How to optimize cybersecurity control decisions when supporting data is scarce

RISK AWARENESS WEEK 2022

Robert D. Brown III
Cybersecurity Risk Management Leader
Resilience Insurance

Introduction

Robert Brown

- 25+ year career as a decision & risk analysis advisor across multiple commercial verticals

- Past RAW contributor
  - 2019 – Value of information on continuous variables
  - 2020 – Bayesian method for judging the likely scenario in a defined set that is unfolding
  - 2021 – Measuring the value of carbon ($/tonne) and its effect on selecting green initiatives

- Author of *Business Case Analysis with R - Simulation Tutorials to Support Complex Business Decisions* (Springer-Nature/Apress, 2018)

- Joined Resilience Insurance in May 2022, reporting to Richard Seiersen, co-author of *How to Measure Anything in Cybersecurity Risk* (Wiley, 2016) and *The Metrics Manifesto* (Wiley, 2022)

Cybersecurity requires balancing multiple business concerns

Security and Operational Resilience

Alternate Responsible Uses of Capital

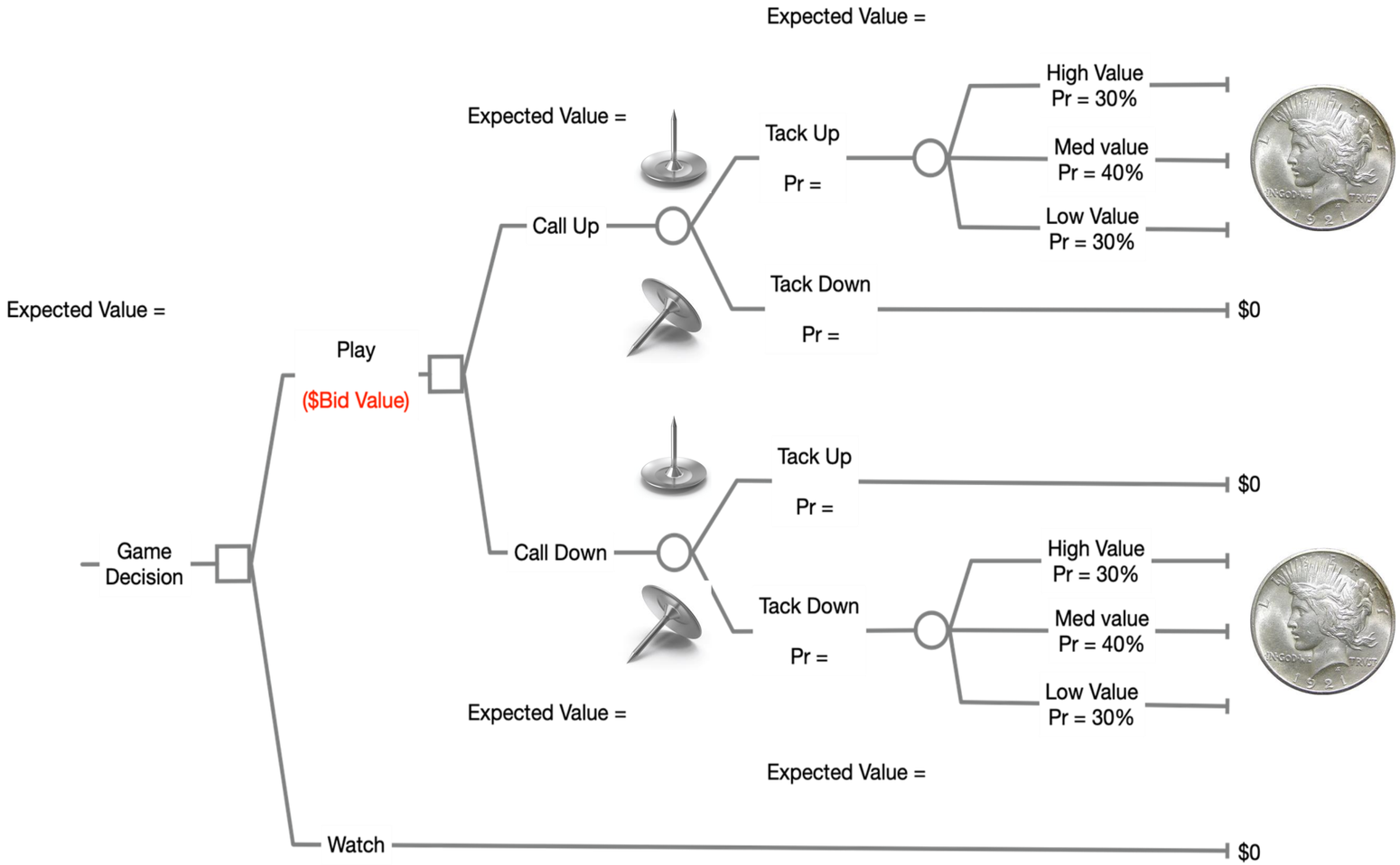
Varying Information Quality

Competing Values and Preferences

Probabilities don’t exist, but they do matter

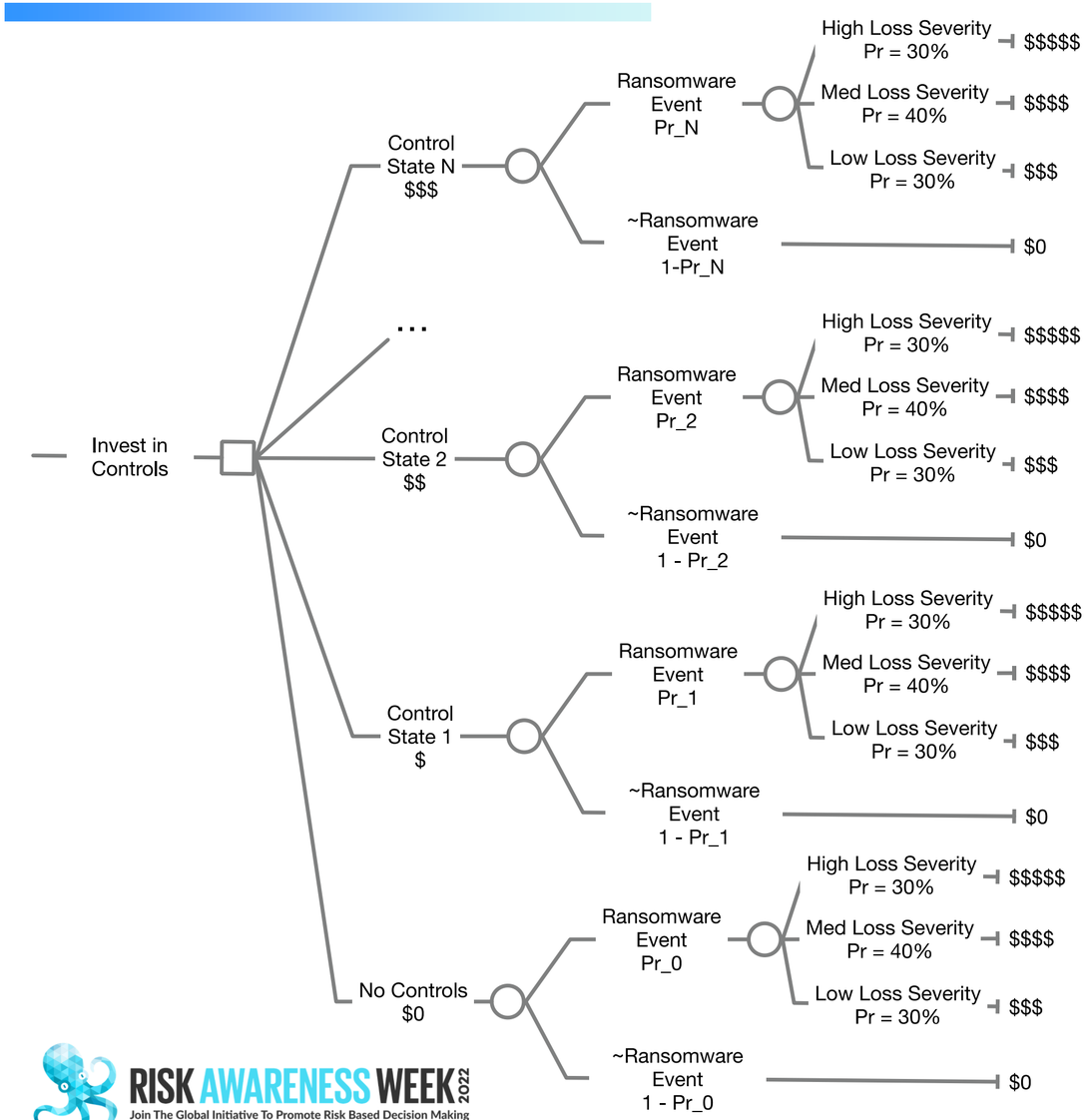
- Probabilities are analogous to discount rate in discounted cash flow analysis, which allows us to compare alternate choices of cash flows in time.

- Probabilities are the mental tool we use to compare alternate choices of games of chance that yield different payoffs if they materialize.



