IT Security Plan for Coop Sweden

A group project assignment of 'Information and IT Security Management (IITS)' course

Group-C

Group members

Muhammad Aqib
Samir Hossain Santo Bepu
Pavan Gupta
Khondaker Refai Arafat
Muhammad Arsalan Khan Mughal

Course coordinator:

Lisa Kaati

Information Security, DSV, Stockholm University

IT Security Plan for Coop Sweden

Project Name: **Coop Sweden Security Enhancement and Resilience Project**

Proposal Date: **November 19, 2024**

Project Team

Project Manager: Khondaker Refai Arafat

Responsibilities: Oversee project scope, timeline, budget management, and coordination among team members.

Security Analyst: Samir Hossain Santo Bepu

Responsibilities: Lead security audits, risk assessments, vulnerability management, and monitoring of security implementations.

IT Infrastructure Specialist: Muhammad Arsalan Khan Mughal

Responsibilities: Implement and maintain technical security controls, manage network security, and ensure system integrity.

Legal Compliance Officer: Pavan Gupta

Responsibilities: Ensure all security measures comply with GDPR and other relevant legal frameworks, manage third-party contracts and compliance.

Training Coordinator: Aqib Muhammad

Responsibilities: Develop and deliver cybersecurity training programs, manage awareness campaigns, and evaluate training effectiveness.

Executive Summary

This project aims to enhance the overall cybersecurity posture of Coop Sweden by implementing a robust IT security plan, incident response and recovery plan, and a third-party risk management policy. The project addresses vulnerabilities highlighted by the REvil supply chain attack, specifically strengthening Coop's defenses against supply chain attacks, ensuring compliance with legal and regulatory standards, and enhancing the organization's preparedness for future incidents. Key components include enhanced cybersecurity protocols, a comprehensive Incident Response and Recovery Plan, and a Third-Party Risk Management Policy. These elements aim to fortify Coop's infrastructure, improve resilience against ransomware attacks, and reduce exposure to third-party vulnerabilities. The proposed strategies will enable Coop to respond swiftly to threats and minimize downtime in future cybersecurity incidents.

Table of Contents

1. Security Strategy

Our security strategy is designed to create a comprehensive and resilient security posture by integrating defense in-depth mechanisms and complying with standards and policies. The key components include:

1.1 Preventive Security

Firewalls: Deploy next-generation firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules. For example Palo Alto Networks Next-Generation Firewall, Cisco Firepower Threat Defense, etc.

Intrusion Detection System(IDS): It will be a critical component of a robust incident response plan. It will detect and alert the security team to potential threats enabling timely and effective responses. e.g. Cisco NGIPS.

Intrusion Prevention System(IPS): Induct the IPS to continuously monitors the network for malicious activity and take action to prevent it including reporting, blocking, or dropping when an intrusion occurs. For example, Check Point Quantum IPS.

Endpoint Detection and Response (EDR): Implement EDR solutions to provide continuous monitoring and response capabilities for all endpoints.

Regular Updates and Patch Management: Establish a rigorous schedule for applying security patches and updates to all systems and software to mitigate vulnerabilities. Before installing any updates, we will test in a sandbox environment to avoid disruption on large and get to know whether the update works properly so that it does not cause reputational and monetary damage.

1.2 Preparedness for Incidents (Incident Response and Recovery Plan)

Planning and preparation: In this phase, plans are made for future incidents. Rules and regulations are made, revised, and published. Develop an IRT(incident response team) that includes a manager, cybersecurity engineer, and analyst. The responsibilities of each person in the company are clearly defined in this phase. Lastly, a complete strategy is made with the support of stakeholders, including disaster planning, continuity planning, who to contact if an incident happens, and a contact list.

Identification: In this phase, the main task is to identify the affected part of the system to contain that section. In order to find an infected part of the system or network, the IRT team scans the system using different tools, once it is identified the containment phase starts. The IRT team also saved a forensic image of the system for analysis.

Containment: In this phase, we have to isolate the affected part of the system so that the attack does not spread to the whole IT system. It could be short time containment or long time

containment. In long-term containment, despite the incident, the part of the infected system continues to run but limited process but in short-term containment the server is discontinued for some time. All the logs and time stamps are documented and backup data.

Eradication and Recovery: In this phase root cause of the incident is discovered and removed. The cause for the incident is documented and countermeasures are made. The IRT team and stakeholders decide whether to go for an escalation or not. The data are restored in the servers. The forensic image, log data, and timestamps are collected and saved in a secure place for cyber forensics and analysis. The system is tested for any infection before going to production again.

