Introduction

The CRC has multiple options for leveraging AI in the services they provide and with the underlying operations of the organization. Examples include using an AI chatbot which could provide an efficient front line interface for potential donors, volunteers, and even individuals seeking training. Operationally, an AI data modelling solution could help identify locations where a natural disaster may occur, what the best locations are for support centres during a natural disaster, and what specific training may be required for a potential disaster. As systems move to the cloud, AI can be used for coding support and for creating marketing materials such as social media posts and emails. Other use cases include using AI to enhance emergency operations, healthcare services, and fundraising efforts.

AI security is important for the CRC to prevent unauthorized access to donor and patient data, ensuring AI models make unbiased and fair decisions, and protecting AI systems from misuse or tampering. This leads to some key risks associated with using AI including data leaks of sensitive data as a result of AI tools being trained with inferior coding that contains coding errors and/or vulnerabilities. As well, data models used to drive decision making could be biased which would risk inappropriate decisions. Finally, there is a risk that bad actors seeking to access the personally identifiable information of donors, staff, and other third parties, including banking information, could leverage AI to understand coding structures or to uncover any 'back doors' that could be exploited to breach the existing safeguards.

Policy Statement

The CRC is committed to the secure, ethical use of Artificial Intelligence (AI) in humanitarian, disaster response, and healthcare efforts. We integrate AI security into our governance framework to protect sensitive data, mitigate cyber threats, and ensure transparency with vulnerable communities. Our focus on human-centered solutions enhances operational efficiency while safeguarding the rights of affected individuals and meeting

compliance requirements such as PIPEDA, PHIPA, and PCI-DSS. Our AI security strategy ensures mission-critical operations remain secure, promoting responsible innovation, compliance with privacy laws, and strengthening stakeholder confidence in our digital transformation.

Key Policy Requirements

Data Protection

● The CRC ensures that data for AI systems is collected, shared, and deleted in ways that respect privacy and align with our Code of Conduct. AI training data must be accurate, fair, and unbiased to protect the rights and dignity of affected individuals, with measures to prevent harm. Confidential information, including personal data, is handled carefully and not transferred to non-approved external AI systems. Data is safeguarded through encryption, anonymization, and access controls, ensuring compliance with relevant privacy regulations, and through regular audits to prevent unauthorized access and data integrity issues.

Access Control

● Effective governance mechanisms shall be used to ensure that AI solutions, including access to models and data, align with organizational obligations and comply with relevant regulations. Competent, trained staff will oversee enforcement and compliance with this policy and internal rules, while role-based access control (RBAC) and multi-factor authentication (MFA) will restrict access to AI models and data. Only authorized personnel, such as AI system administrators, data scientists, and security teams, will be granted access, ensuring AI systems are used solely for approved humanitarian and operational purposes.

Model Security

● AI systems, models, and tools will be protected by cybersecurity measures, including encryption, access controls, and regular vulnerability assessments to prevent tampering and misuse. Legal counsel will be involved in decision-making to ensure AI deployments comply with laws, regulations, and ethical standards, minimizing risk and ensuring accountability. Secure development lifecycle practices, version control, and real-time monitoring, along with regular security assessments, will safeguard AI systems from attacks. Third-party AI vendors must comply with our security policies before integration.

Bias & Fairness

● The CRC proactively identifies and mitigates AI-related biases, including those based on gender, race, and other factors, ensuring equitable assistance. We prioritize ethical, neutral, and independent AI solutions, avoiding technologies that could compromise impartiality, and explore open-source alternatives to reduce risks. AI systems are designed to complement human engagement and maintain empathy, avoiding those that manipulate behavior or rely on biometric categorization or social profiling. Bias detection, fairness metrics, and regular audits will ensure AI systems are ethical, non-discriminatory, and aligned with our core principles.

Transparency and Accountability

● The CRC will provide clear information about AI systems to stakeholders when these systems may impact their rights or involve significant decisions. We will implement traceability, disclosure, and notification measures based on risk levels, including releasing AI systems as open-source when appropriate. AI decisions will be interpretable and auditable, with explainability frameworks to help stakeholders understand AI model conclusions. Documentation, model logs, and governance reports will be maintained for external reviews and regulatory compliance.

