Threat Modeling & Simulation

Using A Model Based Systems Engineering Approach to Quantify Cyber Risks

Stephen Watkins MS, CISSP
VP & Chief Security Strategist
steve@g2-ops.com

Opening Exercise – Do I provide Cyber Coverage?

- New independent retail client
- Accepts all major Credit Cards
- Provides Health Coverage for 25 employees
- No dedicated Technology staff
- Owner fills out technology questionnaire

What sort of risk does this client present?
What kinds of coverage does this client require?

What is MBSE?

Model-based systems engineering (MBSE) is a systems engineering (SE) methodology that focuses on creating and exploiting domain models as the primary means of information exchange between engineers, rather than on document-based information exchange.

Source: https://en.wikipedia.org/wiki/Model-based_systems_engineering

MBSE Differentiators

	TRADITIONAL SYSTEMS ENGINEERING	MODEL BASED SYSTEMS ENGINEERING
DATA STORAGE	STANDALONE FILE SYSTEMS	SINGLE DATA STRUCTURE (MODEL)
ANALYSIS	TIME CONSUMING TO GATHER DISPARATE SOURCES	SINGLE SOURCE OF TRUTH
EFFICIENCY	TIME CONSUMING	EFFICIENT
IMPACT ANALYSIS	TIME CONSUMING	MODELING & SIMULATION

Source: http://www.businessdictionary.com

MBSE – Building a Data Model

CAPTURE

- Workshops
- Interviews
- Critical Mapping
- Topology Diagrams
- Artifact Discovery

