commonwealth
CyberSecurity'17

22 - 24 MARCH 2017, LONDON, UK

CONFERENCE & EXHIBITION

Organised by
CTO COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Hosted by
BT

Executive Summary

The Commonwealth Telecommunications Organisation held a 3–day cybersecurity Forum 2017, from 22–24 March 2017 in London, UK at BT Center, under the theme **‘Cybersecurity: from Strategy to Implementation**’. The forum brought together cybersecurity stakeholders from across the world including policy makers, regulators, implementing agencies as well as private sector and civil societies, a good sign of future global cooperation in Cybersecurity. The stakeholders shared views in areas such as policy and regulation, technology evolution, operations, investment and multilateral cooperation with a call on all to rise up against cybercrime and collaborate in fighting the canker.

Various speakers and panellists addressed the forum on salient topics such as Cyber Threat Landscape, Economic of Cybersecurity, Strategic Approach to Cybersecurity, Implementing National Cybersecurity Strategies, Privacy and Data Protection, Internet Governance, Protecting Critical Information Infrastructure, Cross-Border Cooperation in Cybersecurity, Cyber Standards, Cyberspace & Extremism, International Cooperation, Protecting the Vulnerable, Cyber Capacity Building and Building A Culture of Cybersecurity.

Participants shared their views on all subjects showing keen interest in all topics.
Over the three days, the event was attended by 255 delegates from 16 countries from more than 50 institutions in and outside UK listed in Annex 1.
.

Day 1

Session 1: Cyberthreat Landscape

- Ransomware are now becoming popular with criminals and putting that in context, in 2015, $26 million was extorted from people using Ransomware, which later rose to a Billion dollars in 2016.
- There are also new threats that will continue to emerge as technology develops, the Internet of Things (IOT) is expected to have 50 – 100 Billion devices connected to the internet by 2020 which will bring a huge new opportunity for vulnerability to be exploited.
- PhotoDNA has helped detect millions of illegal images online and over 100 organizations use the technology to keep their platforms safe.
- Illegal images are reported to the National Cyber Security Center of UK and other appropriate authorities for missing and exploited children.
- Microsoft is currently working with Law Enforcement & other agencies to disrupt the criminal infrastructure.
- Microsoft now embeds malware intelligence into their products and services.
- Increase on Cyber extortion based on **Information Assurance Advisory Council (IAAC)** statistics in UK.
- Internet of Things gives a broadening attack surface and more opportunities for attackers.
- Threat actors are learning from, and using, one another's skills and capabilities.
- Threat actors will not just encrypt or leak data they tamper with it.
- Attribution will become more difficult as attacks become more tailored.

Session 2: Economic of Cybersecurity

- Guidance on Information Sharing for public/private sectors.
- In conducting cost benefit analysis with regards to the cost of technology and business, the cost of brand of the business should be included as component of business cost.
- The private sector is not interested in the source of attack but how to prevent the attack.
- The cyber attackers do not go through change process. Many businesses were not able to recover after cyber-attacks. Impact of cyber-attacks could be as much as **$3 trillion** in **lost productivity and growth.**
- Companies lose $400 Billion from cyberattacks each year.

Session 3: Strategic Approach to Cybersecurity

- CTO is currently conducting a **National Cybersecurity Strategy (NCS)** for these member countries: Rwanda, Tanzania, Malawi, Mozambique, Botswana, Uganda & Cameroun who are either developing or reviewing national cybersecurity strategies

- Presently, 11 partners are actively involved in developing models & implementing Cyber Security strategies around the world by CTO.
- Continuous collaboration between CTO and Oxford university on cybersecurity capacity maturity model with CTO in the process of developing national cybersecurity toolkits.

Session 4: Implementing National Cybersecurity Strategies

- The UK's new **National Cyber Security Strategy (NSCC) 2016 - 2021** was published in **November 2016.** It has 3 Pillars which are: "**Defend** against cyber threats", "**Deter** our adversaries" & "**Develop** our skills and capabilities".
- Countries should allocate resources including budgets for Cybersecurity as UK' Cyber Security Programme, is supported by **£**1.9bn of transformative investment over 5yrs with international partnerships.
- Nations should get the buy in from top political leadership or executives.

Session 5: Privacy and Data Protection

- Balance between security and data protection keeping guidelines on democratic principle on which nations and stakeholders should operate as government is responsible for protecting her people, investors must also play their roles in contributing to safe environment with government providing good laws to enable the investors to do business.
- Privacy by design should be incorporated at planning stage

DAY 2

Session 6: Internet Governance

- In the UK, there is this issue with private actors like Google taking laws into their hands with regards to cyber infringement instead of informing the Law enforcement.
- Cooperation between Law enforcement & Internet service providers and vice versa should be established.

