Openforum europe

open, competitive choice for IT users

ROUND TABLE REPORT

CYBERSECURITY AND CERTIFICATION

Leveraging international standards to build trust in the Digital Single Market

Report

Round Table

Cybersecurity and certification - leveraging international standards to build trust in the Digital Single Market

Brussels: December 6, 2017

Hotel Berlaymont, Boulevard Charlemagne 11, 1000 Bruxelles

DISCLAIMER

This report is prepared by OpenForum Europe (OFE). The summaries of the speaker presentations and panel discussions in this report are based on the OFE's notes and they are not in any way binding or necessarily complete. All effort has been given to reflect and convey objectively the essence of the speakers' presentations and the discussion.

The views expressed in the report do not necessarily reflect those of OFE. OFE should not be held accountable for any claimed deviation from the original speeches.

Credits

Speakers

Ms. Catherine Stihler
Member of the European Parliament
S&D Group, United Kingdom

Mr. Duncan Harris
Vice President of Security Assurance
Oracle

Dr. Stefan Weisgerber
Head of Digital Technologies
DIN

Moderator

Graham Taylor
Chairman
OpenForum Europe

Rapporteur

Tony Ford
Director and Legal Consultant
OpenForum Europe

Foreword

In September 2017, the European Commission published a proposal for a Regulation on Cybersecurity (the 'Cybersecurity Act') which includes a section which defines a regulatory framework for the cybersecurity certification of ICT products and services.

Improved trust is key to delivering the Digital Single Market, but:

- to what extent does the proposed framework address real cybersecurity needs?
- can existing structures and processes be better leveraged to improve security and build trust?

1. Mr Graham Taylor ('GT')

Graham Taylor opened the event. After welcoming the participants, he went on to introduce OpenForum Europe (OFE) - of which he is the Chairman – and to remind those present of the purpose of OFE, its status as a not-for-profit think tank, its focus on 'openness', its access to a wide range of OFA Fellows, and the close participation of OFE in Digital Agenda topics (such as: copyright reform, text & data mining, e-Government, and the free flow of data).

This Round Table would focus specifically on cybersecurity and its link to the world of standards, in the light of the Commission's proposals for a new regulation in the field of cybersecurity, as published on September 13, 2017[1].

GT reminded attendees of OFE's close connection to this topic:

- OFE is one of the founding members of the MSP[2];
- OFE chairs the MSP's "Rolling Plan" task force;
- OFE has established its own task force on cybersecurity;
- OFE is this month releasing a new White Paper (with a separately available Executive Summary) on "ICT Standardisation in a Digital World – the power of Open Innovation"; and
- OFE has prepared a position paper for the MSP session to be held on December 7 (i.e., the day after the Round Table).

GT went on to introduce the three main invited speakers, and a contributor from ANEC[3]; he explained that the event would commence with informal presentations by the three main speakers and the ANEC contributor, following which the floor would be opened up to all attendees for discussion and debate. GT made it clear that the discussion and debate were to take place under the Chatham House Rule[4], and reminded the audience that in practice

[1] See: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en
[2] i.e., the *European Multi Stakeholder Platform on ICT standardisation*; see e.g.: https://ec.europa.eu/digital-single-market/en/european-multi-stakeholder-platform-ict-standardisation
[3] ANEC is the *European Association for the Coordination of Consumer Representation in Standardisation aisbl* (or the "European consumer voice in standardisation").
[4] https://www.chathamhouse.org/about/chatham-house-rule

this meant that whilst attendees were free to use information shared at the event, and the identities and the affiliations of the main speakers (and the contributor from ANEC) could be quoted, neither the identity nor the affiliation of any other participant could be revealed.

- **Ms. Catherine Stihler** – Member of the European Parliament
- **Mr. Duncan Harris** – Vice President of Security Assurance, Oracle
- **Dr. Stefan Weisgerber** – Head of Digital Technologies, DIN

GT invited the three main speakers to make their opening statements, in the order shown above.

2. MEP Catherine Stihler ('CS')

In this first statement, CS revealed herself as an optimist, a 'digital adopter', who is keenly aware of the opportunities for technology, which we all increasingly use, to provide input to the economy and the DSM[5]. She underlined the importance of ensuring that "digital should not recognise borders", whilst recognising the associated security risks, citing (for example) the growing trend for ransomware attacks, now measured at over 4,000 / day, impacting on all levels of commerce.

Separately, CS stressed the increasing need for us to be protected against other digital / technology risks, such as behavioural manipulation and the subversion of democratic processes – as well as emerging IoT[6] risks associated with previously mundane but now connected domestic appliances.

