



**The Geneva Security Forum &
ITU Telecom, World 2009**

***Open Networks-Connected Minds
5-9 October, Geneva***

We are delighted to inform you about the Geneva Security Forum's partnership with the ITU in the preparation of Telecom, World 2009 and hope that you will be able to join us at the beginning of October in Geneva. Please follow this link for further program details and registration information. <http://www.itu.int/WORLD2009/forum/index.html>

Since its successful launch in June 2007, the Geneva Security Forum has been actively furthering the global dialogue on cybersecurity issues, working closely with the ITU in the preparation of the cybersecurity stream for the World 2009 Forum. Please see the attached list of sessions (also available via the above link).

The GSF is both a partner of World 2009 and a member of the Forum Advisory Committee. This close relationship, supported by the Government of Geneva, has provided an opportunity for the GSF to help structure the development of the Forum program and to be involved in the shaping of the cybersecurity agenda 2009. Other components of the World 2009 Forum program include development issues, ICTs and climate change, access, technology foresight and new business models.

I look forward to seeing you at World 2009 and to enjoying this stimulating, thought-provoking Forum together.

With my best regards,

Daniel Stauffacher
President
Geneva Security Forum
www.genevasecurityforum.org
Tel: +41 79 459 7279



ITU Telecom, WORLD 2009
Cybersecurity

SEC.1 : Tackling cyberthreats: towards effective global partnerships
Tuesday, 06 October 2009, 11:00 - 12:30, Room B

No country or operator acting alone can ensure its own cybersecurity; global partnerships are necessary and unavoidable. The day-to-day functioning of the global economy, basic services, health programs and individual activities rely on efficient and fully operational Information and Communication Technologies.

KEY QUESTIONS: - How vulnerable is the system that is now the base of every service, transaction, communication and exchange required for the steady functioning of the global economy, security and individual well-being? - Is there a real risk? From who? What? What are the most vulnerable targets? - Did we learn from Estonia? - How are international multilateral cooperative mechanisms evolving? - What gaps still need to be filled?

This session has been prepared in cooperation with the Geneva Security Forum (GSF)

Moderator

* [Mrs Maria Livanos Cattai](#), Chair, Strategic Advisory Committee, Geneva Security Forum, Switzerland

Panellists

* [His Excellency Mr Juhan Parts](#), Minister, Ministry of Economic Affairs and Communications, Estonia

* [Mr Eugene Kaspersky](#), CEO and Founder, Kaspersky Lab, Russian Federation

* [Mr Mohd Noor Amin](#), Chairman, Management Board, International Multilateral Partnership Against Cyber-Threats - IMPACT, Malaysia

* [Dr Botaro Hirotsuki](#), Senior Executive Vice-President, NEC Corporation, Japan

* [Mr Carlos Solari](#), Vice President, Central Quality, Security, Reliability, Alcatel-Lucent USA, United States

* [Mr Abdulaziz Sager](#), Chairman, Gulf Research Centre, United Arab Emirates



SEC.2 : The real costs of cybersecurity
Tuesday, 06 October 2009, 14:30 - 16:00, Room E

One estimate is that cybercrime, stolen data and the associated repairs, cost business US\$1 trillion in 2008. Despite the countermeasures, there has been continuing rapid evolution in the malware "industry", such as the development of botnets to deliver spam, trojan attacks on social networks and phishing to obtain personal details for identity theft. New threats will require new spending to limit their effects.

KEY QUESTIONS: - How high can, or should, the costs of effective cybersecurity go? - What are the best (affordable) management tools to protect data, identities, the integrity of businesses, governments and individuals? - How do we persuade individuals to protect their computers and mobile phones? - Where will the next generation of cyberthreats come from?

This session has been prepared in cooperation with the Geneva Security Forum (GSF)

Moderator

* [Mr Richard C. Beard](#), Senior Deputy U.S. Coordinator, Department of State, International Communications and Information Policy (CIP), United States

Panellists

- * [Mr Pirkka Palomäki](#), Chief Technology Officer, F-Secure Corp., Finland
- * [Mr Alexander Seger](#), Head of Economic Crime, DG Human Rights and Legal Affairs, Council of Europe, EC
- * [Mr Jean-Pierre Therre](#), Chief Security Officer, Pictet & Cie, Bankers, Switzerland
- * [Mr Ross Anderson](#), Professor, Computer Laboratory, University of Cambridge, United Kingdom
- * [Mr Raj Puri](#), CEO, Yaana Technologies LLC, United States
- * [Ms Cristine Hoepers](#), Senior Security Analyst and General Manager, CERT, Brazil

SEC.3 : Managing digital identity: the good, the bad, the ugly
Tuesday, 06 October 2009, 16:30 - 18:00, Room E

Digital identities are central to modern life, in performing banking transactions, making purchases, obtaining medical treatment, not to mention building and maintaining your personal or corporate reputation. Identity theft has become a serious threat, both on the Internet and in data recovered from stolen or second hand discs and computers. Protecting corporate, customer, employee and personal digital identity is of critical



importance.

