FINANCIAL INDUSTRY CYBERSECURITY COUNCIL LAUNCH

Moving towards a cyber secure financial industry

It is intended that the Council serve as an effective platform through which the banking and non-bank financial sectors can facilitate discussion and formulate operational approaches, either collectively or individually, for participants to combat cyber fraud.

Bank of Namibia

WHAT IS A CYBERSECURITY FORUM/COUNCIL?

Cyber risk poses a system-wide risk because of the macro-vulnerabilities present in the financial sector. These vulnerabilities arise from technological dependencies, interconnectedness and mutual dependencies, dependencies on Technical Service Providers, disruption of critical functions and the threat of a simultaneous attack.

The forum aims to create a common approach, improve maturity levels, improve risk management tools, initiate cybersecurity efforts and share intelligence for addressing cyber security within the sector.

WHY IS THERE A NEED FOR A CYBERSECURITY COUNCIL IN NAMIBIA?

The Council is envisaged to be an effective platform through which the bank and non-bank financial sector can facilitate discussion and be able to formulate operative approaches, either collectively or separately for participants to combat cyber fraud by 1) working together to roll out a cyber strategy for the Namibian financial sector; 2) sharing best practices on cyber risk management, and 3) information sharing regarding cybersecurity threats, vulnerabilities, and incidents.

WHO SHOULD FORM PART OF THE CYBERSECURITY COUNCIL?

The Council comprises of cyber and information security specialists from financial sector regulatory bodies, other regulators, critical financial market infrastructures (FMI), financial sector associations, commercial banks, and other non-bank financial institutions.

MOVING TOWARDS A CYBER SECURE FINANCIAL INDUSTRY

As the reliance of the financial sector on Information Technology and the interconnectedness of systems continue to rise, cybersecurity has become a financial stability risk. There are three transmission channels as a result of cyber risk that can lead to instability in the financial system, loss of confidence, lack of substitutability, and interconnectedness. Financial industry experts need to understand the nature of the risk, learn the essential concepts of cyber risk management, and acquire basic skills needed for effective monitoring and management of cyber risk. As we strive to be a more cyber-secure financial industry, we trust that the information provided herein will go a long way towards fostering an understanding of cyber risk management.

Cyber risk and cyber risk management

- Cyber-risk in the financial context refers to the operational risks that may result aavailability of data or information; and risk that can negatively impact the information technology (IT) infrastructure or business operations.
- Cyber-risk management is the process of identifying, analysing, evaluating and addressing the institution's cyber security threats.

Information Sharing & Threat Intelligence

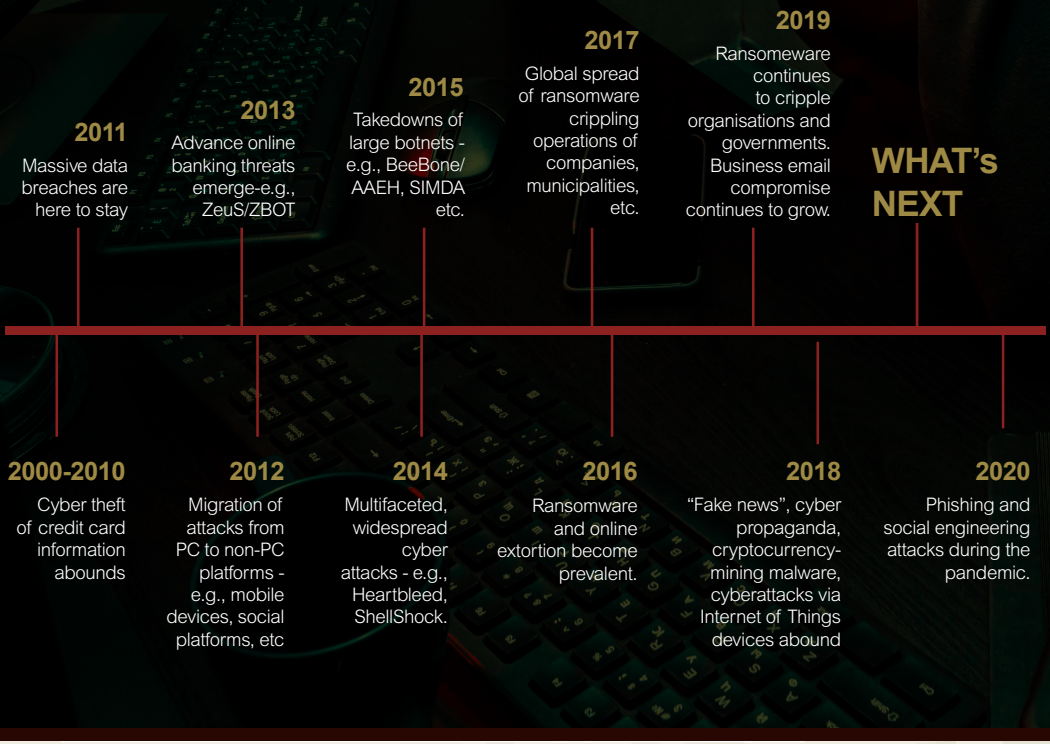
- Cyber information sharing and threat intelligence involves the exchange of knowledge about threats, incidents, vulnerabilities, mitigations, leading practices, or tools relevant to a technology-based or technology-leverages risk set.
- The core objectives of this is to protect the financial system by preventing, detecting and responding to cyberattacks; to facilitate the sharing of information, intelligence and good practices between financial infrastructures; and to raise awareness of cybersecurity threats.
- Information is the lifeblood of risk mitigation and is the basis for risk management. Pooling of information can enhance situational awareness, help detect new risks, and build better responses.

How is Cyber a financial Stability Risk?

- Cyber risk poses a system-wide risk because of the macro-vulnerabilities present in the financial sector. These vulnerabilities arise from technological dependencies, interconnectedness and mutual dependencies, dependencies on Technical Service Providers, disruption of critical functions and the threat of a simultaneous attack.
- Therefore, it is important to have a view, monitor and manage information on the concentrations of technology, service providers, system integrators, cloud service providers, payment systems, etc.
- Threat information sharing therefore, comes in handy, in preventing system-wide compromise of data and information systems.

HOW HAS CYBER SECURITY CHANGED IN THE LAST DECADE?

Cyber Threats are many, varied, and always evolving. Below is how cyber threats have evolved over the last two-decades:



CONTACT US

For more information, contact
+264 61 283 5111 | info@bon.com.na

www.bon.com.na