

# Nishchal Kush

## *Information Security and Systems Specialist.*

### Personal Details

Nishchal Kush

T:

E: [kush@kush.id.au](mailto:kush@kush.id.au)

W: [kush.id.au](http://kush.id.au)

### Areas of Expertise

- Information Security.
- Systems Administration.
- Networks Administration.
- Project Management.
- Software Engineering.

### Academic Qualifications

- MInfoTech, QUT – 2010  
Majored in Security.
- BInfoTech, QUT – 2000  
Majored in Software Engineering and Data Communications.

### Academic Awards

- 2014 - Science and Engineering Faculty (QUT) Scholarship.
- 2012 - Australian Postgraduate Award.
- 2012 - Deputy Vice Chancellor Top-up Scholarship (QUT).
- 2011 - Best Paper: 2<sup>nd</sup> Cyber Resilience Conference (ECU).
- 2010 - Dean's Merit Award (QUT).
- 2010 - Golden Key International Honour Society.
- 1996 - Australian Mathematics Competition Prize (AMT).

## Professional Overview

I am an Information Security, and Information and Communications Technology (ICT) specialist. I have a Master of Information Technology majoring in Security from the Queensland University of Technology and have cumulative professional experience of 15+ years in the planning, deployment, maintenance and management of information assets across a breadth of industries.

### Technical Abilities

- Systems and Network Security.
- Risk Management.
- Vulnerability and Penetration Testing.
- Auditing and Compliance.
- Linux and Windows Systems Administration.
- Cisco Switch and Router Configuration.
- Technical Writing.
- Project Management.

## Industry Exposure

- Government.
- Telecommunications.
- Banking and Finance.
- Electricity Utility.
- Higher Education.

### Technology Summary

Security: Firewall, Application White-listing, Intrusion Detection System.  
Systems: Linux, Windows, MacOS X, Unix.  
Networking: Microwave/RF, Copper, Fibre optics.  
Programming: C/C++, Java, PHP, PERL, HTML, Dataflex, shell scripting.

### Professional Memberships

Association for Computing Machinery (ACM).  
Australian Information Security Association (AISA).  
Institute of Electrical and Electronics Engineers (IEEE).  
System Administrators Guild of Australia (SAGE-AU).

### Academic Activities

University of California, Santa Barbara (UCSB) International Capture the Flag Competition (iCTF) competition.

- Team member (Cheddar Horsemen) 2013 – Dec 2013.
- Team member (Cheddar Horsemen) 2012 – Mar 2013.
- Team member (Cheddar Horsemen) 2011 – Dec 2011.
- Team member (Cheddar Horsemen) 2010 – Dec 2010.

## Professional Experience

### Queensland Government – Public Safety Business Agency, Brisbane, Australia.

20<sup>th</sup> June, 2016 - Present

#### Senior Information Security Specialist

- Requirement: Provide direction, technical guidance, design, installation and configuration services to deliver security solutions for PSBA and inter-agency systems ensuring that the information resources, data and network are secure and comply with relative standards and policies such as IS18 and ISO 27000
- Role: Assisted project managers and solutions architects in defining security systems by undertaking objective and systematic analysis of proposed solutions
- Outcome: Successfully developed and implemented security design and architecture for projects in line with QGCIO IS18 using technology such as Cisco ASA, Cisco Ironports, Big-IP F5, Checkpoint, Palo Alto, AppSense Application Manager
- Projects:
  - Application White-listing: Technical lead on application white-listing project using Appsense Application Manager. Developed detailed implementation plan and policy for application white-listing.

### Queensland Government – Public Safety Business Agency, Brisbane, Australia.

22<sup>nd</sup> December, 2015 – 19<sup>th</sup> June, 2016 (6 months)

#### Senior Information Security Specialist (Contract)

- Requirement: Provide direction, technical guidance, design, installation and configuration services to deliver security solutions for PSBA and inter-agency systems ensuring that the information resources, data and network are secure and comply with relative standards and policies such as IS18 and ISO 27000
- Role: Assisted project managers and solutions architects in defining security systems by undertaking objective and systematic analysis of proposed solutions
- Outcome: Successfully developed and implemented security design and architecture for projects in line with QGCIO IS18 using technology such as Cisco ASA, Cisco Ironports, Big-IP F5, Checkpoint, Palo Alto.
- Projects:
  - Multiple Network Proof-of-concept: Developed and implemented firewall rules on Cisco ASA for highly secure mobile VPN project using Radio Mobile MultiIP product.

