MY RESUME (2018)

Song Jian Tat (WILLIAM)

CISM, CRISC, CEH, ISO 27001 Lead Auditor

Williamsong168@gmail.com **| 39 years old**

Contact: +6017-6660228

Experience	**17 years**
Previous	**Enterprise IT Security Specialist in AIG (Cyber Defense for APAC)** **Technical Lead, Compliance cum Project Director** **Deputy Director cum Head of IT Security (*8 years in IT Security Banking Industry, 4 years in Insurance Industry, 5 years in other industries)***
Education	**Coventry University, UK** **B.A (Hons) Degree in Business I.T, year 2000 (Dec)**
Nationality	**Malaysian**

Experience

Jan 2016 – Present

Head of IT Security (Regional role)

Company – Qi Group

- Define IT Security Strategy for the company that aligns with corporate directions

- Managing multiple Departments (5 different departments) across different countries (Regional role) – Security Operating Centre SOC 24X7, Network Operating Centre NOC 24X7, IT Security Engineering, IT Service Management (ITSM) and GDPR Info Governance departments (For all Europe Offices and 126 countries)

-Act as a Business and IT Drivers to Setup and manage the Information Governance and Compliance Department (NEW) department (Regional role) for **GDPR (General Data Protection Regulation**) European Law for all global offices including Europe's 16 offices

-Perform thorough analysis on both Business and IT areas and find out the gap and risks between Business and IT via GDPR regular audits and compliance checks. After the analysis, recommend and propose the best solutions to the board of directors for immediate actions.

-Maintain, publish, enforce corporate policies, guidelines and assist various teams across different regions in defining their corresponding IT Security policies and procedures

-Manage a Regional Security Architect team to assist in the development and review of overall security architectures, operations concepts, Information protection policy, methodologies for assessing the security and vulnerability of programs, prepare security documentation, and maintain a repository for all system certification documentation and security documentation.

-Develop strategic solutions and programs across multiple regions such as Hong Kong, Malaysia, Philippines, Singapore, Thailand, India, Dubai and Europe.

-Managing security engineering team to work with test teams and quality assurance teams to ensure our own self developed ecommerce platform are secured and stable.

- Develop SOP and governance rules and to ensure complete compliance with all the regional operational procedures.

- Managing SOC 24 X 7 X 365 and NOC 24 X 7 X 365 both monitoring teams. Provide guidance and strategic planning to both teams and making sure that the incident response time met the SLA benchmarks.

- Monitor and enforce policies and procedures. Respond to, investigate, and report on security incidents and violations, as appropriate.

-Oversee a network of security directors, vendors, consultants, contractors, IT security SMEs who safeguard the company's assets, intellectual property and computer systems, as well as the physical safety of employees and visitors.

Dec 2012 – Dec 2016

Enterprise IT Security Specialist (APAC)

1. **Cyber Threat Specialist (APAC) (Promoted)**
2. **Database Specialist (APAC regions)**

Company - AIG Global Services (Malaysia) Sdn Bhd, Cyberjaya

•Serve as a subject matter expert (SME) on matters of Enterprise IT Security with a specific focus on Database and Cyber Threat technologies for all regional areas. Proactively identify possible cyber threats and information security risks.

•Serve as a Security Incident Response SME to mitigate and response to any security incidents for APAC and lead the incident response team to investigate and mitigate any cyber threat issues/risks. Proactively suggest any improvements to avoid future cyber threat risks by improving the procedures, processes, technology solutions and others.

•Maintain the organization's various Database and Cyber security/compliance tool sets and standards.

•Research, analyze, recommend and implement new security processes, procedures, security checklists, products, technologies, applications, and/or services as needed to ensure the efficiency and integrity of the corporate IT environment for all AIG regional areas. Assist and support the audit team to provide regulatory audit support and complying with regulatory requirements whenever necessary.

•Perform security monitoring analysis on all kinds of cyber threats including Malware and Phishing’s threats and also develop the APAC’s cyber threat incident response procedures and security policies

•Implement new technology solutions and improve the current procedures and processes to comply with the internal policies and external regulations.

Apr 2012 - Nov 2012

Project Director, Technical Lead cum Compliance Manager

(Contract)

• IT Security Projects mainly for Philippines' government agencies

•Act as a Technical lead and Project Director roles to lead and manage the security teams to complete project from end to end.

•Shape the next 3- 5 years IT Security Roadmap for the Government agencies (4 Departments) by understanding their network architecture and IT Security benchmarks.

•Compliance Manager role to check on all non-compliance issues and check on all security policies and procedures and provide recommendations.