Session 7: Protecting Critical Information Infrastructure

- Risk based approach should be applied in protecting critical information infrastructure.
- **18%** of the data that was exfiltrated through cyberattacks in Europe in 2016 related to companies' industrial control systems.
- In 2016, hackers most often targeted **financial, manufacturing, telecom industries and governments.**
- In addition, **politically-motivated hacking** is on the rise.

- Terrorists are also now invading this space. On 13 February, the UN Security Council called on Member States to address the danger of **terrorist attacks** against critical infrastructure.
- The EU **Network & Information Security (NIS) Directive** is the first-time UK adopted a new focused law, whose one of its objectives is to increase security baselines for critical infrastructures & digital service providers.
- The NIST Cyber Security Framework emerges as a global best practice in managing cyber risk and its core consists of IDENTIFY -> PROTECT -> DETECT -> RESPOND -> RECOVER.
- Microsoft's vision in the fight for cybercrimes, A Digital Geneva Convention is needed for **Governments**, Tech Accord for the **Industry** & Attribution Council for **Public-Private Partnership**.
- **BT,** suggested that to exploit in the digital opportunity, Major corporations should rethink the cyber security threat, Entrepreneurs need to be ruthless in taking the fight to the attackers and the need for cybersecurity organizations to be as creative and agile as their opponents.
- The CYTADEL Delivery Scope & Governance by **BT** is a significant drive and investment towards big data and intelligence. This CYTADEL also helps in protecting BT & its customers from being Hunter Gatherers.

Session 8: Cross-Border Cooperation in Cybersecurity

- Benefits of countries being a member of the Budapest Convention includes a legal framework compatible with International best practice & rule of law standards and Effective international cooperation.
- The Commonwealth believes Coordination and Partnership are key to combating crime of whatever nature.
- In tackling cybercrime, it is and always will be a shared responsibility between individuals, industry & Government.
- The **Budapest Convention** represents the criminal justice response. This convention is currently the most effective and viable model for all Commonwealth Member States. It also helps in securing Countries right in cyberspace.

Session 9: Cyber Standards

- There is a need for SMEs to have embedded **Cyber Essentials (CE)** in their operations. This CE is designed to align with other standards like ITIL & ISO/IEC families and it is also affordable.
- The World Bank's ICT Unit offers integrated solutions in the ICT project portfolio to **address cybersecurity gaps** in their country clients.
- **Digital Development Partnership (DDP)**, a platform created by World Bank for digital innovation and development financing, will help advance the capacity of World Bank clients in the development of cybersecurity policies and standards, and support good practices in the use of cybersecurity tools, safeguards, and risk management instruments.
- **Nominet** are the .uk domain Registry and currently has 10 million registered domains.
- Analysis done by **Nominet** shows that 43% of attacks are towards SMEs and 60% of these affected SMEs close 6 months after the attack.
- **Cyber Essential Standard** aids in protecting business from more common attacks, enables SMEs to participate securely in the value chain and it is simpler & affordable to implement.
- **5** Stages are involved in Cyber Essentials (CE) implementation which are: Cyber Standards Sensitizations, Cyber standards Workshop, CE Assessors Selection, Cyber Essentials Assessment and Cyber Essentials Certification. Among the 6 countries evaluated by CTO, only Botswana has reached the Cyber Essential Assessment stage.
- To sustain **CE,** it requires a sustainable business model, encourage supply & demand and create more awareness & outreach about the standard.
- **IASME Consortium LTD,** suggested ways of protecting our devices from cyber-attacks, which includes: Enabling firewall on computer/laptop devices, disabling the "Auto-Run" function from Laptops/Computers, Updating the Windows operating system anytime new patches are released, operating as a user instead of as an Administrator of your device.

Session 10: CYBERSPACE & EXTREMISM

- **Countering Violent Extremism (CVE) unit** is a dedicated facility that advances the Commonwealth's role in international efforts in countering violent extremism. They respond to mutually identified gaps in the capacity of member countries, mapping existing support mechanisms and resources, sharing best practise and harnessing the full family of Commonwealth governments, networks and organisations in a coordinated fashion.
- From the **Countering, Violent Extremism (CVE) Unit analysis** carried out in 2014, shows 12-15 yrs. old prefer watching you – tube to TV, 10 – 13 yrs. kids use the social media while 12 – 15yrs may be in contact with people they don't know on social networking sites.