TRANSFORM

- Normalization
- Enrichment
- Data Format Standards
- Data Model

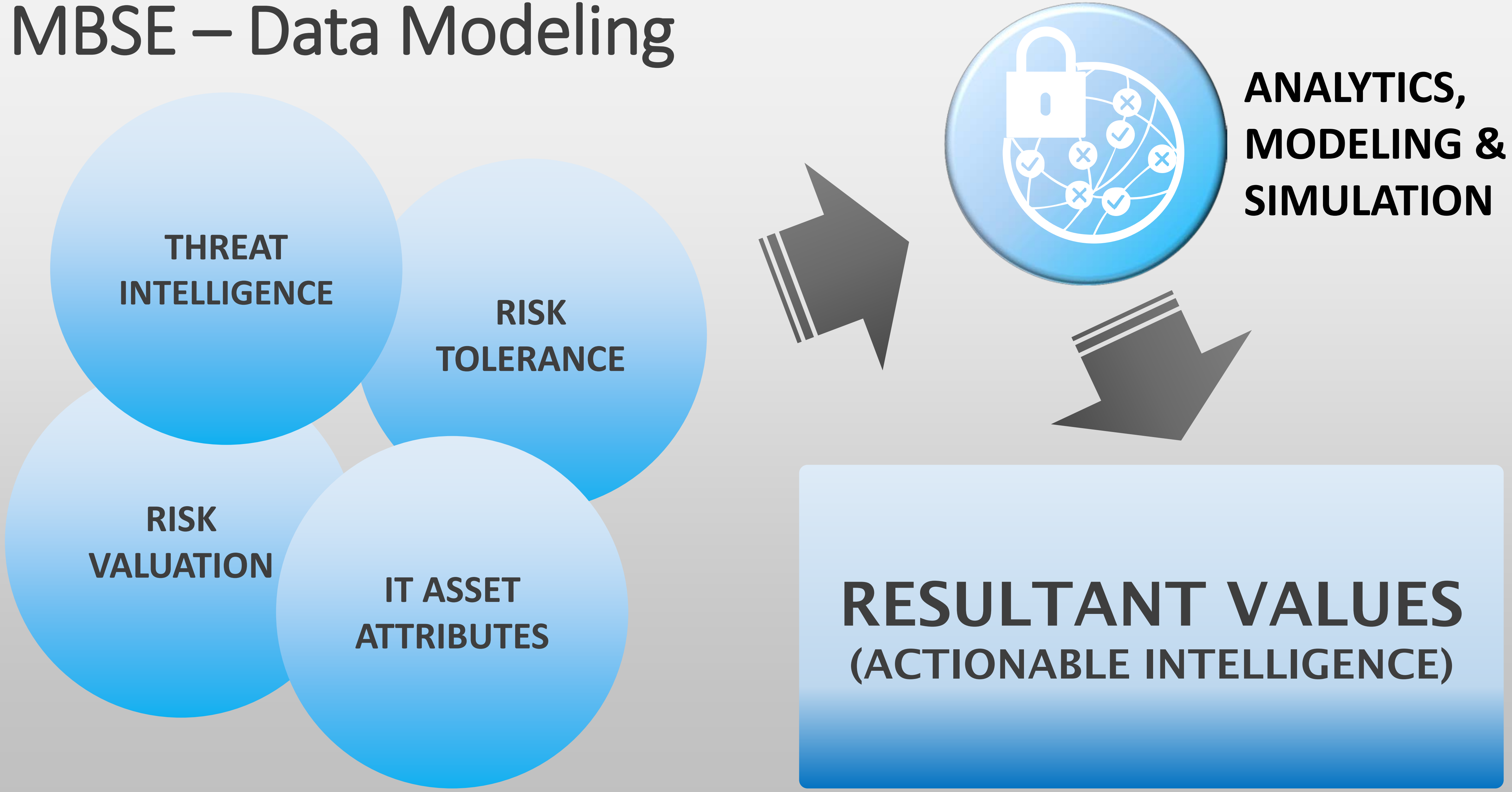
ANALYZE

- Modeling & Simulation
- Risk Analytics
- Loss Value Predictions

VISUALIZE

- Risk Awareness
- Impact Analysis
- Remediation
- Planning
- Operations

MBSE – Data Modeling



THREAT INTELLIGENCE

RISK TOLERANCE

RISK VALUATION

IT ASSET ATTRIBUTES

ANALYTICS, MODELING & SIMULATION

RESULTANT VALUES (ACTIONABLE INTELLIGENCE)

Question: Audience Participation

Which two (2) characteristics describe differentiators between Traditional Systems Engineering and Model Based Systems Engineering?

a) MBSE is a Single Source of Truth

b) Traditional SE is More Efficient

c) MBSE is More Time Consuming

d) Traditional SE is Less Efficient

Answer:
a & d

Business → Risks ← Cyber

Security Principles

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

Cyber Threat

the possibility of a malicious attempt to damage or disrupt a computer system or network

Source: http://business.simplicable.com/business/new/65-business-risks-list

Quantifying Cyber Risk

THREAT LANDSCAPE

- Types of Adversaries
- Threat Vectors
- Types of Attacks
- Attack Trends

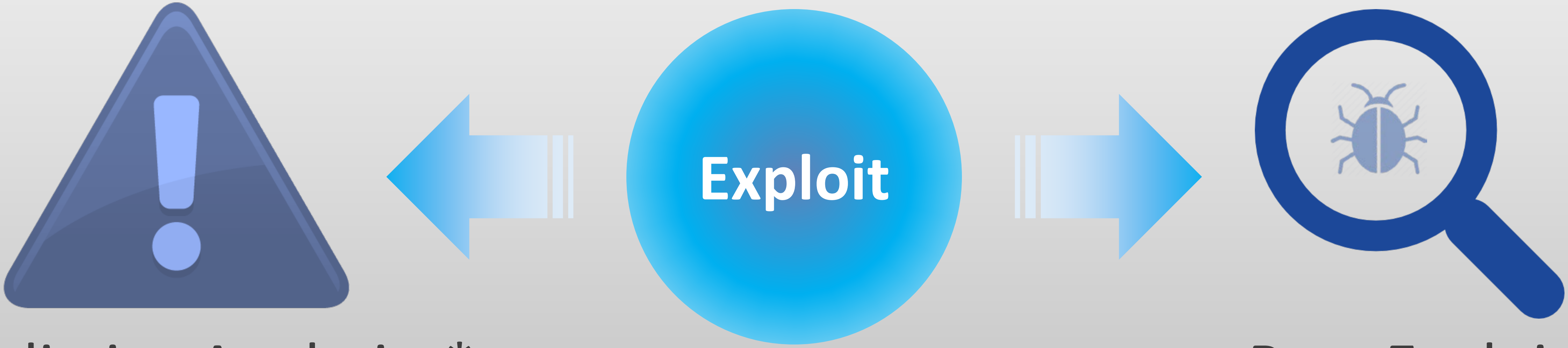
SECURITY POSTURE

- Organizational Vulnerability
- Security Controls
- Remediation
- Awareness & Training

