SCOTT MACLEAN

NOVEMBER 2024

CIBC CYBERSECURITY ENHANCEMENT STRATEGY:

AN EXECUTIVE SUMMARY

TABLE OF CONTENTS

INTRODUCTION

This report presents a cybersecurity enhancement strategy to fortify CIBC's defenses against evolving cyber threats. It aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and incorporates best practices to safeguard employee and customer data, ensuring business continuity and regulatory compliance.

ISSUES

CIBC faces increasing cybersecurity risks including data breaches, phishing scams, and malware infections. These threats can damage our reputation, disrupt operations, and compromise sensitive information. Proactive measures are crucial to address vulnerabilities and maintain stakeholder trust.

RECOMMENDATIONS

This strategy focuses on user education and robust technical controls, guided by NIST principles:

Strong Passwords (NIST SP 800-63B):
Recommendation: Enforce strong, unique passwords across all systems with:
Minimum length of 12 characters.
Complexity requirements (uppercase, lowercase, numbers, symbols).
Regular password audits and proactive password monitoring tools to identify weak or compromised passwords.

Password Expiration Policy (NIST SP 800-63B):
Recommendation: While recent guidance suggests moving away from frequent forced password changes, a balanced approach is crucial. Implement a risk-based approach, considering factors like user roles and data sensitivity, to determine appropriate password expiration intervals.

Multi-Factor Authentication (MFA) (NIST SP 800-63B):
Recommendation: Implement MFA across all critical systems and applications, including email, VPN, and financial systems. Prioritize phishing-resistant authenticators like security keys and biometrics.

Secure Email with Personal Certificates (NIST SP 800-177):
Recommendation: Implement S/MIME encryption with personal certificates for all internal and external email communications involving sensitive data. This ensures confidentiality and integrity, mitigating risks like phishing and email spoofing.

RECOMMENDATIONS

VPN IPSec on Laptops (NIST SP 800-113):
Recommendation: Mandate the use of VPN with IPSec encryption on all company laptops to secure data transmission when employees connect to public Wi-Fi networks or work remotely. Regularly update VPN software and configurations to address vulnerabilities.

Encrypted Hard Drives/Flash Drives (NIST SP 800-111):
Recommendation: Enforce the use of encrypted hard drives and flash drives for all portable devices. This protects sensitive data in case of device loss or theft. Implement a policy for secure disposal of these devices.

BENEFITS

Implementing these measures will:

- Reduce the risk of unauthorized access: Strong authentication and encryption minimize successful cyberattacks.
- Protect sensitive data: Encryption and secure email protocols safeguard confidential information.
- Improve employee awareness: Training programs empower employees to identify and respond to threats.
- Enhance CIBC's reputation: Demonstrating a commitment to cybersecurity builds trust.
- Ensure regulatory compliance: Meet industry standards and regulatory requirements.

IMPLEMENTATION PLAN

A phased approach will ensure effective implementation:

Phase 1: Employee cybersecurity awareness training, strong password policy and MFA implementation for critical systems.

Phase 2: Secure email with personal certificates, VPN IPSec deployment on laptops.

Phase 3: Encrypted hard drive/flash drive policy enforcement, ongoing monitoring and evaluation.

CONCLUSION

This strategy, aligned with NIST controls, is crucial to protect CIBC. By addressing vulnerabilities and fostering a culture of security awareness, we can mitigate risk and ensure business continuity.

NEXT STEPS

- Secure budget approval for security tools and technologies.
- Develop and deliver employee cybersecurity awareness training programs.
- Collaborate with IT teams to implement and enforce security policies.
- Establish a process for ongoing monitoring, evaluation, and improvement.

REFERENCES

- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

- NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final1

- NIST Special Publication 800-63B: Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html

- NIST Special Publication 800-177: Guide to Securing Web Services: https://csrc.nist.gov/publications/detail/sp/800-177/final