Why Businesses Continue To Fail Cyber Security!

by Edward MILLINGTON

Global media headlines continue to demonstrate the Global Cyber War many businesses are confronting in the digital world, where Cyber Attacks from Advanced Persistent Threats (APT's), Phishing Emails, Ransomware, Malware, Exploitation of Vulnerabilities, etc., makes it difficult in having the possibility of winning such war - unachievable, unbelievable and financially prohibiting. Adversaries always seem to be one or more steps ahead, possibly demoralizing Boards and their management infrastructures, inflicting organisational risk - strategic risk, reputational risk, operational risk, transactional risk, and compliance risk.

Adherence to data protection laws, regulations, policies, standards, and nation-state directives should therefore be driving IT and Information Security Governance programs maturity capabilities levels higher, but the continuing loss of data and information (affecting the CIA), including the availability, integrity, and safety of systems through incidents, compromises, and breaches; demonstrates that such governance programs are not being managed and operated well within their lifecycles, which reflects severely at the C-Level - who ultimately holds the full responsibility of the organization.

"For an organization to manage its cyber-risk - cyber threats and attacks, nation-states attacks, including insider cyber-criminal activities, it is essential that its existing Information Security Governance Program must be continually evaluated, monitored, and updated for its effectiveness and efficiencies."

The Information Security Governance Program must be RISK-BASED, where all risk management processes and functions that govern the development and implementation of Security Controls (whether administratively, technically, and or physically) are instituted appropriately - reducing organizational risk and attack surfaces. For the program to be effective, IT Risk Management must also be integrated into the organization's risk management framework, thereby allowing risks to be managed and operated upon by the Enterprise Risk Management System.

The following are possible reasons why cyber-affected businesses' Information Security Program fails in protecting them.

1. The risk management activities were not thoroughly carried out in the development of the program, resulting in ineffective, inefficient, and insufficient policy-based security controls.
2. Outdated Security Controls in reducing risks associated with the cyber-defense against adversaries Tactics, Techniques, and Procedures (TTP)
3. Inadequately directing security engineering designs
4. Incorrectly advising on the procurement of security solutions
5. Institute minimum critical monitoring controls that would provide the visibility and awareness needed, where data collected is analysed using Machine Learning, AI, and other techniques to evaluate and highlight potential risks (including safety risks), attacks, compromises, and breaches.
6. Inability to identify, protect, detect, respond and or recover from cyber threats in all areas of the business due to immature and or non-compliant security policies.

While a cyber-attack will occur, the business priority is to make sure that attack surfaces are small and the dwell time (time taken to detect an incident) is in seconds to minutes and not hours, thereby raising the Incident Response Maturity level to the highest.

"An Information Security Governance Program is a guiding document that strategically aligns the organization, its people, process, and technology to the organization's vision, goals and objectives; through security frameworks, policies, standards, procedures, and guidelines in securing business assets."

While any business information security governance program should contain risk management activities, there is a strong possibility that those activities may not be mature enough or have stopped working, especially if the business is not compliant or does not need to be in complaint to existing standards, laws or regulations. The risk assessments needed to identify threats, vulnerabilities, assets value and the probability and impact of threats occurrence may not be carried out efficiently and accurately, in the determination of the true risk to the asset(s) for risk treatment. The end result of ineffective risk management processes can lead to ineffective, inefficient, and insufficient security controls, thereby expanding the organization's attack surfaces to be compromised and breached; exposing assets on a greater scale for exfiltration, unauthorized access and changes, damages, and or unauthorized control. In addition, the Risk Register that is used to track identified risks does not reflect risks in its entirety and risk level. In essence, the risk management life-cycle that is needed to keep risk to an acceptable level is nonfunctional.

Not understanding the true risk to assets for risk treatment, the implementation of Security Controls like 1) Antivirus 2) Firewall(s) 3) Configuration & Change Management 4) Identity and Access Management 5) Logging & Auditing 6) Security Methodologies, etc. may not be appropriate in the identification, protection, detection, response, and recovery from an incident(s) - can allow a cyber-attacker into the organization affecting its operational risk – as mentioned earlier at the beginning of this article.

The Information Security Governance Program in operation also implements an Information Security Incident Management Program - in the management of security incidents. The maturity of this program demonstrates how capable the business' Security Incident Response Plan functions and operates in the handling of a security incident, throughout its lifecycle phases.

A good design Incident Response Plan implies that the incident response to an attacker can be swiftly managed, reducing the dwell-time and attack surfaces coverage. For the incident response to be efficient and effective, the incident response plans much have the following:

1. Resources with the correct skills and tools
2. Assigned personnel with roles
3. Playbooks
4. Testing plans
5. Detection, eradication, and recovery tools
6. Effective communication between all parties and resources

