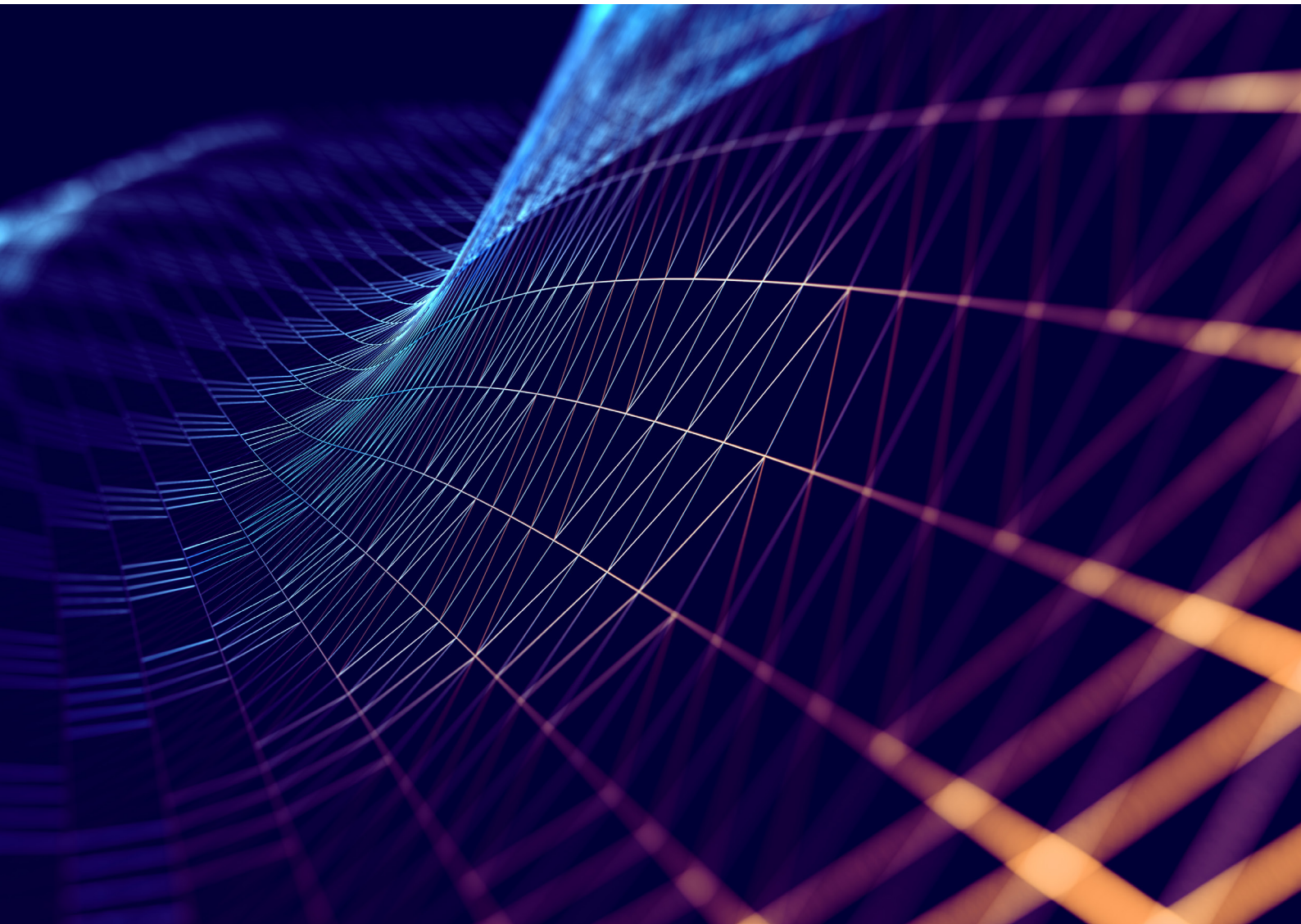
# ICC Policy Primer on Cybersecurity



# Contents

# Introduction

The private sector has, and continues to assume significant roles and responsibilities in the development of information communication technologies (ICTs). As the representative of 45 million companies of all sizes and sectors in over 100 countries, the International Chamber of Commerce (ICC) is committed to ensuring that digital technologies work for everyone, every day, everywhere, in order to fully realise the potential of the digital economy and to safeguard proper functioning of critical infrastructures. While this was always an important goal, in the context of the current COVID-19 pandemic it is fundamental, as safe, secure and resilient digital networks are vital to maintain the proper functioning of our economies and societies and protect lives and livelihoods across the globe.

