Cybersecurity assurance practices

Study period

2022-2025

Question 3/2

Securing information and communication networks: Best practices for developing a culture of cybersecurity

Interim deliverable 2023

Executive summary

The World Telecommunication Development Conference, held in Kigali in 2022, reviewed the mandate of Study Question 3/2, which focuses on sharing experiences on cybersecurity practices. Cybersecurity threats are a significant concern globally, with the increasing reliance on technology leading to the escalation of cyberattack risks and consequences. Cybersecurity assurance practices have emerged as a critical element in protecting networks, systems and data from malicious activities.

This report reflects the contributions and discussions from the Question 3/2 meetings and a dedicated workshop on cybersecurity assurance practices. Six key takeaways from these discussions are presented below:

1. Different levels of criticality and risk require different levels of assurance. Risk assessments can help to determine what level of assurance is appropriate taking into consideration the sensitivity of the data and assets being protected, the consequences of a breach as well as the threat environment.
2. Engaging with partner organizations, industry, and multiple stakeholders can be an effective way to drive cybersecurity assurance. Cooperation among policy-makers, civil society organizations and industry can boost demand for security and inform policy and regulatory development.
3. Consider an evolving regulatory approach, informed through dialogue and consultations. Cybersecurity assurance practices may be introduced on a voluntary basis before becoming mandatory, depending on the need for stronger measures to protect against cyberattacks.
4. Given the dynamic threat landscape and evolving cybersecurity risks, cybersecurity assurance practices should be reviewed and adapted over time. Regular internal audits and threat intelligence subscriptions are considered good practices.
5. Efforts are being made to educate consumers and manufacturers about the importance of cybersecurity and the benefits of choosing more secure products. Cybersecurity labelling schemes and awareness campaigns can help to inform users about the security of technology products.
6. Reciprocity agreements can help to ease compliance for industrial actors operating across multiple markets, while harmonization of baseline security requirements reduces the regulatory burden on providers of products and services.

Introduction

During the last World Telecommunication Development Conference, held in Kigali, Rwanda, in June 2022, the mandate of Study Question 3/2 "Securing information and communication networks: Best practices for developing a culture of cybersecurity" was reviewed and one of the specific issues identified for study was to "share experiences on cybersecurity assurance practices" [1]

The approved Terms of Reference for Study Question 3/2 recognize that cybersecurity threats continue to be a major concern for governments, organizations and individuals worldwide. With the increasing reliance on technology, the potential risks and consequences of cyberattacks are also escalating, and cyberattacks are becoming increasingly profitable[2]. Cybercriminals are operating a lucrative business, which is estimated to cost USD 8 trillion worldwide[3].

Cybersecurity assurance practices[4] have emerged as a critical element in protecting networks, systems and data from malicious activities. These broadly refer to the procedures used to ensure that relevant controls are in place to protect the confidentiality, integrity and availability of electronic devices, systems, networks and data. Although they do not directly prevent cyberattacks, their goal, if correctly implemented, is to minimize the risk of such attacks. Cybersecurity assurance practices can be checked against specific security controls, guidelines and standards and can either be imposed by regulations or voluntarily adopted by the industry. However, there is no one-size-fits-all approach, with national authorities and sector regulators often using different practices, ranging from self-assessments and voluntary guidelines to labelling schemes and rigid compliance checks.

While there is no one single approach to be recommended, it is evident that there has been a sustainable shift towards the adoption of cybersecurity assurance practices worldwide in recent years and months, with different developments in several countries and regions. As an example of this momentum, in December 2022 the Organisation for Economic Co-operation and Development launched the Recommendation of the Council on the Digital Security of Products and Services, which recommends the adoption of policies to enhance digital security of products and services that are proportionate to the risk, starting with a light-touch approach based on voluntary policy measures, and exploring the need for mandatory measures[5].

