UNCDF
Unlocking Public and Private Finance for the Poor

The role of cybersecurity and data security in the digital economy

As economies shift to digital and online models, threats can quickly outpace traditional approaches to data security. More than ever, governments and organizations need to be proactive in creating and adapting systems to face these threats. By safeguarding their own operations, the information of people who use their services will be better protected as well.

The brief, written in close collaboration with Macmillan Keck, seeks to identify specific attributes cybersecurity and data security frameworks that can help policymakers and regulators build a digital economy that includes — and serves — everyone.

BRIEF

February 2022

Macmillan Keck

Seharish Gillani,
Ahmed Dermish, and
Jeremiah Grossman
of the UNCDF
Policy Accelerator

Summary

The economic cost of information and technology asset security breaches in 2020 was a staggering USD 4-6 trillion, equivalent to about 4-6% of global GDP. Data security and cybersecurity each seek to maintain the confidentiality, integrity and availability of information assets. Most cyberattacks are financially motivated. Typically, a threat actor will infiltrate the target system and then employ malware to extract information assets, withdraw funds, demand a ransom, or carry out other misdeeds.

Strengthening cybersecurity requires coordinated action. The ITU has a cybersecurity capacity building programme for developing countries.[1] At least 114 national governments have adopted cybersecurity strategies and 118 have established national Computer Security Incident Response Teams (CSIRTs). Many have set up cybersecurity agencies and some have established sector CSIRTs to protect critical infrastructure. Many are updating criminal laws and strengthening enforcement. The Council of Europe Convention on Cybercrime, which promotes international harmonization in the investigation and enforcement of cybercrimes, has been joined by 45 member states and 22 states in Africa, the Americas, and the Asia-Pacific.

In addition, national and international standards organizations have developed cyber risk management frameworks. Enterprises are also increasingly establishing their own internal CSIRTs. Public and private institutions have increased the focus on awareness and education. Developed countries are investing to close the global cybersecurity skills gap of needed workers.

Considerations while reading this brief

1. Which challenges related to cybersecurity and the digital economy are most prominent in your market, both a) in general and b) for underserved groups such as women and low-income people?

2. Do cybersecurity and data security regulations in your country address:
   - **Digitization:** The application of cybersecurity and data security regulation to the digital economy?
   - **Inclusivity:** The specific cybersecurity and data security challenges faced by women, low-income people, and/or other underserved groups?

3. Which entities are responsible for regulation of cybersecurity and data security? Are responsibilities clear, and are mechanisms in place to avoid regulatory arbitrage? If not, how could this be improved?

Nature and importance of data security and cybersecurity

Securing the confidentiality, integrity and availability of information assets

The terms ***data security***[2] and ***cybersecurity***[3] are often used interchangeably because both seek to protect ***information assets*** (valuable data and information)[4] and secure ***technology assets*** (hardware, software, systems, servers, networks and other electronic containers that collect, process, transport, store and retrieve information assets).[5] The distinction is subtle, with data security emphasizing direct protection of information assets themselves and cybersecurity emphasizing securing technology assets as a means to protect information assets.

Both data security and cybersecurity seek to maintain the confidentiality, integrity and availability of an organization's information assets. In this context, ***confidentiality*** means ensuring access to information assets is limited to authorized persons and systems; ***integrity*** means ensuring information assets remain in the condition intended by the owner; and ***availability*** means ensuring reliable access to information assets by authorized persons and systems.[6] These three security pillars are known as the *CIA triad.*[7]

A ***security incident*** is an event that compromises the integrity, confidentiality or availability of information assets, a ***data breach*** is a security incident that results in disclosure of confidential data to an unauthorized person, and a ***cyberattack*** is an unauthorized attempt by a ***threat actor***[8] to compromise information or technology assets.[9] Security threats to information and technology assets today are wide-ranging and evolving.[10]

The growing importance of information and technology assets

Public and private enterprises are amassing massive and growing volumes of information assets as individuals are also increasingly creating, collecting, sharing and consuming data.[11] Enterprises and individuals rely increasingly on information and technology assets to provide or procure goods, services and information.[12] Enterprises[13] and individuals[14] are also entrusting their information to other enterprises or individuals at growing rates. In both high-income and developing countries, individuals are embracing digital technologies.[15]
The percentage of developing country households with a home computer grew from 15.6% in 2005 to 36.1% in 2019,[16] while mobile phone subscriptions per 100 people grew three-fold globally and four-fold in low-and middle-income countries between 2005 and 2020.[17] Moreover, in 2020, the number of registered mobile money accounts grew by 12.7 per cent globally to 1.21 billion accounts – double the forecasted growth rate.[18]

The increasing threat of security breaches

As developing country enterprises become increasingly reliant on information and technology assets, they face similar security threats to their counterparts in developed countries. For example, there have been multiple security incidents related to digital financial services, such as unauthorized third-party access to corporate information systems gained by luring unsuspecting employees to disclose user login information in Ghana, Kenya, Tanzania, Uganda and Zambia, an outage during a system upgrade in Zimbabwe, and a malicious denial-of-service attack in Kenya.[19] More broadly, one cybersecurity firm reported 24 million malicious software incidents in Africa in

2016,[20] and in the same year, Ghana's financial sector alone was reported to experience more than 400,000 incidents related to malicious software.[21] Traditional infrastructure assets in developing countries also are increasingly reliant on information and technology assets, such as for the monitoring and management of electricity grids.[22] Cyberattacks on such assets are increasing,[23] for example disrupting electricity supply in Ukraine in 2015 and 2016[24] and in South Africa in 2019.[25]

The economic cost of security breaches

The global direct monetary losses from cybercrime in 2020 were estimated to have nearly doubled to USD 945 billion from USD 522.5 billion in 2018,[26] while spending on cybersecurity in 2020 was expected to exceed USD 145 billion,[27] together comprising 1.3% of global GDP.[28] In 2017, cybercrime cost Africa an estimated USD 3.5 billion in direct losses.[29]

