Risk Treatment Plan

ISO31000 standard section 6.5.3

Introduction:
The rise of the Internet of Things (IoT) has ushered in an era of unprecedented connectivity, transforming the way we live, work, and interact with technology. From smart homes to industrial automation and healthcare solutions, IoT devices have become an integral part of our daily lives. However, with this increased interconnectivity comes a pressing concern: cybersecurity. As the number of IoT devices continues to surge, ensuring robust IoT cybersecurity has become an absolute necessity to protect sensitive data, critical systems, and individuals' privacy.

Vulnerabilities in IoT Devices:
One of the primary challenges with IoT cybersecurity lies in the inherent vulnerabilities present in many of these devices. Manufacturers often prioritize functionality and cost over security during development, leaving weak spots that hackers can exploit. Without adequate safeguards, these devices become easy targets for unauthorized access and control, endangering the safety and privacy of users.

Impact of IoT Breaches:
The repercussions of IoT breaches can be far-reaching and devastating. In various instances, cyberattacks on IoT devices have led to disruptions in critical infrastructure, financial losses, and breaches of personal information. Notable cases include compromised industrial control systems, healthcare data breaches, and home surveillance camera hacks. Such incidents underscore the urgency of prioritizing IoT cybersecurity.

The Challenge of Scale and Complexity:
Securing a vast network of interconnected IoT devices presents unique challenges. IoT ecosystems involve diverse devices, each with its own set of security requirements. Managing the security of these devices at scale can be daunting, particularly when considering the frequent introduction of new devices into the network.

Data Privacy Concerns:
IoT devices often collect copious amounts of data, ranging from personal information to business-critical data. Inadequate security measures can lead to unauthorized access or tampering with this data, jeopardizing individual privacy and corporate confidentiality.

Emergence of IoT Botnets:
Botnets, networks of compromised devices controlled by cybercriminals, pose a significant threat in the IoT landscape. IoT botnets can be used to launch large-scale cyberattacks, such as Distributed Denial of Service (DDoS) attacks, causing massive disruptions to online services and businesses.

Regulatory Gaps:
The rapid growth of IoT has outpaced the development of comprehensive cybersecurity regulations. The absence of unified standards and regulations exposes IoT devices to potential security loopholes.

Extended Device Lifecycles:
Many IoT devices have long lifecycles, and manufacturers may not consistently provide security updates and patches. This leaves devices vulnerable to new and emerging threats over time.

Risk Treatment Plan

Risk: Increased risk of intrusion through IoT devices.	
Treatment options	1. Device Discovery and Visibility: Get the exact number of IoT devices connected to the organization's network. Discover which types are connected and keep an up-to-date inventory of all connected IoT assets. 2. Patch: Regularly patching and upgrading IoT software using a secure boot to validate firmware. 3. Monitor: Register all IoT devices within an organization to effectively assess the perimeter. Use an IoT-aware Network Detection and Response (NDR) solution and a SIEM solution to auto-discover and monitor devices for anomalous or unauthorized behavior. 4. Reduce Attack Surface Area: Eliminate unnecessary access points (idle internet connections), and use VPN access with MFA authorization when remote access is required. 5. Network Segmentation: This limits the attacker's ability to move laterally within the network after the initial intrusion. Use firewalls to isolate IoT and OT devices from the corporate network or connect IoT devices to segmented networks such as VLANs and DMZs. 6. Secure password practices: maintaining strong password security is critical to securing IoT endpoints.
Rationale for selection of the treatment options, including the expected benefits to be gained	1. Reduce attack surface area to prevent intrusions. 2. Avoid financial losses and reputational damage due to data breaches. 3. Avoid fines imposed by regulatory bodies if sensitive information is compromised.
Who is accountable and responsible for approving and implementing the plan	Leaderships: CISO, CIO Internal stakeholders: SOC team, IT team External stakeholders: vendors (IoT device providers). Vendors are the ones who are responsible to provide us with patches in due time.
Proposed actions	1. Maintain asset inventory list. 2. Discover, eliminate, or replace legacy IoT devices. 3. Conduct monitoring of devices on an ongoing basis. 4. Conduct regular patching. 5. Ensure strong password practices are followed with regular password changes.

	6. Enable MFA to access devices. 7. Ensure IoT devices are connected to isolated segmented networks and use a VPN connection. 8. Ensure the elimination of idle internet connections and open ports. 9. Penetration testing and vulnerability scanning for IoT devices.
Resources required, including contingencies	1. NDR and SIEM solutions for monitoring and detection. 2. MFA solution. 3. VPN solution. 4. VLANs and DMZs. 5. Training and enforcement of personnel to follow secure password practices. 6. Budget to replace legacy IoT devices.
Performance measures	1. Level of preparedness of IoT devices (patches, passwords, VPN, MFA). 2. Unidentified IoT devices on the internal network. 3. Number of intrusion attempts through IoT devices. 4. Number of data breaches through IoT devices. 5. Patching cadence.
Constraints	1. Lack of appropriately skilled labor resources for treatment plan implementation and monitoring. 2. Financial constraints.
Required reporting and monitoring	The SOC team should have real-time monitoring of the IoT devices with NDR and SIEM. Quarterly reporting of performance measures to leadership.
When actions are expected to be undertaken and completed	Immediate: 1. Discover and inventory all IoT devices. 2. Educate staff members on secure password practices and enforce them. 3. Discover, discard, and replace legacy IoT devices. 4. Set secure passwords and MFA. 5. Connect IoT devices to VLAN or DMZ. 6. Scan for open ports and remove idle internet connections. 7. Monitor. Quarterly: 1. Change passwords. 2. Review existing policies and performance measures. Annually: 1. Patching and upgrading software. 2. Asset inventory list.