**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. Some recommendations are offered at the end for steps forward in strengthening current efforts and provisioning for future technological trends.

## 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.

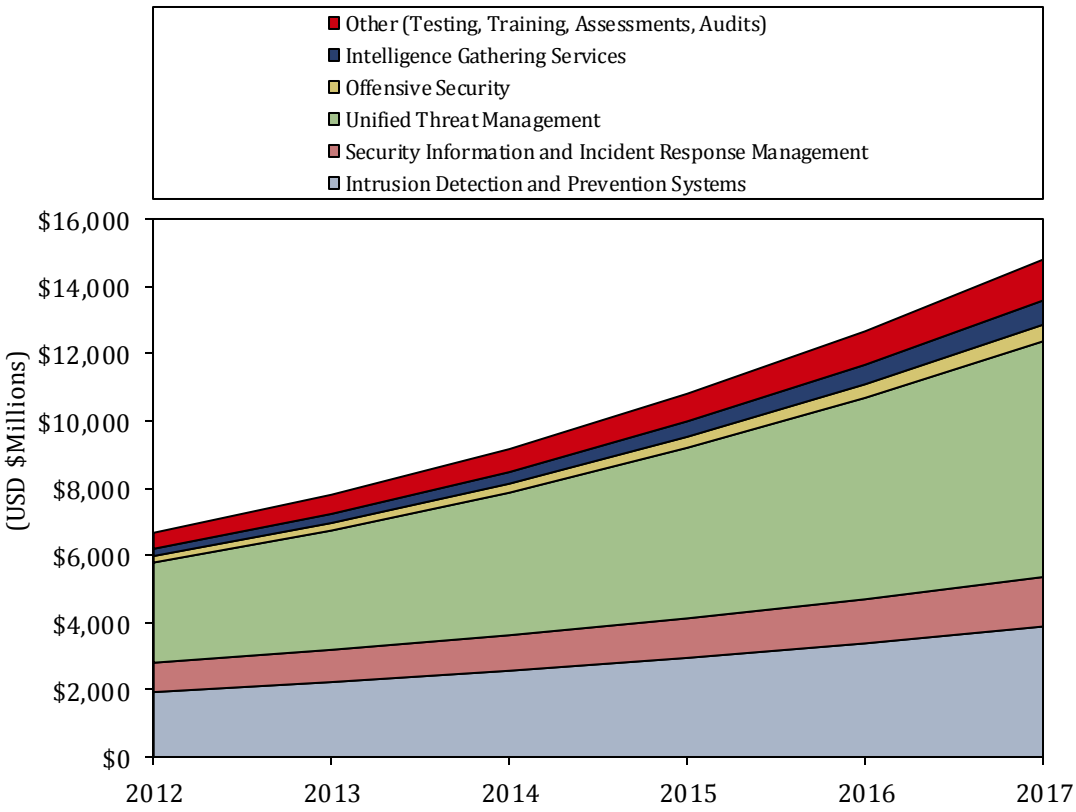
***Use of electronic documents and transactions*:** Electronic payment transaction is growing worldwide; the growth is also due to the improvement of security measures that kept frauds under acceptable levels. In 2001 3.2% of online revenues were lost due to online fraud versus 1.0% in 2011.[3]

***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. ABI Research calculates that in 2012, the enterprise security incident response market totalled $6.67 billion USD and will grow to reach 14.79 billion by 2017. The chart below breaks down the market by product and

[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.jpmorgan.com/cm/BlobServer/13th_Annual_2012_Online_Fraud_Report.pdf?blobkey=id&blobwhere=1320571432216&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs

services.[4] Also, the number of Computer Emergencies Response Teams has increased over the years: FIRST, the Forum for Incident Response and Security Teams has tripled its members in 10 years, from 112 members in 2001 to 275 in 2012.[5]




***Security of Online Transactions*:** In the last several years, the focus on security of online transactions has increased and numerous initiatives have been established in this regard[6].

**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. Symantec Internet Security Threat Report has reported a 42% increase in the number of cyber attacks in 2012 worldwide, with new sectors becoming now targets of Cyber Attacks e.g. Manufacturing (+24%)[7]. 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

[4] https://www.abiresearch.com/press/enterprise-incident-response-market-booms-to-14bn-
[5] http://www.first.org/about/history
[6] http://www1.american.edu/initeb/sm4801a/epayment8.htm
[7] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

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[8].

***Developing a nation-wide approach to cybersecurity - integrated within the overall national ICT policy and strategy:*** Many countries are addressing cybersecurity as a separate element and not as an integral part of the national ICT strategy. Furthermore cybersecurity efforts are often confined to specific elements (e.g. incident response without the supporting legal framework, or regulations without enforcing mechanisms). Finally cybersecurity legislations, harmonized at the regional and international levels, are still not fully developed in several countries and not integrated within the overall cybersecurity efforts.

## 3. Developments and challenges

***Challenge #1*:** The ubiquitous nature of the Internet has facilitated the cross-border emancipation of digital activity, both legitimate and illegal. The lack of adequate supranational cooperative efforts aimed at tackling the issue has been a real boon for cybercrime. While a few like-minded countries have developed strong cooperation through bi-lateral or regional agreements, **international cooperation** is still quite fragmented. ITU identified 35 public national cybersecurity strategies and in almost all of them international cooperation is recognized as a critical element. Cooperation is especially important for effective investigation and prosecution of cybercriminal activity. Regional operational cooperation remains a major challenge in the area of cybersecurity. When confronted with cyber-attacks, traditional mutual legal assistance frameworks have often proven ineffective and new cooperation structures are not yet sufficiently developed.

At the regional level, important initiatives have been undertaken, for example, by the European Union, the Council of Europe, the G8 Group of States, Asian Pacific Economic Cooperation (APEC), Organization of American States (OAS), the

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

Association of South East Asian Nations (ASEAN), the Arab League, the African Union and Network Operations Groups (NOG).[9]

The Draft African Union Convention on the *Establishment of a credible legal framework for Cyber security in Africa* for example highlights international cooperation as a key element of African national strategies. Despite the relevance given to international cooperation, we have 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" [10]. Further 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"[11]. The 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.

At the international level, important initiatives have been undertaken by United Nations General Assembly; International Telecommunication Union (ITU); International Multilateral Partnership Against Cyber Threats (IMPACT) through its partnership with ITU; Interpol; Europol; Organisation for Economic Cooperation and Development (OECD); United Nations Office on Drugs and Crime (UNODC); UN Interregional Crime and Justice Research Institute (UNICRI); Internet Corporation for Assigned Names and Numbers (ICANN); International Organization for Standardization (ISO); The International Electrotechnical Commission (IEC); Internet Engineering Task Force; and FIRST (Forum of Incident Response and Security Teams), among others.

Launched in 2007, the ITU Global Cybersecurity Agenda (GCA)[12] is a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging multistakeholder collaboration with and between all relevant stakeholders and building on existing initiatives to avoid duplicating efforts. Promoting a comprehensive approach, the GCA is built upon five strategic pillars or work areas (1) Legal Measures, (2) Technical and Procedural Measures, (3) Organizational Structures, (4) Capacity Building and (5) International Cooperation.

In November 2013, the United Nations Chief Executives Board endorsed the UN-wide framework on cybersecurity and cybercrime, highlighting seven basic principles for assisting UN Member States in this area. Work on this framework, which began in 2010, was led by ITU and UNODC, and coordinated with the active participation of

[9] ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group, Chapter 1 Legal Measures, subsections 1.2 and 1.3 on existing regional legislative measures and United Nations International Provisions
http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_1.html
http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html
[10] 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
[11] EU cyber cooperation the digital frontline http://www.enisa.europa.eu/media/key-documents/eu-cyber-cooperation-the-digital-frontline
[12] http://www.itu.int/cybersecurity/

all UN agencies. Under this framework, all UN agencies will be working together towards improving internal coordination mechanisms to better serve their members.

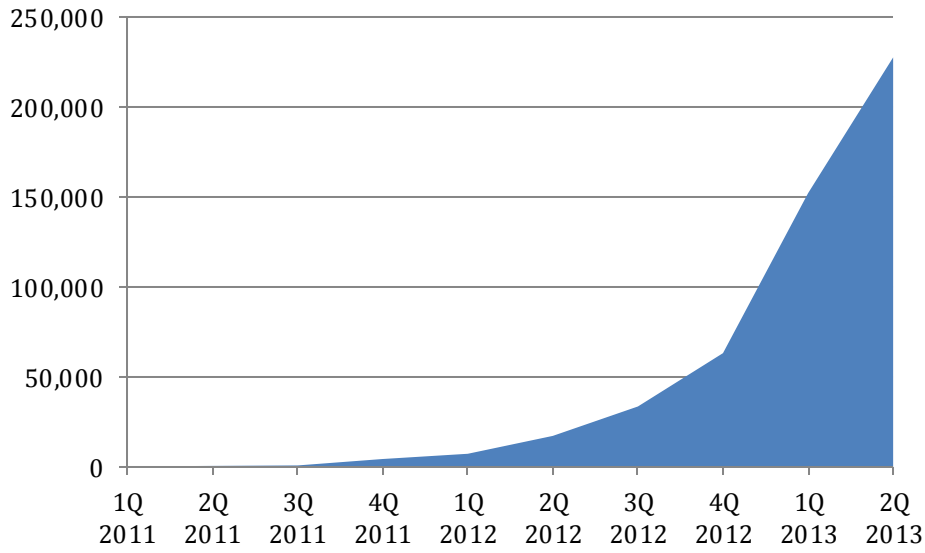
However many of these cooperative efforts remain high-level, with agreement on the necessity for better cooperation, but with little substantive or actionable results in terms of exchanging information or improving legislative procedures. Law enforcement investigations and the sharing of sensitive vulnerability information in particular are especially challenging obstacles to overcome in terms of international cooperation. Different socio-political alignments and interests are the major obstacles to complete cooperation, often resulting in positioning of individual countries with others of similar ideological persuasions. This has been exacerbated by the growing number of nation states that are actively engaging in state-sponsored cyber espionage.[13] This state of affairs has only been brought to light recently and has served to damper international relations.

State-sponsored groups represent the most dangerous threat actors currently because they can take advantage of vaster resources than is currently accessible to lone actors or even organized cybercriminal groups. The nation state sponsored threat actor often uses advanced persistent threats (APTs).[14] They are organized and well-funded, operating a division of labour for different stages of attack, and escalating sophistication of tactics as needed. They have specific objectives, long-term goals, and persistence tools to ensure ongoing access. Nation-state sponsored attacks are relentlessly focused on their objectives and this makes them the most dangerous threat actors today, and the primary inhibitor of international nation-state cooperation for the fight against cybercrime.[15]

***Challenge #2:*** Malware is becoming **increasingly complex**, using a variety of tools and techniques to mount high-level cyber attacks that can thwart even the most comprehensive cybersecurity defences. Cyber attacks directed against organizations have grown both in numbers and sophistication over the past decade to the point where breach and data theft have become all too common. Three basic levels of malware sophistication have emerged.