These estimates exclude indirect costs to victims such as opportunity cost, downtime, lost efficiency, brand disparagement, loss of trust, intellectual property infringement, and damage to employee morale. They also exclude systemic costs such as supply-chain impacts on upstream suppliers and downstream customers. The full economic cost of cybercrime, including direct, indirect, and upstream systemic costs, has been estimated at three times its direct cost[30] – putting 2020 total global cost near USD 4 trillion, about 4% of global GDP. This figure aligns with estimates that annual all-in global cybercrime costs will be USD 6 trillion in 2021.[31]

Developing country enterprises face outsized cybercrime losses, such as the USD 81 million Bangladesh Bank heist in 2016. This followed similar earlier incidents in Ecuador, India, Poland, Russia, Taiwan and Vietnam.[32]

Threats and motives

Threat actor motives

It has been estimated that 70% of security incidents in 2020 were financially motivated and organized crime was behind 80% of data breaches.[33] However, some threat actors, known as ***hacktivists***, are motivated by political, socio-cultural or religious ideology. In June 2011, hacktivists attacked MasterCard's website, causing it to crash, in protest of the blocking of payments to WikiLeaks.[34] Others are motivated by vanity, revenge, outrage, or other non-financial objectives.[35] State-sponsored threat actors may pursue geopolitical or military objectives through cyber espionage, interfering with foreign elections or sabotaging public services to undermine the political stability of adversaries.[36]

Threat actor methods

Threat actors often combine a series of actions to pursue their objectives. The first step is usually to infiltrate the target system by gaining unauthorized access to information or technology assets. Sometimes access is gained by using technologies to penetrate ***firewalls*** designed to prevent unauthorized access. One example is the March 2017 data breach of Equifax, the global credit reporting agency, exposing personal data of 147 million consumers. Equifax was initially hacked through a consumer complaint web portal. The hackers exploited a security vulnerability allowing them to obtain usernames and passwords to access further systems and pull data out of the network.[37]

Increasingly, threat actors gain access through ***social engineering***, convincing insiders to unwittingly enable intrusions. The most common form of social engineering is ***phishing*** attacks whereby a perpetrator is disguised as a trusted party (including ***spear phishing***, which is targeted and personalized to individual insiders).[38] One study found social engineering was employed to support infiltration in 92% of data breaches in 2020.[39]

In a ***distributed denial of service (DDoS) attack***, the threat actor obtains unauthorized access to third-party computers. The threat actor then commandeers the compromised systems, using them as ***zombies*** or ***bots***, to launch an attack on the targeted network resource. By releasing a flood of incoming messages or connection requests to the targeted system, the threat actor forces it to slow down or crash, denying service to legitimate users or systems.[40] DDoS attacks often have non-financial motivations.

Once gaining access, threat actors typically employ ***malware*** (malicious software used to extract information assets) and may withdraw funds or demand ransom payments (using malware known as ***ransomware***). The European Agency for Cybersecurity (ENISA) reported that malware was Europe's top cybersecurity threat from January 2019 through April 2020.[41] One study found that malware was employed to locate, access, and capture data in a majority of 2020 data breaches.[42] The same study found that denial of service hacking was involved in almost 60% of all security incidents.[43]

Public and private countermeasures to strengthen cybersecurity

Strengthening cybersecurity requires coordinated action by international institutions, governments, enterprises, civil society, and individuals.

International cooperation and coordination

The long reach and fast pace of the digital ecosystem transcends borders and enables bad actors to act anonymously and quickly, adversely impacting vast swaths of humanity.[44] International institutions are stepping in to facilitate cooperation on cybersecurity matters. The UN first addressed the topic in the World Summit on the Information Society (WSIS), held in Geneva in 2003 and Tunis in 2005.[45] These sought to increase Internet access in the developing world, develop a global culture of cybersecurity, and increase cooperation among countries on cybercrime.[46] At the 2003 Geneva summit, the International Telecommunication Union (ITU) was designated as facilitator for WSIS cybersecurity actions to build confidence and security in the use of Information and Communications Technologies.[47] The ITU has established a cybersecurity programme that offers developing countries capacity building support.[48] The UN Office of Counter-Terrorism has also established a cybersecurity programme.[49]

National government initiatives in cybersecurity

Digital technologies have disrupted legacy public safety frameworks, which are often not fit-for-purpose to protect against cyberattacks. Legal and policy reforms and implementing activities are required in every country to meet ever-growing cybersecurity challenges.

A national cybersecurity strategy

Facing these challenges, many governments have adopted a ***national cybersecurity strategy***, which is an action plan to improve security and resilience of national infrastructure and services. These strategies reflect high-level, top-down approaches to cybersecurity that establish national objectives, priorities, and timelines.

The first national cybersecurity strategy, the US Government's National Strategy to Secure Cyberspace, was released in February 2003 after the 11 September 2001 terrorist attacks on the World Trade Center.[50] Cybersecurity plans with more limited focus were adopted in Germany and Sweden in 2005 and 2006. The world's second broad national cybersecurity strategy was published by Estonia in 2008 following a severe cyberattack in 2007.[51]

The approach of adopting national strategies has now gained significant traction. The European Union Agency for Cybersecurity (ENISA) has recommended cybersecurity strategies for all EU member states since 2012[52] and maintains extensive resource materials on national cybersecurity strategies.[53] In 2018, the ITU co-published a Guide to Developing a National Cybersecurity Strategy with the World Bank and other institutions.[54] At least 114 countries have adopted or are in the process of adopting a national cybersecurity strategy, including 17 in sub-Saharan Africa, 18 in the Americas, 11 Arab states, 21 in the Asia-Pacific, 6 in the Commonwealth of Independent States, and 41 in Europe.[55]

A dedicated agency for cybersecurity

Many countries have established standalone national cybersecurity agencies to provide leadership. Such agencies can direct development of cybersecurity policy and coordinate implementation across all sectors. They may also serve as the official government voice and point of contact in case of cybersecurity incidents. Based on data for 198 economies, the World Bank recently found that standalone cybersecurity agencies had been established in 86% of high-income countries, 65% of upper-middle-income countries, 66% of lower-middle-income countries, and 24% of low-income countries.[56]

National, regional, and sectoral incident response teams

To prepare for security incidents, organizations have established ***computer security incident response teams (CSIRTs)***, also known as ***computer emergency response teams (CERTs)***.[57] To coordinate preventive measures and incident responses across the national territory, governments have established or designated ***national CSIRTs (nCSIRTs)*** with specified cybersecurity responsibilities.