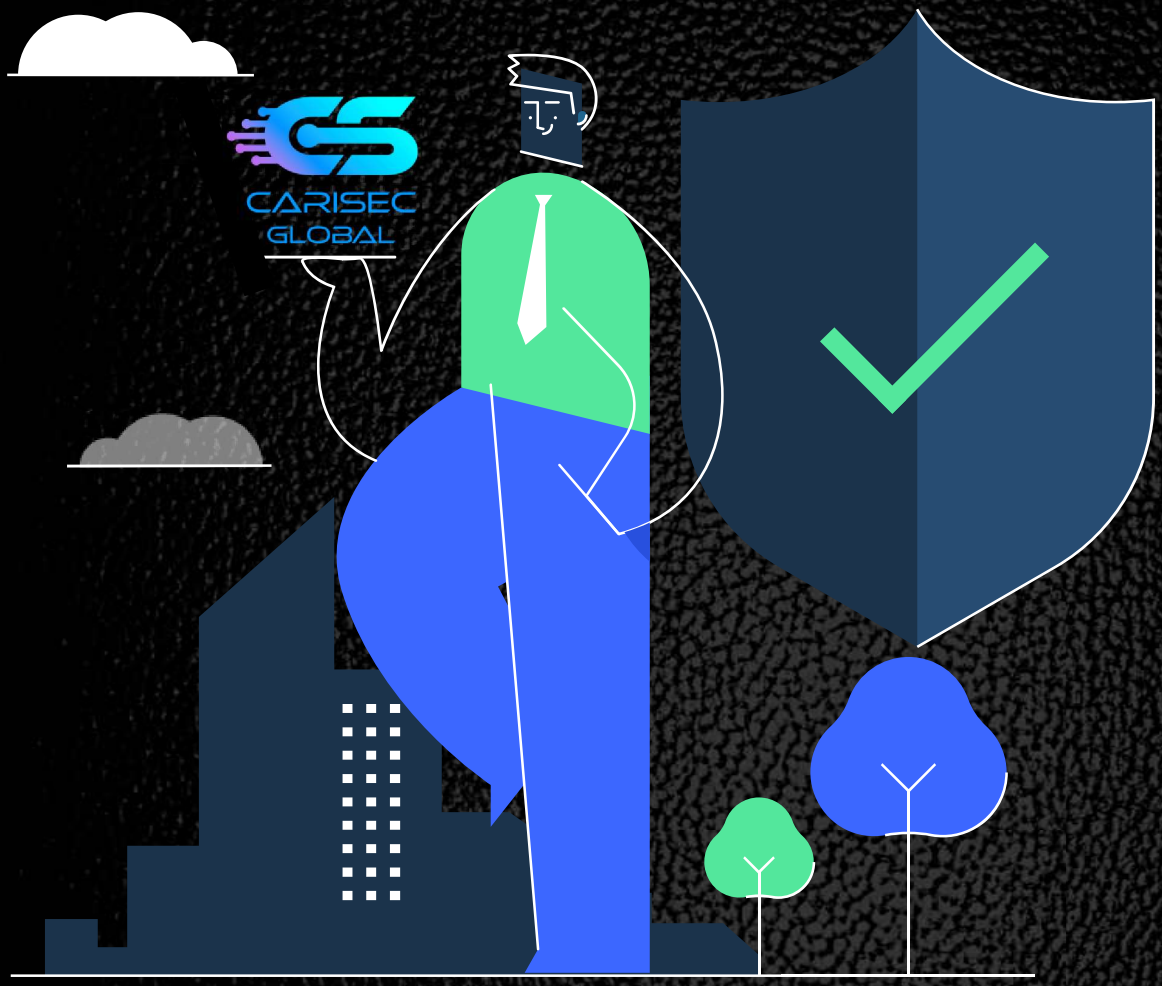
The failure to respond to a security incident accurately and timely can occur by not appreciating the business impact and critical analysis performed in the realization of a threat to the business – again through risk management activities.

In many instances, the inability to identify, detect, protect, respond, and recover can also imply the inadequacies of the plan, where Threat Intelligence usage may be limited and network visibility is lacking due to insignificant data gathering throughout all aspects of the organization, inefficient threat hunting tools, and unskilled resource teams.

The capability maturity model of the Information Security Governance Program is critical in the operation and defense against an attack and it is therefore very important that the organization keep it alive as new risks arise.

CariSec Global

Your Partner For Cyber Security



CariSec Global Creates Partnerships in the Development of Organizations Information Security and ICT Programs.

https://carisec.global

Edward MILLINGTON, Barbados

Edward MILLINGTON, (BSc, CISSP, ISSA, MCIIS, MIET, PAN-ACE) is the Founder and Managing Director of CariSec Global Inc., a Caribbean (Barbados) based company, strategically focused in 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 21yrs, where he directed organisations, leading them in the achievement of further financial goals through strategic planning, designing, and solutions direction. His specialties are in Policy Development, IT & Security Governance, Information & Cyber Security, Risk Management, Enterprise Defense & Security, Cybersecurity Incident Management, Malware & Attack Technologies and Security Operations. His complex skills, knowledge and experience assisted many organisations such as Internet Services Providers, ICT Service Providers, Telcos, Banking, Government, and Governmental Organisations in their development and services evolution. One key highlight of his veteran career was his instrumental service to the Government of Barbados, developing and enhancing its Information and Cyber Security Posture.

As a Cybersecurity Awareness Advocate, he has been advocating for True XDR and Zero-trust implementations to organisations since 2018, encouraging them to continue the advancement and development in Security Engineering, thereby enhancing Defense & Security in the identification, detection, protection, responding and recovery from Cyber threats and attacks, and Malicious Insider Activities and in 2021, as an active member and promoter of the Chartered Institute of Information Security (CIISec), led international Masterclasses with Palo Alto Networks on such subject matters. He is also heavily in the promotion of Information Security Governance to organisations with a focus in Governance, Risk & Compliance (GRC).