Turning to standards, CS stressed the need for any new European standard to be meaningful and to fill a need (ensuring better interoperability, at a global level), rather than merely duplicating existing ISO standards.

On the topic of voluntary measures, whilst acknowledging the attraction of the concept, CS drew attention to the magnitude of the challenge, especially taking account of the dependency here on the strength or resolve of individual Member States.

CS stressed the importance of ensuring that the voice of consumers and other citizens should be heard, and particularly in the area of privacy, where the interests and needs of citizens should be paramount.

CS concluded her remarks by indicating her view that there is an 18-month window to get this right, and to position ourselves on a good path for DSM; if we have to wait until the next Parliament, this is likely to prove much harder to accomplish.

3. Mr Duncan Harris ('DH')

Next, Mr Harris presented a view from industry: he introduced himself as a practitioner in cybersecurity, with over 20 years' experience at Oracle, where he is responsible for the Product Security Certification Group; however, DH took care to indicate that his remarks were being contributed also on behalf of smaller companies.

[5] Digital Single Market
[6] Internet of Things

DH referred to ISO/IEC 15408, the so-called 'Common Criteria' (or 'CC') standard[7]. This was in the context of the US Department of Defense ('DoD'), which has up to 1.5 million individual users, many with clear tendencies to download external 'apps' and other code onto their work 'desktops'. DH described how the DoD decided to control the exposure: it created a product security certification, by developing a profile describing how an application must behave when running on an operating system. DoD users are only allowed to install applications compliant with the certification / profile on their work desktops and mobile devices.

DH explained how a number of other nations (e.g., China, Russia, the UK) have developed their own security standards based on CC; moreover, as of today 28 countries (including 13 EU Member States, but not including either China or Russia) are signatories to the latest Common Criteria Recognition Arrangement, which in summary provides for mutuality of recognition of each other's implementation of security evaluation standards based on the CC model.

DH underlined the over-arching need for the establishment of a global security evaluation standard, so as to maximise the range of fully compliant products available to purchasers; in a world of parallel country-specific standards, purchaser choice is reduced as a consequence of the inability of all but the very largest suppliers to achieve certification under all the various national schemes.

Turning to the Commission's proposals, DH noted that 3 levels of assurance are proposed: Basic, Substantial and High. In the view of DH, that is 2 levels too many, especially as smaller specialist vendors will find it harder to compete. The level of assurance may describe the number of security functions included in the relevant product; yet at the assurance level, the rating achieved will tend to reflect trust in the product's performance rather than necessarily describing the functional content; in turn, the level of confidence will tend directly to reflect the depth of the investigation.

DH closed by noting that today in the case of CC, multiple levels of assurance are being abandoned - in favour of a single (binary: pass/fail) assessment as to whether or not the test product meets the standard.

4. Dr Stefan Weisgerber ('SW')

SW announced that he would be sharing his views on standards, certifications and security.

Standards create trust, by providing transparency; they have the potential to raise levels of safety and security; and are an important supported of innovation, by providing solid ground and understanding for multi-party co-operation – all provided, however, that the standards themselves have been developed in an open way, rather than "behind closed doors". Standards have been of great value for the European market – they act in support of regulation and open markets.

SW briefly sketched the so-called New Legislative Framework as a smart tool in support of EU regulation. Its ingredients are "essential requirements", which are a regulatory

[7] Common Criteria for Information Technology Security Evaluation

prerequisite for market access, and harmonised European Standards, which underpin the essential requirements with detailed technical provisions. Compliance with the relevant harmonised European Standards induces the presumption of conformity with those essential requirements, which removes the need for proof, individually by product.

As to certification: one can choose to opt for it when one really needs it, but self-declaration is the standard option even in situation when life safety is at risk, e.g. safety of machinery. Manufacturers take this very seriously.

European standards are driven by their stakeholders (i.e.: consumers, authorities and producers); and clearly linked to International Standards to ensure connectivity of the European industry. Increasing technical coherence flows directly from the national implementation of European Standards and the disappearance of genuine national ones.

As to the DSM: strong security is needed to support the DSM – cybersecurity is one of the critical success factors for digitisation. Yet the flaws in the Commission's recent proposals will delay the achievement of the DSM as a result of the "time to market" for new products being extended through slower processes.

The increasing level of interconnectedness in today's world means that industry has a corresponding need to know what is coming. Yet the absence of an international interface in the Commission's proposals is risky: the regime for security regulation needs to be compatible with those suppliers which work with the global value chain.