Post-incident event: This is a learning phase. In this phase, the whole incident is documented and shared with the partner organization internationally so that everyone can learn about that. Brief the incident to the company employees and set up an awareness training program for the employees. Countermeasures and strategies are reviewed and modified.

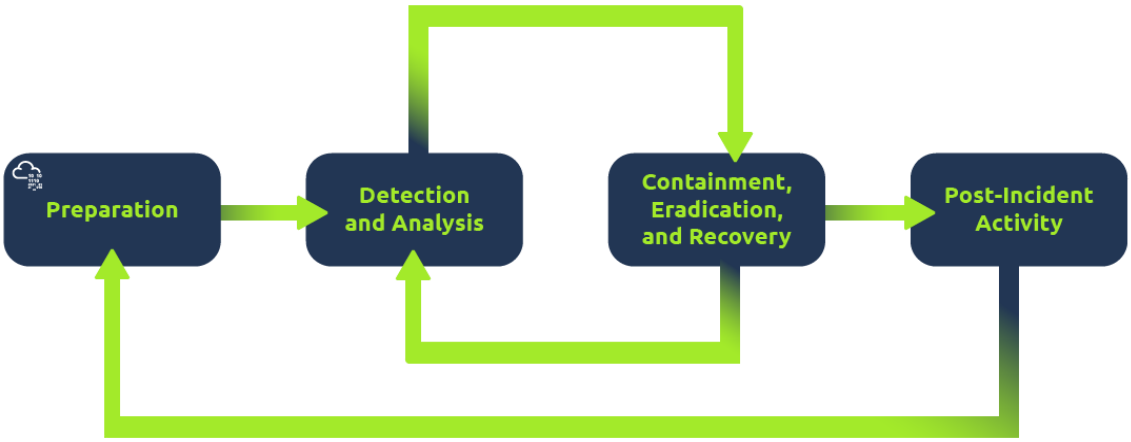

Figure 1: Incident Response and Recovery Plan

Regular Backups: Implement automated daily backups of critical systems and data, ensuring backups are stored securely and tested regularly for integrity.

Disaster Recovery Plan (DRP): Establish a DRP to guide the restoration of operations and systems in the event of a significant disruption.

1.3 Third-Party Risk Management

Initial Vendor Security Assessments: We will demand from all the third parties involved for independent security audits of the vendor's security policies, practices, and infrastructure. This will include evaluating the vendor's security controls, such as access management, data protection measures, and compliance with industry-standard "ISO 27001".

On-Site and Remote Audits: Depending on the vendor's criticality and the sensitivity of data they handle; Coop may conduct either remote audits or on-site inspections. During these audits, Coop's

security team assesses technical and administrative controls by reviewing documentation, inspecting physical security measures, and conducting interviews with the vendor's security personnel.

Penetration Testing and Vulnerability Scanning: Audits will include penetration testing and vulnerability scans on the vendor's systems, with the vendor's permission, to identify exploitable vulnerabilities, to further rectify them, and to verify.

Compliance and Certification Checks: There will be a check for verifying the vendor's compliance with required security certifications, ISO 27001, ensuring that they follow industry-recognized standards for information security management. If the vendor is not certified, Coop may request a plan for obtaining relevant certifications as a condition of the partnership.

Regular and Periodic Reviews: Coop will conduct periodic audits throughout the partnership to ensure vendors continuously adhere to Coop's security standards.

Reporting and Risk Mitigation: After the audit, Coop will generate a detailed report outlining the vendor's security posture, areas of improvement, and any identified risks. Coop and the vendor will then work collaboratively on a risk mitigation plan to address weaknesses, ensuring that the vendor's systems and processes meet Coop's security requirements and reduce potential vulnerabilities.

2. Legal and Compliance Considerations

2.1 GDPR Compliance

Ensuring GDPR compliance is essential for Coop to protect customer data and avoid regulatory penalties.

Data Protection Policies: Coop must establish robust data protection policies that outline the guidelines for collecting, processing, and storing personal data. These policies will cover data access controls, encryption standards, and secure data transfer protocols to prevent unauthorized access. Additionally, the policies should specify roles and responsibilities for data protection within Coop, ensuring that employees understand their obligations under GDPR. Regular training sessions will be conducted to keep staff informed about GDPR requirements and Coop's data handling procedures.

