EVENT REPORT

2ND ANNUAL
# cybersecurity
A CTO FORUM | 2011

14 & 15 June 2011
BIS Conference Centre, London, UK

Hosted by

Cabinet Office
Office of Cyber Security & Information Assurance

BIS Department for Business Innovation & Skills

In association with

RUSI
www.rusi.org

Organised by

CTO
COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

## Common Responses to a Global Challenge

### Key Topics

- Critical information infrastructure protection and the role of government
- Security in mobile channels
- Promoting international cooperation in cybersecurity
- Security in the Cloud
- Blocking child abuse content online while preserving freedom of speech
- Setting norms & standards for cybersecurity
- Identity fraud
- Privacy on the net

http://www.events.cto.int/cybersecurity2011

Gold Sponsor

BlackBerry

Bronze Sponsor

NetClean
There are things that cannot be ignored

Associate Sponsor

Knowledge Transfer Network
ICT

Media Partners

AFRICA TELECOMS

CIO EAST AFRICA

Contingency Today

DEVELOPING TELECOMS

GHANA BUSINESS & FINANCE

InterComms
INTERNATIONAL COMMUNICATIONS PROJECT

mobileworld

pc tech

## Contents

# Executive summary

This report summarises the events of the 2nd Annual Cybersecurity Forum 2011 held at the BIS Conference Centre, London, UK from the 14-15 June 2011, hosted jointly by the Commonwealth Telecommunications Organisation, the Office of Cyber Security & Information Assurance, UK Government Department for Business Innovation & Skills and the Royal United Services Institute.

Delegates gathered with the aim of understanding the challenges of improving and enforcing security in the cyber realm.

It was an opportunity to discuss the following topics:

- Critical information infrastructure protection and the role of government
- Security in mobile channels
- Promoting international cooperation in cybersecurity
- Security in the Cloud
- Blocking child abuse content online while preserving freedom of speech
- Setting norms and standards for cybersecurity
- Identity fraud
- Privacy on the net

Key themes that emerged from the Forum included the need for multi-stakeholder engagement in tackling cybercrime and creating a safe global cyber environment and the importance of creating norms and behaviours in the cyber space on an international, regional and national level.

Model legal and regulatory frameworks will help to strengthen cybersecurity in the developing world while a cooperative global strategy is essential to agree norms of behaviour on cybersecurity.

Transparency, trust and good governance are vital elements in ensuring security on mobile and internet channels. While educating users on security is a major part of assuring security, international, government, industry and civil society buy-in is essential to tackle cybersecurity.

## Day 1

# Opening ceremony

CEO of the CTO, **Dr. Ekwow Spio-Garbrah:** As the use of ICTs penetrates deeper affecting all facets of life, cybersecurity becomes ever more important. Exercising leadership is essential to formulate policies, regulation and legislation to enhance cybersecurity.

**Mr. Steve Cutts,** Assistant Secretary General, Commonwealth Secretariat: Technology is developing all the time; with Cloud technology there is a common perception it is safe because it is sophisticated.

The challenge of cyber-security is that the Cyberworld has no boundaries. Already in 2011 a number of high profile news stories demonstrate the various challenges and risks people face.

Privacy and protection is a shared responsibility between the various stakeholders including the individual, which requires awareness and education.

Commonwealth initiatives to combat cybersecurity include the setting up of the Commonwealth Internet Governance Forum, developing model legislation on cybercrime based on Council of Europe convention (Budapest Convention), providing legal and regulatory frameworks on ICTs and carrying out an inventory of cybercrime and child protection legislation across the Commonwealth.

The challenges of cybercrime can only be addressed by building on existing initiatives and by creating a coherent strategy through the engagement and participation of all the stakeholders.

