

# WELCOME TO the 10<sup>th</sup> WEST COAST SECURITY FORUM

**Join our renowned delegation of information security specialist in beautiful Vancouver, B.C. for the 10th West Coast Security Forum – “Information Everywhere - Protecting New Perimeters”**

**WHEN: November 19 - 20, 2007**

**WHERE: Sheraton Wall Centre, Vancouver, British Columbia, Canada**

**ON-LINE REGISTRATION: <http://www.wcsf.com>**

## **Who Should Attend**

- **CIOs, CSOs, CISOs, and CTOs**
- **IT vice-presidents and directors**
- **Network and system managers**
- **Risk managers and Auditors**
- **Senior business executives**
- **Anyone involved in enterprise-wide or information security**

## **“Information Everywhere - Protecting New Perimeters”**

The growing presence of computers of all shapes and sizes in almost every aspect of our lives has generated a great number of potential advantages, but is also raising new concerns with respect to security and privacy. Tougher safeguards are needed as new security perimeters are needed to protect information in an ever changing world in which users, small enterprises, large conglomerates and governments increasingly have the need to share information. Computing technologies are woven into the fabric of our everyday lives offering a multitude of functions with networking capabilities seeking out and communicating with other devices - often transparent to the user. Information security is fast becoming the foremost concern of many organizations and the individual, whether it is to protect valuable corporate information, your personally identifiable information, or even to ensure your kid is safe on the Internet.

A different approach is needed to protect these new security perimeters and finding the balance of enabling controlled access whilst protection valuable information assets. New threats challenge us in the form of intelligent hackers, bot-herders, virus writers, script-kiddies, corporate spies, organized crime bosses, and even journalists who see new opportunities to grow rich off of these relatively unprotected network assets. The potential for loss for the individual and the organization and the corporation has never been greater - whether through malicious attacks or data loss through accidents or theft.

Our conference provides a fresh perspective and new insights into the increasing complexity of the world that you are charged with protecting, as well as highlighting new opportunities to enhance services and access to information. Come out and meet your fellow professionals and exchange information in a friendly surrounding while learning from the people who are on the edge of the 'New Perimeters'.

## Call for Papers - Backgrounder

The 10<sup>th</sup> West Coast Security Forum will be held in Vancouver, B.C. November 19 -20, 2007 and original papers on all aspects of information security are solicited for submission. Areas of interests include but not restricted to:

Theme	Scenario
<p><b>Technology for protecting new perimeters</b></p>	<p>Computers are becoming ubiquitous and have become woven into the fabric of our everyday lives. The potential advantage of ubiquitous access to information has created new challenges to secure information at home, on the road, at the office, within governments.</p> <p>New security threats require a new approach to security – new tools, new technologies and new techniques.</p> <p>Key issues:</p> <ul style="list-style-type: none"> <li>▪ Authorization and Authentication</li> <li>▪ Biometrics</li> <li>▪ Cryptography</li> <li>▪ Smart Cards</li> <li>▪ Identity &amp; Access Management</li> <li>▪ Intelligent tokens</li> <li>▪ Intrusion Detection</li> <li>▪ Security Solutions</li> <li>▪ Patch management</li> <li>▪ Service Oriented Architecture</li> <li>▪ Hackers</li> <li>▪ Security threats</li> <li>▪ Network Security</li> <li>▪ Fraud Detection</li> <li>▪ RFID Security and Privacy</li> <li>▪ Security Issues for Ubiquitous Systems</li> </ul>
<p><b>Extended perimeters - securing the business-to-business collaboration perimeter</b></p>	<p>In conducting business-to-business (B2B) electronic commerce over the Internet, organizations effectively extend their security perimeter to other organizations. By definition this means that organizations share each other's security requirements. However, each organization may have different security requirements, policies, and technical standards, making it difficult to come to agreement. Other options, such as joining a trading exchange might exclude interoperability with parties that do not join the exchange or adhere to the standard.</p> <p>Key issues</p> <ul style="list-style-type: none"> <li>▪ E-Commerce security</li> <li>▪ Security of small to medium size enterprises</li> <li>▪ Certification and accreditation</li> <li>▪ Evaluation of Information Security in companies</li> <li>▪ Information security surveys and case studies</li> <li>▪ Security and Privacy aspects of Electronic Government (e-Government)</li> <li>▪ Internet Dependability</li> <li>▪ Secure service-oriented B2B</li> <li>▪ Online collaboration architectures</li> </ul>