The thumb tack game represents the essential elements of any allocation decision

How does this apply to cybersecurity (e.g., ransomware)?

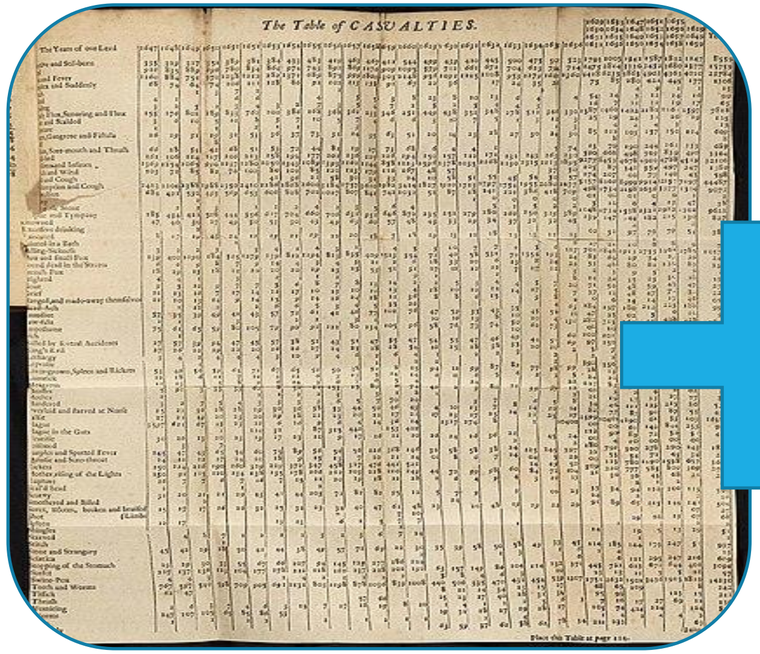


- Optimization goal: choose the control state that minimizes the expected value of material ransomware event losses.
- Loss Severity and Cost of Control State (i.e., configuration) might be uncertain, but are reasonably bounded and assessed by SMEs directly.
- Probability that a ransomware event results in a material loss given a Control State is a little more difficult to assess across the multiple levels of control states.
- Probability of the ransomware event is the connective tissue between the investment decision and the desired payoff.

RISK AWARENESS WEEK 2022
Join The Global Initiative To Promote Risk Based Decision Making