ICC works with governments and businesses worldwide to build a common understanding of what constitutes a robust cybersecurity policy given the proliferation/ever increasing tide of attacks and best practices in order to foster a more secure Internet for businesses and users.

With a hundred-year history of developing globally recognised applicable rules by convening experts and practitioners, ICC considers it essential that businesses and governments have a shared understanding of how to conceptualise cybersecurity risks, targets, impacts, and responses, including national and international laws and norms. While governments and business have different roles in addressing cybersecurity, they are mutually reinforcing.

This policy primer highlights some of the main issues and challenges that businesses and society are facing. Part 1 of the paper presents a non-exhaustive list as a starting point to identifying key issues, so that all stakeholders can work together towards effective solutions. Part 2 of the paper outlines key areas where ICC and its members will develop further issue papers to provide further considerations, practical tools and policy recommendations for both private and public sector actors.

# Context: The impact of cyber threats on business

With damage related to cybercrime projected to hit $6 trillion annually by 2021[1], businesses, policymakers and users struggle to keep up with rapidly evolving online threats. Today, cybercrime impacts all businesses regardless of size or industry or geographical location, with around 50% of all cyber attacks being committed against small and medium-sized enterprises (SMEs).[2]

The digital economy, the Internet, and the cross-border data flows that support it have already accounted for considerable GDP growth in many countries.[3] Arguably, the greatest economic impact of the digital economy comes from the digitalisation of traditional industry processes, as companies across all sectors seek to use technology to improve their business operations and models.[4] However, cybercrime threatens to thwart the potential economic impact of ICT and digital, as consumer and business express concern over cybersecurity.[5]

As the COVID-19 pandemic spread across the globe, many organisations started moving substantial parts of their operations online in order to ensure business continuity, protect workers and continue to serve customers. In the wake of the crisis, there has been an upsurge in the use of online and digital tools that created and continues to create new opportunities for malicious actors to take advantage of the disruptive effects of the crisis and target businesses, especially SMEs for cyber-attacks.

---

**1** Cybersecurity Ventures (2020), Cybercrime Report
**2** Cybersecurity Ventures (2017) *Cybercrime Report*
**3** McKinsey (2011) *The great transformer: The impact of the Internet on economic growth and prosperity*
**4** UNCTAD (2017) World Investment Report 2017: Investment and the Digital Economy.
**5** Mckinsey (2015) *Digitizing the value chain*

Even before the current crisis, the impact of cyber attacks was increasingly worrying. In 2019, the average cost of a data breach was USD$ 3.92 million.[6] A recent report suggests that small businesses are the target of over 40% of cyber-attacks with an average loss per attack of more than US$ 188,000.[7] Yet, the cost of cyber breach for business extends beyond just purely monetary damage, as the loss of trade secrets, privileged and proprietary information, or reputational damage could threaten to destroy a business altogether.[8] In the United States, 60% of SMEs are out of business within six months of a cyber attack.[9] As businesses across all parts of the traditional economy, from manufacturing to energy, seek to digitalise their operations as a way to increase competitiveness, this provides new opportunities for cybercrime to further expand, especially as state and non-state actors increasingly seek to target and disrupt critical infrastructure and systems.[10]

The borderless nature of the Internet, the digital economy, increased cyber-physical interdependency through IoT, and cybercrime paints a complex legal and operational picture for cybersecurity. Almost all sectors utilise ICT and rely on the Internet for everything from the simplest to the most strategic tasks. Global supply chains are increasingly interconnected, and the ICT systems along those supply chains have both internal and external devices meant to facilitate business operations. However, these interconnected systems create a complex landscape where combating cybercrime can prove particularly challenging, as malicious actors can easily exploit vulnerabilities in business processes and target individual employees across all parts of the supply chain. In addition to operational and behavioural risks, the technical manifestations of cyber attacks—from Malware to Ransomware to supply chain cyber attacks—are constantly evolving.