ASSET VALUATION

- Business Value Attribution
- Data Type Association
- Inherent Value
- Loss Value (DBI)

Cyber Security Goal: Identify & Mitigate Risk



Predictive Analytics*

Exploit

Post-Exploit

Risk = Potential for Financial Impact

***Unknown Future Events**

MBSE & Cyber Risk

DATA MODEL

ANALYTICS

POTENTIAL RISK

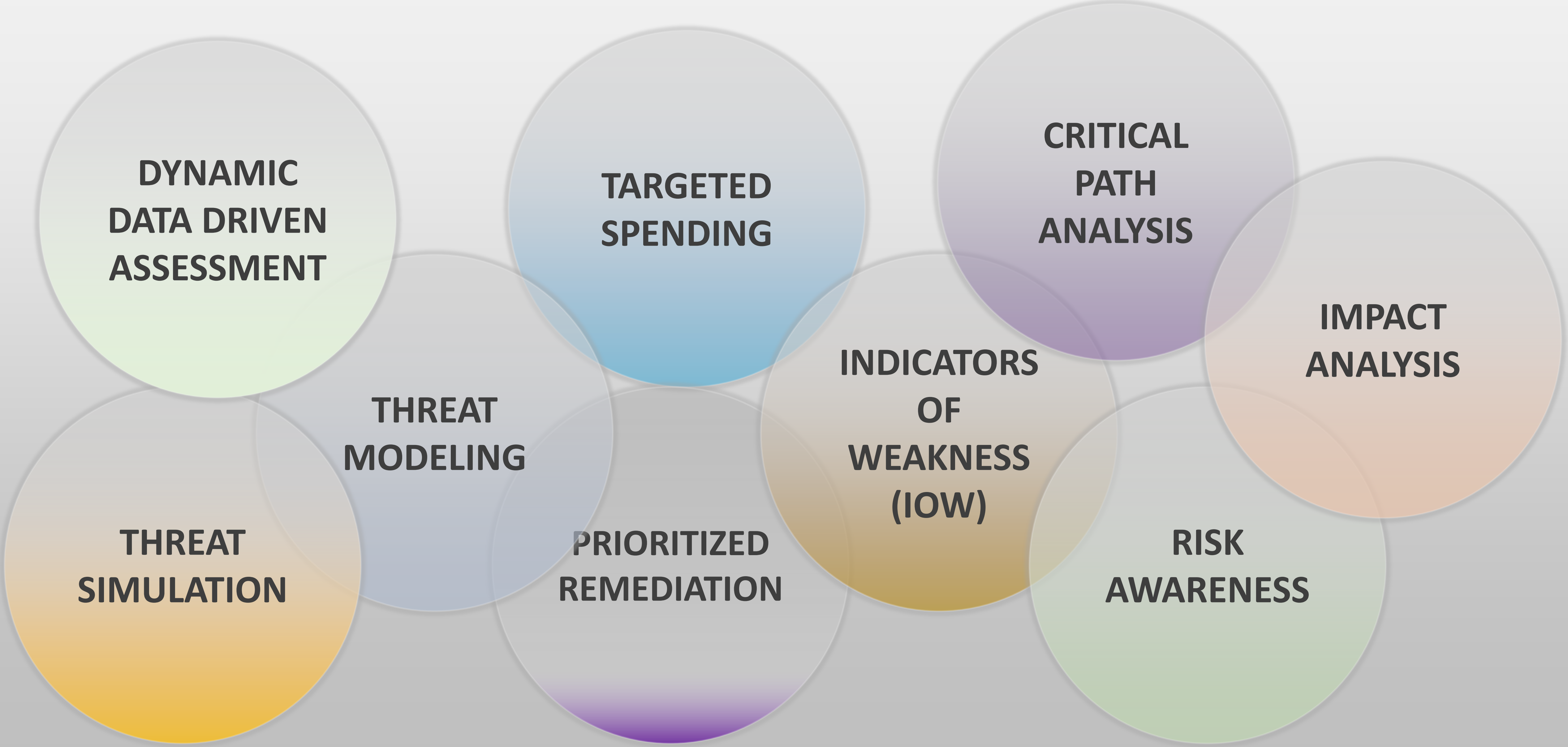
Threat Modeling & Simulation

Digital Twin

Model Change → Updating Data

Simulate Environmental Impact

MBSE & Predictive Analytics



DYNAMIC DATA DRIVEN ASSESSMENT

TARGETED SPENDING

CRITICAL PATH ANALYSIS

IMPACT ANALYSIS

THREAT MODELING

INDICATORS OF WEAKNESS (IOW)