Because it is external to its constituency, an nCSIRT typically has limited authority to access or implement security measures within the information and technology assets of its constituents. Its focus is on coordination of response, analysis of threats and incidents, and other forms of support.[58] The UN has recommended that member countries establish nCSIRTs and support and facilitate cooperation among nCSIRTs across borders.[59] The ITU has conducted nCSIRT assessments for 79 countries, helped 14 countries establish or enhance their nCSIRT, and confirmed that at least 118 countries had established nCSIRTs by March 2019.[60]

Some nCSIRTs have banded together regionally to enhance their efforts dealing with cross-border cyberattacks, such as the Asia Pacific Computer Emergency

Response Team (APCERT), which includes 33 nCSIRTs from 23 economies across the region.[61] Other similar organizations include AfricaCERT, with nCSIRTs and other members in 26 African countries,[62] and OIC-CERT, under the remit of the Organization of Islamic Cooperation, with nCSIRTs and other members in 30 countries.[63] ENISA supports cooperation among European CSIRTs.[64]

In some industries, ***sector CSIRTs*** enable public and private sector stakeholders to join forces to address risks, threats, and other challenges that are unique to a particular sector.[65] A key focus of sector CSIRTs is protecting ***critical infrastructure*** essential for society and the economy to function and protecting national security. A country's critical infrastructure may include information and technology assets used for energy, transportation, finance, banking, healthcare, food, water, other essential supply-chains, and critical government activities. The United States Department of Homeland Security (US DHS) has identified 16 sectors for critical infrastructure.[66] Under national laws, operators of critical infrastructure may be legally required to comply with enhanced security standards and procedures and establish incident recovery plans to mitigate harm and foster resiliency after a cybersecurity incident. These activities may be coordinated through a sector CSIRT. US DHS continues to monitor and update laws and regulations as it sees gaps in the existing legal framework. For example, when the Colonial Pipeline was hacked, US DHS issued two cybersecurity directives governing pipelines.[67]

Cooperation and coordination also occur among nCSIRTs, sector CSIRTs, and individual enterprise CSIRTs internationally through the Forum of Incident Response and Security Teams (FIRST). FIRST's current membership includes 585 CSIRTs in 98 countries.[68]

Updated criminal laws and law enforcement capabilities

Developing fit-for-purpose criminal laws and law enforcement capabilities is essential to cybersecurity efforts. Updated substantive criminal laws are needed when legacy criminal laws do not cover acts committed in the digital ecosystem.[69] Many governments have begun to analyse and update national laws to close gaps. Common offences that may be added are:

- unauthorized access to information or technology assets (hacking),
- unauthorized monitoring of communications,
- unauthorized interception or alteration of information assets,
- unauthorized interference with an information system, and
- misuse of devices and software.[70]

Cybercrime laws may also address more traditional crimes, such as fraud, forgery, and intellectual property infringement, when they occur in the digital ecosystem.[71] New restrictions on online content (such as child pornography) or online behaviour (such as cyber stalking or cyber bullying) have also been added.[72]

Law-enforcement agencies also need new criminal procedures, powers, and tools to investigate and prosecute cybercrime. These include computer forensics capabilities in investigations, procedures to preserve and seize electronic evidence, and mechanisms to promote cooperation of the private sector in threat identification and investigations.[73]

Law enforcement against cybercrime also faces jurisdictional challenges due to its inherently borderless nature.[74] Perpetrators can act quickly and from any location, using compromised third-party technology assets to mask their identity. For example, the 2017 WannaCry ransomware attack impacted 200,000 computers in 150 countries.[75] A harmonized approach to cybercrime legislation and enforcement can facilitate investigative and enforcement efforts across jurisdictions.

The Council of Europe's Convention on Cybercrime, which entered into force in 2004 and is known as the Budapest Convention, is the only binding international treaty on crimes committed via the Internet and other computer networks.[76] Its main objective is to pursue a common criminal policy against cybercrime by adopting appropriate legislation and fostering international cooperation. It addresses network security violations, computer-related fraud, copyright infringement, and child pornography. It also defines powers and procedures for officials to search computer networks and intercept communications. Originally conceived as a European treaty, the Budapest Convention has been joined by 45 of 47 Council of Europe member states and 22 non-members from Africa, the Americas, and the Asia-Pacific.[77] It remains open for other states to join.

The African Union adopted a Convention on Cyber Security and Personal Data Protection in June 2014. It will not enter into force until ratified or acceded to by 15 countries and has only been signed by 14 countries and ratified by 8.[78] Meanwhile, six African countries have joined the Budapest Convention. The Organization of American States (OAS) has not adopted a cybersecurity treaty. It addresses cybersecurity in the Americas through the Inter-American Committee against Terrorism (CICTE), a Cyber Security Program, and through technical assistance and training, policy roundtables, crisis management exercises, and exchange of best practices.[79] Ten OAS members have joined the Budapest Convention. The Association of Southeast Asian Nations (ASEAN) has also not adopted a cybersecurity treaty. In April 2018, the heads of state issued a statement on cybersecurity cooperation.[80] One ASEAN member, the Philippines, has joined the Budapest Convention.