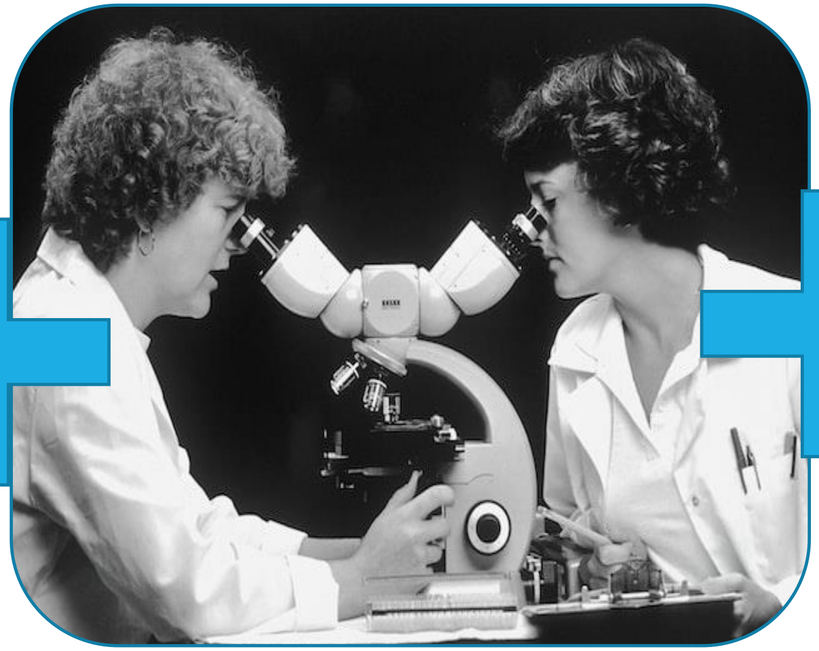
The alchemy of probabilities

Actuarial Tables



Formalized and peer reviewed empirical data

Subject Matter Experts

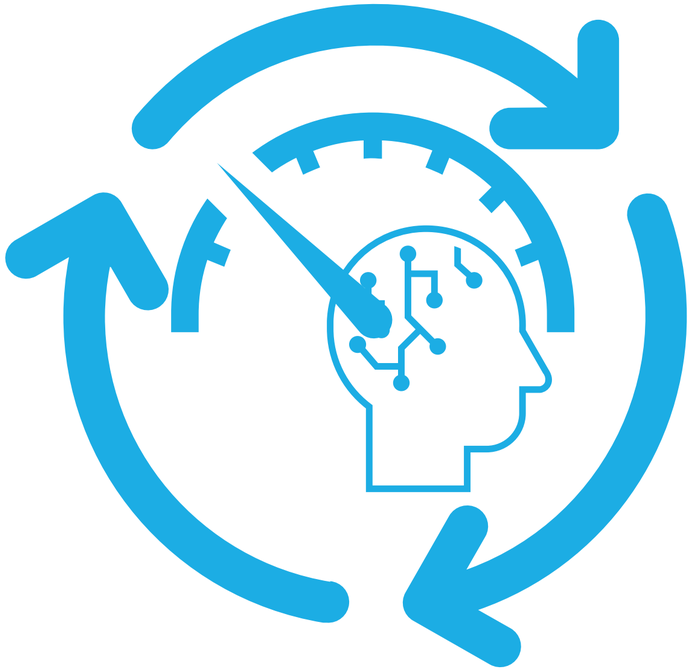


People who possess fine-grained understanding of causal factors

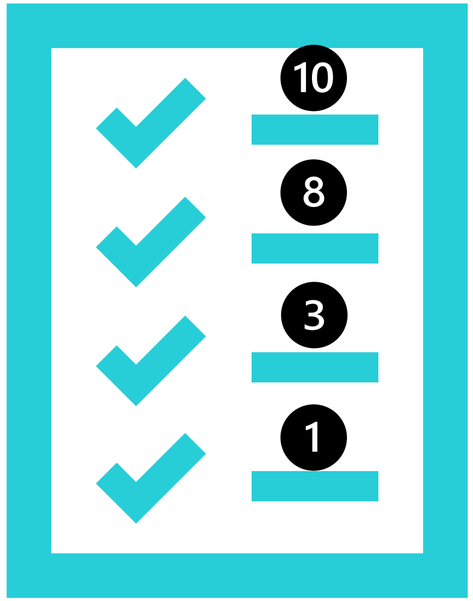
Bookies

People who aggregate and synthesize information to set odds

On the care and feeding of your SMEs



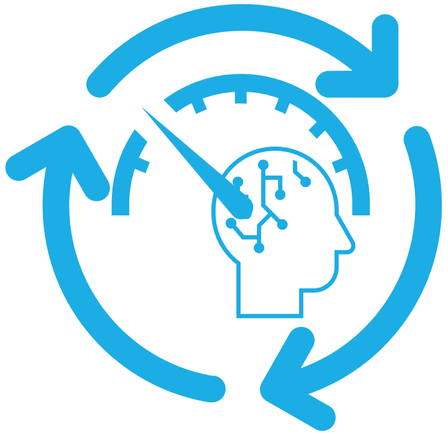
Iteratively Calibrate



Keep a Running Score

Employ Best for Real Assessments

Calibrate and Score



Iteratively Calibrate

Question

1. The melting point of tin is higher than the melting point of aluminum.

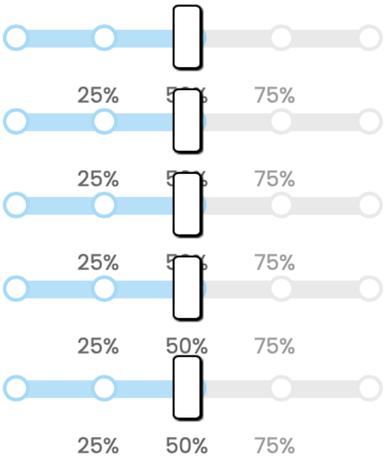
2. In English, the word “quality” is more frequently used that the word “speed”.

3. Any male pig is referred to as a hog.

4. California’s giant sequoia trees are named for an early 19th century leader of the Cherokee Indians.

5. The Model T was the first car produced by Henry Ford.

Probability Statement is True

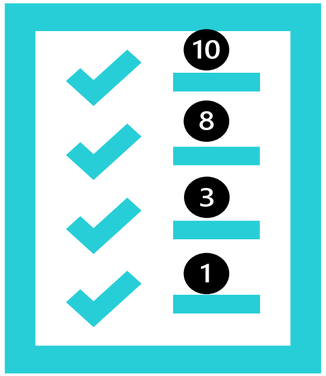


Previous

Next

Submit Quiz

The Brier Score



Keep a Running Score

Database of Assessments and Scores

	forecast	outcome	sqr_error
1	0.75	1	0.0625
2	0.61	0	0.3721
3	0.56	1	0.1936
4	0.60	1	0.1600
5	0.68	1	0.1024
6	0.38	1	0.3844
7	0.68	1	0.1024
8	0.27	1	0.5329
9	0.68	1	0.1024
10	0.43	1	0.3249
11	0.85	0	0.7225
12	0.71	0	0.5041
13	0.69	1	0.0961
14	0.56	0	0.3136
15	0.71	1	0.0841