Data Minimization: The principle of data minimization requires Coop to collect and retain only the personal data necessary for specific business purposes. This involves reviewing data collection practices to ensure they align with operational needs and regulatory requirements. Coop should avoid collecting excessive information, and all data that's no longer relevant or needed should be deleted or anonymized.

Data Subject Rights: GDPR grants individuals specific rights regarding their personal data, including the right to access, rectify, erase, and transfer their information. Coop should implement

a streamlined process for handling data subject requests, with clear instructions for individuals on how to exercise their rights.

2.2 Industry-Specific Standards

PCI DSS Compliance for POS Systems: Ensure all POS systems adhere to PCI DSS standards by encrypting card data, using access controls, and segmenting POS networks. Regular updates, vulnerability assessments, and transaction monitoring are essential to protect cardholder data and detect fraud.

Regular Audits for Compliance: Conduct routine audits to verify compliance with PCI DSS, GDPR, and other regulations, addressing security gaps proactively. These audits reinforce data protection practices, ensure secure data handling, and foster a culture of accountability across Coop.

3. Risk Assessment and Security Audit

3.1 Risk Assessment

Asset Identification: Asset identification will involve cataloging all critical assets within the organization, such as POS (Point of Sale) systems, customer databases, and network infrastructure.

Threat Identification: Identifying the potential threats that could impact the organization, including ransomware, phishing attacks, and vulnerabilities within the supply chain.

Vulnerability Analysis: Perform a detailed assessment of existing vulnerabilities within systems, applications, and third-party integrations.

Risk Evaluation: Evaluate the likelihood of each identified threat exploiting known vulnerabilities and assess the potential impact on the organization. By prioritizing risks based on severity, this step resources will be allocated effectively to mitigate the most significant risks first.

3.2 Security Audit

Comprehensive Audit: Conduct an in-depth security audit across Coop's IT environment, covering all systems, applications, and network infrastructures. The objective will be to assess the effectiveness of current security controls, policies, and procedures, and to uncover any existing security gaps or weaknesses.

Audit Findings: Document all findings from the audit, including vulnerabilities, compliance issues, and other areas needing improvement. This report will serve as a detailed record of Coop's current security posture, highlighting specific areas where security standards are not being met or where potential risks are identified.

Remediation Plan: Develop a comprehensive remediation plan based on audit findings. This plan should outline actionable steps to address identified issues, designate responsible parties for each action item, and establish clear timelines for resolution.

4. Security Measures and Controls

4.1 Technical Controls

Multi-Factor Authentication (MFA): Implement MFA for all critical systems to provide an extra security layer beyond passwords, reducing the likelihood of unauthorized access even if passwords are compromised.

Network Segmentation: Segment the network into smaller sections to contain any potential breaches. This setup limits attackers' ability to move across systems, reducing overall impact in the event of a breach.

Advanced Threat Monitoring: Deploy a Security Information and Event Management (SIEM) system for real-time monitoring of security alerts from network hardware and applications. SIEM enables quicker detection and response to threats.

Encryption: Apply strong encryption protocols, like AES-256, to secure sensitive data both at rest (when stored) and in transit (during transmission), protecting data from unauthorized access and ensuring compliance with security standards.

4.2 Administrative Controls

Third-Party Risk Management Policy: Establish a comprehensive policy for evaluating, selecting, and monitoring third-party vendors based on their security practices. This policy should ensure that vendors meet Coop's security standards and maintain a secure environment that aligns with organizational risk management strategies.

Vendor Security Protocols Review: Conduct regular reviews and updates of security protocols with vendors to ensure they remain compliant with the latest security requirements. This helps address emerging threats, mitigate risks, and maintain continuous protection for sensitive data and systems.

Access Control Policies: Implement strict access control measures to ensure that employees have only the minimum level of access necessary to perform their tasks. This policy helps prevent unauthorized access and reduces the potential for data breaches by limiting access to sensitive systems and information.

5. Training and Awareness

5.1 Cybersecurity Training

Mandatory Training Programs: Ensure that all employees undergo regular, mandatory cybersecurity training. This training should cover essential topics such as identifying phishing attempts, understanding ransomware threats, and recognizing social engineering tactics. Empowering employees with the knowledge to spot and avoid cyber threats is a key step in reducing the likelihood of successful attacks.