KEY QUESTIONS: - How should one properly protect critical data? - What tools are now available to protect digital identity and how best to implement them in your country or company? - How to implement and improve identity management processes?

This session has been prepared in cooperation with the Geneva Security Forum (GSF)

Moderator

* [Ms Deborah Taylor Tate](#), Former Commissioner, U.S. Federal Communications Commission, United States

Panellists

* [Mr Ron Williams](#), Senior Enterprise Architect, Security and Privacy, IBM Corporation, United States

* [Mr R Ramamurthy](#), Chairman, Cyber Society of India, India

* [His Excellency Mr Robert Hensler](#), State Chancellor, State of Geneva, Switzerland

* [Ms Jaya Baloo](#), Practice Lead Unified Communications, Professional Services NL, ME, A, Verizon Business, Netherlands

* [Mrs Kelly Richdale](#), VP International Sales & Managing Director International Operations, L1 - Enterprise Access Division, United States

* [Mr Pascal Thoniel](#), Chairman & CEO, NTX Research SA, France

SEC.4 : Best practices for cybersecurity: What should governments be doing for protecting children online?

Wednesday, 07 October 2009, 14:00 - 16:00, Room E

The expansion of the Internet has included and often been led by younger users sometimes with little, if any, parental oversight or guidance on the dangers of cyberspace. In some developed countries, children get their first mobile phone at eight years of age, allowing them in many cases uncontrolled access not only to text messaging but also to the Internet. Irresponsible use of cameras on PCs and mobile phones has compounded the danger, creating the practice of "sexting"; sending sexual images between children, which can be manipulated or intercepted. Pedophiles have been shown to be a significant threat to children, using the Internet to "groom" future victims and to exchange horrifying images. In addition, cyber-bullying, the indiscriminate use of "chat rooms" on-line, and the access to age-inappropriate content are growing problems. Children, lacking the experience and life-skills to manage deceptive situations make easy victims for predators.

KEY QUESTIONS: - What can be done to improve the tracking and prosecution of pedophiles? - What is the role of child-friendly safe zones? - How do we revise



legislation for computer-generated images and sexting? - Should there be an obligation to report images and sites? What other threats are children facing on-line? What can governments do?

Moderator

* [Mr John Carr](#), Executive Board Member, European NGO Alliance for Child Safety Online

Panellists

- * [Her Excellency Mrs Jasna Matic](#), Minister, Ministry of Telecommunications and Information Society, Serbia
- * [Mr Mohamed Sharil Tarmizi](#), Acting Chairman, Malaysian Communications and Multimedia Commission, Malaysia
- * [Ms Nenita La Rose](#), Executive Director, Child Helpline International, Netherlands
- * [Ms Natasha Jackson](#), Head of Content Policy, GSM Association, United Kingdom

SEC.5 : Interconnected and vulnerable: the weakest link in cybersecurity
Thursday, 08 October 2009, 16:30 - 18:00, Room E

The recent financial crisis has demonstrated to what extent the world is interconnected, integrated and interdependent. Continuous international transactions amongst individuals, companies and nations, and the constant flow of people and money around the world, bring not only positive economic benefits but also increased cyber-vulnerability. The cybersecurity net we have developed complete with firewalls, anti-spy and anti-virus software, is only as strong as the weakest link in the chain. How can we develop a truly global approach? How can developed countries and corporations contribute to the "cybersecurization" of developing countries who do not have the means or the expertise to implement responsible and adequate cybersecurity programs? What about the role of the individual?

This session has been prepared in cooperation with the Geneva Security Forum (GSF)

Moderator

* [Mr David A. Gross](#), Partner, Wiley Rein LLP, United States

Panellists

[Mr Bashir Patel](#), Director Programmes and Business Development, Commonwealth Telecommunications Organisation - CTO, United Kingdom



- * [Ms Jody Westby](#), CEO, Global Cyber Risk LLC, United States
- * [Mr Arkadiy Kremer](#), Chairman ITU-T SG 17 and Chairman, Russian Association for Networks and Services - RANS , Russian Federation
- * [Mr Basil Udotai](#), Managing Partner, Technology Advisors, ICT Lawyers & Consultants, Nigeria
- * [Mr Victor-Emmanuel de Sa](#), Strategy Director, Geneva Solutions SA, Switzerland