STUDY GUIDE: Quantitative Risk Calculations for GRC Professionals

Prepared by: Aminu Idris, AMCPN

1. Introduction to Security Metrics

Why We Quantify Risk

- **Business Language:** Executives understand dollars, not just "high/medium/low" risk
- **Budget Justification:** Prove why security investments are needed
- **Performance Measurement:** Show if security controls are actually working
- **Compliance Requirements:** Many regulations require quantitative risk assessment

Key Concepts

- **Risk:** Potential for loss due to a threat exploiting a vulnerability
- **Vulnerability:** Weakness in your defenses
- **Threat:** Something that can exploit a vulnerability
- **Impact:** The cost if a threat succeeds

2. Fundamental Phishing Metrics

Basic Rate Calculations

Formula: Rate = (Number of Events ÷ Number of Emails Sent) × 100*

Example:

- Emails Sent: 200
- Emails Opened: 150
- Open Rate = (150 ÷ 200) × 100 = **75%**

Key Metrics to Calculate:

1. **Email Open Rate** = (Opened ÷ Sent) × 100
2. **Click-Through Rate (CTR)** = (Clicked ÷ Sent) × 100
3. **Credential Submission Rate** = (Credentials Submitted ÷ Sent) × 100
4. **Data Entry Rate** = (Data Submitted ÷ Sent) × 100

Conversion Metrics

How effective is each step of the attack?

Formulas:

- **Open-to-Click Conversion** = (Clicked ÷ Opened) × 100
- **Post-Click Submission** = (Credentials Submitted ÷ Clicked) × 100

Example:

- Opened: 150
- Clicked: 90
- Credentials Submitted: 45
- Open-to-Click = (90 ÷ 150) × 100 = **60%**
- Post-Click Submission = (45 ÷ 90) × 100 = **50%**

3. Financial Risk Calculations

Annualized Loss Expectancy (ALE)

This is your most important risk calculation

Formula: ALE = SLE × ARO

Where:

- **SLE** (Single Loss Expectancy) = Cost of one successful breach
- **ARO** (Annual Rate of Occurrence) = How many times per year you expect it to happen

Example Calculation:

- Cost of one data breach (SLE): $5,000,000
- Expected breaches per year (ARO): 2
- ALE = $5,000,000 × 2 = **$10,000,000**

Projecting Organizational Risk

Scaling your phishing results to the entire company

Formula: Projected Victims = Total Employees × Phishing Success Rate

Example:

- Total Employees: 2,000
- Phishing Credential Rate: 15%
- Projected Victims = 2,000 × 0.15 = **300 employees**

4. Statistical Analysis for GRC

Confidence Intervals

How reliable are your results?

Formula for 95% Confidence Interval:
$p \pm 1.96 \times \sqrt{[p(1-p)/n]}$

Where:

- p = success rate (as decimal)
- n = sample size
- 1.96 = constant for 95% confidence

Example:

- Phishing success rate: 20% ($p = 0.20$)
- Sample size: 100 employees ($n = 100$)
- Calculation:
  1. $\sqrt{[0.20(1-0.20)/100]} = \sqrt{[0.16/100]} = \sqrt{0.0016} = 0.04$
  2. $1.96 \times 0.04 = 0.0784$
  3. Confidence Interval: 0.20 ± 0.0784 = **12.16% to 27.84%**

Interpretation: We're 95% confident the true phishing success rate for our entire organization is between 12.16% and 27.84%

5. Cost-Benefit Analysis for Security Controls

Return on Investment (ROI)

Formula: ROI = (Benefit - Cost) ÷ Cost × 100

Example:

- Security Control Cost: $100,000
- Risk Reduction Benefit: $2,000,000
- ROI = ($2,000,000 - $100,000) ÷ $100,000 × 100 = **1,900%**

Risk Reduction Calculation

How much risk does a control actually eliminate?

