31-3459 Wilkie Ave.
Coquitlam, B.C.
V3B 0E6, Canada

Resume – Rui Pereira

B.Sc. (Hons), CISSP, CISA, CPTE/CPTC
Procyon Security Group

Mobile: 1 (604) 961 0701
E-mail: rpereira@procyonsecurity.com

Synopsis

- Over 35 years of professional experience in most aspects of Information Technology, in a wide range of industries and disciplines; specializing in IT Security and Audit for the last 20 years;
- CISSP, CISA and CPTE/CPTC (pen-test) and CWSP (wireless) certified; CIPS ISP (retired)
- Member Vancouver Security SIG (past chair), Westcoast Security Forum (past chair), ISACA and OWASP (past chair, Vancouver Chapter);
- Expertise in IT Security, incl. penetration testing (ethical hacking) and vulnerability assessments, incl. applications, wireless networks and cloud services (Amazon & Azure)**;** Threat / Risk Assessments; Compliance and Privacy, incl. PCI DSS; Firewalls; Intrusion Detection / Prevention (IDS/IPS); Wireless audit and survey; training, incl. course development;
- Extensive experience with Windows and UNIX / Linux Operating Systems;
- Broad knowledge of communications systems and Local and Wide Area networking, including wireless;
- Solid database background: Microsoft SQL-Server, Oracle, MySQL, Informix, Sybase and DB2.

Work History

July 1998 – present, Principal Consultant, WaveFront Consulting Group (WCG)

(The WCG joined the Procyon Security Group partnership in January 2012; history pre-1996 has been omitted.)

- Web application (incl. web services), database and network security assessment (incl. exploitation) for Alberta Health Services (AHS; 2017 – 2019);
- Web application security (incl. APIs); penetration testing & vulnerability assessments, incl. wireless networks; and assistance with incident response planning - for BC Land Title and Survey Authority (LTSA / Landsure) (2015 – present);
- Review of IT security controls (incl. network, database, applications, wireless) for the Public Employees Benefits Agency (PEBA), Ministry of Finance, Government of Saskatchewan; ad hoc security consulting, application and network testing (2012 – present);
- External penetration test (network, 50+ applications, wireless networks, social engineering, Denial of Service (DoS) for large local municipal government (2014-2015);
- Network penetration and exfiltration testing for BC Ministry of Health (MoH) (2017 - 2018);
- Security consulting for the BC Liquor Distribution Branch (LDB) - Penetration Testing and Vulnerability Assessments (PCI and non-PCI); Assistance with PCI DSS efforts, incl. threat modeling and penetration testing; firewall and router audits; security assessments of Special Occasion Licenses Online (SOLO), Oracle Financials, Vendor Facing Web, Liquor Inspection Support, Wholesale Order Management, Store Ops, Web Store, and other systems; wireless security assessment & remediation; secure Linux and Windows server deployment; assistance with Identity Management strategy; Security review for IDS deployment; architect & deployment of secure remote access facilities (2001-2011, 2014 - present);
- Penetration testing for PCI DSS compliance for BC Transit (2012-2013), BC LDB (above), College & Association of registered Nurses of Alberta (CARNA, 2016-2019) and Pacific Blue Cross (2015). The Blue Cross work included thick client and mobile (smartphone) applications;
- Security architecture design, threat modeling and security testing of web applications; security assessments, pen-tests and incident response (Top Producer Systems / Move Inc.) (2005-12);
- Web Application Security Assessments, Training, Architecture Design & Security Consulting for BCIT (BC Institute of Technology); IAP Life; BC Ministries of Health, Social Services, Finance and Citizen Services; WPS-Disaster Recovery; Best Buy / Future Shop; Pro-Training / Yardstick); Simon Fraser University; BC College of Registered Nurses (CRNBC); BC Campus; Pacific Blue Cross; HY Louie (IGA); BC/Yukon Panorama public health project; BCMoH iEHR/PLIS Deployment Project; Provincial Health Services Authority (PHSA); Pathways (online resource for family doctors); (2000 – present);
- Security Reviews, Vulnerability Assessments & Penetration Tests (incl. wireless and applications) for the BC Medical Association (BCMA); BC Ministry of Health (MoH); the Colleges of Registered Nurses of BC (CRNBC); Yukon Govt. & College; nZone Media; Mark Anthony Group; Ministry of Citizens Services; Workers Compensation Board (Alberta); General Fusion; Harper Grey; various forestry companies and municipalities, etc. (1998 - present);

