Critical national infrastructures under cyber attack

Guest Column

By Edward Millington

During the last 12 months, Critical Infrastructure (CI) or Critical National Infrastructure (CNI) around the world (and just recently, the Port of Nagoya, the largest and busiest port in Japan and the Office of the Attorney General and Ministry of Legal Affairs (AGLA), Trinidad and Tobago) have suffered critical cyber-attacks by cyber-criminals, causing operational services issues, data losses and data breaches – all of which affect the confidentiality, integrity, and availability of systems and services. Communicating it differently, the trust in such systems, services, and operations is affected for unknown periods, while incident management activities and processes are comprehensively undertaken to provide trust verification and certification. Services to the public and to other entities, are often impacted.

CI can be classified as systems, operations, and or services that are essential to society as a whole and the economic development of a country, and if compromised, they create dire consequences for the society and the economy as a whole. Healthcare and public hospitals, transportation, education, electricity generation, water authorities, Government facilities, attorneys general offices, law enforcement, etc. are all CIs.

Protecting CI requires governments and non-governmental entities – to collaborate and work together to understand the risks beyond general risks such as floods, electrical outages (all can be due to a cyber-attack), earthquakes, etc, and include cyber risks in the main risk management programme. When such a programme does not take cyber risk management into its overall risk management plan, cyber-attacks (which can occur literally at any moment) can take advantage of the governing risk management programme's vulnerable nature, thereby hampering the resilience of CI. You may ask how this can be. The maturity of the programme affects the efficiency and effectiveness of instituted controls in managing risks, especially cyber-risks. It is therefore important that CI operators consider all risks in developing resilience programmes, especially cyber-resilience schemes to survive such cyber-attacks.

On another note, disruption of CI can be considered a national security Issue. Therefore, it is very crucial to understand cyber risks and establish the necessary and crucial security controls to build resilience. These cyber resilience controls are critical to the offensive and defensive nature of the programme to prevent and or reduce the effects of a cyber-attack on all systems, operations, and services. In fact, cyber-attacks on CI can sometimes affect public safety and economic viability.

For controlling entities to achieve the resilience required, the following will be needed:

Public awareness of digital risks and the importance of cybersecurity in the connected world

Political commitment with actionable attributes in formalising committees and workshops to effectively and efficiently study the risks cyber posed to CI – a comprehensive cybersecurity risk assessment

The creation of national security-aware policies, regulations, laws and guidelines in designing, planning, implementing, managing, monitoring, and reviewing CI resilience.

Building highly capable cyber-resilience programmes into IT and OT (operational technology) infrastructures.

Competent human resources in the management and operations of CI

Appointing cybersecurity advisors/consultants to boards or senior executive structures for cybersecurity advisory or cybersecurity awareness, aiding in business policies, strategies, and goals development.

Cyber-criminals' targeted objectives are solely financial with no regard to governing, social, cultural, and economic impacts and understanding this grave criminal mindset should help CI operators, governments, and non-governmental organisations to take this risk seriously and act quickly before it can cause harm and, in some cases, cause harm again.

Edward MILLINGTON, (CISSP, ISSA, MCIIS, MIET, PAN-ACE) is the Founder and Managing Director of CariSec Global Inc., a Caribbean (Barbados) based company and a Lead Security Consultant, strategically focused on providing Security & ICT Governance and Services to organisations operating in the following sectors: financial, government, health, manufacturing, private, retail, and energy and utilities. He is an Information Systems Security/ ICT/Telecommunications veteran of two decades.