- ISIS controls as many as 90,000 Twitter accounts which it uses to spread sick propaganda & radicalize Westerners, terror experts revealed.
- **CVE Units** provided strategic solutions which are; Social awareness programmes, ICT system/tools & Building partnerships.
- Furthermore, they also provided Operational Solutions which are: Developing counter/alternative narratives, disruption, E – safety lessons & Critical thinking classes.
- Disrupting social media accounts of extremists, Advocacy projects on extremism should be promoted to expose their modus of operandi and the realization of a Digital Forensic Capacity Building will also help in this fight.
- Government and Service providers should have a better dialogue in delivering safe & secure services.
- In Bangladesh, there is need to Raise awareness, Policies needs to be revisited to respect National Laws against Cyber bully, defamatory information about young girls.
- Reasons why Bangladesh is serious about securing the Cyberspace include widespread of young generation to pornography, attacks from extremists & terrorists, issue-motivated activists, defamatory & indecent exposure in the internet warrants many of their female citizens' deciding to commit suicide, cyber fraud in mobile banking, e.t.c.
- Measure taken by Bangladesh regarding this Cyber-attacks include: they have Information & Communication Technology Act, 2006 (amended 2013), Introducing 'National Cyber Security Strategy' which is conformance with the Global Cybersecurity Agenda of ITU, Mandatory SIM/RUIMs registration through verification of biometric data with their NID, an MOU with Microsoft for cooperation in fighting Cyber threats, etc.
- Recommendations from Bangladesh includes: Special attention to emerging technologies (IOT, Robotics, etc), Social medias revisiting their policies & amend for different cultures, societies & countries, strengthening the social awareness campaign, addressing new threats & adjusting National Laws accordingly, proper training of Law Enforcement & investigation agencies including judges.

Day 3

Session 11: International Cooperation

- In Malta, they are working on focusing on cyber threat social awareness campaign, their citizens, SMEs.
- A Digital Assembly to be held in Malta on **15th – 16th 2017**, regarding International cooperation on Cyber threats and registration is free and can be done online.
- Global Forum on Cyber Expertise (GFCE), which is an informal global platform with 56 members that focuses on cyber capacity building has achieved the following results in their last meeting: Various deliverables, through initiatives

(toolkits, reports, etc.), Global database of capacity building initiatives, exchanging expertise through international expert meetings and many more.

- Future developments on Cyber expertise by GFCE includes: Results initiatives more focused on real implementation, Interaction between initiatives by strengthening one another & More initiatives like Cybersecurity Education, Cybercrime training, etc.
- Having practical cooperation in the fight of Cybercrimes.
- Not only creating awareness on Cybersecurity but over the years' International bodies should focus more on real implementation (Capacity Building).
- GFCE pleads for global approach towards cyber capacity building.
- International cooperation is important in the cyber domain and this will help in being effective and prevent over lapping.

Session 12: Protecting the Vulnerable

- The two documents have been produced by ICMEC and GSMA respectively discussing the Child sexual abuse content.
- ICMEC has 5 standards that govern them, which are: 1). Legislation Specific to Child Pornography, 2). Child Pornography defined, 3). Computer Facilitated offences, 4). Simple Possession & 5). ISP reporting.
- From analysis done by ICMEC on the 52 commonwealth countries that follow their 5 standards proved that only 28 Countries met 4/5 of their criteria, 14 countries met between 1 & 3 while 10 countries did not meet any of the criteria.
- Nominet runs .uk and all its contracts make it clear that any domain name that appears to signal sex crime content or amount in themselves to sex crimes are prohibited.
- ICMEC believes that Pakistan, Nigeria & South Africa are the only Commonwealth countries that have clauses which speaks expressly about disallowing certain types of domain names but was unable to find any direct references to child protection issues.
- The **Internet Watch Foundation (IWF),** whose vision is global elimination of child sexual abuse imagery online, offer the public a place to securely and anonymously report such content.
- Their remit includes; child sexual abuse hosted anywhere in the world, non-photographic images of child sexual abuse hosted in the UK, criminally obscene adult content hosted in the UK, etc.
- IWF are different from Police in the following ways; industry self-regulatory body, charity, not-for-profit organization and funded by internet industry Members and European Union (EU).
- IWF helps by actively searching for child sexual abuse images & videos on the public network, providing an international reporting portal, working with industry members, sharing their expertise and playing an active role in the UK Safer Internet Centre.

- **SafeTonet** operates as an app installed Parents and children devices to help them in detecting child sexual abuse imagery.
- **BT** ensures that all emails coming through their network to their customers are strictly protected from phishing attacks.

