MEDICAL
MEDICAL
MEDICAL
MEDICAL
MEDICAL
MEDICAL
MEDICAL

RISK MATRIX EXAMPLE - HEALTHCARE

KW
Chris Miele

MB
JP

TABLE OF CONTENTS

INTRODUCTION & PURPOSE

The healthcare industry faces constant threats and risks on a daily basis. The massive quantity and quality of sensitive information this industry holds creates an admirable target for attackers looking to gain information. Not only is the personal information attractive, but the healthcare industry commonly uses outdated software and hardware. This is done for convenience but creates vulnerabilities that attackers know they can exploit. The industry is also not too well educated in cyber risks because the majority of staff do not have to work in a virtual environment. This lack of awareness means that the employees do not know how to safely manage and access any online devices they may have to use.

Due to these inherit vulnerabilities, it is important that each business/organization in the healthcare industry be aware of the threats they face and be able to constantly assess the risk level of each threat they come across. The purpose of this report is to act as an example of some common threats the healthcare industry faces. It also gives a guide on how the risk level can be calculated. This method can be adapted to any environment in the industry and aspects should be changed as needed to better fit each specific organization.

CALCULATING RISK

INTRODUCTION

Risk is calculated by the equation LIKELIHOOD x VULNERABILITY x IMPACT = RISK. For the purpose of this report, because this is an example that should be molded to each individual organization, vulnerability will be excluded from the calculation. Vulnerability is subjective to the specific location, environment, staffing, opposition, and practices that each organization has and should be included when applying this method practically. Since vulnerability is so specific and it can not be applied in a general sense, the risk calculation for this report will be LIKELIHOOD x IMPACT = RISK.

LIKELIHOOD

The first portion of the risk calculation is likelihood. This is the chance that the threat will materialize and become a reality. It is a vital portion of the equation because if the threat has no chance of actually happening, there is no point in using resources trying to mitigate or control it. Some things to take into consideration when assessing likelihood is the organization's history - if it has happened before it could happen again. The culture of the organization is important to note. If there is a weak focus on security, the threat could be more likely to materialize. These are just a few of the many avenues that should be considered when determining the likelihood of a specific threat occurring.

This matrix should be adapted and changed to suit each different organization.
For the purposes of this report, the matrix for calculating likelihood will be as follows:

Likelihood	
MINIMAL	The chance of the threat materializing is minimal and would likely never happen.
LOW	The chance of the threat materializing is low and would only happen under a few certain circumstances.

MEDIUM	The chance of the threat materializing is likely and would happen in some circumstances.
HIGH	It is almost certain that the threat will materialize and would happen under any circumstance.

IMPACT

Impact measures the amount of damage that the organization would face assuming the threat materializes. The damage can be financial, reputational, operational, or physical and can include a number of things such as loss of life, equipment damage and repairs, operational downtime, and negative media attention. Impact is important to measure when calculating risk because if the outcome of the threat does minimal damage, it should not be ranked as high and can be acted on later than threats that would pose more damage to the organization. Time and resources are better spent focused on threats that would harm the organization more so that they can be prevented.

This matrix should be adapted and changed to suit each different organization.
For the purposes of this report, the matrix for calculating impact will be as follows:

Impact	
INFO	If the threat materialized it would only release general information about the organization. Daily operations would not be interrupted.
LOW	If the threat materialized it would cause a small amount of financial damage. A small amount of reputational loss would occur. Little downtime would occur as a result.
MEDIUM	If the threat materialized it would cause a moderate amount of financial damage. A moderate amount of reputational damage and operational downtime would occur.
HIGH	If the threat materialized it would cause a severe amount of financial damage. Severe reputational damage and a lengthy amount of operational downtime would occur.

RISK

The final risk calculation is done by taking both the likelihood score and impact score and comparing them. This method allows us to be able to consider multiple aspects of the threat instead of looking at it from a surface level. This allows us to get a better understanding of each threat, thus also allowing us to better consider appropriate countermeasures and mitigation strategies.

The final matrix for calculating risk is as follows:

Calculating Risk		Impact			
		INFO	LOW	MEDIUM	HIGH
Likelihood	MINIMAL	▨	▨	🟨	🟧
	LOW	▨	🟨	🟨	🟧
	MEDIUM	🟨	🟨	🟧	🟥
	HIGH	🟨	🟧	🟥	🟥

Risk levels explained:

Risk Level	
MINIMAL	The risk the organization faces is minimal and steps to remediate it should be taken if all higher-level risks are already taken care of.
LOW	The risk the organization faces is low and steps to remediate it should be considered and scheduled within the year.
MEDIUM	The risk the organization faces is moderate and steps to remediate it should be taken within 3 months.
HIGH	The risk the organization faces is critical and steps to remediate it should be taken immediately.

