Ciências ULisboa

Risk Assessment and Incident Response Plan for PowerPlus

An Information Security Analysis

Denis Ungureanu fc56307
Leonardo Monteiro fc58250
Gustavo Henriques fc64361

Prof. Dr. Ana Respício

Risk Analysis and Management in Information Security
MSc in Computer Science and Engineering

November 2024

Contents

Chapter 1

Introduction

1.1 Purpose of the Report

This report aims to conduct a comprehensive risk assessment and develop an initial incident response plan for PowerPlus. The project addresses the organization's need to protect its critical assets, secure its technological infrastructure, and manage cybersecurity risks. The findings will guide the Information Security and IT Risk Management teams in implementing effective controls and preparedness strategies for potential security incidents.

1.2 Background on PowerPlus

PowerPlus is a multinational energy company, focusing on managing critical infrastructure across Europe and the Americas. With 15,000 employees (including 5,000 external contractors), PowerPlus serves 20 million electricity and 1.3 million gas customers. Its strategic goals emphasize sustainability, innovation, expanding into new regions, boosting renewable energy, and advancing digital transformation. Operating within a highly regulated industry, PowerPlus complies with stringent sectoral and data privacy regulations, such as GDPR. The Information Security department, part of Corporate IT, works closely with a Corporate Risk division. Their infrastructure spans both Operational Technology (OT) and Information Technology (IT), necessitating tailored security protocols for each. A key component of PowerPlus's security is its Security Operations Center (SOC), which provides real-time monitoring, incident response, and vulnerability management. The IT environment includes 200 applications, cloud services, extensive data centers for disaster recovery, and a BYOD policy. These measures highlight PowerPlus's commitment to secure operations across a complex technological landscape.

1.2.1 Industry-Specific Security Challenges

Energy companies like PowerPlus face significant security challenges, including advanced persistent threats (APTs) from nation-state actors, ransomware attacks targeting critical systems, and vulnerabilities in their supply chains. Operational Technology (OT) security is especially crucial, as OT systems often lack the robust protections of IT networks. Insider threats also pose risks, alongside the pressures of meeting regulatory compliance requirements, such as GDPR. These factors highlight the need for strong, layered cybersecurity measures to protect against frequent and evolving threats in the industry.

1.3 Objectives of the Risk Assessment and Incident Response Plan

This report outlines the key objectives of PowerPlus's risk assessment and incident response plan, developed to strengthen the organization's cybersecurity posture and ensure resilient business operations.

- **Cybersecurity Risk Identification and Evaluation:** The primary goal is to systematically identify, analyze, and assess cybersecurity risks affecting PowerPlus, focusing on critical infrastructure and identifying potential vulnerabilities within both IT and Operational Technology (OT) systems.
- **Proactive Incident Response Strategy:** PowerPlus aims to establish a proactive approach to cybersecurity incidents. By preparing strategies to respond effectively to potential threats, PowerPlus can minimize damage and facilitate quick recovery in the event of an incident.
- **Compliance with ISO/IEC 27005:2022 Standards:** The risk management framework is aligned with the ISO/IEC 27005:2022 standards, ensuring that PowerPlus follows systematic and industry-recognized practices in identifying and managing security risks.
- **Guidelines for the Security Operations Center (SOC):** Clear guidelines are set for the SOC to enable prompt detection, response, and mitigation of cybersecurity incidents. The SOC's protocols include real-time monitoring, analysis, and structured incident response to reduce the impact of threats.

1.4 Methodology Overview

This report will employ a structured methodology for risk assessment and incident response planning, grounded in industry-standard frameworks. The approach is as follows:

- **Primary Standard – ISO/IEC 27005:2022:** ISO/IEC 27005:2022 will serve as the main standard for guiding the risk assessment process, offering a comprehensive framework for systematically identifying, analyzing, evaluating, and treating cybersecurity risks specific to PowerPlus's infrastructure.
- **Supplementary Standards – ISO/IEC 27001:2022 and ISO 31000:2018:** To enhance the security and risk management framework, references will be made to ISO/IEC 27001:2022 for information security standards and ISO 31000:2018 for general risk management guidance, ensuring a holistic approach to risk and security.
- **Structured Risk Management Process:** The methodology will involve clearly defined phases of risk management: identifying potential risks, analyzing their likelihood and impact, evaluating them in the context of PowerPlus's operations, and developing appropriate treatments to mitigate or manage identified risks effectively.
- **Incident Scenarios and SOC Strategies:** Based on identified threats and vulnerabilities, specific incident scenarios will be developed. These scenarios will inform the preparation and response strategies for the Security Operations Center (SOC), ensuring that PowerPlus is equipped to handle various potential cybersecurity incidents with proactive and targeted responses.

1.5 Structure of the Report

- **Establishing the Context:** Defines the scope of the assessment, identifies PowerPlus's critical assets, outlines the risk environment, and describes the methodology used for evaluating cybersecurity risks.
- **Risk Assessment:** Documents the process and outcomes of identifying and evaluating risks that are specific to PowerPlus, providing insight into the organization's security landscape.
- **Incident Scenarios:** Presents three hypothetical attack scenarios to assess PowerPlus's readiness and resilience, helping to evaluate the effectiveness of current security measures.
- **SOC Preparation:** Details the monitoring requirements for PowerPlus's Security Operations Center (SOC) and provides three specific incident response cases, offering guidelines for effective response and mitigation.
- **Conclusions:** Summarizes the assessment's main findings and offers recommendations to enhance PowerPlus's cybersecurity posture.
- **References:** Lists all standards, frameworks, and resources cited in the report in APA format, ensuring proper attribution and traceability.