By December 2016, some 132 countries were following the model of the Budapest Convention, including the 67 parties to the treaty.[81]

Private sector role in cybersecurity

Government efforts to improve cybersecurity require a robust and vibrant ecosystem to succeed. In the market-based systems of many national economies, significant responsibility for cybersecurity falls on public and private enterprises. Most have a strong self-interest — and contractual and legal duties — to adopt and implement reasonable security procedures and practices. Directors and officers have a duty to creditors and shareholders to preserve and protect business assets and to exercise due care in securing information and technology assets. Many enterprises now have a ***chief information security officer (CISO)***.[82]

Various national and international standards organizations have developed ***cyber risk management frameworks*** to guide enterprises in securing information and technology assets.[83] These frameworks prescribe processes for enterprises to identify their information and technology assets; identify threats and vulnerabilities to those assets; assess risk of loss (as a function of probability and impact); and prescribe security controls to reduce risk to an acceptable level. ***Security controls*** include management, operational, and technical measures to protect the confidentiality, availability, and integrity of information and technology assets. Under all the frameworks, risk management is iterative and evolving.

Individual enterprises are also increasingly establishing their own internal CSIRTs to provide services and support to the enterprise in assessing, managing, and preventing cyberattacks and coordinating incident responses. Such internal teams have a clear mandate and knowledge to perform hands-on incident management activities within an organization's information and technology assets.[84]

Education, support, and resources for cybersecurity

Humans are the weakest link in cybersecurity,[85] so public awareness and education are essential elements of effective cybersecurity. Public or private enterprises have good reasons to provide security awareness training to employees: to prevent security incidents, build a culture of security, strengthen technology defences, instil customer confidence, ensure compliance, be socially responsible, and improve employee wellbeing.[86] Yet, many enterprises continue to underinvest in training. A 2020 survey of 3,500 workers in Australia, France, Germany, Japan, Spain, the United Kingdom, and the United States found that many were still unaware of fundamental best practices.[87] Governments and enterprises also have good reasons to increase consumer awareness and education on cybersecurity. Private enterprises increasingly consider educating consumers as good business.[88]

Capacity building is also vital. A 2019 study found a global skills gap of 4 million fewer cybersecurity professionals than needed.[89] Developed countries are supporting training programs through public and private universities. For example, the US National Institute of Standards and Technology established an initiative to advance an integrated ecosystem of cybersecurity education, training, and workforce development.[90] Similarly, the Australian Government established and funded Academic Centres of Cyber Security Excellence at two universities to encourage students to study cybersecurity and increase the number of cybersecurity graduates.[91] ENISA is considering similar efforts.[92] Governments in developing countries often lack sufficient financial resources to support cybersecurity capacity development comprehensively. However, developing countries such as Mauritius and Egypt have demonstrated high levels of commitment towards building a robust cybersecurity framework as reflected in the Global Cybersecurity Index (GCI).[93] The ITU has also provided extensive technical support for CSIRTs, but the international community has so far not provided sufficient funding to train cybersecurity professionals in developing countries.[94]

Emerging issues

Work-from-home leads to new vulnerabilities

The COVID-19 pandemic and resulting lockdowns changed how many people perform basic life activities such as working, shopping, and attending school. The shift from working in an office to working remotely from home introduced and exposed cybersecurity vulnerabilities. Home computers often lack the security protocols found in the office. Firms that use third-party vendors to monitor and address cyber threats may find that these solutions do not extend seamlessly to remote work.

Cybercriminals have exploited these gaps. The US Federal Bureau of Investigation reported the number of cyberattack complaints in 2020 increased by 400% from pre-COVID rates, reaching as many as 4,000 per day. One cybersecurity vendor reported more attacks on corporate networks in the first half of 2020 than in all of 2019.[95] The use of ransomware increased significantly.[96] These new vulnerabilities will require enterprises and other organizations to adapt and to educate employees on how to avoid and minimize threats while working remotely.[97]

Blockchains and cryptocurrencies

A ***blockchain*** is a type of database that employs ***distributed ledger technology (DLT)***, a decentralized network infrastructure that enables simultaneous access, validation, and record updating in an immutable manner across multiple locations.[98] By eliminating the need for any one centralized authority, blockchain is potentially more resilient to tampering, fostering trust and making it a potentially useful and strong cybersecurity technology.

Cryptocurrency is a form of digital currency that relies on blockchain technology to track value and record transactions without any clearing authority. Cryptography enables transaction participants to remain anonymous. Cryptocurrency exchanges face potential regulation to prevent money laundering and other illegal activities and to ensure traders report profits and pay taxes to authorities. But so far, the law has not kept up and cryptocurrencies and transactions in those currencies are largely unregulated. They have become a preferred payment medium for cybercriminals. Industry experts believe this contributed to a 311% increase in ransomware payments from 2019 to 2020.[99]

Central bank digital currencies (CBDCs) are another type of digital currency that rely on DLT, but are issued by a nation's central bank, similar to the issuance of paper currency. Because of the security and reliability of the underlying DLT, CBDCs could reduce the cost and increase the efficiency of transactions, allowing immediate settlement of transactions that previously took days. Unlike cryptocurrencies, CBDCs are not meant to be anonymous, and the immutable record of transactions created by DLT raises potential privacy concerns. In October 2020, the Bahamas launched the world's first CBDC, known as the "Sand Dollar." One year after the launch, usage was still low but increased public education and awareness efforts were planned.

