Policy Statement for the 2017 WSIS Forum
How to improve cybersecurity

Richard Hill
Association for Proper Internet Governance[1]

Security experts have long recognized that lack of ICT security creates a negative externality.[2] For example, if an electronic commerce service is hacked and credit card information is disclosed, the users of the service users will have to change their credit cards. This is a cost both for the user and for the credit card company. But that cost is not visible to the electronic commerce service. Consequently, the electronic commerce service does not have an incentive to invest in greater security measures.[3] Another, very concrete, example is provided by a software manufacturer's decision to stop correcting security problems in old versions of its software, with the consequence that a large number of computers were affected.[4] The cost of the attack was borne by the end-users, not by the software manufacturer.

As the Global Internet Report 2016 of the Internet Society puts the matter[5]:

> There is a market failure that governs investment in cybersecurity. First, data breaches have externalities; costs that are not accounted for by organisations. Second, even where investments are made, as a result of asymmetric information, it is difficult for organizations to convey the resulting level of cybersecurity to the rest of the ecosystem. As a result, the incentive to invest in cybersecurity is limited; organisations do not bear all the cost of failing to invest, and cannot fully benefit from having invested.

There can be little doubt that many organizations are not taking sufficient measures to protect the security of their computer systems, see for example the May 2017 attack[6] that affected a large number of users and many hospitals.

As the European Union Agency for Network and Information Security (ENISA) puts the matter[7]: "Today we are seeing a **market failure for cybersecurity and privacy**: trusted solutions are more costly for suppliers and buyers are reluctant to pay a premium for security and privacy" (emphasis in original).

---

[1] http://www.apig.ch
[2] https://www.schneier.com/blog/archives/2007/01/information_sec_1.html ; a comprehensive discussion is given in pages 103-107 of the Global Internet Report 2016 of the Internet Society, see in particular the examples on p. 101. The Report is available at: https://www.internetsociety.org/globalinternetreport/2016/
[3] See also pp. vii and 66 of GCIG.
[4] https://en.wikipedia.org/wiki/WannaCry_cyber_attack
[5] See p. 18 of the cited Global Internet Report 2016.
[6] https://en.wikipedia.org/wiki/WannaCry_cyber_attack
[7] Preamble of https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

As noted below, the externalities arising from lack of security are exacerbated by the Internet of Things (IoT)[8]. As a well known security expert puts the matter[9]: "Security engineers are working on technologies that can mitigate much of this risk, but many solutions won't be deployed without government involvement. This is not something that the market can solve. ... the interests of the companies often don't match the interests of the people. ... Governments need to play a larger role: setting standards, policing compliance, and implementing solutions across companies and networks."

Recent research shows that a perceived lack of security is reducing consumer propensity to use the Internet for certain activities.[10]

Some national authorities are taking some measures.[11] In particular, the President of the USA issued an Executive Order[12] on 11 May 2017 that states:

> [certain high officials will lead] an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet [sic] and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets).
>
> ...
>
> As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet [sic] and must work with allies and other partners toward maintaining the policy set forth in this section.

ENISA is recommending[13] the development of "So called **baseline requirements** for IoT security and privacy that cover the essentials for trust, e.g. rules for authentication / authorization, should set **mandatory reference levels for trusted IoT solutions**." And it is recommending that the European Commission encourage "**the development of mandatory staged requirements for security and privacy in the IoT, including some minimal requirements.**" (Emphases in original)

Despite those national or regional initiatives, at present, there does not appear to be adequate consideration of these issues at either the national (in many countries) or international levels.

---

[8] See p. 107 of the cited Global Internet Report 2016.

[9] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html

[10] https://www.cigionline.org/internet-survey

[11] For example, for cybersecurity for motor vehicles, see: http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_cybersecurity_best_practices_10242016 . For a general approach see Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[12] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, available at: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[13] Sections 2.1 and 2.3 of https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

We recommend to invite IETF, ISOC, ITU, UNCITRAL, and UNCTAD to study the issue of externalities arising from lack of security, which has technical, economic, and legal aspects. In particular, UNCITRAL should be mandated to develop a model law on the matter.

Further, as stated by the President of a leading software company (Microsoft)[14]:

> The time has come to call on the world's governments to come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules and get to work implementing them.
>
> In short, the time has come for governments to adopt a Digital Geneva Convention to protect civilians on the internet.
>
> …
>
> … governments around the world should pursue a broader multilateral agreement that affirms recent cybersecurity norms as global rules. Just as the world's governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, we need a Digital Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace.
>
> Such a convention should commit governments to avoiding cyber-attacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property. Similarly, it should require that governments assist private sector efforts to detect, contain, respond to and recover from these events, and should mandate that governments report vulnerabilities to vendors rather than stockpile, sell or exploit them.
>
> In addition, a Digital Geneva Convention needs to create an independent organization that spans the public and private sectors. Specifically, the world needs an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries.
>
> While there is no perfect analogy, the world needs an organization that can address cyber threats in a manner like the role played by the International Atomic Energy Agency in the field of nuclear non-proliferation. This organization should consist of technical experts from across governments, the private sector, academia and civil society with the capability to examine specific attacks and share the evidence showing that a given attack was by a specific nation-state. Only then will nation-states know that if they violate the rules, the world will learn about it.

[14] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00017arazqit2faipqq2lyngzmxx4

In a press conference on 11 May 2017[15], the official presenting the cited US Executive Order[16] stated:

> ... I think the [security] trend is going in the wrong direction in cyberspace, and it's time to stop that trend ... . We've seen increasing attacks from allies, adversaries, primarily nation states but also non-nation state actors, and sitting by and doing nothing is no longer an option.
>
> ...
>
> ... [several] nation states are motivated to use cyber capacity and cyber tools to attack our people and our governments and their data. And that's something that we can no longer abide. We need to establish the rules of the road for proper behavior on the Internet, but we also then need to deter those who don't want to abide by those rules.

