Operationalizing Risk Quantification: Insights from the Frontlines

Jonathan C. Trull
CISO and SVP, Solutions Strategy

Richard Seiersen
Chief Risk Technology Officer

Agenda

- The Why, What, and How of Risk Quantification
- Perils of Risk Assessment without Quantification
- Qualys Risk Quantification Journey
- Top Down, Bottom Up, or Hybrid Approach: Where to Start and Why
- A Model Framework for Operationalizing Cyber Risk

TEA POT

J. E. JEFFORDS

Patented Aug. 6, 1889.

Fig. 1.

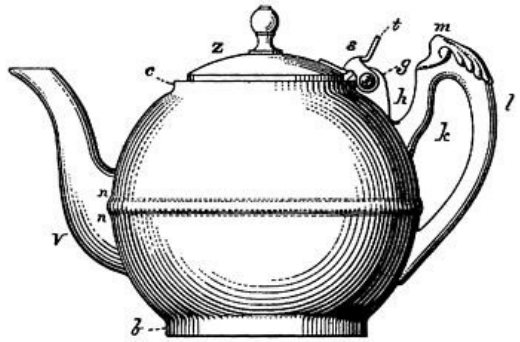
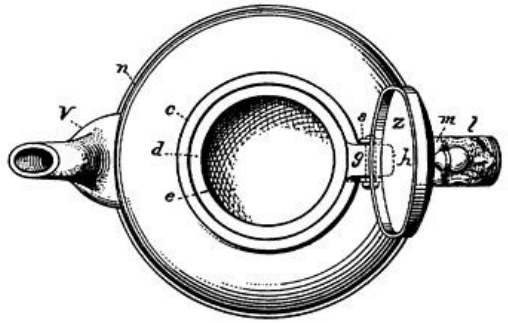


Fig. 2.



WITNESSES

Villette Anderson

J. W. Anderson

INVENTOR

John E. Jefford

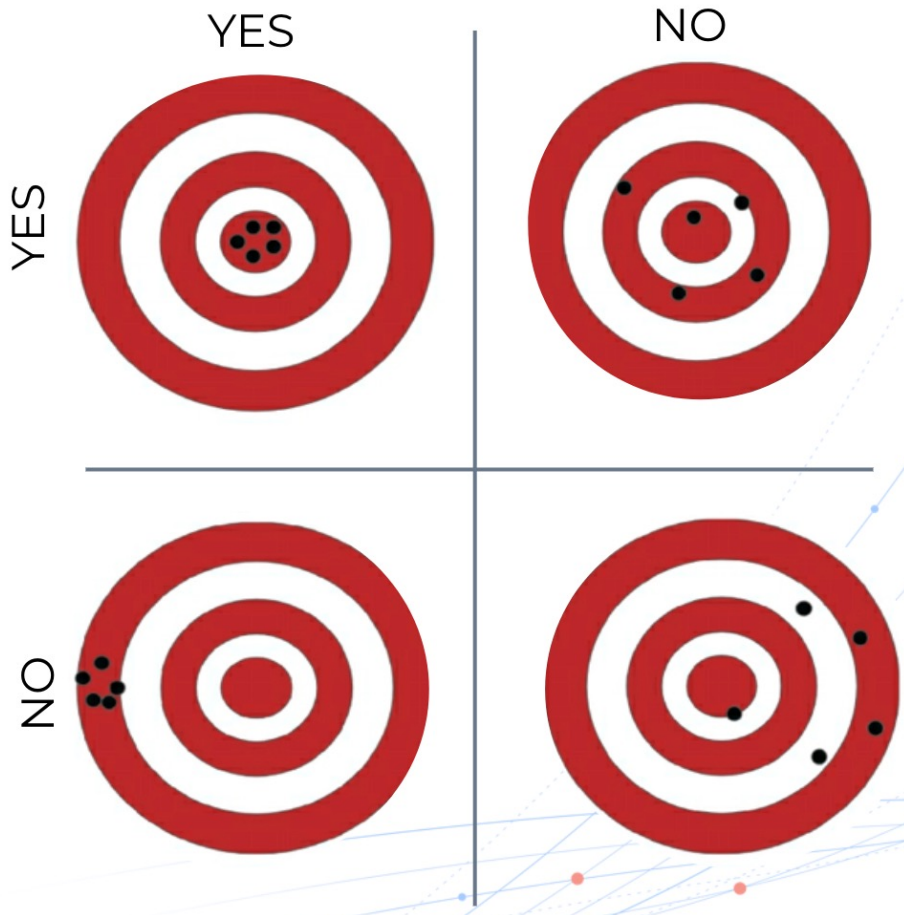
by E. W. Anderson

Attorney

WHY Do People Struggle With Risk Quantification?

