Jesse Enriquez

M.S Project

Risk Management Framework Guide

Part One: Communities of Interest

Name	Role(s)	Responsibilities
Joe Shmoe	**Head of Agency**	**Oversees risk management process while promoting organization-wide collaboration and cooperation. Establishes a risk management strategy.**
Corey Stone	**Business Owner**	**Assist in the development of organization-wide plan/procedure**
Mary Berry	**Chief Acquisition Officer**	**Monitors and manages the performance of acquisition programs. Establishes procurement policies and practices. Ensures that the security and privacy requirements are defined in company policy**
Toby Toe	**Security Architect**	**Manages controls and coordination with system owners, common control providers, and security officers. Advises senior leadership on privacy and security issues. Manages the enterprise and architecture that protects the system and information from unauthorized activity.**

Part Two: Risk Management Plan

Purpose: There has been a critical preach within our company's security architecture, information is extremely vulnerable. The issue is a team/organizational-wide problem that needs to be solved.

Scope: Anything where mass amounts of information have become vulnerable and accessible to others/the public. This can be due to a hacker in or out of the company, or an emergency situation where everyone must vacate the building and safety requirements must be ignored.

Assumptions and Constraints: Information can be actively farmed and possibly sold to others for an undisclosed amount which would put our user base in further danger. This puts a constraint on our user's based personal information safe and enables the long-term loss of trust.

Sources of information: The source we will be receiving this emergency information from is our security team. Either the alarms built into the system will trigger and give us a warning that there has been a breach, or the team will manually discover the breach and notify the team immediately.

Table 2: Assets Classification

Information Assets	**Classification: Confidential, Private, Public**	**Impact on Profitability: Critical, High, Medium**	**Impact on Public Image: Critical, High, Medium**	**Impact on Revenue: Critical, High, Medium**	**Weighted Score / 100**
Web Server	Public	CRITICAL	High	Critical	99
Security Architecture	Private	Medium	Medium	Medium	70
Userbase private information server	Private	High	High	Medium	85

Part 3: Threat Assessment

Asset Vulnerability Assessment Table

Threat	**Possible vulnerabilities**	**Internal or External**	**Probability of occurrence/Success**	**Reputation loss if Successful**	**Financial loss if Successful**
Information extortion	Loss of private/company information	Both	50%	20%	20%
Data leak	Complete loss of a majority of company data	External	2%	80%	50%
DOS Attack	Deluge website with traffic	External	15%	10%	1-3%
Employee phished	Loss of important credentials	Internal	10%	5%	5-10%
Man in the middle attack	Private information leaked via trusted 3rd party	External	5%	20%	20%
Spyware	Loss of company information	Internal	7%	10%	5%
Computer Worms	Company information	Internal	3%	2%	10%
Natural Disaster	Information critically open	External	2%	30%	50%
Physical	Live	External	1%	20%	15%

threats (Robbery/building safely issues)	information left vulnerable				
Employee strike/walkout	Noone to watch over systems	internal	1%	40%	20%

Part Four: Risk Evaluation / Report Findings

Table 4:

Asset	**Vulnerability**	**Likelihood**	**Impact**	**Risk Rating Factor**
Web Server	Web Server which is our main source of activity could fail	3	3	8
Security Architecture	Can be harassed and effected by unwanted users.	2	4	9
Userbase private information server	If accessed, holds all of the users private information	2	6	9

Evaluation:

Any Risk factor that may be added at any point has to be taken seriously until fully solved. The threats the company can “live with” are any that have a risk factor of 4 or below. If it does not, it is an all-hands-on-deck situation until fully under control!