World Economic Forum
Global Future Council
on Cybersecurity

WORLD ECONOMIC FORUM

International Cybersecurity Certification Framework: Pathways to Collaboration and Situational Analysis

BRIEFING PAPER

SEPTEMBER 2021

Images: Getty Images

Contents

Executive summary

Cybersecurity allows the economy to function. It protects critical infrastructure, such as oil pipelines, water treatment facilities and hospitals, and supports the day-to-day operation of services, from online banking, to public transport, to food delivery.

Cybersecurity also poses a challenge: decision-makers must balance the competitive advantage of digitizing their organization's operating environment against the greater exposure it brings to malicious cyberthreats, alongside non-malicious – but often damaging – human error and systems errors.

Communities must see products and services as cybersecure and the experts that protect them as competent if they are to trust and adopt them. Yet headline-making attacks on essential services are commonplace and undermine trust in services and in the ability of societies to cope with technological change. Governments, organizations and the people that depend on them need to be able to trust that they are protected by recognized cybersecurity best practices that defend against cyberthreats.

There is a pressing need to:

– **Incentivize the security of consumer internet of things (IoT) devices:** Governments and international standard setters can provide clarity on how to make a new product secure and create economic incentives, such as clear cybersecurity labelling. This can have an impact internationally as more secure IoT devices are traded globally.

– **Bring clarity to the cybersecurity services market:** It is notoriously difficult to judge the relevance of a cybersecurity product until an organization has tested it in its own environment. Public sector agencies and industry should promote initiatives that increase the transparency of assurance over cybersecurity services. This might take the form of an internationally recognized scheme to certify cybersecurity service providers that can apply to be recognized across borders.

– **Provide cross-border recognition of cybersecurity qualifications:** When cyberattacks occur, cybersecurity professionals need to be able to collaborate across borders to respond to them. Mutually recognized professional certification facilitates cross-border collaboration by experts. It also creates opportunities, providing a level playing field on which countries can train and develop new generations of cyber professionals.

1 A global call for action

The World Economic Forum's Global Future Council on Cybersecurity believes that strategic gains can be made to the security of data, devices and organizations through cross-border cooperation that begins with urgent work on gaps in cybersecurity certification.

This report investigates the current gaps arising from the lack of unified, holistic, adapted international certification schemes and points to the opportunities provided by collaboration on an international certification model.

This includes collaboration on certification for digital products, the expansion and creation of internationally recognized assurance for cybersecurity service providers, and the creation of a level playing field in the certification of cybersecurity experts.

Impact

International certification frameworks have a long-term impact on validating the security context of devices, applications and systems.

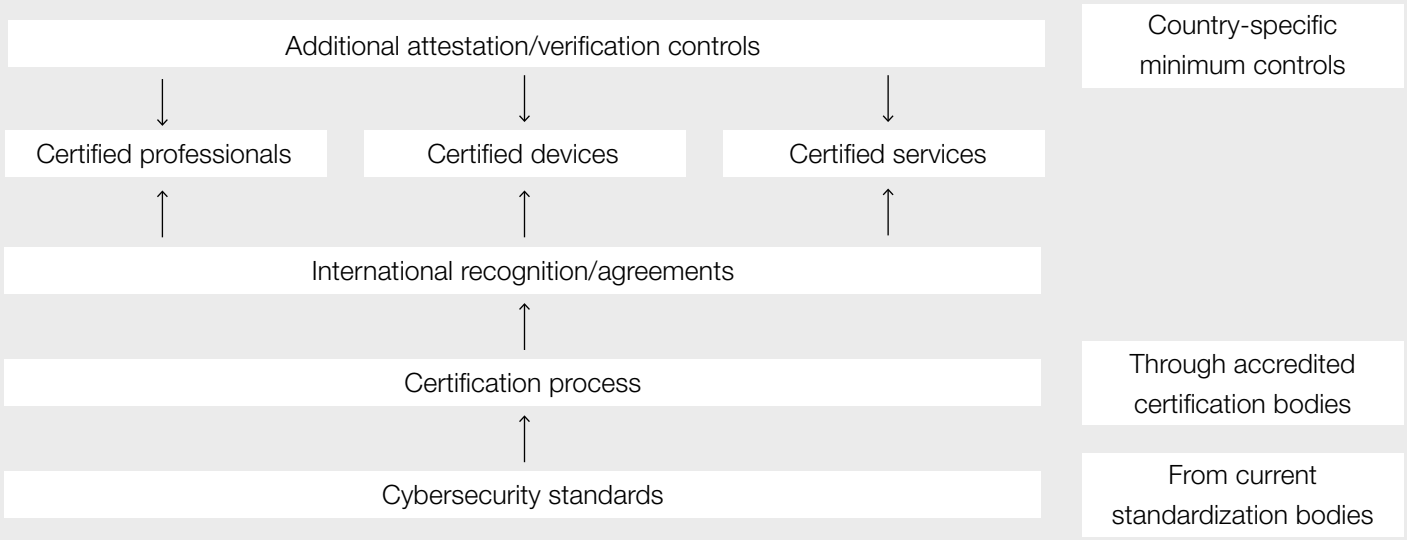
Certification also supports the creation of trusted pools of *cybersecurity service providers* and *professionals* globally. Certification schemes that are recognized across borders can help provide customers with confidence and trust in the quality of services and expertise they are purchasing, regardless of the country of origin of those services.