Following the WannaCrypt attack[17] in mid-May 2017, Microsoft reinforced its call for action, stating[18]:

> Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.
>
> The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.

We recommend to invite the UN General Assembly to consider the appropriate ways and means to convene a treaty-making conference to develop and adopt a binding treaty on norms to protect civilians against cyber-attacks, in particular on the Internet, in times of peace, and to consider whether to

---

[15] https://www.whitehouse.gov/the-press-office/2017/05/11/press-briefing-principal-deputy-press-secretary-sarah-sanders-and

[16] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, available at: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[17] https://en.wikipedia.org/wiki/WannaCry_cyber_attack

[18] https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.00017arazqit2faipqq2lyngzmxx4

develop a new treaty, or whether to invite the ITU to integrate such norms into its own instruments, for example the International Telecommunication Regulations.

Internet of Things (IoT)

In the current environment, it can be expected that networked devices (the so-called Internet of Things – IoT)[19] will transmit data to manufacturers and service providers with little or no restrictions on the use of the data.[20] The recipients of the data could then correlate the data and resell it, as is currently the case for data collected by so-called free services such as search engines. Further, national surveillance programs could acquire such data and use it to construct profiles of individuals.

Such uses of data that are collected automatically for a specific purpose could have wide-reaching and unforeseen consequences.[21]

Further, interconnected devices may make decisions affecting daily life,[22] and this may call for the development of a regulatory framework to protect the interests of citizens. In particular, the issue of product liability may require changes to existing legal regimes.[23]

Increasingly, the safety of IoT devices will be affected by their security.[24] Thus, the security risks[25] posed by interconnected devices may require government actions.[26] For example, there may be a need to provide incentives to those who make interconnected devices to make them secure: such incentives might be penalties for failure to build-in adequate security[27]. In this context, it is worth considering past experience with various devices, including electrical devices: they all have to conform to legal standards,

---

[19] A good overview of the technology, and the issues it raises, can be found at: http://www.internetsociety.org/doc/iot-overview ; a more detailed account is at: http://www.gao.gov/assets/690/684590.pdf

[20] See https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance and the articles it references.

[21] See for example: http://www.itu.int/en/ITU-T/Workshops-and-Seminars/01072016/Documents/S1P3_Corinna_Schmitt_v3.pdf ; see also the "weaponization of everything", see p. 2 of GCIG.

[22] http://policyreview.info/articles/analysis/governance-things-challenge-regulation-law

[23] http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/

[24] http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

[25] http://about.att.com/story/iot_cybersecurity_alliance.html ; see also http://www.businesswire.com/news/home/20170313005114/en/Tripwire-Study-96-Percent-Security-Professionals-Expect

[26] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html and https://www.scribd.com/document/328854049/DDoS-Letter-to-Chairman-Wheeler#download and https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/ and http://www.dailydot.com/layer8/bruce-schneier-internet-of-things/ and https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

[27] http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/

all countries enforce compliance with such standards. It is not legitimate to claim that security and safety requirement stifle technological innovation. It must be recalled that the primary goal of private companies is to maximize profits. The purpose of regulation is to prevent profit-maximization from resulting in the production of dangerous products. As IBM Resilient Chief Technology Officer Bruce Schneier puts the matter[28], cybersecurity risks associated with the IoT require governmental intervention, as "the market is not going to fix this because neither the buyer nor the seller cares".

Since IoT products will be interconnected, at least to some degree, chaos can ensue if the products are not sufficiently secure[29] (e.g. all medical systems fail to work). Thus it is important to ensure that the products are sufficiently secure for mass deployment.

This is not a theoretical consideration. Insufficiently insecure IoT devices have already been used to perpetrate massive denial of service attacks, and such attacks could be used to bring down critical infrastructures.[30] As one security manager put the matter[31]: "In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters." A thorough study of the matter, which identifies gaps and contains recommendations for remedial actions, was published on 8 February 2017 by ENISA, see:

https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape

At present, there does not appear to be adequate consideration of this issue at the international level.

We recommend to invite ITU, UNCITRAL and UNESCO to study issues related to IoT (including security of IoT devices, use of data from IoT devices, decisions made by IoT devices, etc.), which include technical, legal, and ethical aspects (for a partial list of such aspects, see Recommendation ITU-T Y.3001: Future networks: Objectives and design goals[32]). The studies should take into account Recommendation ITU-T Y.3013: Socio-economic assessment of future networks by tussle analysis[33].

[28] https://digitalwatch.giplatform.org/updates/new-government-agencies-are-needed-deal-iot-security-regulations-says-ibm-resilient-cto and
http://searchsecurity.techtarget.com/news/450413107/Bruce-Schneier-Its-time-for-internet-of-things-regulation

[29] A particularly frightening scenario is presented at:
https://www.schneier.com/blog/archives/2016/11/self-propagatin.html

[30] See http://hothardware.com/news/latest-iot-ddos-attack-dwarfs-krebs-takedown-at-nearly-1-terabyte-per-second
http://hothardware.com/news/your-iot-device-could-be-part-of-a-ddos-botnet-how-to-shut-it-down
https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

[31] Jeff Jarmoc, head of security for global business service Salesforce, quoted in the excellent summary article at:
http://www.bbc.com/news/technology-37738823

[32] https://www.itu.int/rec/T-REC-Y.3001-201105-I

[33] http://www.itu.int/rec/T-REC-Y.3013-201408-I/en