The first group is basic malware that is not targeting anyone in particular and has already been analysed and categorized by security companies. This type of malware can be detected at numerous stages through their signatures with up-to-date anti-virus solutions. Low-level malware includes ransomware, which locks users out of their desktops, and fake antivirus products. A high incidence of low-level malware occurs on mobile operating systems. ABI Research aggregated statistics from a number of antivirus companies in order to get a more inclusive view of malware sample evolution. By Q2 2011, on average 765 unique samples were floating around in the wild. By Q2 2013 reaching, the number of samples reached 227,750 samples. Chart 1 below illustrates the growth curve.

[13] World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, FireEye, http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf
[14] Cyber Espionage: The harsh reality of advanced security threats, Deloitte, https://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_cyber_espionage_07292011.pdf
[15] THE CYBER ESPIONAGE BLUEPRINT: Understanding Commonalities In Targeted Malware Campaigns, Alex Cox, Principal Research Analyst, RSA FirstWatch, https://blogs.rsa.com/wp-content/uploads/2013/07/BLUEPRINT_WP_0713_final.pdf




The second level is slightly more developed malware, often part of a package, and generally commercially available in the darknet markets, with additional possibilities of tailoring the malware for specific targeting. This category includes remote access Trojans (RATs), which enables intruders to gain unauthorized administrative access to a target computer. Exploit kits are at the higher end of this category, exploiting vulnerabilities and finding zero-days to facilitate delivery of malicious payloads, such as RATs. Malware in this category includes infamous tools like Zeus, the banking Trojan and corresponding botnet[16], and backdoors like DarkMoon/Poison Ivy.[17]

Top-tier malware makes up the third level and most sophisticated level of malware. These are high-end exploit kits, such as Black Hole, and custom-made malware like Stuxnet. These types of malware are often targeted, can use a combination of social engineering techniques, unique code, and zero-day exploits. Malware of the Stuxnet kind appear to be backed by nation states. Their creators, therefore, have access to greater resources than organized crime, meaning their development and deployment is not necessarily constrained by financial requirements.

Sophisticated targeted attacks are called advanced persistent threats (APTs). An initial compromise will establish a foothold before seeking to escalate privileges and undertake internal reconnaissance in order to identify their target data. This means moving laterally across the organization and accessing other servers and files. They maintain their presence by deploying persistence mechanisms until they can complete their mission by packaging and stealing their target data. Often, those attackers deploying APTs will use the least sophisticated tools first to try and get the job done. This includes buying off-the-shelf black market products. It also means that they will target the weakest link in the value chain – whether these are third-party service providers or smaller players further down the supply chain.

***Challenge #3:*** **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 increasingly at risk of becoming simply "dumb pipes", as many services are increasingly delivered and

[16] http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99
[17] http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=24379
http://www.symantec.com/connect/blogs/java-zero-day-used-targeted-attack-campaign

managed by Over-the-top (OTT) service providers. Usually, OTT are large international companies with little presence and traction in the users' countries.

At the moment, the global telecoms industry seems to be in relatively robust health; developing economies are driving subscriber and revenue growth, 4G is being rolled out, smartphones are being connected with data plans in huge numbers, service providers are selling bundled integrated offers to maintain revenues, and costs are being controlled with network sharing and other strategies.[18]

A macro-analysis of mobile carrier revenue is misleading however, the continued growth of developing markets is concealing the challenges being faced in more advanced markets where subscriber saturation has seen the market move into a replacement cycle and increased price pressure as the market matures. Mature markets are indicative of the future of mobile carrier revenues and profitability in the future. Carriers in Western Europe for example have been losing out on messaging revenues to OTT players like WhatsApp, Skype, and Viber, or suffering outright reductions in revenues and subscriber numbers. Western Europe does have a more competitive and regulated economic environment than most other markets, but it is still indicative of the future evolution of the carrier market worldwide.

It is also worth noting that revenue growth is not keeping up with subscription or connection growth. So while more and more devices are being connected, average revenue per connection (ARPC) is falling and putting further pressure on the subsidy model.[19] Globally the vast majority of new subscribers will be low income individuals producing low ARPU further exacerbating this trend. Higher data traffic requires more investment in mobile networks and handset subsidy is increasingly driven by competitive pressure rather than strategy. Carriers found themselves in the position of the enabler of mobile data through network CAPEX expenditure and device subsidy, but not necessarily the main beneficiary of higher revenue generation and therefore return on investment. From the security standpoint, the rapid growth of connections and subscriptions forced companies to upgrade security features and in certain cases to make significant investments in building back-end security infrastructures to support the business, without pushing such security toward end users.

Text message use, for instance, a killer application that for years has generated a decent revenue stream for carriers, is falling.[20] Smartphones began to use instant messaging on their devices, like BlackBerry's BBM or OS agnostic WhatsApp. The use of instant messaging for no extra charges, if users have a data plan, is widespread among heavy messaging young users. However, in some instances, the security associated to such recently developed applications may not be adequate to protect the content exchanged.

Plenty of other ideas, from mobile money to M2M[21] to API exposure[22] have been the subject of huge efforts by carriers.[23] As yet, none has really driven revenue compared

[18] Carrier Strategies to Alleviate the Capacity Crunch: Spectrum Sources, RAN Technologies, and Network Topology, https://www.abiresearch.com/research/product/1016087-carrier-strategies-to-alleviate-the-capaci/
[19] Mobile Carrier Operating Performance Assessment, https://www.abiresearch.com/research/product/1015907-mobile-carrier-operating-performance-asses/
[20] Future of Voice and Messaging – WebRTC and Telco APIs https://www.abiresearch.com/research/product/1014539-future-of-voice-and-messaging-webrtc-and-t/
[21] Machine to Machine communications
[22] Application Programming Interface offered by telecom operators to developers
[23] Convergence of Social Networking and M2M Services, https://www.abiresearch.com/research/product/1016360-convergence-of-social-networking-and-m2m-s/

to the legacy telephony and SMS services that still make up a large share of most operators' top line revenues. The only bright spot has been plain vanilla Internet access, initially with 3G dongle modems for PCs, and more recently for smartphone data plans. But the former has stopped growing and the low cost unlimited data bundles and user traffic are creating unprofitable subscriptions. Carriers are currently losing the revenue generation battle for the next generation of digital services.

There is increasing concern that this loss of control over mobile data traffic translates into loss of control over the security of carrier networks. However, carriers are in a very favourable position to provide network security at the macro-level. Ownership of the infrastructure provides the unique possibility of cybersecurity service provisioning for mobile networks, especially in 3G and 4G deployments. For carrier Wi-Fi and small cell deployments are still highly vulnerable technologies, open to man-in-the-middle attacks, and interception. Not all carriers are deploying IPsec protocols over their next-generation networks. Carriers have the opportunity to offer dedicated business services centred on secure networking and interconnection that could serve highly sensitive industries, such as government, healthcare, or finance. This may enable new revenue streams in a decreasingly profitable consumer subscription market.

As an overall consideration, we are witnessing a shift in the provision of some ICT and related information services from traditional operators (such as National Telcos) to global companies (such as OTTs), with new challenges emerging regarding adequately addressing some aspects such as ensuring confidentiality, integrity and availability of the information exchanged.

***Challenge #4*:** Lack of strong authentication mechanisms for verifying identities and granting access to online resources are challenges in combating fraud and forgery.[24] 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"[25].

The problem with passwords is that often individuals will use weak passwords, or use the same password multiple times across different sites. This poses a big problem for security. For this reason it is preferable to use several security mechanisms in order to provide additional security measures if weak passwords are being used. Passwords are not necessarily obsolete however. One Time Passwords (OTP) for example can provide a high level of security. OTPs are one of the most secure ways to protect endpoints and systems although they often need to be used in conjunction with another mechanism to generate the password. Further, if the password is unique and complicated enough, it may be suitable. The eradication of passwords is therefore unlikely to happen in the near future, but increasingly passwords will be used in conjunction with other tools, as in the case of multi-factor authentication through the use of mobile phones, or even biometrics (fingerprint readers, voice recognition, or face recognition) to increase access and identification security.

[24] Mobile Authentication & Encryption,
[25] http://www.twitip.com/75-use-same-password-for-twitter-and-email-study-finds/

Multi-factor authentication is the most likely way forward, since OTPs can be used with mobile devices, and at its simplest form, through an SMS sent to a feature phone for example. It may be the most ubiquitous and cheapest way to deploy multi-factor authentication since the identity of an individual can be tied to the smartcard in their phone and authenticated by the carrier. However, the cost and complexity of deploying multi-factor authentication is the major barrier and most available solutions are not yet conducive to a seamless and user-friendly experience. Users are unlikely to undertake repeatedly long and complex authentication mechanisms to access the growing number of digital accounts to which they subscribe.

Behavioural authentication is a fledgling technology that may answer some of the issues of intuitive and easy access without compromising security. Authentication can be done by matching the way a user interacts with a program or device to determine whether it is the same user behaviour patterns as registered to an identity. If the program decides that it is not, it could prompt the user for a password for example. This technique however is still nascent and is yet to emerge as a fully-tested concept.

Another technology that is emerging slowly but still faces considerable hurdles is device fingerprinting or identification. A device fingerprint is a set of system attributes that takes a combination of values that is unique for each device and can serve as a device identifier. The fingerprint itself is generated by creating a hash[26] of all the values obtained and may then be used as identifiers for authenticating the device. The list of attributes can include: plug-ins, screen size, language settings, time zones, secure cookies, flash objects, user agent string, browser characteristics, device hardware configuration, network characteristics, geo-location, and historical context.

One advantage of smart devices is the growing sophistication of sensors that can verify user identity. The advance of touchscreen functionality and micro-electro-mechanical systems (MEMS) can greatly improve user authentication or be used to encrypt data stored on mobile devices. Sensors can be used to record and validate biometrics, such as fingerprints, voiceprints, and iris scans, among others. Apple's recently released iPhone 5S, for example, incorporates a fingerprint recognition feature, the Touch ID. It allows users to unlock phones and validate purchases on Apple digital media stores. The fingerprint information is stored within the device, rather than on the cloud, thereby minimizing the risk of external access. Handwritten signatures are the oldest form of biometric authentication and can now more easily be implemented on touchscreen devices. Other sensors, such as the accelerometer, gyroscope, ambient light sensor, magnetometer, or multi-touch, can also be used to effect touch gestures for authentication and encryption. Innovative research in this area is focused on a mix of different technologies and sensors.

