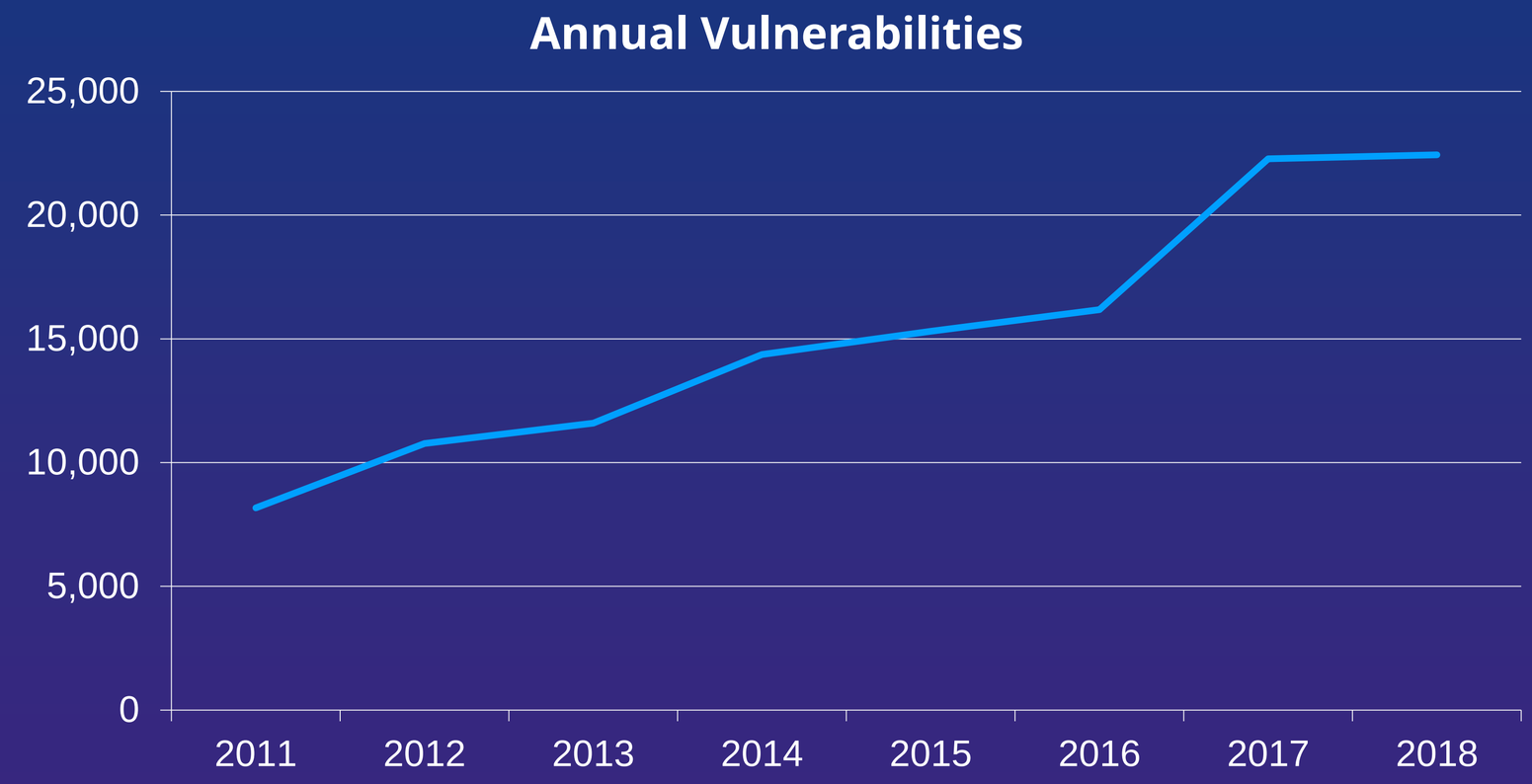
Data Breaches



40,419 Beaches All Time