AI Security Standards

The table below outlines the various standards that the Canadian Red Cross should ensure that their AI systems adhere to:

Category	What Needs to Be in Place?
Data Security	AI-related data must be protected using AES-256, and sensitive data should be kept in a secure location on servers or cloud services
Access Control	Multi-factor authentication (MFA) and role-based access controls (RBACs) should be used for any systems that have access to AI models and data.
Model Validation	AI models should be thoroughly tested using both historical and real-time data to ensure accuracy and performance. Models must also be evaluated for adversarial resilience and robustness.
Logging & Monitoring	AI activity should be continuously logged, including interactions with models, inputs, outputs, and errors. Also, real-time monitoring technologies should be used to identify unusual data inputs or anomalies in AI behaviors.
Regulatory Compliance	Audits for compliance against all relevant regulations (PIPEDA, PHIPA, CASL, PCI-DSS), and data protection impact assessments (DPIAs) should be done.
Third-Party Risk	Vendors supplying AI services must follow the same security and privacy guidelines as the Canadian Red Cross, and they should be periodically audited.

AI Security Guidelines
AI Development & Deployment

The best practices that the organization should follow when developing and deploying AI include:

- Conducting thorough assessments to identify potential risks associated with AI systems, considering ethical, legal, and technical factors.
- Implementing robust data governance to maintain high-quality, representative datasets, which are crucial for effective AI performance
- Prioritizing data privacy and security to protect sensitive information, adhering to relevant regulations and standards.
- Protecting sensitive information by ensuring that AI systems do not inadvertently expose confidential data through their outputs
- Maintaining comprehensive documentation of AI development and deployment processes to support transparency and accountability.

Before being used, AI systems should be tested for security risks by:

- Implementing mechanisms to validate and sanitize outputs before they are used or displayed to prevent inadvertent code execution or data leakage.
- Ensuring that inputs to AI systems are thoroughly validated to prevent prompt injection attacks that risk unauthorized access or data breaches.
- Developing and validating AI models rigorously to ensure accuracy, fairness, and reliability. Also by utilizing techniques like adversarial testing to identify and address vulnerabilities.
- Setting up ongoing monitoring to detect and respond to anomalies or performance issues in real-time, and by implementing feedback mechanisms
- Developing test cases with varied prompt structures to identify potential injection points.
- Implementing code analysis and validation tools to detect and prevent unauthorized code execution.
- Conducting testing to assess the risk of information leakage through model queries.

AI Access & Use

Before employees use AI, the following security measures should be in place:

- Use of Role-Based Access Control (RBAC) as well as MFA controls
- Adherence to the principle of Least Privilege to ensure users access only necessary data and functionalities.
- Collection and processing of only essential data
- Applying encryption to both stored and transmitted data
- Performing regular security audits to identify vulnerabilities and compliance
- Regular updating of systems to ensure that patches for various vulnerabilities have been applied.

The following AI decisions require human oversight:

- AI system performance and compliance with ethical standards.
- All decisions that may change the level of risk or the risk mitigating measures

AI Security Monitoring & Response

AI security threats should be detected by:

- Establishing systems that continuously monitor AI models and network traffic to identify unusual behavior or potential attacks.
- Conducting regular vulnerability scans and penetration tests
- Educating employees about AI security risks and best practices
- Periodically assessing the system's architecture and data flows

Should any of the AI systems become compromised, the CRC should:

- Utilize monitoring tools to confirm the breach and assess the impact
- Disconnect compromised components and apply fixes or workarounds
- Rebuild and validate AI models and data from secure backups.

