DATA BREACH INTELLIGENCE: DOES HISTORY ALWAYS REPEAT ITSELF?

Jake Kouns
Open Security Foundation

Alex Hutton
Zions Bancorporation

Session ID: DSP-F42

Session Classification: Intermediate

About This Talk

- What we want you to get out of it:
  - There is useful data out there
  - There is a better, data-driven way to run a security or risk management program than current standards support
  - There are people actually using data!

About This Talk

- What we hope you'll want to do afterwards:
  - Incorporate data and data science techniques in your security program
  - Not be susceptible to *bias* or *dogma* common in our industry

Does History Repeat Itself?

Does History Repeat Itself?

Figure 8. VERIS A⁴ Grid depicting the frequency of high-level threat events

		Malware			Hacking			Social			Misuse			Physical			Error			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Confidentiality & Possession	381			518		1				9	8	1					2	1			
	Integrity & Authenticity	397			422		1				6	1	1									
	Availability & Utility	2			6						5											
Networks	Confidentiality & Possession										1											
	Integrity & Authenticity	1									1											
	Availability & Utility	1			1						1											
User Devices	Confidentiality & Possession	356			419						1			86								
	Integrity & Authenticity	355			355						1	1		86								
	Availability & Utility										1			3								
Offline Data	Confidentiality & Possession											23							1			
	Integrity & Authenticity																					
	Availability & Utility																					
People	Confidentiality & Possession							30	1													
	Integrity & Authenticity							59	2													
	Availability & Utility																					

Figure 6. A⁴ Grid depicting the frequency of VERIS Threat Events across 2010 caseload

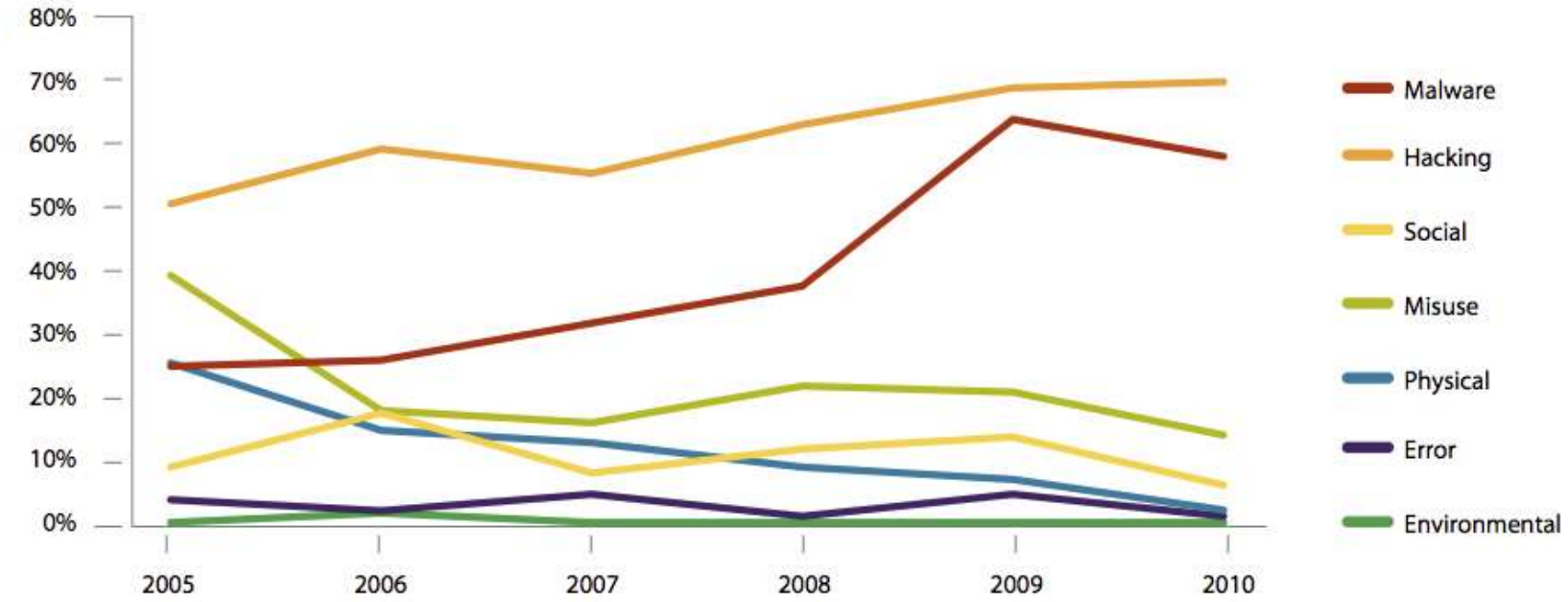
		Malware			Hacking			Social			Misuse			Error			Physical			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Conf	319	1		369						10	50	1			1						
	Poss																					
	Integ	321	1		353	2					3	43										
	Auth	2			16	2					3	16										
	Avail	3			4						2	1										
	Util																					
Networks	Conf	1			1												11					
	Poss																					
	Integ	1			1												11					
	Auth																					
	Avail																					
	Util																					
User Devices	Conf	214	1		174						2	4					201					
	Poss																					
	Integ	214	2		171							3					201	4				
	Auth	2			2												2	1				
	Avail				2												1					
	Util																					
Offline Data	Conf	1										67			1		1					
	Poss																					
	Integ	1																				
	Auth																					
	Avail																					
	Util																					
People	Conf							8	1													
	Poss																					
	Integ							72	24													
	Auth																					
	Avail																					
	Util																					

