Defence iQ
a division of IQPC

PRESENTS

CYBER SECURITY 2011

BOOK AND PAY BY 11th MARCH 2011
SAVE UP TO €250!

VENUE: Le Plaza, Brussels, Belgium
MAIN TWO-DAY CONFERENCE: 31st May and 1st June 2011
PRE CONFERENCE WORKSHOPS: 30th May 2011

Gen/Flag officers 1* and above go for free

Protecting Critical National Infrastructure from the Cyber Threat

Conference highlights will include:

- Gain an insight into the **serious threats and IT incidents that governments are facing** and learn how to **monitor, analyse, detect and respond to cyber attacks** and unauthorised activities within your network
- Understand how nations such as the **United Kingdom, Germany, Sweden, Denmark and Norway** are improving their national cyber security through improved working **relationships with private sector companies such as BT and Barclays**
- Hear the latest **legal trends in cyberspace** arising from international incidents such as **Stuxnet and Conficker** and what they have meant for the rules surrounding aspects such as **data exchange, attribution, early warning and self-defence**

WORKSHOP: 30th May 2011: 14:00 – 17:00

CLOUD COMPUTING FOR THE 'EDGY'

Led by: Mary Ann Malloy, Principal Information Systems Engineer, The MITRE Corporation

MEDIA PARTNERS

SPONSORS

NETWITNESS

CISCO

Expert Speakers from across the world:

- **Paul Collacott, Deputy Director, Cyber Policy, GCHQ**
- **Dr Michael Pilgermann, Section IT 3 - IT-Security, Federal Ministry of the Interior, Germany**
- **Thomas Kristmar, Head of Danish GovCERT**
- **Malin Fylkner, Senior Advisor, Swedish Civil Contingencies Agency**
- **Michael Boyer, Director, RCERT Europe, US Army**
- **Dr. Christophe Birkeland, Director of NorCERT, Norwegian National Security Authority**
- **Dr Robert Nowill, Director of Cyber Security, BT**
- **Tim Hind, Global Head of Intelligence, Barclays Global Retail Bank (Technology)**
- **Don Proctor, Senior Vice President, Cisco Systems**
- **John Bumgarner, Chief Technologist, US Cyber Consequences Unit**
- **Gregory Radabaugh, Technical Director, Cyber Analysis Squadron, US Air Force**
- **Christopher Richardson, Burnham Lecturer, Defence College of Communications and Information Systems, UK MoD**
- **Eneken Tikk, Legal and Policy Branch Chief, CCD COE**
- **Dr. Steve Purser, Head of Technical and Competence Department, ENISA**
- **Michael Corcoran, Acting Head, MoD Cyber & Influence S&T Centre, UK MoD**
- **Geoff Harris, Management Counsel, Information Systems Security Association (ISSA) – UK**
- **Russell Buchan, School of Law, University of Sheffield**

TEL: +44 (0)20 7368 9373 FAX: +44 (0)20 7368 9377 EMAIL: team@iqpc.co.uk

Now in its second year, Cyber Security 2011 is Europe's leading cyber security conference. The event brings together the key actors involved in securing a nation's critical national infrastructure from a cyber attack including international organisations, national cyber security departments, CERT teams and private companies responsible for aspects of critical national infrastructure. With an expert crowd, this is your chance to leverage the global expertise of the cyber security community to assist in the major challenges facing your organisation such as the monitoring, detection and response to cyber attacks within your network.

PRE CONFERENCE WORKSHOP
MONDAY 30TH MAY 2011

14:00 – 17:00 CLOUD COMPUTING FOR THE 'EDGY'

Led by: Mary Ann Malloy, Principal Information Systems Engineer, The MITRE Corporation

Introduction:

"Edgy" means nervous! And a lot of us are really nervous about the risks we've heard come along with cloud computing. But an "edge" is also "a boundary condition," and in a cyber context, "edge users" are those who are at the boundary or limit of what the solution can handle. In other words, they have requirements that go beyond "typical user" profiles. As public sector and government organisations continue to move into the clouds, you have to ask the question, 'Which aspects of cloud computing make sense for your organisation?' Particularly for your "edge users" in light of their special requirements.

