MINISTERIAL STATEMENT
By
Minister of National Security,
The Honourable Wayne Caines, JP, MP

Cybersecurity Strategy Update

February 28th, 2020

Mr. Speaker, I rise this morning to update this Honourable House on the new developments being done within Government in regards to I.T and cybersecurity.

As we know **Mr. Speaker,** around the world cyber-attacks continue to impact Governments, multi-national corporations, small organizations and individuals. Major Cybersecurity breaches at organizations such as the retailer **Target** and the credit reporting agency **Equifax** clearly demonstrate the importance of ensuring that IT Management, staff, vendors and contractors are following good security practices. When IT Systems are not securely implemented, operated and maintained it can have a devastating impact on the organization.

Mr. Speaker. The Government of Bermuda is dependent on the IT Systems that support vital services for the public. We must ensure these systems and services are securely implemented, operated and maintained. The Information Systems Risk Management Programme Policy was approved by Cabinet in October 2017 to address this need. The policy requires the development of a comprehensive risk based security programme aligned with industry standards to protect Government information and IT Systems.

Mr. Speaker, the Cyber Risk Management Committee is chaired by Collinwood Anderson, Permanent Secretary for National Security. This committee has developed a comprehensive set of cybersecurity policies and standards to protect the Government and Bermuda from cyber threats. In compliance with these policies the Heads of Government Departments are responsible for ensuring Government IT Systems are in accordance with Government standards and industry leading security practices.

The Cyber Risk Management Committee **Mr. Speaker,** is currently finalizing the Cybersecurity Status Reporting Policy. The policy will require the Chief Information Officer to provide formal quarterly security status reports to the Cabinet Cybersecurity Committee and the Civil Service Executive. Management, staff and IT Service Providers must be required to report the security status of the Government information, systems and processes for which they are responsible to demonstrate compliance with Government policies and leading industry practices. The Cybersecurity Status Reporting Policy will ensure that Cabinet and the Civil Service Executive are provided with the accurate and reliable information they need to maintain executive level oversight of critical IT Systems and processes within Government.

Mr. Speaker, the Bermuda Cybersecurity Strategy was approved by Cabinet and launched in September 2019 to protect Bermuda's cyberspace. The Cybersecurity Governance Board, a public\private partnership has been established and is working to implement the strategy. This includes the development of appropriate legislation to address cybersecurity and cybercrime within the jurisdiction. It also includes raising awareness and capacity building to enhance cybersecurity preparedness, information sharing and collaboration.

At present **Mr. Speaker,** Bermuda has a limited capability to respond to cyber incidents at the national and international levels. A National Cybersecurity Incident Response Team (CSIRT) will provide a centralized capability facilitating communication, coordination and collaboration to more effectively deal with cybersecurity threats impacting the jurisdiction.

The CSIRT will also support threat sharing and threat intelligence, while raising awareness of cyber related risks and an improved understanding of effective safeguards.

Mr. Speaker, in March 2020, the International Telecommunications Union (ITU) will be on island to assist the Cybersecurity Governance Board with assessing Bermuda's readiness to establish a National CSIRT. The ITU is a United Nations Agency that has assisted more than 75 other jurisdictions with performing CSIRT readiness assessments. Collaboration with this leading international agency will prepare Bermuda to implement an effective National Cybersecurity Incident response capability.

In June of last year **Mr. Speaker,** the Ministry of National Security's Permanent Secretary and the Cybersecurity manager travelled to the Dominican Republic to participate in the Regional Conference on policies and strategies on Cybercrime for the Caribbean Community. The conference focused on international cooperation and the establishment of good practices to combat cybercrime at the national and international levels.

Mr. Speaker, as part of the National Cybersecurity Strategy the Cybersecurity Governance Board is working with the Council of Europe to review Bermuda's cybercrime legislation against the Budapest Convention on Cybercrime. The Budapest Convention is the only binding international treaty on cybercrime and electronic evidence. Aligning Bermuda's cybercrime legislation with the articles of the Budapest Convention will empower our investigators, prosecutors and judiciary to more effectively deal with cybercrime within our jurisdiction and facilitate cooperation at the international level.

Mr. Speaker, aligning Bermuda's cybercrime legislation with the Budapest Convention is an important first step. However, this must be followed by capacity building and training for our investigators, prosecutors and judiciary. The Ministry of National Security will work closely with the Council of Europe and these key stakeholders to harden our defenses against cybercrime.

Mr. Speaker, in addition to protecting the Government and other Critical Information Infrastructures against cyber-attacks, the Cybersecurity Governance Board is working to develop a cost-effective cybersecurity and privacy certification programme for small and medium-sized organizations within Bermuda. The scheme will help local organizations assess and improve cybersecurity. Certification will also allow them to demonstrate their commitment to responsible cybersecurity and privacy practices to their customer and business partners.

In December **Mr. Speaker,** I gave the opening address at the second annual International Cyber Risk Management Conference in Bermuda. This conference brought leading cyber risk management experts together from within Bermuda and around the world. The conference highlighted the key role of Bermuda based reinsurers in the evolution of the cyber insurance industry. This high visibility conference was an opportunity to show the world that we take cybersecurity seriously in Bermuda. It is a part of our Government and corporate cultures.

Mr. Speaker, last October, members of the Cybersecurity Governance Board led a series of public presentations on cybersecurity. These presentations covered a diverse range of topics that included how individuals and organizations can protect themselves from threats such as Ransomware. They also covered corporate board level security considerations including the necessity for good Governance practices to ensure cybersecurity risks are effectively managed within the enterprise.

Mr. Speaker. Cybercrime and cybersecurity issues continue to threaten individuals, the Government and Bermuda. They threaten our privacy, our financial success and our reputation. We must continue to drive the implementation of the Bermuda National Cyber Security Strategy and the internal Government security program. We must also continue to promote awareness and build our capacity to protect our jurisdiction against cyber threats.

Thank you, **Mr. Speaker.**