•Lead the Security Penetration Testing team to check on the security gap analysis and security loopholes and later on provide technical recommendations and proposals to overcome the security loopholes

•Business Manager and Pre Sales Manager Role – Identify customer challenges and develop strategic solutions and action plans. Perform good analytical ability and advice on the resources planning for these assigned IT projects with proper revenue forecasting to my clients. Present technical solutions, business ROI and IT Costing to the clients and follow-up till the project closure.

•Define proper incident handling process, Business Continuity Plans (BCP),risk management processes and procedures for my clients

Jul 2011 - Mar 2012

Deputy Director cum Head of IT Security (Prof Service Unit – Pen Test and Security Operation Teams)

Company - Extol MSC Berhad

•Manage and Lead the Professional Service Unit (PSU) Department (2 teams – Pen Test and Implementation Team)

•Set the technical directions, strategy planning & technical solution designer for Professional Service Unit (PSU) – mainly on Pen Test, IT Security Architecture, security implementation projects and operation projects

•Manage and Lead the security implementation team to resolve any major security incidents

•Act as the point of contact for all security incidents (Incident Manager)

•Involve in clients' governance team as an advisory role and provide recommendations and suggestions for improvements

•Manage a Pen Test team to provide all kinds of security health check analysis reports and recommendations to improve the overall IT Security environment for my clients

•Manage the security operation team to maintain all the security operations for IT Security related products (such as Data Loss Prevention (DLP), Intrusion Prevention System (IPS), Antivirus, System Hardening, Database Security , SIEM (Novell Sentinel) backup all IT audit logs, guiding the operation team to handle security incidents and defined the incident handling process, critical incident process and other security operation procedures

•Assist in Managed Security Services (MSS) which I need to perform site visit to all my key customers in every month to explain all Managed Security Services monitoring results (Examples: any unusual ports open in my client's network, provide recommendations to improve their network security and making sure that their networks are totally secured)

•Member of the Strategic Management Team (to discuss and set on future company's directions, technical solutions and business strategic) to achieve all business goals. Provide team progressive reports, performance reports and also budgeting proposals to my management

•Collaborate with business users and IT Security team to create business continuity plans (BCP plans) and also define critical incident processes and procedures for my clients

•Project Manager role to manage and coordinate the project team members to complete the projects from end to end in timely manner.

•Pre-Sales Manager role to accompany the Sales team to understand the customers' technical and business requirements and then propose the technical designs with complete solutions to cope with their expectations.

•Perform good analytical skills and advice on the resources planning for the assigned IT projects with proper revenue forecasting to the Sales team. I will also propose reasonable project implementation schedule plans to the customers and seek for their approvals.

•Establish long term business partnership and relationship with suppliers, clients, consultants, principals, IT security associations (Example: ISACA, ITIL) and event organizers.

Major Accomplishments:

-Completed a series of security gap analysis finding reports and audit findings report for 2 government agencies on their current service provider's performance. Based on the findings and proposals, we found some major security loopholes that lead to some critical security risks for their web security. As a result, we proposed a new architecture design and improve their current security processes and procedures and we resolved all the issues. After that, we received good response from their management team and they even provided my company a 3 years IT Security contract (Managed Security Services- MSS monitoring service for 24X7).

-Able to lead the PENTEST team to complete quite a number of high quality **Pen Test** analysis findings which later converted to more sales contracts to my company (Pen Test as an open door)

-Maintain good rapport with major banks, insurance, government and SME companies (my clients) and I was recommended by them to a few major sales contracts for my company

Mar 2009 - May 2011

(Promoted, Total 5 years of service in CSC)

Security Architect cum New Business Manager

Company - Computer Science Corporation (CSC)/ CSA, Maybank Account

•Able to design and propose complete IT security solutions and provide business costing (in-charge for Maybank Malaysia and Singapore accounts)

•Evaluate on different IT security products and vendors to provide proper technical and business justifications to my CTO when choosing the right security products in order to meet my customers' expectations

•Define and manage service continuity plans with the Business Continuity Planning (BCP) teams

• Support the development of policies, best practices and tools on security operation and management as a standard for Maybank group

•Assist the Security Assessment team on the post-test remediation actions.

•Analyze and review security related business requests from Maybank Malaysia and Maybank Singapore. I will ensure an effective evaluation on all the business risks (by following global CSC risk management processes), applied the agreed CSC's global and standardized IT Service Management processes into the design of all the solutions, prepare IT costing, technical designs and project discussions with all my project teams - CTO/ Project Managers/Subject Matter Experts/Finance/Other Business Leaders/Vendors/Suppliers to assign the right resources and the right technical solutions to meet all my customers' requirements.