How to make progress

Cybersecurity requires sustained international collaboration. Defending people, societies and economies from common cyberthreats is a challenge. Cross-border multistakeholder cooperation helps countries and industry benefit from and then build on each other's successes.

Cross-border collaboration and mutual-recognition incentivizes best practices by increasing the value of certification, as widely recognized certification can be applied to a larger number of markets. This need for cohesive action that links existing certification silos is a tactical necessity that will help build the trust, reliability and mutual recognition of best-practices that is the basis for strategic collaboration.

FIGURE 1 | **A model for cross-border collaboration on cybersecurity certification**



Source: Dubai Electronic Security Center

The challenges

Certification regimes are fragmented. Certifications and registers, whether for devices, services or individual experts, are not generally recognized across borders and tend to cover specific cybersecurity sub-sectors rather than supporting holistic approaches to cybersecurity spanning people, products and services.

The uncoordinated multiplication of certification schemes does not provide clarity for cybersecurity service end-users, particularly as devices and services are traded and sold across borders.

The costs created by the need to obtain multiple certifications for the same product, or to have services and skills accredited with several organizations in multiple countries, is a barrier to the growth of new innovators and puts an artificial limit on the markets in which they can operate. It also makes it difficult for people to assess the level of confidence they can have in the services they depend on.

Existing certification schemes have difficulty incentivizing the development of responses to known near-future threats. These are threats that are known to affect products made today that remain in service for several years, such as the impact of quantum computing on encryption.[1] To address this it is necessary to change the way in which these frameworks are built.

Long-term collaboration

Fixing this is not just a matter of joining up policy development at the point where new technologies enter the market. It is necessary to form longer term structures for collaboration. For example, the creation in the late 20th century of the Common Criteria,[2] an international programme for product security evaluation that is now ISO/IEC 15408 compliant, was a positive development and continues to bring value today. However, over time and to deal with emerging technologies, countries within the Common Criteria consortium felt the need to develop separate criteria that, while referring back to the common criteria, are country-specific.

This reflects a challenge that should not be underestimated. The value of a certification system is always at risk of becoming frozen in time if it is not built with a governance structure that allows for agile updates and adaptations. Where countries feel that standards are not changing to meet new threats, they will, understandably, take independent action to enhance security in their jurisdictions.

These country-specific responses to emerging threats, such as Singapore's and Finland's approaches[3] to cybersecurity labelling on consumer products, could be the starting point for new forms of bilateral and then multinational collaboration.

1.1 Pathways to collaboration: Cybersecurity certification frameworks

Government cybersecurity agencies and industry regulators are called on to work on the compatibility of security requirements, such as through recognition of industry frameworks, to achieve mutual recognition of device and service certifications, as well as professional certifications.

This would support consumers of services, suppliers, training providers and academia.

It would help consumers make informed decisions on whether the connected products they purchase are safe, support organizations in acquiring high-quality cybersecurity services, and aid the development of cybersecurity experts who can serve their local market and build opportunities for the export of skilled cybersecurity services.

Targeted areas for maximum impact

> If the security of one IoT device in the system is compromised, the whole system can be susceptible. IoT is increasingly being applied where there is potential for great harm.

1. **Internet of things (IoT) devices:** IoT device cybersecurity is becoming crucial. These devices commonly form part of a large networked system of devices. If an attacker compromises the security of one IoT device in the system, the whole system can be susceptible to compromise. IoT devices are also increasingly being applied to areas where there is potential for great harm, such as biomedical devices. IoT is an area where mutual recognition of conformity assessment and certification, alongside a clear articulation of security requirements, will enhance trust, reliability and safety.