### Queensland Government – Public Safety Business Agency, Brisbane, Australia.

12<sup>th</sup> October, 2015 – 21<sup>st</sup> December, 2015 (3 months)

#### Senior Security Specialist (Backfill Contract)

- Requirement: Provide immediate short-term support to the PSCS Design team.
- Role: Developed information security design documentation templates.
- Outcome: Successfully provided immediate support to the PSCS Design team by completing design documentation templates for use by solutions architecture teams to include security design as part of high-level solutions documentation.

### NOJA Power Switchgear Pty. Ltd., Brisbane, Australia.

9<sup>th</sup> Mar 2015 – 9<sup>th</sup> October 2015 (7 months)

#### **Embedded Software Engineer (Contract)**

- Requirement: Development of specifications and implementation of distributed control and automation for the NOJA Power recloser control RC10.
- Role: Eliciting requirements from stakeholders and documenting high level requirements specifications. Developing technical design specifications. Evaluation of commercially sensitive technology and documenting instructions for use in end-user documentation. Developing code in C and C++ for the RC10 embedded platform using Linux. Performing code reviews.
- Outcome: Discussed project requirements and documented high-level system and technical requirements. Developed software in C and C++ for the RC10 embedded platform using Linux software development tools. Performed software performance testing, troubleshooting and debugging using valgrind and gdb.
- Projects:
  - Smart Grid Automation – Software development of NOJA Power’s smart grid automation product which provides IEC 61499 functional blocks to RC10 reclosers for rapid development of smart grid integration and distributed automation.



### Qscan Radiology Clinics Pty. Ltd., Brisbane, Australia.

16<sup>th</sup> Feb 2015 – 27<sup>th</sup> Feb 2015 (2 weeks)

#### **Technical Consultant (Contract)**

- Requirement: Technical support to assist in commissioning new branch.
- Role: Advising on systems and network security issues. Risk management and investigating security incidents and issues. Performed security audits.
- Outcome: Successfully developed and deployed computer image using Windows System Centre 2012 R2 Configuration Manager (SCCM) for 5 different platforms. Developed and documented guidelines for SCCM management, set-up and deployment of drivers, packages and system images. Provided assistance to client in-house staff to physically image and package computers.
- Projects:
  - Qscan Carindale Branch – Developed and deployed system images for office administration, diagnostics, and radiology computers using SCCM 2012.



### Packwolf Consulting Pty. Ltd., Brisbane, Australia.

17<sup>th</sup> Feb 2014 – 12<sup>th</sup> Dec 2014 (10 months)

#### **Technical Consultant (Contract)**

- Requirement: Technical expertise on information security. Systems and network administration. Sales support.
- Role: Advising on systems and network security issues. Risk management and investigating security incidents and issues. Performed security audits.
- Outcome: Successfully evaluated customer requirements and configured and installed Endian based unified threat management (UTM) hardware on customer network. Developed anti-malware policy and configured AVG anti-virus software for remote deployment on customer networked Windows 7 workstations. Liaised with third-party service vendors to make changes to customer domain name service (DNS) settings. Provided training to junior team members and client technical staff. Investigated issue with client websites compromise, identified issue and provide advice and technical guidance on mitigation. Provided assistance to client in-house staff on the development of security policies.
- Projects:
  - 2-factor Authentication – Planned, tested and implemented Google Authenticator based 2-factor authentication on in-house Linux servers.

## Queensland University of Technology, Brisbane, Australia.

4<sup>th</sup> Sep 2013 – 23<sup>rd</sup> Oct 2013 (1 month)

### **Project Officer (Casual)**

- Requirement: Design and implementation of virtual network environment for Red vs. Blue team exercises.
- Role: Planned and developed virtual infrastructure for Red vs. Blue team exercise as part of the QUT Cyber Security (Industrial Control Systems) training.
- Outcome: Successfully deployed virtual machines and network using VMware ESXi hypervisors. Set-up CentOS Linux servers for domain name servers (DNS) using Bind, e-mail using Exim, virtual private network (VPN) access using OpenVPN, and web-based file sharing using Apache. Integrated virtual network environment with physical Cisco switches and routers. Cisco equipment was configured to provide access to Red room, Blue room, White room, and Industrial Control System (ICS).
- Projects:
  - QUT Cyber Security (Industrial Control Systems) Training – The entire infrastructure was used during the Red vs. Blue team exercise. As member of the White team, monitored the infrastructure and provided guidance to Red and Blue teams.
  - Panoply 0x7DD – The VPN infrastructure was duplicated and used as part of the Panoply 0x7DD exercises to provide access to the ICS equipment.