Furthermore, increased government investment in advanced cyber capabilities has in no small part driven the escalation of sophisticated attacks.[11] Reports suggest that more than 60 nations are now developing such capabilities[12] as the business community continues to be exposed to serious and growing cyber threats from state actors.[13] State-sponsored espionage has been on the rise, with 20% of global businesses ranking it as the most serious risk to their business.[14] Many of today's most sophisticated cyberattacks have been attributed either directly to States or to the actions of their proxies. Even attacks conducted by independent malicious actors are often a downstream consequence of government activity, as cyber capabilities proliferate quickly when they are stolen, sold, or otherwise repurposed to criminal ends. Increasingly, we are seeing advanced cyber powers sitting atop a toxic pyramid of malicious actors, with their tools and tactics proliferating downward and into a dangerous ecosystem of affiliated and unaffiliated threat actors with both political and criminal objectives.

At the same time, when it comes to cyber-attacks there are significant asymmetries between offenders and defenders in skills, tools and cost. Out of 10,000 attacks, the defender needs to be right 10,000 times, while the offender only once, to be successful. Offenders oftentimes have a larger, better equipped toolbox compared to the defence capacities of businesses (especially MSMEs) and users. Cybercrime has a high pay-out ratio, with relatively small cost from the attacker, while defensive cyber-expenditures are considerably higher. Thus, businesses, consumers and users of technology are fighting a losing battle, without the support of governments both in the domestic and international realm.

---

**6** Ponemon (2019) *Cost of a Data Breach Report*

**7** Verizon (2019) Data Breach Investigation Report

**8** Eubanks (2017) The True Cost Of Cybercrime For Businesses. *Council Post*; Ponemon (2016) *Cost of Cyber Crime Study & the Risk of Business Innovation*

**9** Miller (2016) 60% of small companies that suffer a cyber attack are out of business within six months. *Denver Post*.

**10** McKinsey (2019) *Unlocking the value of digital operations in electric power generation;* UNCTAD (2017) *World Investment Report 2017: Investment and the Digital Economy*

**11** Hi-Tech Crime Trends 2018. Group-IB. Oct. 2018. https://www.group-ib.com/media/hi-tech-crime-trends-2018/

**12** Valantino-DeVries, Jenniter, Lam Thuy Vo, Danny Yadron. *Cataloging the World's Cyberforces.* Wall Street Journal. http://graphics.wsj.com/world-catalogue-cyberwar-tools/

**13** Council on Foreign Relations (n.d.) State-sponsored cyber operations tracker

**14** Businesswire (2017) Cyber Espionage Tops the List as Most Serious Threat Concern to Global Businesses in 2017

Neither businesses nor governments can combat these borderless threats on their own. Cybersecurity is a resource intensive activity, tapping into both private and public sector reserves. As businesses and regulators both seek to find meaningful ways to mitigate cybersecurity concerns, collaboration is required in order to build awareness of vulnerabilities and incidents and to increase resilience against these complex, borderless cyber threats.

The private sector relies on a secure, stable and trustworthy policy and regulatory environment to foster opportunity, spur innovation, and create value for communities. Actions that undermine this enabling environment pose a threat not only to security, but also to economic development and livelihoods. It is therefore imperative that industry take part in international policy discussions on cybersecurity, for two main reasons.

First, a common interpretation of international law and norms is necessary to ensure legal certainty and the predictability of state behaviour, which in turn has a very significant impact on investment decisions and on the risks that companies can quantify in their multinational operations.