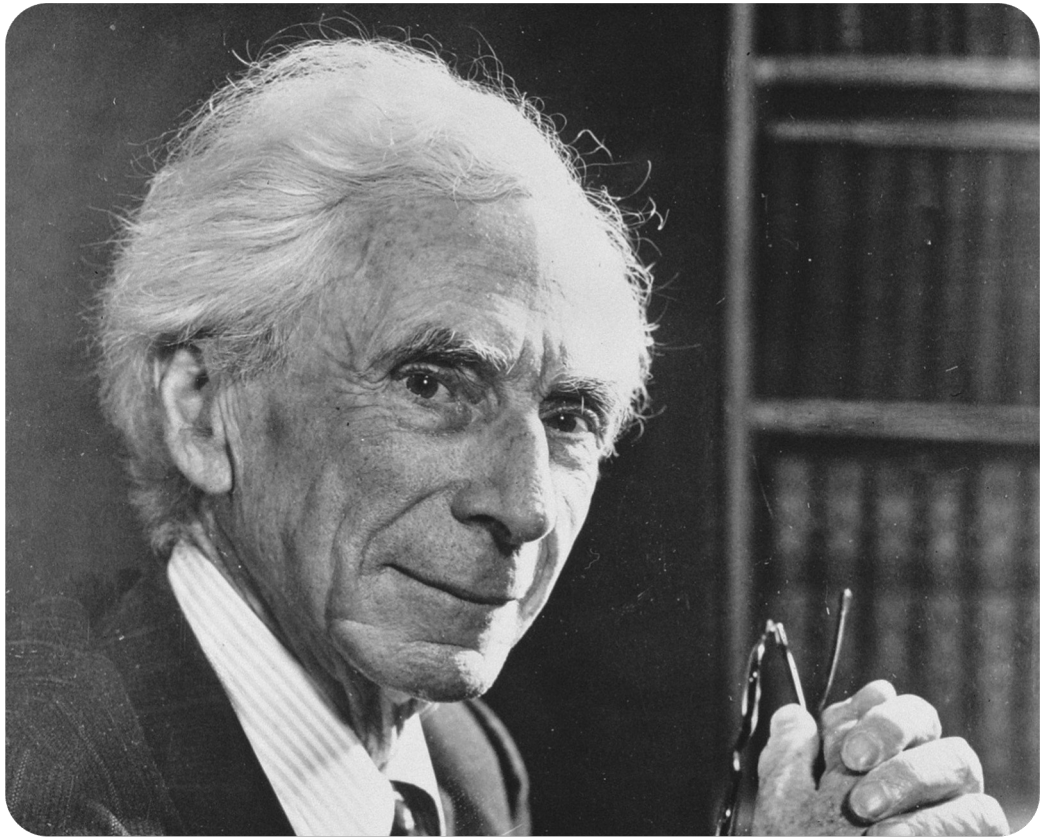
PRECISION

ACCURACY



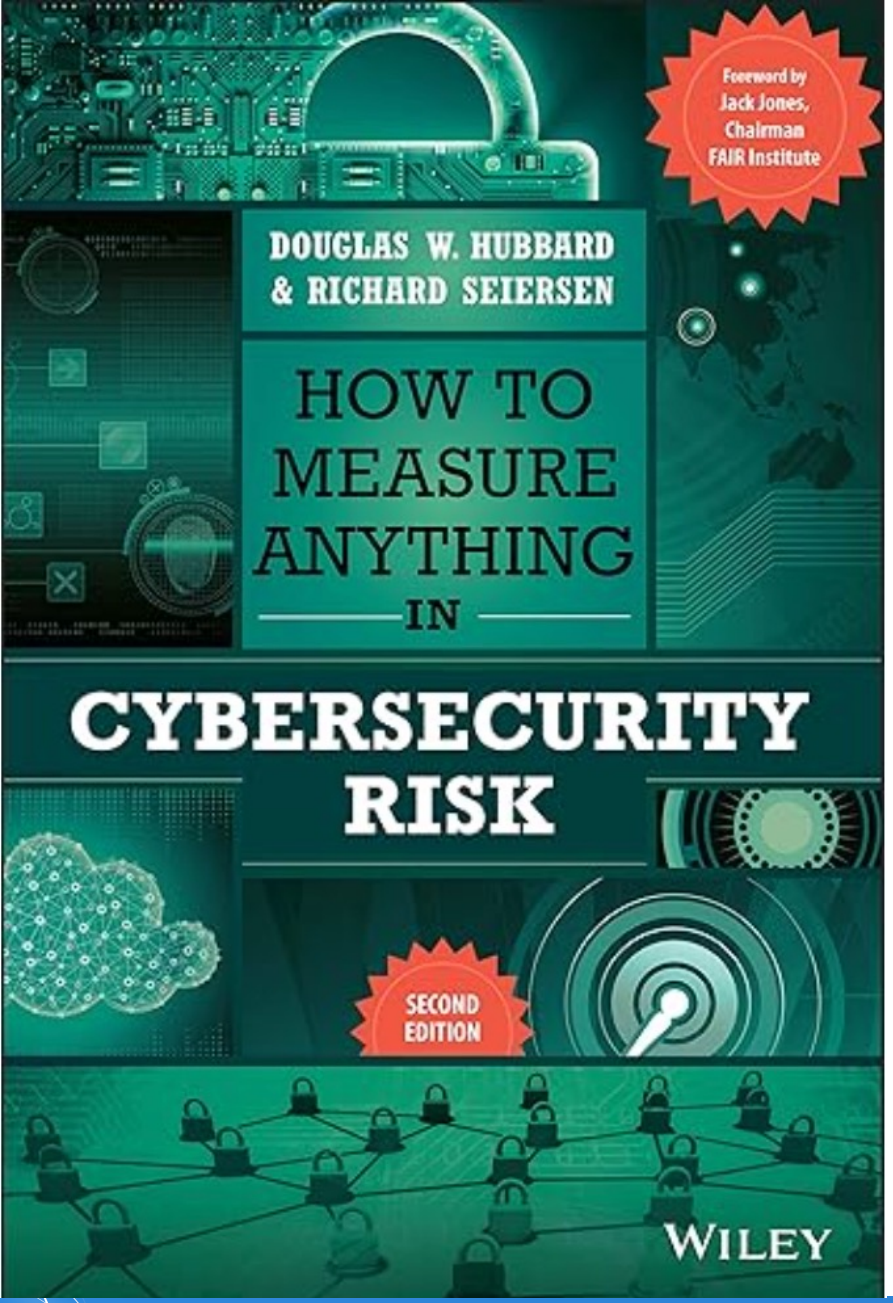
Although this may seem a paradox, all exact science is based on the idea of approximation. If a man tells you he knows a thing exactly, then you can be safe in inferring that you are speaking to an inexact man.

