aliv business

CYBER SECURITY SUMMIT 2026

CYBER RESILIENCE
DEFENDING THE DIGITAL FRONTIER
EMPOWER, PROTECT, EVOLVE

When Critical Infrastructure Becomes a Target

Lessons from the Queen Elizabeth Hospital Cyber Incident

EDWARD MILLINGTON
Managing Director, CariSec Global Inc.
Founder & Chairman of Caribbean Chartered Institute of Cyber and Information Security

CARISEC GLOBAL
CyCIS

Critical Infrastructure Under Threat

- **Attacks on CI exceeds 21% globally** (PRiSM Data-Leaking Ransomware Report 2025)
- **The Healthcare sector faces significant risks,** ranking just below the financial sector (PRiSM Data-Leaking Ransomware Report 2025)
- **13% of Latin America and the Caribbean region** have a high degree of confidence in their country's ability to protect CI (WEF Global Cybersecurity Outlook 2026)
- **23% of public-sector organisations** report having insufficient cyber resilience capabilities (WEF Global Cybersecurity Outlook 2026)
- **Geopolitical tensions** are contributing to vulnerabilities in CI (WEF Global Cybersecurity Outlook 2026)

Data-Leaking Ransomware

2025 (January 2025-December 2025)

Global Victims Summary

Data Breaches Digest

#	Flag	Country / Island	Victims
1		United States	4062
2		Canada	429
3		Germany	296
4		United Kingdom	261
5		Italy	182
6		France	175
7		Spain	166
8		Brazil	146
9		India	143
10		Australia	125

#	Flag	Industry Type / Sector	Victims %
1		Manufacturing	15.94%
2		Construction & Civil Engineering	9.51%
3		IT Services, Software & Communications	9.36%
4		Finance	7.06%
5		Healthcare	5.84%
6		Retail	5.37%
7		Legal	4.86%
8		Food & Beverages	3.95%
9		Education	3.78%
10		Logistics, Transport & Storage	3.70%

#	Flag	Ransomware Operator	Victims
1		Qilin	1158
2		Akira	721
3		CL0P	498
4		PLAY	392
5		SAFEPAY	379
6		INC Ransom	373
7		Lynx	260
8		RansomHub	236
9		DragonForce	224
10		Sinobi	194

Executive Summary

The **Queen Elizabeth Hospital** is the main public healthcare facility and the critical national referral hub for Barbados's healthcare system, providing acute, secondary, tertiary, and emergency care.

- **Incident Overview**: On December 12, 2022, the QEH experienced a major cyber attack that disrupted internet connectivity and essential services.
- **Key Impact**: Hospital systems were taken offline, necessitating a return to manual operations and causing delays to non-emergency services.
- **Response Approach**: A phased and long recovery led by local and international experts, with a focus on security before full restoration.
- **Core Lesson**: This incident highlights the weaknesses in healthcare infrastructure and emphasises the necessity for proactive cybersecurity governance and resilience planning.

Incident Timeline & Response

Dec 7-8, 2022
CariSec Global warns the Government of Barbados about cyber risks to healthcare, based on threat intelligence.

Dec 12, 2022
Cyber attack detected, systems encrypted.
Systems taken offline

Dec 13, 2022
Public Announcement
Investigation launch with MIST and Cybersecurity Experts.

Dec 14-31, 2022
Manual Operations initiated
System cleaning and assessment underway.

Jan 1-13, 2023
Phased reconnection plan announced.
Priority departments identified

Jan 14-18, 2023
Limited internet restored priority departments - Medial Records, Laboratory, Radiology, etc.

Jan 19+, 2023
Full Restoration ????

Operational and Clinical Impact

Service Disruptions

- **Clinical Delays:** Radiology were limited to emergency tests; CT Scans, X-rays and ultrasounds were postponed.
- **Administrative Challenges**
  - Medical records could not issue appointment dates; manual logging was implemented.
  - Pharmacy medication deliveries were suspended; patients were required to visit in person.
- **Staff Adaptation:** A Reversion to paper-based systems, decreasing efficiencies, increasing workloads and potential errors.

Patient Care Continuity

- **Emergency Services:** A&E, ambulance services and blood collection remained operational.
- **Outpatient Services:** Significant delays in Clinics operation, in addition to patients requiring physical documents for efficient processing.

Cybersecurity & Data Concerns

- Inadequate monitoring and logging systems to alert and record security incidents.
- Many systems and software solutions were outdated
- Inadequate security configurations
- Security best practices (e.g., Defence-in-Depth) were not applied.
- Data risk management solutions were not implemented to assess potential data losses and or data integrity issues.
- Incident Response Planning lacks maturity and capabilities
- Overall, no mature Cyber, Information and Privacy Programs were adopted to protect an evolving Digital Transformed Health System.

Lessons Learnt

As industries and sectors undergo digital transformation, effective Cyber Risk Management (CRM) becomes vital for protecting Critical National Infrastructures (CNIs). This creates a safe, secure, highly available, and private ecosystem that promotes **Digital Trust and Operational Resilience** well-being for all stakeholders.

Through CRM, Cyber Resilience can be achieved, creating Digital Excellence!

Recommendations

Institute of Management Systems with good Governance.

- ❑ Implement an Information Security Management System (ISMS) based on ISO 27001.
- ❑ Implement a Privacy Information Management System (PIMS) based on the ISO 27701.
- ❑ Implement a Cybersecurity Management System (CSMS) based on the ISA/IEC 62443 to address OT Security of medical equipment and facilities.
- ❑ Implement an AI Management System (AIMS) based on the ISO 42001 for the development, deployment and utilisation of trustworthy AI Systems.

Closing

The **Queen Elizabeth Hospital** serves as a devastating reminder of how vital cybersecurity and cyber risk management are to the resilience of critical national infrastructures.

- The need for cyber resilience sectoral frameworks to build measurable and effective resilience is vitally needed to protect our digital economies, sovereignty, and national security.
- Finally, to achieve true resilience, good leadership and governance are needed both within the private and public sectors.
- Therefore, the importance of private-public partnerships is crucial.

Thank you