Payments Network Malaysia Sdn Bhd (836743-D)

Job Description	
Position	Chief Information Security Officer (CISO)
Department	CISO Office
Division	Risk and Compliance

Summary of responsibilities

1. Drive the implementation of PayNet's cyber security strategy (to achieve and maintain a security capability that is consistent with PayNet's peers) and related cyber security requirements across the Industry
2. Proactively lead PayNet in advancing PayNet's cyber security posture, explore and recommend the latest available technologies on cyber resilience, regularly report on cyber security performance, progress of controls implementation, and levels of cyber resilience automation
3. Guide and organise PayNet's security efforts, expenditure and capital investment for implementation for the Cyber Resilience Framework (CRF) and perform appropriate financial budgeting for security to achieve PayNet's cyber resilience vision and desired security posture

Key Requirements

1. Deep understanding of cyber security covering both internal PayNet and external Payments eco-system. Ability to appraise senior management and Board on cyber security related matters
2. Accountable for all security related reporting to the senior management, Group Audit & Risk Committee and the Board. Provides strong cyber security voice at senior management level
3. Represent PayNet when dealing with external parties such as national cyber risk agencies, customers, partners, Participants, service providers, the general public on cyber resiliency

Key Areas of Responsibilities

1. Implement PayNet's cyber security strategy and framework, explore and recommend the latest available technologies on cyber resilience**,** advance PayNet's cyber security posture proactively, regularly report on cyber security performance and perform financial budgeting for security to achieve PayNet's cyber resilience vision and desired security posture
2. Represent PayNet when dealing with external parties such as law enforcement agencies, customers, partners, Participants, service providers, the general public on cyber resilience related matters
3. Increase PayNet's cross functional capability to manage security
4. Establish and embed cultural and behavioural goals in the cyber security strategy
5. Review and update remuneration structures to ensure sufficient emphasis is placed on cyber security to adequately support the goal to achieve the cyber security strategy
6. Develop a cyber security threat model / landscape to help guide use-case tuning, security reporting and incident response
7. Establish automated patch management reporting to security management and review the thresholds to reflect the changes in cyber threat landscape.
8. Ensure crisis communication media training, inclusive of press conferences and media interviews, is adequately conducted for senior management and relevant stakeholders
9. Establish a comprehensive suite of incident response processes, reporting templates and rules to formalise ecosystem messaging in response to cyber incidents
10. Conduct comprehensive review and establish actions on how Governance Risk and Compliance (GRC), User and Entity Behaviour Analytics (UEBA), Network Analytics and an integrated asset inventory, can

improve the effectiveness of cyber response activities

11. Conduct comprehensive review and improve the value and coverage of security reporting. This includes:
    - Thresholds for security operations alerts and triggered escalation
    - Reporting of security related matters to senior management (set format, content, risk acceptance and archiving requirements) taking into account operational and strategic reporting needs
    - Reporting requirements surrounding Cyber Threat Intelligence (CTI), managed security services and technology vendors, security training and culture, vulnerability and patch management
    - Reporting requirements for Red Team security, data privacy, network analytics, cyber analytics, cyber war game and ecosystem cyber risk (information exchange and incident response)
    - Security Operations Centre (SOC) Graphical User Interface (GUI) to ensure actionable content is displayed and can be extracted to support reporting
    - Ensure risk treatment plan progress is monitored and visualised in the SOC

Qualifications

Minimum Qualifications

1. Degree in Information Technology (IT), Computer Science or other related discipline with relevant experience in managing cyber risk in financial market infrastructures, critical national infrastructure, military, security intelligence or equivalent
2. Cyber security expert with 7 to 10 years or more hands-on experience or more than 15 to 20 years relevant experience in the capacity of Chief Information Officer (CIO), Head of IT Risk, Head of IT audit or Head of IT Security
3. Professional certification such as CISM, CISA, CSXP, CISSP, CREST, GPEN or equivalent
4. Hands-on working experience on best practice standards for cyber resilience such as FMI Cyber Resilience Guidelines, BNM GPIS, MAS Technology Risk Management Guidelines, ISO27001, National Institute of Standards and Technology (NIST), Centre for Internet Security (CIS) or equivalent
5. Thorough understanding of end-to-end IT operations and how IT interfaces with business, risk management and compliance processes and IT Security
6. Able to work under broad direction and a self-motivated individual who is able to work independently. Responsible and accountable for work performed and decisions taken
7. Must possess excellent interpersonal skills and able to communicate and manage relationship at all levels including senior management, business users, participants, vendors and team members
8. Fluency in written and spoken English is essential for this position