Major hurdles need to be overcome before mobile device sensors can be successfully used for authentication and encryption that can meet corporate requirements. Sound acquisition may be degraded, due to a loud environment, for example, or will vary based on the quality of the embedded microphone. Facial recognition will depend on light quality and the resolution of the camera. Other effecting factors inherent to the device include processing power and memory. These issues need to be resolved before such authentication mechanisms can hope to effectively counter the growing cybercriminal threat.

***Challenge #5*:** Adoption of **smart devices** is increasing constantly and is predicted to reach around 24 billion devices by 2020. The emergence of connected smart devices other than smartphones and tablets is increasingly being made possible by the growth

[26] A hash function is any algorithm that maps data of arbitrary length to data of a fixed length.

of machine to machine (M2M) communications. The much anticipated outcome of increased M2M connections is the emergence of an Internet of Things (IoT). As the IoT merges with human social interaction, the advent of an Internet of Everything nears and purports to structure next generation societies.

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".[27] In a few years almost all users will have access to smart devices, providing the opportunity to use new techniques and services to secure use. The evolution to IoT - in which sensors and actuators embedded in physical objects such as household or office appliances, vehicles, roadways, electricity meters, pacemakers, and various wearable devices - 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[28]. In response, the industry is beginning to embed security 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.[29]

As smart devices enable better M2M communications, the number of deployments is set to surge. However, the technology's continued success will depend on its ability to respond to a number of pressing challenges. M2M needs to be not only reliable, but also future-proof. This means integrating features, such as security, that have become de facto standards for other information and communications technology (ICT). Minimally, security must protect the confidentiality, integrity, and availability of data in M2M communications. This is becoming imperative as M2M is increasingly used in critical infrastructure settings, such as industrial control systems (ICS) for the energy sector, and telemedicine and eHealth.

Currently, the M2M landscape lacks basic security requirements. Key organizations, such as the European Telecommunications Standards Institute (ETSI), the Telecommunications Industry Association (TIA), the International Telecommunication Union (ITU), the Open Mobile Alliance (OMA), and the Alliance for Telecommunications Industry Solutions (ATSI), have developed a number of vertical-specific standards. However, almost all the security requirements in these standards primarily address network security.

The real issue is the consistent lack of interoperability as applied horizontally across M2M applications. Such a shortfall could be a serious impediment to the continued growth of M2M applications, and by default IoT, if not addressed in the near future. The effective delivery of M2M services and applications relies on the functionalities provided by the M2M core. These include naming, addressing, mobility management, service control, application interaction, QoS, and security aspects, among others. Since M2M can be deployed using a number of different technologies (cellular, Wi-Fi, WiMAX, RFID, etc.), the functionalities can be provided by various entities including mobile network operators (MNOs), enterprises, or industrial operators.

[27] http://www.gartner.com/newsroom/id/2227215
[28] http://www.lockheedmartin.com/content/dam/lockheed/data/isgs/documents/LM-Cyber-Security-Transformational-Technologies.pdf
[29] http://www.eurosmart.com/about.html

Such diversity makes coordination of interoperability efforts difficult at the application level and even more so deeper into the specific core functionalities.

Consequently, security at the application level is slow to develop, since it is much simpler and more cost-effective to deploy network security. M2M security is primarily ensured at the gateway level, using firewalls and anti-virus solutions, and at the communication level through encryption. The M2M device itself is generally left unsecured and as they increasingly connect to enterprise backbones, such exposure poses a risk by providing a vulnerable backdoor into the network.

Although M2M threats are still few and far between, security researchers have been exposing vulnerabilities in M2M applications for some time. These affect a range of different sectors, from automotive to ICS and medical devices. Some of these findings are significant and exploitation of their vulnerabilities could be potentially life-threatening. The concern is that hackers could access M2M devices over the Internet. At a minimum, they would invade privacy and, in a worst case scenario, take control and cause malicious damage to M2M endpoints.

Telemetry is becoming more and more popular, including for locking and starting automobiles, and on-board entertainment. Yet, these systems have been the object of a few successful hacking attempts. In 2011, security firm iSec Partners managed to breach an M2M module in an automobile, obtaining information about programmed commands the module had received over SMS. The firm then replicated the SMS messages using another device, allowing them to unlock the doors and start the car remotely.

Perhaps of greater concern is the exploitation of M2M in critical infrastructure applications. Security researchers have exposed a number of inherent vulnerabilities in ICS using Supervisory Control and Data Acquisition (SCADA) systems. As these systems increasingly connect to the Internet, their vulnerabilities become exposed to the wider world. Stuxnet is the first known large-scale virus to have been deployed against ICS. Its discovery in the wild not only revealed that exploitation of ICS vulnerabilities is possible, but also that it can be highly effective.

The limited security features of M2M applications in this scenario are worrying, to say the least. M2M satellite services, for example, are popular among large-scale and geographically dispersed industrial installations, such as smart grids and oil and gas fields. The resulting environmental disasters and monetary costs associated with disrupting M2M communications could potentially be huge. Critical infrastructure is already the object of repeated and persistent cyber espionage on a global scale and it is just a small step from surveillance to destructive sabotage.

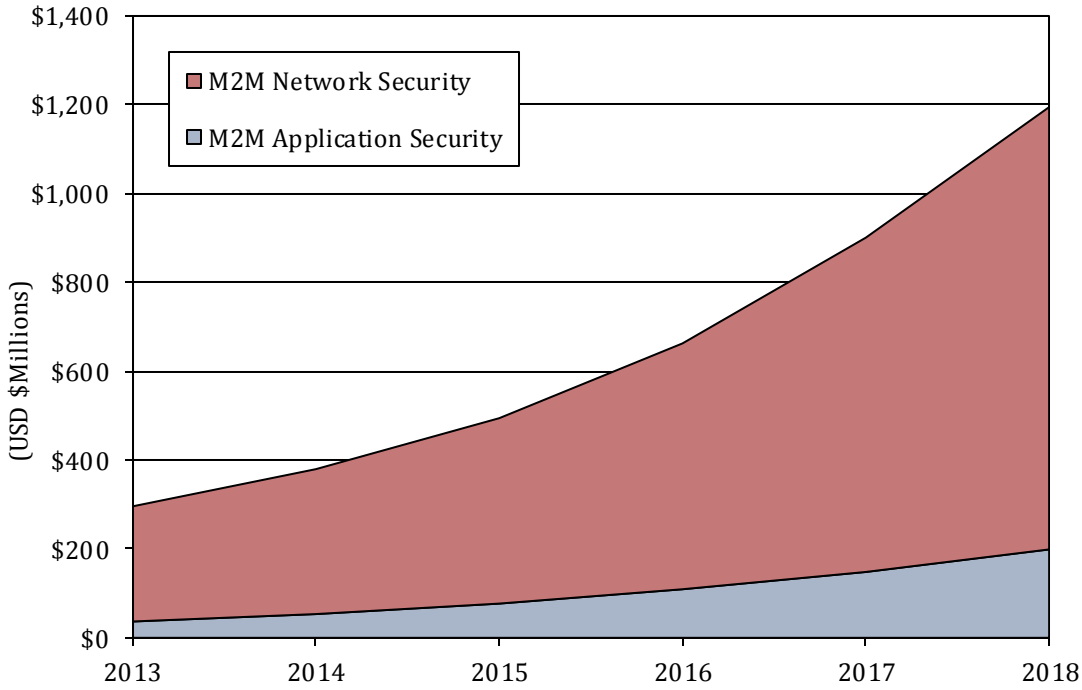
Another sector that has been the focus of security scrutiny is eHealth and medical devices in particular. The increasing connection of software-controlled hospital equipment and associated medical devices has been particularly useful for patient care delivery and monitoring. Security research, however, reveals that hospital equipment and computers are highly vulnerable to malware, which means that infections can have serious repercussions on patient-monitoring systems.[30] The

[30] http://web.eecs.umich.edu/~kevinfu/
NIST Information Security And Privacy Advisory Board (ISPAB), http://csrc.nist.gov/groups/SMA/ispab/index.html
US Government Accountability Office MEDICAL DEVICES: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices http://www.gao.gov/products/GAO-12-816
Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility, http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm189111.htm

problem is that most of the equipment is made specifically for medical applications and many health-related systems run on commercial off the shelf (COTS) software that has been tailored specifically for the industry in accordance with health regulations. Once connected to the Internet, malware and other threats easily propagate to all other connected devices in the network including mobile medical devices.

Recent academic publications from MIT[31], the University of Massachusetts, the Swiss Federal Institute of Technology, and the French National Institute for Research in Computer Science and Control[32] have gone some way in addressing the security issues for such devices. However, there is still a long way to go before such research is practically applied, tested, submitted for regulatory approval, and installed and deployed in medical devices and other eHealth systems.

ABI Research calculates that the global M2M security market will be worth $295.72 million by the end of 2013, growing to $1,193.85 million by 2018. The chart below illustrates the revenue breakdown by segment for the M2M security market for the forecasted period.




***Challenge #6*:** High-profile enterprises, such as multi-national organizations, and those in critical sectors, such as finance, energy, and pharmaceutical, for example, will be preferred targets across all threat actor groups. Valuable data often targeted in these sectors include patents and other intellectual property (IP) rights; information related to mergers, acquisitions, and joint ventures (JVs); executive strategy documents; financial account information; and management and IT staff credentials, among other data.

The malware used to obtain enterprise data is not always very sophisticated; in fact, it rarely is. Threat actors will attempt to breach an enterprise's security using the simplest tools and many of these attempts can be countered relatively easily if adequate security measures are in place. However, certain actors perpetrate persistent

[31] http://www.technologyreview.com/news/425059/personal-security/
[32] http://www.technologyreview.com/news/416214/keeping-pacemakers-safe-from-hackers/

threats in specific sectors that will be difficult to detect, let alone counter. Enterprises targeted by APTs will likely suffer a breach at some point in their existence, if they are not already affected.

For this reason, intelligence and effective incident response mechanisms are key advantages for organizations. Understanding the threat landscape, the nature of current attacks, and the motivations of threat actors can improve responses to attacks and mitigate threats at the enterprise level. 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.

There is no doubt that the majority of large organizations today will suffer from some form of incident breach during their lifetime. One reason for this is that most companies are generally unaware of threats and do not fully understand the value of data. Security beyond simple anti-virus solutions and a firewall is not seen as a necessary requirement. IT personnel are limited by budget requirements and management usually understands the security issue even less than their IT counterparts. Many organizations find it difficult to justify spending money on potential threats that may or may not happen. It is usually only after a breach has occurred that an enterprise will start reassessing their security strategy.