SW concluded by recommending that international standards should be used by default, with genuine European standards being developed solely to meet specific needs. Any conformity assessment needs to be built on top of existing standards, rather than side-by-side. The aim should be to achieve a greater degree of self-certification on the part of manufacturers.

Following the three main speakers' prepared remarks, a contribution was received from Ms. Chiara Giovannini (Senior Manager responsible for Policy & Innovation, ANEC):

5. Ms Chiara Giovannini ('CG')

By prior arrangement, CG made a specific contribution from the standpoint of consumers' interest in cybersecurity and standardisation; she proposes that the Commission's proposed Cybersecurity Act should offer new tools to help protect consumers.

Accompanied at the Round Table by a (battery-less, and so non-functioning) doll called "My Friend Cayla"[8], CG made the point that cybersecurity threats could manifest themselves completely unexpectedly in everyday products purchased by consumers (such as the "My Friend Cayla" doll, where children are clearly the intended users).

[8] This internet-connected product has been the subject of news reports in recent years, in particular after Germany's Federal Network Agency declared in February 2017 that it had classified Cayla as an "illegal espionage apparatus", thus exposing retailers and owners to the risk of fines if they continued to stock the product or failed permanently to disable the doll's wireless connection.

CG stated that certifications systems can only be as good as the standards and requirements on which they are based – what is needed is for consumers to be provided with reliable information.

Yet under the proposed 'Cybersecurity Act' it is not clear who is responsible – for example, in the case of the "My Friend Cayla" doll, who exactly would be responsible?

CG recognised that standards can be a formidable tool for embedding value in a product's design – at the same time, what is needed is someone "to police the market, to make consumers safe and secure"; a consumer-centric approach is required, which takes account of the fact that consumers are not perfect, hence we should aim to achieve security and safety "by design" – in a way that is not only practical, but also allows for speedy updates to be deployed.

6. Round Table discussion

Following the submissions from the four contributors named above, GT reflected that there was no dispute about the overall objective – the issue lay in how to reach it. He then opened the meeting up for discussion with members of the audience - from this point on, subject to the Chatham House Rule.

Following this, some participants pointed out that:

Certification schemes are not "magic bullets"; the example was quoted of a well-known manufacturer's "smart card" which had been fully certified under not one but two standards – but turned out to make use of a key-generation algorithm which was vulnerable to a well-documented attack.

In order to be workable, any certification scheme needs to be industry-led, realistic and economic - it cannot be driven purely by politics. And whilst the public sector will also have requirements, an compromise agreement ought to be achievable, following a dialogue (or even a "multi-logue").

As well as the need for dialogue to take place between industry and the public sector, one of the key questions to be resolved through that dialogue is agreement on what is reasonable in terms of the requirements to be imposed on industry.

A 3-step system operates in Europe today: 1) legal requirements are published, which apply across the EU; 2) industry generates standards to meet those requirements; and 3) producers self-certify against [relevant] standards. Yet the Commission's Cybersecurity Act proposal clearly diverges from that pattern, by omitting any legal requirements. Industry needs to know what requirements are to be satisfied through standards. Moreover, plenty of standards already exist, which could be adapted or transposed – or it may be necessary to establish a new standard.

Politically today in the EU, a contest is taking place to establish which institution(s) will be responsible for cybersecurity (not least, as Defence is involved); and all dialogue inevitably takes time. Resolving this during the remainder of the term of this Parliament will require consensus.

The limited time available dictates that we have to build on what's there already, focusing on users' needs. It's necessary to tease apart: 1) standards; 2) legal requirements (which can become obsolete and so require the capability of being continuously updated); and 3) certification. Moreover, it's necessary to ensure that self-certifications are open to challenge, and we need to differentiate between "declarations" (of conformity) and "self-certification".

One aspect of this question is that certification is focused on a product's security features, but most people are more concerned about flaws in the product. The real need is to build products securely from the beginning, which logically implies following a defined process in building any product. In turn, if such a process is followed, the resulting product can be built and safely shipped (released to the market) as soon as its development is complete. However, this implies the need for the same process always to control how any update is added to such a product. Further, when new vulnerabilities come to light (as they inevitably will), the actions to be taken as a result by the developer must include the updating of the development process itself, to the extent this is identified as a requirement in the analysis.

Theoretically, use of formal specifications and formal methods to demonstrate a product's security could be an answer; however, the application of such specifications and methods will most likely only be justified in scenarios such as: (i) safety-critical systems; and (ii) complex financial systems.

The fact that applications operate on general-purpose computer systems is linked to the vulnerabilities which we see identified in code; previously certified software can still turn out to have vulnerabilities (see e.g. the OpenSSL / HeartBleed vulnerability issues[9] which came to light in 2014).

