The Maine Information Security Policy establishes various standard procedures to ensure the security of assets while referencing the National Institute of Standards and Technology (NIST) as a benchmark for protecting information assets. The categorization of information assets covers a variety of tools, software, and hardware, with different policies and responsibilities assigned to the Chief Information Officer. (Maine State Government, 2024)

The Federal Trade Commission (FTC) has identified various cyber threats experienced by consumers and internet users in the United States, including identity theft, romance scams, e-consumer losses, credit card theft, fraudulent activities, and data breaches. (FTC, 2024)

According to Bardach (2024), smart practices are internally complex, context-sensitive, and capable of being used by different parties to pursue slightly different goals. The Maine Information Security Policy covers different areas of security, establishing security standards for various scenarios. The policy's attempt to solve problems and achieve the goal of securing assets is commendable. However, in terms of addressing the specific cyber threats posted by the FTC, the policy has some limitations. While it covers areas like access control, authorization, background checks, data classification, data exchange, and risk assessment, it does not explicitly address issues such as e-consumer losses, identity theft, and romance scams. Additionally, the policy does not clearly outline how different entities, including public/private organizations, employees, contractors, and consumers, can collaborate to ensure asset security. The policy also lacks specific provisions for users/consumers, who are crucial to security operations.

Furthermore, while the policy has some realistic expectations, its effectiveness in addressing the specific cyber threats identified by the FTC is limited. It is a robust policy but may not be fully context-based, as it does not directly address the core issues raised in the FTC report. While it focuses on general security areas, it lacks specific policies on recovering resources lost to fraud or identity theft, procedures for reporting attack incidents by consumers, and guidelines for educating and empowering users/consumers. (FTC, 2024)

In conclusion, while the Maine Information Security Policy is a solid foundation for securing information assets, it could be further enhanced by addressing the specific cyber threats identified by the FTC. By incorporating more specific guidelines for user education, incident response, and recovery procedures, the policy can become more effective in protecting against emerging cyber threats.

References

Bardach, E., & Patashnik, E. M. (2024). *A practical guide for policy analysis: The eightfold path to more effective problem solving* (7th ed.). CQ Press.

Federal Trade Commission. (n.d.). Start with security: A guide for business. FTC. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

Maine State Government. (2024). Information Security Policy. Department of Administrative & Financial Services, Office of Information Technology. Retrieved from https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityPolicy.pdf