Day 1

## Session 1: Critical information infrastructure protection and the role of government

**Chair:**
**Mr. Peter Burnett**

**Panellists:**

**Mr. Neil Thompson,** Director, Office of Cyber Security & Information Assurance

**Mr. Marnix Dekker,** European Network and Information Security Agency

**Mr. John Crain,** Chief Technical Officer, ICANN

**Mr. John Bassett,** Associate Fellow, Cyber Security, Royal United Services Institute

While governments have been focusing on the protection of critical information infrastructure on an individual basis, the need for a common approach by states is increasingly becoming evident.

**Mr. Thompson:** In view of the strong transformational power of the cyberspace, technology alone is not sufficient to unleash its potential; confidence in its use is a critical underpin. Cost and impact of cybercrime and cyber espionage are increasing which requires effective preventive action. The UK Government has committed over £650 million to invest in cybersecurity.

The three elements of the UK's approach are high level political buy-in; high level engagement with industry; and comprehensive international engagement.

Creating norms and behaviours in the cyber space on an international level is critical and the UK has to play a central role in assuring cyber security by working with other countries to build relevant norms and standards.

**Dr. Dekker:** Cyber attacks are a full-fledged economy with diverse players. An International tribunal wouldn't help in the short term because the internet doesn't have a territory. Instead there are two options to protect against Cyber attacks; reducing software vulnerability and associated risks and social engineering. Importantly social networking could be used to improve security such as by evaluating individuals.

**Mr. Bassett:** Key elements of improving security are education, trust and communication. There has to be a balance between raising awareness and inducing panic in order to ensure trust.

**Mr. Crain:** Encouragingly interactions between the governments and private sector on cybersecurity are improving.

**Key discussion points:**

- It is important for countries to clearly spell out their own priorities in shaping the cyber space lest they are not decided by others
- An appropriate framework, such as the Budapest Convention, is required
- cybersecurity should be tackled nationally but with an international perspective rather than aim for a central authority
- International community should work together to deny safe havens for cybercrime
- Though there is emerging political support for agencies involved in tackling cybercrime, the process will take time to attain the required level
- In order to improve trust, standards in software and systems are critically important, as well as openness about incidences
- Robust policies, education and awareness raising, training in law enforcement, higher penalties and other measures that make attacks less economical are central ingredients to improve cybersecurity
- The individual has an important role in assuring cybersecurity as life styles and other personal factors impact security
- Setting up robust policy frameworks requires a multilateral multi stakeholder approach involving public sector, private sector, academia and civil society.

## Day 1

## Session 2: Security in mobile channels

**Chair:**

**Mr. Paul Killworth,** Government Communications Head Quarters (GCHQ)

**Panellists:**

**Mr. Nader Henein,** Security Advisor, Research in Motion (RIM)

**Mr. James Allen,** Head of Fraud and Security Strategy, Three

**Mr. David Smart,** RUSI

**Mr. James Lyne,** Sophos

**Mr. Henein:** Information assurance and intelligence are crucial along with understanding what information is valued at and how to secure it. Awareness and educating the value of security are also crucial. It is important to have air tight IT policies. Blackberry has taken responsibility for security in their product and service offerings through several new initiatives. Certification provides better security and assurance. As there are no guarantees in security, risk mitigation, data assurance and understanding the threats are important elements in assuring security.

**Mr. Allen:** Viruses, spam/denial of service and phishing are growing in the mobile Smartphone domain as well.

The mobile domain is a highly competitive market which brings with it a rapid pace for change. Alongside evolving threats, consumer demand and expectations are also growing, making security a high priority.

Strategic planning is crucial to protection. Industry need to educate, inform and support customers on best ways to protect themselves from threats as well as invest in hardware solutions. As threats are dynamic and evolve at a more rapid pace than ever, cross-industry collaboration on security is critical.

**Key discussion points:**

- It is essential to make security measures visible
- Though cyber threats on mobiles are less prevalent than on computers, this has more to do with the fact that only recently have people started using Mobiles to store valuable information
- A competitive approach at industry level may lead to improving security measures
- While public demand has a role in driving the development of devices, technology providers have a responsibility to adopt relevant technologies that customers may not yet be aware of
- Fear is a great driver, but the public fear on cybersecurity has not yet reached a high level.