Additional resources

Cybersecurity Model Frameworks

- US Department of Homeland Security, Cybersecurity Strategy, 2018
- Australia Cyber Security Strategy 2020
- Budapest Convention on Cybercrime
- EU Cybersecurity Act

Resources for further reading

- Recommendation of the Council on Digital Security of Critical Activities, OECD, 2021
- Cybersecurity Policy Framework, A practical guide to the development of national cybersecurity policy, Microsoft, 2018
- Guide to Developing a National Cybersecurity Strategy, ITU, 2017
- Combatting Cybercrime, Tools and Capacity Building for Emerging Economies, World Bank, 2017

Organizations

- Information Society and Action against Crime Directorate of the Council of Europe
- Cybersecurity & Infrastructure Security Agency (CISA)
- ITU (Cybersecurity page)
- National Cybersecurity Alliance
- United States Department of Homeland Security (Cybersecurity page)
- European Union Agency for Cybersecurity (ENISA)
- Payment Card Industry Security Standards Council
- Cloud Security Alliance
- McAfee Resource Library
- Microsoft Cybersecurity
- Cybercrime Magazine

Notes

[1] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[2] Data security is the process of maintaining the confidentiality, integrity, and availability of an organization's data in a manner consistent with the organization's risk strategy. https://www.nccoe.nist.gov/data-security

[3] Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. https://csrc.nist.gov/glossary/term/cybersecurity

[4] See, e.g., Richard A. Caralli, James F. Stevens, Lisa R. Young & William R. Wilson, Software Engineering Institute, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Technical Report CMU/SEI-2007-TR-012, Appendix A, Step 2 at 34-35 (May 2007) [the OCTAVE Allegro Technical Report]. Available at https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf.

[5] See, e.g., OCTAVE Allegro Technical Report, supra, at 34-35.

[6] See, e.g., the OCTAVE Allegro Technical Report, supra, §2.4.2.2 at 12 & Appendix A, Step 2 at 34.

[7] The three information security elements of confidentiality, integrity and availability were first articulated in the proceedings of a March 1977 workshop of the US Institute for Computer Sciences and Technology. See Zella G. Ruthberg, ed., Institute for Computer Sciences and Technology, National Bureau of Standards, Computer Science & Technology: Audit and Evaluation of Computer Security, Proceedings of the NBS Invitational Workshop held at Miami Beach, Florida, March 22-24, 1977 at xxii (Oct 1977) (identifying "three vital audit components – access control, accuracy, and availability"). Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf. These three components are still considered the core objectives of information security. See, e.g., Center for Internet Security, "EI-ISAC Cybersecurity Spotlight – CIA Triad" (2021). Available at https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/.

[8] An individual or a group posing a threat. https://csrc.nist.gov/glossary/term/threat_actor

[9] The first known cyberattack occurred in November 1988, when graduate student Robert Morris released a malicious computer worm, known as the Morris Worm, from a computer at MIT he had hacked (accessed without authorization) from his terminal on the Cornell University computer system. The worm copied itself from computer to computer, depleting system resources. The incident occurred before introduction of the worldwide web – when the Internet was still dominated by military and academic users. Within 24 hours, 6,000 of the 60,000 computers on the Internet were disabled.

[10] See, e.g., Michelle Drolet, "The Evolving Threat Landscape: Five Trends to Expect In 2020 And Beyond," Forbes (14 Jan 2020). Available at https://www.forbes.com/sites/forbestechcouncil/2020/01/14/the-evolving-threat-landscape-five-trends-to-expect-in-2020-and-beyond/?sh=23d52320521d.

[11] The annual volume of data created, captured, copied and consumed globally grew over 3,000% from 2 zettabytes in 2010 to 64.2 zettabytes in 2020. Arne Holst, "Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025" (Statistica, 7 Jun 2021) Available at https://www.statista.com/statistics/871513/worldwide-data-created/.

[12] Equinix, the global leader in data centers, projects that by 2023 enterprises will reach 50% year-on-year growth rates in bandwidth required to interconnect with suppliers and customers. Equinix, Global Interconnection Index Volume 4 (2020). Available at https://www.equinix.com/gxi-report#forecast.

[13] The global market for enterprise synchronizing and sharing documents, photos, videos and files is expected to grow from USD 4.23 billion in 2019 to USD 16.99 billion in 2025. See ReportLinker, Enterprise File Synchronization and Sharing (EFSS) Market - Growth, Trends, Forecasts (2020 - 2025) (May 2020). Available at https://www.reportlinker.com/p05865744/Enterprise-File-Synchronization-and-Sharing-Market-EFSS-Growth-Trends-and-Forecast.html.

[14] By January 2021, Facebook had over 2.6 billion active monthly users, with 80% accessing their accounts exclusively from mobile devices. H. Tankovska, "Countries with the most Facebook users 2021," Statistica (9 Feb 2021). Available at https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/.

[15] By mid-2020, over 850 million mobile money accounts had been opened in 90 countries, and an average of USD 1.3 billion per day was being transacted through those accounts. Ceyla Pazarbasioglu & Alfonso Garcia Mora, "Expanding digital financial services can help developing economies cope with crisis now and boost growth later," World Bank Blogs (29 Apr 2020). Available at https://blogs.worldbank.org/voices/expanding-digital-financial-services-can-help-developing-economies-cope-crisis-now-and-boost-growth-later.

[16] Thomas Alsop, "Computer penetration rate among households in developing countries 2005-2019," Statistica (18 Feb 2021). Available at https://www.statista.com/statistics/748564/developing-countries-households-with-computer/.

[17] https://data.worldbank.org/indicator/IT.CEL.SETS.P2

[18] GSMA, State of the Industry Report on Mobile Money 2021 (2021). Available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money-2021_Full-report.pdf.

[19] Silvia Baur-Yazbeck, "Cyber Attacks Growing Problem in Developing Nations," Opinion, Inter Press Service News Agency (8 Oct 2018). Available at http://www.ipsnews.net/2018/10/cyber-attacks-growing-problem-developing-nations/

[20] Kshetri, Nir, "Cybercrime and Cybersecurity in Africa," Journal of Global Information Technology Management, Vol. 22, No2, 77-81 (2019). Available at https://doi.org/10.1080/1097198X.2019.1603527.

[21] Business Ghana, "Bank of Ghana launches Cyber Security Directive for Financial Institutions," (25 October 2018). Available at https://www.businessghana.com/site/news/business/175019/Bank-of-Ghana-launches-Cyber-Security-Directive-for-Financial-Institutions.

