WORLD ECONOMIC FORUM

State of the Connected World 2023 Edition

INSIGHT REPORT

JANUARY 2023

Contents

3 Preface

5 Executive summary

6 Introduction

7 1. Key priority areas

8 1.1 Ethics and integrity

14 1.2 Cybersecurity

20 1.3 Equal access

26 2. Other focus areas

27 2.1 Environmental sustainability

29 2.2 Financial and operational feasibility

31 2.3 Interoperability and system architecture

33 3. The pandemic effect

36 Conclusion

38 Appendices

39 Appendix A: Methodology

40 Appendix B: 2023 State of Connected World survey demographics

42 Contributors

45 Endnotes

Cover: @Rick Muigo/Unsplash

Preface

Shahid Ahmed
Group Executive Vice-President, New Ventures and Innovation, Nippon Telegraph and Telephone, Japan

Madeline Carr
Professor of Global Politics and Cybersecurity, Department of Computer Science, University College London, UK

Mariam Nouh
Vice-President, Economies of the Future, King Abdulaziz City for Science and Technology (KACST), Saudi Arabia

Jeff Merritt
Head of Urban Transformation, World Economic Forum LLC

The internet of things (IoT) and related technologies continue to transform people's lives, with use cases growing in such areas as healthcare, education, living and workspace, and more. The COVID-19 pandemic that spread around the world in early 2020 and continues to affect it today has underscored the important roles IoT and other technologies have in confronting the world's myriad challenges. For example, as governments put social distancing measures in place to curb the spread of the pandemic, businesses are using IoT tools to maintain continuity by digitizing processes and monitoring output.

Understanding the opportunities and potential risks of IoT and related technologies is critical to ensuring the maximization of their benefits, while recognizing and minimizing the risk associated with their use. This has many implications, particularly regarding questions about the ethical use of the technology, security and privacy, and equal access to the technology. To strengthen global governance and the innovation of IoT technologies for the benefit of society, the World Economic Forum Council on the Connected World, a global group of diverse executive leaders and subject-matter experts, was formed in 2019. It published the first edition of this report in 2020, the result of its effort to better understand how IoT is viewed worldwide and to establish clear priorities for action.

This edition builds on that work. It aims to help understand and prioritize key governance gaps in the development and expansion of IoT technologies. Through a survey and interviews of experts around the globe, we set out to capture the trends of governance gap perceptions since the last edition, revitalize stakeholder support and commitment to address the gaps, and reprioritize the actions and resources to address them.

The findings of this research highlight the importance of greater public-private collaboration and emphasize clear areas of alignment. These include a shared resolve to build transparency and trust in IoT technologies; a commitment to ensure that the public interest, privacy and security are protected; a responsibility to enable equal access for all; a desire to encourage the use of IoT to help solve humankind's biggest challenges; and a determination to bring people together to create a global consensus on these critical issues.

Executive summary

As the world begins to emerge from the COVID-19 pandemic, technological advances, such as the internet of things (IoT) and related technologies, have offered an exceptional opportunity to help build a more prosperous and sustainable future. The pandemic has emphasized the importance of IoT and related technologies in people's lives and work; from contact tracing to wearable devices, these technologies provide critical data to curb the spread of the virus, saving lives and allowing businesses and governments to continue operating. As dependence on connected devices and networks continues to grow, however, so do risks and governance challenges in areas such as security, privacy, sustainability, interoperability and equity.

The *State of the Connected World 2023 Edition* aims to examine the current state of governance gaps on IoT and related technologies, establishing a clear priority for action for businesses and government leaders to address risks and maximize benefits. The findings include:

1. The COVID-19 pandemic has changed the face of IoT and related technologies using new cases and applications, bolstering demand in areas such as health, manufacturing and consumer IoT.

2. The increase in innovation of IoT devices and related technologies presents plenty of benefits to society, governments and businesses, but the lack of confidence in areas including privacy and security may stifle progress.

3. Rapid advances of IoT technology have challenged the ability to regulate industries and implement industry standards. The survey conducted points towards ethical and responsible use as the area with the largest perceived governance gap.

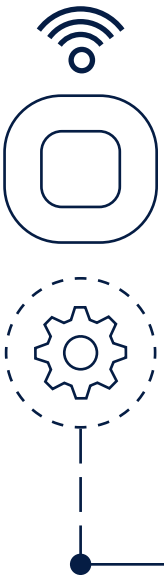
4. The pandemic shed light on user data vulnerabilities, leading users to prioritize privacy and security when using IoT devices and applications. In turn, governments and businesses have had to respond with regulations and updates to systems and devices to build justified user trust.

5. The second-largest perceived governance gap is in cybersecurity. Growing reliance on connected devices and related technologies have made organizations, governments and individual users increasingly susceptible to cyberthreats, making the ability of connected devices and related technologies to protect individuals from cyberattacks a leading concern.

6. The survey respondents indicated that equal access to technology and its benefits is another area that needs to be prioritized. Technological advances have shown potential to improve societal welfare through a plethora of applications in various fields. Barriers in infrastructure, economics, expertise and inclusivity, however, still hinder the ability of all members of society to fully benefit from these advances.

In response to the findings, in this report the World Economic Forum highlights the primary areas of opportunity for collective action from businesses and governments, especially those pertaining to ethics, security and accessibility. By establishing the principal areas of perceived governance gaps, the report urges businesses and governments to develop and implement better privacy and security practices to protect individuals, as well as to build their trust and develop practices that seek to create a more inclusive and accessible IoT and related technologies. These actions address systems challenges and require the commitment and efforts of the wide slate of stakeholders and experts in the public and private sectors, academia and civil society. Readers are invited to consider how their organization might contribute to the progress of one or more of these actions.

Introduction



The internet of things (IoT) and related connected technologies provide efficient and effective solutions for myriad daily challenges for individuals, businesses and governments. While estimates of the current number of connected devices around the world vary, every approximation puts it in the tens of billions and all projections show a dramatic increase over the coming years. Harnessing the power of these connected devices and related technologies is important to improving and optimizing how people live and work.

The network of physical objects connected to the internet that are embedded with sensors, software, thermostats, cameras, speakers and other related technologies have found various applications in day-to-day life, allowing for governments, businesses and individuals to digitize the physical world into harmonious connectivity. Cities have tackled infrastructure challenges through applications to detect maintenance needs for bridges and streets. Industries have adopted the use of smart devices to create business efficiencies by providing insights on supply management, logistics, human resources and production. Consumers have increasingly adopted the use of devices and technologies to make their lives easier and safer through the transformative power of wearables and other smart devices.

With the onset of the COVID-19 pandemic, individuals, businesses and governments found themselves increasingly dependent on IoT and related technologies to ensure connectivity and the continuity of activities. Users relied heavily on devices and applications that would enable them to work and study remotely; industries implemented technologies of automation and connectivity to ensure business continuity and resiliency; and governments developed policies and regulations to deliver services and necessary health measures to curb the spread of the virus through social distancing and contact tracing. The healthcare industry also underwent rapid acceleration in its IoT developments to promptly deliver solutions to novel challenges posed by the pandemic, deploying emergency approvals for devices and legislations to safeguard the public against the threats of the virus.

Nonetheless, rapid developments in IoT and related technologies have also introduced risks and raised concerns about their security, privacy, sustainability, interoperability and fair distribution of benefits.

The *State of the Connected World 2023 Edition* aims to examine the current state of governance gaps on the IoT and related technologies, establishing a clear priority for action for businesses and government leaders to focus their efforts on the upcoming year. It builds on the work of the inaugural 2020 report.

