NIST
Cybersecurity Framework Success Story
Government of Bermuda

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.

Benefits Received from Implementing the Framework:

- Alignment of information systems with business security needs across ministries and departments.
- Identification of information gaps and security controls deficiencies to focus on specific areas for improvement.
- Identification of relevant guidance in each area of program development.
- Support of informed governance and management at the department, executive and Cabinet levels.

Situation

- Difficult to consistently manage cybersecurity risk across all Government ministries and departments.
- Information systems environment contained centralized and decentralized components.
- Security requirements were inconsistently established on a system-by-system basis.
- Personal Information Protection Act 2016 established penalties including fines and potential imprisonment if reasonable security measures are not implemented to protect sensitive personal information.

Drivers

- Government's increasing dependence on Information and Communication Technology (ICT) to process sensitive information and provide critical services.
- Cybersecurity seen as an important component to economic resilience for the island.
- Cybersecurity leadership needed for Government and Critical National Infrastructure entities within the jurisdiction.
- Recognition of the need for information systems and security governance was met with the political will to initiate programs.
- High-profile Fintech Initiatives were launched.

"NIST's Cybersecurity Framework has provided us with a comprehensive roadmap to ensure effective cybersecurity practices are implemented across Government."

- Hon. Wayne M. Caines, JP, MP., Minister of National Security

Drivers (Continued)

- The cyberthreat environment intensified.
- Island needed to increase cyber awareness internally and in the wider community.
- Continuous investment was needed by all stakeholders in order to enhance their collective ability to protect their systems and data.

Process

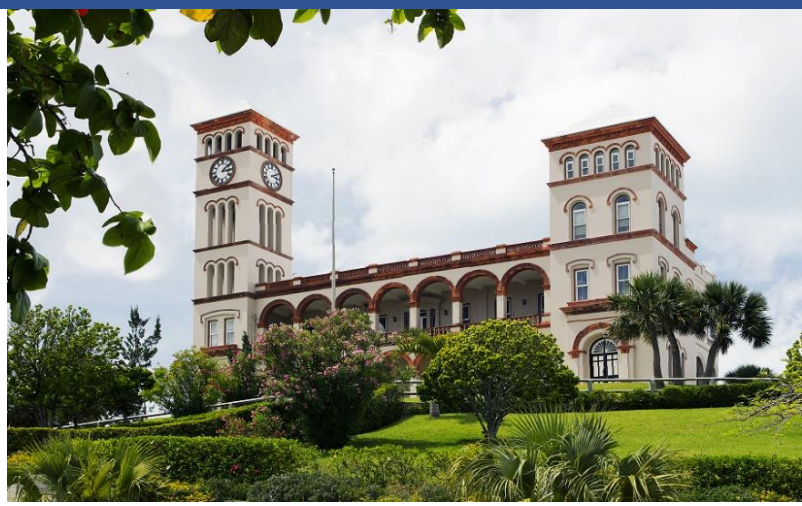
- Cabinet Cybersecurity Committee established to provide oversight of the Information Systems Risk Management Programme development and administration.
- Self-assessment performed using the NIST Cybersecurity Framework to identify gaps in information, control deficiencies and areas of high risk.
- Asset identification, valuation and categorization performed by each department to reduce information gaps identified during the initial self-assessment.
- Control deficiencies and risk ratings identified and used to create prioritized action plan.
- Results of the self-assessment garnered Cabinet support for remediation initiatives.

Process (Continued)

- Informative references used to provide guidance in areas such as policy development and implementation steps.
- Regular reporting of security posture to Cabinet using the Cybersecurity Framework as a dashboard.
- Strategic partnerships with public and private entities were formed to develop the jurisdictional Cybersecurity Strategy.

Results and Impacts

- Consistent standardized approach to address business security across all ministries and departments.
- Addressing complex cybersecurity risks across organization more manageable.
- Security activities more closely aligned with business needs.
- Information System Risk Management Committee established to ensure program, policies and standards were developed in a collaborative manner focused on stakeholder needs.
- Development of policies and processes that enable the risk management program.
- Close integration with records management and privacy policies and processes.
- Implementation of regular training for staff and information security professionals.



What's Next

- Dashboard for system owners and authorizing officials.
- Integration of quantitative methods into the risk assessment processes.
- Closer work with Government's Internal Audit Department.
- Work with the Disaster Risk Reduction and Mitigation Unit on jurisdiction-wide cybersecurity response.
- Enhancement of educational programs to encourage further integration of computer science in curricula and to provide further professional development opportunities for information security professionals.

Contact Information & Resources

Government of Bermuda Website:
https://www.gov.bm/

Bermuda contact: sidaniels@gov.bm

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

NIST contact: cyberframework@nist.gov