Formula:
New Risk = Current Risk × (1 - Control Effectiveness)

Example:

- Current ALE: $10,000,000
- Control Effectiveness: 90%
- New ALE = $10,000,000 × (1 - 0.90) = **$1,000,000**

- Risk Reduction = $10,000,000 - $1,000,000 = **$9,000,000**

6. Practical Examples & Exercises

Exercise 1: Basic Metrics

Scenario: You send a phishing test to 500 employees

- 400 open the email
- 250 click the link
- 75 submit credentials

Calculate:

1. Open Rate = ? (400/500)*100 = 80
2. Click-Through Rate = ? (250/500)*100 = 50
3. Credential Submission Rate = ? (75/500)*100 = 15
4. Open-to-Click Conversion = ? (250/400)*100 = 62.5
5. Post-Click Submission Rate = ? (75/250)*100 = 30

Exercise 2: Financial Impact

Scenario:

- Company Size: 5,000 employees
- Phishing Credential Rate: 12%
- Cost per Data Breach: $8,000,000
- Probability of breach if credentials stolen: 30%

Calculate:

1. Projected credential thefts = ? 5000 * 0.12 = 60
2. Expected breaches per year = ?
3. Annualized Loss Expectancy (ALE) = ?

Exercise 3: Control Justification

Scenario:

- Current ALE: $15,000,000
- Proposed MFA Cost: $250,000
- MFA Effectiveness: 99.9%

Calculate:

1. New ALE with MFA = ? $15,000,000 * (1 - 99.9%) = $15,0
2. Risk Reduction = ? $15,000,000 - $15,000 = $14,985,0
3. ROI = ?

7. Real-World Industry Benchmarks

Average Phishing Rates (2024 Data)

- **Open Rate:** 30-40% (varies by industry)
- **Click-Through Rate:** 10-15%
- **Credential Submission:** 3-5%
- **Data Breach Cost:** $4.45 million average

Control Effectiveness

- **MFA:** 99.9% reduction in account takeover
- **Security Training:** 40-60% reduction in phishing susceptibility
- **Email Filtering:** 70-90% of malicious emails blocked

8. Common Mistakes to Avoid

1. **Sample Size Too Small:** Results from testing 50 people don't represent 5,000 employees
2. **Ignoring Statistical Significance:** Small variations might be random chance
3. **Overestimating Control Effectiveness:** No control is 100% effective
4. **Forgetting Ongoing Costs:** Training needs refreshers, software needs renewals
5. **Underestimating Indirect Costs:** Reputation damage, stock price impact, customer churn

9. Quick Reference Formulas

Basic Metrics

text

Open Rate = (Opened ÷ Sent) × 100

CTR = (Clicked ÷ Sent) × 100

Credential Rate = (Credentials ÷ Sent) × 100

Financial Risk

text

ALE = SLE × ARO

Projected Victims = Total Employees × Success Rate

$$\text{ROI} = (\text{Benefit} - \text{Cost}) \div \text{Cost} \times 100$$

Statistical Reliability

text

$$95\% \text{ CI} = p \pm 1.96 \times \sqrt{[p(1-p)/n]}$$

10. Preparation Checklist

Before starting the lab, make sure you can:

- Calculate basic percentages and rates
- Understand the difference between "rate" and "conversion"
- Perform multi-step calculations (A leads to B leads to C)
- Convert between percentages and decimals
- Use a calculator for square roots and exponents
- Explain what "95% confidence" means in practical terms
- Calculate Return on Investment (ROI)
- Scale results from a sample to a larger population

STUDY TIPS

1. **Practice with the exercises** above until you're comfortable
2. **Understand the logic** behind each formula, don't just memorize
3. **Use real calculators** - don't rely on mental math for complex calculations
4. **Think in steps** - break complex problems into smaller pieces
5. **Always check your work** - do the results make sense?

Remember: You're learning to speak the language of business. The ability to quantify risk in financial terms is one of the most valuable skills a GRC professional can have!

This study guide will prepare you for the intensive calculations in the upcoming lab. Review these concepts and practice the exercises until you feel confident with each type of calculation.