Date: 03/10/2025

Lab 3: Advanced GRC Phishing Simulation & Quantitative Risk Analysis

1. Introduction

Welcome to the ULTIMATE phishing risk analysis lab! As a GRC professional, you must not only understand human risk but be able to QUANTIFY it in financial terms that executives understand. This lab will transform you from someone who "knows phishing is bad" to someone who can PROVE exactly how bad it is with hard numbers and financial calculations.

2. Scenario

You are the lead GRC analyst at "GlobalTech Inc." The CISO has provided you with data from THREE different phishing simulations conducted last quarter. Your mission: conduct a comprehensive risk analysis that will determine next year's security budget and strategy.

3. Learning Objectives

- Master advanced phishing metric calculations
- Learn to calculate financial risk exposure
- Conduct cost-benefit analysis for security controls
- Create executive-level risk reports with quantitative justification
- Understand statistical significance in security testing

4. Lab Data Set

Campaign Results:

Campaign A: "HR Bonus Notification"

- Target Group: 100 Employees
- Emails Sent: 100
- Emails Opened: 82
- Links Clicked: 47
- Credentials Submitted: 18
- Data Entry Points: 5 (employees who also entered personal information)

Campaign B: "IT System Password Reset"

- Target Group: 250 Employees
- Emails Sent: 250
- Emails Opened: 200

- Links Clicked: 150
- Credentials Submitted: 75
- Data Entry Points: 25

Campaign C: "CEO Urgent Document Review"

- Target Group: 80 Executives & Assistants
- Emails Sent: 80
- Emails Opened: 72
- Links Clicked: 60
- Credentials Submitted: 12
- Data Entry Points: 8

Organizational Context:

- Total Employees: 2,000
- Average Employee Salary: $85,000/year
- Estimated Cost of Data Breach: $4.35 million (industry average)
- Probability of Major Breach if Credentials Stolen: 25%

PHASE 1: BASIC METRIC CALCULATIONS

Step 1: Calculate Fundamental Rates

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

YOUR TURN: Fill in the blanks

Answer:

Campaign	Email Open Rate	Click-Through Rate	Credential Submission Rate	Data Entry Rate
A	(82/100)×100 = **82%**	(47/100)×100 = 47%	(18/100)×100 = 18%	(5/100)×100 = 5%
B	(200/250)×100 = 80%	(150/250)×100 = 60%	(75/250)×100 = 30%	(25/250)×100 = 10%
C	(72/80)×100 = 90%	(60/80)×100 = 75%	(12/80)×100 = 15%	(8/80)×100 = 10%

Step 2: Calculate Efficiency Metrics

How effective is each step of the attack?

Conversion Rate from Open to Click:

- Campaign A: (47/82)×100 = **57.3%**
- Campaign B: (150/200)×100 = 75%
- Campaign C: (60/72)×100 = 83.3%

Post-Click Credential Submission Rate:

- Campaign A: (18/47)×100 = 38.3%
- Campaign B: (75/150)×100 = 50%
- Campaign C: (12/60)×100 = 20%

PHASE 2: ADVANCED RISK QUANTIFICATION

Step 3: Calculate Organizational Risk Exposure

Scaled Risk Projection:
If these rates apply to our entire organization of 2,000 employees...

For Campaign B (most successful):

- Expected Credentials Stolen: 2,000 × (75/250) = 600 **employees**
- Expected Data Breaches: 600 × 25% probability = 150 **breaches**

CALCULATION:

- Campaign B Credential Rate: 75/250 = 30%
- Organization Exposure: 2,000 × 0.30 = **600 employees**
- Expected Breaches: 600 × 0.25 = **150 breach incidents**

Step 4: Financial Impact Analysis

A. Calculate Potential Financial Loss:

- Single Breach Cost: $4,350,000
- Expected Number of Breaches: 150
- Total Exposure: $4,350,000 × 150 = **$652,500,000**

B. Calculate Annualized Loss Expectancy (ALE):
ALE = Single Loss Expectancy × Annual Rate of Occurrence

- Single Loss Expectancy (SLE): $4,350,000
- Annual Rate of Occurrence (ARO): 150 expected breaches
- ALE = $4,350,000 × 150 = **$652,500,000**

Step 5: Control Effectiveness Analysis

MFA Cost-Benefit Analysis:

- Cost to Implement MFA: $45 per user × 2,000 users = **$90,000**
- MFA Effectiveness: 99.9% reduction in credential theft impact
- Risk Reduction: $652,500,000 × 0.999 = **$651,847,500**
- **ROI: ($651,847,500 - $90,000) / $90,000 = 724,175%**

Security Training Cost-Benefit:

- Training Cost: $50 per user × 2,000 users = **$100,000**
- Expected Effectiveness: 60% reduction in click-through rates
- New Click-Through Rate: 30% × (1-0.60) = 12%
- New Credentials Stolen: 2,000 × 0.12 = 240
- New Expected Breaches: 240 × 0.25 = 60
- New ALE: $4,350,000 × 60 = **$261,000,000**
- **Risk Reduction: $652,500,000 - $261,000,000 = $391,500,000**
- **ROI: ($391,500,000 - $100,000) / $100,000 = 391,400%**