Day 1

## Session 3: Promoting international cooperation in cybersecurity

**Chair:**

**Mr. Mario Maniewicz,** Chief, Policies and Strategies Department, ITU

**Panellists:**

**Rt. Hon. Alun Michael,** Member of Parliament, UK

**Mr. Martin Euchner,** Advisor, Study Group 17, ITU

**Mr. Shadrach Haruna,** Legal Advisor, Legal Division, Commonwealth Secretariat

**Mr. Mark Carvell,** Department for Culture, Media and Sports

**Dr. Rogers W'O Okot-Uma**

**Rt. Hon. Michael:** The issue is international and the stakeholders have to work together and to think strategically about it; at a national level, a regional level, and within the nation to recognise the problems. Human factor is as important as the technological factors to tackle cybercrime; hence minimising institutional vulnerabilities require training, education and awareness. The challenges can only be addressed through cooperation in each area of expertise and by meeting the challenge head on by drawing on the sum total of knowledge, expertise and best practice.

**Mr. Euchner:** Collaboration is a major component on global cybersecurity strategies of which the establishment IMPACT, as a multi-stakeholder public-private alliance, is an example. IMPACT has pioneered the development of solutions and services to address global cyber threats and has assisted the Global community to improve cybersecurity through access to Global Response Centres (GRC) that facilitate identification of threats, establishment of Computer Incident Response Teams and providing assistance to countries in the response to cyber attacks.

CYBEX facilitates a Global cybersecurity Model, which is a simple request and response protocol between two entities; information acquisition and information use. The information exchange base is developed from best practice.

Current models of authorisation and identification rules are too static, making it difficult to extend security with existing technologies; a more dynamic model with stronger authentication capabilities to ensure enhanced security, such as the development of adaptive authentication, is needed.

The current trust systems are also too limited; a more flexible and scalable trust framework for the facilitation of new e-commerce business is needed.

**Mr. Haruna:** The Commonwealth is uniquely placed to promote ICTs and has developed model legislation for members to adopt. The Harare Scheme provides for seamless cooperation among members to track, protect and report cybercrimes.

**Mr. Carvell:** The Steering Committee of the Commonwealth Internet Governance Forum is a powerful bottomup process for stakeholders to present issues. Commonwealth IGF seeks to bring all stakeholders together to engage, talk, and share ideas and knowledge.

**Dr. Okot-Uma:** Technology solutions are necessary but not sufficient. Legal aspects of e-commerce, e-evidence etc. also need to be addressed. Cyber ethics is becoming more important, particularly with the growing popularity of social media.

**Key discussion points:**

- Infrastructure security requires addressing security in devices, user access channels, copyrights, and user rights management
- There is a distinction between technical and human factors in privacy. Privacy is not a technical issue but an issue of problems users face when using technology.

## Day 1

# Session 4: Security in the Cloud

**Chair:**

**Dr. Jason Shepherd,** Home Office

**Panellists:**

**Ms. Kathleen Moriarty,** EMC Corporation

**Mr. Patrick Goldsack,** HP Labs, HP

**Mr. Eric Pigal,** European Economic and Social Committee

**Ms. Moriarty:** Cloud computing has raised concerns about security and privacy. GRC (Governance, Risk and Compliance) creates a good a level of trust and confidence. It is important to have better insight into own network security posture, compliance and security monitors. Accountability is critical for moving into the cloud environment and collaboration is important to be able to move across silos. Visibility and multi-tenancy are major barriers to having trust in the cloud which requires secure separation, service assurance, security and compliance, availability and data protection, tenant management and control, as well as service provider management and control. Cloud presents opportunities to generally increase security because users can demand and drive change. An information-centric agreement is needed with the providers for protection of data in the cloud environment.

