Curriculum Vitae

Nick Ooi Eng Hooi, ITIL,CEH,ECSA,PMP,TMDS,ACE-PAN

Mobile: +60-165575449
Email: noeh80@hotmail.com

Professional Summary:

Over 16 years of IT Experience in project management, running multimillions IT operation & Cybersecurity. Experienced in vendors' management, managing team of managers & engineers comprised of various technical level. Provide guidance to team members in assuming managerial roles. Real-world practical hands-on experience in project planning and implementation, solution designing helps in preventing any critical risk from bogging down project delivery. Self-driven initiative in kick starting FY project & departmental goals to support enterprise information & cybersecurity strategy and translating them to support growth and protection from critical cyber & data breach. Proven track record in spearheading change, improvement, innovation & IT dept restructuring that bring people & business to next level as well as in reviving many near failed projects thru out my career. Leading team members with high spirit to work round the clock to accomplish result.

On technical side, a few incredible things I've done including building up Redhat server farms without any prior Linux knowledge, passing PCIDSS audit without any prior knowledge. Building Oracle Database & Oracle cluster by googling with a work buddy. Setting up HP blade server series and building the underlying network fabrics module without any prior knowledge of blade. Perfectly built.

Corrected too many wrongly implemented solutions throughout my career to help business run more efficiently. Literally means number of years in a company not necessarily relate to the amount of contribution.

Information Systems Literacy:

- Windows, Linux (Centos, Redhat), IBM X5, HP Blade Server, SAN Storage: IBM DS3000/5000/HP 3Par series
- Juniper SSG550, SRX650, Checkpoint Firewall, IPS, Imperva & Barracuda WAF, FIM, SIEM Novel Sentinel & Mcafee, AlgoSec, CloudFlare, Incapsula, Nessus, FoundStone, Tripwire, NetMRI, Network & Server hardening. TrendMicro ApexOne, TMCAS, Dsaas, DLP. Secure DNS infrastructure, Acunetix, BurpSuite, Veracode, Quest Kace, PAM, Tenable.IO.
- F5 BigIP (DSC, LC & LTM, GTM, ASM, iApps, iRules), Network: HP & Cisco, Switching, Routing
- CoreJava & Android, AMX programming
- Multimedia*:* Kramer, Extron, clearone, polycom, Tandberg, DSP Processing, AMX.

Credential:

ITIL V3, CEHv6.1, ECSAv4, PMPv5, PDPA (SG), TMDS10-CP, ACE-PAN8.1, AWS-SecEn

Other Experiences:

Agilent Project Mgmt, I3M, PCIDSS**,** C-TPAT, 5S, LEAN 6 Sigma, ISO27001:2013

Professional Experience

SeekAsia

Seek Limited and its subsidiary companies, known as the Seek Group Headquartered in Melbourne, Seek is a public company listed on the Australian Securities Exchange

Information Security Manager (Dec 2016 to current)

On the second day at work, we discovered a major data leak and since been busy engaging various stakeholders for incident management. The data breach was posted online as well as in the darkweb 10mths later in Oct 2017 https://www.bbc.com/news/technology-41816953. Stories begin …

Chapter 1 - Stop the Bleed
Cut all access to database leaving only service account required by major apps and DBA team. Firewall rules and switch ACL inserted to block all access to database segment except prod server. All shared account of any form was put onto red flag list for logs investigation, eternal forensic was engaged for security audit. Enterprise wide privilege account reset and core database OS was hardened single handed by myself. Sudoer was enforced in all Linux instances.

Chapter 2 - Over Agility
Possible application breach point was remediated - to list a few: login password upgraded to strong encryption+salt hashing, password complexity also upgraded and enforced, login account reset process to all clients was establish and EDM was blasted to all clients. All data access process was refined and multi-layer approval are put into the process. Apps log containing login details and password was identified and removed.

