Lab 3: Advanced GRC Phishing Simulation & Quantitative Risk Analysis

Reg No: 2025/GRC/11032

Deliverable 1: Completed Calculation Worksheets (Phases 1 & 2)

Campaign	Email Opened Rate	Click Through Rate	Credential Submission Rate	Data Entry Rate
A	[82/100]x100= 82%	[47/100]x100= 47%	[18/100]x100= 18%	[5/100]x100= 5%
B	[200/250]X100= 80%	[150/250]x100= 60%	[75/250]X100= 30%	[25/250]X100= 10%
C	[72/80]X100= 90%	[60/80]X100= 75%	[12/80]X100= 15%	[8/80]X100= 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 = 83.33%

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%

Risk Assessment Matrix (Phase 3)

Campaign	Overall Risk Score	Financial Exposure	Priority Level	Recommended Action
A	MEDIUM-HIGH	(18/100)×2000 × 0.25 × $4,350,000 = $156,600,000	2	Enhanced Training
B	CRITICAL	(75/250)×2000 × 0.25 × $4,350,000 = $652,500,000	1	Immediate MFA
C	HIGH	(12/80)×2000 ×	2	Executive

		0.25 × $4,350,000 = $104,400,000		Training

Statistical Analysis With Confidence Intervals

Campaign A (18%, n=100):

- p = 0.18
- Margin of Error = 1.96 × √[0.18×0.82 / 100]
- = 1.96 × √(0.1476 / 100)
- = 1.96 × √0.001476
- = 1.96 × 0.0384 ≈ **0.075** (7.5%)
- = 0.18−0.075=0.105. (10.5%)
- = 0.18+0.075=0.255 (25.5%)
- True Rate Range = **10.5% – 25.5%**

4. Executive Briefing

To: Board of Directors, CISCO, CFO
From: GRC Risk Analysis Team
Date: 1/10/2025
Subject: CRITICAL: Phishing Stimulation Risk Exposure

Executive Summary:

Our phishing simulations show that the organization faces very high levels of risk exposure.

- **Campaign A** resulted in an 18% credential capture rate. This translates into a potential financial exposure of about **$156.6 million**, with the true risk likely falling between 10.5% and 25.5%.

- **Campaign B** was the most concerning, with a 30% credential capture rate. This equates to a projected exposure of about **$652.5 million**. Even at the lower end of the confidence interval (24.3%), the financial impact would still be extremely damaging.

- **Campaign C** showed a 12% credential capture rate, giving us an exposure of roughly **$104.4 million**.

Taken together, these campaigns show potential losses of about **$913 million**. With the cost of a single breach averaging **$4.35 million**, even a small number of successful incidents could create catastrophic financial consequences.

Key Quantitative Findings

Risk Metrics	Value	Industry Average	Severity
Overall Credential Theft Rate	22.1&	15.3%	HIGH
Maximum Campaign Success Rate	30%	18.7%	CRITICAL
Annualized Loss Expectancy [ALE]	$652m	$285m	SEVERE
MFA Implementation ROI	724.175	350%	EXCELLENT

To address this, we recommend prioritizing strong preventive measures such as **multi-factor authentication**, **targeted employee awareness programs**, and **executive-level security training**. These controls provide substantial financial protection and can reduce our exposure by hundreds of millions of dollars.

5. Control Recommendation Table with ROI Calculations

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

Bonus Challenge

- Investment: $490,000
- Cost per breach: $4,350,000
- **Breaches to prevent:** 490,000 ÷ 4,350,000 ≈ **0.11**→ Preventing **even 1 breach** covers the investment.