Risk can be difficult to calculate if the organization attempting to do it does not have a predetermined method with specific laid-out guidelines. This method gives criteria that can be adapted as the organization grows and shrinks to keep the final risk level calculation accurate.

IMPLEMENTATION

INTRODUCTION

The remaining portion of this report will give an example of implementing this risk calculation matrix in a healthcare industry setting. Four threat categories will be assessed:

- Physical – Threats that have an impact on the tangible environment of the organization, including the building and non-technological equipment
- Virtual – Threats that have an impact on the digitally implemented software
- Hardware – Threats that have an impact on the hardware associated with the information technology landscape
- Operational – Threats that have an impact on the organization’s operational abilities

These 4 categories will be broken into 4 subcategories, with 10 specific threats associated with each that will be given a calculated risk level using the aforementioned matrix. This will provide an example of the methodology that should be used to obtain a well-rounded understanding of an organization’s risk landscape.

1.0.0 PHYSICAL THREATS

1.1.0 HUMAN

1.1.1 Security Staff Unavailability

LIKELIHOOD = HIGH	IMPACT = MEDIUM
RISK = HIGH	

1.1.2 Vandalism - Building Interior

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

1.1.3 Vandalism - Building Exterior

LIKELIHOOD = HIGH	IMPACT = LOW
RISK = MEDIUM	

1.1.4 Bomb Threat

LIKELIHOOD =MINIMAL	IMPACT = HIGH
RISK = MEDIUM	

1.1.5 Terrorist Attack

LIKELIHOOD = MINIMAL	IMPACT = HIGH
RISK = MEDIUM	

1.1.6 Hostile Client

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

1.1.7 Equipment Stolen - Internal

LIKELIHOOD = MEDIUM	IMPACT = LOW
RISK = LOW	

1.1.8 External Access to Restricted Area

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

1.1.9 Disgruntled Employee

LIKELIHOOD = LOW	IMPACT = LOW
RISK = LOW	

1.1.10 Physical Client Data Stolen - External

LIKELIHOOD = LOW	IMPACT = INFO
RISK = INFO	

1.2.0 HEALTH & SAFETY

1.2.1 Improper Biohazard Disposal

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

1.2.2 Equipment Misuse

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

1.2.3 Chemical Misuse

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

1.2.4 Ladder Misuse

LIKELIHOOD =HIGH	IMPACT = INFO
RISK = LOW	

1.2.5 Employee Slip and Fall

LIKELIHOOD = MEDMIUM	IMPACT = LOW
RISK = LOW	

1.2.6 Improper Chemical Storage

LIKELIHOOD = MEDIUM	IMPACT = LOW
RISK = LOW	

1.2.7 Sick Employee on Shift

LIKELIHOOD = LOW	IMPACT = LOW
RISK = LOW	

1.2.8 Outdated Health and Safety Training

LIKELIHOOD = MEDIUM	IMPACT = INFO
RISK = LOW	

1.2.9 Employees Misusing PPE

LIKELIHOOD = MEDIUM	IMPACT = INFO
RISK = LOW	

1.2.10 Unavailability of PPE

LIKELIHOOD = LOW	IMPACT = INFO
RISK = INFO	

1.3.0 HUMAN-CAUSED INFRASTRUCTURE

1.3.1 Medical Equipment Malfunction

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

1.3.2 Power Outage - Full

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

1.3.3 Building Maintenance

LIKELIHOOD = HIGH	IMPACT = LOW
RISK = MEDIUM	

1.3.4 Partial Building Collapse

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

1.3.5 Security System Failure

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

1.3.6 Locking Mechanism Failure

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

1.3.7 Full Building Collapse

LIKELIHOOD = MINIMAL	IMPACT = HIGH
RISK = MEDIUM	

1.3.8 Plumbing System Malfunction

LIKELIHOOD = MEDIUM	IMPACT = LOW
RISK = LOW	

1.3.9 HVAC System Malfunction

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

1.3.10 Burst Water Pipe

LIKELIHOOD = MINIMAL	IMPACT = MEDIUM
RISK = LOW	

1.4.0 ENVIRONMENT

1.4.1 Fire

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

1.4.2 Tornado

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

1.4.3 Hurricane

LIKELIHOOD = MINIMAL	IMPACT = HIGH
RISK = MEDIUM	

1.4.4 Earthquake

LIKELIHOOD = MINIMAL	IMPACT = HIGH
RISK = MEDIUM	

1.4.5 Snowstorm

LIKELIHOOD = MEDIUM	IMPACT = LOW
RISK = LOW	

1.4.6 Ice Storm

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

1.4.7 Rainstorm

LIKELIHOOD = MEDIUM	IMPACT = INFO
RISK = LOW	

1.4.8 Climate Change

LIKELIHOOD = MINIMAL	IMPACT = LOW
RISK = INFO	

1.4.9 Air Pollution

LIKELIHOOD = MINIMAL	IMPACT = LOW
RISK = INFO	

1.4.10 Draught

LIKELIHOOD = MINIMAL	IMPACT = LOW
RISK = INFO	

HARDWARE THREATS

2.1.0 INFRASTRUCTURE-CAUSED

2.1.1 Power Failure

LIKELIHOOD = MEDIUM	IMPACT= HIGH
RISK = HIGH	

2.1.2 Fire

LIKELIHOOD =MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.1.3 Structural Failure