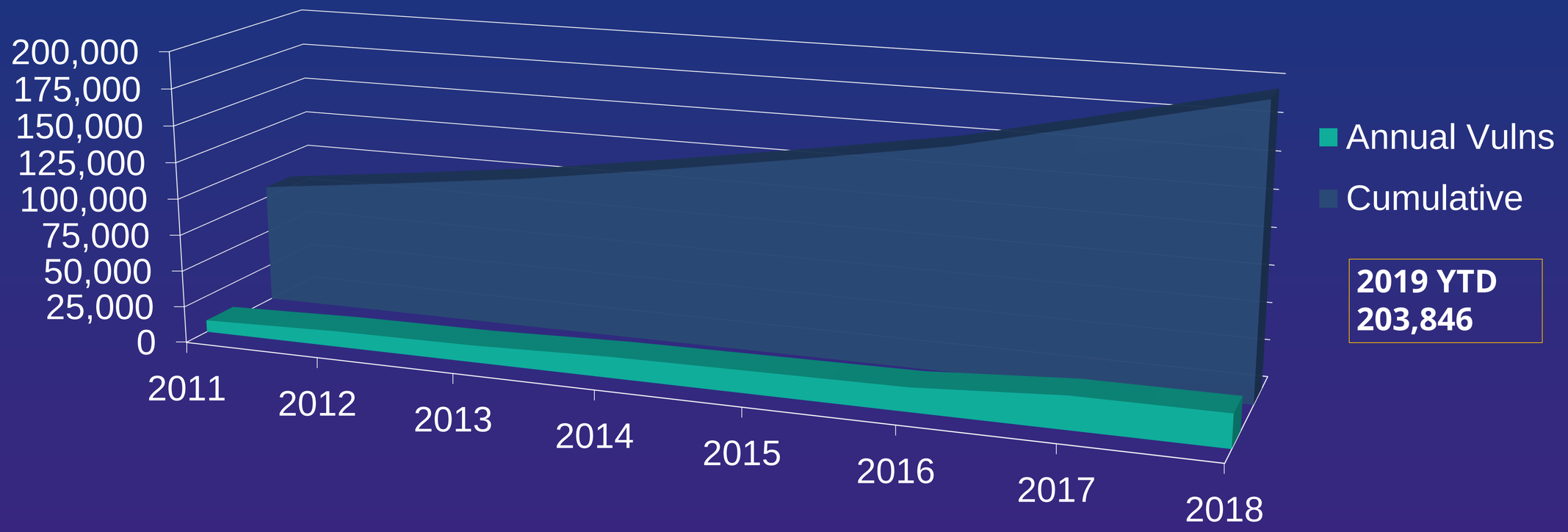
2019 YTD: 3,004 Breaches and 2.7 Billion Records

