Lab 3 Assignment: Advanced GRC Phishing Simulation & Quantitative Risk Analysis

Student Name: Oluwatimilehin Oluwagbemi

Reg. No: 2025/GRC/10712

Date: 7th October, 2025

Executive Briefing

To: Board of Directors, CISO, CFO

From: GRC Risk Analysis Team

Date: 07-10-2025

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: $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

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

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

Phase 1: Basic Metric Calculations

Step 1: Fundamental Rates Calculation

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

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

Step 2: Efficiency Metrics Calculation

Conversion Rate from Open to Click:

- Campaign A: (47/82) x 100 = 57.3%
- Campaign B: (150/200) x 100 = 75%
- Campaign C: (60/72) x 100 = 33.3%

Post-Click Credential Submission Rate:

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

Phase 2: Advanced Risk Quantification

Step 3: Organizational Risk Exposure Calculation

For Campaign B (most successful):

- Expected Credentials Stolen: 2,000 x (75/250) = 2,000 x (72/250) = 600 employees
- Expected Data Breaches: 600 x 25% probability = 150 breaches

Calculation:

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

Step 4: Financial Impact Analysis

A. Potential Financial Loss:
- Single Breach Cost: $4,350,000
- Expected Number of Breaches: 150
- Total Exposure: $4,350,000 x 150 = $625,500,000

B. Annualized Loss Expectancy (ALE):

ALE = Single Loss Expectancy x Annual Rate of Occurrence

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

Step 5: Control Effectiveness Analysis

MFA Cost-Benefit Analysis:

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

Security Training Cost-Benefit:

- Training Cost: $50 per user x 2,000 users = $100,000
- Expected Effectiveness: 60% reduction in click-through rates
- New Click-Through Rate: 30% x (1-0.60) = 12%
- New Credentials Stolen: 2,000 x 0.12 = 240
- New Expected Breaches: 240 x 0.25 = 60
- New ALE: $4,350,000 x 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) x 2000 = 360 employees x 0.25 x $4,350,000 = $156,600,000
- Campaign C Exposure: (12/80) x 2000 = 300 employees x 0.25 x $4,350,000 = $104,400,000

Step 7: Statistical Significance Analysis

Calculate Confidence Intervals (95% Confidence):

For Campaign B Credential Rate (30%):

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

For Campaign A Credential Rate (18%):

- p = 0.18, n = 100
- Margin of Error = 1.96 x √ [0.18(1-0.18)/100] = 1.96 x √[0.1476/100] = 1.96 x √0.001476 = 1.96 x 0.038 = 0.07448; 0.18 + 0.07448 = 0.25448 x 100 = 25.4%; 0.18 – 0.07448 = 0.10552 x 100 = 10.6%
- True Rate Range: 10.6% to 25.4%

For Campaign C Credential Rate (15%):

- p = 0.15, n = 80
- Margin of Error = 1.96 x √[0.15(1-0.15)/100] = 1.96 x √[0.1275/100] = 1.96 x √0.001275 = 1.96 x 0.036 = 0.07056; 0.15 + 0.07056 = 0.22056 x 100 = 22.1%; 0.15 – 0.07056 = 0.07944 x 100 = 7.9%
- True Rate Range: 7.9% to 22.1%

Bonus Challenge:

Break-even point for our security investments. Investing $490,000 in controls, how many breaches must we prevent to justify the cost.

$490,000 / $4,350,000 per breach (150 breaches)= 16.8965517 approximately 16.9 breaches must be prevented to justify the cost.