**Mr. Goldsack:** As people will increasingly access the cloud from their own devices, enterprises will know much less of what is on the device and less control on security. The main concerns are security, regulatory controls, data clarity concerns and the geo-location of data. There is a mismatch of expectations in the environment on the issue of who is responsible for security, regulation, traceability and transparency; cloud providers believe the problem of security is in the hands of the user and users believe it lies with the provider. There is a multifaceted interaction of security-related transactions between stakeholders within the cloud, often making it difficult to place responsibility for security breaches. The biggest single risk in the cloud space is the administrator because that is the easiest way to penetrate the wider cloud.

There is also a need to consider the cloud as a vehicle for carrying out attacks.

**Mr. Pigal:** Cloud computing is a high priority topic in Europe, for Europe to be cloud-friendly, cloud-active as well as cloud-productive. The strengths are mobility, cost, the focus on core business and opportunity for growth. The negatives to be aware of are the lack of governance, need for high performance, and overbooking. Need to think of cloud computing in terms of size and the higher propensity for attacks in the larger cloud spaces.

**Mr. Henein:** Mobility when it comes to the cloud is an end point so it has to comply with whatever the cloud requires of it; it is a master-slave relationship.

In terms of how mobile computing integrates with the cloud, the mobile has to comply with the web standards, support functionality, and from a mobility perspective to make sure users have a rich development environment so that mobile technology can fulfil whatever the cloud requires.

**Key discussion points:**

- Providing people with more capabilities makes a service harder to secure
- The problem of protecting infrastructure has never really been solved completely
- Cloud computing security will become acute in years to come and is a working topic of discussion.

## Day 2

## Session 5: Blocking child abuse content online while preserving freedom of speech

**Chair:**

**Mr. Will Gardner,** Chief Executive Officer, Childnet, UK

It is important that young people have a voice in the Internet arena, particularly given the long term psychological impact of negative effects.

**Panellists:**

**Mr. John Carr,** Secretary, UK Children's Charities' Coalition on Internet Safety

**Mr. Christian Sjoberg,** Founder & CEO, NetClean Technologies

**Mr. Martin Euchner,** Advisor, Study Group 17, ITU

**Mr. Carr:** The UK has adopted a grading system according to the severity of images which determines the punishment. The International Centre for Missing and Exploited Children (ICMEC) in Washington DC monitors events in the world in the context of sexual abuse of children, particularly looking at the issue of child abuse images. It is important to have an adequate legal framework in place but the concern is the possibility of perpetrators of crime moving from jurisdictions with stronger laws and technical infrastructure to those that are weaker. There is often controversy surrounding filtering, so it is essential for the filtering process to be transparent. It is also important that any child protection system established is subject to judicial review.

**Mr. Christian Sjoberg:** Child abuse images are the only thing the NetClean technology blocks because there is universal solidarity in the need to protect children. It is more effective to take preventive measure than remedial measures.

**Mr. Euchner:** In November 2008 The ITU implemented the Child Online Protection initiative (COP), established under the Global Cybersecurity Agenda, as an international collaborative network to create a strategy for child safety online. Its deliverables include legal measures, technical and procedural measures, organisation structures, capacity building, and an online platform.

**Key discussion points:**

- Though it is not the preferred solution, filtering is the most effective solution available. The key is enforcing transparently, introducing with clarity and handling carefully
- The ITU has a sector (ITU-D) that provides specific assistance to developing countries on a broader scale to help the countries implement cybersecurity measures.
- It is important to deal effectively with content on mobile networks
- Children need to be educated about the long term impact of their actions and the legal implications.

Day 2

## Session 6: Setting norms & standards for cybersecurity

**Chair:**

**Mr. John Bassett,** Associate Fellow, Cyber Secrurity, Royal United Services Institute

**Panellists:**

**Mr. Mike St. John-Green,** Deputy Director, Office of Cyber Security & Information Assurance, UK Cabinet Office

**Mr. Stuart Jack,** Foreign & Commonwealth Office

**Dr. Ekwow Spio-Garbrah,** CEO, CTO

**Mr. St. John-Green:** Having identified Cyber Security as one of the top four risks in its National Security Strategy, the UK is developing a comprehensive National Cyber Security Programme on which UK seeks an open dialogue with international partners. It is important to build Cyber security in an environment of openness, interoperability and stability in order to maximise the opportunities available in Cyber space particularly in improving governance, empowering people and strengthening understanding, which can only be achieved by developing mutual trust through norms of behavior.