None | Least frequent | Most Frequent

- 2012
- 2011

Does History Repeat Itself?

Figure 16. Threat action categories over time by percent of breaches (Verizon cases)



Does History Repeat Itself?
Data says “Pretty Much”

Session ID:

Session Classification:

Does History Repeat Itself?

Data says “Pretty Much”

TYPES OF SECURITY PROFESSIONALS (as they approach the use of data)

Types of Security Professionals

- We don't have any data!

Types of Security Professionals

- We don't have perfect data!

Types of Security Professionals

- Data is great as long as it supports my decisions!

Types of Security Professionals

- We have all the data we need!

Types of Security Professionals

Types of Security Professionals

- We have too much data to handle!

THE CASE FOR DATA

Session ID:

Session Classification:

THE CASE FOR DATA

What Is Risk Management

- Risk Management is about decisions
- Being able to clearly communicate risk decisions

Data helps us discuss the situation with a certain ***focus***

Focus

Why do we need that focus?

Kouns/Hutton Security Metric Axiom 1

- Any security metric you present will ***always*** be interpreted in a risk model.
  - Either **formal** modeling
  - Or **informal** (gut-level interpretation) modeling

Kouns/Hutton Security Metric Axiom 2

- Without instituting ***rational*** decision making efforts, that risk model is subject to a myriad of cognitive biases
  - Gut-level interpretation (informal modeling) ***rarely*** accounts for these biases

Decisions Can Be Made By Many Means

Some are proven better than others;

- Usually, the more rational the better
- The less rational, the more susceptible to bias
- Bias can lead us to worry about the wrong things

BACK STORY

WHAT SHOULD YOU REALLY BE AFRAID OF?

Fear, as FDR noted in 1933, paralyzes those who succumb to it. And yet much of what we worry about today is based on hype rather than reality. Yes, media headlines are partially to blame. But some things (sharks!) are just downright scary. Using the most recent U.S. data available, we hereby present a list of unsettling threats and their far riskier counterparts.