Second, due to the borderless and interconnected nature of both the digital economy and cyberthreats, national approaches to cybersecurity require international agreements and cooperation in order to work properly.

Tangible outcomes and concrete indicators that objectively reflect responsible state behaviour in cyber-space are needed. While the important issues regarding the process and norms that aim to provide conduits and mechanisms to achieve outcomes continue to be essential, there is an urgent need for measurable improvements on the ground. Defining shared outcomes, indicators and follow up procedures in the short and long term are critical. The private sector is best placed to inform policymakers of the uses and desired effects of such measures as well as to point out potential barriers that might impact their implementation.

# **Part 1**
# Current challenges in cybersecurity

## Lack of common understanding of cybersecurity threats and concepts

The impact of a cyber attack varies significantly due to the nature of the actor, the motive, the target and the threat category, as well as the frequency, the degree of success of an incident and the severity of the consequence. One of the challenges of fostering comprehensive approaches to cybersecurity is the lack of definition and common understanding of the types of threats. This complexity and consistently changing environment makes conceptualising threats difficult, fragmenting approaches to cybersecurity and thus contributing to an environment where cybercrime can flourish.

## A lack of common and effective interpretation of norms and laws

Collaboratively addressing cybercrime is important for creating effective global cyber resilience. While there have been a number of international and bilateral policy statements to restrain cyber attacks targeting enterprises and critical infrastructure, progress in developing and adopting international norms governing and binding states to responsible behaviour in cyberspace has been slow.[15]

---

**15** The Group of Governmental Experts is a UN-mandated working group on Advancing responsible State behaviour in cyberspace in the context of international security that has been working since 2004.See, UNGA Resolution 73/266.

**At the international level**

While many agree that laws offline should also apply online, currently there are major differences among States on the interpretation, applicability and implementation of international law. Without common understanding on how international law, in its entirety, is applied in cyberspace, there is little hope for defining and enforcing accountability for responsible State behaviour in cyber space, and as a consequence, improving the trust landscape for all stakeholders is impaired.

Cross-border cooperation for cybercrime also faces its own challenges without common effective cross-border criminal investigation and prosecution that is consistent with the rule of law and international treaties, arrangements and international cooperation mechanisms. Arrangements and international cooperation mechanisms between enforcement agencies can often be an effective way to deal with cybercrime that crosses borders. Currently, the Convention on Cybercrime of the Council of Europe (Budapest Convention) is the only binding international instrument on cybercrime aimed at facilitating this level of cooperation. Mutual Legal Assistance Treaties (MLATs) whether bilateral or regional provide another mechanism to enable law enforcement to access data in other jurisdictions with greater efficiency. In this respect, the Convention on Transboundary Organised Crime also has an important part to play.

**At the national level**

Businesses rely on the support of government to ensure that the necessary laws are in place so that cybercrime activity is illegal. Governments should ensure similar criminalisation of specific cybercrimes and crimes committed in cyberspace to avoid the creation of 'cybercrime havens'

Lack of cooperation or awareness of similar efforts across jurisdictions and regions poses further challenges to the alignment of policies and regulations, that could help reduce uncertainty and foster trust in the digital ecosystem.

## Deficiencies in capacity and confidence-building measures

First-time users and certain demographics (e.g. children, women) are most often affected by the impact of cybercrime, cyberbullying and other cyber risks. These groups and all other Internet users need to be able to identify risks and manage threats effectively to take advantage of the opportunities that the Internet offers.

From a business perspective, it is vital that a company—large or small, click-and-mortar or high-tech—be able to identify their cyber security risk and effectively manage threats to their information systems. At the same time, all business managers spanning from directors of small family business to executives of large multinational companies must recognise that absolute security is an elusive goal. Unlike many business challenges, cyber security risk management remains a problem with no easy fix available.

A critical dimension to consider is that many developing countries want and need technical assistance to create the legal, regulatory, and related infrastructure to support the development of a secure, trusted, rules-based digital environment. The need remains great: too many countries still do not have a CERT, data protection at law, cybersecurity legislation in force or national cyber strategies—and the related technical and practical infrastructure that is essential to support them.