•Discuss with the Vendor (to get the right pricing and products evaluations), And also regular meetings with the other Business Leaders (to calculate their resources efforts in my proposals), Finance (to adjust the right costing and margins), project managers (to get the right project schedule and resources planning across all departments), other IT related dept (to allocate Subject Matter Experts and agreed on costing, technical designs and solutions) and then CTO (to explain and justify on my high level technical and costing proposals and the right business margins) to get final approvals.

•Project Management role – To guide the security and operation engineers to implement the projects based on CSC's global and standardized project management processes and ITIL processes

•Review IT Security risks and compliance risks when receive business requests from the customers and evaluate on the pros and cons before proceed further to the next steps

•Design and Implement Password Management solution, Identity Management, ATM Server's File Integrity Solutions, Antivirus, IPS, Intrusion Prevention System (IPS) and Data Loss Prevention (DLP)

•Regional IT Process and Project Management experience and applied CSC's global change management processes for all change activities

Major Accomplishments:

-Designed and Implemented Password Management solutions for all Maybank's branches nationwide (this project involved more than 12,000 branch users). This project involved lots of parties, including business unit, application teams, branch users' team, IT Security team, Compliance team, BCP team, Network team and others.

I was involved in this project as a security architect, implementer, Project Manager and Coordinator, Team Lead (security team), Costing and also Operation Lead. I also developed various processes and procedures in order to coordinate with all Maybank users (about 12,000 branches nationwide, users involved in this project were about 60,000). This project was implemented successfully.

-Designed and proposed technical solutions for Maybank Singapore to secure their ATM machines for file integrity security management solutions

-Propose and design high availability (HA) for IPS network architecture and technical proposals plus IT costing via tender documents.

-Proposed and designed the Data Loss Prevention (DLP) solution for Maybank Etiqa.

Aug 2006 - Jan 2009

Senior Security Engineer, SLA Lead

Computer Sciences Corporation (CSC) /CSA, Maybank Account

•Mainly focus on IT security operations, IT projects and Network Security solutions for customers (Maybank Malaysia and Singapore)

•Root Cause Analysis (RCA) Representative (for IT Security team) to investigate the root cause of any security incidents, discussions to minimize the company's business impacts from the incidents in future (with Service Level Agreement – SLA team) and find out the actual problems and then propose suitable solutions to management and customers to resolve the issue permanently.

•Planning, scoping and supporting audits review sessions with Maybank's appointed third party Auditors (Big 4 and Maybank's internal auditors)

•Capability to run Vulnerability and Risk Assessments via tools such as Nmap and Nessus to interpret the security analysis reports and then provide recommendations and mitigations methods to improve the IT Security environment for Maybank

•In-charge for Service Level Agreement (SLA) and manage the vulnerability management (make sure all updates for security patches are most current and implement an auto alerts update methods across all security products for a better monitoring process

•Responsible for Security Event monitoring and response procedures - defining the monitoring requirements for logs and operational procedure/practices for any security incidents

•Propose technical improvements on current network security solutions and infrastructure into customer's network (**Example: Proposed and Implemented successfully for the Identity Management and Password Management solutions**

for Maybank which speed up the response time (3 times faster) and reduce operation costs by at least 40-60%.

•Design/Configure/troubleshoot the first batch of Intrusion Prevention System/Intrusion Detection System (IPS/IDS) for Maybank and perform regular maintenance and security logs analysis for any suspected intrusion behaviors (in shift rotations).

•Research and propose new security technologies and security enhancement initiatives

•Develop IT security policies and procedures and conduct regular security awareness training (Example: Cybercrime attacks and Social Engineering)

•Provide 3rd level support to technical team in resolving security related issues

Major Accomplishments:

- Promoted to Security Architect cum New Business Manager for CSC- Maybank account.

- Able to communicate with my clients efficiently and met all their expectations, which normally from management levels such as CEO, CTO, Head of IT Security, Audit and Compliance team, Head of Business team and etc.

- Performed research, technical evaluation of products and Proof of Concept (POC) for various security products and implemented successfully for my clients

- Setup and implemented IPS for Maybank Malaysia, Password auto management for Windows and Unix servers (about 300-500 units of servers),

- I was appointed as the SLA representative for my team. I managed to improve some major security incidents that breached SLAs via new processes and procedures. One of the few major accomplishments was to avoid SLA breach with penalty more than RM120K with thorough investigations on the firewalls during one critical security incident. I had also implemented some automation for servers password management solution and reduce the audit findings and SLA penalty.

- I am very familiar and confident with Malaysia 's IT security policies and procedures and flexible enough to apply my knowledge and experience in any industries to achieve a secured working environment.