– Bertrand Russell



WHAT Is Risk Quantification?

"A Problem Well Defined Is A Problem Half Solved." – Kettering

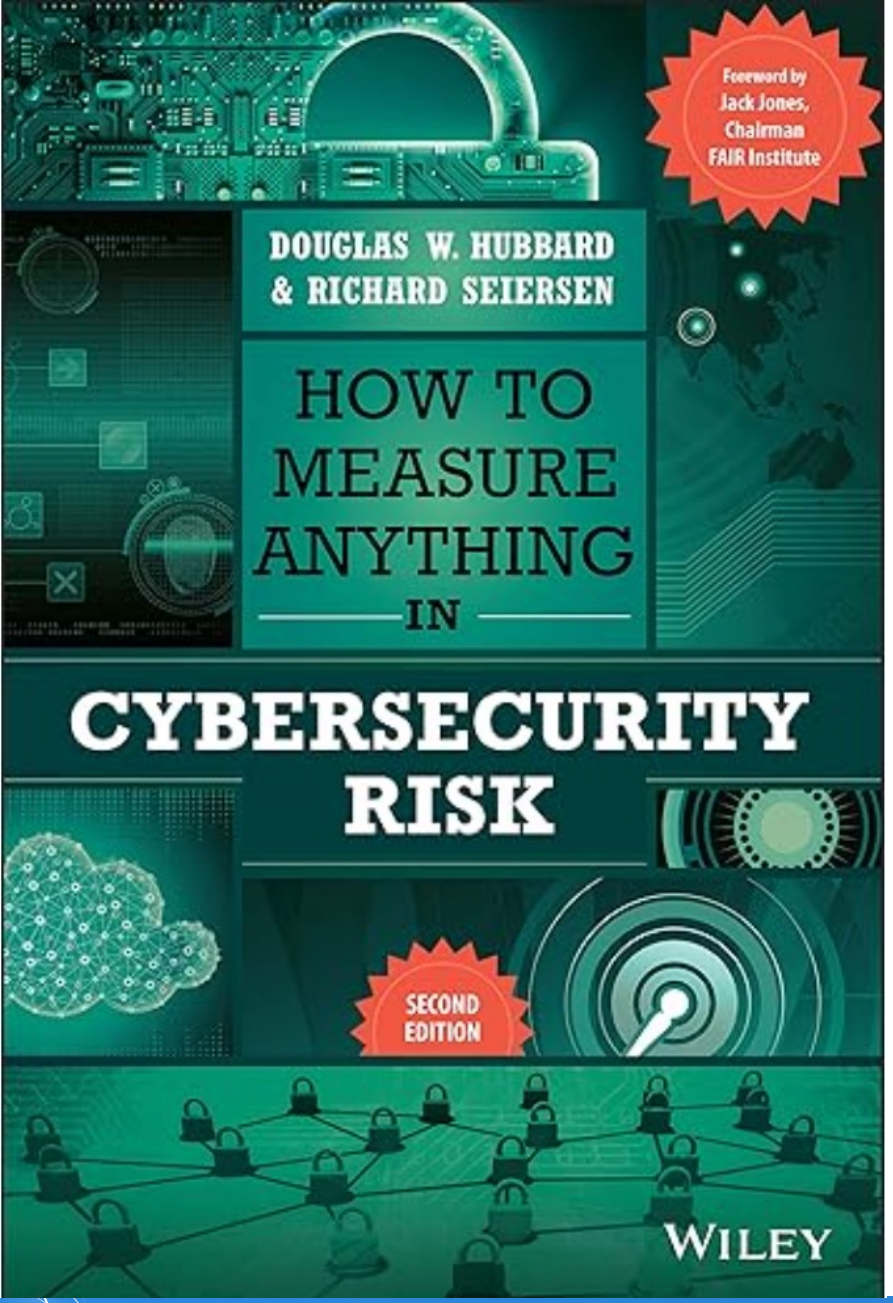


Measurement: A quantitatively expressed reduction of uncertainty based on one or more observations.

Risk: A state of uncertainty where some of the possibilities involve loss, catastrophe, or some other undesirable outcome.

Risk Management: The remediation, mitigation and or transfer of plausible loss impacting business objectives.