In this workshop, participants will evaluate:

- The state of cloud computing practice; Alternative paths into the clouds with use cases
- Edge user requirements, including security and privacy risks; What can be done to mitigate them
- How to gauge your organisation's "cloud readiness"
- How to use checklists and worksheets (provided) to profile users, establish migration plans and investment roadmaps

This will allow you to fully and properly assess which aspects of cloud computing are best suited to your organisation and its needs.

DAY ONE AGENDA
TUESDAY 31ST MAY 2011

8.30 Registration and Coffee

09.00 Chairman's Welcome and Opening Speech
Geoff Harris, Management Council, Information Systems Security Association (ISSA) - UK

09: 10 CYBER SECURITY – UK GOVERNMENT COMMUNICATIONS HEADQUARTERS ACTIVITIES AND ROLES IN THE DEFENCE OF UK INTERESTS
Paul Collacott, Deputy Director, Cyber Policy, GCHQ

09:50 CYBER SECURITY IN GERMANY – PROTECTING THE CRITICAL INFORMATION INFRASTRUCTURE

- Threat situation and need for action
- Shared responsibility: Strategies and objectives
- Implementation by engaging administration, industry and citizens
- How cyber security within Germany is likely to evolve in the future

Dr Michael Pilgermann, Section IT 3 - IT-Security, Federal Ministry of the Interior, Germany

10:30 Networking Coffee Break

11:00 NATIONAL RESPONSE PLAN FOR SERIOUS IT INCIDENTS: GUIDING PRINCIPLES FOR THE SWEDISH EMERGENCY MANAGEMENT SYSTEM

- What is considered a serious IT-incident?
- Roles and responsibilities
- Outline of the national response plan for serious IT incidents

Malin Fylkner, Senior Advisor, Swedish Civil Contingencies Agency

11:40 PREREQUISITES FOR STRONG NATIONAL COOPERATION ON CYBER SECURITY

- The sensitivity of incidents that take place on government or critical national infrastructure networks
- The problems that this causes for the exchange of information between the different actors in cyberspace
- How to overcome these concerns to create a culture of information exchange

Thomas Kristmar, Head of Danish GovCERT

12:20 BUILDING AN ARCHITECTURE OF TRUST - THE NETWORK'S ROLE IN SECURING CYBERSPACE

- This session provides an industry context for the market transitions occurring in cyber security, articulate the role of the network in defending our information and infrastructure, and offer a vision for how the network can enable a platform for innovation in cyber security going forward.

Don Proctor, Senior Vice President, Cisco Systems

13:00 Networking Lunch

14:00 ICT THREATS: HOW TO DETECT ATTACKS AND HANDLE INCIDENTS IN CLOSE COLLABORATION WITH THE PRIVATE SECTOR

- Examples of the serious threats that have targeted Norwegian critical national infrastructure
- Cyber espionage with targeted Trojans: Trends in technology and methods
- Cyber attacks, prevalent in all modern conflicts
- The use of a sensor network within critical national infrastructure for intrusion detection
- The success criteria for this sensor network
- International collaboration information exchange and trust

Dr. Christophe Birkeland, Director of NorCERT, Norwegian National Security Authority

14:40 COMPUTER NETWORK DEFENCE FOR THE US ARMY: MONITORING, ANALYSING, DETECTING AND RESPONDING

- Protecting the US Army's networks from cyber attack
- Monitoring the network for unauthorised activities
- Analysis and detection of cyber attacks
- Responding to a cyber attack against US Army networks

Michael Boyer, Director, RCERT Europe, US Army

15:20 Networking Coffee Break

15:50 THE EVOLVING THREAT IN CYBERSPACE: INFLUENCING YOUR BEHAVIOUR AND DECISION MAKING PROCESSES

- The current operational environment
- The evolving threat – How the adversary takes advantage of the operational environment
- The resulting consequences – How the threat will influence your behaviour and decision making processes

Gregory Radabaugh, Technical Director, Cyber Analysis Squadron, US Air Force

16:30 UNDERSTANDING THE 5TH DOMAIN'S VIRTUAL PLANE: AN EDUCATIONAL PERSPECTIVE TO THE COMPETENCES AND COMPLEXITIES OF CYBERSPACE