This report reflects the contributions and discussions from the Study Question 3/2 meetings and the dedicated workshop on cybersecurity assurance practices. The public, full-day workshop, held in Geneva on 23 May 2023, was an opportunity to explore the global landscape of cybersecurity assurance in various domains (the Internet of Things (IoT), telecommunications, etc.) by showcasing an array of ongoing practices and voices from across the globe. It gathered Member States and representatives from industry and technical authorities as well as civil society.

The management team of Study Question 3/2 would like to take this opportunity to thank all the speakers and contributors for their valuable inputs on this topic. This endeavour would not be possible without their commitment.

In the light of the valuable inputs received, this report predominantly conveys the challenges faced, impact assessed and lessons learned to date in considering and implementing cybersecurity assurance practices through the presentation of six takeaways.

These takeaways can serve as important input for the ITU membership to assess existing practices and evaluate the need to adopt additional or different approaches, taking into consideration the experiences and lessons learned by other administrations and organizations.

Takeaway 1: Different levels of criticality and risks require different levels of assurance

When considering the implementation of cybersecurity assurance practices, it is crucial to determine first what an entity is trying to protect and the risks faced by the identified assets. Countries and companies wanting to protect against cyberattacks should, as a priority, identify what systems and assets need protection and assess their vulnerabilities. In this regard, a blueprint for conducting risk assessments is a helpful tool. One of the most well-known frameworks is the National Institute for Standards and Technology (NIST) Cybersecurity Framework[6], which is currently being updated[7] and offers a widely used approach to help determine and minimize organizational risks. It establishes non-regulatory guidelines allowing organizations globally to identify their own risk landscape and apply appropriate cybersecurity controls in relation to this. The revised framework, due to be finalized by early 2024, builds upon a wide and long-term engagement with the community of stakeholders that use these guidelines, as well as continued alignment with other international standards.

At the workshop, the NIST representative highlighted the fact that the organization's beneficial position as a non-regulatory agency has allowed deeper engagement with industry stakeholders from around the world to understand real challenges and receive feedback, which have been incorporated in the new guidelines[8]. These are meant to be adaptable and flexible, and applicable to all organizations and sectors. BitSight, a private sector member in the ITU-D Sector, spoke about its platform, which incorporates the NIST Cybersecurity Framework and has been used by various government agencies responsible for cybersecurity (such as

---

1 https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/ToR/Q3-2.aspx#Question

2 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090023PDFE

3 https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023

4 Operational security is intricately linked to cybersecurity assurance practices, in that operational security can provide a good foundation for assurance practices. Broadcom, vice-chair of ITU-T SG 17, presented the model for good conditions highlighting that it is comprised of four key elements: people and processes, knowledge, security products (exogen security) and security in assets (endogen security). See 'Reduce Risk and Protect Reputation', https://www.itu.int/md/T22-SG17-C-0214/en

5 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

6 https://www.nist.gov/cyberframework

7 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

8 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090017PDFE

computer emergency response teams (CERTs), national cybersecurity agencies, telecommunication regulators)[9]. Through the platform, countries can conduct risk assessments of their infrastructure and assets that are considered critical and measure their risk factors.

Risk assessments can also help to determine what level of assurance is appropriate taking into consideration the sensitivity of the data and assets being protected, the consequences of a breach as well as the threat environment (i.e. whether an entity is susceptible to a cyberattack). In some cases, the levels of assurance will be dictated by regulatory requirements. The higher the level of assurance, the stricter the security controls. For example, a low level of assurance could require a system password or a firewall, whereas a higher level of assurance would require the addition of more advanced controls such as advanced encryption and multifactor authentication.

Although cybersecurity assurance practices add to information technology budgets, the failure to put in place security controls can be more costly. During the workshop, representatives urged the audience to think about the costs of suffering a cyberattack not only in financial terms: the additional reputational cost can be far more damaging. Losing the trust of customers and citizens has a long-term effect that goes beyond money, and organizations must be able to strategically understand that. Equally, for the public sector, successful attacks may impact the provision of public services and critical activities, the disruption of which also cannot be assessed only in financial terms, since it affects the lives of citizens.