At the Munich Security Conference in February 2011, the Rt. Hon. William Hague, Secretary of State for the Foreign and Commonwealth Office outlined seven principles on norms of behaviour which, in the view of UK, should apply to states' activities in cyber space and which could form the basis for broad international consensus.

Recognising that these principles are not exhaustive and others will have their own views, the UK seeks a more focused multilateral debate.

The conference due to be held in November 2011 in London with wide geographical representation, and involving industry and academia, will set the stage for this dialogue. Given the range of potential views, UK aims to arrive at a pragmatic political and diplomatic consensus, not a new international legal instrument.

**Dr. Spio-Garbrah:** Norms could be set on various aspects such as legal, regulatory, education, law enforcement, and international institutions. States should have their own internal legislation for cybersecurity but should also collaborate on an international level. Governments, regulators, policy makers, manufacturers, and other stakeholders are essential in setting norms and standards.

**Mr. Jack:** It is important to note cyber is a multi-stakeholder issue and governments are responsible to stakeholders of industry and society.

**Key discussion points:**

- The social aspects should not be overlooked when dealing with security but should not allow it to dominate
- For developing countries cybercrime is a priority along with other socio-economic issues
- It is important to prevent criminals using some countries as safe havens for cyber crimes
- Norms would not apply only to states; they apply to businesses, society and individuals. Norms should be built on law but enforced based on moral behaviour.

Day 2

## Session 7: Identity fraud

**Chair:**

**Mr. David Artingstall,** Senior Consultant, John Howell and Co.

**Panellists:**

**Mr. Richard Simpson,** Commonwealth Secretariat

**Mr. Alexander Fisher,** Fraud Strategy and Prevention Manager, CIFAS

**Mr. Brian Hall,** Office of Cyber Security and Information Assurance

**Mr. Mohan Koo,** Managing Director, Dtex System UK

**Mr. Simpson:** There is an economic imperative at the heart of cybersecurity and a strong economic rationale to create a safer, more secure global internet. The social and economical costs of cybersecurity to businesses, SMEs, online practices and services result in slowing down innovation.

A multi-level response with a multi-level integrated set of tools is needed to make the internet safe and secure for businesses and consumers, which should include legislative and policy responses, technology measures and industry self-governance. The three areas that are essential components of a cybersecurity strategy are criminal law remedies and enforcement, civil and legal measures to protect the Internet economy, and mechanisms for private sector self-defence through multi-stakeholder involvement. Main features of effective cybersecurity frameworks are legislation broad in scope to cover a wide range of threats; technology-neutral language; flexible enforcement; mechanisms for monitoring and coordinating; built-in international facilitation; and enabling private sector action.

**Mr. Fisher:** An information age makes information easily available. The speed with which it can be exchanged and the speed with which it can be used, increases threat. Fraud is becoming a lot more indiscriminate and widespread as it is no longer focused on population centres, suggesting greater use of the Internet.

The Internet has revolutionised the way in which identity fraud can be perpetrated. Identity fraud has changed from a high risk theft to an online theft as it is easier to obtain personal information online, particularly with the use of social networking sites and sharing on information on these sites. Mobile phones are points of data compromise, particularly with the increased use of mobile phones in less developed countries. Mobile phones can store increasing amounts of data, which encourages people to hold information on their phones for convenience.

**Mr. Hall:** There is a clear requirement for a government identity proposition. The proposition is more about how does the private sector provide identity assurance while preserving privacy rather than the government forcing an identity scheme on the population. It should be customer-focussed, consider data minimisation, customer control, decentralisation of information, collaboration of the public sector, private sector and civil society, and create an open and transparent market.