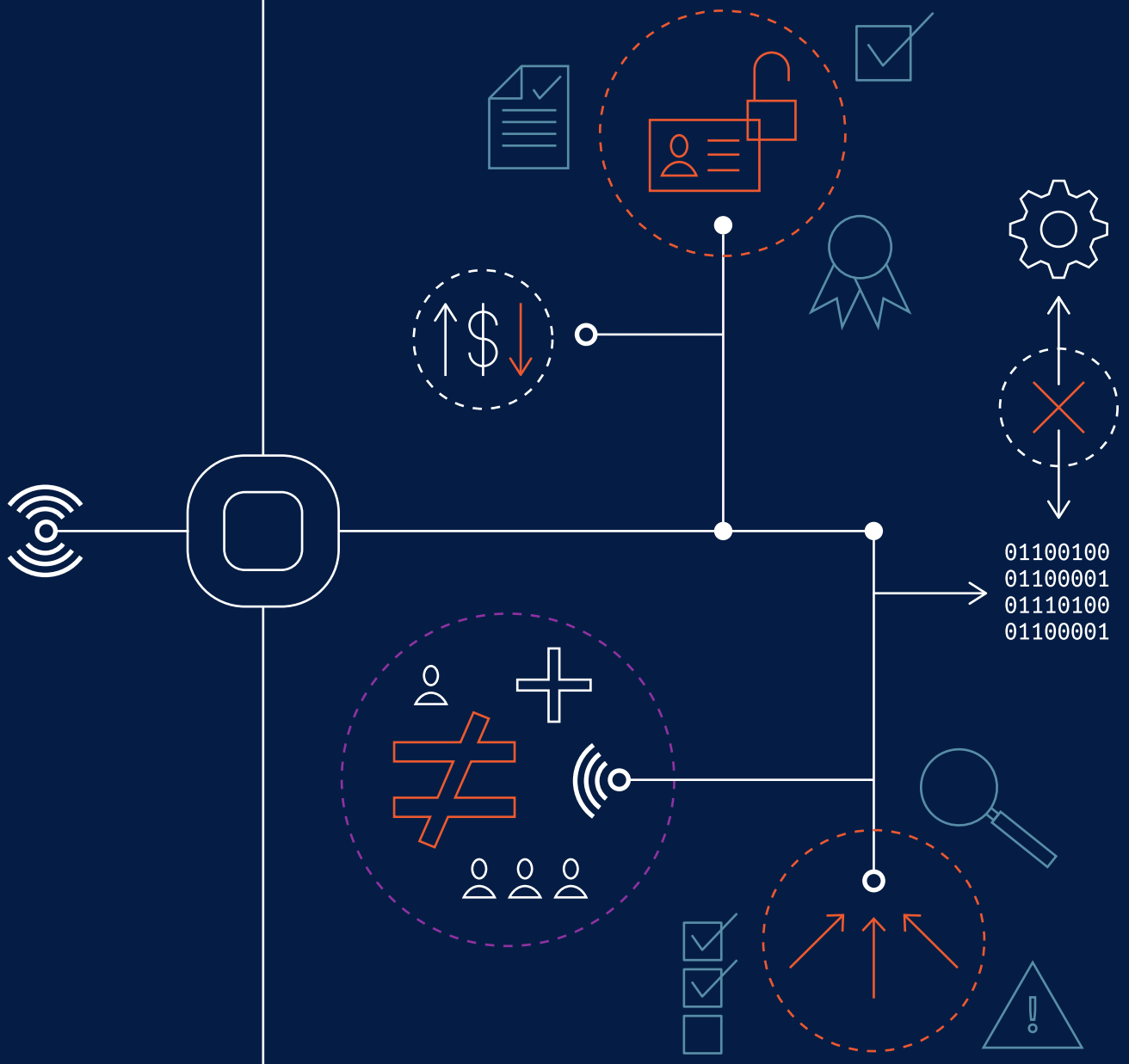
In this context, a governance gap is defined as "the difference between the potential risks posed by a technology and society's efforts to safeguard itself against these risks through laws, industry standards and self-governance approaches designed to achieve the greatest potential benefit of that technology for society as a whole".[1] The six areas evaluated are ethics and integrity, cybersecurity, equal access, environmental sustainability, financial and operational feasibility, and interoperability and system architecture.

To further understand the global priorities and challenges for IoT and related technologies, a survey of over 270 global IoT and connected device stakeholders was conducted, including interviews of more than 25 experts from the public, private and civil society sectors in 39 countries on six continents and in 19 industries. These provide key insights on their perceptions of risks and current governance levels of IoT and related technologies in the governance gaps.

Governance gaps in these six areas were evaluated by comparing data collected through the survey sent to experts, conducting interviews to discuss survey findings and perceptions in governance gaps, and doing desktop research of real-world data. Through this framework, the World Economic Forum seeks to provide action items for businesses, academia, government and civil society to work towards in closing the most pressing governance gaps and to deliver the promise of IoT and connected devices for an improved quality of life for as many people as possible.

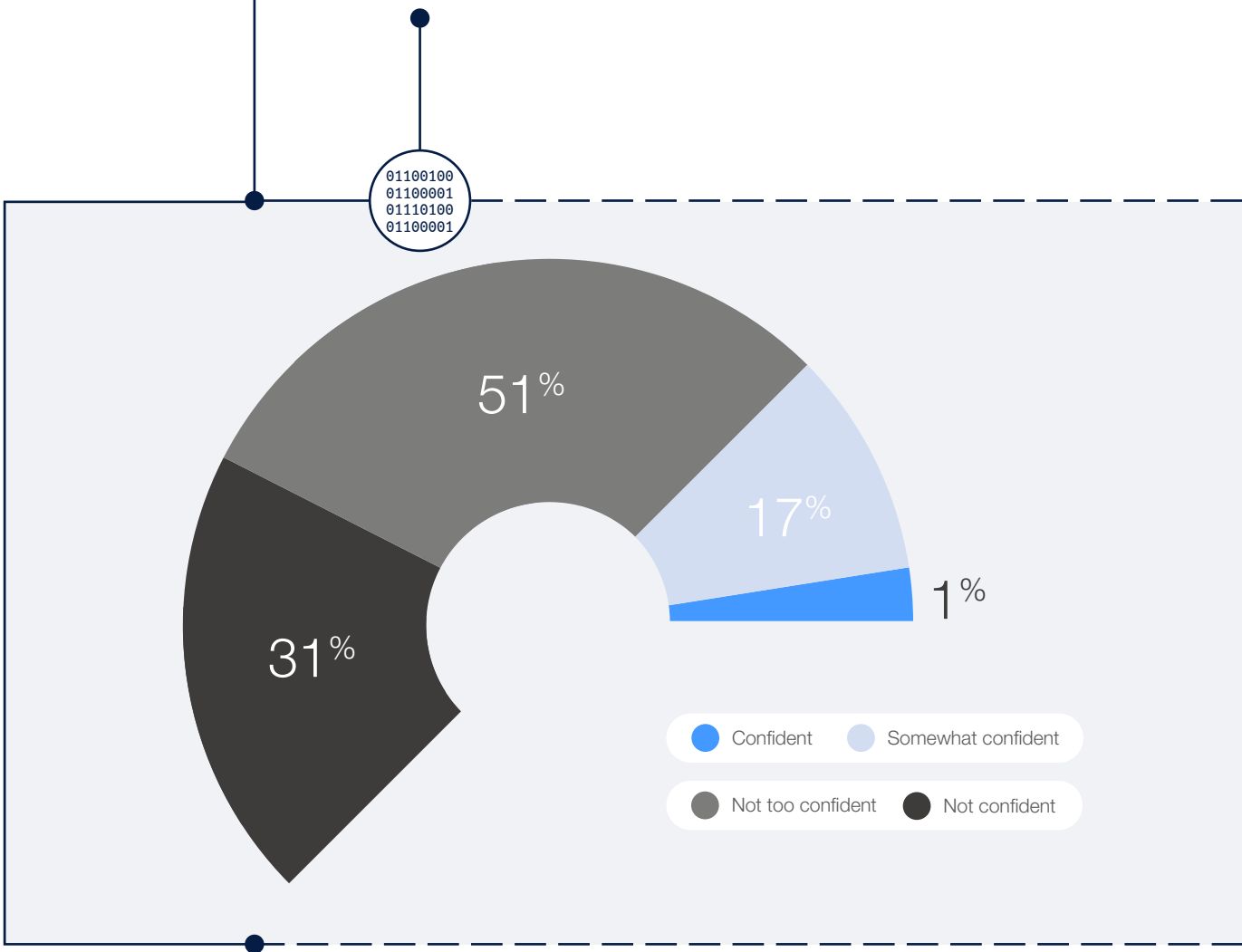
1

Key priority areas



1.1 Ethics and integrity

Figure 1: **Confidence that users of connected devices and related technologies are protected against the unethical and irresponsible use of the technology**



