

**TECHNOLOGY RISK
MANAGEMENT SERVICES
FOR AN INTERNETWORKED
BUSINESS WORLD**

**Do you know where your
data has gone today? And
do you know who took it?**

What are the threats to your data and systems? What is credible, what is hype, what have you missed? What would a privacy or security breach cost your organization? What are your legal and contractual duties to protect confidential private, financial and medical information? Just how secure are your systems and sensitive information? Really?

What you don't know **can** hurt your business! Visit us at www.wavefrontcg.com to see how we can help you answer these questions. Then contact us at ruiper@wavefrontcg.com or (604) 961-0701.

**GENERAL SERVICE
AREAS**

Security Reviews

Vulnerability Assessments;
Ethical Hacking / Penetration
Testing; Audits; Wireless & Web
Application Security

Security Architecture

Design, Implementation &
Review; Network, System &
Application Security

Risk Management

Threat / Risk Assessments
(TRA); Control Selection &
Deployment

Compliance Services

PCI DSS; SOX; Digital Forensics;
Privacy Impact Assessments
(PIA) & Reviews

Security Training

User Awareness Programs;
Training Courses; Skills Transfer

Policies & Procedures

Development & Review

Specialized Offerings

Wireless Surveys & Rogue AP
Detection; Disaster Recovery &
Business Continuity Planning;
Security Investigations

WAVEFRONT

Consulting Group Ltd.

2029 Turnberry Lane • Coquitlam • British Columbia
Canada • V3E 3N2

1 604 961-0701 • ruiper@wavefrontcg.com • www.wavefrontcg.com

Company Profile

The WaveFront Consulting Group (WCG), established in early 1998, is dedicated to helping organizations large and small protect their systems and data. Our assessment, design, implementation, review, training, and security awareness services allow organizations to conduct business without fear of the unknown. By understanding the technology risks that they face in an increasingly inter-networked and dangerous world, organizations can focus their efforts on getting business done.



Our Consultants have solid industry certifications and business experience to ensure that projects run smoothly and professionally, and are completed correctly, on time and within budget. Some of us have been doing this for over 20 years, so we know what we're doing!

We believe that Information Security is fundamentally a business issue, and we put business risk at the heart of our consulting approach. This allows us to get to the root of what really matters to the organization, and it means that we don't get hung up on the technology.

Professional, thorough, independent and affordable. Especially given the current business climate, you should contact us today to see how we can help you manage your technology and business risk.

Rui A. Pereira, B.Sc.(Hons), CIPS ISP, CISSP, CISA, CWNA/CWSP, CPTS/CPTE
Principal Consultant, WaveFront Consulting Group Ltd.
ruiper@wavefrontcg.com | www.wavefrontcg.com | (604) 961 0701

TRAINING SCHEDULE - 2009

Secure Web Application Development and Testing* (4 days)

Victoria BC - February 24 - 27

Vancouver - April 28 - May 1

Calgary AB - TBD

Ethical Hacking, Penetration Testing and Vulnerability Assessments* (4 days)

Victoria BC - March 3 - 6

Vancouver BC - May 5 - 8

Wireless Network Security Complete (3 days)

Cyber Ethics and Professionalism (2 days)

* Please turn over page for a brief outline.

Consult <http://www.wavefrontcg.com/Training.html> for full course outlines, schedule updates, other training offerings and additional information. To enroll call Rui at (604) 961 0701 or e-mail ruiper@wavefrontcg.com.

Helping to Secure the Digital Frontier!

Course: Secure Web Application Development and Testing (4 days)

The Internet may be a great place to do business, but it is also a dangerous place. According to recent Symantec Internet Threat Reports, 66% of disclosed vulnerabilities affect Web Applications. In 2007, Sophos Labs discovered a new infected webpage every 14 seconds – in 2008 that figure dropped to one in every five seconds - and 79% of these infected sites were legitimate websites! Cyber-criminals are always looking for ways to make easy money, and insecurely coded Web Applications provide effortless pickings. Given that most organizations are not even aware of the problem, this is a disaster waiting to happen. And it has already happened to many high profile organizations - see <http://www.webappsec.org/projects/whid/byyear.shtml> for a year-by-year tally.