In many cases, breach and data theft will have been ongoing for some time and the damage done to the enterprise will already be significant. An alarming 94% of companies investigated learn about the breach from an external source, normally law enforcement or press releases from hacktivist groups. And even more worryingly, an average number of days that elapse before a breach is discovered is 416 for large enterprises.[33]

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."[34] 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.

The real problem is that cost and supply are real barriers to the implementation of adequate security policies and products. It involves people with specialist skills and experience, as well as knowledge of the problem. One single solution cannot solve all problems – the issue requires a combination of different hardware, software, and personnel. This requires long-term planning, training and education, spending, and critically, a change in business practices.

In recent years, organizations are seeing the importance of deploying intrusion detection systems (IDS) and intrusion prevention systems (IPS), security information and events management (SIEM) systems, and unified threat management (UTM) systems to minimize losses due to security breaches and to adhere to pro-actively protecting systems and data to ensure regulatory compliance. This encompasses an increasing market in services including CIRT/CERT/CSIRT training, systems testing, as well as security assessments and audits. In addition, there is an emergence in intelligence gathering services as well as offensive security products by those

[33] Verizon 2013 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2013/
[34] http://www.ponemon.org/news-2/44

enterprises that have the budget, in an effort to anticipate future attacks or even strike back against attackers.

***Challenge #7:*** The lack of public awareness of new threats, such as APTs and mobile threats and vulnerabilities is hampering the full development of a global culture of cybersecurity. End-users and individual consumers have not yet realised the full implications of not securing their devices and personal data, despite the surge of mobile malware and social networking frauds in the past few years. Many view their smart devices as different pieces of equipment to their PCs, thereby dismissing potential threats to mobile platforms as irrelevant. It may take some time, and perhaps even a global mobile virus infection, to attract the attention of end-users and make them aware of the dangers of unprotected devices. Awareness-raising is an important aspect of ensuring better practices are undertaken at the personal level.

However, current efforts in **awareness-raising are not sufficient**. A successful awareness campaign should lead to informed action. Promoting awareness is a key element in national strategies and organizational policies. Educating and empowering people and organizations to protect themselves online is a key challenge and it is needed to enhance both local and global cybersecurity levels. Governments need to do more to support awareness-raising efforts that lead to effective informed action.

The best guarantee for cybersecurity is the development of a reliable cyber-culture, with established norms of behaviour that users follow voluntarily. However, such a cyber-culture has to be nurtured. Useful guides in this area are the UN General Assembly Resolution 57/239 on the Creation of a Global Culture of Cybersecurity and the OECD's Guidelines for the Security of Information Systems and Networks. Yet it is usually the prerogative of sovereign states to create frameworks that can push users into informed action. Sovereign states also command the resources needed to address these issues.

However, resources are unequally distributed and countries need to prioritize resources to support cybersecurity. Cybersecurity needs the development of a cyber-culture and acceptable user behaviour in the new reality of cyberspace, but it is also based on norms of correct behaviour and the capacity to pursue wrong-doers and bring them to justice, albeit in the online world. The need to deter cybercrime and prosecute wrong-doers is universal, even for countries with low Internet access rates. However, countries' capacity to promote cybersecurity is uneven and countries must build capacity to address these issues. There is only limited authority to impose national laws on the borderless environment of the Internet, therefore voluntary collective action is important for improving security.

Further, capacity-building to promote cybersecurity is complex, for several reasons. Cybersecurity has long been considered as a technical field, belonging to specialized agencies. In addition, global connectivity and instant communications mean that every country have to initiate actions to promote cybersecurity at the national level.

Mechanisms for awareness-raising certainly vary between countries, as do needs and methods. The leading role is often taken by non-governmental organizations, but government and the private sector need to take on more actionable roles. For governments, building a culture of cybersecurity includes incorporating safe online behaviour lessons into school curricula. Many countries have in fact already done this. 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 attacks[35].

The private sector can also take the initiative. In Estonia, the private sector (e.g., the financial sector and telecommunication operators) decided that a safer Internet would directly benefit their business. In 2006, they established the ambitious goal of becoming the most cyber-secure nation by 2009, and launched an awareness campaign, dedicated website and projects using Public Key Infrastructure and digital ID cards, that were already in use by the government.

For awareness campaigns to be effective, it is vital that decision-makers are fully informed, in order to become champions for the cause. This is best accomplished by educating decision-makers and by keeping cybersecurity in the news. Awareness campaigns should also educate key decision-makers in government.

***Challenge #8:*** Many governments and organisations have developed **best practices** that could reduce vulnerabilities and could help better manage cybersecurity incidents. Unfortunately these best practices are not always shared and are underused. The reasons are varied. Most governments in developed countries in North America and Europe actively share best practices and guidelines publicly. ENISA, NIST, US and EU CERTs are highly active in this sector. However, private sector operators are much less likely to share best practices, and therefore knowledge about the effective application of such best practices in industry remains largely unknown. Further, there is real hesitancy to share threat and vulnerability information for fear of enabling either enemy states or competitors to take advantage of this information against the disclosing party. A lot of information sharing goes on behind closed doors, in small groups and between limited partners.

There is no doubt that the sharing of actual best practices on Threat Analysis, Risk Assessment and Risk Mitigation, would lead to 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"[36]. Also a study of the US State Department has demonstrated more than 94% reduction in "measured" security risk through the rigorous automation and measurement of the Top 20 Controls[37].

A limiting factor to the integration of best practices or the dissemination of such guidelines or information about threats is the often voluntary nature of these activities. Certainly the private sector's interest is in monetization opportunities, and governments are also fearful of exposing too much information about their own weaknesses. Regulation in terms of cybersecurity compliance requirements could help in making disclosure compulsory. However, some experts suggest that the way forward would be a legal requirement for organizations to implement at the very least some form of information governance structure.

The industries currently adopting information governance frameworks are essentially those that are heavily regulated in terms of data protection: healthcare facilities, medical service providers, financial institutions, payment processors, military and defense contractors, government agencies and public sector departments. These

[35] https://www.getsafeonline.org
[36] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[37] http://www.sans.org/critical-security-controls/

sectors are particularly concerned because they are data controllers and often hold personally identifiable information. Military and defense contractors are recipients of state secrets and sensitive national information that requires a high level of security.

Critical infrastructure operators in sectors such as energy, water management, and transport are still far behind comprehensive adoption and integration of information governance frameworks. They will likely be increasingly turning to such frameworks as regulatory requirements are imposed on them in the name of cybersecurity. The national strategies announced in the United States and the European Union indicate that auditing security systems and compulsory reporting of serious incidents will eventually become the norm. Services such as Security Information and Event Management (SIEM) and Intrusion Detection/Protection (IDS/IPS) management offer promising solutions in this area.

Increasingly, however, the advantage of having a well-planned information governance structure (including information security) is conducive to bettering core business models and modes of operation. The current progression and expansion of cybercrime means that most organizations with a digital presence will eventually have to deal with an incident. Automated malware, drive-by downloads, the growing connectivity of mobile devices, and the advent of the IoT reinforce the notion that machine connectivity will be ubiquitous and cybercrime will continue to expand. The burden will increasingly come to lie at the victim's door. Legitimate organizations have the most to lose: they will need to deal not only with cyberthreats, but also with the consequences of deficient security. Liability can be controlled however with a well-implemented information governance framework.

Information governance underlies the very idea of corporate governance. Consequently, organizations are finding it difficult to address the issue and best protect corporate assets. They need to successfully navigate through compliance requirements, estimate risks in order to minimize cost, and sift through the hoard of market offerings to select the solution that will best suit their needs. Government support in terms of greater dissemination of best practices and guidelines would go a long way in enabling better application of information governance within organizations.

***Challenge #9:*** **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[38]. 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.

Different laws in different countries impose cybersecurity related requirements on various sectors, but each law covers a different set of entities. Some entities, such as power marketing administrations,[39] health administrations, or financial institutions are required to comply with more than one law when implementing cybersecurity.

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

[39] A Power Marketing Administration (PMA) is a United States federal agency within the Department of Energy with the responsibility for marketing hydropower, primarily from multiple-purpose water projects operated by the

With regards to general information security standards, the most often applied by financial institutions include the International Telecommunication Union (ITU) X.509 standard on public-key and attribute certificate frameworks. This standard has been further elaborated by the Internet Engineering Task Force's (IETF) Public-Key Infrastructure (PKI) Working Group. PKI is widely used for transaction and data security. All financial institutions use some form of encryption, whether based on PKI or a proprietary encryption algorithm.

ITU-T Study Group 17 (SG 17) is the lead study group on Security and Identity Management. SG 17 continues to be instrumental in standardization activities in the area of cybersecurity (ref. Recommendations ITU-T X.1500 series), anti-spam, identity management, X.509 certificates, information security management, ubiquitous sensors networks, telebiometrics, IPTV security, virtualization security towards cloud computing security, and security architecture and application security, often in cooperation with external Standards Development Organizations (SDOs) and Consortia.

In the financial domain, the International Standard Organization (ISO) has formed the JTC 1/SC 27 IT Security Techniques committee in cooperation with the International Electrotechnical Commission (IEC). This group has issued numerous standards on digital signatures, message authentication codes, entity authentication, hash functions, key management, trusted platform modules, evaluation criteria for IT security, cryptography, encryption algorithms, time-stamping, and identity management, among others. Perhaps the most renowned and widely-used standard series is the ISO/IEC 27000, which deals with information security management systems.

Other organizations developing standards in information security include the World Wide Web Consortium (W3C), the Organization for the Advancement of Structured Information Standards (OASIS), and the NIST Information Technology Laboratory (NIST ITL). Most of these organizations propose standards that are used equally across all types of sectors and industries.

The cybersecurity requirements imposed by laws also sometimes take the form of standards, as in the case of the NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) standards. However, the word standard is also used to identify cybersecurity guidance and strategic documents (e.g., NIST [National Institute of Standards and Technology] standards, such as SP 800-82) and consensus technical standards (e.g., ISO 27001), as well as regulatory mandates. Standards describe uniform engineering or technical criteria, methods, processes, and practices and may actually be a regulatory requirement.

The confusing proliferation of standards and guidance on cybersecurity has understandably made it more difficult for individual operators and organizations to quickly determine what is required of them and has certainly posed a challenge for those who would like to review or provide input to the many parallel efforts.