Software Vulnerabilities



2019 YTD 8,319

Software Vulnerabilities



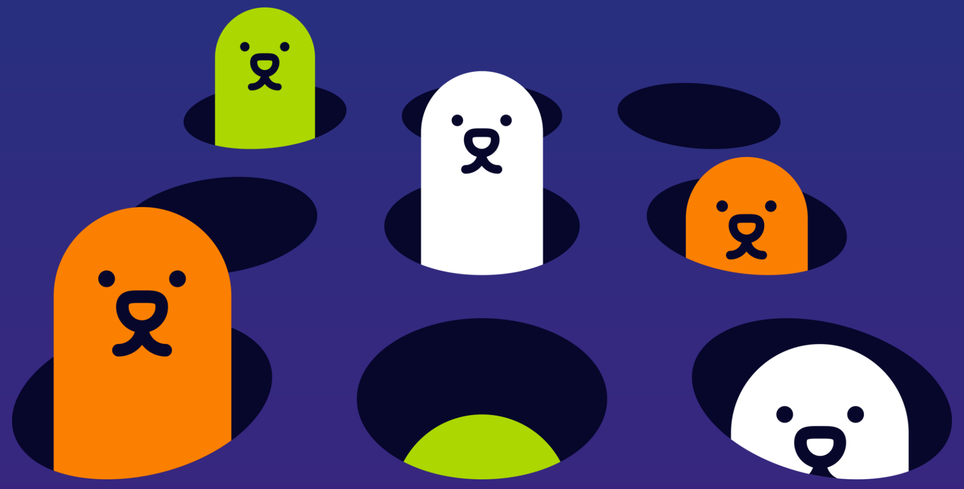
The problem: **more risk than money…**

But it's even *worse...*

Most organizations lack a formal risk assessment process and are forced to be reactive or arbitrary when applying security controls.

…leading to ineffective security programs.

We need to evolve beyond Information Security
“Whack a Mole”



We need to make sure we focus on the “assets” that matter, and;

The greatest threats to our organizations.

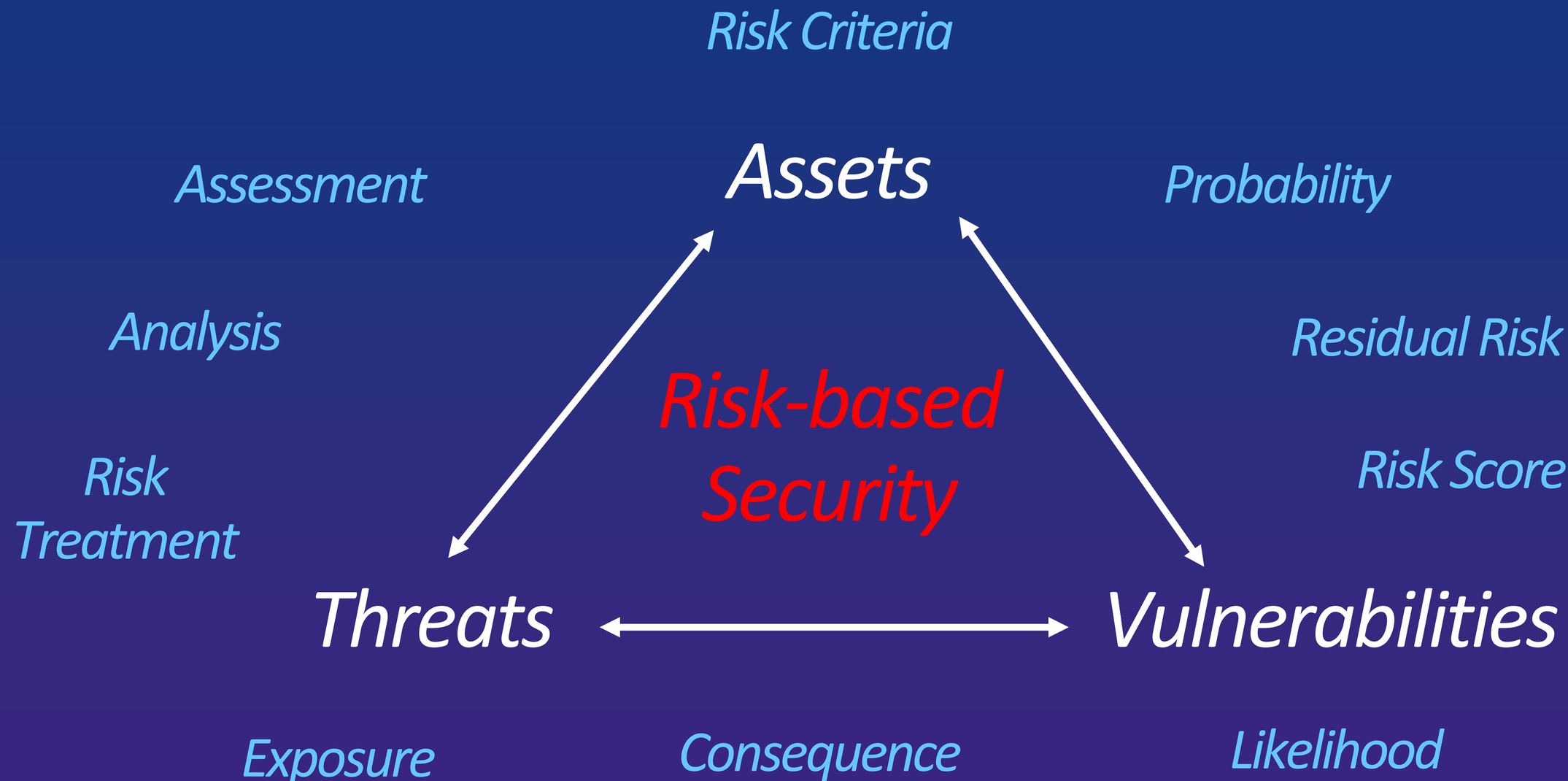
Information security teams need to implement
risk-based security.