- Developed by Glenn Brier, a meteorologist, to provide feedback to improve quality of weather forecasts.
- A strictly proper scoring rule that measures the accuracy of probabilistic predictions.
- Equivalent to the mean squared error as applied to predicted probabilities.

$$\mathrm{BS} = \frac{1}{N}\sum_{k=1}^{N}(f_k - o_k)^2$$

https://docs.lib.noaa.gov/rescue/mwr/078/mwr-078-01-0001.pdf

Perform virtual experiments with the calibrated SMEs

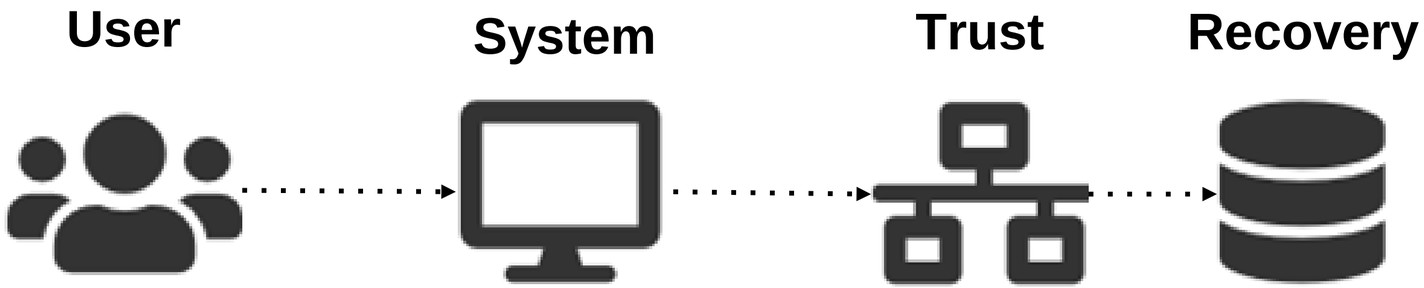
Employ Best for Real Assessments

- We calibrate on verifiable but difficult questions, then apply the thinking process to very difficult to verify judgments.
- Egon Brunswick lens model – means to reverse engineer how SMEs perceive their environment on the basis of observed cues correlated to outcomes they judge.
- Combine all SMEs' "data"
- Regress response ~ control levels

Reverse engineering the SME brain – a ransomware model example

- **Our Goal: Discover the value of security controls**
- We review about 10-50 control states
- Each state is composed of different control levels across seven control type
- SMEs assess the probability of a material event for each state
- We score the SMEs for noise: consistency and discrimination
- We combine the SMEs' assessments into a database
- **The Result:** A probability model for ~650+ control combinations

The conceptual ransomware system model sets the context



FUNCTIONS

- Training
- Email Security
- Vulnerability
- Endpoint
- Identity
- Network
- Backup

CONTROLS

NOTHING | DEPLOYED | MANAGED

LEVELS

RISK AWARENESS WEEK 2022
Join The Global Initiative To Promote Risk Based Decision Making

Security Controls – Probability of Material Event Assessment

	User Controls		System Controls		Trust Controls		Backup Controls	Likelihoods		
	Security Training	Email Security	Vulnerability Patch Sla	Endpoint Protection	Identity Verification	Network Segmentation	Backup Security	P(Ransomware), 1 yr	Year 3	Year 5
1	UNMANAGED: No Training	UNMANAGED: No Controls	UNMANAGED: Adhoc Patch	UNMANAGED: No Controls	UNMANAGED: No Controls	UNMANAGED: Ext Firewall	UNMANAGED: No Backups	+4.00%	+11.50%	+18.50%
2	MANAGED: Attack Simulations	DEPLOYED: Email Security Gateway & Email Auth	UNMANAGED: Adhoc Patch	DEPLOYED: EPP	DEPLOYED: MFA	DEPLOYED: Users Segmented	DEPLOYED: Backups			
3	UNMANAGED: No Training	UNMANAGED: No Controls	MANAGED: 30 Days Patch Critical	UNMANAGED: No Controls	UNMANAGED: No Controls	MANAGED: Micro-Segmentation	MANAGED: Tested Backups			
4	UNMANAGED: No Training	UNMANAGED: No Controls	MANAGED: 30 Days Patch Critical	MANAGED: EPP & EDR	UNMANAGED: No Controls	MANAGED: Micro-Segmentation	UNMANAGED: No Backups			
5	UNMANAGED: No Training	DEPLOYED: Email Security Gateway & Email Auth	UNMANAGED: Adhoc Patch	DEPLOYED: EPP	UNMANAGED: No Controls	DEPLOYED: Users Segmented	UNMANAGED: No Backups			