For example, the U.S. government, through NIST, has issued many standards, and best practice guidelines over the years. The most notable is the 2001 Federal Information Processing Standard (FIPS) Publication 140-2. FIPS is essentially a computer security standard used to accredit cryptographic modules, with the aim of coordinating the requirements for cryptography modules that include both hardware

Bureau of Reclamation, the U.S. Army Corps of Engineers, and the International Boundary and Water Commission.

and software components. FIPS provides security accreditation for both proprietary and open source cryptographic modules. Accredited technologies can then be used in government departments and regulated industries such as finance and healthcare, although both sectors also have further standards and legislation for data protection. While essentially specified for US based entities, many foreign nations and organizations often look to NIST standards since often it is esteemed as a leading authority on the latest and most comprehensive cybersecurity standards development.

Standards use within the financial sector is highly advanced. The financial sector has also developed its own standards, but from a private sector perspective. The Payment Card Industry Data Security Standard (PCI DSS) is essentially a technical proprietary standard, resulting from collaboration between major credit card vendors (e.g., American Express, Discover, JCB, MasterCard, and Visa). The standard does not exclusively address encryption, but it does include a measure that requires encrypted transmission of cardholder data across open and public networks. The standard has been adopted into law in three U.S. states: Minnesota, Nevada, and Washington. Breach of the standard is essentially viewed as a breach of contractual obligation. The payment providers themselves can fine up to $200,000, depending on the number of violations, or could permanently ban a violator from the card acceptance program.

The ISO TC68 standard is specifically developed for financial services security. The SC2 subcommittee, in particular, is composed of four working groups: PKI management for financial services; encryption algorithms used in banking applications; security in retail banking; and information security practices. Over the past decade, they have published a number of financial security-related standards.[40]

Currently under development by the committee are a standard for cloud security and multiple standards for various implementations of mobile security. It is clear that the financial community is requesting standards that are aligned to the current market direction and recognize that security is an essential element if they want to avail themselves of emerging technologies such as cloud computing and mobile payments.

The healthcare sector is also subject to data protection requirements in most countries. In the US, the Health Insurance Portability and Accountability Act (HIPAA) includes security and privacy requirements for computer systems and for Personal Health Information (PHI). The technical safeguards specifically require encryption be used when information is transmitted over open networks. The Health Information Technology for Economic and Clinical Health Act (HITECH) was enacted in 2009 to complement HIPAA for implementing and managing an adequate Electronic Health Records (EHR) system. The act also offers financial incentives for demonstrating meaningful use of EHR systems, which can be a significant driver for implementing data encryption solutions. Other notable legislation in the United States includes Sarbanes Oxley (SOX)[41] and the Gramm-Leach-Bliley Act[42]. Canada has followed in a similar suite with the Personal Information Protection and Electronic Documents Act (PIPEDA).

[40] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=49650&published=on&development=on

[41] The legislation came into force in 2002 and introduced major changes to the regulation of financial practice and corporate governance. http://www.soxlaw.com/

[42] The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

In 1999, the International Organization for Standardization and the International Electrotechnical Commission jointly published the Common Criteria for Information Technology Security Evaluation[43] to provide IT security evaluation guidelines that extend to an international community. The assurance requirements, including pre-packaged sets of Evaluation Assurance Levels (EALs) in the Common Criteria (CC), represent the paradigm that assurance equal evaluation and more evaluation leads to more assurance.[44]

Standards can play a major role in ensuring that organizations deploy the best and the latest security mechanisms. The heavy involvement of institutions within the standardization process has had positive effects for bolstering security as a whole. However, these efforts are still highly fragmented and disparate, serving first and foremost those industries which have the resources to invest in standardization. The greatest challenge is for governments to pull ahead and actively support standards development through public-private partnerships and international cooperation.

***Challenge #10*: 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, Philip Reitinger[45], Deputy Undersecretary of the US Department of Homeland Security's National Protection and Programs Directorate and Director of the National Cybersecurity Center, noted 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[46]. 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.

A primary obstacle is that cybersecurity is a sensitive issue, whether from a government or private sector perspective. Admission of vulnerabilities can be seen as a weakness. This is a barrier to the discussion and sharing of threat information and best practices, as outlined previously. Yet security through obscurity is not a viable defense model against modern cyber threats. The answer is to implement cybersecurity mechanisms in all layers of society. However, the drive and the incentive to do so are inadequate, either due to cost constraints or simply lack of awareness. A first step towards remedying the situation lies in comparing cybersecurity capabilities of nation states and publishing an effective ranking of their status. A ranking system would reveal shortcomings and motivate states to intensify their efforts in cybersecurity. It is only through comparison that the real value of a nation's cybersecurity capability can truly be weighed.

That being said, cybersecurity is a significantly wider discipline than the scope of cybercrime. Cybersecurity includes aspects of encryption technologies, digital

[43] ISO/IEC 15408, Oct. 1999, http://www.commoncriteriaportal.org/cc/
[44] Developer-Focused Assurance Requirements, Gary Stoneburner, Johns Hopkins University/Applied Physics Laboratory
[45] http://www.dhs.gov/news/2009/03/11/reitinger-named-deputy-undersecretary-national-protection-programs-directorate
[46] http://www.tripwire.com/ponemon/2013/#metrics

signatures, data protection, electronic transaction security, institutional capacities, compliance and reporting obligation, technical minimum standards, certification, threat analysis, incident response, back-up and recovery, etc. as well as a carving up of indicators according to legal, technical or operational attributes. This is a challenge and narrowing down to a universal and harmonized measurement metric is extremely complicated. Not only does it require multi-sectoral and multi-disciplinary participation, but in the end, it ultimately requires agreement on the scope and expanse of the applicable definitions and metrics, requiring an incredible amount of resources and coordination.

In a recently launched initiative, ITU is leading the Global Cybersecurity Index (GCI) project to rank the cybersecurity capabilities of nation states. The project will identify performance metrics for categories against which countries will be measured and ranked. The objective is to publish six regional indices, eventually constituting one global index. The GCI project is a joint effort between the ITU and ABI Research, a market intelligence company specializing in global technology markets. Under the arrangement, ITU and ABI Research will develop the ranking mechanism, perform primary research, and benchmark national capabilities.

***Challenge #11*: Cloud computing** is a big opportunity and 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 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[47]. At the same time, cloud computing presents cybersecurity issues at different levels - technical, organizational, procedural and legal – that have to be addressed.

This is because cloud computing is a broad concept, encompassing a number of different traditional computing architectures. The technology can provide different services between the front-end (client facing) and back-end. The three generally accepted stacks are application, platform, and infrastructure. While the cost and flexibility advantages may be a positive driver for the adoption of cloud services, security remains a primary concern. The potential exposure of sensitive data or the failure to meet regulatory obligations is a strong barrier to cloud adoption generally. The critical questions remain: how reliable are cloud providers and can they offer an acceptably proven level of security? The cloud offers an inviting business model, but organizations need to first understand the services offered and assess whether these meet not just their own internal policies, but also any regulatory requirements.

The situation is complicated by different national legislation. European Union (EU) directives on data protection set high standards and requirements. [48] For EU organizations, using a cloud provider outside of the EU necessitates a minimum level of due diligence: can the provider ensure the legally required level of protection? While the provider based outside the EU is not bound by EU law, the EU organization still remains liable for any breach. While many North American security service providers boast of Health Insurance Portability and Accountability Act (HIPAA) - and Payment Card Industry Data Security Standard (PCI DSS)-compliant

[47] http://www.mckinsey.com/insights/business_technology/disruptive_technologies
[48] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

solutions, they are not necessarily compliant with EU law, even if the standards remain relatively similar.

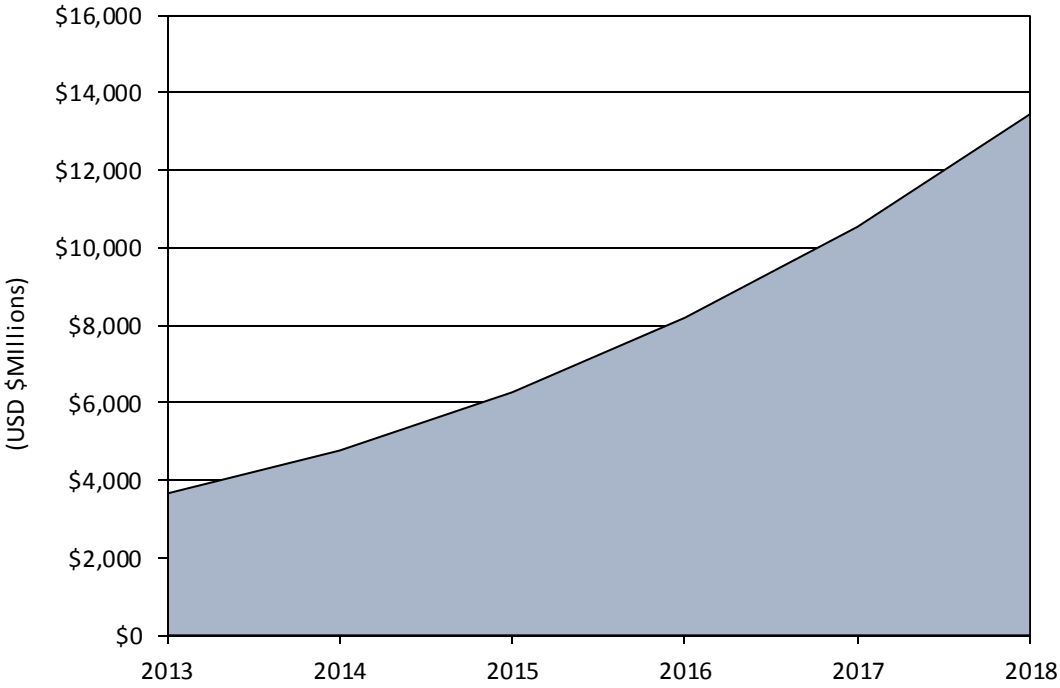
In order to bridge these differences in approach and provide means for U.S. organizations to comply with data protection directives, the U.S. Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework. The Framework was approved by the EU in 2000. Self-certifying to the U.S.-EU Safe Harbor Framework will ensure that US organizations provide "adequate" privacy protection, as defined by the Directive.[49]

In addition to understanding the complexities of data protection legislation, a number of other concerns weigh in against adopting a cloud solution: loss of control, availability, and resilience, among others. The unavailability of a service is a major issue because it can leave an organization completely vulnerable; a very risky state of affairs in the current multi-threat environment. Solutions that cannot be effectively relied upon, or that add complexity, will not fully deliver on the promises of greater security.