## Queensland University of Technology, Brisbane, Australia.

Oct 2012 – Dec 2012 (2 months)

### **Senior Research Assistant (Casual)**

- Requirement: Assist in the design and implementation of virtual environment for Red vs. blue team exercise and develop training material.
- Role: Assisted in the planning of training environment for Red vs. Blue team exercise. Developed learning resources, including lecture notes and hand-on exercises for firewalls and intrusion detection systems.
- Outcome: Successfully deployed virtual machines and network using VMware ESXi hypervisors. Set-up CentOS Linux servers for domain name servers (DNS) using Bind, e-mail using Exim, virtual private network (VPN) access using OpenVPN, and web-based file sharing using Apache. Integrated virtual network environment with physical Cisco switches and routers. Cisco equipment was configured to provide access to Red room, Blue room, White room, and Industrial Control System (ICS). Successfully delivered lecture on firewalls and intrusion detection systems and hands-on training on IPTables and Snort.
- Projects:
  - QUT Cyber Security (Industrial Control Systems) Training – Delivered training on firewalls and intrusion detection systems with hand-on exercises using IPTables and Snort.



## Packwolf Consulting Pty. Ltd., Brisbane, Australia.

27<sup>th</sup> Jul 2010 – 17<sup>th</sup> Feb 2014 (3 years 6 months)

### Technical Consultant

- Requirement: Technical expertise on information security. Systems and network administration. Sales support.
- Role: Advising on systems and network security issues. Risk management and investigating security incidents and issues. Performed security audits.
- Outcome: Successfully provided advice on systems and network security issues. Investigated security incidents and provided advice on mitigation. Performed Vulnerability and Penetration testing of customer web-applications and web sites. Performed Vulnerability and Penetration of customer servers and networks. Assisted customers in ad-hoc risk management exercises. Provided sales support for Cisco, Endian, AVG and Redhat Linux. Provided advice on web, e-mail and file hosting in accordance with amended Privacy Act. Planned and configured technical security controls on Cisco routers and switches. Planned and implemented virtual private network (VPN) for remote access using OpenVPN. Investigated e-mail spoofing incident and liaised with external systems vendors. Investigated incident relating to client website compromise and reported findings to client for mitigation. Configured Snort based intrusion detection system (IDS) for customer. Configured IPTables based firewall for customers. Configured server room monitoring using ZoneMinder. Provided advice to clients on technical solution selection to comply with the amended Australian Privacy Act.
- Projects:
  - Server Room Set-up – Planned server migration and consolidation for Credit One Group of companies from Southport and Upper Mt. Gravatt to Eight Mile Plains. Migrated stand-alone Windows workgroups to Windows Active Directory. Developed policies and plan for data backup and user access control.
  - Rapid+ - Designed and started developing web-based loan brokerage software called Rapid+ using PHP: Hypertext Preprocessor's (PHPs) Phalcon framework.



## Marinoc Pty. Ltd., Brisbane, Australia.

1<sup>st</sup> Feb 2010 – 27<sup>th</sup> Jul 2010 (5 months)

### Systems Engineer (Part-time)

- Requirement: Systems and network administration.
- Role: Monitored and maintained client Microsoft Windows SBS servers.
- Outcome: Successfully maintained Microsoft Exchange e-mail services. Provided end-user support for OpenVPN based virtual private network (VPN) connection. Maintained and configured Endian hardware based network firewall.



## Polyfone Telecom Pty. Ltd., Yatala, Australia

28<sup>th</sup> Apr 2008 – 18<sup>th</sup> Dec 2009 (1 year 7 months)

### Technical Officer

- Requirement: Systems and network administrator to maintain network infrastructure.
- Role: Monitored and maintained network infrastructure and servers. Site surveyed new customer installations. Configure and deploy network hardware to connect new sites.
- Outcome: Successfully commissioned new customers on wireless connections using SkyPilot Networks, Infinet Wireless, Bridgewave, Dragonwave, emSolutions, Redline, Motorola, Solectek, and WaveRider equipment. Implemented bash scripts to perform backup of all Polyfone servers to network attached server (NAS). Implemented PERL script to connect to all Cisco devices and backup the configuration. Assisted in decommissioned customers and retrieving customer hardware. Installed and configured OpManager and Zenoss to monitor network infrastructure. Implemented Network Time Protocol (NTP) for time synchronization across all network devices which supported the protocol. Performed network throughput testing. Provided customer support via e-mail and telephone.
- Projects:
  - Southern Cross Credit Union – Assisted in site survey. Configured Motorola PTP 300 radios. Assisted in the installation and alignment of the radio units between Mt. Springbrook and Murwillumbah. Assisted in the configuration and installation of Cisco 857 routers to 11 branch locations.
  - Griffith University Village – Path profiling of link using RadioMobile. Configured point-to-multipoint Infinet Wireless radios. Liaised with riggers to install radios. Assisted in alignment of antennas for optimal connection.