THREAT SIMULATION

PRIORITIZED REMEDIATION

RISK AWARENESS

Question: Audience Participation

True or False: Organizational Security Posture is not an important factor in quantifying an organization’s Cyber Risk.

Answer:
False

Revisiting Initial Exercise

CIA – Protecting Critical Assets

Analyze All Available Information

Make Informed Decisions

Balanced Client Risk Portfolio

Remediate Risk *BEFORE* Events Occur

Reduce Impact of Security Events

Managing Risk With MBSE

MODEL DATA FRESHNESS

- Ingest
- Normalize
- Analyze
- Visualize

VISISBILITY & AWARENESS

- DDAs
- Heat Maps
- Loss Value
- Threat Paths

MODELING & SIMULATION

- On Demand
- Dynamic
- Threat Centric
- Value Ordered

Rinse & Repeat

Holistic Risk Management

BASELINE

- Define a starting point
- Not SAQ
- Security Assessment

MEASURE

- Define metrics
- Simulate Cyber Threats
- Calculate Risk Needle

VISUALIZE

- Cyber Views
- Risk Needle Movement
- Operational Cadence

Question: Audience Participation

Which answer below is NOT meaningful when it comes to using MBSE to manage risk?

a) Keeping the data fresh

b) Understanding the threat landscape

c) Maintaining an unchanging data set

d) Executing multiple simulation scenarios

Answer:
c

Cyber Insurance Challenges

SECURITY POSTURE

SAQs are seldom accurate exposing an organization to rejected claims

OFFER COMPLEXITY

Which coverages cover what and which ones does an organization really need?

HOW MUCH IS ENOUGH?

Risk transfer is a great idea, but how much coverage is appropriate?