Takeaway 2: Engaging with partner organizations, industry, and multiple stakeholders can be an effective way to drive cybersecurity assurance

Firstly, it is important to benchmark initiatives against others to understand best practices and learn from others' success and mistakes during the development of initiatives. Secondly, it is important to engage with multiple stakeholders, including industry, to gain important insights for the initiative itself as part of the development.

Although cybersecurity assurance practices are becoming increasingly necessary in less developed countries, they may still be hard to apply. The representative from Cyber Defense Africa (CDA) in Togo explained the challenges experienced in the local market in providing cybersecurity assurance across essential service operators (ESOs)[10]. A lack of funding, a lack of trust in the government as a service provider and a lack of local human capacity and facilities were cited as some of the factors faced. To support ESOs in complying with newly published cybersecurity controls, the Government of Togo created a public–private partnership with a large reputable cybersecurity provider to provide cybersecurity services in the public and private sectors. Through this model, Togo created CDA as a self-sufficient and high-quality local cybersecurity provider to support ESOs on a non-mandatory basis. The self-sufficient model employed allowed Togo to address the many challenges mentioned above and to begin to foster local talent in cybersecurity, as well as encourage the development of the local market. The representative noted the importance of CDA as a private entity in a competitive market in order to ensure adaptability, high quality of services and competitive pricing.

It is also important to foster cooperation between policy-makers who may set the regulatory environmen, and civil society organizations that can boost the demand for security and also inform policy and regulatory development on the basis of existing identified regional and international practices. For instance, the DiploFoundation is an international organization delivering training programmes and capacity building to governments, regulators, businesses and civil society on topical questions related to cybersecurity, and is involved in the Geneva Dialogue on Responsible Behaviour in Cyberspace (Geneva Dialogue)[11]. In 2020, the Geneva Dialogue produced a collection of good practices[12], which include suggested definitions of secure design and vulnerability management, threat modelling, third-party and supply chain security, secure development, vulnerability management and disclosure, as well as organizational culture. The Global Forum on Cyber Expertise (GFCE) is an international platform supporting coordination of projects, promoting the sharing of knowledge and expertise, matching requests to offers of capacity-building support and developing research projects[13]. The GFCE set up four regional hubs – the Pacific Islands, Africa, the Americas and the Caribbean, and South-East Asia. Given its global footprint and its varied support in developing countries, the Forum is well placed to bring more diverse regional views on the needs and demands of cyber capacity building. The GFCE has an online portal, which serves as a repository of implemented and ongoing projects in cyber capacity building, globally, as well as resources and tools. Such a portal also helps to reduce duplication of effort and to identify some programmes or gaps and patterns in capacity-building provision.

Takeaway 3: Consider an evolving regulatory approach, informed through dialogue and consultations

In many cases, cybersecurity assurance practices will be introduced on a voluntary basis before becoming mandatory. The shift usually happens when governments consider that industry is not doing enough to secure products and that consumers do not necessarily have the knowledge to assess if the products are safe or not. This can lead governments and national authorities to act and stipulate assurance practices that they expect industry to meet. For example, in Brazil, the telecommunication regulator, Anatel, has created a system of certification bodies and testing labs within the country for the certification of customer premise equipment (CPEs, or home gateways). Anatel's approach has traditionally been to provide voluntary cybersecurity guidelines for

[9] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090024PDFE
[10] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090025PDFE
[11] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090020PDFE
[12] https://genevadialogue.ch/goodpractices/
[13] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090021PDFE

the telecommunication sector. However, by carrying out risk assessments it found that recommendations were not enough for CPEs given the vulnerabilities and threats associated with this type of equipment and that it was necessary to establish mandatory minimum safety requirements for such products. Such mandatory requirements for communication service providers (CSPs) were published in early 2023 and focus on vulnerabilities, such as unsecure passwords and unnecessarily enabled service parts. The requirements will become effective in early 2024 as part of mandatory laboratory tests for product approval[14]. Anatel explained that the evolution from a non-mandatory approach to a cybersecurity compulsory certification requirement for a specific set of equipment was only possible following a comprehensive debate with the sector.

