SWE 267P - Cloud and Security Foundations

PharmaX Security Risk Assessment Report

Instructor: Ian G. Harris

Cheng-Yi Tang
Master of Software Engineering
University of California, Irvine
chengyit@uci.edu

I. INTRODUCTION

The objective of this security risk assessment was to evaluate and identify the top 10 security risks of PharmaX, a pharmaceutical company that develops and sells both pharmaceutical products and enterprise software solutions. The assessment is critically needed for the several reasons:

• Current Security Posture - PharmaX has never performed a security risk assessment before, and the company's security maturity level is notably low. With weak security awareness among management and employees, there is an urgent need to establish a baseline understanding of the organization's security risks.

• Complex Operating Environment - The company operates across multiple physical locations with 50% of workforce being remote and employ 12.5% external consultants, processes sensitive medical research data, and relies heavily on third-party service providers for critical functions including cloud connectivity (CloudX), data center management (HostingX), firewall monitoring (SecX), and automated CI/CD solution (CodeX). This complex ecosystem increases the potential attack surface and risk exposure.

• Regulatory Compliance - As a pharmaceutical company handling sensitive medical research data and customer information, PharmaX must ensure compliance with relevant regulatory requirements and protect its intellectual property. A comprehensive risk assessment is essential to identify potential compliance gaps and security vulnerabilities.

This assessment follows the NIST Guide for Conducting Risk Assessments [1] methodology and considers *threats*, *vulnerabilities*, *likelihood*, and *impact* in determining the risk levels. By conducting this systematic evaluation of security risks, PharmaX will be able to identify and address potential threats before they can be exploited by malicious actors. This proactive approach is especially crucial given the sensitive nature of pharmaceutical research data and the increasing sophistication of cyber threats targeting the healthcare and pharmaceutical sectors. Early identification and remediation of vulnerabilities will help protect PharmaX's intellectual property, customer data, and business operations from unauthorized access and potential breaches.

[1] NIST Guide for Conducting Risk Assessments, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

II. ASSUMPTIONS

Based on the provided information about PharmaX's current state, following assumptions were made:

Organizational Structure and Governance

The company operates with minimal security oversight from the board level, and there is no dedicated security governance structure. Dealing with cyber risk has been dumped on the security and IT teams which operate largely independently from business management.

Technical Environment

• Cloud Connect provides the primary network infrastructure and is assumed to be configured according to industry standards

• The primary and secondary data centers operated by HostingX maintain standard physical security controls

• All remote access occurs via CloudX-managed VPN solutions

• Third-party development work by CodeX has privileged access to internal systems through the CI/CD pipeline

• Personal devices used by executives and consultants are not under central management control

Data Management

• Critical business data is distributed across cloud, on-premises servers, and personal devices

• Physical documents containing sensitive information exist but are not tracked systematically

• There is no formal data classification system in place

Security Controls

• Basic technical controls (firewalls, antivirus) are present but may not be optimally configured

• No formal security policies or procedures are consistently enforced

• Security monitoring is limited to firewall traffic analysis by SecX

• HostingX physical access controls are not regularly audited

• Employee security awareness training is minimal or non-existent

Threat Landscape

• The company is a potential target for intellectual property theft due to its pharmaceutical research

• Internal threats are elevated due to the high number of third-party consultants

• Remote work increases the attack surface and potential for security incidents

III. FINDINGS AND RECOMMENDATIONS

Based on the company description and assumption, technical infrastructure, and NIST's assessment guide framework, here are the top 10 critical risk events for PharmaX (ordered by risk from high to low):

1. **Deliver targeted malware for control of internal systems and exfiltration of data**

Threat Sources

Adversarial: Competitor, Nation-State, Insider, Privileged Insider

Vulnerability

Vulnerability Severity: High

- Information-related: Handles proprietary research data
- Technical: Weak CI/CD controls with Vietnam developer
- Operational: Large remote workforce population

Likelihood

Overall Likelihood: Very High

Assumptions:

- Valuable pharmaceutical IP makes company an attractive target
- Third-party developer in Vietnam has privileged access
- No security monitoring in place

Impact

Impact Type: Harm to Assets (Loss of intellectual property)

Scale: Very High

Rationale: Could lead to theft of critical pharmaceutical research IP

Risk

Very High

Recommendation

- Implement Endpoints Detection and Responses (EDR)
- Deploy Data Loss Prevention (DLP) controls
- Regular vulnerability scanning and patch management

2. **Exploit vulnerabilities using zero-day attacks**

Threat Sources

Adversarial: Nation-State, Competitor, Established Group

Vulnerability

Vulnerability Severity: Very High

• Information-related: Outdated technical documentation

• Technical: No formal security procedures or patches

• Operational: No security monitoring

Likelihood

Overall Likelihood: High

Assumptions:

• High-value pharmaceutical target

• Outdated systems and documentation

• No patch management process

Impact

Impact Type: Harm to Operations & Assets

Scale: High

Rationale: Could cause major service disruption and data compromise

Risk

High

Recommendation

• Implement robust patch management process

• Enable system hardening and security baselines

• Deploy intrusion detection/prevention systems

• Subscribe to threat intelligence feeds

3. **Craft spear phishing attacks**

Threat Sources

Adversarial: Competitor, Nation-State, Ad hoc Group, Established Group

Vulnerability

Vulnerability Severity: High

• Information-related: Handles sensitive data

• Technical: No user training or email filtering

• Operational: 50% remote workforce

Likelihood

Overall Likelihood: Very High

Assumptions:

• 50% remote workforce

• Low security awareness stated in documentation

• No email filtering mentioned

Impact

Impact Type: Harm to Operations & Assets

Scale: High

Rationale: Could lead to credential theft and system compromise

Risk

Very High

Recommendation

• Implement comprehensive security awareness program

• Deploy advanced email filtering solution

• Enforce multi-factor authentication

• Regular phishing simulations and training

4. **Insert subverted individuals into privileged positions**

Threat Sources

Adversarial: Competitor, Nation-State, Partner, Supplier

Vulnerability

Vulnerability Severity: High

• Information-related: Access to proprietary information

• Operational: Large contractor population with minimal vetting, No clearance/vetting procedures

Likelihood

Overall Likelihood: High

Assumptions:

• 20 external consultants

• No formal screening procedures

- Access to sensitive data

Impact

Impact Type: Multiple (Operations, Assets, Organization)

Scale: Very High

Rationale: Privileged access could affect all aspects of operations

Risk

High

Recommendation

- Enhance background screening process
- Implement privileged access management
- Regular access reviews
- Monitor privileged user activities

5. **Exploit multi-tenancy in cloud environment**

Threat Sources

Adversarial: Competitor, Nation-State, Privileged Insider

Accidental: Privileged User/Administrator

Vulnerability

Vulnerability Severity: High

- Information-related: Sensitive data in cloud
- Technical: Reliance on shared cloud infrastructure (Cloud Connect by CloudX)
- Operational: No cloud security controls documented

Likelihood

Overall Likelihood: High

Assumptions:

- Complete reliance on CloudX infrastructure
- No visibility into cloud security controls
- Shared environment

Impact

Impact Type: Harm to Assets & Operations

Scale: High

Rationale: Could affect all cloud-hosted services and data

Risk

High

Recommendation

- Cloud security assessment and compliance review
- Implement cloud security posture management
- Regular security audits of CloudX services
- Enhanced monitoring of cloud environment

6. **Exploit split tunneling**

Threat Sources

Adversarial: Insider, Privileged Insider, Competitor, Nation-State

Accidental: User

Vulnerability

Vulnerability Severity: High

- Information-related: Sensitive data in cloud
- Technical: Unmanaged personal devices, No security controls on endpoints
- Operational: Mobile/Remote workforce

Likelihood

Overall Likelihood: High

Assumptions:

- Remote workers using personal devices
- VPN managed by third party
- No endpoint controls

Impact

Impact Type: Harm to Assets

Scale: Moderate

Rationale: Could lead to data exposure but limited to specific endpoints

Risk

Moderate

Recommendation

- Enforce VPN security policies
- Implement endpoint security controls
- Network segmentation
- Regular VPN security audits

7. **Conduct supply chain attacks targeting critical hardware/software**

Threat Sources

Adversarial: Supplier, Partner, Nation-State

Vulnerability

Vulnerability Severity - Very High

- Information-related: Critical service providers
- Technical: Multiple third-party dependencies (CloudX/HostingX/CodeX/SecX)
- No vendor security assessments

Likelihood

Overall Likelihood: High

Assumptions:

- Multiple critical third-party vendors
- No vendor security assessments
- Automated CI/CD pipeline from external provider

Impact

Impact Type: Harm to Operations & Assets

Scale: Very High

Rationale: Could affect entire infrastructure through third-party services

Risk

Very High

Recommendation

- Implement vendor risk management program
- Security requirements in contracts
- Regular third-party security assessments
- Monitor third-party access

8. **Exploit vulnerabilities in mobile systems**

Threat Sources

Adversarial: Nation-State, Competitor, Established Group

Accidental: User

Vulnerability

Vulnerability Severity: High

• Information-related: Handles sensitive data

• Technical: No MDM solution, No BYOD policies

• Operational: Mobile devices with sensitive data

Likelihood

Overall Likelihood: Very High

Assumptions:

• Executives using personal devices

• No MDM solution

• No BYOD policies

Impact

Impact Type: Harm to Assets

Scale: High

Rationale: Could expose sensitive data on executive devices

Risk

High

Recommendation

• Deploy Mobile Device Management (MDM)

• Implement BYOD security policies

• Regular mobile security assessments

• Secure container solutions

9. **Conduct insider-based social engineering**

Threat Sources

Adversarial: Insider, Trusted Insider, Privileged Insider

Vulnerability

Vulnerability Severity: High

• Information-related: Access to sensitive data

• Operational: Large contractor base, No security awareness training

Likelihood

Overall Likelihood: High

Assumptions:

• Large contractor workforce

• Weak security awareness

• Handling sensitive data

Impact

Impact Type: Harm to Assets & Operations

Scale: High

Rationale: Could lead to data theft and operational disruption

Risk

High

Recommendation

• Enhanced security awareness training

• Clear security policies and procedures

• Regular security culture assessments

• Incident response plan

10. Exploit poorly configured systems

Threat Sources

Adversarial: Insider, Privileged Insider, Partner

Accidental: Privileged User/Administrator

Structural: Software (Operating System, General-Purpose Application)

Vulnerability

Vulnerability Severity: Very High

• Information-related: Outdated documentation

• Technical: Low security maturity

• Operational: No configuration management

Likelihood

Overall Likelihood: Very High

Assumptions:

- Explicitly stated "low security maturity"
- Outdated documentation
- Previous pentest report ignored

Impact

Impact Type: Multiple (Operations, Assets, Compliance)

Scale: High

Rationale: Could affect multiple systems and lead to compliance issues

Risk

Very High

Recommendation

- Implement configuration management
- Regular security assessments
- Security baseline standards
- Automated compliance checking