- We set a baseline annual probability based on claims data and other firmographic data ~ 2.5%.
- Well calibrated SMEs assess how the baseline updates based on control combinations.
- We present 10-50 control states at a time chosen to span the full set of combinations after several SMEs provide input over several sets.

Combine all SME judgements to “recreate Giambi”

	USER CONTROLS		COMPUTE CONTROLS		TRUST CONTROLS		RECOVERY CONTROLS	
Security_Training	Email_Security	Vulnerability_Patch_SLA	Endpoint_Protection	Identity_Verification	Network_Segmentation	Backup_Security	Annual_Prob
UNMANAGED:No Training	DEPLOYED:Email Security Gateway & Email Auth	MANAGED:30 Days Patch CRITCAL	MANAGED:EPP & EDR	MANAGED:MFA & PAM	DEPLOYED:Users Segmented	DEPLOYED:Backups	1.90%
MANAGED:Attack Simulations	DEPLOYED:Email Security Gateway & Email Auth	UNMANAGED:Adhoc Patch	UNMANAGED:No Controls	UNMANAGED:No Controls	MANAGED:Micro-Segmentation	UNMANAGED:No Backups	3.90%
UNMANAGED:No Training	DEPLOYED:Email Security Gateway & Email Auth	UNMANAGED:Adhoc Patch	DEPLOYED:EPP	DEPLOYED:MFA	DEPLOYED:Users Segmented	UNMANAGED:No Backups	2.40%
UNMANAGED:No Training	UNMANAGED:No Controls	MANAGED:30 Days Patch CRITCAL	DEPLOYED:EPP	UNMANAGED:No Controls	UNMANAGED:Ext Firewall	MANAGED:Tested Backups	2.80%
UNMANAGED:No Training	DEPLOYED:Email Security Gateway & Email Auth	MANAGED:30 Days Patch CRITCAL	UNMANAGED:No Controls	UNMANAGED:No Controls	DEPLOYED:Users Segmented	MANAGED:Tested Backups	2.65%
MANAGED:Attack Simulations	UNMANAGED:No Controls	UNMANAGED:Adhoc Patch	MANAGED:EPP & EDR	UNMANAGED:No Controls	UNMANAGED:Ext Firewall	MANAGED:Tested Backups	2.70%
UNMANAGED:No Training	UNMANAGED:No Controls	UNMANAGED:Adhoc Patch	MANAGED:EPP & EDR	DEPLOYED:MFA	MANAGED:Micro-Segmentation	UNMANAGED:No Backups	2.40%
UNMANAGED:No Training	DEPLOYED:Email Security Gateway & Email Auth	UNMANAGED:Adhoc Patch	MANAGED:EPP & EDR	DEPLOYED:MFA	MANAGED:Micro-Segmentation	MANAGED:Tested Backups	2.10%
MANAGED:Attack Simulations	UNMANAGED:No Controls	UNMANAGED:Adhoc Patch	DEPLOYED:EPP	UNMANAGED:No Controls	DEPLOYED:Users Segmented	UNMANAGED:No Backups	2.95%
UNMANAGED:No Training	DEPLOYED:Email Security Gateway & Email Auth	UNMANAGED:Adhoc Patch	MANAGED:EPP & EDR	DEPLOYED:MFA	MANAGED:Micro-Segmentation	UNMANAGED:No Backups	2.80%
MANAGED:Attack Simulations	UNMANAGED:No Controls	UNMANAGED:Adhoc Patch	MANAGED:EPP & EDR	DEPLOYED:MFA	UNMANAGED:Ext Firewall	UNMANAGED:No Backups	2.90%
MANAGED:Attack Simulations	DEPLOYED:Email Security Gateway & Email Auth	UNMANAGED:Adhoc Patch	MANAGED:EPP & EDR	DEPLOYED:MFA	MANAGED:Micro-Segmentation	UNMANAGED:No Backups	2.35%

Guys, you’re still trying to replace Giambi. I told you we can’t do it…Now what we might be able to do is recreate him. We create him in the adding field.