What do we mean by
risk-based security?

Risk-based security identifies the true risks to an organization's most valuable assets and directs spending where it's needed most.

A risk-based approach performs an assessment of the threats facing an organization and the vulnerabilities in its current operating environment.

How do we move this concept forward, **and make some real progress?**


Risk Criteria
Assets
Assessment
Probability
Analysis
Residual Risk
Risk-based Security
Risk Treatment
Risk Score
Threats
Vulnerabilities
Exposure
Consequence
Likelihood

A risk-based security approach,

speaks the language of risk assessment.

(And Information Security)

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 27002:2013

Physical assets

- Computer equipment/infrastructure
- Communication equipment
- Non IT equipment
- Furniture / fixtures/storage media

Information assets

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

Software assets

- Application/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

ISO/IEC 27002:2013 defines Information Security as the preservation of:

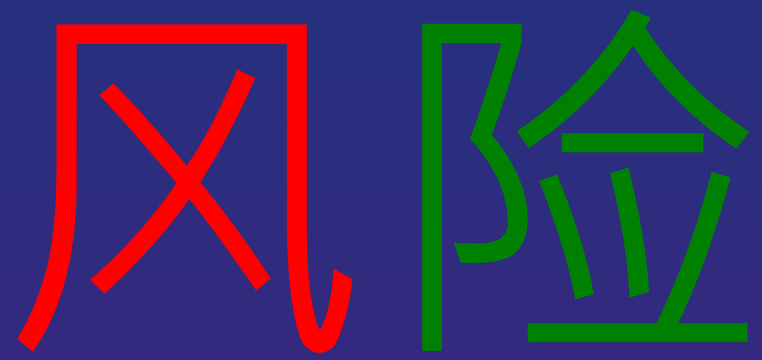
Confidentiality

Information Security

Integrity

Availability

Chinese Definition of Risk



Danger + Opportunity

My Personal Definition of Risk

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

Calculating Risk

Risk – a combination of consequence and probability

Consequence – The impact to the organization's assets of a potential breach to an asset's Confidentiality, Integrity or Availability. [Asset Value (AV)]

