ITU Backgrounders

ITU: BUILDING TRUST IN ICTS AND CYBERSPACE

The Global Cybersecurity Agenda (GCA) facilitates ITU's efforts to build the technological capacity necessary to help nations combat cyberthreats, recommend global standards for cybersecurity and technology, and act as a platform for knowledge and public policy discussion.

ITU predicts almost 3 billion people will be using the Internet by end 2014, opening up exciting new possibilities for access to information and communication. But at the same time, security concerns and vulnerabilities in networks and services are exposing users everywhere to increasingly sophisticated cyberthreats. Identity theft, spam, malware, exploitation and harm to children and other at-risk groups can all have dramatic and sometime devastating real-world consequences beyond the 400 billion dollar estimated annual loss to the global economy.[1]

Because information and communication technologies (ICTs) have become a critical national infrastructure, disruption can mean catastrophic interruption of essential services. And in the always-on, anytime, anywhere environment of broadband technology, attacks can be committed in one country – or even several countries simultaneously – while the perpetrator is somewhere else entirely.

Cyberthreats have emerged as a risk for every country, even the most technically advanced. Greater international cooperation can help mitigate this risk.

A GROWING INTERNATIONAL THREAT

- There were almost 400 million victims of cyberthreats in 2013.
- The year 2013 saw a 91% increase in targeted attack campaigns. The number of breaches increased by 62%, and 38% of mobile users experienced mobile cybercrime.
- The number of 'exposed identities' skyrocketed more than five-fold in 2013 to 552 million, compared with 93 million in 2012.
- The three sectors most at risk from targeted attacks are government, mining and manufacturing (Symantec, 2014 Internet Security Threat Report).

Mobile users often store sensitive files online (52%), store work and personal information in the same online storage accounts (24%), and frequently store logins and passwords with families (21%) and friends (18%), putting their data and their employers' data at risk. Only 50% of users take even basic security precautions, according to ITU partner Symantec.

1. MacAfee

ITU's Child Online Protection (COP) initiative is an international collaborative network for action, designed to identify risks and vulnerabilities worldwide to children in cyberspace, create awareness, share resources and develop practical tools to help minimize risk and promote responsible digital citizenship.

As the 'Internet of Things' becomes a reality, with millions of interconnected devices exchanging machine-to-machine information without the need for human intervention, our physical and cyber worlds are increasingly overlapping. Bringing together different stakeholders in global partnership, ITU is at the forefront of providing both technical and policy solutions to combat cybersecurity issues.

A key development was the establishment of ITU's Global Cybersecurity Agenda (GCA), an international framework for cooperation. The GCA facilitates ITU's efforts to build the technological capacity necessary to help nations combat cyberthreats, recommend global standards for cybersecurity and technology, and act as a platform for knowledge and public policy discussion.

Responding to national cyber-attacks

A national cyber-attack can wreak havoc on critical infrastructure, having a direct impact on daily lives; from not being able to access your bank accounts, to disruption of transport networks, electricity outages, blocked communications and worse.

There is a clear need for effective institutional structures to deal with cyber incidents and attacks. ITU is working with Member States, regions, and industry partners, to deploy capabilities to build capacity at national and regional level.

ITU builds capacity and expertise through extensive training and support programmes. Such initiatives include:

- Assisting 50 Member States assess their national cybersecurity preparedness and response capabilities. Seven Member Stats have received support to set up a national computer incident response team (CIRT), with a further seven confirmed to receive ITU assistance.

- To date, seven CIRT Cyber-drill exercises involving more than 60 countries have been conducted. These evaluate whether the core functions of established CIRTs are consistent with international standards and good practice.

- The establishment of national cybersecurity strategies is particularly challenging for Least Developed Countries (LDCs) who lack adequate legal and regulatory frameworks, and have limited human capacity/expertise and financial resources to identify, manage and respond to cyberthreats. ITU's "Enhancing Cybersecurity in Least Developed Countries" project supports LDCs in strengthening their cybersecurity capabilities to ensure the enhanced protection of their national infrastructure and maximize socio-economic benefits.

- At the regional level, further assistance is provided in the form of ITU Regional Cybersecurity Centres – a physical centre hosted by a Member State which then acts as the regional ITU focal point for cybersecurity issues. The Arab Regional Cybersecurity Centre is located in Oman with plans for an African Regional Cybersecurity Centre hosted by Nigeria now underway.

- ITU assists Member States in understanding the legal aspects of cybersecurity, in order to help harmonize their legal frameworks, making them internationally applicable and interoperable.

- The growing role of ICTs in services as varied as health, education, finance and commerce, means there is an increased need for a wholly secure cyber environment, yet there is a chronic global shortage of qualified cybersecurity professionals. To help bridge this gap, ITU has organized cybersecurity training workshops for more than 1,900 government officials, regulators and public and private sector ICT professionals around the world.

Security is fundamental to ITU recommendations and standards, and all ITU Study Groups now routinely review security related questions as part of their work.

Child Online Protection (COP)

Children are one of the most vulnerable groups online, with the new generation of 'digital natives' far more likely to reveal personal data online, making them easy targets for criminals and hackers.

The division between the online and physical world is becoming increasingly porous – with serious ramifications for a child's mental and physical well-being. In a recent survey, almost half of teenagers aged 13 to 17 reported that they had experienced some form of cyberbullying in the past year. Even more disturbingly, three quarters of young people involved in aggressive sexual solicitations in the real world met their aggressors online.

ITU's Child Online Protection (COP) initiative is an international collaborative network for action, designed to identify risks and vulnerabilities worldwide to children in cyberspace, create awareness, share resources and develop practical tools to help minimize risk and promote responsible digital citizenship. Under the COP umbrella, more than 54 international partners from government, the private sector, civil society, academia and international organizations work together to achieve these goals.

Technical standards (Recommendations)

ITU technical standards (known as Recommendations) play a key part in protecting users online. ITU-T Study Group 17 is the lead Study Group on telecommunications security and identity management, with a primary focus on building confidence and security in the use of ICTs.

Security is fundamental to ITU recommendations and standards, and all ITU Study Groups now routinely review security related questions as part of their work. Achievements to date include: technical Recommendations for Internet Protocol (IP) networks, Next Generation Network (NGN) standards, and ensuring clear security principles for today's and tomorrow's mobile cellular networks. A prominent example is **X.509,** an ITU-T recommendation for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, among other things, standard formats for public key certificates, certificate revocation lists, and attribute certificates.

A global, multi-stakeholder approach

- An increasing dependency on ICTs in Least Developed Countries (LDCs) makes cybersecurity a growing priority, with studies showing that developing countries are the most vulnerable when it comes to cybercrimes and cyber threats. ITU's Enhancing Cybersecurity in LDCs project focuses on protecting users and making the Internet safer by implementing policy level assistance.

- ITU has partnered with ABI Research on the Global Cybersecurity Index (GCI) to provide benchmarks of national cybersecurity capabilities and enable Member States to learn from best practices.

- ITU has also established formal cooperation with cybersecurity companies such as Symantec and Trend Micro to share information on current and emerging global cyberthreat trends on a regular basis.

- ITU is currently working with other agencies/bodies of the UN family on enhancing internal coordination amongst UN agencies in their assistance to Member States with regard to cybersecurity.