[22] Digitized supervisory control and data acquisition (SCADA) systems are used in all but the smallest developing countries to monitor and manage electricity grids. Varun Nangia, Samuel Oguah & Kwawu Gaba, "Managing the Grids of the Future in Developing Countries: Recent World Bank Support for SCADA/EMS and SCADA/DMS Systems," LiveWire (World Bank Group 2016). Available at https://openknowledge.worldbank.org/handle/10986/24717; and Tal Avrahami, "SCADA for Remote Utilities Monitoring: 4 Layers to Grasp," IIoT World (23 Mar 2017). Available at https://iiot-world.com/industrial-iot/connected-industry/scada-systems-for-remote-utilities-monitoring-the-four-layers-you-need-to-understand/.

[23] Protecting such information and technology assets is vital to safe and reliable power delivery. The World Energy Council found an increase from 87 attacks in 2014 to 150 in 2019, with 80% of energy sector enterprises unprepared to manage cyberattacks. Power Africa, "Cybersecurity for Transmission and Distribution in Africa" (20 Jul 2020). Available at https://powerafrica.medium.com/cybersecurity-for-transmission-and-distribution-in-africa-475676074534.

[24] Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks (Dec 2016). Available at https://www.technologyreview.com/2016/12/22/5969/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

[25] "Cyber attack shuts Johannesburg City authority's network," Reuters 25 Oct 2019). Available at https://www.reuters.com/article/us-safrica-crime/cyber-attack-shuts-johannesburg-city-authoritys-network-idUSKBN1X41RF.

[26] Direct costs globally in 2020 were up from USD 522.5 billion in 2018, USD 475 billion in 2014, and USD 300 billion in 2013. Zhanna Malekos Smith & Eugenia Lostri, McAfee and the Center for Strategic and International Studies & McAfee, The Hidden Costs of Cybercrime, Report (7 Dec 2020) [the "2020 McAfee Report"]. Available at https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

[27] See 2020 McAfee Report, supra.

[28] Global GDP in 2020 was estimated at USD 84.54 trillion. Aaron O'Neill, Statistica, Global gross domestic product (GDP) at current prices from 1985 to 2026 (1 Jun 2021). Available at https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/.

[29] "The cost of cyber-crime," The Economist (22 Jun 2018). Available at https://www.eiu.com/industry/article/1586874742/the-cost-of-cyber-crime/2018-06-22.

[30] Paul Dreyer et al., Estimating the Global Cost of Cyber Risk: Methodology and Examples at ix (2018). Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2299/RAND_RR2299.pdf.

[31] See Steve Morgan, "McAfee Vastly Underestimates the Cost of Cybercrime," Cybercrime Magazine (9 Dec 2020). Available at https://cybersecurityventures.com/mcafee-vastly-underestimates-the-cost-of-cybercrime/.

[32] The Bangladesh central bank held its currency reserves at the Federal Reserve Bank of New York. Despite warnings from the SWIFT interbank transfer system, the central bank had not segregated its SWIFT server from its computer network. In late 2015, intruders remotely broke into the bank's computer network and installed malware. On 4 February 2016, timed to coincide with bank closings, they issued 70 payment instructions to transfer USD 1 billion of the bank's funds to fake accounts in the Philippines and Sri Lanka. Human scrutiny blocked some payments, but USD 81 million was sent to fraudulent accounts and laundered through the Filipino casino system. Joshua Hammer, "The Billion-Dollar Bank Job," The New York Times (3 May 2018). Available at www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html.

[33] A 2021 investigation analysed 29,207 security incidents in 88 countries, including 5,258 data breaches, reported in 2020. Verizon, 2021 Data Breach Investigations Report at 6, 12 & 14 (2021) [the Verizon 2021 DBIR]. Available at https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.

[34] "WikiLeaks hacktivists take down MasterCard," Finextra (28 Jun 2011). Available at https://www.finextra.com/newsarticle/22713/wikileaks-hacktivists-take-down-mastercard.

[35] See, e.g., Lyndon Sutherland, "Know Your Enemy: Understanding the Motivation Behind Cyberattacks," SecurityIntelligence (31 Mar 2016). Available at https://securityintelligence.com/know-your-enemy-understanding-the-motivation-behind-cyberattacks/.

[36] The running list of significant cyber incidents since 2006 compiled by the Center for Strategic & International Studies reveals multiple cyberattacks believed to have been carried out by state-sponsored threat actors. Center for Strategic & International Studies, "Significant Cyber Incidents" (May 2021). Available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[37] Josh Fuhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?" CSO (12 Feb 2020). Available at https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

[38] Cheryl Conley, "Navigating the Phishy Social Engineering Ocean," SANS Institute Blog (27 Jun 2019). Available at https://www.sans.org/blog/navigating-the-phishy-social-engineering-ocean/.

[39] Verizon, 2021 Data Breach Investigations Report at 6, 12 & 14 (2021) [the Verizon 2021 DBIR]. Available at https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.

[40] See US Cybersecurity and Infrastructure Security Agency, Security Tip (ST04-015): Understanding Denial-of-Service Attacks (updated 20 Nov 2019). Available at https://us-cert.cisa.gov/ncas/tips/ST04-015.

[41] ENISA, From January 2019 to April 2020, The year in review: ENISA Threat Landscape at 11 (20 Oct 2020) [ENISA 2020 Review]. Available at https://www.enisa.europa.eu/publications/year-in-review.

[42] Verizon 2021 DBIR, supra, at 17.

[43] Verizon 2021 DBIR, supra, at 15.

[44] See, e.g., Chuck Brooks, “Alarming Cybersecurity Stats: What You Need to Know For 2021,” Forbes (2 Mar 2021). Available at https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=c0017958d3df.

[45] See, e.g., United Nations, Department of Economic and Social Affairs, Public Institutions, World Summit on Information Society (WSIS), Available at https://publicadministration.un.org/en/Themes/ICT-for-Development/World-Summit-on-Information-Society.