X

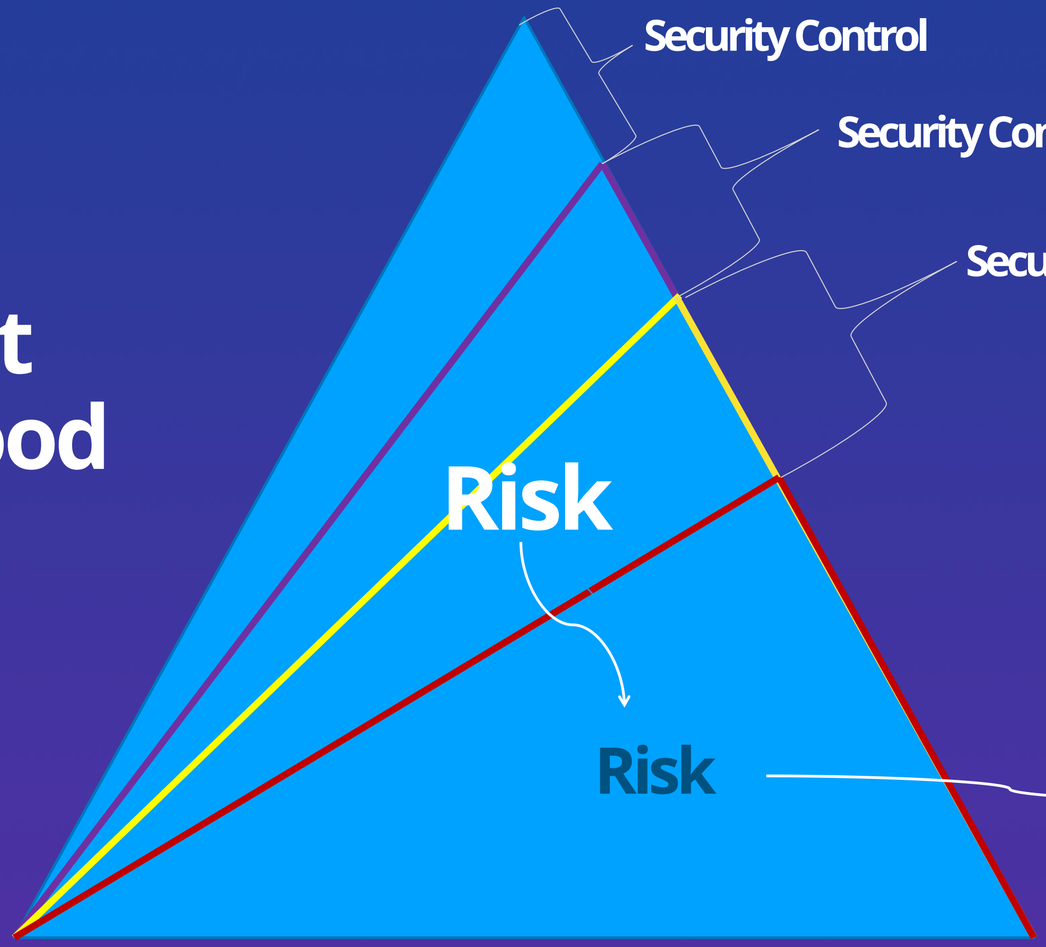
Probability – Likelihood of a threat occurring. (TL)

X

The probability of a Vulnerability Exposing an asset to the threat . (VE)

	Consequence	X	Probability
Risk =	AV	x	(TL x VE)