Chapter 3 - Security at Stake
Mid Jan - Imperva WAF was immediately deployed follow by 6mths of extensive fine tuning to granular level as small as a button action on the portal with Realtime data masking for PII and CHD.
All Nextgen/UTM for both production and branch office was with default configuration - tweaked, replaced deprecated vpn tunnel encryption, enabled IP spoofing, flood protection threshold, necessary IPS rules, gateway AV+ATP, web reputation filtering to Mobile, Guest & Office Wi-Fi, removing Guest & Mobile Wi-Fi network from direct access to Office LAN and production network, cleanup firewall rules that open up both branch office and production to external network. AppCtrl to block unauthorized VPN, P2P software. Any C&C, botnet, malware, darkweb connection was completely block as an effective Zeroday prevention for instance WannaCry and Petra outbreak.

Chapter 4 - Discover the Horizon
Apr 2017, Network & VA scanning reviewed and config corrected leading to multiple identification of compromised DNS server and more. A Cloudbased SecureDNS architecture was introduced and all DNS was migrated to the new architecture. Old DNS & ADFS server put to retire.
June 2017, Cloudflare was introduced and implemented to improve website performance thru CDN & Cache, DDOS protection, L7 WAF with proprietary and OWASP ruleset, anti IP spoofing protection, HTTP response security with workers module. Manual user-agent blocking and anti-scraping has fine tuned to a point where whitelisting is required to allow similar nature task to run internally.

Chapter 5 - Fast forward into the future 2018 and beyond

- PDPA requirement was incorporate into the IT Sec and business process including awareness training, privacy agreement, vendor compliance and governed by ITSec compliance officers together with DPO community.
- *first version of cloud policy released.*
- *Run the first ever annual refresher awareness across all regional offices in Seek Asia in conjunction with ABC awareness with risk department. Vendor assessment checklist was introduced and later incorporated with PDPA requirements.*
- *all ITSEc related tools was handed over from Infra team.*

- *All on-prem ITSec solutions migrated to principal or aws cloud, never miss any version update. This enabled technology such as behavioural analysis, machine learning, virtual analyser to be available on detection engine, dramatic detection and prevention rate increase and reduce BAU task for manual analysis and blocking. integration with other cloud services was made easy such as O365, SharePoint, OneDrive, Veracode, Okta for SSO+MFA, DLP, Cloudflare...etc*
- *Internal Pentest framework and process refined for more effective work process and producing quicker result.*
- *Critical Backend API with PII data processing & transfer function was tested more rigorously and lead to discovery of many more exploitable critical security flaws, such apps token authentication was refined by dev team and bring backward into protected perimeter segment.*
- *Privilege Identity Mgmt system was deployed and enforced as the only access method for all user's remote connection to production system.*
- *Tenable IO was introduced and implement for further detection.*
- *SIEM & Patch Lifecycle system POC and introduced to mgmt.*
- IT Security framework, Roadmap & Goal, Security Posture Improvement & Annual Budgeting as part of annual team achievements and contribution.
- PDPA governance and compliance matter with regulatory. Actively monitoring regulatory change for MY, SG, HK and other regional offices with DPO community.
- IT Security baseline checklist, Cookbook, Code Security guide knowledge base to speed up team adoption process.

Astro (MBNS & GoShop)

One of the key multimedia and broadcast conglomerate in Malaysia

AVP, Technical Security & infra mgr (Jul 2014 - Dec 2016)

- Anything pertaining to Cybersecurity especially Security Incident and Suspected Breach investigation, PCIDSS compliance audit and Payment Gateway. All technical security project pertaining to business process implementation wrap around PCIDSS for payment gateway.
- Mcafee MVM+EPO, Websense DLP+Proxy+mail gateway, Novell Sentinel, FIM, Tripwire, Algosec, Nessus Scan, Hardening Standard. Completed the 1st POC project for cross platform Win+Linux+HP-UX patch management system.
- Workout the correct SAQ, QSA, ASV scope needed for internal and external merchant with PCIDSS auditor to prevent scope creep. In charge of all payment merchant onboarding projects

Pioneer in setting up GoShop business for Astro.