One attendee reported how self-certification can work in context of a global manufacturer, so as to convince prospective and actual customers, provided that the manufacturer's internal PEN-testing practices are described to those customers, and the test results shared with them. Moreover, in today's economy, the same approach has to be adopted globally, and the regime adopted needs to accommodate components acquired via a supply chain; this is because (say) the global manufacturer creates an overall "solution" which comprises a multiplicity of products from various suppliers – and each of those products similarly could imbed multiple components, again from various other producers – and the various certifications applicable to such products and components in the overall solution may well have been granted / made in the context of completely different use cases.

Another contributor underlined how the Commission's Cybersecurity Act proposals fail to specify whether the focus should be on the security function of internal product components, on interface vulnerabilities, or on the overall environment (especially in the case of Cloud scenarios).

Essentially, before a producer can certify, the standard needs to be developed. Yet, it's also true that top-down standards imposed by governments tend not to be followed – this underlines the key role of industry in their development. In parallel, it has to be noted that the Commission's Cybersecurity Act proposals also fail to build on existing international standards, which raises further doubts in terms of links to international markets (outside the EU). Will the new Certificates envisaged under the Commission's Cybersecurity Act proposals be recognised outside the EU? And vice-versa?

[9] CVE-2014-0160

Before closing the proceedings, GT invited the main speakers and CG for their suggestions as to what key points to feed back to the Commission. The responses can be summarised as follows:

- ask the Commission:
    - not to reinvent an existing international scheme;
    - to collapse the proposed three level certification hierarchy down to a single level; and
    - for clear separation between legal requirements, standards and conformity assessments – as well as a link to international standards; and
    - underline the importance of privacy and security by design as a precondition before allowing any product on to the market – and aim to have existing products which are found not to be conformant to be taken off the market.

Finally, to close the event, GT as Moderator thanked the panellists, and concluded the discussion.

Speaker's biographies

Catherine Stihler, MEP from the UK

MEP Stihler has been a Member of the European Parliament since 1999. Catherine has performed in the role of Deputy Leader of the European Parliamentary Labour Party (EPLP) from 2004 to 2006 and EPLP health spokesperson in the previous Parliament. Nowadays, Catherine is vice chair of the Internal Market and Consumer Protection Committee (2014-) and is a substitute on the Economic and Monetary Affairs Committee (2009-). Having been an active Labour Party member from the age of 18, Catherine is also a member of Community the Union,e the Co-operative Party, the Fabians, SERA, Labour Movement for Europe and the Christian Socialist Movement.

Mr Duncan Harris, Vice President of Security Assurance at Oracle

Duncan Harris is vice president of security assurance at Oracle, responsible for all product and cloud service security vulnerability handling and disclosure, for Oracle's internal ethical hacking team, and for formal product security certifications including Common Criteria and FIPS 140, and helps define, educate, evangelise and ensure compliance to internal secure development policies and standards. He provides broad security advice to Oracle's product development, information security, legal, HR, marketing, PR, internal audit, and corporate affairs teams, and contributes to external security standards setting groups and committees, based on weaknesses and vulnerabilities his team and external researchers identify and expose. Duncan notably constructed the technical proof behind Oracle's marketing campaign which was partly based on the strength of Oracle's commitment to Common Criteria. Over his 23 years at Oracle, Duncan has also been the product manager for Trusted Oracle7, Oracle's B1 multilevel secure database, now replaced by Oracle Label Security, and involved directly or indirectly with all the product security certifications and validations Oracle has ever done. Prior to Oracle, he worked as a UK product security certification laboratory evaluator and on various UK classified defence and intelligence systems.

Dr Stefan Weisgerber, Head of Digital Technologies at DIN

Dr. Weisgerber is serving as Head of Digital Technologies at DIN. In this capacity, he is responsible for DIN's activities related to Digital Transformation. He is convenor of the CEN-CENELEC BT Working Group on ICT Standardisation Policy and alternate representative of CEN to the European Commission's Multi-Stakeholder Platform for ICT Standardisation (MSP).

OpenForum Europe (OFE) is a think tank that draws support not only from some of the largest global ICT players, but also from organisations across Europe, that represent both SMEs and Open Source communities. The focus of OFE is to encourage openness in the ICT market, eliminate lock-in, and maximise the opportunity for all market players in Europe.

Views expressed by OFE do not necessarily reflect those held by all its supporters.

OFE Limited, a private company with liability limited by guarantee Registered in England and Wales with number 05493935 Registered office: 1 Blunt Road, South Croydon, Surrey CR2 7PA, UK