Chapter 2

Establishing the Context

2.1 Overview of the Risk Management Context

In establishing an effective risk management framework for PowerPlus, it is essential to align the context of the risk strategy with the overall organizational context, as outlined in ISO 31000. This involves creating clear risk criteria that consider both internal and external factors, types of risks, and appropriate measurement and control processes. The risk management approach should not operate in isolation but as an integral part of PowerPlus's daily operations and strategic goals. The risk context will be defined to include the scope of PowerPlus's business environment, regulatory obligations, and key security challenges, drawing on ISO/IEC 27005:2022 and ISO/IEC 27001:2022 to structure the approach.

2.2 Scope and Boundaries of the Risk Assessment

This risk assessment is constrained by the data available for PowerPlus, focusing primarily on information security and IT risk management. Given PowerPlus's complex infrastructure, the scope of the assessment will cover:

- **Critical assets**, including data, physical assets, and technological infrastructure.
- **Key processes and systems**, particularly those integral to security operations, data integrity, and business continuity.
- **Regulatory and compliance requirements**, especially those relevant to the energy sector and data privacy.

2.2.1 Objectives of the Risk Assessment

The primary objectives of this risk assessment are to:

1. Identify significant risks that could impact PowerPlus's operations, data integrity, and reputation.
2. Propose initial steps to enhance PowerPlus's incident response readiness.
3. Provide a foundation for developing an integrated risk management strategy in alignment with ISO 31000 principles.

2.3 Organizational Context of PowerPlus

PowerPlus is a critical player in the energy sector, with operations spanning across multiple countries and regulatory environments. The company manages a substantial infrastructure, serving millions of electricity and gas customers, and faces stringent requirements for maintaining operational integrity and data protection. The organizational context includes:

- **Business Objectives**: PowerPlus aims to expand geographically, increase its share of renewable energy, drive digital transformation in operations, maintaining risk under control and to create proximity channels with the client in order to antecipate needs and to serve with mpre quality.
- **Stakeholders**: Key stakeholders include executive leadership, IT and SOC teams, regulatory bodies, third-party vendors, and PowerPlus's customer base.
- **Regulatory Compliance**: PowerPlus must adhere to regulations such as GDPR for data privacy and industry-specific requirements from entities like ENISA.

2.4 Risk Environment and Threat Landscape

Given PowerPlus's position in the energy sector, the organization faces an evolving landscape of threats that encompass internal and external risks:

- **Cyber Threats**: Phishing, ransomware, and DDoS attacks are prevalent, with PowerPlus's reliance on OT and IT systems exposing it to IoT vulnerabilities and legacy system risks.
- **Insider Threats and Third-Party Risks**: Involvement of external contractors and vendors introduces data breach and security lapse risks.
- **Physical Security Risks**: Environmental hazards and sabotage pose threats to PowerPlus's data centers and infrastructure.

2.4.1 Stakeholders and Their Roles in Risk Management

Stakeholders play a critical role in PowerPlus's risk management efforts, contributing to security awareness, policy enforcement, and incident response:

- **Executive Leadership**: Responsible for approving and supporting the risk management strategy and allocating resources.
- **IT and SOC Teams**: Tasked with implementing security controls, monitoring incidents, and ensuring compliance.
- **Customers and Regulatory Authorities**: Customers rely on PowerPlus for secure services, while regulatory authorities enforce compliance standards.
- **Third-Party Vendors**: Vendors provide critical support but also increase the company's exposure to external risks.

2.5 Risk Management Framework and Methodology

PowerPlus's risk management framework will be developed in alignment with ISO/IEC 27005:2022 and ISO 31000 standards, ensuring a structured and consistent approach:

- **Risk Assessment**: A comprehensive risk assessment will be conducted, focusing on identifying, analyzing, and evaluating risks specific to PowerPlus.
- **Risk Identification**: Key threats, vulnerabilities, and potential impacts on PowerPlus will be identified.
- **Risk Analysis**: Each identified risk will be assessed in terms of its likelihood and potential impact on the organization.
- **Risk Evaluation**: Risks will be prioritized based on their assessed impact and likelihood, allowing PowerPlus to focus resources on the most significant threats.
- **Risk Treatment**: Initial recommendations for risk treatment will be proposed, aligning with best practices from ISO/IEC 27001:2022 for implementing security controls.

2.6 Justification for the Approach

ISO/IEC and ISO 31000 standards are foundational for this risk assessment as they provide well-established frameworks for identifying, analyzing, and treating risks in critical infrastructure environments. These standards ensure that PowerPlus's approach is comprehensive, systematic, and adaptable to its unique operational and regulatory context. The chosen methodologies are suited to PowerPlus's needs, given the limited data available and the high importance of regulatory compliance in the energy sector. Limitations due to data availability will be addressed by focusing on risk scenarios that are well-supported by the information provided. This approach allows for a realistic yet thorough assessment, enabling PowerPlus to take actionable steps toward effective risk management.

Chapter 3

Risk Assessment

Chapter 4

Incident Scenarios

Chapter 5

SOC Preparation

Chapter 6

Conclusions