MURDERS (2008) **14,180**	SUICIDES **33,289** (2008)
CHILDREN ABDUCTED BY STRANGERS (1999) **115**	CHILDREN WHO DROWN IN POOLS **288** (2008)
BURGLARIES (2007) **2.2 MILLION**	IDENTITY THEFTS **8.3 MILLION** (2005)
SHARK ATTACKS (2009) **28**	DOG BITES **4.5 MILLION***
AMERICANS KILLED BY TERRORIST ATTACKS AROUND THE WORLD (2008) **33**	AMERICANS WHO DIE FROM THE SEASONAL FLU **36,171***
DEATHS BY ALLERGIC REACTION TO PEANUTS **50–100***	DEATHS BY UNINTENTIONAL POISONING **27,531** (2006)
WOMEN WHO DIE FROM BREAST CANCER (2009) **40,170**	WOMEN WHO DIE FROM CARDIOVASCULAR DISEASE **432,709** (2008)
FATAL AIRLINE ACCIDENTS (2005) **321**	FATAL CAR CRASHES **34,017** (2008)
AMERICANS AUDITED BY THE IRS (2009) **1.4 MILLION**	U.S. DEATHS **2.4 MILLION** (2007)

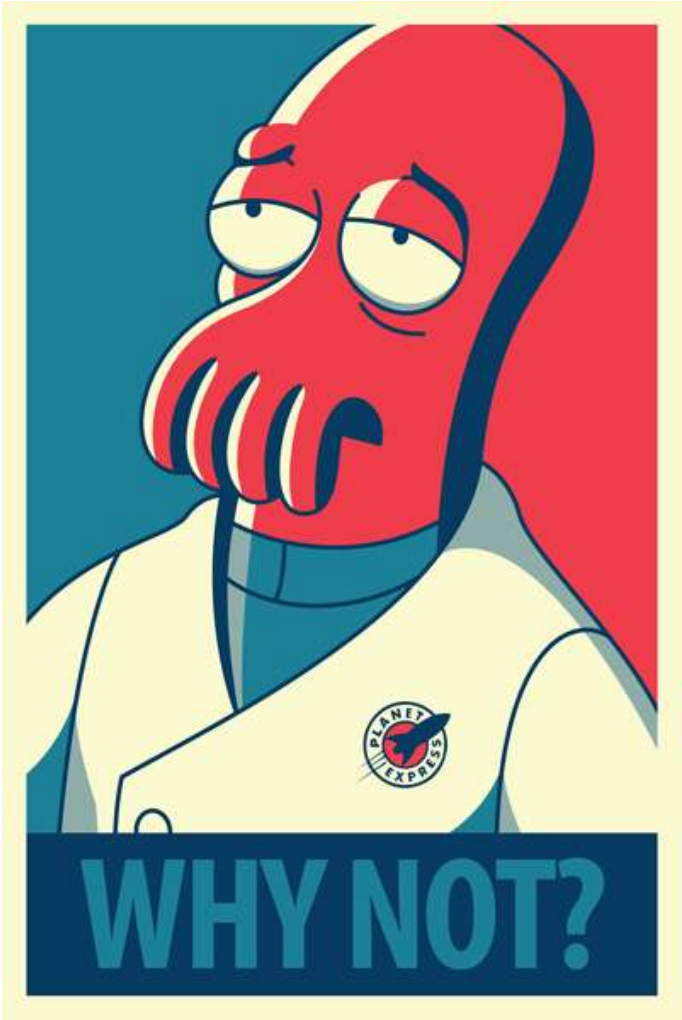
* ANNUAL AVERAGES AND ESTIMATES

SOURCES: AMERICAN CANCER SOCIETY; AMERICAN HEART ASSOCIATION; CENTERS FOR DISEASE CONTROL AND PREVENTION; CONSUMER PRODUCT SAFETY COMMISSION; FEDERAL TRADE COMMISSION; INTERNAL REVENUE SERVICE; INTERNATIONAL SHARK ATTACK FILE; NATIONAL COUNTERTERRORISM CENTER; NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION; NATIONAL TRANSPORTATION SAFETY BOARD; NEW ENGLAND JOURNAL OF MEDICINE; U.S. DEPARTMENT OF JUSTICE

BY NUMBER 17, NYC, CLAUDIA KALB, AND ELIZABETH WHITE

Evidence-Based Decisions – The Bias Killer!