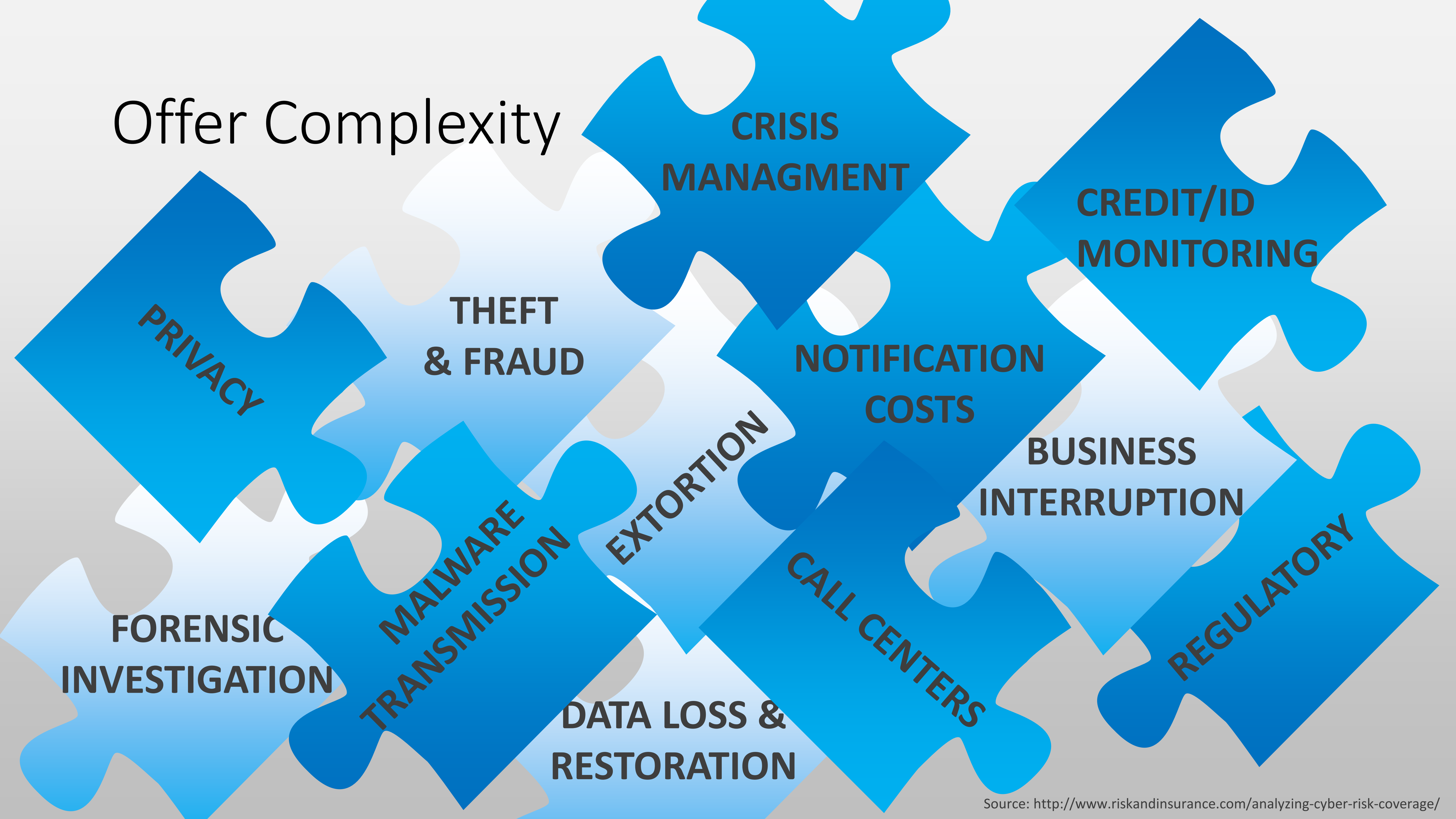
Security Posture

PEOPLE

PROCESS

TECHNOLOGY

Offer Complexity



CRISIS MANAGMENT

CREDIT/ID MONITORING

PRIVACY

THEFT & FRAUD

NOTIFICATION COSTS

BUSINESS INTERRUPTION

EXTORTION

MALWARE TRANSMISSION

CALL CENTERS

REGULATORY

FORENSIC INVESTIGATION

DATA LOSS & RESTORATION

Source: http://www.riskandinsurance.com/analyzing-cyber-risk-coverage/

How Much Coverage?

IT
RISK

#PCI Records x $2.42

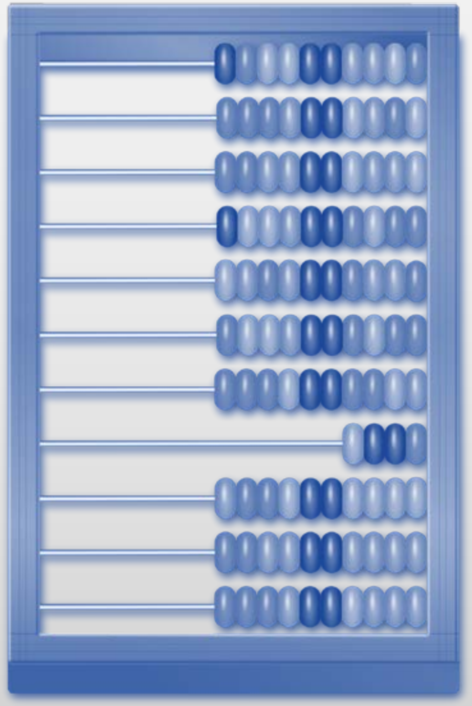
+

#PII records x $16.23

+

#PHI records x $43.92

Total Risk Value?



RISK
VALUE

AN MBSE APPROACH

DATA STRUCTURE

SECURITY POSTURE BASELINE

ANALYTICS

THREAT MODELING & SIMULATION

RISK VISUALIZATION

ACTIONABLE INTELLIGENCE

Thank You!

Stephen Watkins MS, CISSP
VP & Chief Security Strategist
steve@g2-ops.com