[46] A chief WSIS aim was to bridge the global digital divide by increasing Internet accessibility in the developing world. The Tunis agenda reaffirmed the need to develop a global culture of cybersecurity through national action and increased international cooperation. WSIS underscored the need for effective and efficient tools and actions, at national and international levels, to promote international cooperation on cybercrime. See World Summit on the Information Society, Tunis Agenda for the Information Society at §39 and §40., WSIS-05/TUNIS/DOC/6(Rev. 1)-E (18 Nov 2005). Available at https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[47] See Alexander Ntoko, Corporate Strategy Division, ITU, “Global Cybersecurity Agenda: a framework for international cooperation,” (Open-ended Intergovernmental Expert Group on Cybercrime, Vienna, 17-21 Jan 2011). Available at https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf

[48] See ITU, “Cybersecurity > Mandate” (2021). Available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/about-cybersecurity.aspx

[49] See United Nations, Office of Counter-Terrorism, “What we do > Cybersecurity” (2021). Available at https://www.un.org/counterterrorism/cybersecurity.

[50] See United States Government, The National Strategy to Secure Cyberspace (Feb 2003). Available at https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[51] See ENISA, National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace §2 (May 2012) [ENISA Cybersecurity Strategies Paper]. Available at https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.

[52] See ENISA Cybersecurity Strategies Paper, supra.

[53] See, e.g., ENISA, Good Practices in Innovation on Cybersecurity under the National Cyber Security Strategies (Nov 2019). Available at https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.

[54] See ITU, World Bank, Commonwealth Secretariat, Commonwealth Telecommunications Organisation, NATO Cooperative Cyber Defence Centre of Excellence, Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity (2018). Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

[55] ITU, National Cybersecurity Strategies Repository (2021). Available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

[56] World Bank Group, Data for Better Lives: World Development Report 2021 at 277 (2021). Available at https://www.worldbank.org/en/publication/wdr2021.

[57] During the Morris Worm incident of November 1988, response was isolated, uncoordinated, and slow in resolving the incident. Afterwards, the US Department of Defense established a computer emergency response team coordinating centre at Carnegie Mellon University Software Engineering Institute. Its mandate was to help other organizations establish CSIRTs. See, US Federal Bureau of Investigation, "The Morris Worm: 30 Years Since First Major Attack on the Internet," News (2 Nov 2018) (FBI Morris Worm Article]. Available at https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

[58] See Global Forum on Cyber Expertise, Global CSIRT Maturity Framework: Stimulating the development and maturity enhancement of national CSIRTs at 6 (Version 1.0, Jun 2019) [Global CSIRT Maturity Framework]. Available at https://thegfce.org/wp-content/uploads/2020/05/MaturityFrameworkfornationalCSIRTsv1.0_GFCE.pdf.

[59] United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report §17(c) & (d) (23 Jul 2015), adopted by the General Assembly in Resolution A/RES/70/237 (2015). Available at https://undocs.org/A/70/174.

[60] ITU, ITU-D Cybersecurity > National CIRT (2021). Available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

[61] APCERT was established in 2003 by nCSIRTs and other CSIRTs in 12 Asia-Pacific countries and now includes countries ranging from Tonga at the smaller end to India and China at the larger end. See Asia Pacific Computer Emergency Response Team, APCERT Annual Report 2020 (27 Apr 2021). Available at http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2020.pdf.

[62] See AfricaCERT, Membership (2021). Available at https://www.africacert.org/african-csirts/.

[63] See OIC-CERT, List of Members > All Members (2021). Available at https://www.oic-cert.org/en/allmembers.html#.YMy0K75KiUk.

[64] See ENISA, Topics > CSIRTs and communities (2021). Available at https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts.

[65] See Carnegie Mellon University Software Engineering Institute, The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities, Technical Report (Jun 2021). Available at https://resources.sei.cmu.edu/asset_files/TechnicalReport/2021_005_001_734796.pdf.

[66] US Cybersecurity & Infrastructure Security Agency, Critical Infrastructure Sectors. Federal election infrastructure is considered part of the Government Facilities Sector.

[67] https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/

[68] FIRST was formed as a non-profit organization in 1985 by a group of CSIRT stakeholders to foster cooperation and coordination in incident prevention, stimulate rapid reaction to incidents, and promote information sharing among members and the community at large. Forum of Incident Response and Security Teams, FIRST members around the world (2021). Available at https://www.first.org/members/map.

[69] See, e.g., ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response at 3 (Sep 2012). Available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

[70] See, generally, World Bank & United Nations, Combatting Cybercrime: Tools and Capacity Building for Emerging Economies at 78 (2017). Available at https://documents1.worldbank.org/curated/en/355401535144740611/pdf/129637-WP-PUBLIC-worldbank-combating-cybercrime-toolkit.pdf

[71] Id.

[72] Id.

[73] Id. at 95 & 109.

[74] Id. at 121.

[75] See Mike Azzara, All You Need to Know about WannaCry Ransomware, Mimecast Blog (5 May 2021). Available at https://www.mimecast.com/blog/all-you-need-to-know-about-wannacry-ransomware/.

[76] See Council of Europe, Details of Treaty No. 185, Convention on Cybercrime (entered into force 1 Jul 2004). Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[77] See Council of Europe, Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime (status at 15 Jun 2021). Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[78] See African Union, List of countries which have signed, ratified or acceded to the African Union Convention on Cyber Security and Personal Data Protection (status at 18 Jun 2020). Available at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

[79] See OAS, Cyber Security (2021). Available at https://www.oas.org/en/topics/cyber_security.asp.

[80] See ASEAN Leaders' Statement on Cybersecurity Cooperation, 32nd ASEA Summit (18 Apr 2018). Available at https://asean.org/storage/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf.

[81] Alexander Seger, Council of Europe, "Implementation of the Budapest Convention on Cybercrime" at slide 3 (Meeting of the Working Group on Cybercrime, OAS Meetings of the Ministers of Justice or Attorneys General of the Americas, Washington, DC, 12-13 Dec 2016). Available at https://www.oas.org/juridico/PDFs/cyb9_coe_cyb_oas_Dec16_v1.pdf.