- Contextual awareness of cyberspace: The 5th domain
- Cyberspace Situational Awareness education
- Trains and planes of the 5th Domain
- Competences of the knowledge workers in cyberspace
- National occupational standards and an assurance framework

Christopher Richardson, Burnham Lecturer, Defence College of Communications and Information Systems, UK MoD

17:10 Chairman's Close

"Valuable; especially for gaining contacts"
Mike Corcoran, Cyber & Influence S&T Centre

"Very informative, useful and filled with country level design features"
Michael Boyer, RCERT Europe

Tel: +44 (0) 207 368 9373 **Fax:** +44 (0) 207 368 9377 **Email:** team@iqpc.co.uk

DAY TWO AGENDA
WEDNESDAY 1ST JUNE 2011

8.30 Registration and Coffee

09.00 Chairman's Welcome
Geoff Harris, Management Council, Information Systems Security Association (ISSA) - UK

09.10 COOPERATION IN SECURING CRITICAL NATIONAL INFRASTRUCTURE
- Introduction to ENISA and what we do
- ENISA's role in facilitating dialogue – Bridging public and private sectors
- The Critical Information Infrastructure Protection (CIIP) action plan
- Pan –European Exercises for resilience – Objectives and current status
- Engaging with ENISA – Opportunities and benefits
- The way forward

Dr. Steve Purser, Head of Technical and Competence Department, ENISA

09.50 A COMMUNICATIONS SERVICE PROVIDER'S PERSPECTIVE ON CYBER SECURITY: TECHNIQUES FOR IMPROVING CYBER DEFENCE
- The role of communications service providers in promoting cyber security
- Current challenges in providing security
- Working with those who use our services to improve cyber defence

Dr Robert Nowill, Director of Cyber Security, BT

10.30 Coffee and Networking Break

11.00 THE IMPACT OF THREATS ON A GLOBAL BANK AND CREATING A FEEDBACK LOOP ON CYBER SECURITY TO IMPROVE PROTECTION
- The common challenges and threats in securing a truly global network
- Efforts to share information on potential threats between banks
- Working with the government to create a feedback loop on cyber security

Tim Hind, Global Head of Intelligence, Barclays Global Retail Bank (Technology)

11.40 THE DIGITAL FLEECING OF OUR PHYSICAL WORLD: ANALYSING CYBER CRIME AND PROTECTING THE PUBLIC
- How prevalent is international cyber crime?
- How invasive are phishing and vishing operations?
- How do you protect the public on the Internet?
- How will cyber crime evolve in the future?

John Bumgarner, Chief Technologist, US Cyber Consequences Unit

12.20 Lunch and Networking

13.30 COMBATING THE INSIDER THREAT: PERSONNEL SCREENING, PROTECTIVE MONITORING TECHNOLOGIES AND FORENSIC READINESS
- Examples of high profile insider attacks and their impact
- How others have been prevented with the help of the police authorities and the greatly improved technical capabilities that they have now developed
- What measures should financial organisations be deploying to reduce the risk of being victims to such attacks?
- Personnel screening, protective monitoring technologies and forensic readiness as some of the key means by which to reduce the incidence of insider attacks

Geoff Harris, Management Counsel, Information Systems Security Association (ISSA) - UK

14.10 CYBER & INFLUENCE: THE WAY AHEAD FOLLOWING THE 2010 STRATEGIC DEFENCE & SECURITY REVIEW
- From a science and technology perspective
- Now a tier 1 risk (from National Security Strategy)
- SDSR cyber security aspects
- The cyber space domain
- Cyber space as an enabler of Influence
- Evolving science and technology priorities

Michael Corcoran, Acting Head, MoD Cyber & Influence S&T Centre, UK MoD

14.50 Coffee and Networking Break

15.20 THE '10 RULES' FOR LEGAL TRENDS IN CYBER SPACE, DERIVED FROM INTERNATIONAL INCIDENTS, INTERNATIONAL LAW AND STATE PRACTISE
- The rules surrounding aspects such as data exchange, attribution, early warning and self-defence
- The impact of international incidents such as Stuxnet, Conficker, Estonia and Georgia
- How these rules are likely to develop and efforts to create a rule of law in cyberspace