Session 13: Cyber Capacity Building:

- The **GIPO Observatory Tool** is designed for all International Stakeholders to help monitor Internet- related policy developments in improving and sharing knowledge among all interested parties.
- This GIPO tool is accessible from "http://observatory.giponet.org".
- Malaysian's concept of outreach & capacity building is by conducting Competency training for their workforce, Professional developments and Cyber safe for non-technical & end users.
- Regional community needs to collaborate and combine ideas to stay ahead of rapidly changing cyber threats.
- Industry professionals are required to constantly train and re-train to upgrade their skills and knowledge while keeping abreast with the latest changes in the global information vectors- hence requiring multi-stakeholders partnership.

Session 14: Building A Culture of Cybersecurity

- **National Cyber Security Centre in UK** programme for all stakeholders (Legal, HR, Risk management, audit, data protection, Senior management, Public Relations, line management & operations management).
- **Facebook** also developed an open source called "**osquery**" that assists users in monitoring low level activities in their operating systems
- Statistics shows that 1.3 Billion people use Facebook daily, with 709 million users living outside US/Canada & Europe. It also proves that more than 6.6 Billion people live within wireless range but only 3 Billion have access to internet.
- **In Cameroun,** they have included Cyber security culture in the curriculum of schools for young students.
- Internet Service Providers needs to have the mindset of taking responsibility of securing their network as well before it is being accessed by their customers.

Conclusion

The forum was highly successful as it brought expertise across the globe to deliberate on cybersecurity with emphasis on collaboration in fighting the cyber crime. While some sessions were engaging, others did not engage the audience enough leading to rushing in closing remarks or close the discussion without thoroughly exhausting the subject as audience were ready to participate but time was of essence and could not present their views. For additional information on sources of data, kindly refer to "Z:\Operations\Events\CTO Events\2017 Events\Commonwealth Cybersecurity Forum 2017\Presentations".

Annex 1

Participating Countries & Organizations.

Country	**Organization**
Bangladesh	Ministry of Post, Telecommunications & Information Technology
Cameroon	National Information Technology Agency
Cyprus	Office of Electronic Communications & Postal Regulations
Fiji	Ministry of Communication
Ghana	Ghana Computer Emergency Response Team
	Ministry of Communications, Ghana
Gibraltar	Ministry of Economic Development, Telecommunications & the GSB
Guyana	eGovernment Unit Agency
International Delegates	APMG International
	Building Respect for IP Division World Intellectual Property
	Commonwealth Professional Fellow
	Commonwealth Telecommunications Organization
	Facebook
	Global Internet Policy Observatory, European Commission
	GSM Association
	Information Society, Council of Europe
	International Telecommunication Union
	Internet Corporation for Assigned Names and Numbers (ICANN)
	Microsoft EMEA
	Nominet
	Privacy International
	SafeToNet
	The IASME Consortium Ltd
	Three Raymond Buildings Barristers
	University of Warwick
	Vodafone
	World Economic Forum
Malaysia	Cybersecurity
	New Media Monitoring, Compliance & Advocacy Sector, Malaysian Communications & Multimedia Commission
Malta	Ministry for Competitiveness & Digital, Maritime & Services Economy
Montserrat	Ministry of Communication, Works, Energy & Labour

Mozambique	Ministry of Transport & Communications
Sierra Leone	Ministry of Information & Communications
	National Telecommunications Commission
South Africa	Independent Communications Authority of South Africa (ICASA)
	ZA Domain Name Authority, South Africa
Sri Lanka	Attorney-General’s Department
The Netherlands	Global Forum on Cyber Expertise
Trinidad & Tobago	Telecommunications Authority of Trinidad & Tobago
United Kingdom	BT
	BT Security
	Capacity Building, Prosperity, Cyber Crime, Cyber Policy Department, Foreign & Commonwealth Office
	Commonwealth Secretariat
	CREST
	Cyber & Government Security Directorate, National Security Secretariat, Cabinet Office
	Cyber & Physical Security Operations and Programmes, BT
	Cyber Policy Centre
	Cyber Security Challenge
	Cyber, Foreign and Commonwealth Office
	Department for Culture, Media & Sport
	EE & Group, BT
	Ethics & Compliance, BT Group
	Information & Communications Law, Queen Mary University of London
	Information Assurance Advisory Council
	Internet Watch Foundation
	Military Influence, Royal United Services Institute for Defense & Security Studies
	National Cyber Security Centre
	Office of Information Commissioner
	RAND Europe
	UK Council for Child Internet Safety
	UK Government Affairs, Microsoft
	United Kingdom’s National Cyber Crime Unit
	University of Oxford