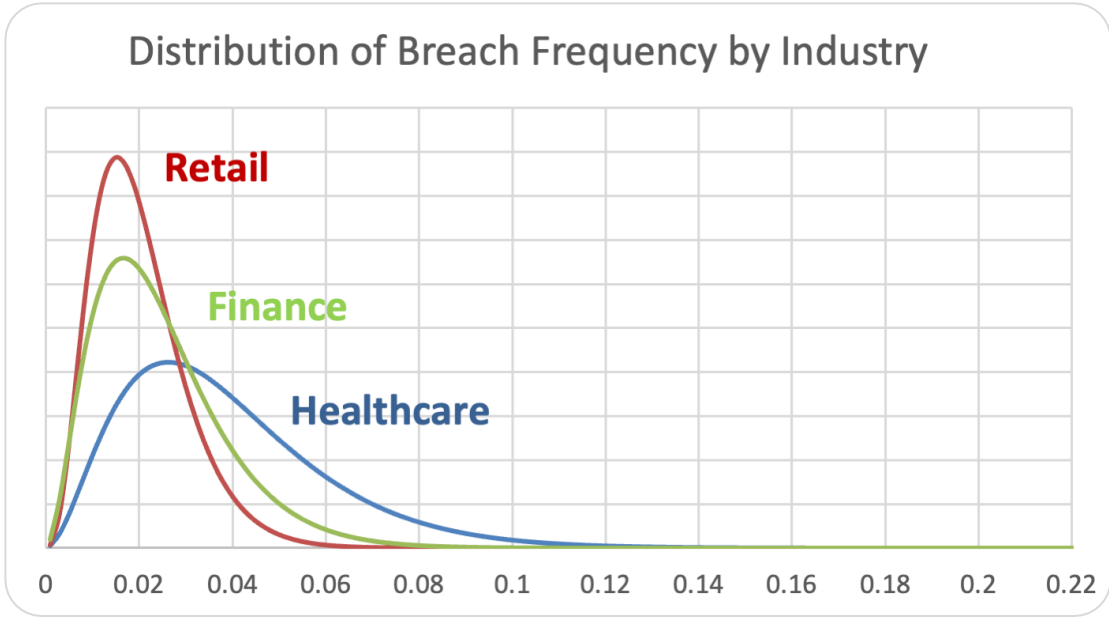
What is the likelihood of a fortune 500 healthcare organization having a public breach?



Measurement: A quantitatively expressed reduction of uncertainty based on one or more observations.

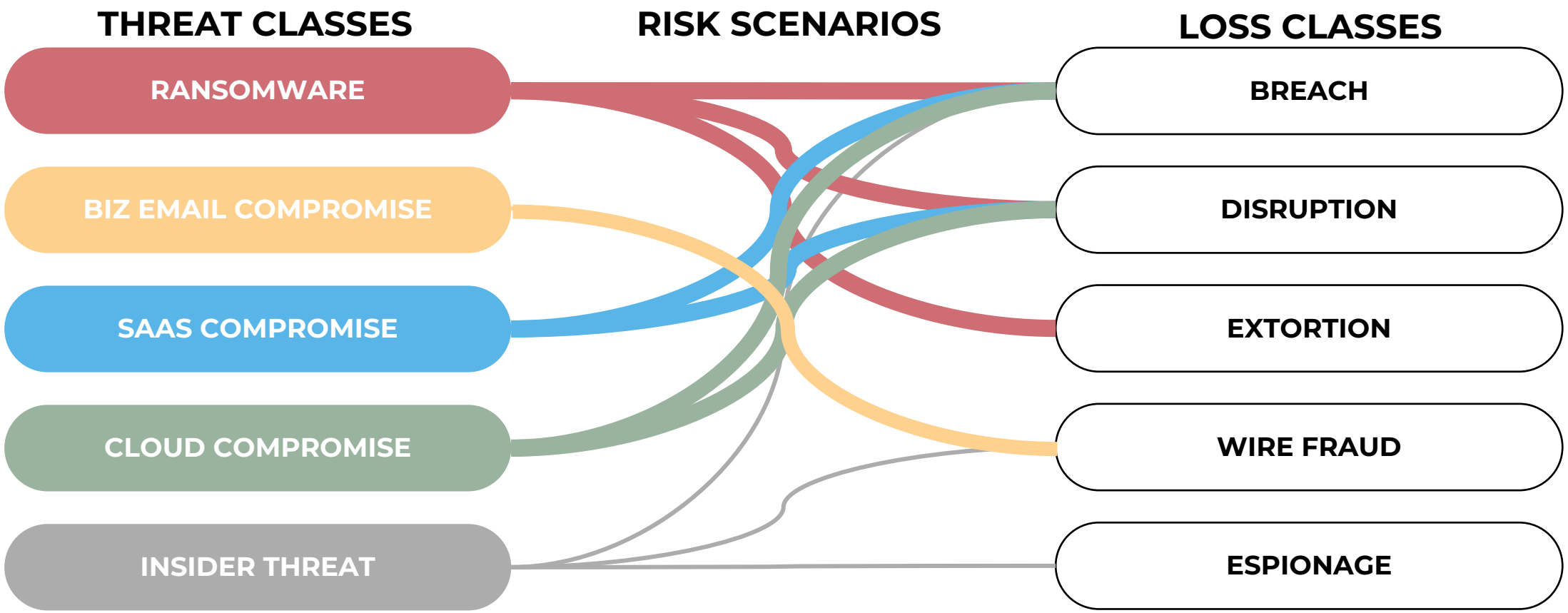
Risk: A state of uncertainty where some of the possibilities involve loss, catastrophe, or some other undesirable outcome.