Similarly, the National Cybersecurity Agency (NCA) of the Kingdom of Saudi Arabia presented its initiative to build an independent verification and validation (IV&V) ecosystem[15] to test and certify products from a cybersecurity assurance perspective at the national level in Saudi Arabia. The initiative also aims to identify and classify hardware and software that are highly sensitive to cyberrisks and threats. Furthermore, it seeks to contribute to the development of human capabilities in IV&V. The roadmap for the initiative considers beginning with a voluntary programme before making it a mandatory obligation. The authority also mentioned the importance of such an ecosystem eventually becoming "self-sustainable", and this informed the NCA's approach of encouraging market stakeholders to conduct such assessments.

In the IoT security domain, the United Kingdom also provides a case study of evolving from a voluntary to mandatory approach. In recent years, the United Kingdom has decided to mandate, through legislation, a baseline security requirement for IoT consumer products based on the European Telecommunications Standards Institute (ETSI) EN 303 645 standard, the first globally applicable cybersecurity standard for consumer IoT devices. In the United Kingdom, manufacturers, importers and distributors will have to comply with 3 of the 13 ETSI security guidelines, and the law gives powers to the government to adopt additional requirements if necessary, depending on regular threat assessments. The decision to mandate baseline security requirements followed a period of voluntary adoption. In 2018, the country formulated a voluntary code of practice[16] for consumer IoT security, but industry compliance was not as expected. Evidence gathered through consultation exercises showed that consumers value security and are willing to pay a price premium for secure products. However, security threats are not subject to the same level of robust regulation as product safety, leading to a lack of transparency from manufacturers and slower adoption of security policies. The evidence also found that the consumer connectable product market disincentivizes the adoption of basic security features, since consumers overwhelmingly assume that products are already secure. The regime aims to address this gap by mandating elements of the code of practice to ensure that manufacturers are aware of vulnerabilities and take steps to mitigate them. The PSTI (Product Security and Telecommunications Infrastructure) regime will come into effect in April 2024 and will apply to any consumer product that can connect to the Internet[17].

One of the challenges identified is the possible impact on small and micro enterprises that may encounter difficulties in complying with the new regime. The United Kingdom enforcement authority is developing guidance to mitigate any disproportionate impact. In addition to working with the industry, the United Kingdom shared that the top three requirements to be mandated in the scheme have been identified and communicated transparently for several years. Over the years, the United Kingdom has conducted exercises on the process of implementing the regime, including password requirements, fundamental product architecture, vulnerability exposure and security transparency requirements. The impact assessment has shown that the overall benefits of reducing the volume of cyberattacks on consumers and businesses are expected to exceed the costs associated with the regime. As the PSTI Act 2022 is the first mandatory cybersecurity product legislation in the world, the cost of enforcing the regime is uncertain, but initial estimates suggest that the allocated funding will be sufficient.

In some cases, the distinction as to whether an assurance practice has been mandated or kept voluntary is dictated by who the user or client is. For example, the Republic of Korea launched its Cloud Security Assurance Program (CSAP), a security certification for cloud computing services[18]. In general, the CSAP certification is voluntary. However, customers in the public sector (i.e. public agencies) are required to use a cloud service that has obtained CSAP certification pursuant to the relevant regulations, and cloud service providers therefore need to obtain certification when providing cloud services to public agencies.

Takeaway 4: Given the dynamic threat landscape and evolving cybersecurity risks, cybersecurity assurance practices cannot be static and should be reviewed and adapted over time

Regular internal audits that can help to identify gaps in controls and risk of exposure as well as threat intelligence subscriptions are considered good practices. Even if a product is certified, it could suffer from security flaws over its lifecycle. A certification scheme requires the submission of information at a specific time, and the process does not account for the dynamic changes in threats in the future. A recent BitSight study showed a strong correlation between poor "patching cadence" for vulnerabilities and the likelihood of experiencing a cybersecurity incident[19], pointing to the critical importance of updating systems as soon as security patches are available, bearing in mind the reported different distribution of patches across the globe.