Specialized Training for IT Staff: Offer advanced, specialized training for IT personnel, focusing on the latest security technologies, threat intelligence, and incident response methods. This training will equip IT staff with the skills necessary to detect, respond to, and mitigate complex cybersecurity threats, ensuring a well-prepared team to handle advanced security challenges.

5.2 Incident Response Drills

Regular Simulations: Conduct frequent incident response drills, including tabletop exercises, to simulate real-world cyberattacks. These exercises will ensure that all employees are well-versed in the response protocols and can act quickly and effectively during an actual security breach, minimizing potential damage.

Post-Drill Reviews: After each drill, conduct a thorough analysis of the results to evaluate how well the response protocols were followed and identify any gaps or weaknesses. These insights will be used to update and refine the incident response plan, ensuring it remains relevant and effective in addressing evolving threats.

6. Incident Response and Recovery

6.1 Incident Detection

Real-Time Monitoring: Implement advanced monitoring tools, such as Security Information and Event Management (SIEM) systems, to continuously monitor network traffic, user activities, and system logs for any signs of suspicious behavior or potential security breaches.

Automated Alerts: Set up automated alert systems that immediately notify the incident response team whenever suspicious activities are detected. These alerts should be configured to highlight critical events such as unauthorized access, abnormal network behavior, or system anomalies, enabling a swift response to mitigate risks.

6.2 Response Team Activation

Defined Roles and Responsibilities: Clearly outline and assign specific roles and responsibilities to each member of the incident response team. This ensures a structured, organized response, with individuals knowing exactly what actions to take. Roles will include incident lead, technical experts, legal advisors, and communication officers.

Communication Protocols: Develop and implement secure communication channels (such as encrypted emails, private messaging platforms, or dedicated incident response tools) to facilitate rapid, secure, and effective communication within the team.

6.3 Recovery

Data Restoration: Ensure that daily backups are systematically created and regularly tested to confirm their integrity. In the event of a data breach or attack, these backups should be leveraged to restore compromised systems quickly, reducing both downtime and the potential impact on operations.

Documentation: Throughout the recovery process, meticulously document each action taken, including timelines, affected systems, and recovery procedures.

Post-Incident Review: After the incident, conduct a thorough review of the entire response and recovery process. Assess the efficiency of the recovery efforts, identify areas for improvement, and document lessons learned. This review should inform any necessary changes in the security posture, policies, and procedures to mitigate the risk of similar incidents in the future.

7. Project work breakdown(WBS)

7.1 Project Management

Planning and Timeline Development: According to the higher authorities' guidelines of Coop, all teams sit together to make a detailed plan for implementation and ensure alignment with the six-month implementation period.

Budget and Resource Allocation: The financial team will monitor the implementation budget, and HR will ensure the resources are allocated effectively across IT upgrades, security tools, and training programs.

Stakeholder and Team Coordination: It will be made sure that communication among all team members, Coop's management, and external partners or vendors is continuous during implementation.

Review and Evaluation: A comprehensive evaluation will be conducted post-implementation, identifying lessons learned and documenting best practices for future security projects.

Monitoring and Reporting: Reporting structures will be followed to track progress, issues, and compliance with the timeline. In addition, regular updates will be provided to Coop's management.

7.2 Security Strategy Development

a. **Security Goals and Objectives**: It is the goal of coop security to maintain confidentiality, integrity, and availability and ensure compliance with GDPR and industry standards and Coop internal policies.

b. **Preventive Security Measures**: It will be the duty of the security team to use robust tools to prevent unauthorized access and threats.

Firewalls: The security team will deploy next-generation firewalls (e.g., Palo Alto, Cisco Firepower) to filter and monitor network traffic, preventing unauthorized access.

Intrusion Detection System (IDS): The security team will install IDS to detect suspicious activities in real-time, enabling the security team to respond swiftly.
Intrusion Prevention System (IPS): The security team will deploy IPS (e.g., Check Point Quantum IPS) to actively block detected intrusions before they impact systems.
Endpoint Detection and Response (EDR): The security team will use EDR tools to monitor endpoints continuously, detecting and responding to potential threats.
Regular Updates and Patch Management: It will be the duty of the security team to implement a routine for security patches, testing them in a sandbox environment before deployment.

c. **Incident Response and Preparedness**: The security team will be able to detect, respond to, and recover from security incidents efficiently.

