{REDACTED} Remediation Requirements Risk Management Plan

Prepared for

by Sean Cooper, on behalf of

Table of Contents

Revision Control Log

Date	Old Version #	New Version #	Revised By:	Description
Oct 6, 2014	0.0	0.1	Sean Cooper	Initial Document Composition
	0.1	1.0	Sean Cooper	Final Document Delivery

Executive Summary

Significant weakness exists in the IT controls for the business, as evidenced by the presence of virus/mal-ware on the end-user workstation terminals and previous account compromise. As analyzed, this was the highest roll-up risk (combination of risk likelihood and risk impact) to the organization.

Contributing factors to that conclusion included:

- Insufficient end-user security awareness training
- Non-standard, non-business software installed on user workstations
- Minimal or non-existent IT process and procedure documentation
- Shared account credentials between users
- Disclosed account credentials to managers

Significant weaknesses exist in the physical security controls for the business, as evidenced by the lack of normal security controls, such as:

- formal sign-in procedure
- no visible badges on employees / visitors
- lack of credentialed (electronic or physical) access control to the back-office spaces
- lack of credentialed (electronic or physical) access to the IT area when not in use
- unsecured backup tapes

Minimal environmental risks were present.

Introduction

A risk management plan is a document that provides guidance and processes that can be used to predict, estimate impact and prepare for risks that an enterprise faces. It also includes a risk assessment matrix of common possible risks that an organization faces, with a rating or categorization system to help implementers understand and anticipate the impact that those risks pose.

A risk is a technological, environmental, or personnel uncertainty that a specific condition or set of events arises that allows or empowers comprise of a services integrity, availability or confidentiality.

An example of some sorts of technological risks are:

- buffer overflow attacks
- stack smashing
- cross-site scripting attacks
- remote code execution attacks
- username / password compromise
- Advanced Persistent Threats (APTs)
- Open-Relay / Spam Generation

An example of some sorts of environmental risks are:

- earthquake
- fire
- flood
- civil unrest
- power / cooling unavailability
- “Act of God”
- biological attack
- nuclear attack

An example of some sorts of personnel risks are:

- striking workers
- insider threats
- corporate espionage actors
- nation state / terrorist actors
- personally identifiable information exfiltration
- theft of company assets (data or items)
-

A perceived risk has 4 possible mitigation strategies, typically expressed in the “ACAT” acronym:

Avoid, **C**ontrol, **A**ccept or **T**ransfer.

Depending on the anticipated likelihood and impact of occurrence, one of the aforementioned ACAT tactics will be employed to combat the risk.

Scope

This document is intended to lay out a plan to analyze and adopt a mitigation strategy to risks that have a business impact, such as the ones cited in the introduction section. It also includes a Risk Assessment Matrix (RAM) that lists several generalized risks, their impacts, and a recommended mitigation strategy. This RAM is not all-inclusive, but does attempt to list the most likely and most impactful risks facing your organization.

Limitations

Due to the real-time nature of Internet-connected systems, and complex configuration of most enterprise technology components, not all threat vectors and risks can be accurately modeled or anticipated. Every effort has been made to

While this document is a strong and necessary component of your Information Security policy, it must co-exist with business objectives and requirements, existing IT policies and procedures, and other information protection strategies.

References

For additional information on the subject, a “References” section has been added to this document, containing a list of other documents which provide guidance and template processes and procedures for this document.

Risk Assessment Process

A comprehensive risk assessment (CRA) is a formal report or document that consists of an analysis of an enterprises:

1. vulnerabilities / threats
2. likelihood of vulnerability / threat occurrence
3. loss or impact from vulnerability exploit or threat occurrence
4. theoretical effectiveness of security measures
5. mitigation strategy suggestions for dealing with vulnerability / threat

A CRA is an artifact that lets senior management and business owners make more informed decisions about operational aspects of their business, such as financial, personnel or IT controls. Utilizing the CRA in development of those controls allows for more efficient and effective use of limited overhead dollars.

Decisions for implementing additional protection features are normally based on the existence of a reasonable ratio between cost/benefit of the safeguard and sensitivity/value of the assets to be protected.

Risk assessments may vary from an informal review of a small scale microcomputer installation to a more formal and fully documented analysis (i. e., risk analysis) of a large scale computer installation. Risk assessment methodologies may vary from qualitative or quantitative approaches to any combination of these two approaches.

Rating Criteria

Risk Likelihood

Risk Likelihood Descriptor	Risk Likelihood Categorization Criteria
High	A "high likelihood" of risk indicates a risk/posture scenario where there are not strong controls in place to prevent, limit or mitigate an attack.
Medium	A "medium likelihood" of risk indicates a risk/posture scenario where there is at least one strong control in place to prevent, limit or mitigate an attack.
Low	A "low likelihood" of risk indicates a risk/posture scenario where there are several strong controls in place to prevent, limit or mitigate an attack.

