6 Steps to maturing the Organisation's Cyber Security & Defense

Cyberattacks carried out by cybercriminals continue to rise at an alarming rate globally, affecting all business sectors and as highlighted in the World Economic Forum: The Global Risks Report 2022, have increased tremendously in 2020 to over 350% from Malware and over 435% from ransomware to the previous year. Fast forward to 2022, we are still seeing such attacks increasing by over 24% per quarter per year. This rate of increase demonstrates that organisations are not fully cyber prepared and ready, where a third of them suffers operational risk losses once per week and in some cases, some experience them more than once a day – as communicated by Help Net Security: Organizations Experience Ransomware Attack.

While the outlook does seem pretty bleak, it really isn't and requires a comprehensive review of the organisation's Cybersecurity Program, developing and enhancing a number of strategies, thereby maturing and improving the capabilities of the program.

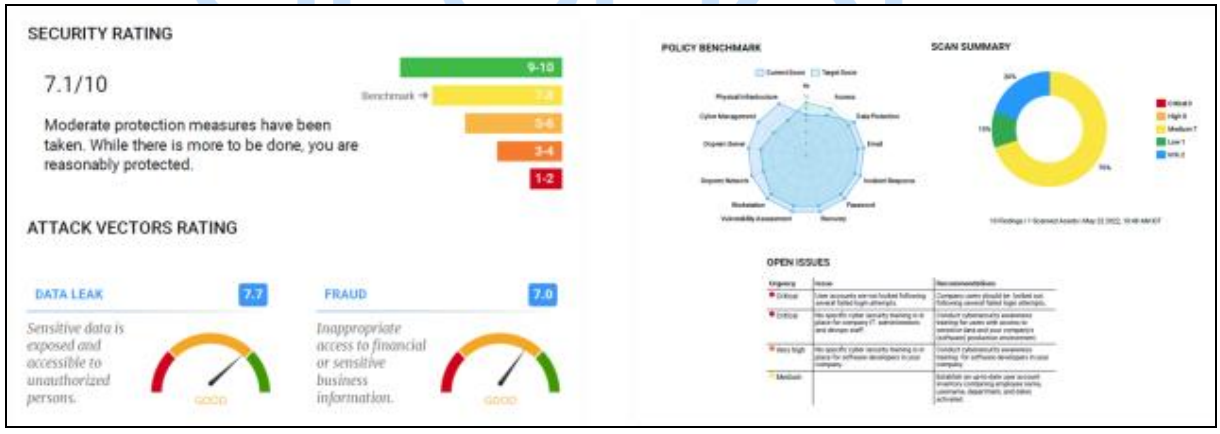
The strategies are as follows in alignment:

1. Seek consultations from Cybersecurity Expert Consultant or a Consulting Business

   Through consulting partnerships, organisations can attain expert information security consultation to critical security needs, issues, and well-being, thereby assisting them along security strategic paths.

   Organisations utilising **CariSec Global's **Consulting & Professional Service**, work very closely with experts in developing and implementing security strategies and achieving security goals as program requirements are defined, refined, and supported by executives.*

2. Undertake an Integrated AI-Driven Cybersecurity & IT Risk Assessments and Compliance Managed Security Service (MSS) to gain an understanding of where security gaps exist and the prioritisation of risks for risk treatment.



The MSS provides the organisation with the following:

- Understanding the effects of a Cyber Impact with Threat Intelligences input
- Complete visibility into the Cybersecurity Posture, Compliance status and Risk Level.
- Continuous assessment demonstrating the efficiency and effectiveness of the organisation's Cybersecurity Program and its capability and maturity in reducing Cyber-risks to the business – all visible through a dashboard.
- Guided remediation plans
- Maintain Compliance through automated readiness assessments for actionable prioritised plans in the maintenance and progression in achieving compliance.

Organisations utilising **CariSec Global's **Consulting & Professional Service** will have a true understanding of their risks and compliance status in reference to the NIST Cybersecurity Framework and or ISO and or CMMC, etc., including the ability to improve their posture and compliance over time through visual representations and reports.*

3. Initiate an organisation-wide Security Awareness Training (SAT) program

   The application of SAT at all levels of the organisation not only improves the security culture but creates a culture of security at all levels of the organisation, its people, process, technology, and service.

   Organisations can gain an upper hand in building and certifying security cultures while creating a culture of security throughout every domain of the organisation utilising **CariSec Global SAT service.*

4. Application of a range of Managed Security Services (MSS)

   To bring capabilities and maturity to the Cybersecurity Program involves the development of Security Policies driving Risk-based Security Controls (resulting from the risk assessments carried out in point 2), affecting all domains of the NIST CSF/CIS Controls/CMMC. There are instances where such services can operate asynchronously to other services previously mentioned, but all centrally project managed.

   ****CariSec Global's portfolio of services** in tandem to its global strategic partners (Trustwave, Converge, etc.) will intimately guide organisations in acquiring the abilities in building and implementing an efficient and effective risk-based cybersecurity Program with Threat Intelligence - providing the capability and maturity in reducing cyber risks, reducing attack surfaces and responding to cyber incidents.*

5. Managed Security Testing

   Security testing allows an organisation to understand its vulnerable points and how those points can be exploited, causing operational risks. In addition, it allows an organisation to prepare for attacks through simulated attacks training, supporting Security Operations and Security Engineering.

   ***CariSec Global's** Red Team Services (RTS) enabled by our leading Global Security Strategic Partner: Trustwave, provides organisations a comprehensive visualisation of the threat landscape (literally) and how vulnerable it is, its people, process, technology and service to cyber criminals and through real-time threat intelligence data from it SpiderLab Team, provide detail recommendations in the risk management of Cyber Risks. This service also initiates a ranged of other orchestrated services to fulfil it recommendations.*

6. Integrate Cyber Advisory into Executives roundtable discussions and strategic designations.

   Attaining Cyber-Advisory Services suggests advanced and strategic cyber-knowledge transfer to Executives and the Board, improving (should be the outcome) the organisation's cyber culture, functions, and processes for further and continued development at all levels of the organisation, as the executive-approved security strategy is operated and maintained.

   ***CariSec Global's** Consulting & Professional Service provides a range of advisory services to all key stakeholders of the organisation, meeting organisation strategic needs in protecting its assets and clients, while being very market competitive.*

Organisations following the strategies above can be sure to bolster their **Cybersecurity Program** to effectively and efficiently secure and protect its asset while being compliant with standards, laws, and regulations, especially meeting data protection and privacy requirements; as they defend against cyberattacks - carried out by cybercriminals.

For further information or consultation, please contact info@carisec.global or visit www.carisec.global

---------- End ----------