Project Prioritization & Gap Alignment

Project	Priority (High/Medium/Flexible)	Gaps Addressed
Purchase and Implement new CMDB	Medium	Outdated Systems, Global Coordination Challenges
System Audit and Risk Assessment	High	Third-Party Risks, Access Management, Limited Cybersecurity Infrastructure
Legacy System Replacement	High	Outdated Systems, Patch Management, Data Protection
Third-Party Policy	High	Third-Party Risks, Data Protection, Ethical Risks
Monitor EDR/SIEM by MSSP	High	Insider Threats, Disaster Response Resilience, NGO Threat Landscape
Identity and Access Management	High	Access Management, Insider Threats, Data Protection
End User Behaviour Analytics	Medium	Insider Threats, Ethical Risks
End User Training	High	Insider Threats, Ethical Risks, NGO Threat Landscape
Encryption Enhancement	High	Data Protection, Global Coordination Challenges
Disaster Response Resilience	High	Business Continuity, Limited Infrastructure, NGO Threat Landscape
Threat Intel Sharing	Medium	Global Coordination, NGO Threat Landscape
Zero Trust Architecture	High	Third-Party Risks, Insider Threats, Access Management
Cloud Security Posture Management	Medium	Data Protection, Limited Infrastructure
DDoS/DLP Protection	High	Data Protection, Ethical Risks, NGO Threat Landscape

Implementation Considerations

- Year 1 Focus: Legacy System Replacement, IAM, End User Training, Encryption, SIEM Monitoring, Zero Trust
- Year 2 Expansion: Cloud Security, Threat Intel Sharing, Disaster Response Resilience, CMDB Implementation
- Year 3 Enhancements: End User Analytics, DLP/DDOS Protection, Third-Party Policy Strengthening

3-Year Cybersecurity Implementation Roadmap

Project	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1. Purchase & Implement new CMDB	▶	▶	▶	✅								
2. System Audit & Risk Assessment	▶	✅										
3. Legacy System Replacement	▶	▶	▶	✅								
4. Third-Party Policy	▶	✅										
5. Monitor EDR/SIEM (MSSP)	▶	▶	✅									
6. Identity & Access Management	▶	▶	✅									
7. End User Behaviour Analytics					▶	▶	✅					
8. End User Training	▶	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
9. Encryption Enhancement	▶	▶	✅									
10. Disaster Response Resilience	▶	▶	▶	✅								
11. Threat Intel Sharing					▶	▶	✅					
12. Zero Trust Architecture	▶	▶	▶	✅								
13. Cloud Security Posture Mgmt					▶	▶	▶	✅				
14. DDoS/DLP Protection									▶	▶	▶	✅

Legend:

▶ = Project Initiation ✅ = Completion

This roadmap prioritizes high-risk projects in Year 1, strengthens defenses and resilience in Year 2, and enhances security posture in Year 3.

Cybersecurity Roadmap (3-Year Implementation Plan)

Year 1 - Q1

Project: System Audit and Risk Assessment

Objective: Identify vulnerabilities and prioritize remediation.

Financial Resources: $100K for external audit and assessment tools.

Technology Stack: Risk assessment frameworks, vulnerability scanners.

Project: Identity and Access Management (IAM)

Objective: Strengthen access controls and implement role-based access.

Financial Resources: $200K for IAM solution deployment.

Technology Stack: Privileged Access Management (PAM), Multi-Factor Authentication (MFA).

Year 1 - Q2

Project: Purchase and Implement new CMDB

Objective: Improve asset management and visibility.

Financial Resources: $150K for licensing and implementation.

Technology Stack: IT Asset Management (ITAM), Configuration Management Database (CMDB).

Project: End User Training

Objective: Enhance cybersecurity awareness among employees.

Financial Resources: $50K for training modules and workshops.

Technology Stack: Online learning platforms, phishing simulation tools.

Year 1 - Q3

Project: Monitor EDR/SIEM by Managed MSSP

Objective: Enable real-time threat detection and response.

Financial Resources: $300K for MSSP services.

Technology Stack: Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR).

Project: Third-Party Policy Implementation

Objective: Mitigate vendor risks through strict security policies.

Financial Resources: $75K for vendor assessments and policy development.

Technology Stack: Third-party risk management software.

Year 1 - Q4

Project: Legacy System Replacement

Objective: Replace outdated infrastructure with secure alternatives.

Financial Resources: $500K for software and hardware upgrades.