2. **Cybersecurity service providers:** It is often difficult for organizations to assess the quality of the cybersecurity services they purchase. Equally, the speed of growth and innovation in cybersecurity services makes it difficult for one government to assess and certify all cybersecurity service providers in each jurisdiction. Cross-border recognition of assessments, attestations, certification or registration of cybersecurity services will be a valuable tool in countering this. An international certification framework that allows for mutual recognition of quality in cybersecurity service provision would provide the assurance that service consumers need, with enough flexibility to allow experts to respond to the global cyberthreat wherever it appears. The creation of a single repository of certified cybersecurity service providers that is internationally recognized is crucial to expanding access to the cybersecurity market pool from different regions, regardless of their countries of origin.

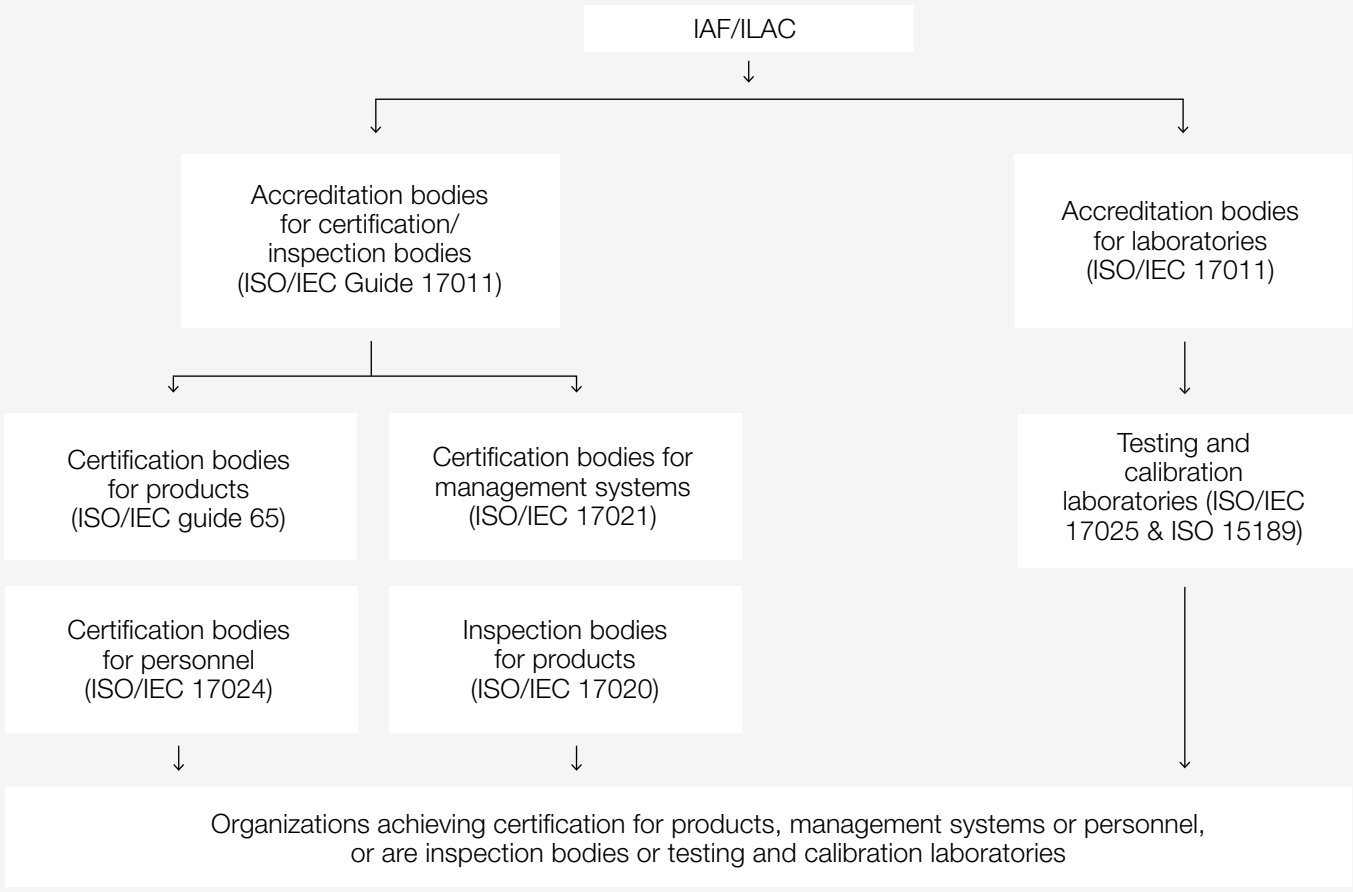
3. **Cybersecurity professionals:** The global shortage of certified/qualified cybersecurity professionals is estimated to be more than 3 million people;[4] one factor aggravating the shortage stems from the industry's lack of a framework that supports cross-border recognition of certifications. This gap can be reduced by promoting the establishment of an international board to certify cybersecurity professionals, like the International Board of Medicine and Surgery (IBMS) or similar organizations operating in professions such as engineering.