**Mr. Koo:** An ordinary person can easily learn how to hack and obtain personal details. An example is a person who has used Google to find out how to crack UNIX passwords, who within three months taught how to hack in to a corporate system through the back end.

**Key discussion points:**

- CIFAS does share its model abroad depending on willingness of members to share their data
- The relationship between data protection regimes and effective private sector and public sector regimes needs to be reconciled. Information sharing and data validation requirements are a challenge and needs to be addressed
- The most important thing is to educate citizens about identity fraud and increase user awareness and regulation. Frameworks need to be put in place to encourage the industry to maintain their house in order
- Simply pursuing criminals is only half the solution, the other being improving systems.

## Day 2

# Session 8: Privacy on the net

**Chair:**

**Mr. Jean-Jacques Sahel,** Director Government and Regulatory Affairs, EMEA, Skype

Privacy is a right under the UN Convention and there are a variety of guidelines on privacy from different international and regional organisations and national agencies. Privacy is fundamental; a view which hasn't changed but the conditions and evolving technological environment is changing rapidly.

Therefore there is a global perspective to this debate which is now on about data protection and online privacy.

**Panellists:**

**Mr. Ivailo Kalfin,** Member of European Parliament, Committee on Industry, Research and Energy

**Dr. Edgar Whitley,** London School of Economics

**Mr. Bruce Lowe,** Senior Manager, Global Policy, Research in Motion

**Ms. Henrietta Abraham,** Reach-Legal

**Mr. Kalfin:** The collection and use of personal data has varied in many ways. With the development of technologies, invasion of privacy has become more sophisticated. There are two main actors: ICT and technology business and the regulators. The ICT and technology players have an interest to develop the Internet on the basis of a trustworthy environment by making the technology more sophisticated in order to protect data, and the regulators try to set some rules to deal coherently with data protection.

Usually the criminals are faster to reach sophistication, the industry follows close behind, and the regulators are the slowest to act. This creates a problem with the development of the Internet, cloud computing, new technologies and the use of Internet over mobile devices.

Criminals exploit the rapid advance of technology, presenting a huge problem for protection of data. There need to be common standards or legislation adopted that go beyond national borders as it will be difficult to be effectively ensure protection of privacy without considering the context of the use of data across borders.

**Dr. Whitley:** Privacy is a basic right and data protection is a legal measure to enforce that right, with cybersecurity being the process to protect data privacy. Individuals have the right to know how their personal information is being used by organisations as well as the right to prevent secondary use of personal information. There should be explicit consent before storing and accessing of personal data, or passing data onto a third party. There is the issue of deletion of private information; having the right to be able to completely erase private data from a database.

**Mr. Lowe:** Privacy as a concept seems simple but technology makes it far more complicated. It is important for the industry to put the control back in the users' hands so they can control their own information.

**Ms. Abraham:** Compliance with the adequate transfer of data flow and how it is regulated across borders is an important topic for discussion.

**Key discussion points:**

- Technologies need to lead in data management with the engagement of regulators. There needs to be broader fundamental agreement and understanding in order to harmonise data protection legislation
- Privacy rules could be a barrier to outsourcing work to less developed countries. The work done by the Article 29 of the Working Party on Corporate Binding Rules' model clauses have helped in overcoming barriers to outsourcing, as many countries outside the EU don't have adequate protection for data. The rules help the data controller to assure protection of data outside EU. There needs to be a line of accountability when outsourcing business
- There are two issues with developing innovative solutions to the problem of accepting consent; firstly the behavioural psychology of signing up and the instant gratification to do so overruling negative perceptions about the future, secondly the issue of the extent of information given in the privacy policy and the ease of understanding.

COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

**64 - 66 Glenthorne Road**
**London W6 0LR**
**United Kingdom**

Tel: +44 (0) 208 600 3800
Fax: +44 (0) 208 600 3819
E-mail: info@cto.int

www.cto.int