Incident Response Plan (IRP): The security team will develop a clear IRP outlining detection and response procedures for security breaches.
Incident Recovery Plan: The security team will document a structured recovery process that defines tasks and assigns responsibility to minimize downtime.
Regular Backups: The security team will implement automatic daily backups of critical data and systems, testing backups regularly.
Disaster Recovery Plan (DRP): The security team will create a DRP for restoring operations after a severe incident, ensuring minimal operational disruption.

7.3 Third-Party Risk Management

Vendor Security Assessments: It is required that security audits from third-party vendors should be reviewed, their policies, practices, and infrastructure. It should be according to rules and regulations.
Conduct On-Site and Remote Audits: For the third parties, audits based on the vendor's data sensitivity, and assessing technical and administrative security controls will be performed.
Compliance and Certification Checks: It is necessary to check and verify third party certifications (e.g., ISO 27001) and compliance with security standards. If certifications are lacking, require a plan for attaining them.
Generate third party Security Reports: There will be documented third party security posture, highlighting areas for improvement.
Collaborate on Risk Mitigation Plans: Security team will work with third parties to address any identified weaknesses to be rectified to meet Coop's security requirements.

7.4 Legal and Compliance Considerations

GDPR Compliance Review: It will be ensured that all processes and controls meet GDPR standards to protect customer data and avoid penalties.
Data Protection Policies: We will create policies for data access, encryption, and secure data transfer. Assign roles for data protection compliance and conduct regular training on GDPR.

Industry-Specific Standards Compliance: We will ensure compliance with standards relevant to retail and point-of-sale (POS) systems.
Conduct Routine Audits: Regular audits will be arranged to verify ongoing compliance with PCI DSS, GDPR, and other applicable regulations.

7.5 Risk Assessment and Security Audit

Risk Assessment: Security team has the responsibility to identify assets and evaluate threats and vulnerabilities. Security team will identify potential threats (e.g., ransomware, phishing) and analyze system vulnerabilities.

Security Audit: Security team will conduct a comprehensive audit to evaluate the effectiveness of Coop's security posture.

Administrative Controls: We will make sure security through policies, effective controls, and regular reviews.

Third-Party Risk Management Policy: We will set policies for vetting and monitoring vendors based on Coop's security standards.
Vendor Security Protocols Review: We will conduct ongoing reviews of vendor security measures, ensuring they meet the recommended requirements.
Access Control Policies: We will make sure that there will be limited access based on the principle of least privilege, and zero trust ensuring employees access only what they need.

7.6 Training and Awareness

Cybersecurity Training Programs: There will be training sessions for staff to recognize, and report threats.

Incident Response Drills: We will prepare employees for potential incidents.

Conduct Regular Simulations: we will use tabletop exercises to simulate potential cyberattacks and improve response protocols.

Post-Drill Analysis and Improvement Plans: We will evaluate drill outcomes, identifying weaknesses to enhance the incident response plan.

Incident Response and Recovery

Incident Detection: We will establish real-time monitoring and alert systems.

Real-Time Monitoring (SIEM): We will use SIEM to track network activity, identify unusual behaviors, and detect threats.

Set Up Automated Alerts: We will configure alerts for critical security events, enabling immediate incident response.

Response Team Activation: Activate response protocols efficiently. We will define and assign specific roles, including incident lead and communication officers.

Recovery: Restore systems to operational status.

Data Restoration from Backups: We should be able to restore systems using tested backups to minimize downtime.

Post-Incident Review and Documentation: We will document each step of the response, including lessons learned, to improve future protocols.

8. Project Risks and Mitigation

Risk 1: Dependency on Third-Party Software Providers

Impact: Potential vulnerabilities in third-party software can be exploited, leading to security breaches.

Mitigation:

- Implement a stringent vendor vetting process, including security assessments and compliance checks.
- Establish contractual obligations requiring vendors to maintain high-security standards and notify Coop of any security incidents promptly.
- Diversify third-party dependencies to avoid reliance on a single vendor.

Risk 2: Insufficient Staff Training Leading to Compliance Gaps

Impact: Employees may inadvertently create security vulnerabilities through lack of awareness or understanding of security protocols.

Mitigation:

- Develop and enforce mandatory, regular cybersecurity training programs for all employees.
- Utilize interactive training methods, such as simulations and quizzes, to enhance engagement and retention of security best practices.
- Monitor and evaluate training effectiveness through assessments and feedback mechanisms.

Risk 3: Budget Overruns

Impact: Exceeding the allocated budget can delay project completion and limit the scope of security enhancements. But if requirements change it means the budget will also have affected.