2 The cybersecurity certification landscape: Future-proofing digital products and devices

Accreditation and certification frameworks are key to facilitating the entry of cyber-resilient products into the market. The way in which they are governed should evolve so that they can adapt to accelerated technological change.

In general, accreditation[5] and certification[6] frameworks have a top-down flow of information, as highlighted by the example of the International Laboratory Accreditation Cooperation (ILAC) process and the International Accreditation Forum (IAF)[7] in Figure 2.

FIGURE 2 **Top-down certification processes**



Source: Dubai Electronic Security Center

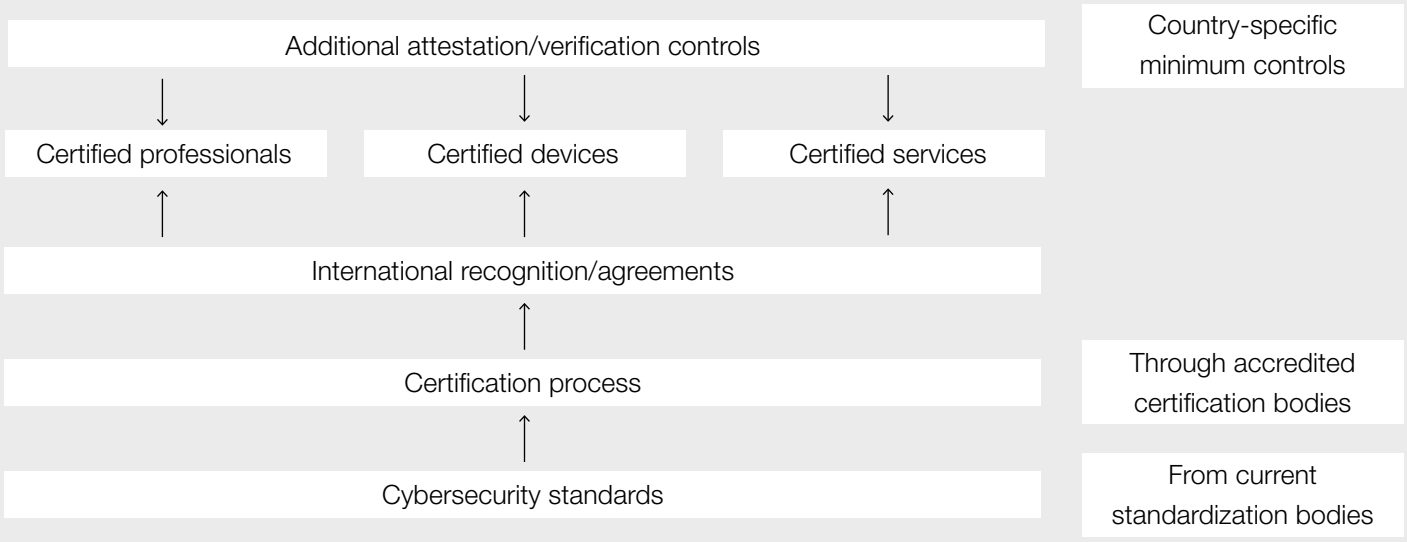
If it is possible to adapt to the speed of product development and incentivize good security practices, there is a need to change how standardization, accreditation and certification systems are governed and recognized in order to adapt to technological developments, changing consumer behaviour and the new security concerns they create.

New connected products, for example, require clear security certification if the public is to trust that innovations are safe. However, the pace of technological development makes it difficult for a cross-border body to respond at speed. Individual countries may be best placed to lead the way, with Singapore and Finland, for example, developing consumer-friendly labelling for products that connect to the internet.[8]

These country-led approaches need not lead to the fragmentation of standards if there are routes to mutual recognition of new best practices.

Rather than introducing new cybersecurity requirements, standards or certification processes, encouraging bilateral or regional recognition of existing certification schemes may provide the flexibility to move ahead securely. As shown in Figure 3, international agreements could work as the basis for the recognition of certifications spanning devices, services and professional expertise. Countries entering such agreements will have the assurance of international standards and certification; and they will also be able to introduce an additional layer of country-specific verification controls.