- Mitigated and rectified erroneous IT solutions as one of the key contributing factors to the successful business startup. workaround by loaning multiple core devices to get the project running. Working round the clock with vendor & Korean developer team using Google translate & sign language to meet harsh timelines, scope & constraint. Over 2 months consecutively working round the clocks, sleepless night to deliver result.
- Hands-on with vendor to setup full sweep of ecommerce business infrastructure - Blade Redhat clusters, Oracle DB, barracuda WAF, Checkpoint, IPS, SSL VPN, metro-E network, transit network, Redhat mgmt servers, FIM, SIEM, Security/pentest scanning, hardening of devices, network & servers.
- Passed PCIDSS audit in 1 month, completed writing fresh process & procedure required for PCIDSS in 2 weeks, closed all security requirements & gaps in 1 month.
- Assume roles of PM, Delivery, Solutions Architect, infra, Cybersecurity, auditcompliance L1 to SME support alone.

Challenges:

Vendor Contract was awarded prior joining the company, was given a copy of vendor proposal with dozen of wrong BOM specification, solutions & scope of work. Multiple meetings and follow up was initiated to rectify some of the critical items while develop workaround for others to get the project going include obtaining free help from vendor and colleagues to support the project implementation that include working round the clock to meet impossible triple constraints.

Nettium Sdn Bhd

Multibillion USD gaming company

Manager, PM & Infra Support (Oct 2010 - Jul 2014) Team: 3 PMs, 2 Support Mgrs, 22 Engineers

Promoted to Mgr, PM & Infra Support (June 2013)

- Oversee Taiwan & Malaysia team whom manages the rented IDC operation & infra.
- Providing career advancement to team members to assume leadership roles in other business entities.

Assigned to lead all Infra PMs (Jan 2013)

- Manage a team of project leads for transition, infrastructure and ad-hoc projects.
- Overseeing new transitions project and existing one's for improvement.
- Provides functional guidance to local team in the area of transferred services (including operation of servers, operation of networks and customer support)
- Establish and maintains clear mechanisms to communicate project status and change with the project team and other stakeholders. Communicate resource needs and project issues with the project management team.

Project manager

- Overall IT infra project management & design for e-commerce, e-gaming, payment gateway solutions.
- Project management for overall scope: new setup, migrations, transitions, geo-location... etc.
- Determined a monthly dashboard.
- Managed various shared resource team members and ensured achievement of all goals for projects.
- Assisted in developing communication in teams in an organization.
- Ensured maintenance of quality services for processes. Ensured all work in compliance with project management practices.
- Determined quality parameters for projects and it partners and ensured project progress accordingly.
- Live expansion on the service infrastructure to hosted up 20+ customers, a significant growth for the company.
- 2 new gaming solutions has been added on final quarter of 2012 into the same infra platform.

National Computer Systems (Singapore)

Multibillion USD system integrator technology company under Singtel.

Project Engineer (Feb 2009 – Oct 2010) Team: 5-10 Contractors
Company Size: 4000

Responsibilities:

- Deliver projects in compliance to CP5 & CP25 (BCA) compliance standard and demand for audio, video, lighting, automation & IT requirements in an integrated Infrastructure & Application Environment.
- Interpret & translate contract agreement into precise Project Scope, making necessary correction to Presale design to drive accurate Project Solution & Planning result – SAP Budgeting, Costing, Baseline Definition for resources & Billings. Hands-on Integrated system designing, schematic detailing, patch & routing table definition, delivering as built, testing, commissioning and handover processes.
- Ability to handle building site issues, M&E coordination matters, PE endorsement requirements.
- AMX programming (RS232/485, contact closure/relay, IO, Infrared Red, TCP/IP Transmission)

Project: 1) NTU-HSS 6 Storey Teaching Facilities – (Feb09-Dec09 SGD1.6 mil)
2) Naval Museum, (SGD2mil)
3) Standard Chartered @ Changi B-Park (Nov09-Feb2010 SGD 1.3 mi
4) NUH Admin Block (Dec –Jul10 SGD1.2mil)

Significant Achievements:

- Successfully revived near fail project - contributing to the award of 2 more projects, the company won more projects from Standard Chartered & NUH the same year. Total value: exceed SGD4mil in 6 months period.

