UNLOCKING THE VALUE OF CYBER RISK QUANTIFICATION

SVAM
INTERNATIONAL, INC.

Kiran Bhujle
kbhujle@svam.com
908-590-1445

October 19, 2023

Agenda


What is Quantification


Need for CRQ


Benefits of CRQ


Approach


Evaluating Cyber Investments


Loss event Scenario


Call to Action

Kiran Bhujle

SVAM Cybersecurity Practice Leader
kbhujle@svam.com
908-590-1445

Global Managing Director at SVAM International, Kiran oversees SVAM's Security Advisory Group, with over 25 years of experience in IT Risk and Cybersecurity.

- Previously Cyber & Technology Risk Client Executive at CohnReznick, Access Risk Transformation Leader at Ernst & Young, IBM Global Business Services, and Deloitte.
- Harvard Business Review - Cybersecurity Advisory Board.
- Forbes Technology Council - Executive member.
- Adjunct faculty at Columbia University focusing on IT Risk Management and Operational Risk Management courses for the Enterprise Risk Management Master's Program.

What is Quantification

Cyber Risk Quantification: Assessing the potential financial impact of an individual cyber threat to your business
- estimate ranges of monetary loss resulting from different cybersecurity events.
- justify security costs and demonstrate how effective security measures can result in significant cost savings.

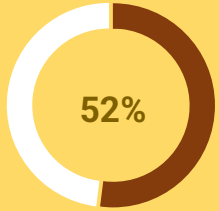
Global Average Cost

$4.45M USD — The global average cost of a data breach

Average Data Breach Life Cycle

277 Days — In 2023, the average Data Breach lifecycle recovery time was **277 days**

Personally Identifiable Information



Breaches contained customer PII

Top Initial Attack Vectors

01 Phishing

02 Zero-Day Vulnerabilities

03 Stolen/Compromised Credentials

04 Cloud Migration / Misconfiguration

05 Business Email Compromise (BEC)

Source: IBM Cost of a Data Breach Report 2023

Need for Quantitative Assessments (vs Qualitative)

		Impact		
		Low	Medium	High
Probabilty	Low	Low Risk	Low Risk	Medium Risk
	Medium	Low Risk	Medium Risk	High Risk
	High	Medium Risk	High Risk	High Risk

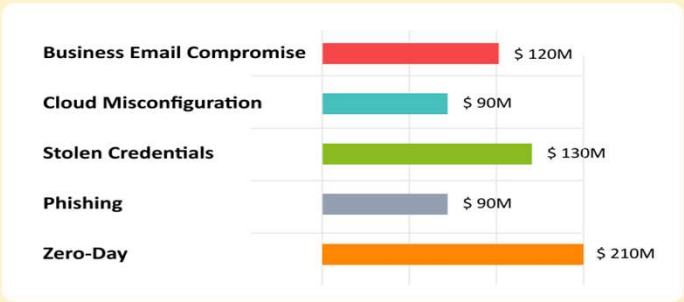
Qualitative Risk Assessment Table

→ Determine subjective level of risk (low/medium/high)