Technology Stack: Cloud-based solutions modernized applications.

Project: Threat Intel Sharing

Objective: Collaborate with Red Cross partners for proactive defense.

Financial Resources: $100K for integration and intelligence feeds.

Technology Stack: Threat intelligence platforms, secure communication channels.

Year 2 - Q1

Project: Encryption Enhancement

Objective: Secure sensitive data at rest and in transit.

Financial Resources: $250K for encryption software and implementation.

Technology Stack: AES-256 encryption, secure key management.

Year 2 - Q2

Project: Disaster Response Resilience

Objective: Ensure IT continuity during crises.

Financial Resources: $400K for redundancy and failover systems.

Technology Stack: Cloud-based backup, disaster recovery planning tools.

Year 2 - Q3

Project: Zero Trust Architecture

Objective: Implement continuous authentication and least privilege access.

Financial Resources: $500K for policy enforcement tools.

Technology Stack: Software-defined perimeters, micro-segmentation.

Year 2 - Q4

Project: Cloud Security Posture Management

Objective: Strengthen cloud security and compliance.

Financial Resources: $300K for automation tools.

Technology Stack: CSPM tools, cloud security monitoring.

Year 3 - Q1

Project: DDOS/DLP Protection

Objective: Prevent data exfiltration and service disruptions.

Financial Resources: $400K for mitigation tools.

Technology Stack: Data Loss Prevention (DLP), DDOS protection services.

Year 3 - Q2

Project: End User Behaviour Analytics

Objective: Detect insider threats and anomalous activities.

Financial Resources: $350K for analytics and AI-based monitoring.

Technology Stack: User and Entity Behavior Analytics (UEBA), AI-driven security monitoring.

Year 3 - Q3

Project: Continuous Security Improvement

Objective: Enhance security controls based on emerging threats.

Financial Resources: $500K for adaptive measures.

Technology Stack: AI-driven threat hunting, automated security orchestration.

Year 3 - Q4

Project: Final Evaluation & Optimization

Objective: Review and refine cybersecurity initiatives.

Financial Resources: $250K for assessments and enhancements.

Technology Stack: Security benchmarking tools, compliance frameworks.

Total Estimated Budget: $4.9M over three years.

So, is there any way to streamline the projects, are there projects that can be merged? If so, lets merge what can be merged and reprioritize

Yes, several of these projects have overlapping objectives and can be streamlined to improve efficiency and resource allocation. Here's how we can merge and reprioritize them

Merged Projects & Streamlined Initiatives

- IT Asset Management & Risk Reduction (Merging: Purchase and Implement new CMDB + System Audit and Risk Assessment)
- A new CMDB implementation should integrate automated risk assessments, eliminating the need for a separate audit initiative.
- Legacy System & Third-Party Risk Mitigation (Merging: Legacy System Replacement + Third-Party Policy)
- Many third-party risks stem from outdated systems. A combined approach ensures secure, modern replacements while enforcing stricter third-party security policies.
- Threat Detection & Response (Merging: Monitor EDR/SIEM by MSSP + Threat Intel Sharing)
- A Managed Security Services Provider (MSSP) should incorporate external threat intelligence sharing into the SIEM, reducing redundancy.
- Identity Security & Zero Trust (Merging: Identity and Access Management + Zero Trust Architecture)
- IAM is foundational for Zero Trust, making them a natural fit for a single strategic initiative.
- User-Focused Security Enhancements (Merging: End User Behaviour Analytics + End User Training)
- Behavior analytics can be integrated into security awareness training programs, allowing for adaptive learning based on user activity.
- Data Security & Resilience (Merging: Encryption Enhancement + Disaster Response Resilience + DLP/DDOS Protection)
- Encryption, disaster response planning, and data loss prevention should be part of a broader data protection and continuity strategy.
- Cloud & Compliance Security (Merging: Cloud Security Posture Management + Third-Party Policy)
- Cloud security measures should align with third-party risk management to enforce compliance and governance.