FIGURE 3 **Outline of the proposed certification programme**



Source: Dubai Electronic Security Center

3 Three areas for priority action

Addressing the certification gaps for internet of things devices, cybersecurity services and cybersecurity professionals

3.1 Cybersecurity of internet of things devices

Already, there are more connected devices than people in the world, according the World Economic Forum's 2020 State of the Connected World report.[9]

Internet of things (IoT) devices connect homes to organizations, organizations to industry, and industry to global supply chains. This creates a risk for individuals, companies and government agencies regardless of their activities or jurisdiction. Despite this risk, the diversity of parties involved in creating the components for an IoT device means that there is no clear international structure ensuring these devices are secure.[10]

With the rising quantity and clear vulnerability of IoT devices, the existing certification process should be upgraded to a model that is effective for this new connected system of devices.

IoT security standards such as ETSI EN 303 645 for consumer IoT and the NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline already exist. Approaches that provide best practice recommendations on security controls for IoT devices, such as ISO/IEC 27002, for example, hold particular value for manufacturers. Because of the vast diversity of IoT devices, the creation of security standards for producers and for the laboratories that are certifying them are welcome. However, without a governance process to link all these processes, it becomes more difficult to support the secure development and use of IoT devices across borders.

Another significant gap is the certification of cybersecurity services relating to penetration testing of IoT networks, as well as IoT cybersecurity audit and consulting services.

FIGURE 4 **IoT device certification gap and recommendation**

IoT device certification

Source: : Dubai Electronic Security Center

Gap

Absence of a unified international standard for security controls for IoT devices and the associated testing

Recommendation

Convene and encourage countries entering appropriate agreements to promote better cybersecurity assurance, for use within the country as well as for easier import and export