- If you're looking for something to make decisions more objective, why not use data?



Evidence-Based Practices

- EBPs are driven by data
- They are our most:
  - Rational, Logical, Ethical
- Means of making decisions
- The key to identifying, resisting, and/or challenging bias
- The institution of scientific method in decision making

EVIDENCE-BASED RISK MANAGEMENT (EBRM)

Session ID:

Session Classification:

Why Not Use Evidence?

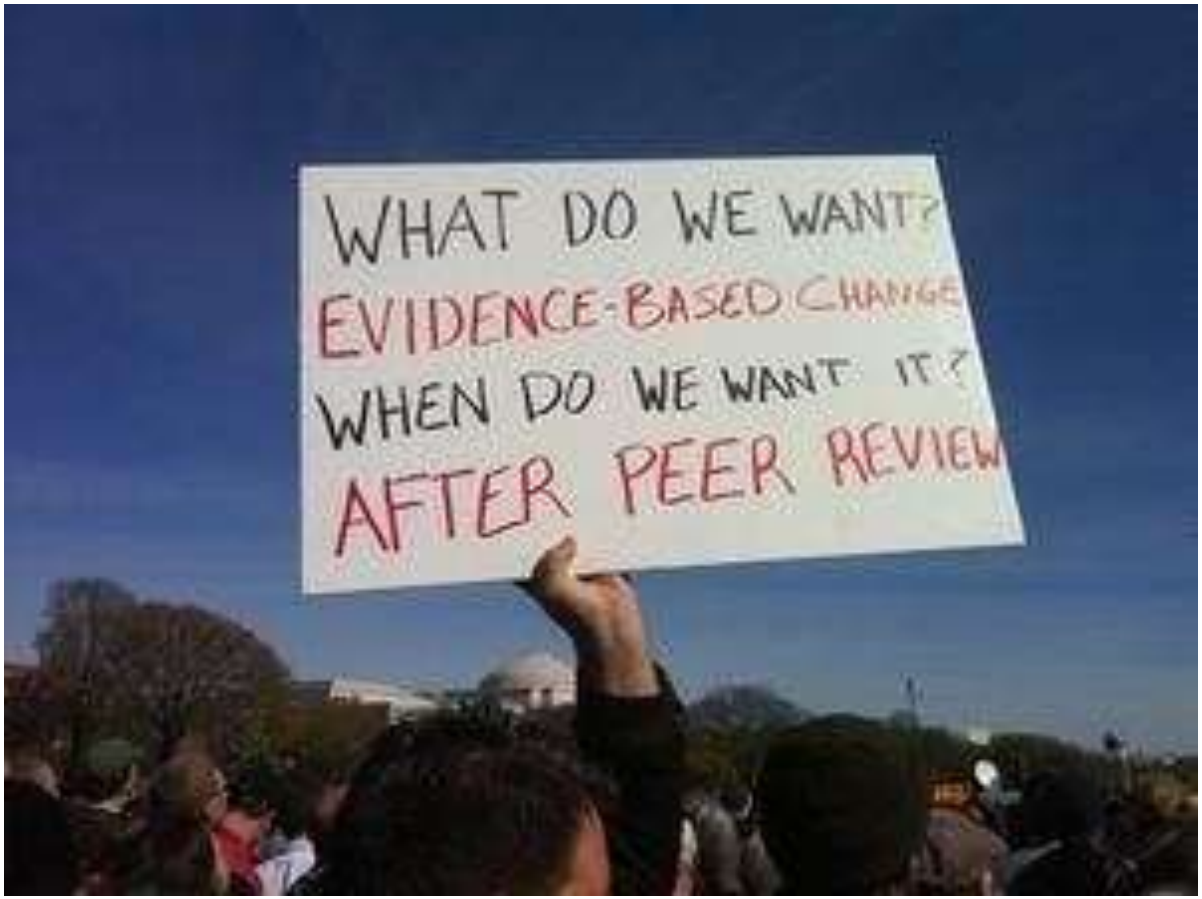
- So if the best decisions are evidence-based;
  - Why not evidence-based risk management?
  - EBRM might be inevitable, see Axiom 1

CAN OUR INDUSTRY *DO* EVIDENCE-BASED RISK MANAGEMENT (EBRM)?