Work History	• Assistance with PCI DSS compliance for several organizations, incl. Vancouver Aquarium and Great Canadian Railway (2010 - present); • Security Architecture Design, Penetration Testing and Security Reviews for Citadel Commerce (Internet Payment Gateway) - Reviewed security issues and developed a prioritized security plan to address gaps; Provided guidance on security controls and policy development; worked on bank clearing- house systems and cryptographic processes (Canada/US); wireless networks; legal and services provider compliance requirements (Visa, MasterCard, STAR, NACHA, PCI, FSA); disaster recovery/ business continuity planning (BCP/DRP); application and network penetration testing (2004-08); penetration testing (internal, external, web applications and services) (as Paramount Commerce, 2018 - present); • Threat-Risk Assessments (STRAs), consulting - BC Health Authorities, Ministry of Health (2008-16); • Information Security Coordinator at Emergency Communications for South-Western BC (E-Comm) – assistance with security requirements, including network security architecture, policy design and reviews, Threat/Risk Assessments, mobile and wireless security, IDS deployment, Disaster Recovery/ Business Continuity, VPN's, application security assessments, two-factor authentication, encryption and remote access, password and user management; liaison with Vancouver, Victoria and other police departments, RCMP, BC Ambulance Services, Public Safety and Law Enforcement agencies (2000-6); STRA (2013); • Security Assessment for Stockgroup Systems – Reviewed IT security issues, developed plan for the remediation of high risk findings (2007); similar process for the Comox Valley Airport Authority (2011); • BC Ministry of Human Resources(MHR) – define security needs; liaise with IT, application development, business areas, privacy and other groups; auditing, compliance and investigations; security architecture design & implementation; application security reviews & Privacy Impact Assessments (PIA's) (2000-2); • Wireless surveys, pen-tests and security architecture consulting for BC Common IT Services (CITS), Ministry of Management Services (2002-2005); Wireless survey for Simon Fraser University (SFU; 2006); • ICBC (Information Security and UNIX Support) – router, firewall and web server/ proxy deployment and administration; security reviews and audits; policy and strategy facilitation; e-business security architecture and implementation (incl. mainframe connection); user and password management (single sign-on and platform migrations); log analysis and consolidation; system hardening; needs assessments and privacy consulting; project management and budgeting; application security reviews**;** firewall / DMZ deployment and testing; forensic investigations (1998-2000); application and network security testing, including annual external penetration testing (2018-2020). • Forensics investigations (2010-12); Develop forensics investigation process for Northern Health Authority (2013); Assistance with development of Business Continuity Plans (BCP/DRP) (2006-2014); Security consulting for various organizations, including assistance with breach management; assess of device security for NeuroCatch (2017) and CARNA (2018). • University of BC (UBC), BC Institute of Technology (BCIT), Mile2 and others (ongoing) – Security course development & training (Security+, Wireless, Cryptography, Cybercrime, Windows, Privacy, Web Application Security, Disaster Recovery/Business Continuity, Penetration Testing/Ethical Hacking); • Security presentations for various groups including PIA-BC, CIPS Security SIG, OWASP Vancouver, VaNTUG, VanLUG, Drupal User Group, APCO/NENA, IAFCI, BCIT, UBC, Nexient / Mile2, etc. (ongoing)
	June 1997 – June 1998, Technical Specialist, Mainland Information Systems Projects included Tivoli Storage manager (ADSM) installation and support (IBM sub-contract), network design and implementation, storage management, disaster recovery, penetration testing and vulnerability assessments, firewall implementations, database administration, and UNIX and Informix support.
	November 1996 – May 1997, Consultant, RGC Consulting • Security evaluation for VanCity Mutual Funds, incl. penetration testing. • Consultant with ICBC, working as UNIX/Internet Security Specialist assisting the corporation's migration from mainframe to client-server systems; firewall penetration testing (as part of firewall deployment).