Eneken Tikk, Legal and Policy Branch Chief, Cooperative Cyber Defence Centre of Excellence (CCD CoE)

16.00 THE APPLICATION OF INTERNATIONAL LAW AND THE USE OF FORCE TO THE STUXNET VIRUS: IRAN 2010
- An overview of the Stuxnet virus that was deployed against Iran in 2010
- Did the Stuxnet virus constitute an unlawful use of force against Iran for the purpose of Article 2(4) the United Nations Charter?
- Did the Stuxnet attack constitute an 'armed attack' for the purpose of Article 51 of the UN Charter, thus enabling Iran to lawfully use force in self-defence?
- The question of attribution: What if the Stuxnet virus was deployed against Iran by a non-state actor? Is Iran able to use armed force under Article 51 of the UN Charter to defend itself against a non-state actor?

Russell Buchan, School of Law, University of Sheffield

16.40 Closing Remarks and End of Conference

ABOUT DEFENCE IQ

Defence iQ
a division of IQPC

Defence IQ is host to a series of global events and runs an online community of military and private sector professionals. We provide the platform on which leading defence experts share their experience, knowledge and strategic thoughts. We are dedicated to providing military personnel and the private sector with strategic defence resources covering current defence issues. Join the community: www.defenceiq.com/join.cfm

4 Reasons Why You Should Sponsor Cyber Security 2011

1. Raise your profile and position yourself as the global product leader to take advantage of major current and future international investment programmes
2. Three full days of networking opportunities with key international government, military and industry decision makers providing you with unparalleled face-to-face time with potential new customers.
3. Tailor made sponsorship packages enabling you to competitively position your brand and increase awareness of your product or service to your target market
4. A strictly enforced end-user to vendor ratio, creating a more intimate environment for networking and knowledge sharing

For further details, or to discuss which option is best for your organisation, please call Simon Benns on +44 (0) 20 7368 9300 or Email: defence@iqpc.co.uk

SPONSORS

NETWITNESS

NetWitness® is the world leader in real-time network forensics and automated threat intelligence solutions, helping government and commercial organizations detect, prioritize and remediate complex IT risks. NetWitness' patented and award-winning solutions solve a wide variety of information security problems, including advanced persistent threats, data leakage, malware activity, and more.

CISCO

Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government and home communications, and Cisco Internet Protocol-based (IP) networking solutions are the foundation of these networks. Cisco hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries to increase productivity, improve customer satisfaction and strengthen competitive advantage. The Cisco name has become synonymous with the Internet, as well as with the productivity improvements that Internet business solutions provide. At Cisco, our vision is to change the way people work, live, play and learn.

MEDIA PARTNERS

Contingency Today
safeguarding tomorrow

ContingencyToday.com and CT Review magazine (print) dedicated to the challenges and opportunities of Critical National Infrastructure protection. Its readership includes policy-makers, decision-influencers and middle management implementers engaged in emergency planning, disaster recovery and infrastructure protection including electronic attack and the sophisticated misuse of computer systems; physical attacks by terrorist organisations and other criminals; the effects of climate change; and other natural disasters, including pandemics, fire and flood.

armedforces.co.uk

The DEFENCE SUPPLIERS DIRECTORY is an authoritative online information resource for all defence purchasers. This comprehensive listing of Defence Suppliers has enabled thousands of purchasing professionals to find exactly what they are looking for - in seconds. THE DEFENCE SUPPLIERS DIRECTORY provides a total overview of all the UK's Armed Forces - with a wealth of valuable information about the organisation and structure of the UK's Defence Services, as well as useful facts about developments in the UK Defence Industry . Contact us: defenceenquiries@armedforces.co.uk Tel: 01743 241962 website: www.armedforces.co.uk