Finally, the fragmented and nascent market for cloud services is still relatively confusing for organizations. A host of providers offer widely different solutions: traditional IT security vendors (e.g. McAfee, Symantec, Kaspersky, Trend Micro, Bitdefender, F-Secure, Total Defense), established cloud service providers (CSPs) (e.g. Rackspace, Veracode), big technology and IT companies (e.g. Microsoft, Google, Amazon, IBM, Intel, HP, CA, Novell), telecommunication operators (e.g. Orange Business Services, AT&T), tech start-ups, and niche players in pure-play cloud services (e.g. CipherCloud, SecureCloud, CyberArk, CloudFlare).

It can be easy for an organization to sign on to a solution that either exceeds its needs or falls short of baseline requirements. Organizations need to weigh the balance between effective security, resiliency, service management, governance, cost, and business planning in order for security as a service to deliver actual business value. However, there is a clear and decisive shift towards cloud adoption, and interestingly, in terms of using the cloud for security specifically. The security-as-a-service (SecaaS) market is witnessing a growing interest from business and is fuelled by the strong belief that it will allow a large number of organizations, and especially small and medium businesses (SMBs), to adopt enterprise-class security technology solutions at affordable prices. Although initially challenging, the economic recession has helped push the adoption of cloud services when companies were in a bid to cut costs, optimize resources, and streamline business processes. With a threat landscape that is continuously evolving and a changing perception of increased security needs, the market for SecaaS is gaining trust and ground. ABI Research calculates that, in 2013, the SecaaS market will total $3.66 billion and will grow to $13.45 billion by 2018.

[49] http://export.gov/safeharbor/eu/eg_main_018476.asp




***Challenge #12*: Protecting children and teenagers** in cyber space is a growing concern. The number of digital platforms from which they can access the Internet is constantly increasing. Smartphones, tablets, and gaming consoles are some of the newer popular connected vectors alongside traditional PCs and laptops. As more online platforms surface over time and occupy a central role in children's lives (interactive online toys, smart TVs in the bedroom, connected screens in the family car, etc.), the need for more parental vigilance will become necessary as the number of potential threats grows exponentially. Understanding the dangers and the motivations behind threat actors, as well as the effects of new technologies on children can help determine suitable solutions.

Children and teenagers face two broad categories of threats online. The first is a transposable set of threats which are, unfortunately, prevalent offline – bullying, pornography, sexual exploitation. Rules and regulations have long been established around them with direct applicability online. The second category concerns threats exclusive to the digital landscape – cyber grooming, geo-location tracking, facilitation of self-harm, abuse of personal data and privacy.

Many of these threats are also subjective, and depend largely on the cultural disposition of a particular group – religious (or non-religious) content, over-usage (or even non-creative use) of the Internet, game addiction, social media, and so forth. While it is universally agreed that children need to be protected, the extent and scope of that protection, both offline and online, is highly dependent on the specific values of a social group and will affect, to a large extent, the development and success of technological solutions in any given region. The use of child online protection solutions will also depend on the parent's understanding of cyber space and the access to new vectors where their child may be exposed to online threats.

Internet use is thoroughly embedded in children's daily lives today. Playing games, watching video clips, and instant messaging are popular activities, and access to these activities is possible through a variety of different vectors, from smart devices to gaming platforms. In many developed countries, children start to use the Internet at

an ever younger age. The 2010 E.U. Kids Online study found that children aged 15-16 years said, on average, that they started using the Internet when they were 11 years old. The 9-10 year old age group reflected this trend at around 7 years of age. This variation will dictate the type of solutions effective on those age groups: younger children will require different protection mechanisms than teenagers.

Further, societal conditions particular to this time and age have a distinct effect on the successful methods for child online protection. The current generation of parents is one that grew up without computers and the Internet, or at a time when the Internet was still nascent and underdeveloped. Their children and teenagers on the other hand are constantly exposed to digital devices and the Internet, often on a daily basis from a young age. This generational difference means that older children and teenagers in particular, are much more knowledgeable about computers than their parents, and can easily circumvent or disable family protection and parental control mechanisms. This knowledge gap will reduce when the younger generation comes of child-bearing age; until that time, however, there is a technological divide making the application of viable solutions difficult.

The digital knowledge gap between the older and younger generation can be compensated by support in other areas. Policy and legislation for child online protection on the back-end can help to alleviate the burden on parents. Those organizations in charge of the supporting infrastructure, such as internet service providers, broadcasters, and mobile network operators, can provide a high-level buffer that will be much more difficult for children to circumvent. This also extends to network owners and administrators in schools, libraries, museums, and other public spaces.

There are a number of different approaches to child online protection driving the development of dedicated software. One approach reflects the need of parents, and society at large, to be more involved in the digital education of children in order to teach them how to protect themselves accordingly in cyber space. This education will help the younger generation to learn how to distinguish between content types, to elaborate habits for fast and productive Internet usage, and to avoid nefarious online elements. This approach supports the idea of monitoring activities in order to understand what children are doing online so that parents can better teach children to use the Internet safely. This idea is often linked with the desire to educate children in information technology.

Another approach is to try and protect children by blocking or restricting access to "bad" content. This approach relies on technologies which can offer automated control over devices used by children and their Internet activities.

In reality, neither approach can guarantee complete security. Most vendors agree that a single solution cannot solve the issues. Cyber space is vast, and search engines currently only index about 10% of available content.[50] The number of devices which can be used to access the Internet is steadily increasing, as are the networks enabling access. Neither approach can be overarching, nor should it be exclusive. Different solutions and services can be mixed and matched, but need to be constantly reviewed as the child ages and their actions and activities change.

[50] What Is the 'Invisible Web'?, http://netforbeginners.about.com/cs/secondaryweb1/a/secondaryweb.htm
Invisible or Deep Web: What it is, How to find it, and Its inherent ambiguity
UC Berkeley - Teaching Library Internet Workshops
http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html

Smartphones and tablets have added new challenges to the issue of child online protection. They offer all the features and possibilities of a computer and more: full browsing, instant messaging, access to hundreds of apps, social networking, and more. Consequently, the same challenges are also present: cyber bullying, sexual predation, identity theft, privacy violations, etc.

Mobile connectivity becomes problematic because children can easily move outside of the physical control area of a parent when using a smart device. Further, technical mobile solutions are relatively new and, to a large extent, are still being tested and tried. Parents concerned with regulating time spent online or playing games, or vetting downloads on a PC, face a new challenge in the mobile sphere. In addition, exposure to dangers of social media is perhaps even greater through mobile devices and privacy becomes a critical issue. Risks of geo-location or tracking by marketing companies or predators are much higher through mobile devices.

Connected gaming platforms are another area of concern. The number of children with access to TV sets and gaming consoles is steadily increasing in most developed societies. In particular, many children have their own sets in their bedrooms. Platforms for Xbox and PlayStation allow players to play online together. This can bring children in direct connection with adults. Currently popular war games (Call of Duty, Battlefield), which are notoriously competitive, are interesting examples. Despite most of such games being age-restricted (16/18+), there are a growing number of children as young as 8 or 9 playing such games and participating in the multiplayer environment. These children are often not emotionally mature to deal with such fierce (and often verbally abusive) environments. In the E.U. Kids Online survey of 2012, one of the main findings was that children were often more hurt by personally directed offensive remarks, harassment, and cyber bullying than by viewing or reading sexually explicit content.

The example is one of many, and there are many multiplayer environments on gaming consoles and on the Internet, where children will mix with adults. The next evolution will be multiplayer games on mobile devices, where virtual contact may more easily become physical contact. Further, there is an often erroneous perception by adults that content ratings equate to capacity or performance ratings; i.e., that a 16 rating means that a specific game is for more advanced children rather than as a warning for inappropriate content. Consequently, adults feel more inclined to let their children play higher age rated games on the mistaken assumption that it is simply a matter of development level.

The digital knowledge gap means that the older generation has been slow to understand and respond to this particular concern, although this is a point that is not often conceded by policy makers and industry leaders. Realistically, it will only be until the generation heavily involved in multiplayer environments currently spawns the next generation of children before the gap is narrowed and the issue is more extensively addressed.

Legislation has been highly effective in ensuring adequate mechanisms are in place for child online protection, for example, in enforcing privacy legislation to protect children from aggressive content and preventing advertisers from using their data for marketing purposes. Regulation can govern the conditions of accessibility for children as well, either by imposing technological mechanisms that limit what or who children can access and how. These include provision of filters, specification of child-friendly default settings, age verification systems, content rating and labelling, design standards, or opt-in/opt-out points. Other practices focus instead on conditions of

children's Internet use, such as building skills, raising awareness, advising parents, training teachers, and so forth.

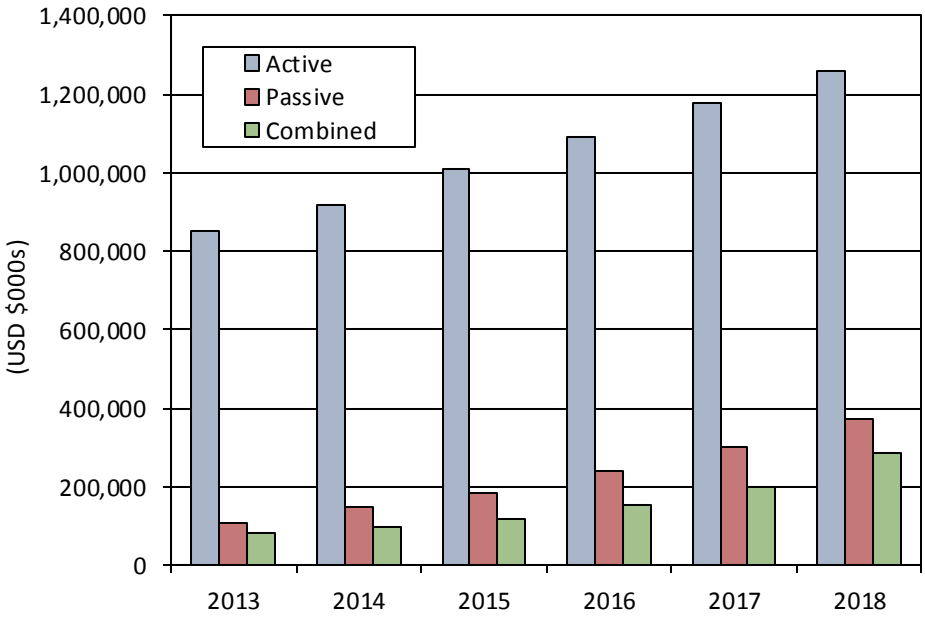
Legislation in most countries has been adapted for criminal codes on child pornography, trafficking, or sexual exploitation to incorporate offences conducted online. This has even been enshrined at the international level; the Council of Europe Convention on Cybercrime explicitly addresses the issue of offences related to child pornography through the medium of computer systems, as does the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.[51] A number of countries have elaborated dedicated legislation or set up law enforcement agencies specifically for child online protection.