## The chilling effect of disproportionate regulatory responses

ICT supply chains are global. Integration and interdependence are key aspects of the digital environment that relies on compatible rules between national jurisdictions and global data flows to work seamlessly.

Further cooperation and efforts are needed to develop practices aimed at ensuring cybersecurity measures not only provides necessary protection, but also enable data driven innovations. Global cross border data flows enable both economic growth and societal benefits. Implementing cyber measures that disproportionately restrict cross-border data flows or reduce market access might negatively impact trade, investment, or innovation.

Security is an essential element of trust in new and emerging technologies and a factor that can impact any organisation connected to the Internet, but it is not a one-size-fits-all solution and thus not suited to narrow top-down prescription. As new technologies continue to develop and emerge, cybersecurity implications need to be considered on a case-by-case basis.

# **Part 2**
# Responding to cybersecurity challenges

In order to address the above-mentioned challenges, ICC recommends that all stakeholders:

- work together to develop a common understanding among both private and public sector actors (at national and international levels) of cybersecurity threats, actors and approaches;
- recognise that international law applies in its entirety in cyberspace; based on this premise, governments, in consultation with all stakeholders, should adhere to agreed international norms as well as develop mechanisms to effectively implement those norms and consider, where appropriate, the development of new international norms and/or national legislation.
- work towards the introduction and application of national criminal policy aimed at the protection of businesses and society from cybercrimes.
- recognise the importance of greater cooperation between national governments in combating cybercrimes with well-functioning and tailored cooperation in criminal matters.
- work together to further expand capacity- and confidence-building measures; and
- consider cybersecurity measures and standards, as they relate to specific existing and emerging technologies, on a case-by-case basis in accordance with international norms and laws, through a risk-based approach.

## Conceptualising cyber threats, actors and responses

In securing their own assets and operations and taking steps to protect users and clients, businesses increasingly understand the importance of implementing holistic cybersecurity risk management processes. Businesses constantly develop and deploy measures designed to ensure the security of networks, protect users, protect devices and protect the content residing on these networks from attack. Such measures include activities to not only identify and mitigate cybersecurity risks but also to detect, respond to, and recover from cybersecurity incidents or events.

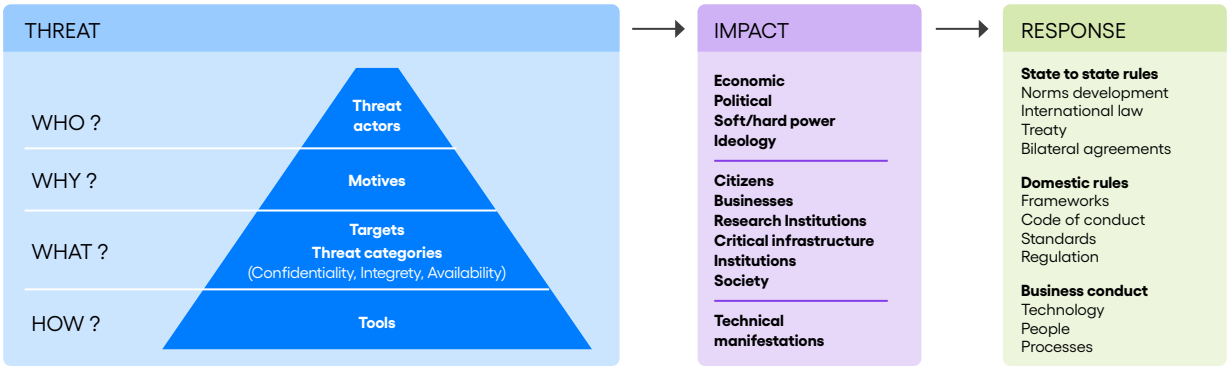
Given the constant threat and responses to cyber attacks, business approaches to cybersecurity, however, can only go so far and effective public-private cooperation is essential to strengthen Internet security and respond to the large and growing range of cybersecurity threats to the global Internet. It is essential that businesses and governments have a shared understanding of how to conceptualise cybersecurity threats, impacts, and responses.