Training	*2016 - Joint Cyber Security Conference (1 day)* — *New York, USA* *2013 - Athcon Security Conference (2 days)* — *Athens, Greece* *incl. Windows Exploit Development Course (Corelan) (2 days)* *2012 - ShakaCon Security Conference (and again in 2017)* — *Honolulu, Hawaii* *2009 - Certified Wireless Security Professional (CWSP) (re-certified in 2012)* — *CWNP* - OWASP AppSec-DC Conference and associated training (4 days) - Washington DC - European e-Identity Management Conference (2 days) - London, UK **2008 -** *RSA Security Conference (5 days) –* — *San Francisco, USA* - Certified Penetration Testing Engineer / Consultant (CPTE/CPTC) (6 days) - Tampa, USA - Annual Security and Privacy Conference - Victoria, BC *1998-2007* **-** Westcoast Security Forum (and again in 2016) — Vancouver, BC Annual 1-2-day conference (committee member 2000-4, chair in 2003) *2006* - Annual PolCyb (Policing Cyberspace) Conference – Richmond, BC *2005* - Certified Wireless Network Administrator (CWNA) – *CWNP* - Designing Security in a Windows 2000 Network – University of British Columbia *2004 – Certified Information Security Auditor (CISA) –* *ISACA* ***2001 -*** *Blackhat Briefings (2-day conference); Defcon9 (3-day conference) -* *Las Vegas, USA* - NT Intrusion Detection and Complete Windows 2000 Security Workshop (1 day each) - Las Vegas, USA *2000* - Intrusion Detection Systems, 2 days - MIS Training Institute, Vancouver, BC *1999* **-** Entrust 4 PKI Administration, 2 days - Geotrain, Vancouver, BC - Information Systems Professional (I.S.P.) certification – Canadian Info. Prof. Society (CIPS) - Certified Information Systems Security Professional (CISSP) certification – $(ISC)^2$ *1983* — University of Cape Town, South Africa - Bachelor of Science (Honors) degree in Computer Science/Applied Statistics (4 years).
Skills	• Solaris / Oracle, IBM AIX, HP-UX, Free & OpenBSD, Digital, Redhat & other Linux / UNIX distributions; • Microsoft Windows, Exchange, SharePoint, Terminal Server / Citrix, Office, Active Directory (AD), IIS; • Microsoft, Citrix, VMWare, Oracle, Docker and other virtualization technologies; • Security tools: NMap, Nessus / OpenVAS / Qualys, NeXpose, Retina & Nipper scanners; Metasploit Framework; Core Impact; Wireshark & TCPDump; Scuba Database Scanner; Immunity Debugger; • Post-exploitation tools like MimiKatz, Empire, PowerSploit, CrackMapExec, etc.; • Social Engineering tools like GoPhish and the Social Engineer Toolkit (SET); • Kali and BlackArch Linux security distributions; Flare and Commando Windows security distributions; • Password cracking tools like John the Ripper, Hashcat, Ophcrack, Hydra, NCrack and Cain&Abel; • Wireless security tools: Kismet, aircrack-ng, AirMagnet, Vistumbler, WiFi Scanners (various), etc.; • Penetration Testing & Vulnerability Assessment methodologies, incl. OSSTM, NIST, PCI and OWASP; • Application security tools: IBM / HCL Appscan, HP WebInspect, AppDetective, Syhunt Sandcat, Fiddler / Watcher, OWASP ZAP, Burp Proxy, sqlmap, SOAPUI, PostMan, Ready! API, browser add-ons; etc.; • Android mobile app testing tools: Genymotion. Android SDK, QARK, ADB, Drozer, etc.; • Firewalls, including CheckPoint, Cisco, WatchGuard, Juniper and Linux (IPTables); • Web Application Firewalls / WAFs (mod_security, mod_evasive, Citrix NetScaler, Barracuda, Incapsula); • Cisco, HP and Juniper routers and switches; • Intrusion Detection Systems (IDS) like Snort and Cisco Secure IDS/MARS; • Some experience with DDoS mitigation technologies from CloudFlare and Imperva; • Security technologies like RADIUS, PGP, S/MIME, VPNs, SSH, Tripwire, 2-factor authentication (2FA), biometrics, PKI, identity management, etc.; Web automation tools such as node.js and puppeteer; • Databases, including Microsoft SQL Server, mySQL, Oracle, Informix, DB2, Sybase and Postgres; • Programming languages such as C, VB and python; • Legal, privacy, compliance & audit standards: FIPPA, PIPEDA/PIPA; Breach Disclosure; Canadian Criminal Code; ISO 27001/27002, COBIT; PCI DSS;