[82] See, e.g., Nader Mehravari & Julia Allen, "Structuring the Chief Information Security Officer (CISO) Organization," Carnegie Mellon Software Engineering Institute Blog (22 Feb 2016). Available at https://insights.sei.cmu.edu/blog/structuring-chief-information-security-officer-ciso-organization/.

[83] See, e.g.: (1) ISO/IEC 27001 information security management system developed by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Available at https://www.iso.org/isoiec-27001-information-security.html. (2) "Factor analysis of information risk" (FAIR) cyber risk framework developed by the Open Group. Available at https://www.opengroup.org/forum/security/riskanalysis. (3) US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Available at https://www.nist.gov/cyberframework. (4) US Department of Defense Risk Management Framework (RMF). Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=qEE2HGN_HE4Blu7161t1TQ%3D%3D.

[84] See Global CSIRT Maturity Framework, supra.

[85] For example, human error has been attributed to 90% of 2019 cyber breaches in the UK. CybSafe, "Human error to blame for 9 in 10 UK cyber data breaches in 2019" (7 Feb 2020). Available at https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/.

[86] CybSafe, "7 reasons why security awareness training is important" (26 Jan 2021). Available at https://www.cybsafe.com/community/blog/7-reasons-why-security-awareness-training-is-important/.

[87] Proofpoint, 2020 User Risk Report: Exploring Vulnerability and Behavior in a People-Centric Threat Landscape at 6 (Apr 2020). Available at https://www.proofpoint.com/sites/default/files/2020-05/gtd-pfpt-us-tr-user-risk-report-2020_0.pdf.

[88] See, e.g., "Eight Ways Companies Can Educate Customers About Cybersecurity Threats," Forbes (30 Mar 2021). Available at https://www.forbes.com/sites/theyec/2021/03/30/eight-ways-companies-can-educate-customers-about-cybersecurity-threats/?sh=5898bc384077

[89] Estimating a workforce gap of over 500,000 in North America, 600,000 in Latin America, nearly 300,000 in Europe and 2.6 million in the Asia-Pacific region. No estimate was provided for Africa or the Middle East (ISC)2, Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)2 Cybersecurity Workforce Study, 2019 at 8 (2019). Available at https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.

[90] See NIST, National Initiative for Cybersecurity Education (2021). Available at https://www.nist.gov/itl/applied-cybersecurity/nice.

[91] See Australian Government, Department of Energy, Science, Energy and Resources, "What is the government doing in cyber security?" (2021). Available at https://www.industry.gov.au/data-and-publications/australias-tech-future/cyber-security/what-is-the-government-doing-in-cyber-security.

[92] See ENISA, Topics > Cybersecurity Education > European Cybersecurity Skills Framework (2021). Available at https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework.

[93] Global Cybersecurity Index (GCI) 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[94] See, e.g., Lilly Pijnenburg Muller, Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities at 12, NUPI Report No. 3 (2015). Available at https://cybilportal.org/wp-content/uploads/2020/06/NUPIReport03-15-Muller.pdf.

[95] R. Ackerman, "Companies need to enhance cybersecurity amid the continuation of COVID-19 in 2021," Security Magazine (7 Jan 2021).

[96] D. Nagel, "K–12 Has Become the Most Targeted Segment for Ransomware," The Journal (11 Dec 2020).

[97] See R. Ackerman, supra; U.S. Chamber of Commerce, Special Report on Cybersecure Working During COVID-19; M. Castelo, "How School Districts Should Respond to Ransomware Attacks," EdTech Magazine (30 Sep 2020).

[98] Frankenfield, Jake, Investopedia, "Distributed Ledger Technology (DLT)," (27 August 2021). Available at https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp.

[99] See, e.g., Chris Matthews, "Bitcoin extortion: How cryptocurrency has enabled a massive surge in ransomware attacks," MarketWatch (15 May 2021). Available at https://www.marketwatch.com/story/bitcoin-extortion-how-cryptocurrency-has-enabled-a-massive-surge-in-ransomware-attacks-11621022496.

About UNCDF

The UN Capital Development Fund makes public and private finance work for the poor in the world's 46 least developed countries (LDCs). UNCDF offers "last mile" finance models that unlock public and private resources, especially at the domestic level, to reduce poverty and support local economic development. UNCDF pursues innovative financing solutions through: (1) financial inclusion, which expands the opportunities for individuals, households, and small and medium-sized enterprises to participate in the local economy, while also providing differentiated products for women and men so they can climb out of poverty and manage their financial lives; (2) local development finance, which shows how fiscal decentralization, innovative municipal finance, and structured project finance can drive public and private funding that underpins local economic expansion, women's economic empowerment, climate adaptation, and sustainable development; and (3) a least developed countries investment platform that deploys a tailored set of financial instruments to a growing pipeline of impactful projects in the "missing middle."

The UNCDF Policy Accelerator works with governments to help them create policies and regulations that include everyone in the digital economy, shares practical tools and guides based on our technical assistance model and our go-to resources, and provides scholarships to policymakers and regulators to study with our world-class partner organisations.

About Macmillan Keck

Macmillan Keck Attorneys & Solicitors advises clients on strategy, advocacy, deals, controversies and reforms in the digital economy. The firm's clients include telecom operators, digital financial service providers, online health and education providers, other digital content, application and service providers, governments and sector and competition regulatory authorities, and international organisations. The firm has successfully completed numerous complex projects across a majority of countries in every continent.

Disclaimer

The views expressed in this publication are those of the author(s) and do not necessarily represent the views of UNCDF, the United Nations or any of its affiliated organizations or its Member States.

This publication was last reviewed in December 2021.

UN
CDF

Unlocking Public and Private
Finance for the Poor

policy.accelerator@uncdf.org

policyaccelerator.uncdf.org | uncdf.org

FIND US