Source: World Economic Forum

- Respondents demonstrated a general lack of confidence in this area, with most reported being either not too confident (51%) or not confident (31%) that connected devices and related technologies are protected against unethical and irresponsible use.
- This is driven by the lack of information and data transparency, insufficient data privacy regulation, the need for more user education and awareness, and asymmetry of information between companies, users and regulators.
- Among proposed solutions to bridge the gap in ethics and responsible use of connected devices and related technologies include policy and regulation, design practices, guidelines and standards, digital literacy and empowerment of users, legal frameworks, and better transparency on users' data.

The ethical implications of IoT

In an increasingly interconnected world, privacy, security and trust issues about the use of IoT and related technologies are becoming significant concerns for individuals.[2] As digital technology continues to pervade all parts of life, the data generated presents both increasing opportunities and mounting challenges.

The survey results indicate that most respondents (82%) lacked confidence in the protection of privacy and the responsible use of data generated from connected devices. Addressing these concerns will allow maximizing the benefit of connected technology by including more people while minimizing its risks in terms of the threat to security, privacy and civil liberty.

Ethical and responsible use of personal information encompasses the ability of connected devices and related technologies to protect the privacy of users and generate trust that data collection is stored and used for the agreed purposes and with the consent from all parties involved.

The survey reveals a need to address this lack of trust and develop and implement legal frameworks based on ethical principles throughout the scope of IoT and related technologies. Users want more control over their privacy and their own data and how it is being used. The opacity and lack of legibility of the uses and applications of these technologies to non-expert audiences, however, is a barrier to governance and accountability.

Current policies and laws regarding online privacy and rights to access data are complex and have been proven a challenge to enforce. Users are increasingly demonstrating concern and distrust of organizations and institutions collecting and using their data without consent or using IoT and related technologies for surveillance.[3] Additionally, there is a general lack of awareness and education on users' rights and how to protect them.

Privacy and the unethical use of data

The lack of a robust framework surrounding ethics in IoT and related technologies has generated widespread distrust among users. People do not know whom companies share their data with, how to delete their data, what their rights are over their personal data or how much of their data is being held. A recent survey conducted by Consumers International and the Internet Society shows that 53% of consumers reported distrusting their connected devices to protect their privacy and handle their data in a responsible and ethical manner.[4] The implications of inadequate ethical standards in IoT and related technologies can be observed in issues that relate to informed consent, privacy, information security, physical safety and trust.

Existing privacy laws do not fully consider the individual's lack of understanding or awareness regarding the collection of their data. Collection of personal information can occur without consent and, even when there is consent, users may not be fully aware of the implications of their decisions.[5] While companies tend to provide an "informed consent" standard to verify and ensure that users are fully aware of the rules and limits of a software or platform, the current model does not effectively educate users of the implication of their choices.[6]

As a response to the abundance of data breaches and controversies regarding IoT and connected devices, governments have developed and implemented new laws to regulate how businesses and organizations access and manage users' data (Table 1). Some governments have faced challenges in enforcing such legislation due to difficulties in integrating requirements across systems, having vendors agree to compliance and adapting to regulatory or judicial clarifications, among many others.[7]

Table 1: **New laws to regulate the use of users' data by businesses and organizations**

Law/regulation	Country/region	Description
General Data Protection Regulation (GDPR)	European Union (EU) and European Economic Area	Considered by many as the precursor to standardizing data protection rules and renewing the debate regarding privacy regulations, the GDPR is considered to be the world's strongest set of data protection rules. It has set the foundation of legislation to enhance how people can access information about them while also establishing limits on what businesses and organizations can do with their personal data.[8] Since its implementation, over 400 million people have been covered and protected under the legal framework.[9]
General Data Protection Law (LGPD)	Brazil	Strongly influenced by the GDPR, Brazil enacted a federal law in 2020 to regulate the use of personal data. It includes a privacy law with "extraterritorial application", i.e. regardless of where organizations are owned or operated from, they must comply with the LGPD.[10]
Personal Data Protection Act (PDPA)	Singapore	Taking effect in 2014, the PDPA sets a baseline standard of protection for personal data in Singapore, integrating sector-specific legislative and regulatory frameworks. The regulation was updated in 2020 to incorporate a stronger consent framework and clearer rules regarding offshore data transfers, making it one of the most tightly regulated data protection acts in South-East Asia.[11]
California Consumer Privacy Act (CCPA)	California, USA	As of January 2020, the CCPA ensures that California residents are entitled to know what kind of personal data businesses collect about them and allows them to oppose the sale of their personal data to third parties. Unlike the GDPR, the CCPA concerns mostly the sale of data, not the collection and processing of data.[12]
Personal Information Protection Law (PIPL)	China	Adopted in August 2021, the PIPL is the first national-level law to comprehensively regulate matters of personal information (PI) protection. PI is defined as information that is recorded electronically or otherwise and is related to an identified or identifiable natural person within the People's Republic of China.[13]
Protection of Personal Information Act (POPIA)	South Africa	Passed in 2013 and put fully into effect in July 2020, POPIA serves as South Africa's federal legal framework to promote and ensure the protection of personal information processed by public and private entities. The conditions set out minimum requirements for the processing of identifying information, established a comprehensive definition of personal information to ensure end-user protection, and created the primary implementer and supervisor of the legislation, the Information Regulatory Authority (SAIR).[14]

Source: World Economic Forum

What can be done

1. Policy and regulation

To protect users from unethical and irresponsible use of the technology, basic ethical frameworks for IoT and related technologies must be designed and established. Governments and organizations are responsible for building trust, guaranteeing transparency and protecting the privacy of consumers. This could include defining roles of responsibility and accountability, what it means to be ethical in this environment, and how enterprises, governments and citizens can promote public interest in the realm of IoT.

"With the onset of so many emerging technologies, policy tends to lag. People tend to focus on the applications, but not on the policy issues or the ethical application of those technologies," says Farnam Jahanian, President of Carnegie Mellon University (USA).[15] To better address this delay, policies and regulations must contemplate and incorporate viable approaches that promote individual rights, data security and trust, including penalties for inappropriate behaviour, corruption and crime.

Governments and industries are responsible for developing and implementing regulations and policies for IoT and connected devices. While the GDPR set a precedent for other countries and regions to adopt robust policies to better regulate IoT and related technologies, many governments have yet to join the debate on user privacy and trust, and are behind in data protection. At the same time, self-regulation within industries is lacking.

Box 1: **Tech Policy Design Lab – A user-centric approach to policy-making**[16]

The Tech Policy Design Lab was created by the World Wide Web Foundation to shape and provide a space for companies, governments and civil society to work together to create product and policy solutions for a better and safer web. The Lab brings together these diverse stakeholders in a collaborative environment using design thinking to develop policy and legal frameworks, as well as services and products that address pressing tech policy issues. These include labels, features and standards.