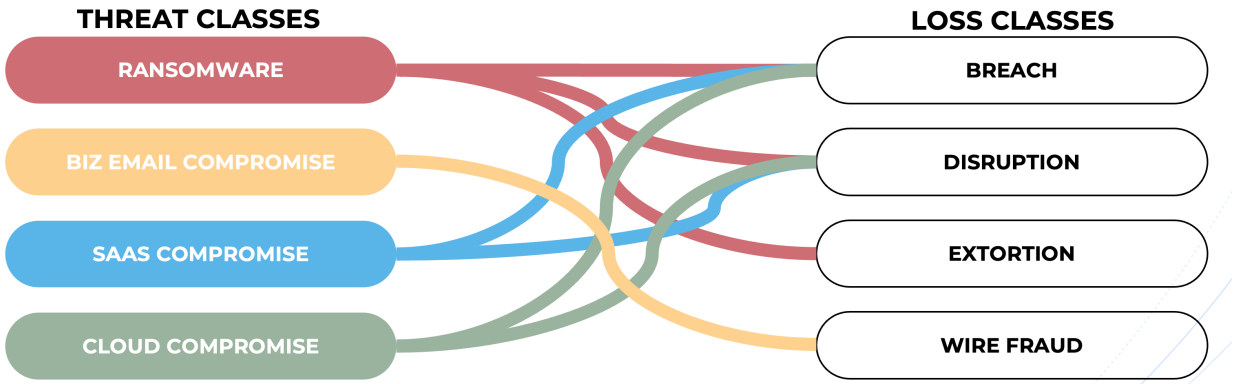
Risk Management: The remediation, mitigation and or transfer of plausible loss impacting business objectives.

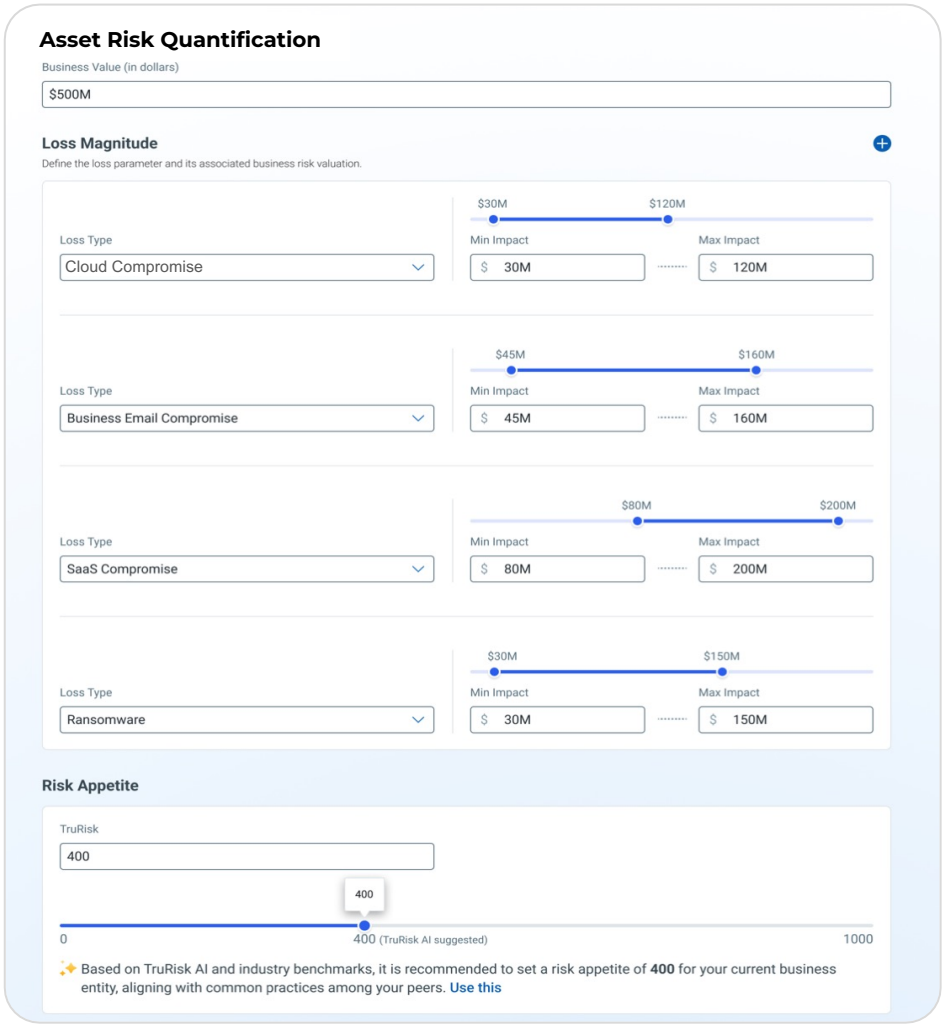


HOW Is Risk Quantification Operationalized?

"Strategy Is The Economy Of Forces." – Clausewitz

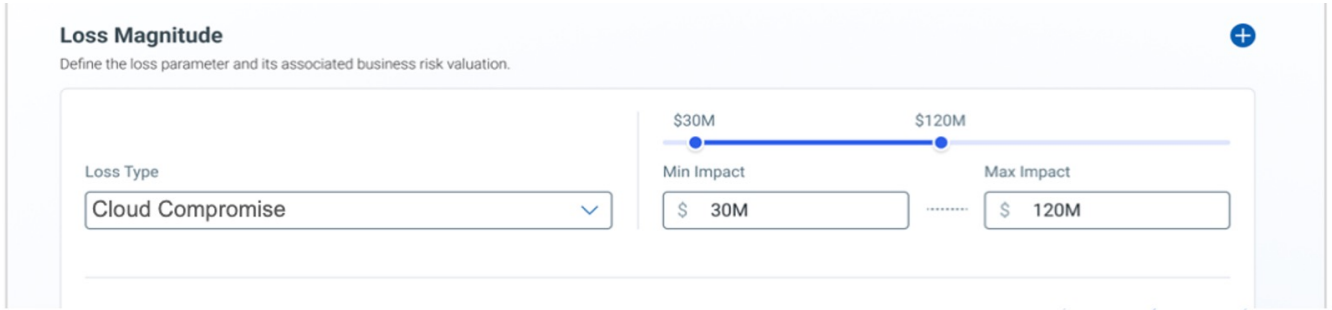

THREAT CLASSES
RISK SCENARIOS
LOSS CLASSES
RANSOMWARE
BIZ EMAIL COMPROMISE
SAAS COMPROMISE
CLOUD COMPROMISE
INSIDER THREAT
BREACH
DISRUPTION
EXTORTION
WIRE FRAUD
ESPIONAGE