ASDNews
aerospace & defence news

ASDNews.com – "Be the first to know" ASDNews brings the latest aerospace, defence and security news from government, industry and major news agencies around the world. Our service has over 60,000 active subscribers and 2 million article readers per year. ASDNews content is categorised in over 25 main news groups - for example: "Training & Simulation News", or "Unmanned Systems News" - making recent and related articles easy to find. Subscribe to our free daily newsletter or weekly group newsletters on www.asdnews.com/subscription

Defense Update
www.defense-update.com

Defense Update online bi-monthly defense magazine highlights defense programs worldwide including land, air, naval, C4ISR, intelligence, and net-centric warfare, infantry warfare, homeland defense etc. The coverage is frequently updated to follow the development of key defense programs. Major global defense exhibitions are covered. Defense Update is available free at our web site.
Website: www.defense-update.com

HMForces.co.uk brings all past, present, and potential members of the UK Armed Forces together to provide resources and services to advance careers and take advantage of everything a community site has to offer. News, education resources, job search, career networking, advice, and mentorship are just a few of those benefits. Helping each other let off steam after a stressful day, or during a difficult deployment is another. www.hmforces.co.uk

CYBER SECURITY 2011

VENUE: Le Plaza, Brussels, Belgium
MAIN TWO-DAY CONFERENCE: 31st May and 1st June 2011
PRE CONFERENCE WORKSHOPS: 30th May 2011

To speed registration, please provide the priority code located on the mailing label or in the box below.

My registration code is: #/R

Please contact our database manager on +44(0) 207 368 9300 or at database@iqpc.co.uk quoting the registration code above to inform us of any changes or to remove your details.

3 WAYS TO REGISTER

Tel: +44 (0)20 7368 9373

Fax: +44 (0)20 7368 9377

Email: team@iqpc.co.uk

DISCOUNTED MILITARY AND GOVERNMENT RATES**

PACKAGES	Register & Pay by 11th March 2011*	Register & Pay by 15th April 2011*	Standard Price
☐ Conference + Workshop	SAVE €250 €948 + VAT	SAVE €150 €1048 + VAT	€1198 + VAT
☐ Conference Only	SAVE €200 €599 + VAT	SAVE €100 €699 + VAT	€799 + VAT

INDUSTRY RATES

PACKAGES	Register & Pay by 11th March 2011*	Register & Pay by 15th April 2011*	Standard Price
☐ Conference + Workshop	SAVE €250 €2348 + VAT	SAVE €150 €2448 + VAT	€2598 + VAT
☐ Conference Only	SAVE €200 €1699 + VAT	SAVE €100 €1799 + VAT	€1899 + VAT

* To qualify for discounts, payment must be received with booking by the registration deadline. Early booking discounts are not valid in conjunction with any other offer. Belgium VAT charges at 21%. VAT registration number BE 081 7979 521
**Military & Government discounted rates apply to serving military officers, government and university personnel only.

***General/Flag officer 1* and above may attend the conference free of charge Please contact defence@iqpc.co.uk for further details. This offer cannot be combined with any other offer and is non-transferable.**

Delegate Details

Please photocopy for each additional delegate

☐ Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Dr ☐ Other

First Name Family Name

Rank Job Title

Tel No.

Email

☐ Yes I would like to receive information about products and services via email

Organisation

Nature of business

Address

Postcode Country

Telephone Fax

Approving Manager

Name of person completing form if different from delegate:

Signature

I agree to IQPC's cancellation, substitution and payment terms.
Special dietary requirements: ☐ Vegetarian ☐ Non-dairy ☐ Other (please specify) _____
Please indicate if you have already registered by Phone ☐ Fax ☐ Email ☐ Web ☐
Please note: if you have not received an acknowledgement before the conference, please call us to confirm your booking.

Payment Method

Total price for your Organisation: (Add total of all individuals attending):

Card Number: VISA ☐ M/C ☐ AMEX ☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Exp. Date: ☐☐☐☐ Sec: ☐☐☐☐

Name On Card: Signature:

Billing Address (if different from below):

City/County/Postcode Cheque enclosed for: € (Made payable to IQPC Ltd.)