Mitigation:

- Develop a detailed budget plan with clear cost estimates for each project component.
- Monitor expenditures regularly and adjust resource allocation as needed to stay within budget.
- Identify potential cost-saving measures without compromising security effectiveness.

9. Project Constraints

Budget: The project is constrained by a fixed budget allocated for IT infrastructure upgrades, security tools acquisition, and training programs. A specific budget is needed to create an incident response and recovery manual.

Time: The security enhancements must be fully implemented within six months to minimize operational risks. After 6 months of implementation, the security team will do the naturalistic post-evaluation.

Resources: Limited availability of internal cybersecurity staff necessitates the potential engagement of external security experts.

Compliance: All security measures must comply with GDPR, the coop internal policies, and other relevant retail stores' industry-specific data protection standards.

Scope: Focus is limited to enhancing security related to point of sale (POS) systems, network infrastructure, and third-party software integrations.

10. Project Assumptions

Resource Availability: Adequate internal and external resources will be available to support project activities.

Vendor Cooperation: Third-party vendors will comply with Coop’s security requirements and provide necessary support.

Stakeholder Support: Executive leadership and key stakeholders will provide the necessary support and approval for security initiatives.

Technological Compatibility: Existing IT infrastructure will support the integration of new security tools and technologies without significant modifications.

11. Detailed Budget and Schedule

Table 1: Budget

Category	**Estimated Cost (SEK)**	**Description**
Personnel Costs	3,200,000	Salaries for project team members
Security Tools	1800,000	Purchase and licensing of firewalls, EDR, MFA, SIEM
Training Programs	1300,000	Development and delivery of cybersecurity training
External Consultants	1000,000	Engagement of external security experts
Incident Response Tools	500,000	Tools for incident detection and response
Backup and Recovery Systems	1400,000	Implementation of robust backup solutions
Miscellaneous Expenses	500,000	Contingency funds for unexpected costs
Total Estimated Budget	**9,700,000 SEK**	

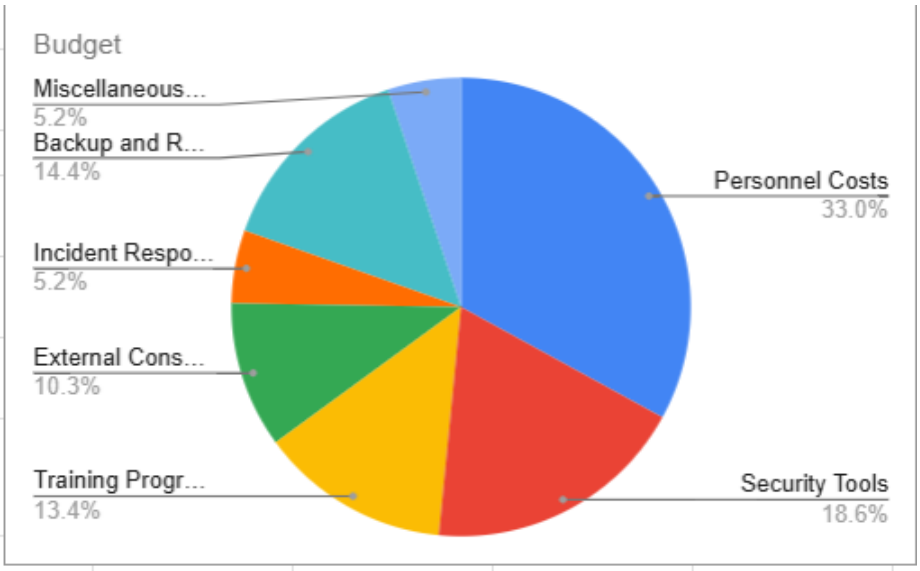

Figure 2: Budget

Table 2: Schedule

Phase	**Timeline**	**Key Activities**
Month 1: Project Planning	November 2024	Define scope, objectives, assign team roles, develop project plan
Month 2: Risk Assessment and Security Audit	December 2024	Conduct risk assessments, perform security audit, document findings
Month 3-4: Implementation of Security Controls	January 2025	Deploy firewalls, MFA, network segmentation, and SIEM systems
Month 4-5: Staff Training and Awareness Program	February 2025	Develop and conduct training sessions, initiate awareness campaigns
Month 5: Incident Response Plan Creation	March 2025	Develop and test incident response and recovery plans
Month 6: Final Testing and Evaluation	April 2025	Conduct penetration testing, evaluate security measures, finalize documentation
Project Closeout	April 2025	Review project outcomes, handover to operations, final reporting

