Rick Abraham

My Company  Dallas, TX

Risk Assessment – Unsecured Devices Risks

Contents

[Introduction 2](#_Toc182584971)

[Purpose 2](#_Toc182584972)

[Scope 2](#_Toc182584973)

[Risk Identification 2](#_Toc182584974)

[Risk Analysis 3](#_Toc182584975)

[Mitigation Recommendations 3](#_Toc182584976)

[Employee Laptops 3](#_Toc182584977)

[Mobile Devices 3](#_Toc182584978)

[IoT Devices 4](#_Toc182584979)

[Unregistered Devices 4](#_Toc182584980)

[Wearables 4](#_Toc182584981)

[Monitoring and Review 4](#_Toc182584982)

[Frequency 4](#_Toc182584983)

[Daily 4](#_Toc182584984)

[Monthly 4](#_Toc182584985)

[Quarterly 4](#_Toc182584986)

[Bi-Annually 5](#_Toc182584987)

[Annually 5](#_Toc182584988)

[Incident Response 5](#_Toc182584989)

[Documentation and Compliance 5](#_Toc182584990)

Risk Assessment – Unsecured Devices Risks

# Introduction

Purpose: This risk assessment identifies vulnerabilities associated with unsecured devices, including employee-owned devices (BYOD), mobile phones, laptops, and IoT devices. It evaluates potential impacts and provides strategies to mitigate risks posed by unauthorized access, malware, and data breaches.

Scope: Includes all devices connected to the network, whether employee-owned, organization-owned, or IoT-based (e.g., smart devices, industrial sensors).

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Employee Laptops | Malware infection or unauthorized access | Lack of endpoint protection, weak passwords | Data breaches, network-wide infection | High |
| Mobile Devices | Data loss or theft through lost or stolen devices | Lack of device encryption and remote wipe capabilities | Exposure of sensitive organizational data | High |
| IoT Devices | Compromise of IoT devices leading to lateral movement | Default passwords, unpatched firmware | Unauthorized access to internal systems | High |
| Unregistered Devices | Rogue or Unauthorized devices connecting to the network | Lack of network access controls | Data exfiltration, operational disruption | Medium |
| Wearables (e.g., smartwatches) | Unauthorized collection or leakage of sensitive data | Insecure connections or lack of policy enforcement | Privacy violations, compliance breaches | Medium |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Employee Laptops | High | High | Critical |
| Mobile Devices | High | High | Critical |
| IoT Devices | Medium | High | High |
| Unregistered Devices | Medium | Medium | Moderate |
| Wearables | Medium | Medium | Moderate |

# Mitigation Recommendations

## Employee Laptops

* Enforce installation of endpoint protection software (e.g., antivirus, EDR) on all laptops.
* Require strong password policies and enable disk encryption for all devices.
* Monitor laptop activity using Mobile Device Management (MDM) tools to detect anomalies.

## Mobile Devices

* Implement device encryption and enable remote wipe capabilities for all mobile devices accessing organizational data.
* Require multi-factor authentication (MFA) for all mobile app logins to secure data access.
* Prohibit jailbroken or rooted devices from accessing the network.

## IoT Devices

* Change default passwords on all IoT devices and implement firmware update schedules.
* Isolate IoT devices from critical systems using network segmentation.
* Monitor IoT device activity for unusual patterns, such as excessive data transfers or unexpected connections.

## Unregistered Devices

* Deploy Network Access Control (NAC) solutions to block unauthorized devices from connecting to the network.
* Require device registration and approval before granting network access.
* Create guest networks for visitors and limit access to non-sensitive areas.

## Wearables

* Restrict wearable device connectivity to personal-use networks where possible.
* Use encryption for any sensitive data transmitted via wearable devices.
* Enforce policies governing wearable usage, especially in sensitive work areas.

# Monitoring and Review

Frequency

### Daily

* Monitor endpoint protection software logs for threats or blocked malware on laptops and mobile devices.
* Review network logs for connections from unregistered or unauthorized devices.

### Monthly

* Audit MDM and NAC systems to ensure policies are enforced for all connected devices.
* Check for updates to IoT device firmware and schedule patching for identified vulnerabilities.

### Quarterly

* Perform device compliance audits to ensure laptops, mobile devices, and IoT devices meet organizational security standards.
* Test the effectiveness of encryption and remote wipe capabilities on a sample of organizational devices.

### Bi-Annually

* Conduct penetration testing targeting IoT devices and other potentially unsecured endpoints to identify weaknesses.
* Evaluate the effectiveness of NAC and MDM policies through simulated rogue device access attempts.

### Annually

* Reassess unsecured device risks based on changes to device types, organizational policies, or threat landscapes.
* Update device security policies to reflect lessons learned from incidents, audits, and tests.
* Conduct an organization-wide training program focused on securing personal and organizational devices.

Incident Response

* Maintain a dedicated Device Security Response Team (DSRT) to address incidents involving unsecured devices.
* Conduct bi-annual incident response drills, focusing on scenarios such as a compromised IoT device or a lost employee laptop.
* Document all device-related security incidents, including causes, impacts, and lessons learned.

Documentation and Compliance

* Maintain logs of device activity, including connection attempts and threat detection events.
* Document device policies, registration procedures, and compliance requirements for all connected devices.
* Ensure compliance with applicable regulations and standards, including:
  + NIST SP 800-53: AC-19 (Access Control for Mobile Devices), SC-28 (Protection of Information at Rest), and SI-4 (Monitoring).
  + GDPR, ISO 27001, and CCPA for device security and data protection requirements.