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 Organizational considerations

2.1.1 Definition and Structure of the Organization

PowerPlus is defined as a group of entities working collaboratively to achieve its objectives within the energy sector. It includes internal and external teams:

- **Internal Workforce:** 10,000 employees working across corporate IT, operational technology (OT), and various business units.
- **External Workforce:** 5,000 external collaborators, supporting application maintenance, operations, and projects.

PowerPlus operates as a multifaceted organization encompassing IT and OT domains, with a central Corporate IT structure managing information security and risk management, and decentralized OT operations supported by individual subsidiaries.

2.1.2 Risk Appetite and Governance

PowerPlus's risk appetite is influenced by its:

- **Size and Complexity:** Operating in 12 countries, the organization serves 20 million electricity customers and 1.3 million gas customers, necessitating a robust risk framework.
- **Sectoral Dynamics:** Operating under stringent energy regulations in Europe and the Americas.
- **Strategic Goals:** Objectives such as digital transformation, renewable energy expansion, and maintaining controlled risks highlight a balanced approach to risk acceptance and mitigation.

2.1.3 Risk Ownership

PowerPlus ensures that risk ownership is clearly defined within its governance framework:

- **Accountability and Authority:** Risk owners, primarily at the corporate and business unit levels, are entrusted with the authority and responsibility to manage identified risks.

- **Specialized Departments:** The PP Risk Department and the Security Operations Center (SOC) play pivotal roles in overseeing and mitigating risks related to cybersecurity, operational disruptions, and compliance.

2.2 Identifying Basic Requirements of Interested Parties

A) Description of Information Security Controls Adopted by the Organization (PowerPlus) to Ensure Compliance with the ISO/IEC 27001:2022 Standard

PowerPlus adopts a series of information security controls aligned with the requirements of the ISO/IEC 27001:2022 standard, with a focus on protecting the confidentiality, integrity, and availability of information and organizational assets. The main controls are presented below, considering the organizational structure, technological reality, and challenges faced by PowerPlus.

Organizational Controls:

- **Information Security Policies (5.1):** PowerPlus has information security policies communicated and understood by all employees and stakeholders. The policies are aligned with corporate objectives and the ISO/IEC 27001:2022 standard.

- **Identity and Access Management (5.16, 5.18):** The company uses strict processes for access control, including the use of identity and access management tools. This involves managing the user lifecycle and assigning permissions in critical systems.

- **Supplier Management (5.19, 5.20):** PowerPlus ensures that information security is monitored across the entire supplier chain, with specific controls for data protection, especially with suppliers who maintain the applications used by the company.

- **Security Incident Management (5.24 to 5.27):** PowerPlus operates a 24/7 *Security Operations Center (SOC)* that monitors cybersecurity incidents in real-time, performing detection, response, and learning from previous incidents, using tools like *SIEM (Security Information and Event Management)*.

Human Controls:

- **Training and Awareness (6.3):** PowerPlus promotes continuous information security training for all employees, ensuring that everyone is up to date with policies and procedures related to security. The *Information Security and IT Risk Management* department coordinates this training.

- **Disciplinary Process (6.4):** A formal disciplinary process is in place to handle security violations, ensuring that infractions are dealt with in an appropriate and transparent manner.

- **Post-Termination Responsibilities (6.5):** When an employee leaves the organization or changes roles, their security responsibilities are maintained and monitored to avoid risks to the organization.

Physical Controls:

- **Physical Security and Perimeters (7.1, 7.2):** PowerPlus adopts stringent physical security measures to protect sensitive areas from unauthorized access. Physical security is managed by one of the companies within the PowerPlus group and integrates appropriate perimeter control.

- **Protection Against Environmental Threats (7.5):** Critical infrastructure, including data centers and OT (Operational Technology) systems, is designed to withstand environmental threats such as natural disasters and ensure business continuity.

Technological Controls:

- **Protection Against Malware (8.7):** PowerPlus implements robust solutions to protect against malware, complemented by continuous awareness and education programs for employees.

- **Technical Vulnerability Management (8.8):** The *Security Operations Center* continuously assesses vulnerabilities and applies necessary corrections to mitigate risks. Penetration tests and forensic analysis are also periodically conducted.

- **Network and System Security (8.20, 8.21):** PowerPlus rigorously manages and monitors its networks and systems, ensuring that communication and data traffic are secure. *Oracle* and *SAP* technologies are widely used within the organization, with intensive access control and monitoring.

2.3 Applying risk assesment

PowerPlus incorporates risk assessments across various organizational processes to ensure comprehensive risk management. These processes include:

- **Project Management:** Evaluating risks associated with implementing new projects, such as integrating renewable energy solutions or expanding into new geographies.

- **Vulnerability Management:** Regularly assessing technological vulnerabilities, especially within its operational technology (OT) and IT systems, which are managed under distinct domains.

- **Incident Management:** The Security Operations Center (SOC) operates 24/7 to detect, assess, and manage cybersecurity incidents, utilizing SIEM tools to analyze data from over 100 technological components.

- **Problem Management:** Addressing recurring issues, such as vulnerabilities in legacy SAP applications.

- **Impromptu Risk Assessments:** Tackling specific ad-hoc concerns, such as risks associated with BYOD policies or cloud services managing personal data.

2.4 Establishing and maintaining information security risk criteria

2.4.1 General

PowerPlus establishes and maintains information security risk criteria based on the requirements of ISO/IEC 27001:2022 ((section 6.1.2.a)) and ISO/IEC 27005:2022. These criteria are designed to ensure that:

- Risks are assessed consistently, ensuring reliable and comparable results.

- Decisions on risk treatment and acceptance are aligned with strategic objectives and organizational capacity.

The criteria used are as follows:

- Impact on organizational objectives - Here the potential costs of an outage (e.g., lost revenue, regulatory fines) are evaluated in financial terms. The reputational impact if the incident happens is also assessed. In addition, the impact that the risk will have on the continuity of the company's services is analysed and whether we are going against specific rules of the energy sector in this case.

- Likelihood - A historical analysis is made to understand the probability that the risk will have to happen.

- CIA - The potential leakage of sensitive information (confidentiality) is analyzed. In addition to data leakage, it is necessary to understand if the data remains accurate and reliable, so as not to affect integrity. Finally, it is also important to understand the company's availability when suffering a certain attack.

- Response time and recovery - Another important criteria is the time that the sistem that to recover from an incident.

- Combination e Risk Sequence - Analyze how multiple risks can occur simultaneously.

2.4.2 Risk acceptance criteria

2.4.3 Criteria for performing information security risk assessments

Chapter 3

Risk Assessment

3.1 Risk Identification

3.2 Risk Analysis

3.3 Risk Evaluation

Chapter 4

Incident Scenarios

Chapter 5

SOC Preparation

5.1 Incident Response Cases

Chapter 6

Conclusions