2. Design practices, standards and guidelines

Implementing privacy by design rather than attempting to incorporate it as a response to users' concerns is not only a more efficient way to safeguard individuals from undesired access to data but is also essential to re-establishing trust that has deteriorated because of a lack of transparency. Best practices, standards and regulations need to consider privacy and ethics by design.

Box 2: **Butlr – An anonymous people-sensing technology platform**

In the artificial intelligence of things (AIoT), Butlr is a real-time behaviour and people-sensing analytics platform. Private by design, it uses body heat to detect rates of occupancy, headcount, body posture and activity to generate real-time and historical spatial insights. Without collecting personal data, Butlr assists in increasing quality of life without compromising privacy.[17]

The technology developed by Butlr has been deployed in senior living settings for frailty and fall detection, workplace planning and asset strategy, employee and tenant experience, facility management, and building operations.

3. Digital literacy and empowerment on the part of users

Most people claim to have little or no understanding of what companies do with their data.[18] Educating individuals on their rights will allow them to make more informed decisions and build trust. Digital literacy education initiatives that better inform users are simple yet effective ways to bridge the current lack of awareness on the user end as to how their data is being used and how to better protect themselves.

Box 3: **Privacy Center – A hub for educating users on data collection and privacy options**

The Meta Privacy Center provides information to US users on their approach to privacy across their apps and technologies, specifically about the privacy topics of sharing, security, data collection, data use and ads. The new feature hopes to serve as a one-stop shop for users to navigate the privacy and security controls across Meta's multiple platforms, including WhatsApp, Instagram and Facebook.[19]

4. Better transparency on the use of users' data

In a study conducted by KPMG, 75% of consumers responded to wanting more transparency on how their data is used and 40% said they would feel more comfortable in sharing their data if they were informed on who would use their personal data and how.[20] Providing such clarity to users can help in building trust as they engage with connected devices. This should be done in a thorough, well-organized and clear manner, where individuals are told who will use their data and how it will be used, and should further clarify the connection between the business use case and the benefit conferred to society.

Box 4: **Smart city technologies and IoT – The tools for unlocking the shared value of smart city data**

When deployed safely and effectively, smart city technologies and IoT could potentially transform urban life, improving businesses and the lives of residents and visitors through everything from safety and public health to waste management and traffic.

To address this potential, the World Economic Forum proposed a framework and best practices to enable the exchange of data from IoT and related technologies that, in turn, helps build trust between providers, operators and end users by protecting the rights and interests of the parties involved.[21] The model framework is composed of data privacy, data security, interoperability, accountability and integrity data, eligibility of platform operators, and a terms of use agreement for data users, providers and operators. Detailed instructions are provided for stakeholders, as are direction and the actions required to implement protocols in local policy and regulations (city regulators and administration, platforms, data providers and users, and third-party or industry associations).

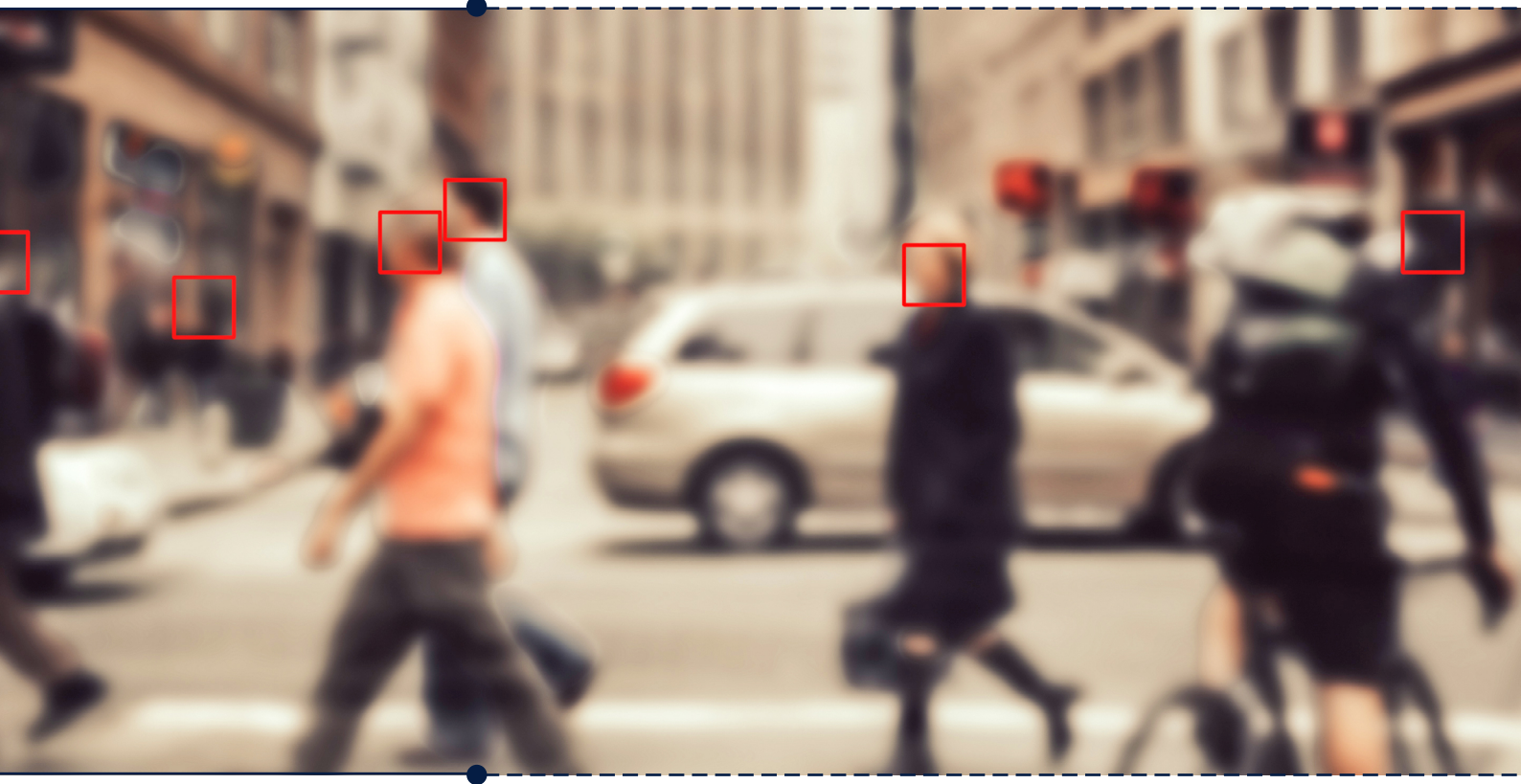
5. Safeguards against potential biases

Care should be taken to ensure that the algorithms developed and running in IoT devices and related technologies are not propagating human biases into digital technology. For example, AI algorithms for facial recognition trained primarily on people with a specific complexion have had difficulty recognizing people with a different complexion, potentially leading to misidentifying people of certain ethnicities and leading to harmful outcomes depending on how these algorithms are used.[22] Developing best practices to minimize unconscious or conscious human biases in the development of IoT technology should be required for deployment for public use.