Session ID:

Session Classification:

First, We Have To Want It.



We Must Demand Systemic Change

- Regulatory Agencies & Standards Bodies Have to:
  - Dictate Taxonomy/Ontologies
  - Enforce Data Collection & Analysis (Hypothesis development) as a Key Control
  - Demand and Review for influence of a Feedback Loop

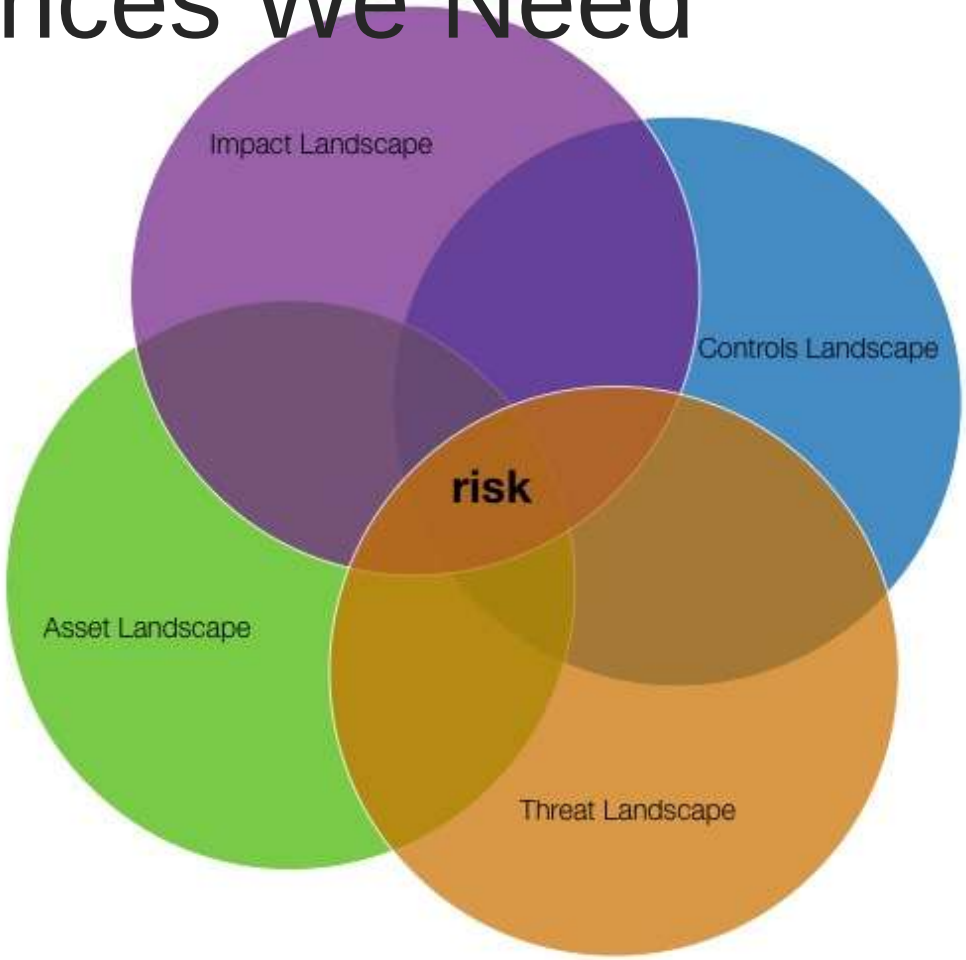

We Must Also
Be Brave
Enough To Start
With Ourselves
Change our own program because it's the right thing to do for us, and for our organization.