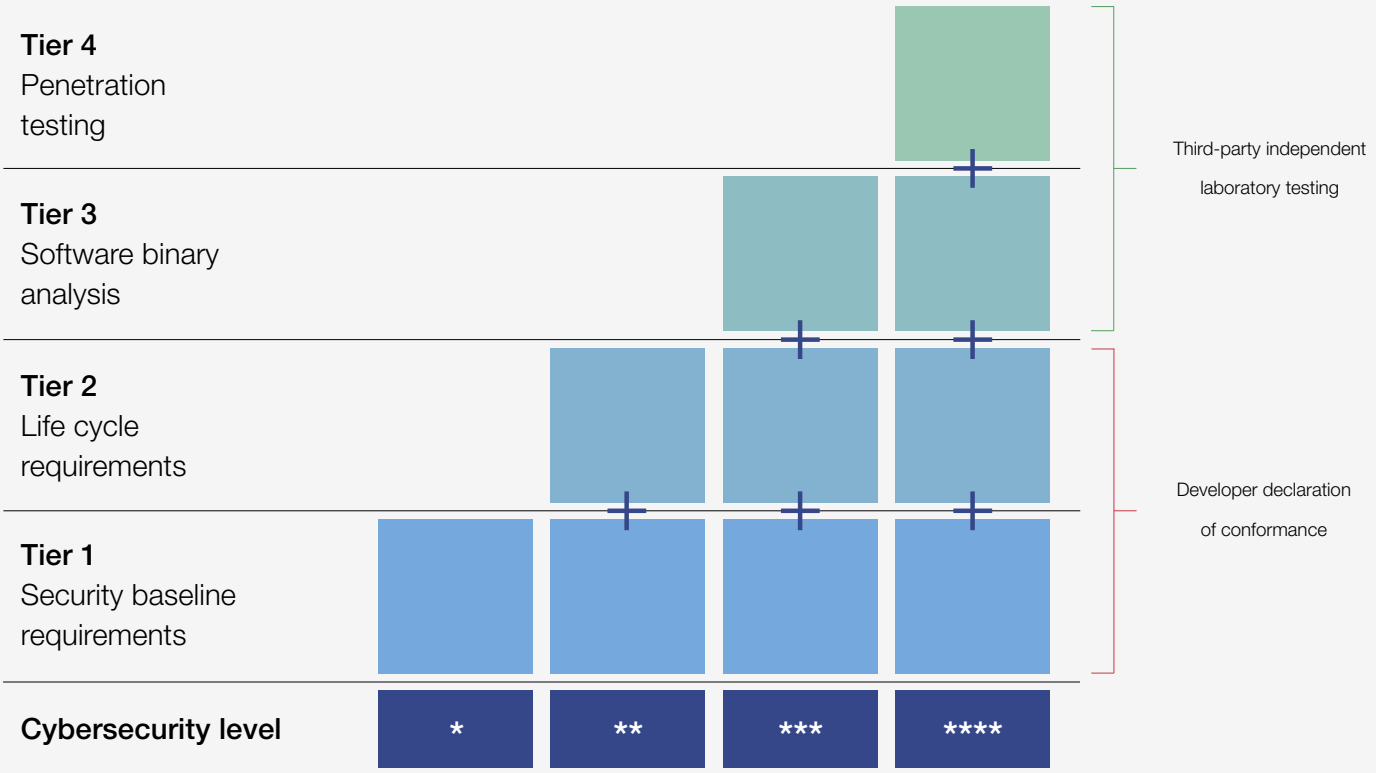
Recommendation

Country-specific certification schemes for IoT device cybersecurity should be combined to develop an internationally recognized certification scheme. This scheme would be based on an agreed set of standards and controls and allow for national add-ons, where needed. For this to be achieved, governments should enter into bilateral or multilateral agreements to promote better cybersecurity assurance for IoT devices.

Case Study: Cyber Security Labelling Scheme, Singapore

The Cyber Security Agency of Singapore (CSA) launched the Cyber Security Labelling Scheme (CLS) for IoT devices in October 2020. It aims to help consumers identify products with better cybersecurity provisions and to incentivize manufacturers to develop more secure products and differentiate themselves from competitors.

FIGURE 5 **Singapore's Cyber Security Labelling Scheme**[11]



Source: : Cyber Security Agency of Singapore

The CLS comprises four cybersecurity levels. Levels one and two are based on self-assessments, with negligible costs for manufacturers. Levels three and four involve third-party independent assessment to provide higher degrees of security assurance. Each assessment tier, to be completed in sequence, reflects the increasing resistance the product has to common internet of things attacks.

It is generally a voluntary scheme with some selective mandatory implementation, such as for home internet routers.

This labelling approach brings clear benefits to consumers and provides manufacturers with an incentive to produce products that meet effective security standards. Currently, the benefit is only for products sold in Singapore; but mutual recognition of standards such as this by other states will increase the economic benefits of designing, manufacturing and marketing, importing and exporting secure digital products.

3.2 Cybersecurity service providers

While international certification of organizations for management system standards is well established, the assessment of how cybersecurity services are provided is fragmented and country-specific, and generally covers only a sample of the cybersecurity providers operating in any one jurisdiction.

A common critique heard from public and private sector partners of the World Economic Forum's Centre for Cybersecurity is that it is difficult to judge the quality of a cybersecurity service provider's capabilities and whether each service they offer fits the needs of the customer until after work has begun.

This is also true in relation to cybersecurity services for emerging products, such as penetration testing of IoT networks, as well as IoT cybersecurity audit and consulting services.

Cybersecurity services can differ greatly in scope and sophistication from vendor to vendor; therefore, the establishment of minimum requirements for such service provisions, whether strategic advice or technical consultation, will be welcome. Another issue is the absence of alignment on important elements, such as the professionalism of auditors, tools and technologies, the exact scope of the audit, the independence of the auditor, etc.

FIGURE 6 **Cybersecurity services certification gap and recommendation**

Cybersecurity service certification

Gap

- Absence of a unified international standard for certifying cybersecurity services
- Absence of alignment on important elements, such as professionalism of consultant, auditors, tools and technologies, determining correct audit scopes, independence of the auditor, etc.

Recommendation

- Promote interoperability between relevant authorities for certification of cybersecurity services
- Certification of an internationally recognized single repository for cybersecurity services and tools

Source: : Dubai Electronic Security Center

Recommendation

An internationally recognized scheme should be developed to certify cybersecurity service providers. This will create a standard framework in which service providers can apply once and will be recognized across borders. At the same time, service consumers will have access to a better certified pool of service providers to react promptly to possible threats and attacks. A single repository of internationally recognized cybersecurity service providers could be created to support this.

Case Study: Israel National Cyber Directorate – Cybersecurity Service Provider Assessments

The Israel National Cyber Directorate[12] (INCD) is focusing on enhancing the level of cyber hygiene of suppliers and has developed an application that serves as a tool for all stakeholders, presenting a supplier's cyber hygiene level. The rationale is encouraging customers to look for secure suppliers with minimum effort. It is also incentivizing suppliers to be more secure. As a first step in certifying cybersecurity services, Israel started to certify professional auditors, qualifying them to certify the level of cyber hygiene of suppliers according to their criticality as suppliers and types of service.

