PRAVEEN NAIR

CISM | CEH | ECIH

☎ +60177976856
✉ praveen.nair.biz@gmail.com

SUMMARY

Head of Group Information Security

Praveen Nair serves as the information security subject matter expert tasked to oversee, manage & maintain information security within the Carsome group of companies. He is an experienced builder that has effectively designed, implemented and led best-in-class enterprise information security programs.

Praveen has built information security from scratch and provides trusted advisory services and guidance to stakeholders that will reduce organizational risk and improve overall security posture. He has also implemented & managed an internal & external security operations center and has a strong understanding of technical and business operations. Praveen has the ability to articulate technical security issues and solutions into business terms for C level staff. He has extensive Information Security experience across many different roles and also collaborates with many security leaders around the globe.

Praveen has a reputation for delivering high value work across multiple functions & has significantly reduced operational costs for his companies. He also participates in industry forums and stays abreast of evolving security trends and affairs to provide subject matter expert feedback. He has also built and managed high performing security teams. His current role is heading the Information Security division for Carsome Group in the Malaysia, Singapore, Indonesia, Thailand and China marketplace.

EXPERIENCE

Carsome Group - Malaysia | Singapore | Indonesia | Thailand

Head Of Group Information Security

2021 – Present

Carsome is Southeast Asia’s largest integrated automotive e-commerce platform with a valuation of over 1 billion USD. With operations across Malaysia, Indonesia, Thailand and Singapore, Carsome aims to digitize the region’s used car industry by reshaping and elevating the car buying and selling experience.

The company provides end-to-end solutions to consumers and used car dealers, from car inspection to ownership transfer to financing, promising a service that is trusted, convenient and efficient. Carsome currently (‘22) transacts around 100,000 cars annually and has more than 4,000 employees across all its offices.

RESPONSIBILITIES / ACHIEVEMENTS

Strategy, Governance, Risk & Assurance, Audit & Compliance, Awareness

- Led the creation of Security roadmaps & long-term risk based strategies to enhance cyber security resiliency at an optimized cost to the organization.
- Performed security budget planning, tracking and reporting.
- Overall security dashboard preparation & monthly reporting to ExCO committees for improved visibility of information security metrics & achievements.
- Performed governance of stakeholders deliverables (2 direct reports & 9 indirect reports).
- Oversaw the ISO 27001 standard readiness for Carsome and its subsidiaries.
- Led cost optimization efforts for the information security department to support business objectives.
- Oversaw end-to-end security compliance management including coordination & execution of security compliance programs (ISMS, Internal Policies / Manuals / SOPs, regulatory requirements, etc)
- Oversaw compliance management activities to various regulatory requirements such as SOX, PDPA, SGX, as well as investor requirements.
- Oversaw end-to-end security risk management including establishing and reviewing risk management strategy as well as risk treatment plans to proactively manage cyber risk.
- Part of the merger team to integrate group policies and controls to the acquired subsidiary.
- Coordinated with multiple teams & led the implementation of security baselines for the technology infrastructure.
- Developed & monitored KPIs & OKRs for the security team to provide measurable outcomes.
- Led the development, implementation & enforcement of group wide information security policies, manuals SOPs and guidelines.
- Established a group wide security awareness strategy to improve awareness of common threats and scams to our employees.
- Oversaw information management activities such as data classification and data labelling.
- Security operations SLA, KPI & delivery monitoring.
- Security liaison for internal & external auditors.

Domino’s Group - Malaysia | Singapore | Cambodia

Group Information Security Manager

2016 – 2021

Domino’s Malaysia, Singapore & Cambodia are proud members of the world’s largest pizza company, Domino’s Pizza International, an American multinational pizza chain headquartered at the Domino's Farms Office Park in Ann Arbor, Michigan.

RESPONSIBILITIES / ACHIEVEMENTS

Strategy, Governance, Risk Management, Compliance, SOC, SecOps, Security Programs, Awareness

- Fostered & led the adoption of NIST frameworks for Domino’s in the Asia Pacific Region.
- Worked with International teams & led the implementation of global security baselines for the group.
- Developed KPIs & SLAs for security operations to provide measurable outcomes.