What do we need for (EBRM)?

What Do We Need For EBRM?

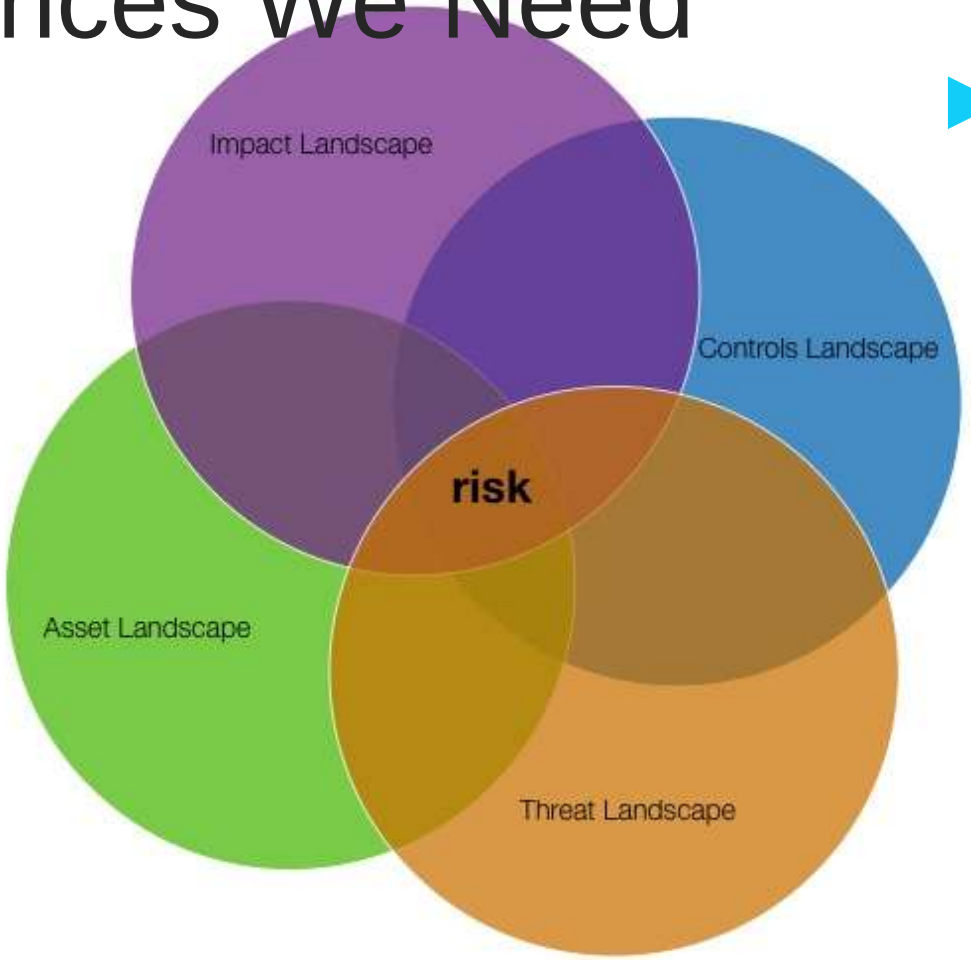
- Understand what evidences we need
- Understand the quality of those evidences

Evidences We Need



including capabilities (skills, resources, decision quality...)

Evidences We Need



- Again, Taxonomies/ Ontologies that describe these sets of information

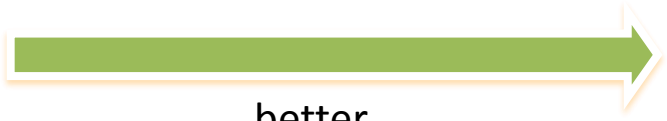
including capabilities (skills, resources, decision quality...)