This is a three-layered approach:

1. **Knowledge base** – A national methodology *developed in collaboration with industry* enables organizations to use a modular questionnaire that adapts the risks to be managed based on an organization's supply chain and the services provided.
2. **Accessibility** – Questionnaires should be clear and straightforward to answer and provide evidence of compliance. To support this, the INCD also facilitates the use of reporting and dashboard tools that improve the user's situational awareness.
3. **Data trust** – A cyber expert supply chain auditor certification scheme ensures auditors have been trained on the basis of the national methodology and meet INCD's requirements.

3.3 Certifications for cybersecurity professionals

Many certifications for cybersecurity professionals exist, ranging from qualifications aimed at organizational risk management through to highly technical certifications.

While these solutions might be adequate individually, there is no unified international scheme that recognizes the existing certification of cybersecurity professionals and makes them translatable across sectors and borders. This lack of comparability exacerbates the shortage of skilled cybersecurity professionals, creates difficulties in recruiting for specialist positions, increases the cost to individuals who are studying for cybersecurity qualifications, and acts as an obstacle in designing reliable high-volume approaches to educating cybersecurity professionals in countries where the skills shortage is most keenly felt.

FIGURE 7 **Cybersecurity professional certification gap and recommendation**

Cybersecurity professional certification

Source: : Dubai Electronic Security Center

Gap

- Absence of a unified international standard for certifying cybersecurity professionals
- Prominent shortage of cybersecurity professionals

Recommendation

Promote the establishment of an international board similar to international boards for physicians and engineers to certify cybersecurity professionals.

Recommendation

Promoting the establishment of an international board for cybersecurity professionals similar to existing international boards for physicians and engineers to certify cybersecurity professionals is a viable route to address the issue. The cybersecurity skills shortage means that cross-recognition of this scheme is important. In the short to medium term, securing economies requires the movement of expertise, physically or virtually, across state borders.

Case Study: CREST

CREST[13] offers certifications in penetration testing, threat intelligence, intrusion analysis and security architecture. CREST has conducted the evaluation of codes of conduct and codes of ethics, and operates a centralized register. There are processes in place for the development, launch and management of new exam content.

Through collaboration with international and regional groups, key stakeholders contribute and review exam content and syllabus areas. Having this international interaction allows the exams to remain relevant and include best practices internationally. This also allows for the matching of the syllabus and content against internationally recognized standards.

There are formal processes in place for the development, launch, review stage and management of new exam content.

CREST has formal agreements with other certification providers, allowing mutual recognition. This facilitates the wider international adoption of examinations and ensures there is no monopoly and that there are clear career pathways between all certifications.

The cybersecurity industry sees a central list of certified individuals as an advantage and generally accepts it. This method is beneficial for the service suppliers who employ the professionals as it allows for the easy transition of staff internationally.

4 What should the community do next?

On the path to a secure future, the lack of widely accepted and scalable cybersecurity certification frameworks that can be applied internationally and across sectors is a stumbling block.

The challenges posed by the security certification of IoT products has been recognized for several years[14] but the IoT space is, arguably, more fragmented than previous technical developments. Even regions with high levels of cybersecurity maturity are still working out how to best analyse and understand this space[15] and no one group is taking the steps needed to clarify and incentivize best practices.

As a matter of urgency, it is necessary to take steps to implement a cross-border approach to assessing and certifying the cybersecurity of IoT products. The best starting point for this may be bilateral or regional multilateral agreements aimed at the mutual recognition of certification and labelling. Some states are already tackling the security concerns arising from emerging technologies and digital products. These efforts can be recognized and built on elsewhere.

Building a cross-border approach to the assessment and certification of cybersecurity services and professional cybersecurity qualifications would unlock significant value. Current approaches are too narrow; they neither include all effective cybersecurity providers and experts nor do enough to highlight where service provider capabilities do not meet the requirements of the tasks they aim to solve.

Establishing an international board for cyber-security professionals could do much to clarify cybersecurity career paths, making it easier for individuals, organizations and countries to increase their cybersecurity skills base. The increasing importance of cybersecurity to the good functioning of an economy means this creates social and economic benefits.

A sense of collective responsibility should now lead to collective action between government agencies, industry and standard setters. An international platform to facilitate the cross-border recognition of cybersecurity certifications is the next step.