→ Opinion-based input of
-Risk
-Threat
-Vulnerability

→ Reduction of Cyber Risk

Qualitative **Quantitative**



→ Provides monetary value of risk

→ Accurately define risk in different scenarios per asset

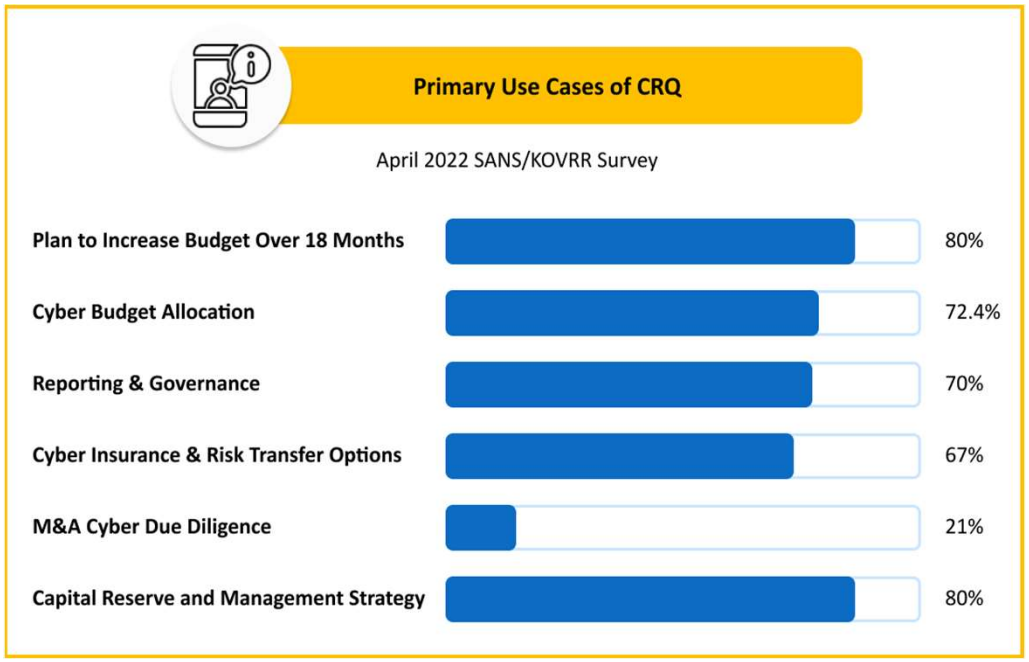
→ Assists in Resource Allocation

Source: IBM Cost of a Data Breach Report 2023

Benefits for CRQ

- Identify and align controls to a component based on the likelihood that a weakness will be exploited
- Integrated view of cybersecurity risk across all organizational systems, devices, and components
- Equips system owners and key stakeholders with relevant and actionable risk insights
- Empowers Data-Driven insights to facilitate ongoing decision-making
- Interactive dashboards across multiple facets and frameworks

Evaluating Cyber Security Investments



- CRQ can aid in assessing Return on Investment (ROI) for cyber initiatives
- Cost Mitigation – Insurance Protection mitigated average cost of data breach by - $196,452
- Investment in KnowBe4 phishing tests reduced the risk of successful phishing attacks and saved the organization from financial impact

Source: SANS/KOVRR Survey

Approach / Methodology

- **Emphasis on Data Life Cycles / Risk Profiles**

By Mapping out the data lifecycle, organizations can determine critical risk areas such as data storage and transmission.

- **Scenario-Based Situations**

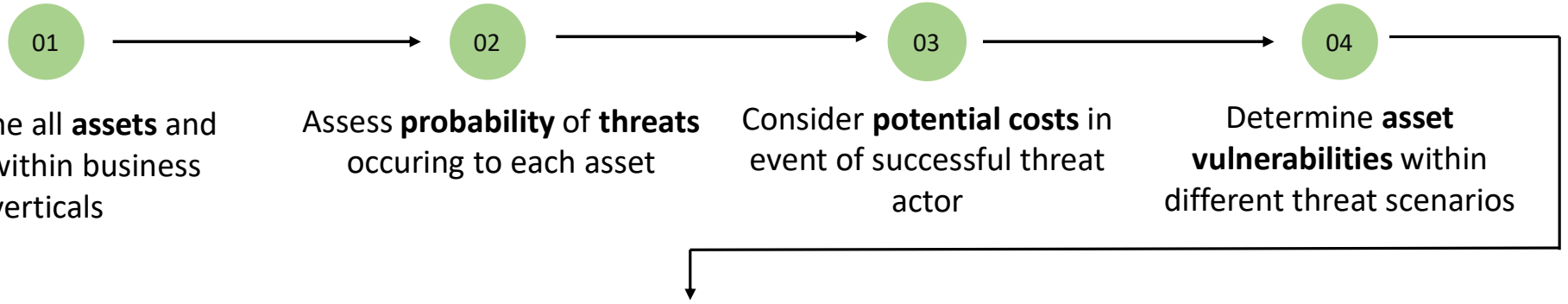
CRQ assesses the financial impact of scenarios such as data breaches or Zero-Day attacks, helping with Risk Mitigation Planning based on data criticality.

- **Focus on Asset Values**

Make informed decisions on which protection strategies to implement for different assets.