Box 5: **Governance framework – An initiative for responsible limits on facial recognition**

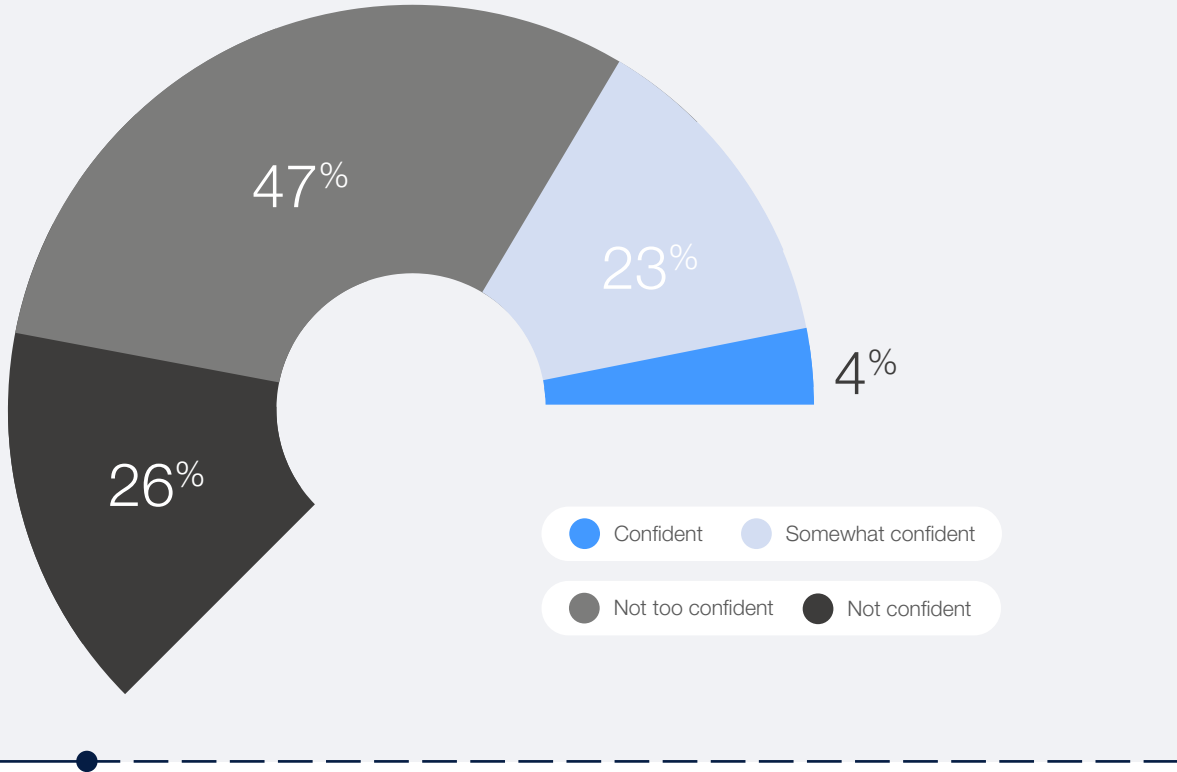
In partnership with the International Criminal Police Organization (INTERPOL), the United Nations Interregional Crime and Justice Research Institute and the Netherlands police, the World Economic Forum published a governance framework for the responsible use of facial recognition in law enforcement investigations.[23] The initiative addresses the need for concrete guidelines to ensure ethical and responsible use of adopting facial recognition technology (FRT).

This work draws on the initial policy framework vision of 2021, providing new insights by highlighting principles that define what constitutes the responsible use of facial recognition in law enforcement investigations, as well as a self-assessment questionnaire used to support law enforcement agencies in complying with the principles for action within the responsible use of FRT.



1.2 Cybersecurity

Figure 2: **Confidence that users of connected devices and related technologies are protected against cyberattacks**



Source: World Economic Forum

- Respondents demonstrated a general lack of confidence in this area, with most reported being either not too confident (47%) or not confident (26%) that connected devices are secured and users are protected against cybercrimes and attacks.
- Experts from the digital/information technology (IT) and electronics sectors were especially concerned about protection against cyberattacks, with nearly half (47%) being not too confident and 27% being not confident.
- This is driven by underdeveloped regulatory frameworks, rapid expansion of markets and companies in IoT and related technologies, technical limitations, lack of knowledge of end users, insufficient incentives for companies to protect users and lack of standardization.
- Nonetheless, the advancements in cybersecurity technologies and maturity levels of digital infrastructure provide optimism for positive development in this area.

– **Among proposed and potential solutions to address challenges in cybersecurity are consumer education through digital literacy campaigns, increased standardization practices of IoT and related technologies, cybersecurity measures, prioritizing security by design and default, and development of agile policies and regulations to better address the quickly changing landscape of cybersecurity.**

Security and IoT

The growing reliance on connected devices and related technologies have made organizations, governments and individual users increasingly susceptible to cyberthreats. The first half of 2021 recorded 1.5 billion IoT-targeted attacks globally,[24] while data breaches increased by 15.1% from the previous year.[25]

These attacks can generate sizeable consequences for individuals and businesses. For example, the financial impact of ransomware attacks is forecast to cost the world $7 trillion in 2022, making cybercrime the world's third-largest economy after China and the United States.[26]

Vulnerabilities and attacks

The uptake[27] of wearable devices, smart homes, sensors, thermostats and other applications of IoT and related technologies for individuals, businesses and governments has provided a host of vulnerabilities that can compromise the entire connected system. An attack on one element of an IoT ecosystem is often aimed at compromising the larger system, such as attacks on cameras, which can communicate with smart assistants and unlock connected doors. It is important to recognize the potential risks that IoT and its many applications pose and how manufacturers and providers can better prepare these devices and services for their users to safeguard themselves.

Users' awareness continues to be a challenge. The prevalence of poor security practices and knowledge, such as weak passwords or an inability to identify phishing emails, has contributed to weaker security systems. Furthermore, technical limitations, such as the lack of basic security measures including basic encryption in default configurations, make systems and devices more prone to malicious attacks. A general lack of transparency in the market is another predominant risk factor as nowadays individuals know little, even about the basic characteristics of the devices and their potential vulnerabilities.[28]

Current cybersecurity regulations lack standardization and are fragmented around the world. This often means organizations must develop and adhere to different requirements for each state, country or region where they may do business. Consequently, this also means that enforcing and holding organizations accountable for implementing best practices and following guidelines becomes challenging given that no clear standards exist.

Security considerations tend to be included late in the design and prototyping phase, leading to unsecured devices and allowing malicious actors to breach systems and connected devices. The notion that security measures can be "add-ons" has strongly contributed to the reactive nature of cybersecurity in the realm of IoT and connected devices.

Finally, the ever-changing nature of IoT and its many applications means that malicious actors are always finding new ways to attack systems and devices. A device that is secure today may not be tomorrow. Connected devices are increasingly connected to intellectual property with some form of exposure to the internet and are expected to be operating past the typical life cycle of most electronics. Devices are increasingly exposed to malicious attacks when hardware is no longer compatible with the necessary software to ensure protection.

Cybersecurity implications of IoT

Financial losses
Cyberattacks can lead to serious and costly consequences for organizations, governments and individual users. Global cybercrime is expected to grow 15% per year over the next five years, reaching $10.5 trillion by 2025.[29]

Physical harm
Cybercriminals are increasingly attacking critical infrastructures, targeting petrol stations, such as through the hack of the Colonial Pipeline system in the United States which emptied stations and caused panic buying; hitting schools in the United Kingdom and New Zealand; and locking dozens of hospitals in Europe and the United States out of life-critical systems.[30]

Reputational damage
When a business suffers a data breach that exposes its clients' personal data, including bank account information, social security and credit card numbers, it loses not only the information but also clients' trust. This could significantly affect its business. According to a *Forbes* Insights report, 46% of organizations suffered reputational damage from a data breach and 19% suffered both reputational and brand damage due to third-party security breaches. This leads to distrust and scepticism and, consequently, to a loss of business.[31]

Loss of productivity
Cyberattacks can disrupt operations and result in financial loses and productivity. Once the attack is carried out, IT staff will be required to perform a clean-up, identify the root cause, fix vulnerabilities and reinforce security measures. Throughout this process, productivity is put to a halt. Depending on the attack, this can mean a disruption or complete shutdown of processes.