Methodology

Research for this World Economic Forum community paper was based on a multi-region review of certification efforts in individual countries, as well as cross-border approaches such as the Common Criteria Recognition Arrangement (CCRA).[16] The International Organization for Standardization (ISO) Committee on Conformity Assessment (CASCO) conformity assessment guidelines and standards,[17] International Telecommunication Union (ITU) interoperability and conformity programme[18] and the European Union cybersecurity certification framework[19] were reviewed. Other work initiatives that influenced the shape of this report include ISO's work on certification and conformity, and ITU's work on conformity and interoperability regimes.[20]

Acknowledgements

Lead authors

Bushra Al Blooshi
Dubai Electronic Security Center,
United Arab Emirates

Ayesha Al Marzooqi
Dubai Electronic Security Center,
United Arab Emirates

Co-authors

Hoda Al Khzaimi
New York University Abu Dhabi (NYUAD),
United Arab Emirates

Angelika Eksteen
AI Directions, United Arab Emirates

Global Future Council Managers

William Dixon
Centre for Cybersecurity,
World Economic Forum

Sean Doyle
Centre for Cybersecurity,
World Economic Forum

Contributors

Samantha Alexander
CREST International

Yosi Averam
Israel National Cyber Directorate, Israel

Ian Glover
CREST International

David Koh
Cyber Security Agency, Singapore

Lim Soon Chia
Cyber Security Agency, Singapore

Henry Tan
Cyber Security Agency, Singapore

Reviewers

Maya Bundt
SwissRe

Michael Daniel
Cyber Threat Alliance

Gabi Dreo
Research Institute CODE

David Mudd
British Standardization Institute (BSI)

Arina Pazushko
BI.ZONE

Dmitry Samartsev
BI.ZONE

Colin Soutar
Deloitte

Endnotes

1. (ISC)², Cybersecurity Professionals Stand Up to a Pandemic, Cybersecurity Workforce Study 2020, 2020, https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B.
2. U.S. Cybersecurity and Infrastructure Security Agency, The Common Criteria, 2013, https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria. Common Criteria Portal, commoncriteriaportal.org.
3. Government of Singapore, About CLS, https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls. Finnish Cybersecurity Label, https://tietoturvamerkki.fi/en/.
4. (ISC)², Cybersecurity Professionals Stand Up to a Pandemic, Cybersecurity Workforce Study 2020, 2020, https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B.
5. Accreditation is the formal recognition by an independent body, generally known as an accreditation body, that a certification body operates according to international standards. See the International Organization for Standardization at https://www.iso.org/certification.html.
6. Certification is the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.
7. ILAC, the international organization for accreditation bodies, https://ilac.org/. International Accreditation Forum (IAF), https://www.iaf.nu/.
8. Government of Singapore, About CLS, https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls. Finnish Cybersecurity Label, https://tietoturvamerkki.fi/en/.
9. World Economic Forum, *The State of the Connected World*, 2002, http://www3.weforum.org/docs/WEF_The_State_of_the_Connected_World_2020.pdf.
10. See Asanghanwa, E., "Solving IoT device security at scale through standards", 19 October 2020, https://azure.microsoft.com/en-us/blog/solving-iot-device-security-at-scale-through-standards/.
11. Government of Singapore, CLS for Manufacturers, https://www.csa.gov.sg/programmes/cybersecurity-labelling/for-manufacturers.
12. Government of Israel, Israel National Cyber Directorate, https://www.gov.il/en/departments/israel_national_cyber_directorate.
13. CREST, https://www.crest-approved.org.
14. European Union Agency for Cybersecurity (ENISA), *Challenges of security certification in emerging ICT environments*, February 2017, https://www.enisa.europa.eu/news/enisa-news/challenges-of-security-certification-in-emerging-ict-environments.
15. European Union Agency for Cybersecurity (ENISA), *Cybersecurity Certification Market Study, Towards a research and analysis methodology*, April 2021, https://www.enisa.europa.eu/publications/cybersecurity-certification-market-study.
16. Common Criteria Portal, https://www.commoncriteriaportal.org/.
17. International Organization for Standardization (ISO), ISO's Committee on Conformity Assessment (CASCO), https://www.iso.org/casco.html.
18. International Telecommunication Union (ITU), ITU Conformity and Interoperability Portal, https://www.itu.int/en/ITU-T/C-I/Pages/default.aspx.
19. European Union Agency for Cybersecurity (ENISA), EU cybersecurity certification framework, https://www.enisa.europa.eu/topics/standards/certification.
20. International Telecommunication Union (ITU), *Establishing Conformity and Interoperability Regimes, Basic Guidelines,* February 2014, https://www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/CI_BasicGuidelines_February2014_E.pdf.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org