Risk Assessment Triangle



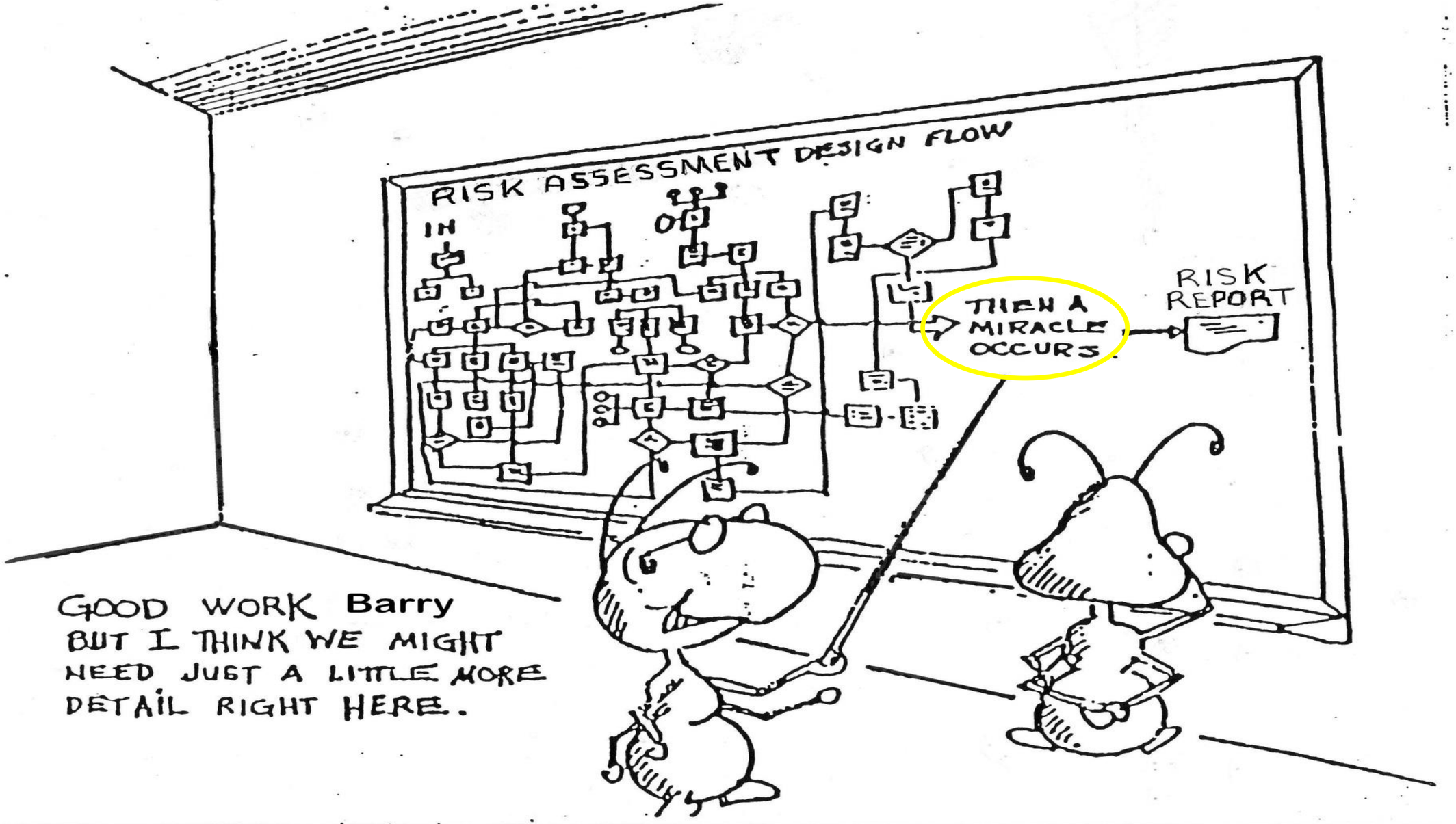
Threat Likelihood (TL)

Vulnerability Exposure (VE)

Acceptable Level of Residual Risk?

Asset Value (AV)

The Risk Assessment Process


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.

Risk Assessment Process

Purpose, Scope & Context

Risk Assessment

- ID and Prioritize Assets
- ID Threats (TL)
- ID Vulnerabilities (VE)
- Calculate Risk Scores
- Compare to Risk Criteria

Risk Treatment

Accept Residual Risk

Record & Report

Monitor & Renew

Communication

Purpose, Scope & Context

(Identify Critical Business Processes)

- Identify the purpose of the assessment
- Identify the Assessment Scope & Context
  - Business Process/ Department Mission Description
  - Information Flow
  - Security Requirements
  - People & Users
  - Physical & Logical Perimeters
  - Network Diagram
  - Critical Information Asset Inventory
  - Assumptions and constraints
  - Sources of information

Identify Assets & Prioritize by 'Value' (AV)

Yes – It's time to identify all your assets.

