**IT 313 Risk Analysis Report**

**IT-313 Risk Management & Mitigation**

**Tatiana Epps**

**October 6, 2024**

**Risk Analysis Report: Workers Werks Credit Union (WWCU) IT Security Risk Management Plan**

**This report evaluates the IT Security Risk Management Plan (v. 1.0, Oct 2015) currently in place at Workers Werks Credit Union (WWCU). The evaluation has revealed significant shortcomings in WWCU’s plan, particularly concerning its scope, risk identification, impact assessment, and mitigation strategies. These weaknesses leave WWCU vulnerable to cyberattacks and data breaches, potentially leading to financial losses, reputational damage, and regulatory non-compliance. This report outlines recommendations to improve WWCU’s Plan and strengthen WWCU's overall cyber resilience.**

**Analysis of WWCU's Current Plan:**

**Scope:**

* The current plan's focus on software and hardware implementation is insufficient. A comprehensive plan should cover the entire IT infrastructure, including hardware, software, networks, data, and people.
* It should consider the impact of cyberattacks on all stakeholders, including customers, employees, and investors.
* The plan should be aligned with organizational business objectives and risk tolerance levels.

**Risk:**

* The current plan lacks a systematic approach to risk identification and assessment.
* It doesn't address industry-specific threats such as phishing attacks targeting financial institutions.
* The plan should consider the increased risk due to the expanding employee base and upcoming infrastructure changes.

**Impact:**

* The current plan doesn't sufficiently assess the potential financial impact of cyberattacks on the credit union.
* It should consider the cost of data breaches, business disruption, and reputational damage.
* The plan should address the importance of business continuity and asset replacement strategies.

**Mitigation:**

* There's a lack of detailed mitigation strategies for identified risks in the current plan.
* The plan should prioritize risks based on likelihood and impact and define specific actions to address them.
* Cost-benefit analysis should be considered when choosing mitigation strategies.

**Legal Compliance and Ethical Considerations**

* While the current plan mentions legal considerations, it doesn't address emerging data privacy regulations such as CCPA and GDPR.
* The plan should align with current ethical codes regarding data protection and responsible data use.

**Recommendations for Improvement:**

* **Develop a more comprehensive risk management framework aligned with industry best practices like NIST CSF (Cybersecurity Framework).**
* **Implement a risk identification methodology that includes regular vulnerability assessments, penetration testing, and industry threat intelligence.**
* **Develop a methodology to estimate the financial impact of security incidents.**
* **Create a data backup and disaster recovery plan to ensure business continuity.**
* **Implement a risk-based approach to prioritize mitigation strategies based on severity.**
* **Address current and emerging legal and regulatory requirements related to data privacy and security.**
* **Highlight the consequences of non-compliance to emphasize the importance of effective risk management.**
* **Incorporate ethical principles of data privacy and responsible data collection into the IT Security Risk Management Plan.**
* **Review and update The IT Security Risk Management Plan regularly to reflect the evolving cyber threat landscape.**

The current plan focuses primarily on security during the software and hardware implementation lifecycle. It needs to be broadened to encompass the entire IT infrastructure, considering all stakeholders and business objectives. In addition, the plan lacks a comprehensive approach to risk identification and prioritization. It doesn't address industry-specific threats or the growing workforce and expanding infrastructure. The plan also doesn't detail specific actions to address identified risks. A robust mitigation strategy with clear priorities and cost-benefit analysis is vital. Finally, the plan focuses on regulations but doesn't address emerging ethical concerns around data privacy. All of these issues need to be addressed in a revised plan.

**The revised plan should address compliance with domestic regulations like Gramm-Leach-Bliley (GLBA) and the California Consumer Privacy Act (CCPA), and international regulations like the General Data Protection Regulation (GDPR) if applicable. In addition, this plan should emphasize the importance of responsible data collection, data minimization, and user privacy. It should also address the ethical implications of potential security breaches and data leaks. By implementing these recommendations, WWCU can significantly strengthen its IT Security Risk Management Plan. A robust plan will better ensure the protection of customer data, reduce the risk of legal and financial repercussions, and ultimately enhance WWCU's cybersecurity posture in the ever-evolving digital landscape.**