Quality Of Evidences

- We can borrow from the UK Evidence-Based Medicine quality descriptions and ratings
- Deduction and Inference can help

Evidence Quality Scales (UK)

Evidence level D	Evidence level C	Evidence level B	Evidence level A
"Expert opinion without explicit critical appraisal, or based on physiology, bench research or first principles."	Case-series study or extrapolations from level B studies.	Consistent Retrospective Cohort, Exploratory Cohort, Ecological Study, Outcomes Research, case-control study; or extrapolations from level A studies.	Consistent Randomized Controlled Clinical Trial, cohort study, all or none, clinical decision rule validated in different populations.



better

EBRM – DO WE HAVE DATA?

Data Risk Factors Are Either

- Endogenic (from within)
- Exogenic (from outside)

Data Risk Factors Are Either

- Endogenic (from within)

LOTS! (too much?)

- Exogenic (from outside)

Endogenic Sources

- Systems data
- Performance data
- Internally generated estimates for losses
- Internally generated estimates for threats

Data Risk Factors Are Either

- Endogenic (from within)

LOTS! (too much?)

- Exogenic (from outside)

NOT ENOUGH! (getting better?)

Exogenic Sources

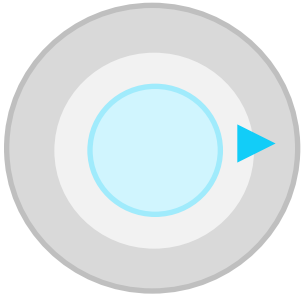
- Breach Reports
  - Open Security Foundation / DataLossDB.org
  - Verizon DBIR
- Threat Intel Sources
  - TrustWave, HP, Microsoft, McAfee, and others
- Industry Studies
  - Claims studies from cyber liability insurance companies
  - Benchmarking
- Industry Surveys
  - Ponemon
- Private Sharing Services

WE DON'T HAVE TO WAIT FOR EXOGENIC QUALITY TO START EBRM.

INTEGRATING EVIDENCE – BASED DECISIONS INTO RISK MANAGEMENT PROGRAMS

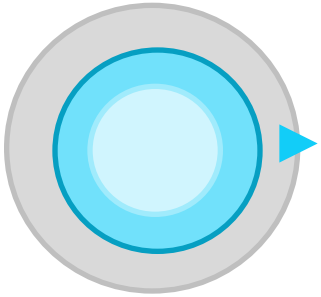
EVERY ORGANIZATION IS PRESENTED WITH 3 “LEVELS” OF DECISIONS -

3 Levels Of Decisions



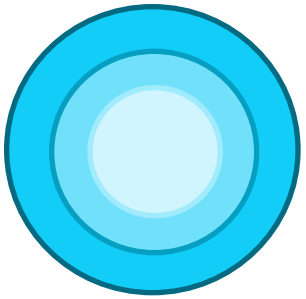
- Tactical
  - Fraud Models
  - Traffic Models (IDS, etc.)
    - THESE ARE CONTROLS IN AND OF THEMSELVES
      - Behavioral Alerting
      - Signature Alerting

3 Levels Of Decisions



- Mid-Range
  - Scenario-Based Analysis
    - (what our risk registers are made up of)

3 Levels Of Decisions



- Strategic (Systemic Risk?)
  - Patterns in operations that create:
    - An understanding of the realization of scenario-modeling
    - The effectiveness of tactical modeling

WE CAN USE THIS MODEL OF KNOWLEDGE (THESE LEVELS OF DECISIONS) TO CHANGE OUR PROGRAMS

Tale Of Two Cases

- Big Company, Big Resources, Big Problems
- Little Company, Little Resources, Big Problems

EBRM In The Enterprise

- Ingredients:
  - Data Scientist(s)
  - Data Engineer(s)
  - Something Like Hadoop
  - A network architecture that supports data in stream
  - A risk management program with incentives (formal, informal) to be data-driven
  - Management that desires excellence