## Mackay Computer Services Pty. Ltd., Mackay, Australia

3<sup>rd</sup> Nov 2006 – 18<sup>th</sup> Apr 2008 (1 year 5 months)

### Technical (RF) Support Engineer

- Requirement: Engineer to support and maintain wireless network infrastructure to provide enhanced user-experience and Internet connectivity to customers.
- Role: Monitored and maintained existing wireless mesh and point-to-point network. Plan and extend existing network infrastructure to provide extended coverage to new areas. Systems and network administration of servers, routers, and firewalls. Responsible for the day-to-day operations of the networking infrastructure.
- Outcome: Successfully maintained existing SkyPilot Networks wireless mesh network, Airspan, Solectek, WaveRider, Dragonwave, emSolutions wireless point-to-point links. Set-up monitoring using Castlerock SNMPc and Cacti. Successfully monitored and maintained all network infrastructure including customer domains, and Linux and Windows servers including Bind domain name service (DNS), Radiator for remote authentication for dial-in service (RADIUS) authentication, Exim based e-mail service, Cisco routers and switches, virtual private network (VPN) end-points using SnapGear hardware, etc. Successfully performed link planning and profiling using RadioMobile and PathLoss software.
- Projects:
  - Mackay-to-Proserpine Link – Assisted in the alignment and monitoring of the emSolutions based point-to-point link between Mackay and Proserpine.
  - Frequency Change – Planned frequency change for frequencies used for mesh and point-to-point links to ensure best frequency separation and enhance network performance. Successfully changed frequencies on all RF links.
  - IP Addressing Change – Documented point of presence (POP) site naming and IP addressing policy. Successfully implemented policy and planned IP addressing change of entire network, including customer premises equipment (CPE) IP addressing change.



## Fiji Electricity Authority, Suva, Fiji Islands.

11<sup>th</sup> Apr 2005 – 1<sup>st</sup> Nov 2006 (1 year 6 months)

### ICT Systems Specialist

- Requirement: Information and Communications Specialist with diverse experience in project management, operational support, and networks and systems administration.
- Role: Provided project management support to FEA's upgrade of the Financial Management Information System (FMIS), Human Resources Information System (HRIS), and Human Resources Management System (HRMS) projects. Systems and network administration of servers, routers, and firewalls.
- Outcome: Successfully prepared request for proposal (RFP) documents and was part of the tender evaluation team for the FMIS, HRIS and HRMS projects. Successfully administered Redhat Linux servers, Cisco routers and switches, and PacketLogic platform.
- Projects:
  - Helpdesk Re-engineering – Successfully re-engineered helpdesk business processes and introduced HelpMaster Pro helpdesk management solution.
  - Broadband Connectivity – Successfully trialed broadband over power-line (BPL) technology by Mitsubishi and wireless mesh based on Skypilot Networks for broadband to provide Internet connectivity to rural schools.
  - Automatic Meter Reading – Provided ICT expertise and operational support to FEA's automatic meter reading (AMR) trial using power-line carrier technology (PLC) on Levuka.
  - Fibre Optic Link – Assisted the infrastructure team pull and splice fibre optic cable from Butoni substation to Sigatoka substation.
  - SCADA Protocol Migration – Assisted the SCADA team with the installation and testing of vendor built protocol converters in substations to convert from Modbus to Distributed Network Protocol version 3 (DNP3).



## Colonial Fiji Limited, Suva, Fiji Islands.

28<sup>th</sup> Jun 2004 – 6<sup>th</sup> Apr 2005 (9 months)

### Assistant Manager Infrastructure Support

- Requirement: Manager to manage IT Infrastructure and IT Support teams.
- Role: Responsible for the day-to-day operations of the IT Infrastructure and IT Support teams and IT Infrastructure projects.
- Outcome: Developed guidelines for IT Helpdesk operations. Documented IT Helpdesk processes and implemented standardized reporting of key performance indicators (KPIs).
- Projects:
  - Bank Branch Hardware Upgrade – Successfully planned and managed the upgrade of computer workstations to all Colonial bank branches.
  - Suva Central Branch- Successfully planned and managed the set-up of new Colonial bank branch at Suva Central.



