Government of Bermuda
Ministry of National Security

Ministerial Statement to the House of Assembly
By
The Hon. Wayne M. Caines, JP, MP
Minister of National Security

Cybersecurity Concerns Us All

Date: 22nd September 2017

Mr. Speaker,

Honourable Members will recall that in this year's Speech from the Throne, the Government determined cybersecurity as a national priority. The Ministry of National Security has been tasked with ensuring that our digital infrastructure is properly protected, and the risks facing it properly mitigated.

Mr. Speaker,

Cybersecurity is not limited to information technologies (IT) or to the business world. This issue concerns us all. Indeed, every person on this Island who has access to and uses the Internet has become keenly

aware of the risks they face when going online – whether at work, at school or at home.

Mr. Speaker,

Bermuda works very hard to uphold its reputation as a trusted, blue chip jurisdiction; any risk facing our Island, even reputational risk, could prove detrimental to our quality of life. One way to be better equipped to face these risks is to educate ourselves and increase our resilience as individuals, because we are the first line of defence when it comes to cybersecurity. One person clicking on the wrong link or responding to the wrong email can –and has– shut down not only businesses of all sizes locally and internationally, but also entire government services and more.

Mr. Speaker,

A very real example of the risk and the impact occurred on 12th May this year. A ransomware script called WannaCry infected networks around the world, devastating hundreds of thousands of targets. In the UK's NHS –the National Health Service– the attack spread to diagnostic equipment and forced hospitals to divert emergencies. Only through sheer luck did an information security researcher find a way to quickly disable the malware responsible.

Mr. Speaker,

Without strong cybersecurity awareness and preparedness, our personal and financial safety, economic prosperity, and national security is at risk.

It is therefore my view that we – and by "we" I mean those of us in the Government as well as those in the private and third sectors – share a responsibility to ensure that we are well-prepared to identify and manage cybersecurity risks, wherever they are and whenever they appear. As part of this effort, we need to adopt, and teach our children to adopt, cyber-safe behaviors at home and at school.

At the organizational level, one of the most effective ways to achieve cybersecurity preparedness is to adopt a cybersecurity framework, and that was the focus of the Cybersecurity Framework Workshops which were held at the BUEI on Wednesday of this week.

Over one hundred individuals benefitted from the expertise and experience of local and international experts in the field, and the Bermuda Government has engaged in cybersecurity work of its own. The Cybersecurity Cabinet Committee, under my chairmanship, is working to address and attempt to mitigate cybersecurity risks to the Bermuda Government. To consistently evaluate and update our cybersecurity measures, we have adopted the National Institute of

Standards and Technology's Cybersecurity Framework. The NIST Framework has much to offer, and it is well worth considering as a starting point for achieving cybersecurity preparedness.

Mr. Speaker,

The road to cybersecurity preparedness requires a multi-stakeholder approach, and we are not going it alone. The Cybersecurity Working Group, which is comprised of private and public sector IT and security professionals, is –as we speak– auditing the cybersecurity preparedness landscape of Bermuda. This Group has assembled the best IT professionals on island led by Mr. Ronnie Viera. The Government is committed to ensuring the Working Group has all necessary resources to complete its important task.

Mr. Speaker,

In Bermuda, we have developed a vibrant digital society that relies on our critical national infrastructure and commercial business, both local and international, for continued prosperity. Our reputation as one of the world's most sought after jurisdictions for international business rests on the proven assumption that doing business here is safe and secure.

Moreover, our national security depends on the uninterrupted functioning of our hospital, banks, and energy grid. One lethal

cyberattack, however, can change the picture entirely, regardless of whether the target is a provider of a public good or a private company. This means that cybersecurity must be addressed collectively by the full range of affected stakeholders, including government, industry, schools, and charities. And that is why the conversations we started this week must continue.

***Thank you, Mr. Speaker*.**