The alarming rise of cyberattacks and its many implications have spurred governments and organizations around the world to address the vulnerabilities of IoT and connected devices by increasing regulatory action, growing collaboration on cybersecurity through alliances and beginning a consensus on minimum security provisions (Table 2).

Table 2: **Examples of regulatory action on cybersecurity**

Policy/ regulation/ programme	Country/region/ organization	Description
Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)	USA	Enacted in March 2022, CIRCIA institutes important new reporting obligations for companies that provide critical infrastructure. The federal law requires entities of critical infrastructure, such as electricity, water and transportation, to report certain cybersecurity breaches and ransom payments within a determined number of hours.[32]
Cyber Resilience Act (CRA)	EU	The proposal introduces mandatory cybersecurity requirements for manufacturers and retailers of devices, extending protection throughout the product life cycle. The CRA is part of a bundle of regulations in digital security that will be reviewed in the EU, ensuring the following: standardization of rules when companies develop devices or software with digital components; a framework of cybersecurity requirements for planning, design, development and maintenance of products; and a commitment to provide responsibility of care for the entire product life cycle.[33]
Cybersecurity Labelling Scheme (CLS)	Singapore	The first of its kind in the Asia-Pacific region, CLS was launched for consumer smart devices as part of ongoing efforts to improve IoT security and make Singapore's cyberspace safer. Under conditions imposed by the scheme, smart devices are rated according to their levels of cybersecurity provisions, which provides transparency for individuals to make educated decisions when opting for products with better cybersecurity.[34]
ISO 27001 and ISO 27002	International Organization for Standardization	These are considered to be the international standards to validate cybersecurity programmes. Organizations with ISO certification are viewed as responsibly managing cyber-risks and to have mature cybersecurity practices in place.[35]
Cyber Aware Campaign	UK	The policy, administered by the National Cyber Security Centre (NCSC), is aimed at helping to defend UK users from cyberattacks by providing the public with tools to protect their email accounts.[36]
Cybersecurity Hub	South Africa	With its mandate from the National Cybersecurity Policy Framework (NCPF), the Cybersecurity Hub acts as South Africa's national Computer Security Incident Response Team (CSIRT). Its goal is to ensure that citizens and businesses can access and navigate a safe cyberspace to communicate, socialize and execute transactions. This is achieved through a multistakeholder effort from the public and private sectors, civil society and the public, to identify and ward off cybersecurity threats through response activities and enabling technology and information sharing.[37]

Source: World Economic Forum

Box 6: **Arm Morello – A research and prototyping programme to ensure a more secured hardware architecture for future Arm technologies**

Through innovative central processing unit design architectures, Morello is a research initiative that aims to update the security foundations of existing computing infrastructure by strengthening processors and to deter certain key security breaches. In partnership with the UK government's Industrial Strategy Challenge Fund (ISCF) Digital Security by Design programme, Arm is developing the Morello board, a prototype system-on-chip and development board, which aims to serve as a test platform for placing safer hardware architecture within Arm processors.[38]

Box 7: **Multistakeholder coalition – A way to build global consensus on five security must-haves**

Through the World Economic Forum Council on the Connected World, leaders from over 400 organizations globally, including Consumers International, the Cybersecurity Tech Accord and I am the Cavalry, worked together to establish a consensus on baseline cybersecurity provisions for consumer IoT devices.[39]

Leaders representing the interests of technology providers, individuals and security researchers decided on five security essentials as baseline requirements for consumer-facing IoT devices: not having universal default passwords, having software updates, having secure communication, ensuring that personal data is secure and implementing a vulnerability disclosure policy.[40]

These efforts resulted in a Statement of Support that calls on device manufacturers and vendors to take immediate action. It has been endorsed by more than 100 organizations from stakeholder groups, including leading technology companies, industry organizations, civil society groups and government cybersecurity agencies.

What can be done

With the rise of cybersecurity risks, persistent governance gaps in standardized security and safety measures, as well as the fragmented policies and regulation surrounding cybersecurity, must be urgently addressed.

1. User awareness and education

More than half of all ransomware attacks are successful because of the lack of user education and best practices.[41] To mitigate the risks of cyberattacks on users, users must be provided with the necessary education and training to ward off bad practices and avoid mistakes that may cause serious losses. Public campaigns can educate individuals and operators regarding risks, and device makers can provide training and warnings. Adoption of best practices, such as two-factor authentication for all devices, higher frequency of password cycling, and better-quality passwords and alternatives to passwords, such as biometrics or security keys, can help protect digital infrastructure against malicious attacks.

Box 8: **Cybersecurity labelling – An initiative to educate consumers on and protect them from cybersecurity risks**

In May 2021, the US government issued an Executive Order to improve the country's cybersecurity.[42] The order required the National Institute of Standards and Technology to develop a labelling programme on cybersecurity capabilities of IoT consumer devices as well as software development practices. The initiative is part of government efforts to further educate society on how to provide better protection from the risks of cybersecurity in IoT devices and related technologies and to make more informed decisions when navigating these networks.

2. A unified IoT and related technologies

Greater alignment of public- and private-sector efforts is required to minimize the fragmentation of current policies and programmes and to increase the incentive of businesses to adhere to guidelines. It is critical for governments and industries to create common shared standards in their cybersecurity practices.

One example is the new California Security of Connected Devices Law,[43] which sets the standard that all connected devices within the state must include security measures for authentication. It is necessary to ensure that all technology providers adhere to key minimum standards.

3. Incorporation of security by design and by default, not by response

Many organizations still approach their cybersecurity reactively, with the bulk of efforts targeted at managing existing damage. Organizations and governments should focus on building a robust cybersecurity infrastructure from the design phase of a product. Security by design approaches device and software development in a way that seeks to make systems as free of vulnerabilities and resistant to cyberattacks as possible. Many market players use weak default options to lower the entry barrier for customers, who might feel confused or intimidated by strong security details. Importantly, these defaults must be strengthened to further ensure that users are being protected from vulnerabilities within devices and systems.

