Europe Technology Policy Committee

COMMENTS OF THE ACM EUROPE TECHNOLOGY POLICY COMMITTEE ON THE CYBER RESILIENCE ACT: A PROPOSAL FOR NEW CYBERSECURITY RULES FOR DIGITAL PRODUCTS AND ANCILLARY SERVICES

25 May 2022

The Association for Computing Machinery (ACM) is the world's largest and longest established professional society of individuals involved in all aspects of computing. It annually bestows the ACM A.M. Turing Award, often popularly referred to as the "Nobel Prize of computing." ACM's Europe Technology Policy Committee ("Europe TPC")[1] is charged with and committed to providing objective technical information to policy makers and the general public in the service of sound public policymaking. ACM and Europe TPC are non-profit, non-political, and non-lobbying organizations. Europe TPC is pleased to submit the following Comments[2] in response to the Commission's above-captioned consultation on the "Cyber Resilience Act."[3]

Europe TPC concurs with the European Commission's premise that "digital products and ancillary services create opportunities for EU economies and societies," but "also lead to new challenges." The Committee is pleased to assist in meeting those challenges through the current consultation. Detailed responses to the Commission's questionnaire have been submitted. In addition, Europe TPC makes the following principal recommendations and observations:

[1] See, https://europe.acm.org/europe-tpc.

[2] The principal author of this document for Europe TPC was Committee Chair Chris Hankin, Fellow of the Institute for Security Science and Technology and Professor of Computing Science at Imperial College, London. Also contributing were: Ricardo Ferreira, Senior Developer Advocate at Amazon Web Services; and Alejandro Saucedo, Engineering Director at Seldon Technologies and Chief Scientist at the Institute for Ethical AI & Machine Learning. *(All affiliations listed for personal identification purposes only.)*

[3] See, "Cyber resilience act – new cybersecurity rules for digital products and ancillary services" (16 March 2022) [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en]

ACM EUROPE TECHNOLOGY POLICY COMMITTEE
SELECT SUPPLEMENTAL QUESTIONNAIRE RESPONSES

SECTION 1: Cybersecurity of digital products and the users of digital products

Q1: [W]hat is the overall level of cybersecurity of digital products marketed within the European Union?

The cybersecurity level of digital products marketed within the European Union is highly sector dependent. The security level for high-risk systems, such as those employed to control critical infrastructures or in healthcare is generally good and improving. Due in large measure to the introduction of secure-by-design and secure-by-default engineering approaches the same also may be said for lower risk systems, like certain non-critical Internet of Things products, which conform to ETSI standards and consumer products. It is too early, however, to quantify the full impact of these secure-by-design and secure-by-default approaches.

Q2: In your view, during the last five years, how has the level of risk of cybersecurity incidents affecting digital products evolved?

Over the last five years, it has become significantly more likely that a given internet-connected digital product will experience a cybersecurity incident. This may be attributed in part to the rapid expansion of the Internet of Things. This “digital transition” has led to vastly more (and more kinds of) products being connected to the Internet at a vast and accelerating rate. In addition, the trend towards increased working from home, accelerated by the pandemic, also has exacerbated the risk of intrusion since employees’ home computer systems often are less well protected than employers’ workplace-based networks and devices. The Mirai botnet incident of 2016 foreshadowed the possibility of the inter-connection of poorly protected devices leading to the rapid propagation of malware, and the WannaCry incident and many other subsequent ransomware attacks puts the problem in high relief. Heightened geo-political tensions also increase the risk of state actors, or their proxies, using cyber-attacks to destabilize opponents. The troubling trend in ransomware that allows increasingly low skilled actors access to ever more destructive tools, is a deep and rising concern as organizations expand their digital footprint.[4]

Q3: How would you evaluate the actual impact of cybersecurity incidents affecting digital products on you or your organisation?

The digital transition has created an environment in which the majority of connected digital products are now integrated into hybrid, cyber-physical systems. Whereas the expected impacts of a cybersecurity incident previously might have been purely financial or reputational,

[4] See, e.g., Costa Rica declares national emergency amid ransomware attacks, *The Guardian* (12 Mat 2022). [https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks]

this hybridization increases the chances that cybersecurity incidents in the future could well cause environmental damage, or result in damage to personal health or even life. Therefore, as with traditional IT systems, products and services associated with cyber-physical systems also must be supported by and subject to Service Level Agreements, business continuity plans, and technical certification regimes. Such mechanisms should be designed to ensure that they do not have a negative impact on smaller service providers whilst still ensuring appropriate levels of system reliability and security.

SECTION 2: Improving the cybersecurity of digital products

Q11: How would you assess the relevance of the following measures for the users' ability to evaluate the cybersecurity properties of a digital product and to make better informed purchase or usage decisions?

Raising user awareness of a product's cybersecurity risks is difficult and varies depending on whether the user is in a work or less formal environment. In an organization, user awareness can be raised by requiring or encouraging appropriate training and, when useful, making product documentation available. It is much more challenging, however, to raise awareness amongst general consumers, although effective advertising campaigns might succeed in "nudging" them towards more secure products and more secure user practices.[5]

Q12: To what extent do you agree that subjecting certain products marketed in the Union to cybersecurity requirements would be effective?

Since any system is only as secure as its weakest element, it is important that any such requirements be applied across the whole product range from hardware to applications, and ultimately to all internet-connected products. In addition, general requirements should be augmented by detailed, industry-specific and/or domain-specific standards that require or encourage the use of best practices to mitigate undesired outcomes. This might, for example, be accomplished by expanding the scope of regulations like NIS2 and DORA[6] to mandate that "secure by design" principles[7] specific to machine learning systems (which are inherently different from traditional systems) be designed, developed, deployed so that they perform consistently throughout their lifecycle and meet an appropriate level of cybersecurity.

[5] Gartner predicts that 40 percent of cyber security programs will deploy socio-behavioural principles (such as nudge techniques) by 2025 to influence security culture across the organisation, up from less than 5 per cent in 2021.

[6] https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

[7] Security-by-design involves considering security as a fundamental requirement from the design stage of a system. It underpins the EU's Digital Services and Digital Marketing Acts. The UK's National Cyber Security Centre have published a set of principles at https://www.ncsc.gov.uk/collection/cyber-security-design-principles.

Q14: In the absence of horizontal cybersecurity requirements at [the] European level, Member States could adopt national laws placing certain requirements on vendors. To what extent do you agree that there is a risk of increasing costs and legal uncertainty for market stakeholders, in the absence of an EU initiative?

Absent an EU initiative in this area, it is highly likely that there will be an increase in costs and legal uncertainty for market stakeholders as they struggle to meet the requirements of different EU Member States. It is thus important to develop horizontal cybersecurity requirements at European level.

Q20: If you consider that self-declaration is not enough to demonstrate compliance with security requirements, do you think that the involvement of a third party should be required under certain circumstances?

Risk-based assessments should be conducted in all EU Member States by competent national authorities. Such assessments should be subject to mutual recognition within the EU to avoid fragmentation and legal uncertainty.

Conclusion

ACM's Europe Technology Policy Committee stands ready to leverage the expertise of its thousands of European members to assist the European Commission in its further consideration of cyber resilience in this proceeding, or otherwise with respect to technical matters implicating any aspect of computing and its societal impacts. To request such technical, apolitical input please contact ACM's Director of Global Policy & Public Affairs, Adam Eisgrau, at acmpo@acm.org or +1 202.580.6555.