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
Cloud Service Provider #1	Confidential	5.0	5.0	5.0	5.0
Marketing Material	Public	1.0	2.0	3.0	2.0

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

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

Threat Likelihood (TL)	Likelihood 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)

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 testing
- Inadequate physical protection
- Located in Flood/tornado zone

Vulnerability Exposure (VE)	Exposure 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

Calculate Risk Scores & Prioritize

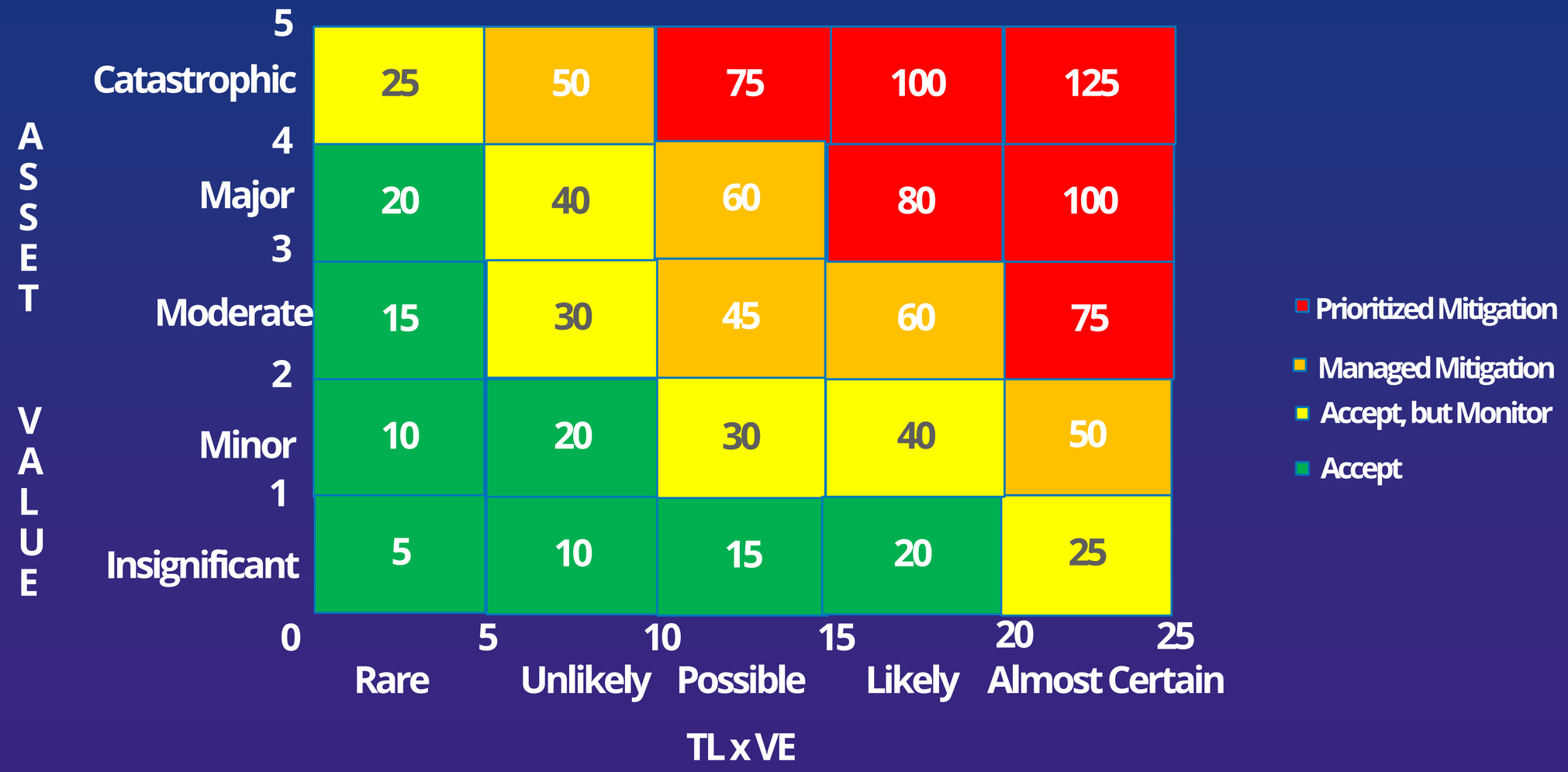
AV x (TL x VE)