Jun 2004 - Jul 2006

IT Security Executive (UNIX and Database Security)

Company - Hong Leong Bank Berhad

-Perform Operating System's security hardening for all Unix platform like Sun Solaris, Redhat Linux, SUSE and IBM AIX to meet Bank Negara's security standards.

- Involve in major security projects for all Unix platform, completed major projects like Unit Trust, Carma, E-Collect, Murex Treasury and etc.

- Perform also AS400 security

- Perform Database security setting too - mainly on Oracle database

- Check and review O/S security logs and audit logs

- Research and recommend to purchase various security tools to enhance security performance and monitoring tasks in the existing Unix servers.

- Define security checklist, policies and procedures for O/S and network security

- Prepare security analysis report for each hardening project

- Familiar with IT security in banking cycle

- Provide Internal trainings(UNIX) to my colleagues

- Work closely with internal and external auditors on the security audit issues

Major Accomplishments:

- Successfully completed the Unit Trust project - secure the entire Unix server and application's security in year 2004

- Completed 5 financial projects from Jan 2005 until November 2005 - applied all security settings in IBM AIX servers, Oracle database and application's security

- Completed 3 major financial projects (from Jan 2006 until June 2006) by applying security standards from Bank Negara to all the Solaris servers, Oracle Database and application's security.

- Prepared all checklist for Unix servers and also for database security checklist

- Improved the application security functions by recommending some ideas to enhance the password management processes and password reset response time

- Familiar with IT banking cycle and banks' IT security policies and compliance procedures

Feb 2004 - Jun 2004

System Engineer

Company - CSA Berhad

•Troubleshoot computer hardware and IT network problems

•Maintain Network Security via IDS and System Security protections.

•Outsourced to ASTRO as a MIS system engineer

Major Accomplishment:

•Voted as the best outsource team of the month-May 2004 (CSC-ASTRO team)

Jan 2003 - Nov 2003

IT Support Engineer

Company - Radius ED Sdn Bhd

- System administrator for Redhat linux environment - configure sendmail, Webmin, Firewall (IP forwarding), network services like Ftp, telnet, ssh, samba and others.

- Configure security settings(hardening) in Redhat Linux servers and Unix servers

- Configure Watchguard firewall and set security policies

- Perform network monitoring by using tools like snoop.

- Setup Redhat linux server for clients like NTT, Time, Unified Communications

- Configure Cisco router

- Configure cisco switch

Feb 2001 - Dec 2002

IT Executive

Company - T & K Autoparts Sdn Bhd (subsidiary of Toyota)

-Setup, configure and plan the Local Area Network (LAN)and Wide Area Network (WAN) network. Plan more on LAN than WAN.

- Novell Netware server 4.11 setup, security configurations and troubleshoot.

- Novell Client 3.2 setup and configuration

- Configure and monitoring IBM AS400

- Setup and configure Lotus Notes R5

- Troubleshoot any computer hardware and software problems

- Hands on experience on COINS, Frame Relay and ISDN

- To prepare all computer documentation

Major Accomplishments:

- Maintained the company's computer hardware and software for better performance

- I learned how to be more independent in my work and communicate with all levels of people in my company.

- Managed to reduce the users’ frustration in Novell’s Email system via new improvements in network bandwidth.

Education

2000	**Coventry University, UK** Bachelor's Degree in Computer Science/Information Technology | Malaysia Major B.A (Hons) in Business I.T Grade 2nd Class Upper
1997	**S.M Sri Istana, Klang** Primary/Secondary School/SPM/"O" Level in Sciences | Malaysia Major SPM Grade Grade A/1st Class

Certifications and Skills

Certificates	ISO 27001 Lead Auditor, CISM, Certified Ethical Hacker (CEH), CRISC (disaster recovery), ITIL v3
Advanced	Cloud security, Advanced Threat Persistent (ATP), GDPR, Malware and Phishing Analysis, Penetration Test (PenTest), ITIL, Firewall, IPS, Data Loss Prevention, SIEM, IT Security Architecture Design (TOGAF) , Microsoft Certified Professional, IT costing and budgeting, IT Strategic and Planning, Unix and Windows Security

Languages

Proficiency level: 0 - Poor, 10 - Excellent

Language	Spoken	Written	Relevant Certificates
English	9	8	-
Bahasa Malaysia	8	8	-
Chinese	7	7	-

References

Name : Mr. Eric Chong
Relationship : My former manager in CSC
Position : IT Advisor
Mobile No. : 6012-352-9063

Name : Miss Chong Ming Fui
Relationship : : My former manager in Hong Leong Bank
Position : IT Security Manager
Monile No. : 6012-250-2072