Global Apparels (Cambodia) Limited

Multimillion USD apparels and packaging manufacturing

IT Manager (Jan 2006 - Dec 2008)	Team: 2 Asst Mgrs, 2 programmers, 12 technicians Company Size: 10,000

Responsibilities:

- Managing overall IT&T operation for 3 factory plants in a fast-changing manufacturing environment.
- Manage Inventory, procurement & acquisition, Vendor selection and Contract review.
- Continuous improvement planning, SLA, policy & procedures.
- Manage ERP, Payroll, HRM system development & customization using .Net to comply with regulation requirements.
- Restructure overall IT system such as mail system, IRIS 3k&4k with HRM, network, inter-plant wired & wireless intranet**.**
- Implemented Firewall, IDPS, Proxy, VPN with filtering rules targeting each Business Unit Functions, System Hardening, Port/Protocol Filtering at Firewall for business-critical server. Define Activity Log, Access and User Traffic Monitoring.
- Lead corporate Voice Network design e.g. Video & Teleconferencing, VOIP & PABX. (Panasonic D500 v2.5, Panasonic D1232)
- Integrated certain function for design center: Lectra Modaris, Diamino, pattern marker & design plotting machine and into production Autocutter Machine.
- Setup new factory plant IT infrastructure & System.
- Report to GM and assist top management in administration operation particularly IT development, HR & operation.

Major Accomplishments:

- IT operation efficiency was polished to new level enabling the company to establish 2 new plants while yielding a higher net profit in overall. IT & Non-IT processes & procedure continuously enhanced to sustain lower head count.

Karensoft Technology Bhd. (MY,CN)

Senior Consultant (Jan 2003 - Nov 2005)	Team: 3 Jr. Consultants

- Provide Full ERP cycle (Accounting, Fixed Asset, Payroll, HRM, MRP, Production Scheduling, SD modules) training to internal staff and customers.
- Requirements analysis and data gathering from stakeholders to understand their business flow and daily operation
- Draft project outline in terms of specifications and requirements to enhance and improve the software to meet customer business operation
- Work with project team to resolve conflict, derive resolution to achieve project completion

Achievements:

- relocate to China to localize ERP system.
- Implemented ERP project: Winery, Distribution (import & export), textiles and electronic industry
- Help to manage the China office in the absence of the Regional GM, help to liaise with China channel sales partner

Educational Qualifications and Training

University of Lincoln (UK) March 2002	B.Sc. (Hons) in Computing & Information System
KDU College (MY)	Higher Diploma in Computing and IT
Heng Ee High School (1998)	‘O’ Level

Extra Curriculums:

Water Polo	:	State representative
Lifesaving	:	Bronze medallion (lifesaving society of Malaysia)
Dragon Boat & Volleyball:		School & club’s representative

References

Dato’ Rozalila
CEO Astro GS Shop
Email: rozalila.rahman@gmail.com
Mobile: +6012-2829130

Mr. Wang Tie Feng
Project Manager - YXTech Pte Ltd (Taiwan)
Email: wangtiehfeng@gmail.com
Mobile: +886-932270916

Mr. Brite Lee Teck Voon (migrated to USA)
Regional General Manager
Karensoft Technology Bhd
Email: Bleetv@hotmail.com

Adrian Lee
CEO @ Tridenttech (Phil) Ltd
Email: adrian.lee@gb2bc.com
Mobile: +63-9178191177

Mr. Wilson Wong
Snr Project Manager - NCS Pte Ltd (SG)
Email: kongpeng@ncs.com.sg
Mobile: +65-97417084