THREAT CLASSES
RANSOMWARE
BIZ EMAIL COMPROMISE
SAAS COMPROMISE
CLOUD COMPROMISE
LOSS CLASSES
BREACH
DISRUPTION
EXTORTION
WIRE FRAUD

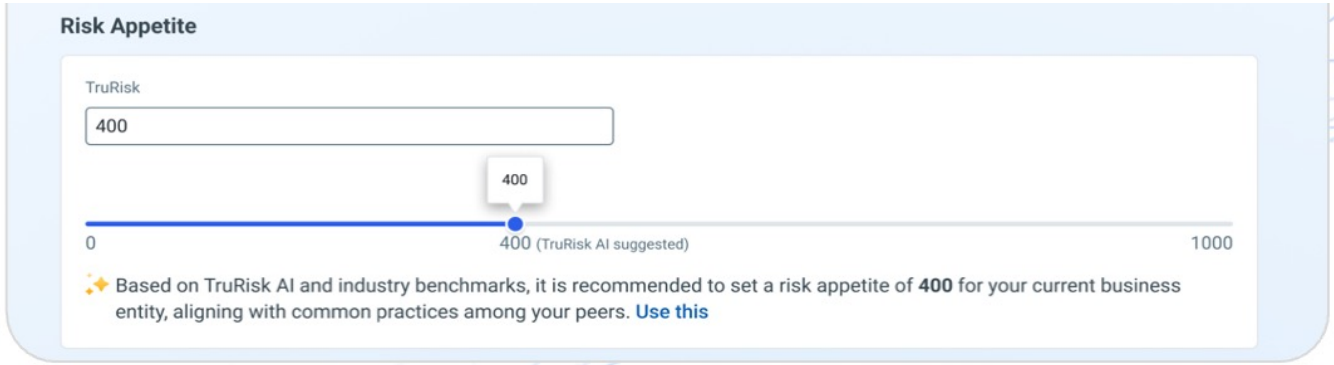

Asset Risk Quantification
Business Value (in dollars)
$500M
Loss Magnitude
Define the loss parameter and its associated business risk valuation.
Loss Type
Cloud Compromise
$30M
$120M
Min Impact
$ 30M
Max Impact
$ 120M
Loss Type
Business Email Compromise
$45M
$160M
Min Impact
$ 45M
Max Impact
$ 160M
Loss Type
SaaS Compromise
$80M
$200M
Min Impact
$ 80M
Max Impact
$ 200M
Loss Type
Ransomware
$30M
$150M
Min Impact
$ 30M
Max Impact
$ 150M
Risk Appetite
TruRisk
400
400
0
400 (TruRisk AI suggested)
1000
Based on TruRisk AI and industry benchmarks, it is recommended to set a risk appetite of 400 for your current business entity, aligning with common practices among your peers. Use this

Business Value
Business stakeholder determined crown jewel asset value

Loss Magnitude
Configurable risk scenarios composed of multiple threat and loss combinations

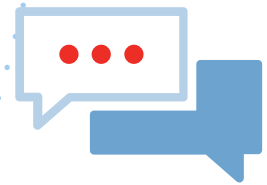


Risk Appetite
Benchmark and AI deduced target score based on:
Threat, Exposure, Control, and Value