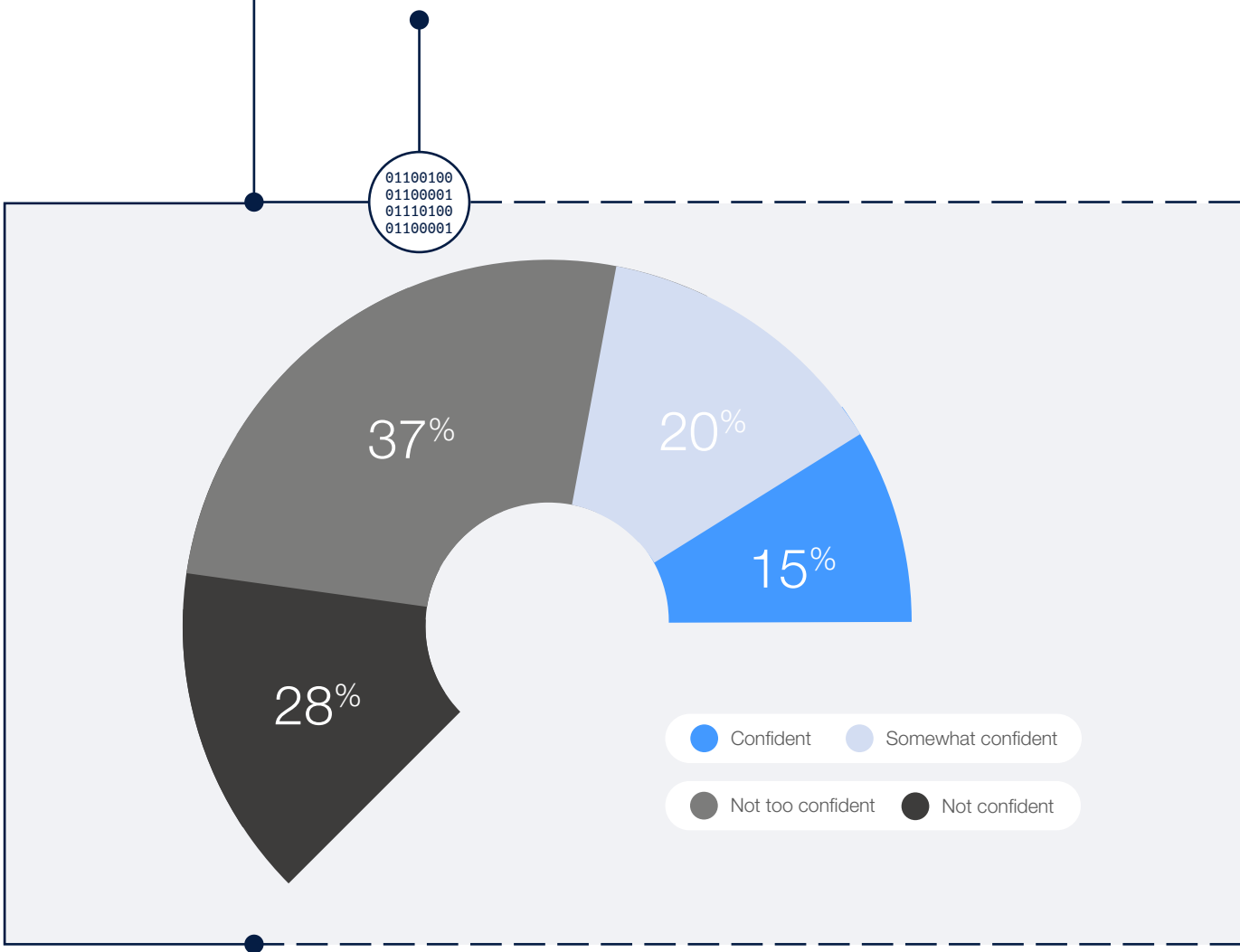
4. Policy and regulation

For governments, organizations and users to better protect themselves from potential cyberattacks, robust policies and regulations must be in place to improve the security of connected devices. These policies further contribute to setting important guidelines, standards of behaviour and best practices to safeguard the IoT and connected devices. Current policies are fragmented by region and at times can stifle innovation.

Governments should work towards proactively and continuously engaging in policy development, aiming for regulatory balance. Furthermore, policy-makers must be adaptive and work alongside experts in the field who develop these innovations. For example, the EU Data Protection Regulation provides guidelines to promote the market while safeguarding an equilibrium between under-regulating and over-regulating.[44]

1.3 Equal access

Figure 3: **User confidence that connected devices and related technologies are accessible and beneficial for all members of society, irrespective of geography, socio-economic status or other factors**



Source: World Economic Forum

- 65% of respondents reported lack of confidence in connected devices and related technologies being accessible and beneficial to all members of society irrespective of geography, socio-economic status or other factors.
- Nonetheless, many respondents were optimistic of the ability of IoT and related technologies to be more accessible, with 45% respondents reporting an increase in confidence in the last three years.
- Most respondents cited the inherent inequality in economic conditions, availability of infrastructure, awareness and digital literacy to be the main drivers of their lack of confidence in the optimal access to connected devices and their benefits.
- Meanwhile, optimism in this area is fuelled by connected devices' scalability and downward trend in prices, which makes them increasingly more accessible to a wider audience.

Ensuring an accessible IoT

One of the promises of technological advance is its potential to improve societal welfare. Connected devices and related technologies have a plethora of applications in various fields – including healthcare, industry, education and commerce – which, if properly harnessed, will result in a net benefit to society. Nevertheless, several barriers, including infrastructure, economics, expertise and inclusivity, are impeding the ability of all members of society, irrespective of geography, socio-economic status, ability and technical ability, from accessing the technologies and benefiting from them.

This was evidenced when connected devices and related technologies became important tools to adapt to the measures imposed to curb the spread of COVID-19. For example, the pandemic revealed the divide between large companies and their smaller counterparts. In a survey across 32 countries, the Organisation for Economic Co-operation and Development (OECD) estimated that 70-80% of small and medium-sized enterprises experienced a drop in revenue of 30-50%.[45] The study found that larger companies are more resilient, partly due to their ability to accelerate digitization and adopt technology better.

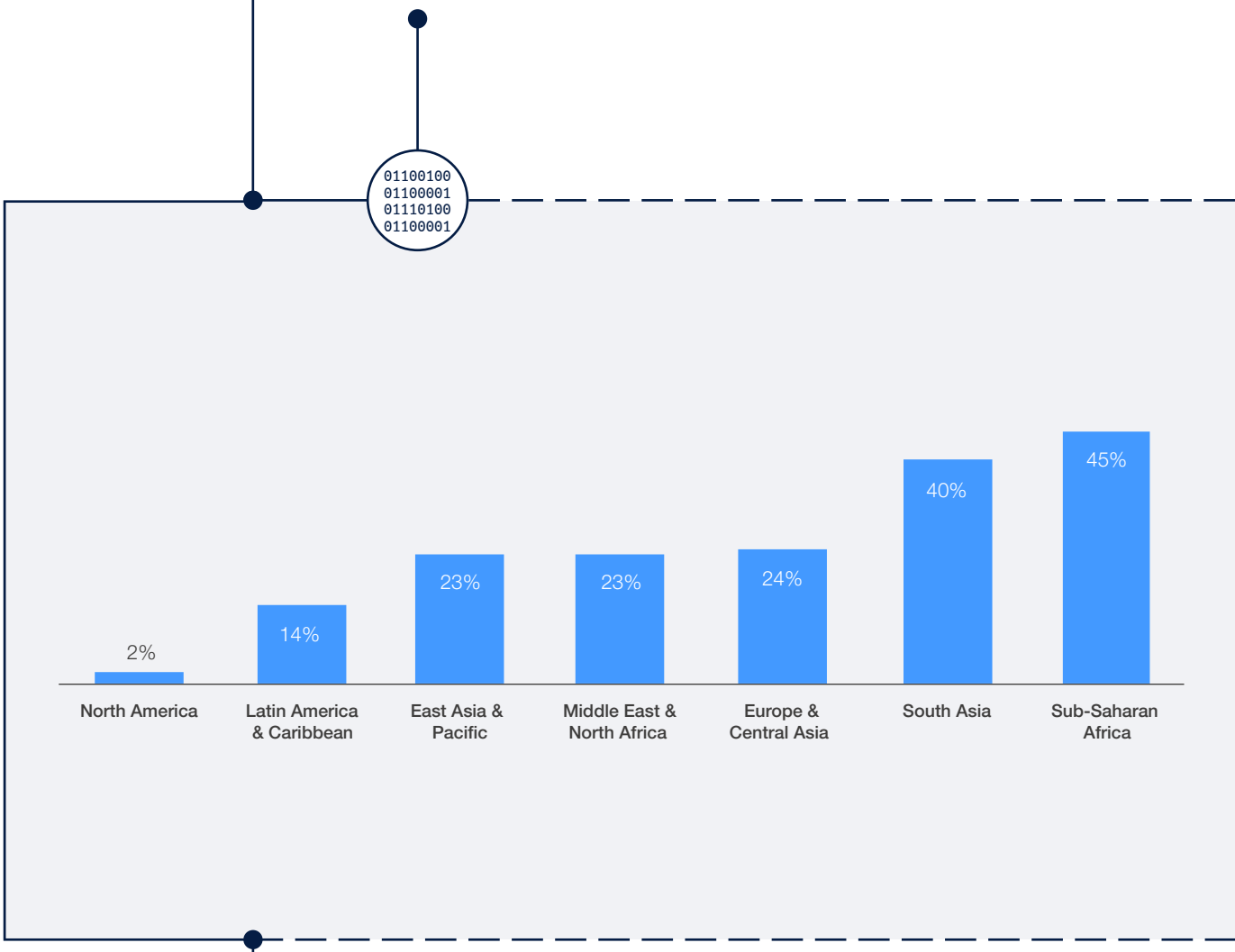
In education, studies show a stark contrast between low-income countries and high-income countries, with only 25% of the former providing any type of remote learning compared to 90% among high-income countries.[46] It will take years to fully understand how this will affect human capital development and the economy in low-income countries.