14 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090018PDFE
15 https://nca.gov.sa/en/news?item=535
16 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
17 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090014PDFE
18 https://isms.kisa.or.kr/main/csap/intro/index.jsp
19 https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity

Penetration testing, or "pen testing", is a security assurance exercise that helps to evaluate the security of an IT system and identify vulnerabilities that could otherwise be used to exploit systems. Ofcom, the United Kingdom communications regulator, runs the TBEST scheme voluntarily with telecommunication providers. This pen testing scheme aims to stimulate a cyberattack in order to identify security vulnerabilities that can then be addressed through a process of remediation to improve the operators' network security posture[20]. The regulator gave an overview of the process and the different stakeholders involved. More broadly, this scheme is an example of a supervisory regime approach being taken by Ofcom, which stresses the importance of building collaborative relationships with the industry that the authority regulates. To date, all United Kingdom communication providers have run the TBEST scheme voluntarily, or are doing so, and have made changes as a result. TBEST is neither a "standard" nor a certification process. The goal is to enable communication providers to gain awareness of cyberthreats and implement appropriate changes in a timely manner to improve their cyberdefence capabilities. By being aware of and addressing such vulnerabilities and weaknesses, the operator is in a much stronger position to protect its networks.

Takeaway 5: Efforts are being made to educate consumers and manufacturers about the importance of cybersecurity and the benefits of choosing more secure products

Efforts have been made to educate the public about the importance of cybersecurity and the benefits of choosing more secure products.

One approach to this end is the development of a cybersecurity labelling scheme (CLS), under which, as exemplified by Singapore, certified products can be accompanied by a label. Labelling schemes serve primarily as an information tool for consumers. The Cybersecurity Agency of Singapore (CSA) discussed a cybersecurity labelling scheme, which aims to help consumers distinguish between more and less secure IoT devices[21]. The scheme is voluntary (with the exception of Wi-Fi routers, for which it is mandatory) and has four levels, with level 1 being the security baseline. Levels 1 and 2 are based on self-assessment by manufacturers and levels 3 and 4 involve third-party assessment by an approved laboratory. The scheme is multilevel to incentivize manufacturers to incorporate additional security measures beyond the basic requirements. The CSA also discussed the trade-offs involved in mandating cybersecurity standards, including the risk of manufacturers bypassing the market due to increased compliance costs. Instead, the goal is to change the mindset of manufacturers to view cybersecurity as an enabler and market differentiator rather than as a cost. Regarding the impact of a cybersecurity labelling scheme in Singapore, the process is still in the early stages and efforts are ongoing to encourage manufacturers to participate in the scheme and improve their cybersecurity. A public survey will be conducted again in the future to assess consumer awareness and behaviour. The cost of compliance is minimized for manufacturers at levels 1 and 2, and there has been no significant increase in the cost of products for consumers. With the voluntary scheme in place, market forces are expected to drive improvements in cybersecurity among manufacturers.

Beyond labels, it is equally important to invest in technical controls and to build awareness and educate the population about the cybersecurity risks that organizations and countries are facing. Currently, ransomware attacks constitute the most concerning trend. For these types of attacks, the main vector of attack – meaning the way a criminal enters a network or system–is through phishing emails[22]. In this context, cybercriminals can often bypass security controls simply when people click on a phishing email. It is therefore crucial to cybersecurity assurance that citizens and employees are made aware of such issues.