Approaches to cybersecurity must be holistic and consistent across sectors and recognise critical interdependencies in both national and international contexts. As governments seek to promote and ensure sufficient use of effective approaches to cyber risk management, they should be cognisant

of similar efforts across jurisdictions and regions and seek to align policies and regulations to the greatest extent practicable.

Globally aligned approaches to cyber risk management can facilitate interoperability and improve visibility and understanding among entities that have cross-border operations. Therefore, it is important that businesses and governments have a shared understanding of how to conceptualise cybersecurity threats, impacts, and responses. Figure 1 helps navigate a common approach to cybersecurity.

***Figure 1*** *A common approach to cybersecurity*




## Developing and implementing shared norms

While business must be proactive in securing their own assets and operations and taking steps to protect users and clients, they should also be able to count on the support of governments to ensure that the necessary laws are in place and implemented to guarantee that certain cybersecurity events are illegal.

With this in mind, ICC urges governments to implement and adhere to norms that have previously been agreed in UN discussions, as well as to develop mechanisms to effectively implement those norms.

As a first step, governments should start by complying with established international norms and/or, as needed to increase clarity, develop recognised global norms and practices in collaboration with relevant stakeholders. For example, governments can:

- Develop recognised international norms that promote a stable ecosystem, in collaboration with industry.
- Improve understanding of and consensus regarding the ways in which existing international law govern state behaviour online.
- Leverage previous agreements on norms to provide a roadmap for future discussions and establishment of more specific standards that protects cross-border data flows and free expression. This should also include the commitment for states to consistently prevent any form of cybercrime emanating from its territory and prohibit offensive use of cyber by State actors in peace time, including cyber-enabled, state-sponsored theft of business confidential information and disruptions of critical infrastructure[16].

Business supports the norms agreed by the UN Governmental Group of Experts in 2015 and looks forward to contributing to their implementation and to further strengthening these norms.

In addition, the private sector has already supported, collaborated on, and launched initiatives to promote ambitious norms for responsible uses of technology, such as the Global Forum on Cyber

16 World Economic Forum: Global Risks Report 2018 http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Expertise, the Cybersecurity Tech Accord, The Paris Call for Trust and Security in Cyberspace or the Internet Society MANRS initiative, to name a few. We will continue to support such work going forward and will support information sharing and cooperation among such initiatives.

When it comes to fighting cybercrime, governments can implement mechanisms to coordinate international law enforcement efforts and facilitate investigation and extradition processes. The Budapest Convention is the only binding international instrument specifically on cybercrime, and States could consider becoming a signatory to the Budapest Convention or using it as a guideline for developing comprehensive national legislation. States should also take advantage of the Convention on Transboundary Organised Crime to improve mutual legal assistance with respect to cybercrime. Governments can also consider establishing bilateral or regional Mutual Legal Assistance Treaties (MLATs), which enable and facilitate cross-border law enforcement cooperation, while maintaining sufficient protections for privacy and security.

As governments seek to promote or ensure sufficient use of effective approaches to cyber risk management, they should be cognisant of similar efforts across jurisdictions and regions and seek to align policies and regulations to the greatest extent possible. Such approaches also ensure that all local organisations can access best-in-class technologies, services, and security offerings and expand their operations, either by directly growing across markets or by integrating into offerings of cross-region suppliers.

## Enhancing capacity building

Increased awareness about cybersecurity and knowledge about how to protect networks can strengthen not only individuals, businesses and communities but also the ability of a whole country to protect critical digital infrastructure and combat cyber threats. This has never been more clear than during the Covid-19 crisis. The maturity of cybersecurity capacity in a country encourages confidence in the online environment and fosters meaningful access by all groups in society, thus helping address digital divides.

