working together towards 2015
World Summit on the Information Society
Geneva 2003
Tunis 2005
Turning targets into action

Progress and challenges in the implementation of WSIS Action Line C5: Building confidence and security in the use of ICTs

This draft document is for information purposes only. It has been prepared by an external expert and does not necessarily reflect the views of ITU or its Secretariat.

1. Introduction

This document presents a brief summary of the progress made in the implementation of Action Line C5 since WSIS (2005), and highlights some emerging trends and related post-2015 potential challenges.

2. Review

2.1 Some of the areas of Action Line C5 that saw good progress are:

- ***Education/Awareness*****:** Most national cybersecurity strategies (and organizational policies) place a particular emphasis on awareness, although these may not have always been followed by the adoption of action plans[1].

- ***Fight against SPAM:*** In the last years, numbers on spam and phishing attacks via traditional routes have fallen. The Estimated Global Email Spam Per Day (in billions) has decreased from 62 in 2010 to 42 in 2011 and to 30 in 2012[2]. Even if total numbers decreased, there is an increase of spam and phishing through social media and through targeted attacks.

- ***Use of electronic documents and transactions*****:** Electronic payment transaction is growing worldwide. For instance, one-third of the world's roughly 280 billion annual non-cash payments occur in Europe—and this number is growing. The number of non-cash transactions increased from 70 billion in 2005 to 91 billion in 2011 and will exceed 175 billion transactions by 2020[3]

- ***Sharing of best practices*****:** Many activities have been initiated to create best practices at national and international levels, although these are not always shared between public and private organizations.

- ***Incident Response*****:** Many organizations and governments have increased their incident response capabilities. According to ABI Research, the Enterprise Incident Response market is set to see a dynamic growth over the next few years, totalling $14.79 billion by 2017[4].

[1] http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf
[2] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-18
[3] https://www.atkearney.com/financial-institutions/featured-article/-/asset_publisher/j8IucAqMqEhB/content/winning-the-growth-challenge-in-payments/10192
[4] https://www.abiresearch.com/press/enterprise-incident-response-market-booms-to-14bn-

- ***Security of Online Transactions*****:** In the last several years, the focus on security of online transaction has increased and numerous initiatives have been established in this regard[5].

2.2 Some of the areas that, despite current efforts, may not have been sufficiently addressed are:

- ***Cooperation between governments*****:** Many national cybersecurity strategies aim to enhance international cooperation[1], emphasizing the socio-economic dimension of cybersecurity. Though, the governments still need to create the right conditions to ensure effective dialogue and cooperation. Some initiatives exist but appear fragmented.

- ***Response to Cybercrime (Public Private Partnership):*** Cybercrime continues to grow and evolve. Pomenon analysis has reported a 42% increase in the number of cyber attacks in 2012 in US, with organizations experiencing an average of 102 successful attacks per week, compared to 72 attacks per week in 2011 and 50 attacks per week in 2010[6]. The attacks are becoming increasingly sophisticated, and highly focused. Considering the global nature of Internet and that cyberspace is largely owned and operated by the private sector, a close cooperation between both public and private actors is needed to reach a shared situational awareness that can help organizations to understand the real risk and the correct action to be taken to counter cybercrime.

- ***Strengthening the Trust Framework*****:** Increasing the level of trust in digital services, in cybersecurity and creating a trusted environment between public and private organizations are key challenges. The level of citizen trust in digital services and the Internet must be improved. Aware of this, the European Union in its Digital Agenda has identified "Trust and Security" as vital to a vibrant digital society. Furthermore, trust between key actors such as governments and operators is a critical enabler of cooperation on cybersecurity and information sharing, leading to a much more effective protection and incident response capabilities.

- ***Encouraging further development of secure and reliable applications*****:** Application security breach and related incidents due to the exploitation of application-level vulnerabilities are common. A survey study conducted involving 240 North American and European software development and software security influencers has revealed that application security incidents are common and have severe consequences. Many organizations still struggle with the most basic security flaws. Most do not have a holistic or strategic approach to application security and often application development and security teams and goals are not aligned for optimized results[7].

3. Developments and challenges

Challenge #1**:** While a few like-minded countries have developed strong cooperation, **international cooperation** is still quite fragmented. There are around 35 public national cybersecurity strategies and in almost all of them international cooperation is recognized as a critical element. Also, the Draft African Union Convention on the *Establishment of a credible legal framework for Cyber security in Africa* highlights

[5] http://www1.american.edu/initeb/sm4801a/epayment8.htm

[6] http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

[7] http://www.coverity.com/library/pdf/the-software-security-risk-report.pdf

international cooperation as a key element of African national strategies. Despite the relevance given to international cooperation, we have very few examples of proficient partnerships. Europe has been promoting international cooperation since 2006. Still, the European Commission is aware of a "fragmented approach at the European Union (EU) level and the need for stronger political commitment to Internet security efforts and for a strategic and comprehensive approach"[8]. Also the European Network and Information Security Agency (ENISA) firmly believes that EU cyber cooperation is crucial to "establishing a proficient and coherent approach to Network and Information Security (NIS) and this includes coordination throughout Europe as well as worldwide in both the public and private sectors"[9]. EU would also like to extend the scope to cross-border cooperation to enhance European capabilities, for example, to "collect and analyse data relating to information security in a cross-border context which could reveal trends that are not visible at present". There are positive examples in the area of Computer Emergency Response Teams (CERTs) that constitute the best example of cooperation between entities in different countries.