LIKELIHOOD = MINIMAL	IMPACT = HIGH
RISK = MEDIUM	

2.1.4 Environmental Disaster

LIKELIHOOD = MINIMAL	IMPACT= HIGH
RISK = MEDIUM	

2.1.5 Pipes Burst/Flood

LIKELIHOOD = MINIMAL	IMPACT = HIGH
RISK = MEDIUM	

2.1.6 Heating/Cooling System Malfunction

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

2.1.7 Cable Failure

LIKELIHOOD = MINIMAL	IMPACT = MEDIUM
RISK = LOW	

2.1.8 UPS Failure

LIKELIHOOD = MINIMAL	IMPACT = MEDIUM
RISK = LOW	

2.1.9 Electrical Short

LIKELIHOOD = MINIMAL	IMPACT= LOW
RISK = INFO	

2.1.10 Electrical Socket Failure

LIKELIHOOD = MINIMAL	IMPACT= LOW
RISK = INFO	

2.2.0 HUMAN INTERFERENCE

2.2.1 External Theft of Hardware

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.2.2 Vandalism of Hardware

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.2.3 Internal Theft of Hardware

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.2.4 Accidental Damage

LIKELIHOOD = HIGH	IMPACT = MEDIUM
RISK = HIGH	

2.2.5 Lost or Misplaced

LIKELIHOOD = HIGH	IMPACT = MEDIUM
RISK = HIGH	

2.2.6 Water Damage

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.2.7 Intentional Damage

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

2.2.8 Improper Use

LIKELIHOOD = HIGH	IMPACT= LOW
RISK = MEDIUM	

2.2.9 Chemical Contamination

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

2.2.10 Bodily Fluids Contamination

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

2.3.0 I.T. ENVIRONMENT

2.3.1 Bugs

LIKELIHOOD = HIGH	IMPACT = MEDIUM
RISK = HIGH	

2.3.2 Component Failure

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.3.3 Hardware Failure

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.3.4 Bug in New Drivers

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

2.3.5 Hardware Overheating

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

2.3.6 Outdated Drivers

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

2.3.7 User Error

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

2.3.8 Worn Out

LIKELIHOOD = MEDIUM	IMPACT= LOW
RISK = LOW	

2.3.9 Outdated Hardware

LIKELIHOOD = MEDIUM	IMPACT= LOW
RISK = LOW	

2.3.10 Hardware Bottleneck

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

2.4.0 SECURITY FAULTS

2.4.1 Ransomware

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = HIGH	

2.4.2 Users with Default Passwords

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.4.3 Virus

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

2.4.4 Keylogger

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

2.4.5 Outside Remote Desktop Access

LIKELIHOOD = LOW	IMPACT = HIGH
RISK =MEDIUM	

2.4.6 Trojan

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

2.4.7 Network Loop

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

2.4.8 Malware

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

2.4.9 Worm

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

2.4.10 Crypto Mining

LIKELIHOOD = LOW	IMPACT=MEDIUM
RISK = LOW	

SOFTWARE THREATS

3.1.0 CODE DESIGN

3.1.1 Sloppy Code

LIKELIHOOD = HIGH	IMPACT = HIGH
RISK = HIGH	

3.1.2 Known Exploit

LIKELIHOOD = HIGH	IMPACT = HIGH
RISK = HIGH	

3.1.3 Poor Communication (Client, Stakeholders, etc)

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.1.4 Low Budget

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.1.5 Lack of Software Functionality

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.1.6 Lack of Secure Code in Software

LIKELIHOOD = LOW	IMPACT = HIGH

RISK = MEDIUM

3.1.7 Poor Documentation

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = MEDIUM	

3.1.8 Inadequate Testing During Coding Design

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.1.9 Lack of Qualified Staff

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.1.10 Time Crunch

LIKELIHOOD = LOW	IMPACT = INFO
RISK = INFO	

3.2.0 HUMAN

3.2.1 Malicious End-User

LIKELIHOOD = HIGH	IMPACT = HIGH
RISK = HIGH	

3.2.2 Poor Working Environment

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.2.3 Lack of Compliancy Knowledge

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.2.4 No Background Checks on Employees Working on Sensitive Information