This course aims to provide web application developers with an understanding of application security issues and attack vectors, and the skills necessary to code defensively against such attacks. We show how hackers can abuse web applications using techniques like SQL Injection and Cross-Site Scripting (XSS), and what developers can do to prevent this. We also show how developers and testers can test their own applications in order to determine if they are susceptible to web application attacks. This material would be of interest for software developers and testers (QA/QC); system, network and database administrators; software, network and system architects; IT Security staff; and Compliance Officers (Privacy, SOX, PCI, etc.). Addressing web application security issues is a key PCI DSS compliance requirement for organizations handling credit card information.

This is a hands-on course with several labs and exercises, where the information presented in the lectures is tested in practice. Secure coding examples are discussed, but in-depth software development expertise is not a pre-requisite for attending the course.

Course: Ethical Hacking, Penetration Testing and Vulnerability Assessments (4 days)

Hardly a day goes by without news of yet another computer security incident: viruses, worms, Trojans, spy-ware; identity theft; stolen credit card numbers and medical records; denial of service attacks; disclosure of private information; Phishing and Pharming attacks; Bot-nets and Zombies; yet more security alerts and exploits; drive-by hacking; etc. Organizations and individuals are advised to take security precautions against this stream of attacks, from firewalls and VPN's, to Anti-virus software and patching. Yet, despite all such precautions, these attacks continue unabated. Cyber-crime remains a plague on the Internet, causing millions of dollars of losses each year. Just how do the script kiddies, hackers, cyber-criminals, hacktivists, and their ilk do it?

This hands-on course (lectures and labs) is based on Sun Tzu's principle that knowing the enemy (hackers) and their techniques, can be very useful in defending our networks and systems against them. After all, it is better for us to find the vulnerabilities in our own systems (and fix them) before the hackers and cyber-criminals find the same vulnerabilities and exploit them. Penetration testing (aka. Ethical Hacking) allows us to simulate hacker attacks, thereby testing our own defenses to ensure they are adequate to the task.

This course describes the major hacking techniques, and shows both how to exploit network & system vulnerabilities, and how to protect against them. With this enhanced understanding of hacking techniques and tools, students are in a better position to appreciate the hacker threat, and better equipped to defend their organizations against them. Vulnerability assessments and penetration testing are key PCI DSS controls for companies handling credit card information. This course is intended primarily for security professionals, auditors, and system and network administrators. Compliance Officers (Privacy, SOX, PCI DSS, etc.), and network and system architects will also benefit.

Rui Pereira, B.Sc (Hons), CISSP, CIPS ISP, CISA, CWNA/CWSP, CPTS/CPTE Principal Consultant, 'Chief' Trainer

Rui has over 25 years of professional experience in most aspects of Information Technology, specializing in IT Security and Audit for the last 13 years. He has consulted for a variety of industries, incl. Insurance, Retail, Financial Services, Law Enforcement and Public Safety, Local and Provincial Governments, Managed Security Services, e-Commerce, Tourism, Health Services, and Education. Customers include ICBC, various BC and Alberta Provincial Government agencies, E-Comm, the BC Liquor Distribution Branch, Top Producer, Pro Training, University of BC and Simon Fraser University, Provincial Health Services Authority, Citadel Commerce, etc. Rui brings a wealth of management and technical expertise to the projects he tackles, as well as a willingness to do what it takes to make any project a success.



Rui has a B.Sc. (Hons) degree in Computer Science and Statistics from the University Of Cape Town, South Africa. He has obtained the Computer Information Systems Security Professional (CISSP) certification from (ISC)², which attests to his experience and skills in IT Security. He is a Certified Information Systems Auditor (CISA), and has the Canadian Information Professional Society (CIPS) Information Systems Professional (I.S.P.) certification. The latter is a professional designation in the Canadian provinces of Ontario, Alberta and BC, among others. He also has Enhanced Security Clearance, as determined by the RCMP, Canada. Technical certifications include CWNA/CWSP (Wireless Security), and CPTS/CPTE (Penetration Testing / Ethical Hacking).

Rui has been directly involved in the Information Security community in Vancouver for many years, and was a committee member of both the CIPS Security SIG and WestCoast Security Forum, as well as being the Webmaster for both groups. He was the Chair of the West-Coast Security Forum in 2003, which attracted over 500 delegates. When not consulting Rui lectures on security topics at UBC and BCIT, and presents his own courses under the WaveFront banner. He has presented papers before the IAFCI, Vancouver Linux Users Group (VANLUG), CIPS Security SIG, Vancouver NT Users Group (VANTUG), IT4BC and other organizations.