Takeaway 6: It is important to seek international synergy/harmonization and reciprocity agreements

The existence of reciprocity agreements between cybersecurity assurance models, namely certification and labelling schemes, can be a determinant for the scaling of these practices. As stakeholders highlighted, reciprocity agreements can help to ease compliance for industrial actors operating across multiple markets. However, considering that reciprocity agreements are a formal mechanism, have many national restraints and take time to be approved and signed, cybersecurity assurance practices need to find synergies with existing international approaches that are in alignment with national needs and priorities. This will reduce the regulatory burden on products and service providers with the aim of avoiding contradictory requirements.

The CSA stressed the importance of international collaboration in the development and implementation of its cybersecurity labelling scheme. Singapore has signed mutual recognition arrangements with Finland and Germany, and is working to expand its partnerships in this area. Singapore reflected on its experience by sharing that governments need to be proactive in establishing recognition, though manufacturers also have an interest in supporting the process of recognition as it reduces the burden of repeated testing and certification, as well as market access, in different jurisdictions. The process involves bringing interested parties together to harmonize requirements and establish common standards that are realistic and not overly burdensome.

At the European level, the European Union Agency for Cybersecurity (ENISA) has a mandate to develop three certification schemes, which would be recognized across the internal market and therefore have automatic 'mutual recognition' across the European Union (EU). These are: the *EU common criteria scheme for ICT products*, for which the legislative act is being prepared with a view to adoption; *the cloud services scheme*, which is under

[20] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work

[21] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E00000090016PDFE

[22] A common tactic used by cyber-criminals to trick people to reveal sensitive information or download malware which infects the targeted system/network.

extensive discussion; and finally, *the 5G scheme*, which is under development[23].

In addition to reciprocity, and considering the international markets in which the industry operates, the harmonization of baseline security requirements is also an important consideration. The ETSI standards on IoT consumer products provide an example of such an endeavour. The main question is to what extent different regulatory frameworks will be in alignment, and to what extent they will be connected through the same international standards. In this regard, strengthening and even finding the right place for dialogue was noted at the workshop to be a challenge. In the area of harmonization, ENISA's activities in cybersecurity standardization and 5G require collaboration among CEN, CENELEC, ETSI, ISO, IEC GSMA, 3GPP and GlobalPlatform. One of the Agency's main outputs has been the consolidation of 5G security controls from different standards development organizations (SDOs) in a single repository[24].

[23] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E00000090019PDFE
[24] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

Annex: Examples of cybersecurity assurance practices

Country or Organization	Name of the Practices	Type of the practice	Scope of the practice	Type of Approach	Reference
Australia	IoT secure-by-design guidance for manufacturer	Guidance	IoT	Voluntary	Link
Australia	Code of Practice: Securing the Internet of Things for consumers	Code of Practice	IoT	Voluntary	Link
Brazil	Act 77/2021 Cybersecurity requirements for telecommunication equipment	Requirements for the certification scheme	Telecommunication equipment	Voluntary	Link
Brazil	Act 2436/2023 - Minimum cybersecurity requirements for conformity assessment of customer premises equipment (CPE)	Requirements for the certification scheme	CPEs	Mandatory	Link
Kingdom of Saudi Arabia	Independent verification and validation (IV&V)	Testing and certification of products. Identification and classification of devices and software	Products	Initially voluntary	Link
Korea (Republic of)	Cloud Security Assurance Program (CSAP)	Certification scheme	Cloud	Combined – voluntary in general. Mandatory for the provision of cloud services to public agencies.	Link
Singapore	Cybersecurity labelling scheme	Certification and labelling scheme	IoT	Combine – voluntary in general. Mandatory only for Wi-Fi home routers.	Link
United Kingdom of Great Britain and Northern Ireland	Product security and telecommunication infrastructure (Product Security) regime	Minimum security requirements	Connectable products	Mandatory	Link
United Kingdom of Great Britain and Northern Ireland	TBEST scheme	Penetration testing	Telecommunication networks	Voluntary	Link

ITUPublications
Published in Switzerland, Geneva, 2023

International Telecommunication Union
Place des Nations, CH-1211 Geneva Switzerland