(Please quote18896.002 with remittance advice)
IQPC Bank Details: HSBC Bank, 67 George Street, Richmond Surrey, TW9 1HG. Sort Code: 40 05 15 Account No: 59090618 Swift Code: MIDLGB22 IBAN Code: GB98 MIDL 4005 1559 0906 18
Account Name: International Quality & Productivity Centre Ltd.

PAYMENT MUST BE RECEIVED PRIOR TO THE CONFERENCE

Team Discounts*

IQPC recognises the value of learning in teams. Groups of 3 or more booking at the same time from the same company receive a 10% discount. 5 or more receive a 15% discount. 7 receive a 20% discount. Only one discount available per person.

Venue & Accommodation

VENUE:
Hotel Le Plaza, Boulevard Adolphe Max 118-126, 1000 Bruxelles, Belgium

ACCOMMODATION:
Travel and accommodation are not included in the conference price, however, a limited number of reduced rate bedrooms are available at the Hotel Le Plaza. Please quote booking reference "IQPC" to receive your discounted rate. Reservations should be made directly to the hotel on Tel: **+32 2 278 0100** or email: **reservations@leplaza.be**. Please note places are limited and so we encourage attendees to book early.

Digital Conference On CD-ROM

A digital version of the conference proceedings, including all presentations, is available to buy.

☐ I cannot attend the event, please send me the CD Rom priced at **£599 plus VAT**

Recent digital conferences available - **£599 plus VAT each**

☐ Cyber Warfare 2011
☐ Network Centric Warfare 2010
☐ Information Operations 2010
☐ Cyber Security 2010

Please send me conference materials indicated above.
I have filled out credit card details below

For further information Please call: 0207 368 9300
or email: knowledgebank@iqpc.co.uk.

Terms and Conditions

Please read the information listed below as each booking is subject to IQPC Ltd standard terms and conditions.

Payment Terms Upon completion and return of the registration form full payment is required no later than 5 business days from the date of invoice. Payment of invoices by means other than by credit card, or purchase order (UK Plc and UK government bodies only) will be subject to a €65 (plus VAT) per delegate processing fee. Payment must be received prior to the conference date. We reserve the right to refuse admission to the conference if payment has not been received.

IQPC Cancellation, Postponement and Substitution Policy You may substitute delegates at any time by providing reasonable advance notice to IQPC. For any cancellations received in writing not less than eight (8) days prior to the conference, you will receive a 90% credit to be used at another IQPC conference which must occur within one year from the date of issuance of such credit. An administration fee of 10% of the contract fee will be retained by IQPC for all permitted cancellations. No credit will be issued for any cancellations occurring within seven (7) days (inclusive) of the conference.

In the event that IQPC cancels an event for any reason, you will receive a credit for 100% of the contract fee paid. You may use this credit for another IQPC event to be mutually agreed with IQPC, which must occur within one year from the date of cancellation.

In the event that IQPC postpones an event for any reason and the delegate is unable or unwilling to attend in on the rescheduled date, you will receive a credit for 100% of the contract fee paid. You may use this credit for another IQPC event to be mutually agreed with IQPC, which must occur within one year from the date of postponement.

Except as specified above, no credits will be issued for cancellations. There are no refunds given under any circumstances.

IQPC is not responsible for any loss or damage as a result of a substitution, alteration or cancellation/postponement of an event. IQPC shall assume no liability whatsoever in the event this conference is cancelled, rescheduled or postponed due to a fortuitous event, Act of God, unforeseen occurrence or any other event that renders performance of this conference impracticable, illegal or impossible. For purposes of this clause, a fortuitous event shall include, but not be limited to: war, fire, labour strike, extreme weather or other emergency.
Please note that while speakers and topics were confirmed at the time of publishing, circumstances beyond the control of the organizers may necessitate substitutions, alterations or cancellations of the speakers and/or topics. As such, IQPC reserves the right to alter or modify the advertised speakers and/or topics if necessary without any liability to you whatsoever. Any substitutions or alterations will be updated on our web page as soon as possible.

Discounts All 'Early Bird' Discounts require payment at time of registration and before the cut-off date in order to receive any discount. Any discounts offered by IQPC (including Team Discounts) require payment at the time of registration. Discount offers cannot be combined with any other offer.

Conference code 18896.002