International, as well as non-profit organizations have also been very active and relatively successful in raising awareness about child online protection in media generally – since the advent of radio and television, and currently in cyberspace. These efforts are sometimes instrumental in doing a lot of the legwork in research and data collection for supporting evidence that eventually leads to policy formulation and new legislation.

The Child Online Protection (COP) initiative, an international multi-stakeholder collaborative effort led by ITU, is an international collaborative network for the online protection of children worldwide, with many UN agencies, as well as private sector and civil society entities as partners. Launched in 2008 under the GCA framework for international cooperation, COP tackles the issue of protecting children online in a holistic manner by addressing all five pillars of the GCA.

Undeniably, such efforts are key drivers in not only raising awareness, but also prompting the drafting of legislation and the consideration of child protection issues at national, regional and international levels. In this light, they are a formidable driver in terms of the market for child protection solutions, whether they are focused on the defensive protection or the proactive educational angle. ABI Research calculates the parental control software market to be worth $1.044 billion in 2013, growing at a CAGR of 12.9% until 2018, reaching $1.918 globally.

[51] http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx




The market for parental control products and services fall essentially into two main categories: active and passive solutions. Active solutions are those primarily intended to filter, block, and restrict access to webpages, applications, and devices. Passive solutions are those that run in the background, namely monitoring, data collection, surveillance, and notification. The growing awareness of parents and the narrowing of the digital knowledge gap between generations will likely lead to a much stronger uptake of solutions that are passive or that are combined with active and passive elements. ABI Research calculates that in 2013, active solutions will represent over 80% of total parental control solutions. By 2018, however, this category will have shrunk to representing only 65% of total solutions available. This is why today, digital citizenship is not just about being a good citizen in the digital world, but also about how to use digital to further good citizenship. It is indeed important to promote the role of digital citizenship at the national, regional and international level, especially by teaching kids and young people how to use new technologies in a safe and responsible way, while also highlighting the opportunities and challenges they offer.

***Challenge #13*:** Despite many countries having launched their **National CERTs**, several CERTs worldwide do not yet have the capability to address the increasing complexity of cyber-related threats. 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 among countries and depend strongly on the specific context of a country[52]. Few guidelines and resources are available to help countries in establishing their national capabilities aligned with national strategies.

This is in large part because most countries do not have a comprehensive **National Cyber Security Strategy**. Unfortunately, cybersecurity is not yet at the core of many national and industrial technology strategies. Although cybersecurity efforts are numerous, they are eclectic and dispersed. Disparities exists between nation states, public and private sectors, and across industries resulting from factors such as

[52] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

differences in internet penetration, technological development, private sector dynamics, government strategies, etc.

Information sharing and cooperation are key to tackling cross-border threats. Such elements require a certain measure of organization in a multitude of disciplines: legal, technical, educational. While a particular country or a specific sector may have developed and adopted a highly effective cybersecurity framework, the knowledge is rarely shared outside of that circle.

The United States has been prominent in promoting cyber security at the national level. A Critical Infrastructure Protection Program has been in place since 1996. The Homeland Security Act of 2002 created the Department of Homeland Security (DHS).[53] Among other things, the DHS was assigned with developing a comprehensive national plan for securing Critical Infrastructures, helping to counter terrorist attacks and working in coordination with other groups, including:

- Department of Energy (DOE): Infrastructure Security and Energy Restoration[54]
- Department of Transportation (DOT): Bridge and Tunnel Security[55]
- Environmental Protection Agency (EPA): Water Security[56]
- Federal Communications Commission (FCC): Cyber Security and Network Reliability[57]

The DHS National Protection and Programs Directorate (NPPD)[58] also runs two divisions directed at securing Critical Infrastructures: the Office of Cybersecurity and Communications (CS&C) for assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure; and the Office of Infrastructure Protection (IP) for a coordinated national effort to reduce risk to the physical and cyber Critical Infrastructure posed by acts of terrorism.

The DHS also has a dedicated US-CERT team[59], which includes a National Cyber Awareness system as well as an Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).[60] The ICS-CERT, in particular, partners with law enforcement agencies and the intelligence community, and is highly active in coordinating efforts among government agencies, control systems operators, and ICS vendors.

The National Infrastructure Protection Plan (NIPP) is the DHS's overarching approach to integrating the nation's Critical Infrastructure protection initiatives in a single effort.[61] The NIPP's objectives include understanding and sharing information about terrorist threats and other dangers with Critical Infrastructure partners; building partnerships to share information and create Critical Infrastructure protection programs; implementing a long-term risk management program; and maximizing the efficient use of resources for Critical Infrastructure protection, restoration, and recovery.

[53] https://www.dhs.gov/homeland-security-act-2002
[54] http://energy.gov/oe/mission/infrastructure-security-and-energy-restoration-iser
[55] http://www.fhwa.dot.gov/research/deployment/security.cfm
[56] http://water.epa.gov/infrastructure/watersecurity/
[57] http://transition.fcc.gov/pshs/about-us/cybersecurity-communications-reliability-division.html
[58] https://www.dhs.gov/about-national-protection-and-programs-directorate
[59] http://www.us-cert.gov/
[60] http://ics-cert.us-cert.gov/
[61] https://www.dhs.gov/national-infrastructure-protection-plan

In May 2012, the Department of Defense (DOD) established the Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Program.[62] Under the program, the DOD provides defense contractors with classified and unclassified cyber threat information and cyber security best practices, while DIB participants report cyber incidents, coordinate on mitigation strategies, and participate in cyber intrusion damage assessments if DOD information is compromised.

The DHS expanded the program beyond the DIB and established the Joint Cybersecurity Services Pilot (JCSP) in January 2012. The DHS made the program permanent in July 2012 and, in January 2013, it was renamed Enhanced Cybersecurity Services (ECS) and expanded to all Critical Infrastructure sectors.[63] The Cybersecurity Executive Order issued in February 2013 builds on this and other established programs to expand the scope of Critical Infrastructure security.[64]

The Cybersecurity Executive Order is a presidential policy directive on Critical Infrastructure security and resilience. The order addresses the issue of how to improve the security and resiliency of U.S. Critical Infrastructure through voluntary, collaborative efforts involving federal agencies and private sector operators. Specifically, the order identifies four action areas:

- Expanding to other Critical Infrastructure sectors of an existing DHS program for information sharing and collaboration.
- Establishing a broadly consultative process for identifying Critical Infrastructure with especially high priority for protection.
- Requiring the National Institute of Standards and Technology (NIST)[65] to lead in developing a Cybersecurity Framework of standards and best practices for protecting Critical Infrastructure.
- Requiring regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks.

The order also builds on the involvement of the NIST in the development of cyber security technical standards applicable to Critical Infrastructure. In 2001, the NIST published the Federal Information Processing Standard (FIPS) Publication 140[66], which recommends the cryptography mechanism that government agencies should use. However, the order provides no authority for regulating Critical Infrastructure under existing law. Further, the order is directed only at government agencies and encourages the participation of operators. In essence, this means that there are no requirements for the private sector to either participate or adhere.

The European Union (EU) has also advanced considerably in developing a union-wide cyber security strategy for its Member States. However, the ideas currently prevailing in Europe are set to reach much further than their American equivalents if they find themselves adopted into regulation.

Directive 2008/114[67] is one of the first pieces of legislation on the identification and designation of European Critical Infrastructures, establishing the European Programme for Critical Infrastructure Protection (EPCIP). The primary and ultimate responsibility for protecting Critical Infrastructures according to the Directive fell on

[62] http://dibnet.dod.mil/
[63] http://www.dhs.gov/enhanced-cybersecurity-services
[64] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[65] http://www.nist.gov/
[66] http://csrc.nist.gov/groups/STM/cmvp/standards.html
[67] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

the Member States and the owners and operators of Critical Infrastructures. In 2009 the European Commission adopted an Action Plan and a Communication on Critical Information Infrastructure Protection (CIIP) geared toward a collaborative European approach to network and information security.[68]

The CIIP was reviewed by the Commission in March 2011, which concluded that national approaches to tackling the security and resilience challenges were not sufficient. Europe needed to continue its efforts to build a coherent and cooperative approach across the EU. The Commission called upon the Member States to set up Network and Information Security (NIS) capabilities and cross-border cooperation. In February 2013, the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy put out a joint communication on the EU's cyber security strategy.[69] The communication reveals a detailed strategy on the priorities and actions the EU has planned to address cyber threats in the digital era. The document gives a concise overview of current initiatives and institutions involved in cyber security, with actionable items for moving these projects forward and addressing the current gaps in the system.[70]

The communication notes all the bodies doing work in cyber security and delineates their roles and responsibilities, at the EU- and the national-level. The EU vision is presented in five strategic priorities:

- Achieving cyber resilience.
- Reducing cybercrime.
- Developing cyber defense policy and capabilities related to the Common Security and Defence Policy.
- Developing the industrial and technological resources for cyber security.
- Establishing a coherent international cyber space policy for the EU.

The strategy is accompanied by a proposal for a draft Directive (2013/0027) to establish common and minimum requirements for NIS at the national level.[71] The proposed legislation tasks private sector operators in a number of key areas to assess cyber security risks, ensure that networks and information systems are reliable and resilient, and share information with the national NIS-competent authorities. These NIS authorities would then be obliged to report to law enforcement any suspected serious incidents.

Nonetheless, the complexity of the EU itself and the difficulty in organizing pan-European efforts in cyber security has hampered progress. In the draft directive, the Commission has tasked a number of EU agencies with various missions in order to expedite the process. In particular, the ENISA has been asked to assist Member States in developing national cyber resilience capabilities, notably by building expertise on security and resilience of ICS, transport, and energy infrastructure. In addition, the ENISA is to examine the feasibility of setting up an EU Computer Security Incident Response Team for Industrial Control Systems (ICS-CSIRT).

The proposed Directive will prompt an increased demand for cyber security services in Europe, including auditing and certification. While data protection regulation has driven the market for encryption technology and associated services, the provision of such services has been highly irregular throughout the EU. The disparity in the

[68] http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip
[69] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[70] http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm
[71] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

national application of the EU data protection directive has fragmented demand for cyber security services, transforming what could have been a unified industry into a fragmented, country-specific market. The EU, however, has acknowledged this inconsistency and is seeking to redress the problem by revising the legislation. There is a strong expectation that the drafters of the proposed Directive (2013/0027) will try to avoid such issues, thereby providing a more narrowly-defined framework for the EU-wide application. This will enable a more regional market for cyber security services to develop homogenously across borders.