PHASE 3: COMPREHENSIVE RISK ASSESSMENT

Step 6: Complete Risk Assessment Matrix

Campaign	Overall Risk Score	Financial Exposure	Priority Level	Recommended Action
A	MEDIUM-HIGH	$156,600,000	2	Enhanced Training
B	**CRITICAL**	**$652,500,000**	**1**	**IMMEDIATE MFA**
C	HIGH	$104,400,000	2	Executive Training

CALCULATIONS FOR TABLE:

- Campaign A Exposure: (18/100)×2000 = 360 employees × 0.25 × $4,350,000 = $156,600,000
- Campaign C Exposure: (12/80)×2000 = 300 employees × 0.25 × $4,350,000 = $104,400,000
- Campaign B Exposure: (75/250)×2000 = 600 employees × 0.25 × $ 4,350,000= $652,500,000

Step 7: Statistical Significance Analysis

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

For Campaign B Credential Rate (30%):

- p = 0.30, n = 250

- Margin of Error = 1.96 × √[0.30(1-0.30)/250] = 1.96 × √(0.21/250) = 1.96 × √0.00084 = 1.96 × 0.029 = 0.057
- **True Rate Range: 24.3% to 35.7%**

YOUR TURN: Calculate for Campaign A:

- p = 0.18, n = 100
- Margin of Error = 1.96 × √[0.18(1-0.18)/100] = 0.0752
- True Rate Range: 10.5% to 25.5%

PHASE 4: EXECUTIVE REPORTING

Step 8: Comprehensive Executive Briefing

To: Board of Directors, CISO, CFO
From: GRC Risk Analysis Team
Date: 03-10-2025
Subject: CRITICAL: Quantitative Phishing Risk Assessment & $652M Exposure

1. Executive Summary:
Our phishing simulation analysis reveals a **CRITICAL risk exposure of $652 million** annually. The "IT Password Reset" campaign showed 30% credential theft rate, projecting to 600 compromised accounts organization-wide. Immediate action is required.

2. Key Quantitative Findings:

Risk Metric	Value	Industry Average	Severity
Overall Credential Theft Rate	22.1%	15.3%	HIGH
Maximum Campaign Success Rate	30%	18.7%	CRITICAL
Annualized Loss Expectancy	$652M	$285M	SEVERE
MFA Implementation ROI	724,175%	350%	EXCELLENT

3. Detailed Financial Analysis:

Current State Risk:

- Annualized Loss Expectancy: **$652,500,000**
- Probability of Major Breach: **93.75%** (150 expected breaches)
- Per-Employee Risk: ALE/Total employee= $652,500,000/2000**= $326,250**

Proposed Security Investment Portfolio:

Control	**Cost**	**Risk Reduction**	**Net Benefit**	**ROI**	**Priority**
MFA Implementation	$90,000	$651.8M	$651.7M	724,175%	**1**

Enhanced Training	$100,000	$391.5M	$391.4M	391,400%	**2**
Email Filtering	$50,000	$130.5M	$130.4M	260,800%	**3**
Phishing Simulation Program	$25,000	$65M	$64.97M	259,900%	2
Continous Security Monitoring	$150,000	$195M	$194.85M	129,900%	3

4. Strategic Recommendations:

IMMEDIATE ACTIONS (Q1):

1. **Implement MFA enterprise-wide** - $90,000 investment
2. **Launch targeted phishing simulation program** - $25,000
3. **Conduct emergency security awareness training** - $100,000

STRATEGIC INITIATIVES (FY2024):

1. **Deploy advanced email security gateway** - $50,000
2. **Establish continuous security monitoring** - $150,000
3. **Implement security behavior analytics** - $75,000

5. Expected Risk Posture After Controls:

Metric	Current	With Controls	Reduction
Credential Theft Rate	22.1%	2.2%	90%
Annual Loss Expectancy	$652M	$65M	90%
Breach Probability	93.75%	25%	73.3%

Total Investment Required: $490,000
Total Risk Reduction: $587,500,000
Net Financial Benefit: $587,010,000

DELIVERABLES

Submit the following completed items:

1. **Completed Calculation Worksheets** from Phases 1 & 2
2. **Risk Assessment Matrix** from Phase 3
3. **Statistical Analysis** with confidence intervals
4. **Executive Briefing** with your specific financial calculations
5. **Control Recommendation Table** with your ROI calculations

BONUS CHALLENGE:
Calculate the break-even point for our security investments. If we invest $490,000 in controls, how many breaches must we prevent to justify the cost?

Hint: $490,000 / $4,350,000 per breach = 0.1126 breaches*

LAB CONCLUSION

You have now mastered the art of quantitative risk analysis for human factors. You can:

- Translate phishing metrics into financial terms
- Calculate ROI for security controls
- Conduct statistical analysis of security data
- Present compelling business cases for security investment

This is what separates junior analysts from strategic GRC leaders. You're not just identifying risks you're quantifying them and proving the value of security in the language business understands: **DOLLARS AND CENTS.**

Remember: If you can't measure it, you can't manage it. Now you can measure AND manage human risk like a pro!