- **Employing Quantitative Techniques commonly used in a wide range of industries for statistical insight**
  - Monte Carlo Simulation
  - Expected Loss Models
  - Value-at-Risk (VaR)
  - Cyber Insurance Modeling

Prioritizing and Measuring Cyber Risks

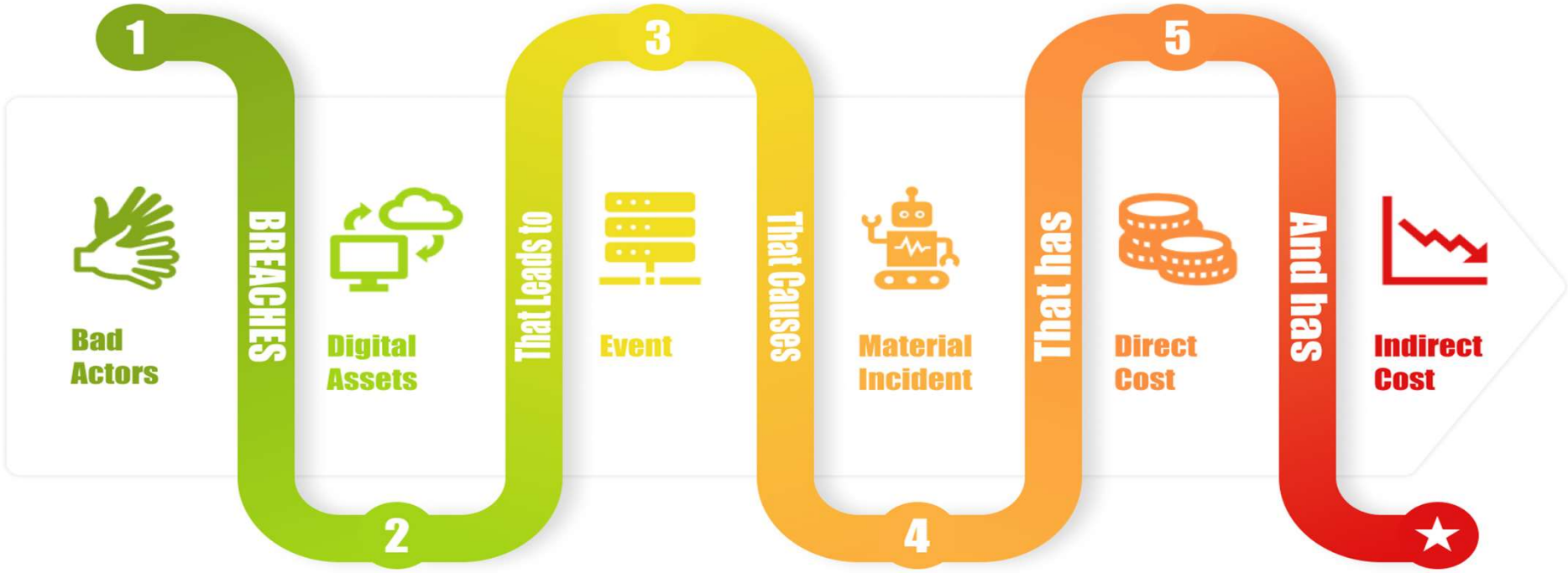


05

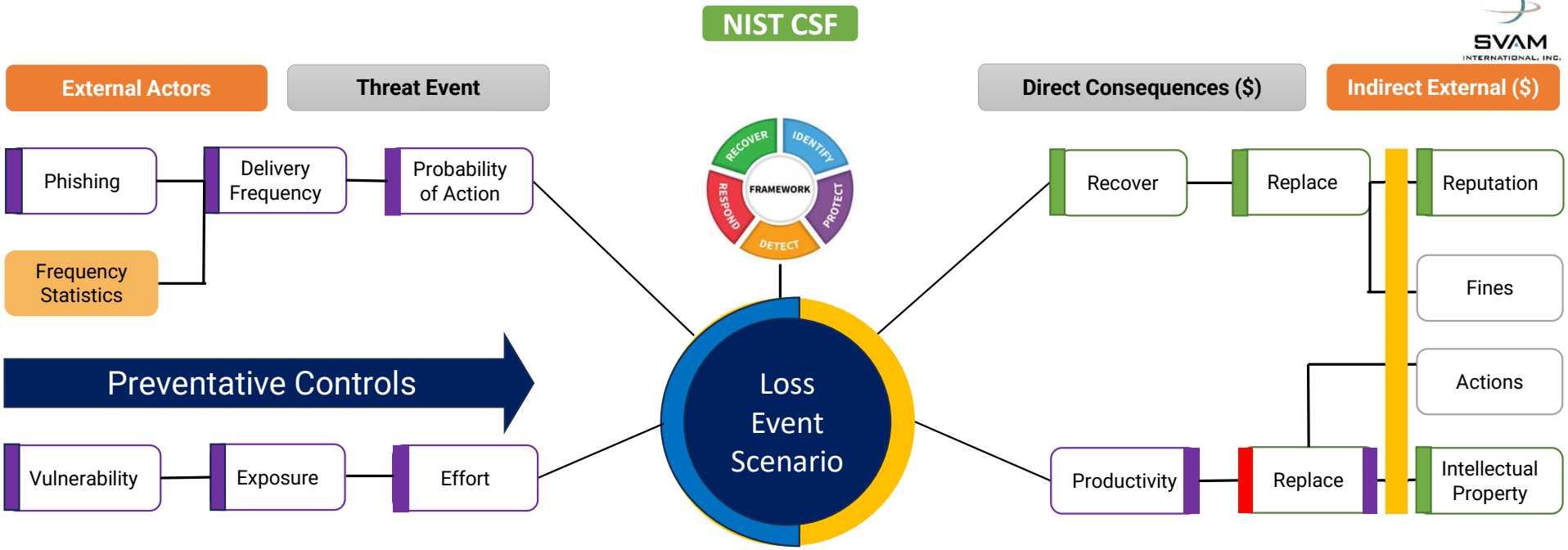
- CRQ assigns a monetary value to each risk
  - Allowing organizations to prioritize/allocate resources effectively
- Results in reduction of potential financial losses, mitigate top risks first
- Assists in developing prioritized list of security actions based on assessment of business and financial risk

Loss Event Scenario

PART 1



PART 2



- Most Prevalent Attack Vector – Phishing
- 2nd most expensive with associated costs of $4.76 million

- Top 3 Data Breach Cost Mitigating Factors
  - DevSecOps approach -$249,278
  - Employee Training -$232,867
  - IR Plan and Testing -$232,008

Source: IBM Cost of a Data Breach Report 2023

Call to Action

- **Identify Variables**: The first step is identifying the variables contributing to the risk. In cybersecurity, these factors are the number of incidents or attacks, frequency, probability of actions, and their associated losses

- **Assign Probability Distributions**: Each variable is assigned a probability distribution. This could be normal, uniform, or any other type of distribution, depending on the nature of the variable

- **Perform Simulations**: Monte Carlo simulation constructs outcomes of various scenarios using values from a probability distribution for any factor with inherent uncertainty. The analysis then uses random values from these probability distributions and puts them through different equations for different results

- **Analyze Results**: The results of these simulations are then analyzed to provide a range of possible outcomes and the probabilities that they will occur. This provides a much more informative and valuable understanding of risk than just providing the average loss

- **Make Decisions**: The results of the Monte Carlo simulation can then be used to make informed decisions about risk management. For example, it can help enterprises proactively secure their digital estate against real-world threats

Recap

- **Precise Risk Assessment:**

CRQ provides a data-driven, precise approach to assessing and quantifying cyber risks, enabling organizations to make informed decisions

- **Resource Allocation:**

With CRQ, organizations can allocate resources effectively by prioritizing risks based on their financial impact, focusing efforts where they matter most

- **ROI Assessment:**

CRQ assists in evaluating the return on investment (ROI) for cybersecurity initiatives, ensuring that investments align with risk reduction and cost savings

- **Effective Communication:**

Clear, data-driven communication of cyber risks to stakeholders and the board is essential for informed decision-making and maintaining trust

- **Informed Strategy:**

By quantifying risks, CRQ guides the development of a strategic cybersecurity roadmap

SVAM
INTERNATIONAL, INC.

Thank you!

Kiran Bhujle

SVAM Cybersecurity Practice Leader

kbhujle@svam.com