Billy Beane, former general manager of the Oakland Athletics, as featured in the movie *Moneyball* (2011).

Transform the event probability assessments into numerical levels and regress to linear coefficients

Security_Training	Email_Security	Vulnerability_Patch_SLA	Endpoint_Protection	Identity_Verification	Network_Segmentation	Backup_Security	
UNMANAGED:No Training	UNMANAGED:No Controls	UNMANAGED:Adhoc Patch	UNMANAGED:No Controls	UNMANAGED:No Controls	UNMANAGED:Ext Firewall	UNMANAGED:No Backups	1
MANAGED:Attack Simulations	DEPLOYED:Email Security Gateway & Email Auth	MANAGED:30 Days Patch CRITCAL	DEPLOYED:EPP	DEPLOYED:MFA	DEPLOYED:Users Segmented	DEPLOYED:Backups	2
			MANAGED:EPP & EDR	MANAGED:MFA & PAM	MANAGED:Micro-Segmentation	MANAGED:Tested Backups	3

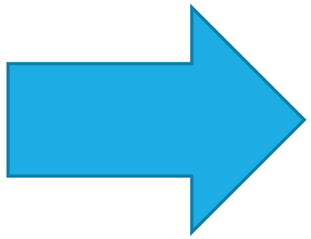
Security_Training	Email_Security	Vulnerability_Patch_SLA	Endpoint_Protection	Identity_Verification	Network_Segmentation	Backup_Security	Annual_Prob
1	2	2	3	3	2	2	1.90%
2	2	1	1	1	3	1	3.90%
1	2	1	2	2	2	1	2.40%
1	1	2	2	1	1	3	2.80%
1	2	2	1	1	2	3	2.65%
2	1	1	3	1	1	3	2.70%
1	1	1	3	2	3	1	2.40%
1	2	1	3	2	3	3	2.10%
2	1	1	2	1	2	1	2.95%
1	2	1	3	2	3	1	2.80%
2	1	1	3	2	1	1	2.90%
2	2	1	3	2	3	1	2.35%
1	2	1	1	1	2	2	3.65%

Multi-linear regression on control levels yields coefficients

	Coefficients
Intercept	0.0708
Security_Training	-0.0032
Email_Security	-0.0043
Vulnerability_Patch_SLA	-0.0047
Endpoint_Protection	-0.0037
Identity_Verification	-0.0038
Network_Segmentation	-0.0023
Backup_Security	-0.0020

Setting control levels by their ordinal designation lets us predict the probability of material events in further risk analysis

	Coefficients
Intercept	0.0708
Security_Training	-0.0032
Email_Security	-0.0043
Vulnerability_Patch_SLA	-0.0047
Endpoint_Protection	-0.0037
Identity_Verification	-0.0038
Network_Segmentation	-0.0023
Backup_Security	-0.0020