EBRM In The Enterprise

- Directions (1)
  - First, Taxonomy vs. Available Data exercise
    - **Think of your controls not as P/D/R, but as data collection devices!**
    - Utilize a data collecting network architecture to, well, collect data
  - Look for resources outside of IT (HR Systems are an awesome example)

EBRM In The Enterprise

- Directions (2)

EBRM In The Enterprise

- Directions (3)
  - Make your processes/workflows accountable to support evidence-based decision making
  - Security & Risk must work together to this end
  - This is probably a policy change as much as a procedural one

EBRM In The Enterprise

- Directions (4)
  - Transform Risk Management into an intelligence function
    - Around exogenic and endogenic data collection and processing
  - Experiment with Metrics and Reporting
    - An actual visualization pro may help here

EBRM In The SMB

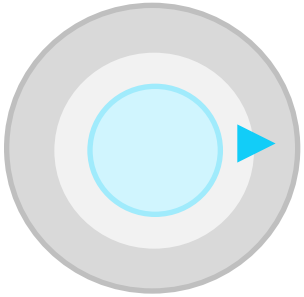
- But I don't have 18 full time analysts and an Alex Hutton……

Now what?

EBRM In The SMB

- EBRM can be done at SMBs
- EBRM does not have to be an all or nothing proposition
- It is possible to right size EBRM

EBRM In The SMB – What You'll Be Missing



- Tactical Tends to Be Outsourced!
  - Fraud Models
  - Traffic Models (IDS, etc.)
    - THESE ARE CONTROLS IN AND OF THEMSELVES
      - Behavioral Alerting
      - Signature Alerting

EBRM in the SMB

- Ingredients:
  - Vendors that support Data/Correlation
    - We're starting to see this happen!
  - Time with your Business Analysts
    - Blue Dollars FTW!
  - Information Designer for reporting
    - Most newly minted Graphic Design folks *have* to have a visualization bent these days
  - Still probably want a data store, but that's optional
    - You'll just be stuck in Spreadmart

Example Service: RiskI/O

EBRM In The SMB

- Directions (1)
  - Consider seeking assistance
  - Make your processes/workflows accountable to support evidence-based decision making
  - Security & Risk must work together to this end
  - This is probably a policy change as much as a procedural one

EBRM In The SMB

- Directions (2)
  - Make the most of your commonly available Exogenic data
  - Work backwards from your reporting opportunities into the data you have

Exogenic Example: DBIR

Figure 8. VERIS A⁴ Grid depicting the frequency of high-level threat events

		Malware			Hacking			Social			Misuse			Physical			Error			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Confidentiality & Possession	381			518		1				9	8	1					2	1			
	Integrity & Authenticity	397			422		1				6	1	1									
	Availability & Utility	2			6						5											
Networks	Confidentiality & Possession										1											
	Integrity & Authenticity	1									1											
	Availability & Utility	1			1						1											
User Devices	Confidentiality & Possession	356			419						1			86								
	Integrity & Authenticity	355			355						1	1		86								
	Availability & Utility										1			3								
Offline Data	Confidentiality & Possession											23							1			
	Integrity & Authenticity																					
	Availability & Utility																					
People	Confidentiality & Possession							30	1													
	Integrity & Authenticity							59	2													
	Availability & Utility																					

EBRM in the SMB

- Directions (3)
  - Account for feedback loops
  - Don’t over complicate things!
  - Risk Management is an Intel Function!

To Change We Must

- Embrace the data available
- Evaluate findings published
- Change or Augment our Current Standards
- Get Interested in Sharing Data
- Take the time to do the work

DATA BREACH INTELLIGENCE: DOES HISTORY ALWAYS REPEAT ITSELF?

Jake Kouns
Open Security Foundation

Alex Hutton
Zions Bancorporation

Session ID: DSP-F42

Session Classification: Intermediate

An example:

Pyschometricization of Vendor Management