Data without insights is meaningless, and insights without action are pointless

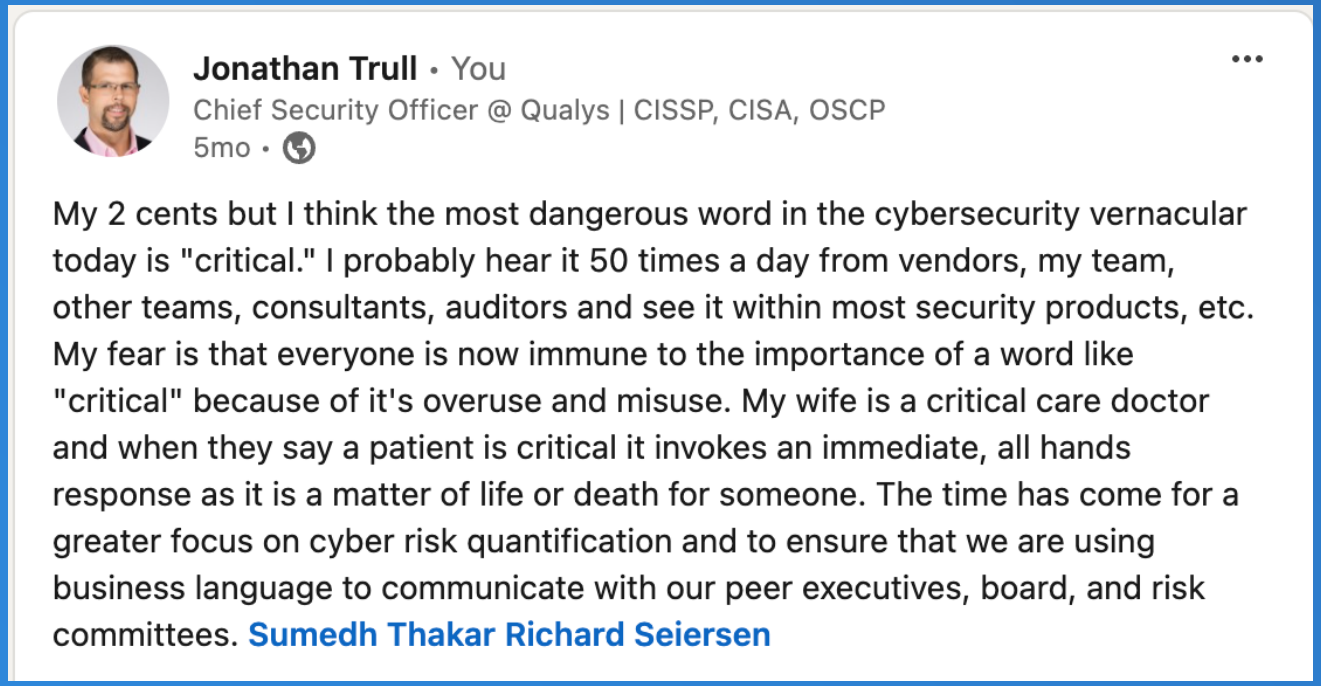
– Harvard Business Review



For cybersecurity leaders, data without insights, **derived from context and intelligence,** is meaningless, and insights without action are pointless.

– Jonathan Trull

Precision and Choice of Words Matter



Jonathan Trull • You
Chief Security Officer @ Qualys | CISSP, CISA, OSCP
5mo •

My 2 cents but I think the most dangerous word in the cybersecurity vernacular today is "critical." I probably hear it 50 times a day from vendors, my team, other teams, consultants, auditors and see it within most security products, etc. My fear is that everyone is now immune to the importance of a word like "critical" because of it's overuse and misuse. My wife is a critical care doctor and when they say a patient is critical it invokes an immediate, all hands response as it is a matter of life or death for someone. The time has come for a greater focus on cyber risk quantification and to ensure that we are using business language to communicate with our peer executives, board, and risk committees. **Sumedh Thakar Richard Seiersen**

This is the kind of thing that ends companies.

Our system is 100% secure.

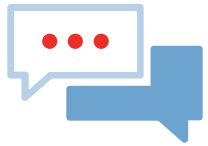
There is no risk to our data because we use encryption.

Please approve this security exception, the risk is low.

Deny the security exception as the risk is CRITICAL.

Perils of Risk Assessment Without Quantification

The Psychology of Security



Security is both a feeling and a reality. And they're not the same. The **reality of security is mathematical,** based on the probability of different risks and the effectiveness of different countermeasures . . .

But security **is also a feeling,** based not on probabilities and mathematical calculations, but on **your psychological reactions** to both risks and countermeasures.

- Bruce Schneier, 2008

Perils of Qualitative Risk Assessments

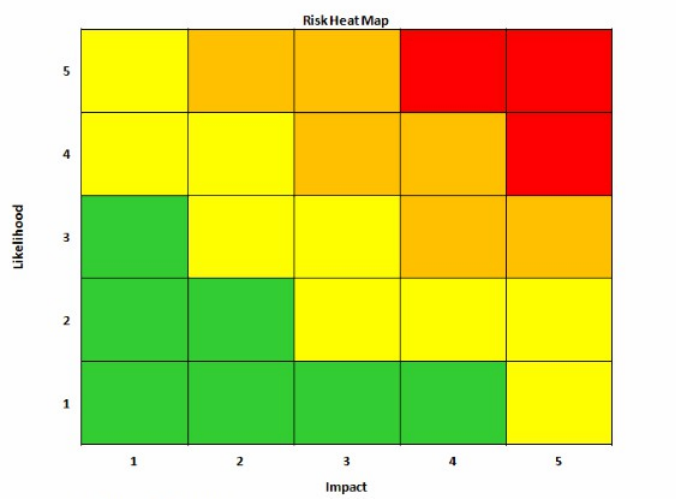
- Subjectivity and bias
- Lack of precision
- Inaccurate results
- Stakeholder confusion and miscommunication

Risk Quantification Adoption Journey

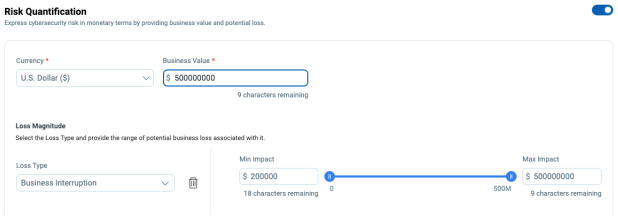
Project Narratives and Operational Metrics

- 122 vendor security assessments were performed
- Patching SLA breached by engineering
- New SIEM deployed

Heat Map by Business Function



Adoption of QLYS TruRisk & KRIs



Top Down, Bottom Up, or Hybrid Approach

Where should you start?

Executive Governance & Oversight	Are we secure? What is the likelihood we'll experience a material breach?
Buying Cyber Insurance	
Budget, Policy, & Strategy Setting	Where should I invest to reduce the company's risk?
Security Exception / Change Review Board	Should I approve this security exception? How much financial risk does it add?
GRC Activities	
Vulnerability Mgmt.	Do I need to patch this vulnerability now, or can I wait? How do I prioritize my work?
AppSec Testing & Remediation	
Security Architecture & Engineering	Do we need a new MFA solution? How should I configure it?