Min Control State	Max Control State
1	2
1	2
1	2
1	3
1	3
1	3
1	3

Annual Probability of Ransomware Event

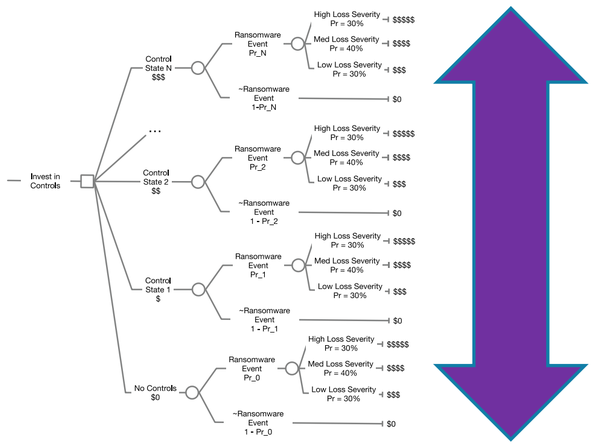
4.67%

1.09%

Cybersecurity requires balancing multiple business concerns

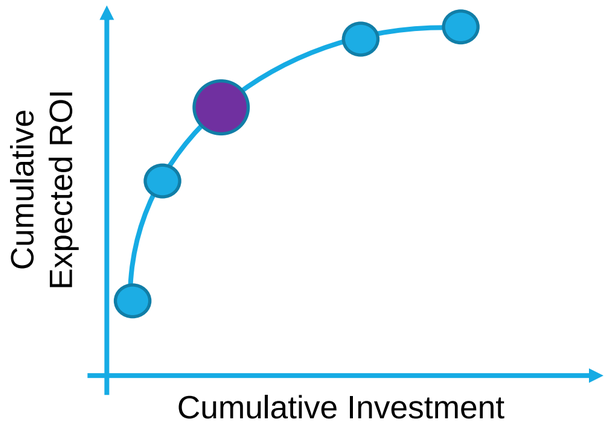
Security and Operational Resilience

Optimize across control alternatives



Alternate Responsible Uses of Capital

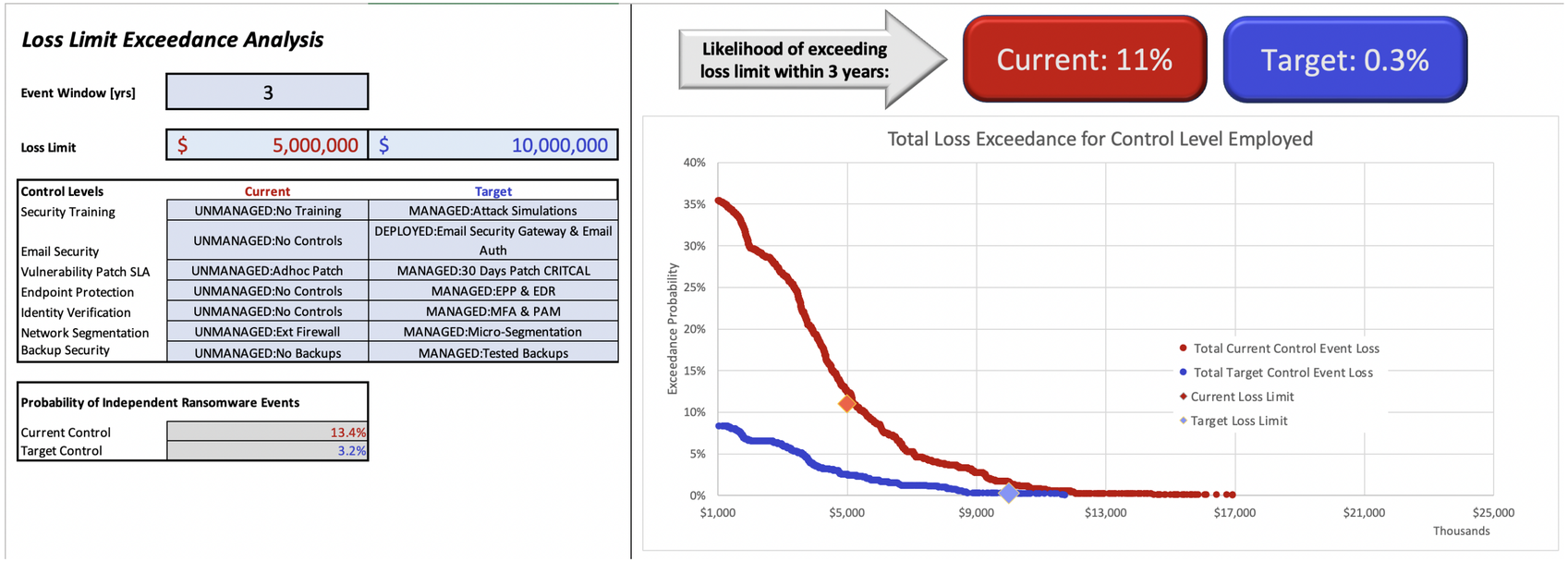
Include in portfolio discussion of all capital allocations



RISK AWARENESS WEEK 2022
Join The Global Initiative To Promote Risk Based Decision Making

Thank you!

- Be sure to download the Excel Ransomware model.
- Reach out for questions or open office hours to go over the Excel model.



Loss Limit Exceedance Analysis

Event Window [yrs]	3	
Loss Limit	$ 5,000,000	$ 10,000,000

Control Levels	**Current**	**Target**
Security Training	UNMANAGED:No Training	MANAGED:Attack Simulations
Email Security	UNMANAGED:No Controls	DEPLOYED:Email Security Gateway & Email Auth
Vulnerability Patch SLA	UNMANAGED:Adhoc Patch	MANAGED:30 Days Patch CRITCAL
Endpoint Protection	UNMANAGED:No Controls	MANAGED:EPP & EDR
Identity Verification	UNMANAGED:No Controls	MANAGED:MFA & PAM
Network Segmentation	UNMANAGED:Ext Firewall	MANAGED:Micro-Segmentation
Backup Security	UNMANAGED:No Backups	MANAGED:Tested Backups

Probability of Independent Ransomware Events	
Current Control	13.4%
Target Control	3.2%

Likelihood of exceeding loss limit within 3 years:

Current: 11%

Target: 0.3%