<p><b>Broken perimeters</b> – prevention, response and recovery</p>	<ul style="list-style-type: none"> <li>▪ Secure Enterprise Architectures</li> </ul> <p>Responding to security breaches and emergencies forms an important part of any organization's security posture. Planning for events, whether as drastic as an earthquake, as common as a virus infiltration, or as dangerous as a terrorist attack, assists in minimizing the impact of such events. In this theme we will explore aspects of planning, responding and recovering to events which have compromised our security perimeters, both physical and electronic.</p> <p>Key points:</p> <ul style="list-style-type: none"> <li>▪ Availability and Reliability</li> <li>▪ Backup strategies</li> <li>▪ Business Impact Assessment</li> <li>▪ Business Continuity Management</li> <li>▪ Disaster Recovery</li> <li>▪ Emergency Response</li> <li>▪ Forensics</li> <li>▪ Encryption</li> <li>▪ Incident Handling</li> <li>▪ Physical security</li> <li>▪ Storage</li> </ul>
<p><b>Mobile perimeters</b> - protecting the perimeter of the road warrior</p>	<p>Road Warriors need access to information wherever they find themselves - the office, at home, and on the road. Not only do they carry sensitive information with them on their laptops and PDAs, but they often need to connect to your network from unsecured locations, leaving them vulnerable to a host of threats. The Road Warrior remains one of the security professional's biggest challenges.</p> <p>Key issues:</p> <ul style="list-style-type: none"> <li>▪ Acceptable use</li> <li>▪ Authentication</li> <li>▪ Digital certificates</li> <li>▪ Email issues</li> <li>▪ Encryption and VPN</li> <li>▪ Firewalls &amp; Perimeter Protection</li> <li>▪ Home and Small Office</li> <li>▪ PDAs and other mobile devices</li> <li>▪ Telecommuting</li> <li>▪ VOIP Issues</li> <li>▪ Wireless Access</li> </ul>
<p><b>New Perimeters</b> – Risk and Regulatory</p>	<p>Security no longer sits on the security professional's desk alone. New requirements are necessitating risk assessments and compliance reporting now a corporate responsibility. This has raised information security to an agenda item on board meetings.</p> <p>Key issues:</p> <ul style="list-style-type: none"> <li>▪ Security policies and governance</li> <li>▪ Security awareness and training</li> <li>▪ International standards for Information Security Management</li> <li>▪ Legal issues</li> <li>▪ Risk management</li> <li>▪ Consumer Protection</li> <li>▪ Policy &amp; Government</li> </ul>

	<ul style="list-style-type: none"> <li>▪ Security and Privacy in E-Health</li> <li>▪ Law &amp; Liability</li> <li>▪ Auditing &amp; Assessment</li> <li>▪ Digital Privacy</li> <li>▪ Legislation</li> <li>▪ The role of government and law enforcement</li> <li>▪ Standards, Guidelines and Certification</li> </ul>
<p><b>Inside the Perimeter –</b> protecting against the internal threat</p>	<p>Security experts will agree that perhaps the most overlooked threat in a security program is the threat posed by employee behavior. Whether malicious or a simple error, the results are often severe and can cripple an organization.</p> <p>Key issues:</p> <ul style="list-style-type: none"> <li>▪ Segregation of duties</li> <li>▪ Security organization</li> <li>▪ Security governance</li> <li>▪ Internal controls</li> <li>▪ Social engineering</li> <li>▪ Security policies and governance</li> <li>▪ Security awareness and training</li> <li>▪ Employee background checks</li> <li>▪ Disgruntled employees</li> <li>▪ E-Mail and Web filtering</li> <li>▪ Patch management</li> <li>▪ Intrusion detection</li> <li>▪ File monitoring</li> <li>▪ Identity Management</li> <li>▪ Data Encryption</li> <li>▪ IM and Chat Rooms</li> </ul>

The 10<sup>th</sup> West Coast Security Forum seeks submissions solutions that present information, research or hands-on guidance on the following, but are not limited to, topics of security and privacy. We will be selecting the best papers and presentations to be given at our conference in person, as well as publishing other submissions on the conference materials disk that will be provided to conference attendees.

### Submission Guidelines

- **Briefing papers:** Short briefing paper need not be extensive. An executive or management briefing on an aspect of security would be enough. Such papers will be presented for evaluation and typical length would be around 1500-2000 words. Selected papers will be also given as presentations at the conference.
- **Case Studies:** Case studies are typically descriptions of a given security situation. Names of organizations can be kept anonymous to maintain confidentiality. Typical length would be around 5000-6000 words.
- **Seminars:** The second day of our conference will be devoted to longer sessions which can be used to deliver more information in a seminar format, typically 1.5 to 3 hours. If you would like to provide a detailed seminar, please provide the topic outline, and the types of information that attendees will learn.

- **Research papers:** A research paper can be longer and included detailed information about to about 10,000 words. These will be published in the conference materials.

If you would like to be on one of our panels, please indicate this and the area which you are interested in.