- Conducted monthly update sessions to the Group CEO and quarterly updates to steering committees for improved visibility of information security metrics & achievements.
- Led the development, implementation & enforcement of a group wide information security policy.
- Fostered a risk-based approach to security resulting in the reduction of security operating cost by 40%.
- Secured buy in from Group CEO for the implementation of the group wide security strategy.
- Led the creation of IT Security roadmaps & long-term plans to enhance cyber security resiliency at a low cost to the organization.
- Led discussions with IT leadership to improve asset classifications resulting in reduction in OPEX for 2020.
- Aligned security strategy to an organizational risk register as well as security frameworks in order to tackle the most important gaps and present a more holistic strategy.
- Spearheaded the security architecture reviews & audits of the acquired entity to identify security gaps to the desired state and briefed senior management on the requirements & recommendations.
- Designed and led the implementation of a group wide security awareness strategy, training over thousands of staff via multiple channels which has helped thwart multiple potential security breaches & improve the security culture in the organization.
- Worked with International security teams to develop a comprehensive breach response plan for business preparedness to inevitable breaches. Led the implementation of the plan, collaborating with stakeholders from various departments. Implemented an annual testing strategy for the plan to spark discussions and ensure readiness of the organization.
- Established a risk management program to proactively manage IT infrastructure & online store risk as well as integrating a proper patch management strategy.
- Led the implementation & improvement of asset inventories with inclusions of asset criticalities and business impact.
- Developed and implemented a risk management strategy and a risk register, which facilitated the identification, assessment and mitigation of cyber risks.
- Compare & contrast multiple cyber insurance policies for the organization. Worked with the CFO and HR to finalize a policy for the organization.
- Enforced an organization wide MFA policy to enhance protection for account takeovers. Led the implementation of the initiative and helped guide IT on technical feasibilities.
- Proactively configured over 400 rules to automate blocking of security incidents. Tools are now over 90% automated reducing burden to security analysts.
- Improved & optimized multiple tools to reduce unnecessary costs.
- Oversee & lead the implementation & enforcement of multiple security policies.
- Worked with the CIO to build & manage an internal SOC purposed to monitor and respond to incidents for thousands of endpoints & servers in multiple countries. Successful in preventing thousands of business crippling cyber-attacks. It was one of the very few such centers for an organization in Malaysia.
- Deployed, managed and monitored multiple tools such as IDS, IPS, NGAV, SIEM, Email Security, Sandbox solutions including performing incident response.

ARTICLES & SPEAKING ENGAGEMENTS

4 Ways to Get More Value Out of Your Information Security Program

Article

Cyber Security During the Pandemic

Article

DigiTech: Innovation & Security Resilience 2022 Singapore

Speaker

Total Security Conference 2022 Malaysia

Speaker

CERTIFICATIONS

Certified Information Security Manager (CISM)
ISACA

Certified Ethical Hacker (CEH)
EC-Council

Certified Incident Handler (CIH)
EC-Council

Certified Vulnerability Assessment & Penetration Testing Professional
CyberSecurity Malaysia

Certified Web Security Professional
CyberSecurity Malaysia

Certified Android Mobile Security Professional
CyberSecurity Malaysia

Certified Security Aware User
CyberSecurity Malaysia

Certified Incident Responder
Cybrary

Certified Incident Management
Cybrary

General Certificate of Education O Level
University of Cambridge

EDUCATION

University of the West of England
Bachelor of Computer Science (Hons) (Computer Security and Forensics), 2012 - 2016

Taylor's University
Bachelor of Computer Science (Hons) (Computer Security and Forensics), 2012 – 2016

COURSES

Enterprise Cyber Security Fundamentals
Charles Sturt University - Australia

Corporate Cybersecurity Management
Cybrary

Chief Information Security Officer (CISO)
Cybrary

Advanced Penetration Testing
Cybrary

STRENGTHS

- Information Security
- Strategic Planning & Partnerships
- People Management
- Relationship Building

- Problem Solving
- Adaptability
- Communication
- Empathy