Challenge #2**:** **The nature of the Internet and Digital services is evolving** at an incredible pace, changing the role of the actors involved. National Telecom operators who used to be the key players in telecommunications are now playing a marginal role, as most of the services are delivered and managed by Over-the-top (OTT) operators. Usually, OTT are large international companies with little presence and traction in the users' countries.

Challenge #3**:** Passwords are a major vulnerability for the Internet and Digital Economy. Most of the online services rely on **Digital identities** that are protected by a password. Such security features have been proved to be weak. The number of attacks, incidents, violations, data breaches caused by weak authentication has now reached significant levels. For example, a study conducted by Internet security company BitDefender, has revealed that "over 250,000 user names, email addresses, and passwords used for Twitter sites can easily be found online and that 75% of Twitter username and password samples collected online were identical to those used for email accounts"[10].

Challenge #4**:** Adoption of **smart devices** is increasing constantly and is predicted to reach around 24 billion devices by 2020. There is significant on-going discussion on the "Internet of Things". Use of smart devices is growing and mobile networks are now an affordable alternative to fixed lines. As Ms. Milanesi, Research Vice President at Gartner said, "in 2016, two-thirds of the mobile workforce will own a smartphone, and 40% of the workforce will be mobile".[11] In a few years almost all users will have access to smart devices, providing the opportunity to use new techniques and services to secure citizens. The evolution to the Internet of Things - in which sensors and actuators embedded in physical objects such as household or office appliances, vehicles, roadways, pacemakers - will further increase the number, type and complexity of smart devices. Mobility is considered one of the key challenges to organizations. A study by Lockheed Martin Cyber Security Alliance revealed that almost 7 out of 10 study participants believe that mobile device management is about the security of the devices[12]. In response, the industry is beginning to embed security

[8] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/cyber-exercise-conference/presentations/2.%20Conf%20Paris%20-June%202012-%20-%20A.%20RONNLUND%20-EC.pdf

[9] EU cyber cooperation the digital frontline

[10] http://www.twitip.com/75-use-same-password-for-twitter-and-email-study-finds/

[11] http://www.gartner.com/newsroom/id/2227215

[12] http://www.lockheedmartin.com/content/dam/lockheed/data/isgs/documents/LM-Cyber-Security-Transformational-Technologies.pdf

in smart devices. A study by Eurosmart, an international not-for-profit association that represents the voice of the Smart Security Industry for multi-sector applications, confirms the growth of the Smart Security Industry with the shipment of over 7.6 billion Smart Secure Devices in early 2013 as compared to 5.5 billion in 2010.[13]

***Challenge #5*:** Detection and response are becoming critical aspects of a modern defence approach. As security countermeasures cannot guarantee full security, it is becoming increasingly important to **detect and respond to incidents quickly and effectively**, re-adapting the countermeasures to block future occurrences of the same attack. According to Ponemon Institute “a slow response to any security incident can be extremely costly –and is getting more expensive every year as attacks become more aggressive and sophisticated.” Over the past two years, Ponemon estimates the average time to resolve a cyber attack has grown to 24 days from 18, with an average cost for participating organizations rising to $591,780 from $415,748 – a 42% increase. This "ticking time bomb" is driving explosive growth in an Enterprise Incident Response market predicted to grow to $14.79 billion by 2017.”[14]

Challenge #6: **Awareness is not enough**; it should lead to Informed Action. Promoting awareness is a key element in national strategies and organizational policies. Educating and empowering people and firms to protect themselves online is a key challenge and it is needed to enhance both local and global cybersecurity levels. Awareness however, should be followed by informed action. A successful example is the UK “Get Safe Online” program, the UK government security service to help protect computers, mobile phones and other devices from malicious attack[15].

Challenge #7: Many governments and organisations have developed **best practices** that could reduce vulnerabilities and could help better manage cybersecurity incidents. Unfortunately, usually these best practices are not shared and are underused. For example, if governments and operators of Critical Infrastructures would share practices on Threat Analysis, Risk Assessment and Risk Mitigation, this would lead to a better common understanding of the threats and a much more effective integrated defence. A study by the UK government has estimated that “80% or more of currently successful attacks are defeatable by simple best practice, such as updating anti-virus software regularly”[16]. Also a study of the US State Department has demonstrated a more than 94% reduction in "measured" security risk through the rigorous automation and measurement of the Top 20 Controls[17].