Risk Impact

Risk Impact Descriptor	Risk Impact Categorization Criteria
High	A "high impact" indicates a scenario where the damages from a realized risk would cause complete stoppage of business activities for more than 5 business days. Significant financial or asset losses would accompany this impact category.
Medium	A "medium impact" indicates a scenario where damages from a realized risk would cause significant interruption of business activities for more than 1 business day. Moderate financial or asset losses would accompany this impact category.
Low	A "low impact" indicates a scenario where damages from a realized risk would cause minimal interruption of business activities for less than 1 business day. Minimal financial or asset loss would accompany this impact category.

Risk Mitigation

Risk Mitigation Descriptor	Risk Mitigation Description
AVOID	Implement IT controls and training to avoid the risk by preventing the threat vector from being applicable to your business. An example of this mitigation could be: avoiding a phishing attack by training staff to understand social engineering and to avoid giving out login credentials, avoiding a software vulnerability by not using that software package, etc..
CONTROL	Implement IT controls and training to control the risk by limiting, compartmentalizing and minimizing the damage. An example of this mitigation could be: strong username/password combinations, strong firewall rulesets, strong physical security controls (locks, badges, etc.).
ACCEPT	Accept the risk as "the cost of doing business", when the likelihood is very low or the impact is very low. This is typically a last resort option after Avoid, Control or Transfer.
TRANSFER	Transference of risk to another business entity, typically an insurer or underwriter. This is accomplished through contractual means and an existing financial relationship. Examples of this would be business liability insurance, disaster insurance, listed property insurance, business umbrella insurance, etc..

Risk Assessment Matrix

Risk	*Risk Likelihood* (High/Med/Low)	*Risk Impact* (High / Med / Low)	*Risk Mitigation* (ACAT)	*Risk Mitigation Details* (Information about Risk Mitigation Strategy and Execution)
Technological				
Vulnerabilities	**H**	**M**	**AVOID, CONTROL**	Avoid through use of IT Security Awareness training and strong vulnerability management program, control through technological controls such as strong passwords, separated account roles, and industry best-practices.
Login / Account Compromise	**H**	**M**	**AVOID, CONTROL**	Avoid through use of IT Security Awareness training and strong vulnerability management program, control through technological controls such as strong passwords, separated account roles, and industry best-practices.
Advanced Persistent Threat	**M**	**M**	**CONTROL**	Control through technological controls such as strong passwords, separated account roles, and industry best-practices including malware scanning, anti-virus technologies.
Environmental				
Building Fire	**L**	**M**	**TRANSFER**	Transfer of liability and costs contractual arrangements such as property insurance, business umbrella insurance, or similar mechanisms.
Building Flood	**L**	**M**	**TRANSFER**	Transfer of liability and costs contractual arrangements such as property insurance, business umbrella insurance, or similar mechanisms.
Foreclosure	**L**	**L**	**AVOID, ACCEPT**	Avoid through the use of contractual vehicles and the ability to work from home, if needed. Accept as very low-likelihood.
Catastrophic Destruction	**L**	**M**	**TRANSFER**	Transfer of liability and costs contractual arrangements such as property insurance, business umbrella insurance, or similar mechanisms.
Biological Threat	**L**	**M**	**TRANSFER**	Transfer of liability and costs contractual arrangements such as property insurance, business umbrella insurance, or similar mechanisms.

Risk	**Risk Likelihood** (High/Med/Low)	**Risk Impact** (High / Med / Low)	**Risk Mitigation** (ACAT)	**Risk Mitigation Details** (Information about Risk Mitigation Strategy and Execution)
Environmental *(continued)*				
Radiological Threat	**L**	**M**	**ACCEPT**	Acceptance of risk given the cost of risk transference and low likelihood of occurrence.
Acts of War	**L**	**M**	**ACCEPT**	Acceptance of risk given the cost of risk transference and low likelihood of occurrence.
Personnel				
Worker Strike	**M**	**H**	**AVOID, CONTROL**	Avoid risk through use of labor relations and regulatory mechanisms, control risk through strong physical security controls and human resource policies.
Disgruntled Worker	**M**	**M**	**AVOID, CONTROL**	Avoid risk through use of labor relations and regulatory mechanisms, control risk through strong physical security controls and human resource policies.
Corporate Espionage	**M**	**M**	**AVOID, CONTROL**	Avoid risk through use of labor relations and regulatory mechanisms, control risk through strong physical security controls and human resource policies.

Acronyms and Abbreviations

Abbreviation or Acronym	Meaning
ACAT	**A**void, **C**ontrol, **A**ccept, **T**ransfer: an acronym describing risk management strategies.
CRA	Comprehensive Risk Analysis

Signatory Page

I/we, the undersigned, accept this document, titled "Risk Management Plan" into our corporate IT policies and procedures, this day, the ____ of _____, _____.

We agree to faithfully execute this Risk Management Plan to the best of our abilities according to the procedural and notional guidance contained herein. We indicate and affirm that this document shall be the controlling document with respect to risk assessment and management within our organization.

We agree to provide funding for both the initial acquisitions listed, as well as maintenance funding to keep those tools up to date and properly licensed.

_____	_____
Signature Date	Signature Date
_____	_____
Printed Name Title / Position	Printed Name Title/Position
_____	_____
Signature Date	Signature Date
_____	_____
Printed Name Title / Position	Printed Name Title/Position