ICC has a proud, hundred-year history of providing companies with tools and self-regulatory guidance to promote good business practice. ICC's Commission on the Digital Economy developed a simple, clear guide in 2015 to help business play their part in addressing the increasingly serious challenge of cyber security. The ICC Cyber security guide for business is informed by global cyber security guidelines and national strategies and presents five principles that help enterprises identify cyber security risks and, drawing on various sources and best practices, goes on to pinpoint six key actions that companies should implement.

ICC also recently partnered with the Cyber Readiness Institute (CRI), a non-profit initiative that convenes senior business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises. Through this partnership, ICC will work to make available the CRI Cyber Readiness Program to all our 45 million members of all sizes and sectors worldwide looking to protect themselves from digital threats.

That said, many countries do not have the fundamentals in their legal codex: data protection frameworks are missing in dozens of countries; many do not have a CERT/CSIRT, and cybercrime and other cyber legislation is outdated, or entirely missing, in others.[17]

---

**17** For more details see the Global Cyberlaw Tracker kept by the UN Conference on Trade and Development, at https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.

There is a need for much greater capacity building to ensure basic legal and infrastructure to build cyber trust and enable participation in global cybersecurity efforts.

## Cybersecurity applications and standards

Trust and confidence in the availability, reliability, and resiliency of information systems and networks, including the Internet, must continue to be strengthened in order to fully realise ICT-enabled economic growth and ensure the seamless operation of global business. All stakeholders must work together to promote effective cyber security practices and the open, secure, stable, resilient, and globally interoperable Internet.

Efforts should be made to both highlight the importance of the issue and encourage continued research, innovation and deployment of context appropriate security solutions. As security solutions are implemented, due regard should also be paid to assure that security measures are consistent and proportionate with the related risks and desired results and consider interoperability across various technology implementations.

In a situation that requires a regulatory response at a national level, proportionality can be achieved by first, assuring good estimates of the impact of cyber attacks on businesses and societies. Second, when considering appropriate (regulatory targeting) and effective (net benefit) regulatory interventions, proportionality can be achieved by balancing the impact of cyber attacks with the private and public resources required to strengthen resilience throughout the entire value chain as costs can become prohibitively expensive for smaller organisations

When considering cyber legislation, states must try to balance the benefits of trade, investment and innovation against genuine national security concerns. In the rare case that national security requirements need to be considered, States should seek to implement measures that are transparent, predictable, proportionate, and not a disguised restriction on trade.

Cyber security standards can often be best achieved through self-commitments of market participants, and various initiatives and cooperation groups already have been set up. Security testing should be permitted in a manner that facilitates the adoption of Common Criteria (see, e.g. https://www.commoncriteriaportal.org/) and is consistent with existing applicable law. The common standardisation approach enables dynamic adaptation, in order to adjust and take into account technology changes, diverse threats and risk scenarios.

# Conclusion

To achieve positive results, governments should collaborate with other stakeholders to promote a culture of security, with appropriate legislation in place to combat cybercrime. Similarly, appropriate policies and legal frameworks related to data protection and privacy are also essential to ensure that consumers and citizens can continue to trust ICTs and use online services.

Multistakeholder collaboration promotes shared understanding of the multifaceted impact of cyber attacks and helps build consensus on the ways in which existing international law governs nation-state behaviour on the Internet. These exchanges will reflect ongoing learnings on the evolving threat environment and help promote a holistic approach to cybersecurity risk management. Expert forums such as European Cybersecurity Industry Leaders, 3GPP SECAM, the OECD's Working Party on Security and Privacy in the Digital Economy and the Forum of Incident Response and Security Teams are commendable efforts providing detailed guidance on ways to conceptualise and understand threat actors, tools and technical manifestations. Additionally, national and regional Computer Incident Response Teams (CIRTS) can act as a convener for stakeholders and enable education and best practices on cybersecurity issues.

Effective public-private cooperation is essential to strengthen Internet security and respond to the large and growing range of cybersecurity threats to the global Internet.

## About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 E icc@iccwbo.org
www.iccwbo.org @iccwbo