Challenge #8: **Standards** could help both governments and the private sector increase their security, identify better solutions and also make international cooperation easier. The Council of Europe has indicated that the adoption of common standards can “remove barriers, safeguard users, protect the environment, ensure interoperability, reduce costs and encourage competition”. Furthermore, a study of the economic impact of standardization in EU has estimated that standardisation adds between 0.3% and 1% to the GDP thereby helping the ICT industry towards the target of contributing 20% of the EU’s GDP by 2020[18]. There are different types of standards such as technical, functional, mandatory, optional and sector-specific. Each of these is the result of knowledge and wisdom acquired on specific cybersecurity aspects that, when shared, can enhance the capabilities of all users.

[13] http://www.eurosmart.com/about.html

[14] http://www.darkreading.com/management/co3-systems-delivers-security-incident-r/240149362

[15] https://www.getsafeonline.org

[16] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[17] http://www.sans.org/critical-security-controls/

[18] http://www.parlament.gv.at/PAKT/EU/XXIV/EU/12/44/EU_124406/imfname_10415050.pdf

Challenge #9**:** Few **measures/metrics** are available for cybersecurity. In technology, what cannot be measured cannot be protected and this is also valid for cybersecurity. There is a general consensus for the need to define better cybersecurity metrics. In an interview in 2009, Reitinger, Deputy Undersecretary of the US Department of Homeland Security's National Protection and Programs Directorate and Director of the National Cybersecurity Center, believed that better metrics are needed to drive better security practices in the private sector. Currently, the US is developing the "Cybersecurity Framework for improving critical infrastructure" that would also include metrics. A survey reveals that while 75% of respondents state that metrics are 'important' or 'very important' to a risk-based security program, 53% don't believe or are unsure that they are used in their organizations in a manner properly aligned with business objectives. In addition, 51% didn't believe or are unsure that their organizations' metrics adequately convey the effectiveness of security risk management efforts to senior executives[19]. Also, even if governments and organizations are aware of the benefits of using metrics, their definition and management are still considered very complex by many. There is a need for better metrics and performance indicators to be developed and shared.

Challenge #10**:** **Cloud computing** will continue to play a major role in the ICT environment. Cloud technologies have already been adopted by many organizations and their number is expected to increase. According to a Lockheed Martin Cyber Security Alliance survey, at the end of 2012, 39% of responding government IT agencies have planned new investments in cloud computing, while 21% have already invested in cloud solutions. Cloud computing is a big opportunity and will play a major role in tomorrow's economy. Cloud has been identified as the fourth of twelve disruptive technologies that will transform life, business and the global economy. Its projected potential economic impact (2025) has been estimated at $1.7-6.2 trillion along with a 15-20% potential productivity gain across IT infrastructure, application development, and package software[20]. At the same time, cloud computing presents cybersecurity issues at different levels - technical, organizational, procedural and legal – that have to be addressed.

Challenge #11**:** The **online protection of children** is a key challenge in the information society. Kids use technology from an early age and have many chances to socialize online. This, however, exposes them to numerous risks. They can be exposed to inappropriate content or contact, including from potential perpetrators of sexual abuse or violence. Parents, teachers and educators are not sufficiently aware of what happening on the net, and training is not a priority yet. Finally, industry and governments need to proactively promote digital citizenship and help facilitate childrens' positive use of ICTs. Some countries have already taken important steps to implement a child online protection strategy and these can be considered as best practises. International cooperation and collaboration among different stakeholders is the key to ensuring a safer online environment for children.

Challenge #12**:** Despite many countries having launched their **National CERTs**, a large number of the CERTs worldwide do not have the right capabilities and tools. As revealed by ENISA's study, the maturity of national cybersecurity and critical information infrastructure protection (CIIP) strategies and the roles of national/governmental CERTs in these strategies are currently not harmonized between countries and depend strongly on the specific context of a country[21]. Few

[19] http://www.tripwire.com/ponemon/2013/#metrics
[20] http://www.mckinsey.com/insights/business_technology/disruptive_technologies
[21] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

guidelines and resources are available to help countries in establishing their national capabilities aligned with national strategies.

***Challenge #13*:** Most countries do not have a **National Cyber Security Strategy**. EU, African Union and Organization of American States are promoting the definition of National Strategies that address a few common aspects of fighting global threats and include phenomenon that are universally recognized as negative (e.g. child pornography). There is a need for countries to work towards defining their own strategies, basing it on a common set of fundamental aspects.

4. Conclusion

The above sections, while reemphasizing that confidence and security are among the main pillars of the Information Society, highlighted the progress made in the implementation of Action Line C5 since 2005 as well as some of the potential challenges beyond 2015.