## Colonial Fiji Limited, Suva, Fiji Islands.

20<sup>th</sup> Oct 2003 – 27<sup>th</sup> Jun 2004 (8 months)

### IT Analyst Programmer

- Role: Software analysis, architecture design, documentation and enhancement of Colonial Consolidated Life Assurance System (CLAS).
- Outcome: Analysed business requirements to document technical specifications and supervised IT Programmers to develop enhancements to CLAS.
- Projects:
  - CLAS Cheque Printing – Successfully analysed business requirements and designed CLAS cheque printing system and project managed development and implementation of the cheque printing system.
  - End-of-year Project 2003 – Successfully managed the EOY2003 roll-over project, including the implementation of fix-up projects.
  - DataFlex Upgrade Project – Successfully managed DataFlex upgrade project to migrate from DataFlex 2.3 to DataFlex 3.2.



## Colonial Fiji Limited, Suva, Fiji Islands.

7<sup>th</sup> Aug 2003 – 19<sup>th</sup> Oct 2003 (2 months)

### IT Programmer

- Role: Software development and maintenance of Colonial Consolidated Life Assurance System (CLAS) which was developed in DataFlex version 2.3.
- Outcome: Successfully developed software as member of the CLAS development team. Working on fix-up projects as part of data cleaning operations. Used traditional waterfall model as the software development lifecycle.

## Colonial Fiji Limited, Suva, Fiji Islands.

17<sup>th</sup> Feb 2003 – 6<sup>th</sup> Aug 2003 (5 months)

### Trainee Programmer

- Role: Software development and maintenance of Colonial Life Assurance System (CLAS) which was developed in DataFlex version 2.3 and ancillary systems in Visual Basic (VB) under the supervision of senior staff.
- Outcome: Learnt software development in DataFlex and successfully met maintenance and software development targets set by senior staff.

## Marinoc Pty. Ltd., Brisbane, Australia.

23<sup>rd</sup> Nov 2001 – 5<sup>th</sup> Jul 2002 (7 months)

### Systems Engineer

- Requirement: Systems Engineer to develop software, perform systems and network administration, and end-user support.
- Role: Develop web-based software using PHP on Redhat Linux. Developed software in C++ using the Fast Light Toolkit (FLTK) for Supervisory Control and Data Acquisition (SCADA) system. Managed Redhat Linux and Windows servers.
- Outcome: Successfully developed web-based application for Sporting Wheelies and Disabled Association using PHP. Assisted in the deployment of Linux Terminal Services based call-center set-up for the Sporting Wheelies and Disabled Association. Managed Sendmail e-mail server. Managed WuFTP File Transfer Protocol (FTP) server. System administration and networking of Windows NT, Windows 98, Windows Me, Windows 2000, and Windows XP desktop.
- Projects:
  - Server Upgrade: Assembled server hardware and configured server. Used Redhat Linux, IPchains, Samba, Squid and custom bash script to backup to tape. Delivered and installed server to Strong Force site in Sydney.
  - ICQA Infrastructure: Assembled server hardware for International College Queensland Australia (ICQA). Used Redhat Linux, IPchains, Samba, Squid, and custom backup script. Installed server on-site.

## QSI Payments Inc., Brisbane, Australia.

4<sup>th</sup> Dec 2000 – 23<sup>rd</sup> Nov 2001 (11 months)

### Software Engineer

- Requirement: Software engineer to develop software in Java, and perform unit, integration and some system testing.
- Role: Member of the Research and Development team working on the Internet Credit Card Payment Gateway.
- Outcome: Successfully developed software using Java with JUnit unit testing and Apache Ant for continuous build and integration testing.
- Projects:
  - QSI XML Validation Framework: Assisted in the software development, unit and integration testing of an Extensible Markup Language (XML) based validation framework to validate data input the QSI Payment's Internet Credit Card Payment Gateway for MasterCard.





Marinoc Pty. Ltd., Brisbane, Australia.

28<sup>th</sup> Oct 1999 – 1<sup>st</sup> Jun 2000 (8 months)

**Junior Information Technology Engineer (Part-time)**

- Requirement: Software developer.
- Role: Developed web-based software using PERL.
- Outcome: Successfully developed web-based CGI application using PERL on Redhat Linux development environment then migrated to BSD Unix production environment.
- Projects:
  - KnowMail – Successfully developed a PERL based CGI application for sending research links to subscribers. Deployed KnowMail application on BSD Unix servers.