The cybersecurity landscape in Latin America is underdeveloped, but emergent. Latin America has a number of powerful and well-entrenched telecoms markets, with strong growth in cellular communications. In parallel, there is a growing cybercriminal element assaulting cyberspace in Latin America.[72] The financial, ICT, public security, and defense sectors are undoubtedly ahead of the game in most developed countries, and should be a priority development area for Latin America. Industrial control systems in energy and water and waste management systems are prime examples. Argentina, Peru, Columbia, Mexico, Chile, Costa Rica, Panama, Ecuador, and Bolivia have a combined total of almost 3,000 industrial control system devices connected to the Internet, which are vulnerable to hacking and publicly viewable on search engines such as Shodan.[73] Yet national policies and strategies for cybersecurity are either absent or in the very first stages of formulation.

In Africa, the scenario is not so different. The African information and communication technology (ICT) landscape is still in an early maturity phase. Most African countries are still in the early stages of realizing their full ICT potential and, therefore, cybersecurity planning and preparation has been limited. The region suffers from a lack of effective information infrastructure development, due in large part to the poor physical infrastructure, and often inadequate maintenance.

Despite a fairly nascent digital identity, the African continent has been very proactive in regional organization and collaboration in terms of tackling issues related to ICTs. Governments and various resident organizations on the vast continent understand the socio-economic benefits of a modern ICT infrastructure. Regional joint efforts have evolved into a rich backdrop of support for the discussion and attempted resolution of technical, policy, academic, and social ICT issues.

While current Internet penetration is still relatively low in Africa, connected entities are still vulnerable to cyberattacks. Nigeria, Egypt, Morocco, and South Africa have the highest number of registered Internet users, and there is growing evidence of cybercrime affecting those countries.[74] The lack of adequate regulatory and policy frameworks in place to counter cyberattacks and online criminal activity adversely affects trust in the digital environment and is not conducive to the economic growth that ICTs so acutely promise. Nigeria in particular has seen the emergence of a very specific and prosperous cybercriminal market in advance-fee fraud and related social-engineering scams (e.g., yahoo yahoo phenomenon). Kenya, Ghana, and South Africa are other countries witnessing a spurt of cybercriminal activity. The promotion of new e-government strategies in these countries is driving reconnaissance and the awareness that cybercrime is a critical problem that must be addressed if such electronic government schemes are to succeed.

[72] Cybersecurity Insight Latin America, ABI Research, https://www.abiresearch.com/whitepapers/cybersecurity-insight-latin-america/
[73] http://www.shodanhq.com/
[74] Cybersecurity Insight Africa, ABI Research, https://www.abiresearch.com/whitepapers/cybersecurity-insight-africa/

The EU, alongside with the African Union and Organization of American States are promoting the definition of National Strategies that address common aspects of fighting global threats and include phenomena that are universally recognized as negative (e.g. child pornography). There is a critical need for countries to work towards defining their own strategies, basing it on a common set of fundamental aspects.

The UN, and in particular the ITU, have been increasingly active in terms of promoting not just ICT development in the developing world through the ITU-D, but also cybersecurity development through significant efforts, such as the IMPACT initiative, which is undertaking a worldwide effort in assessing and facilitating the implementation of national CIRTs.

## 4. Recommendations

**Possible revisions and new topics, improvements of the action line facilitation mechanisms, possibly for post-2015 goals and mechanisms**

### 4.1 Continue to strengthen international cooperation mechanisms:

- **Country to country relations through discussion forums and information sharing.**

Providing a forum where nation state representatives can meet to discuss cyber treats and how to effectively combat its advance can enable information sharing and further the establishment of cooperation mechanisms between countries. Legal measures in particular, such as investigation and prosecution support, require formal agreement by national representatives. International forums allow nation states to be present in the same space at the same time. At the very least, they can kick-start discussions on the latest threat trends or best practices, and at best provide the premise for formal negotiations between countries. International forums provide an all-inclusive environment where all nations can learn and share information on an equal footing.

- **Public-private partnerships.**

Private sector organizations play a huge role in providing latest threat information and developing best in breed technologies to combat cybercrime and to enforce cybersecurity. Commercial organizations are also often heavily involved in standardization efforts through industry associations which can carry significant weight in setting the stage for promoting technology internationally. The public sector greatly benefits from engaging in discussions and supporting cooperation with the private sector. Such collaboration can help to form a more comprehensive approach to combatting cyber threats. International forums provide the ideal setting for bringing together the expertise of the private sector and the supporting framework of nation states.

### 4.2 Support the development of national capabilities by nation states, such as the assessments for national CIRTs/CERTs / CSIRTs and the elaboration of national cybersecurity strategies.

Many countries lack national capabilities for combating cybercrime and promoting cybersecurity. In large part, this is due to the absence of a national strategy and a national agency responsible for handling such matters. The elaboration of a national strategy for cybersecurity, and the designation and implementation of a responsible

body are the first steps to building a sustainable framework to combat cyber threats. Organization and procedural measures are necessary for the proper implementation of any type of national initiative. A broad strategic objective needs to be set by the nation state, with a comprehensive plan of implementation, delivery and measurement. Structures such as national agencies need to be put in place in order to put the strategy into effect and evaluate the success or failure of the plan. Without a national strategy, governance model and supervisory body, efforts in different sectors and industries become disparate and unconnected, thwarting efforts to reach national harmonization in terms of cybersecurity capability development. International organizations should support countries – especially developing and least developed countries - in their efforts to elaborate such strategies and provide them with assistance in forming appropriate technical support through the establishment of a national CIRT (Computer Incident Response Team), CERT (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team). These bodies provide the capabilities to identify, defend, respond and manage cyber threats and enhance cyberspace security in the nation state.

### 4.3 Enable better understanding of cybersecurity demands and requirements by working on indices and metrics for measuring cybersecurity development and implementation levels.

Although cybersecurity efforts are numerous, they are eclectic and dispersed. Differences in internet penetration, technological development, private sector dynamics, government strategies, means that cybersecurity is emerging from a bottom up approach; a natural occurrence where disparities exist between nation states, public and private sectors, and across industries. Measurement exercises can help to better understand the demands and requirements of these different areas. By understanding where development efforts stand, different entities can better formulate strategies and coordinate efforts to move up towards the next level of cybersecurity development. Elaboration and development of metrics and indices which can provide such measurement capabilities should be promoted. These metrics should look not only at technical specifications, but also at different social, economic and political factors which may affect cybersecurity development.

### 4.4 Underpin cooperation and support efforts for the elaboration of cybersecurity standards and other technical specifications

Technology is the first line of defense against cyberthreats and malicious online agents. Without adequate technical measures and the capabilities to detect and respond to cyberattacks, individuals, organizations, and nation states remain vulnerable to cyberthreats. The emergence and success of ICTs can only truly prosper in a climate of trust and security. The establishment of accepted minimum security criteria and accreditation schemes for software applications and systems is therefore crucial. These efforts are often driven by standards, and to a certain extent, also drive future standardization efforts. These standards are forged by a number of international organizations, consortiums and industry associations, such as the ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, ISI, ETSI, ISA, IEC, NERC, NIST, etc. The work already done by such bodies in certifications, accreditations and standards schemes should be supported and promoted.

### 4.5 Support cybersecurity development as applied to different sectors and technologies: critical infrastructure, mobile, cloud services, etc.

Cybersecurity is a broad term and does not always apply uniformly across different sectors and technologies. Specific areas have different demands and priorities, and

understanding how cybersecurity applies to different scenarios can go a long way in developing effective and workable security solutions. For example, critical infrastructures such as healthcare facilities demand special attention to data protection, privacy and confidentiality of patient information. Mobile applications for consumers also demand that confidentiality and privacy be respected with regards to location-based services being pushed out on mobile devices. On the other hand, in the utilities sector, SCADA security places much higher requirements on availability and integrity than for confidentiality. For cloud-based services, uptime, availability, and data security are all contending priorities. As more and more devices connect to the internet, and services proliferate to maximise their use, the different applications and technologies will have differing security requirements. It is important to promote cybersecurity development with a strong focus on the different requirements of each technology and sector, in order to efficiently promote the best security practices for each specific use case.

### 4.6 Understand and further cooperate for the protection of vulnerable groups: children, newly connected people, etc.

Many different people are connecting to the internet every day, each with different levels of digital literacy and understanding. At one end of the spectrum, there are highly technically capable and informed users, and at the other, there are young children and people connecting to the internet for the very first time. The Internet hosts all kinds of content, and much of it is not always age-appropriate or easy to understand even for adults. Cybercriminals are highly effective at defrauding even the most well-informed people through social engineering and other scams. It is necessary to support awareness-raising, education, and manpower development in order to enable people to more effectively navigate the dangers of the internet. Through these educational efforts risks can be reduced and all stakeholder groups should continue to drive campaigns for the protection of vulnerable groups as well as support and drive cooperation in this area. Educational development should include promotion of widespread publicity campaigns to reach as many people as possible as well as making use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centres, technology stores, community colleges and adult education programmes, schools and parent-teacher organizations to promote cyber hygiene. It is also necessary to implement curricula in schools which aim at sharing knowledge and information on current online risks and possible crimes. Finally, it is important to focus on the educational approaches needed to proactively develop young people's critical thinking skills and understanding of the digital landscape, their roles and responsibilities, and the skills and knowledge they need to use these technologies innovatively, positively and safely.

### 4.7 Provide a repository and database for multi-national efforts, information sharing, standardization work, events, best practices, guidelines, legal practices of bodies working on cybersecurity development and cybercrime prevention.

Numerous groups, initiatives, campaigns, forums, best practices, guidelines, standards, certification procedures, and other efforts already exist. The global nature of the internet makes them relevant across-borders and regardless of national boundaries. However, the various levels of development and implementation mean that information about the different efforts are not always widely shared. The primary obstacle is that cybersecurity is a sensitive issue, whether from a government or private sector perspective. Admission of vulnerabilities can be seen as a weakness. This is a barrier to the discussion and sharing of threat information and best practices. Yet security through obscurity is not a viable defense model against modern cyber

threats. The answer is to implement cybersecurity mechanisms in all layers of society. However, the drive and the incentive to do so are inadequate, either due to cost constraints or simply lack of awareness. It is important to actively promote cybersecurity development through cooperation mechanisms, information sharing, educational awareness. This could be done through the establishment of a global repository of information to promote awareness, disseminate information about legal, technical, organizational, capacity building, and cooperative measures underway in cybersecurity and for the combat of cybercrime.

## 5. 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. Of critical importance is the understanding that cyber threats cannot be eliminated absolutely, whether these are criminal or accidental. However, the conditions for limiting the damage caused by vulnerable or faulty technology exist, and can be fully supported by a comprehensive and informed application of cybersecurity. Individuals, organizations, and nation states must learn to live within a digital landscape that offers both untold opportunities and new dangers.