Risk = AV x (TL x VE)

Asset ID#	Asset Description	Asset Value (AV)	Threat	Threat Likelihood (TL)	Vulnerability	Vulnerability Exposure (VE)	Risk Score AV x TL x VE
SW001	Server	5 Very High; 4 High; 3 Medium; 2 Low; 1 Very Low	Hacking	5 Very High; 4 High; 3 Medium; 2 Low; 1 Very Low	Late Patching	5 Very High; 4 High; 3 Medium; 2 Low; 1 Very Low	4 x 5 x 5 = 100

Calculate Risk Scores & Prioritize

AV x (TL x VE)



Compare Risk Scores to

'Risk Criteria'

Risk Acceptance Criteria – the amount of risk the organization is willing to accept.

Risk Scores

1 to 125

Risk Treatment

- Avoid
- Transfer
- Control (Reduce)
- Accept

Risk Acceptance Criteria

- Risk Scores <= 40

Develop Risk Treatment Plans to Mitigate Risk

Risk = AV x (TL x NVE)

Risk Score for each asset - threat / vulnerability pair	Risk Treatment: • Avoid, • Transfer, • Accept or Control	Rationale if Avoiding, Transferring or Accepting Risk	Security Control to Reduce 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	Risk Treatment Action	Action/ Control Owner	Target Implementation Date
100			Patch Policy		40			

Risk Register

	Risk Assessment							Risk Treatment Plans							
Asset Description	Asset Location	Asset Value (AV)	Threat	Threat Likeli-hood (TL)	Vuln. Before Security Controls	Vuln. Exposure (VE)	Risk Calc.	Risk Treatment: Avoid, Transfer, Accept or Control	Rationale if Avoiding, Transfer or Accepting Risk	Security Control to reduce risk	New Vuln. Exposure (NVE)	Risk Calc. with Additional Controls	Action	Action/ Control Owner	Target Date
Laptops	Building A	5.0	Theft	4	No security policy	5	100.00	Control	N/A	Alarm	2	40.0	Policy	BK	May-19
Work stations	Main Building	4.0	Hacking	4	No Patch Mgmnt.	5	80.00	Control	N/A	Policy	2	32.0	Training	DB	Jun-18
Server Room	Remote Site	5.0	Fire	4	Poor Physical Security	3	60.00	Transfer	N/A	Insurance	1	20.0	Purchase	JP	Apr-19
DEF Server	Server Room	5.0	Un-authorized access	3	Poor segregation of duties	3	45.00	Accept	Below Risk Criteria	N/A	3	45.0	N/A	JR	N/A
ABC Firewall	Server Room	3.0	Human Error	4	Weak training	3	36.00	Accept	Below Risk Criteria	N/A	3	36.0	N/A	PS	N/A

Accepting Residual Risk

The level 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 to define an acceptable level of risk.
- Each company's acceptable risk level is derived from legal and regulatory compliance responsibilities, its threat profile, and business drivers and impacts.

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

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

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 owners to acknowledge their responsibility for risk ownership;
- Risk requires consistent terminology to discuss and measure; and
- Risk assessment is the foundation of better decision making.

Better Risk Assessments

Better Security Decisions

Risk assessment is NOT about 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.”

NOT JUST SECURITY, THE RIGHT SECURITY.

THANK YOU!

RiskBased SECURITY

Let’s talk more.

Barry Kouns

barry@riskbasedsecurity.com

RiskBased
SECURITY