LIKELIHOOD = MINIMAL	IMPACT = HIGH
RISK = MEDIUM	

3.2.5 Poor Coding Knowledge

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.2.6 Poor Time Management

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = MEDIUM	

3.2.7 Employees Disregarding NDA

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.2.8 No Qualification (Education)

LIKELIHOOD = LOW	IMPACT = LOW
RISK = LOW	

3.2.9 Employee Lacks Problem Solving Skills

LIKELIHOOD = LOW	IMPACT = LOW
RISK = LOW	

3.2.10 No Documentation for Software

LIKELIHOOD = LOW	IMPACT = LOW
RISK = LOW	

3.3.0 TECHNOLOGY

3.3.1 Software Lacks Compatibility with New Operating Systems (Linux, Apple, etc.)

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.3.2 Software Is Not Compatible with Certain Device Drivers (Linux, Apple, Microsoft)

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.3.3 Software Runs on Outdated Physical Hardware

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.3.4 Poor Software Development works off different APIS That You Cannot Control

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.3.5 Software Lacks Compatibility with Legacy OS

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.3.6 Software Lacks Compatibility with Legacy Drivers

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.3.7 Software Lacks Compatibility with Certain Programming Languages

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.3.8 Software Is Not Compatible with certain WIFI

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.3.9 Software Lacks Frequent Updates

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.3.10 Software Lacks Compatibility With TCP/IP Networks (Linux, Apple, Microsoft)

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.4.0 SECURITY IMPLEMENTATION

3.4.1 Software Prone to Malware Attacks

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.4.2 Software Lacks Frequent Pen Tests

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

3.4.3 Poor Authentication Mechanism for Software

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.4.4 Passwords Stored in Plain Text

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.4.5 Passwords Use Legacy Hashes

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.4.6 Poor Implementation of End-To-End Channel Encryption

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.4.7 Software Data Stored in Unsecure Database

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.4.8 Poor Implementation of Principle of Least Privilege

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

3.4.9 Software Lacks Defense in Depth Approach

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = MEDIUM	

3.4.10 Software Lacks Threat Modeling Implementation

LIKELIHOOD = LOW	IMPACT = LOW
RISK = LOW	

OPERATIONAL THREATS

4.1.0 BUSINESS DISRUPTION/SYSTEMS FAILURES

4.1.1 Process Failure, Gap in Flow

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.1.2 Loss of Vendors/Suppliers

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.1.3 Cyber Fraud

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.1.4 Cyber Attacks

LIKELIHOOD = MEDIUM	IMPACT = HIGH

RISK = HIGH

4.1.5 Environmental (Catastrophic Events)

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.1.6 Poor Outsourcing Reliability

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

4.1.7 New/Growing Competition

LIKELIHOOD = MEDIUM	IMPACT = MEDIUM
RISK = MEDIUM	

4.1.8 New Distribution Methods

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = MEDIUM	

4.1.9 Insufficient Resources (Processes, Staff)

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

4.1.10 Changes in Customer Behaviour

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

4.2.0 HUMAN

4.2.1 Human Error

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.2.2 Excessive Employee Privileges

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.2.3 Inadequate Training

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.2.4 Unauthorized Activities

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.2.5 Misuse of Data

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.2.6 Intentional Fraud

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.2.7 Unintentional Fraud

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.2.8 Disgruntled Employees

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.2.9 Loss of Key People / Talent Retention

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.2.10 Organizational Changes

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

4.3.0 SYSTEMS

4.3.1 Lack of Quality Assurance in Applications

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.3.2 Poor IT Implementation

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.3.3 Failure of IT Systems

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.3.4 Development Failures

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.3.5 Insufficient Testing

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.3.6 Poorly Defined Security Controls

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.3.7 Infrequent Security Patching

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.3.8 Insufficient Client Support

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.3.9 Insufficient Technology Budget

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

4.3.10 Inadequate Resources

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	

4.4.0 BUSINESS PRACTICES

4.4.1 Failure to Adhere to Internal Policies

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.4.2 Poor Recovery Operations

LIKELIHOOD = MEDIUM	IMPACT = HIGH
RISK = HIGH	

4.4.3 Inadequate Systems Maintenance

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.4.4 Poor Environmental Security

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.4.5 Poor System Safeguards

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.4.6 Poor Data Media Access and Disposal

LIKELIHOOD = LOW	IMPACT = HIGH

RISK = MEDIUM

4.4.7 Poor Security Incident Reporting Procedures

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.4.8 Infrequent System Auditing

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.4.9 Faulty Labeling and Distribution of External Data

LIKELIHOOD = LOW	IMPACT = HIGH
RISK = MEDIUM	

4.4.10 Poorly Defined Internal Frameworks

LIKELIHOOD = LOW	IMPACT = MEDIUM
RISK = LOW	