Reprioritized List of Projects

1. IT Asset Management & Risk Reduction (High Priority)
2. Legacy System & Third-Party Risk Mitigation (High Priority)
3. Threat Detection & Response (High Priority)
4. Identity Security & Zero Trust (High Priority)
5. User-Focused Security Enhancements (Medium Priority)
6. Data Security & Resilience (High Priority)
7. Cloud & Compliance Security (Medium Priority)

10-Slides Presentation to secure funding from executives

Slide 1: Title Slide

Title: Security Investment Proposal – Strengthening Our Cybersecurity Posture

Subtitle: A Strategic Approach to Address Critical Security Gaps

Presented by: [Your Name]

Date: [Presentation Date]

Slide 2: Executive Summary

- Cyber threats are evolving; our organization faces increasing risks.
- Key vulnerabilities identified across systems, users, and third-party integrations.
- Strategic security initiatives proposed to mitigate risks and enhance resilience.
- Investment in security will protect reputation, data, and business continuity.

Slide 3: Top Security Priorities for Next Year

- IT Asset Management & Risk Reduction – Improve visibility & security posture.
- Legacy System & Third-Party Risk Mitigation – Replace outdated systems & enforce policies.
- Threat Detection & Response – Strengthen SIEM & MSSP monitoring.
- Identity Security & Zero Trust – Implement strong access controls.
- Data Security & Resilience – Enhance encryption, DLP & disaster recovery.

Slide 4: Business Impact of Security Investments

- Financial Protection: Reducing breach costs and non-compliance fines.
- Operational Efficiency: Strengthening IT infrastructure and automating security.
- Reputational Safeguard: Maintaining trust among donors, stakeholders, and partners.
- Regulatory Compliance: Meeting industry and global security standards.

Slide 5: 3-Year Implementation Roadmap

- Year 1: IT asset visibility, IAM improvements, MSSP expansion.
- Year 2: Legacy system replacement, enhanced encryption & Zero Trust adoption.
- Year 3: Full cloud security optimization, threat intel sharing, and resilience testing.

Slide 6: Budget Overview

- Year 1: $2.5M – Foundational security upgrades & critical risk mitigation.
- Year 2: $3M – Advanced security enhancements & Zero Trust implementation.
- Year 3: $2M – Optimization & proactive security initiatives.

Total Investment: $7.5M over three years.

Slide 7: Resource & Personnel Requirements

- New Roles Needed: Security Analysts, IAM Specialists, Incident Response Team.
- Third-Party Support: MSSP for 24/7 monitoring, penetration testing, and threat intelligence.
- Technology Stack: SIEM, EDR, Zero Trust framework, cloud security tools.

Slide 8: Negotiation Strategy & ROI

- High-Priority Initiatives: Essential for regulatory compliance & breach prevention.
- Flexible Initiatives: Can be phased in if needed based on budget constraints.
- ROI Justification: Avoidance of potential $10M+ in breach-related costs.

Slide 9: Addressing Potential Objections

- "Can we defer investments?" Delaying increases risk exposure and costs more in the long run.
- "What's the ROI?" Preventing even one major breach saves millions.
- "Why so many initiatives?" Each initiative addresses a critical risk, ensuring comprehensive security.

Slide 10: Call to Action & Next Steps

- Approval of Phase 1 Budget: Immediate funding for foundational security upgrades.
- Executive Sponsorship: Support from leadership for cultural and policy changes.
- Implementation Kickoff: Begin Year 1 projects with clear milestones.

Thank You!

Questions?

New Direction for Slides

ZERO TRUST PROJECT

Slide 8: Zero Trust Architecture

Why Zero Trust? Traditional perimeter security is insufficient against modern threats.

Business Impact:

- Prevents unauthorized access & insider threats.
- Reduces attack surface, minimizing breach risks.
- Strengthens compliance with data protection regulations.

Budget & Resource Request:

- Estimated Cost: $1.5M (implementation, tools, training).
- Personnel: IAM Specialists, Security Engineers.
- Technology Stack: Zero Trust Network Access (ZTNA), Multi-Factor Authentication (MFA), Micro-Segmentation, Endpoint Protection.