Insights from the Frontlines

Risk quantification requires a top-level change in strategy, policy, executive alignment, and training

To achieve enterprise scale, a new cybersecurity risk fabric is needed that can ingest and normalize a wide range of data

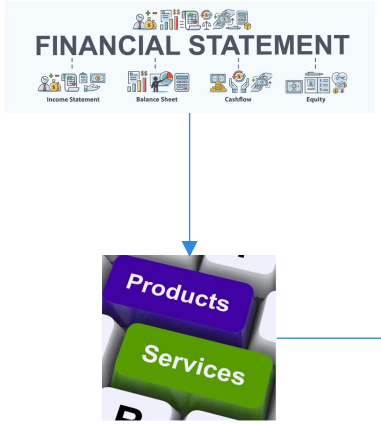
Don’t get lost in the trees - focus time and energy quantifying risks that are essential and supportive of better decision making

Set guardrails on how loss magnitude will be determined

Automate risk quantification and decision making if possible (e.g., Zero Trust)

Framework for Operationalizing Risk Quantification at Scale

Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
Identify Business Drivers	**Inventory Digital Assets & Map to Products & Services**	**Identify, Ingest, & Normalize Risk Signals**	**Establish Thresholds & Define Actions**	**Monitor and Fine Tune**



TruRisk™ Summary: ACME Corp

Download Report

TruRisk™ Score

Last Calculated: 22 May 2024 11:36 AM

Total Assets 110K

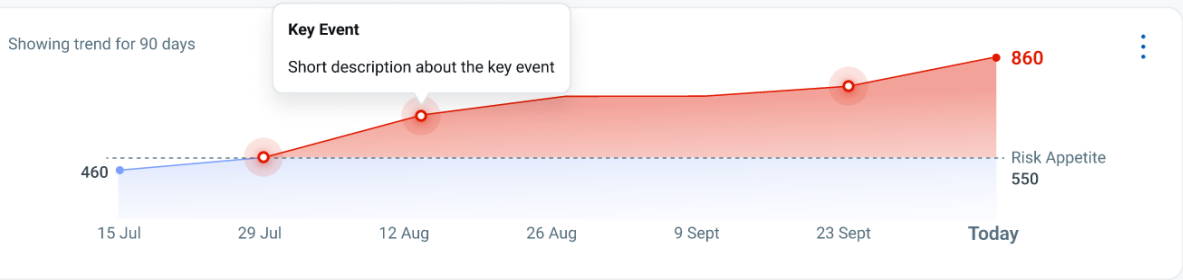
Risk Appetite
4/10 business entities are above risk appetite

Asset Exposure
40 Critical internet exposed assets

+62 pts Since last 7 Days

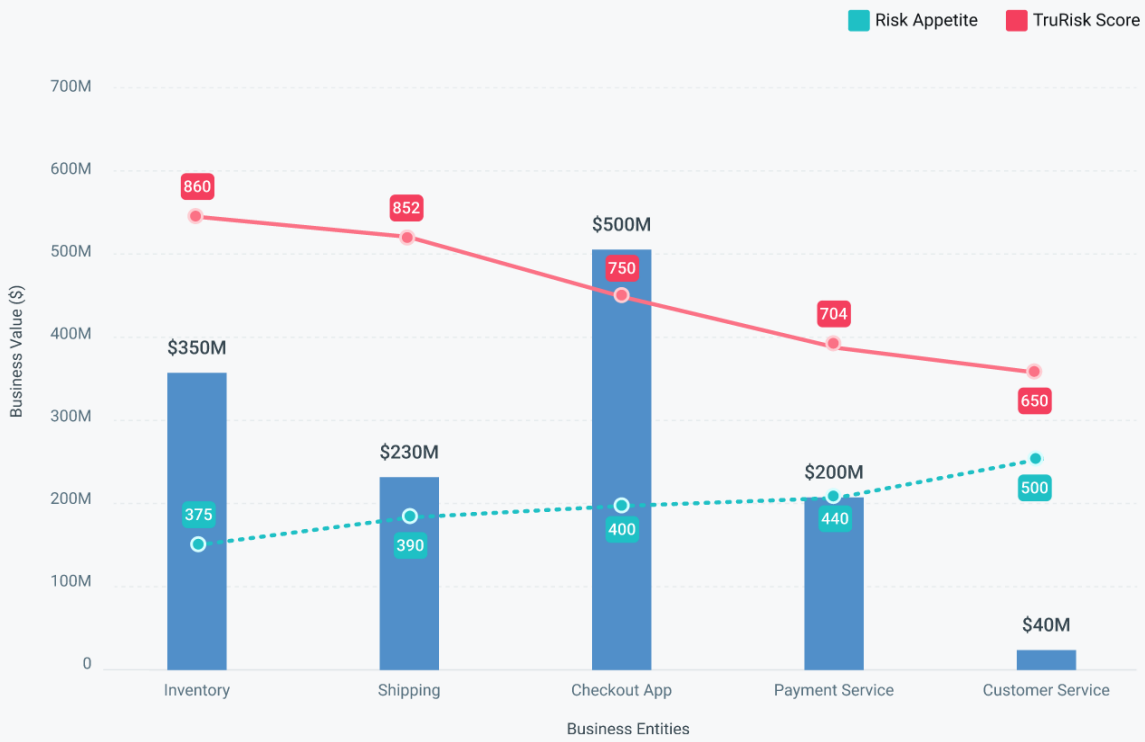
Top Risk Factors

143.2K Weaponized Vulns
20.4K Associated Threat Actors
92.4K Critical Failed Controls
19 Weak Credentials



Business Entities

View All | Create Business Entity



Key Highlights

Take a look at some of the key highlights that we've gathered