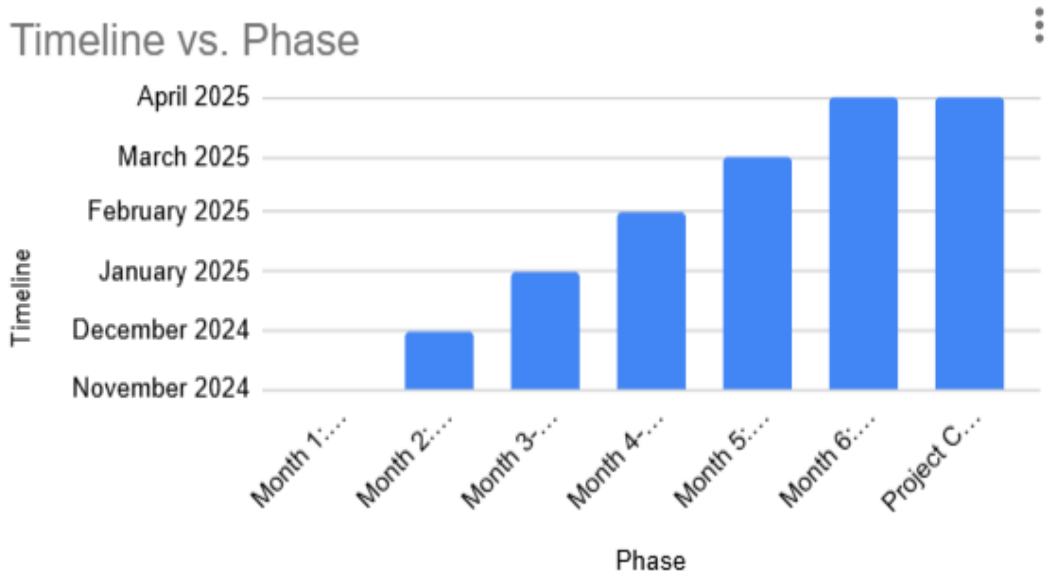

Figure 3: Schedule

Conclusion

The Coop Sweden Security Enhancement and Resilience Project is a strategic initiative designed to fortify Coop's IT infrastructure against sophisticated cyber threats. By implementing a comprehensive security strategy, enhancing third-party risk management, and fostering a culture of cybersecurity awareness, Coop Sweden will significantly reduce the risk of future ransomware attacks, and phishing attacks along with their variations, and ensure the continuity of its operations. This detailed IT Security Plan provides a clear roadmap for achieving these objectives within the defined constraints, ensuring that Coop remains secure and resilient in an increasingly hostile cyber landscape.

Appendix A

Policy According to ISO 27001/27002

1. Third-Party Risk Management Policy

1.1 Purpose
To mitigate risks associated with third-party vendors and ensure that all external entities accessing Coop's systems adhere to strict security standards.

1.2 Scope
This policy applies to all third-party vendors, including IT service providers, contractors, and software providers, with access to Coop's network, data, or systems.

1.3 Policy Statements

- **Risk Assessment and Due Diligence**: All third-party vendors must undergo a security risk assessment before engagement. This includes evaluating vendors' compliance with security standards, such as ISO/IEC 27001 and 27002, and assessing the vendor's cybersecurity controls and incident history.
- **Contractual Security Requirements**: Contracts must specify Coop's information security requirements, including access controls, incident reporting, data handling, and encryption standards. Contracts should include clauses that mandate prompt notification of any security incidents affecting Coop's data.
- **Access Control**: Vendors will be granted access to systems following zero trust and least privilege principles. Access controls should follow Coop's data classification and labeling protocols.
- **Regular Monitoring and Compliance Audits**: Coop will regularly monitor third-party activities and review security measures through periodic audits to ensure continued compliance with Coop's security policies. Any changes in third-party service delivery or security practices must be reviewed, and assessed for risks.
- **Termination and Data Management**: Upon the end of a contract, all access must be revoked, and Coop's data must be returned or securely deleted in line with contract requirements.

1.4 Roles and Responsibilities

- **IT Security Team**: Conducts third-party risk assessments, monitors compliance, and ensures appropriate access controls.
- **Legal and Compliance**: Reviews and enforces security clauses in vendor contracts.
- **Department Heads**: Oversee vendor activities and adherence to security requirements.

2. Incident Response and Recovery Policy

2.1 Purpose
To establish a systematic approach for identifying, responding to, and recovering from security incidents to minimize operational impact and restore Coop's systems swiftly.

2.2 Scope
This applies to all Coop employees, third-party vendors, and contractors who access or handle Coop's information systems.

2.3 Policy Statements

- **Incident Detection and Reporting**: Employees and vendors must report any suspected or actual security incidents immediately to the Incident Response (IR) Team. Coop will maintain multiple channels (e.g., hotline, secure messaging) to facilitate timely incident reporting.
- **Incident Classification**: The IR Team will assess and classify incidents based on potential impact, from minor security events to critical incidents, such as ransomware attacks. This classification helps prioritize response actions and ensures proper resource allocation.
- **Containment and Mitigation**: Upon detecting an incident, containment measures will be implemented promptly to isolate affected systems and prevent lateral spread. Containment may involve disconnecting infected systems, resetting credentials, and activating backups.
- **Forensic Analysis and Evidence Preservation**: The IR Team will perform forensic analysis to determine the incident's cause, scope, and impact. All relevant evidence will be preserved for potential legal actions or regulatory investigations.
- **Communication and Escalation Protocol**: The IR Team will communicate incident details to stakeholders, including management, legal, and external authorities, as appropriate. The incident escalation protocol will be followed to ensure timely engagement with executive leadership in critical incidents.
- **Recovery and Restoration**: After containment, Coop will restore affected systems and validate data integrity through backups. Systems will only return to full operation once all security checks confirm stability and safety.
- **Post-Incident Review and Continuous Improvement**: A post-incident review will be conducted to identify lessons learned and apply improvements to Coop's security measures. Insights from this process will be used to update policies, procedures, and employee training materials.

2.4 Training and Awareness
Coop will conduct regular training for all employees and vendors on incident detection, reporting procedures, and role-specific response actions. This ensures preparedness and minimizes response times during real incidents.

2.5 Roles and Responsibilities

- **Incident Response Team**: Leads incident classification, containment, forensic analysis, and communication.
- **IT Department**: Assists in technical containment, recovery efforts, and system restoration.
- **All Employees and Vendors**: Must report incidents immediately and cooperate with the IR Team.

3. Ransomware-specific controls and Business Continuity Measures

3.1 Ransomware Detection and Prevention

- Implement endpoint detection and response (EDR) solutions to monitor for ransomware behavior patterns.
- Conduct regular phishing awareness training for employees to reduce the likelihood of malware infection via email.

3.2 Data Backup and Recovery

- Regularly back up critical data and store backups in isolated, encrypted environments. Conduct frequent testing of backup systems to ensure reliable data restoration.

3.3 Business Continuity Planning (BCP)

- Establish and periodically test BCP protocols to ensure Coop can continue critical operations in the event of a ransomware attack or similar disruption.

3.4 Incident Simulations

- Conduct regular incident response exercises, including ransomware attack simulations, to assess and enhance Coop's readiness.

Compliance and Enforcement

Non-compliance with this IT Security Plan, including the Third-Party Risk Management and Incident Response policies, may result in disciplinary actions for employees or termination of contracts for third parties. Regular audits will assess compliance with security policies, and Coop will ensure continual improvements through policy reviews and incident learning.

Appendix: B Sample Security Training Materials

Coop Sweden Employee Security Awareness Training

This training material will be designed to equip employees with essential knowledge and practices to protect Coop Sweden from cyber threats, focusing on recognizing and responding to incidents, secure handling of third-party relationships, and understanding personal responsibilities in maintaining Coop's IT security. The training will be provided according to the employee or company's needs and it will be paid for by the company to acquire the right skills.

Internal educational material will include topics like the following:

- Introduction to Cybersecurity Awareness
- Recognizing and Responding to Security Incidents
- Incident Reporting Process
- What to Include in a Report
- Key Actions to Take and Avoid
- Phishing Awareness and Social Engineering
- Protecting Coop's Data When Working with Third Parties
- Employee Responsibilities
- Data Handling and Access Control
- Incident Response Procedures and Ransomware Prevention
- Data Protection Best Practices
- Compliance and Security Culture

The education will not be limited to the above-mentioned topics.

References

https://www.ibm.com/blogs/nordic-msp/how-a-supply-chain-attack-closed-one-of-swedens-largest-supermarket-chains