As technology continues to rapidly evolve and pervade more aspects of people's lives, the ability to widen access to the technology and, consequently, its benefit to marginalized groups, will have a lasting impact on economic equality, educational attainment, access to healthcare and more.

Economic factors, infrastructure and other structural issues affecting access

The economic barrier is one of the main reasons driving the lack of confidence among respondents regarding the inclusiveness of connected technology. Economic disparity between different countries, as well as diverse groups within a country, still determines the level of access to connected technology and countries' ability to benefit from it. In some consumer spaces, the cost of connected devices, such as mobile phones, wearable devices (e.g. health trackers and smartwatches) and smart home products, are still prohibitively high (Figure 4).[47]

Figure 4: **Average cost of a smartphone, as a percentage of average monthly income**



Source: Alliance for Affordable Internet (A4AI), "Device Pricing 2021", 7 October 2021 (accessed 10 November 2022).

Box 9: **Voice assistant market – Competitive practices**

As a subset of IoT and related technologies ecosystems, the voice assistant market is developing quickly as new technology becomes available. Along with it, competition becomes a concern where leading global platform operators may engage in practices that lead to significant obstacles for any new entrants that attempt to enter the market and compete with them. Leading providers in this field have the advantage of benefiting from advanced technologies and financial resources to maximize scope and scale.[48] These advantages can be used to impede or slow competition by imposing exclusivity, self-preferencing their own products and services or limiting technical interoperability.

To address these obstacles, the voice assistant market would benefit from governance-related initiatives in respect of disintermediation risks, as to how leading voice assistance providers control the user relationship and user experience, access to consumer IoT services and related data, technical performance and related processes.

For enterprises, while the average cost of IoT sensors has fallen over the years, it represents only about 30% of the cost of an IoT solution. The implementation of IoT and related technologies involves myriad other costs and considerations, including software, infrastructure, retrofitting, planned downtime, implementation and consultation, subscription fees, and security measures, which can be exorbitant.[49] In addition, fragmented systems that favour non-competitive practices, such as vendor lock-in, also increase the barriers and cost to access this technology.

In addition, the ability of users to access connected devices depends on the overall infrastructure. Connected devices rely on consistent and affordable internet access and electricity supply to charge and power the devices. The International Telecommunication Union (ITU) estimated that as of 2021, 37% of the world's population, or 2.9 billion people, still have not used the internet.[50] Meanwhile, 759 million people still live without electricity.[51] This disproportionately affects those in developing economies, from low-income groups and those living in rural areas. As Greg Hrebek, President of Railspire, notes: "Connected devices have a reliance on socio-economic advantages that include access to technology along with the supporting infrastructure. This reliance limits access, usability, and diminishes the value that could be provided to the groups that would benefit most."[52]

The ability of people of all backgrounds to access and benefit from technology is also affected by their knowledge of how to use the technology. Digital literacy differs among people of different socio-economic backgrounds (income, age, gender) and geographical location (rural vs urban), among others. Respondents have also pointed out the lack of consideration given to people with disabilities, non-standard accents or dialects, and other discriminatory factors in the designing of connected devices and digital solutions.

What can be done

1. Investment in infrastructure

Investment in infrastructure to improve access to the internet and electricity is important to increasing access to digital technology at the last mile. The World Bank estimates that $100 billion is needed to achieve universal, good quality internet access across Africa alone, of which 80% is needed for infrastructure to establish and maintain broadband networks.[53] While the private sector has led much of the investment in digital infrastructure, government plays an important role in providing a conducive regulatory environment, absorbing earlier risks and bridging investment gaps.[54]

Box 10: **Public-private partnership – A submarine fibre optic cable built in São Tomé and Príncipe**[55]

Public-private partnerships (PPPs) have the potential to absorb early risks in major infrastructure investments. The experience in São Tomé and Príncipe illustrates the power of government-initiated investment in broadband infrastructure.

The country's early reliance on satellite technologies for international connectivity generated expensive and low-quality communications outside its borders. To remedy this situation, the federal government and incumbent local telecommunications service providers came together to bring high-speed connectivity to São Tomé and Príncipe by establishing a new limited company to invest in the Africa Coast to Europe (ACE) submarine fibre optic cable. Following the successful launch of ACE cable service in 2014, the government awarded licences to a new service provider, creating competition and encouraging further substantial price reductions throughout a variety of services in the country, including more investment by the private sector to expand infrastructure.

2. A conducive regulatory environment

To ensure that investment for digital infrastructure rises to the level needed to achieve universal access for internet and technology, the government can make the regulatory environment more conducive for investment. This includes improving market competition and incentives through more competitive spectrum policies, harmonizing fragmented regulatory regimes and providing tax credit for critical investment. Regulation should also address non-competitive practices that impede access to users, such as vendor lock-in, and promote open space/source use cases.

3. Public policies to improve access to technology and digital literacy

Demand-side policies are also important to ensure that people can access the technology and benefit from it. Various schemes and programmes can be put in place to increase affordability and digital literacy, including subsidizing equipment and training for marginalized groups or underserved communities. To ensure the future generation is not left behind, education in information and communications technology should be included in schools. The public and private sectors should also work in tandem to establish standards that promote inclusive and universal design at the outset, such as better end-user interfaces that help integrate a variety of user abilities.

Box 11: **GSMA Assistive Tech programme – The Principles for Driving the Digital Inclusion of Persons with Disabilities**[56]

The GSMA Assistive Tech programme has developed a set of principles to guide mobile operators and promote action for the industry to reduce the digital inclusion gap of persons with disabilities. The Principles for Driving the Digital Inclusion of Persons with Disabilities present three core tenets: embracing disability inclusion at every level of the organization, understanding how to reach and better serve persons with disabilities, and delivering inclusive products and services that meet the varied needs of persons with disabilities.

Box 12: **Matter – The open standards to drive inclusion**

In the smart home space, the barrier to access stems from the reliance on proprietary protocols and ecosystems, as well as on devices tied to user accounts. Open standards like Matter are improving this, enabling devices that can be used with any smart home platform, or even just with each other — making it easier to build into homes and buildings in a manner that can be used by multiple, successive residents. It also helps to make these devices cheaper and thus more accessible.[57]

Box 13: **EDISON Alliance – An initiative to prioritize digital inclusion to achieve the Sustainable Development Goals**[58]

The EDISON Alliance is an initiative of leaders from the public and private sectors worldwide who have prioritized digital inclusion as a key step towards achieving the Sustainable Development Goals (SDGs). The movement champions collaboration and multisector action to accelerate and expand digital investment to ensure everyone can affordably participate in the digital economy. It seeks to improve 1 billion lives through affordable and accessible digital solutions in health, finance and education by 2025.

Beyond basic access, all stakeholders must also ensure that infrastructure is in place for people to connect meaningfully. Meaningful connectivity includes appropriate speed, devices, data availability and regular use to ensure that people can maximize the benefit of connectivity.[59]

Reasons for optimism

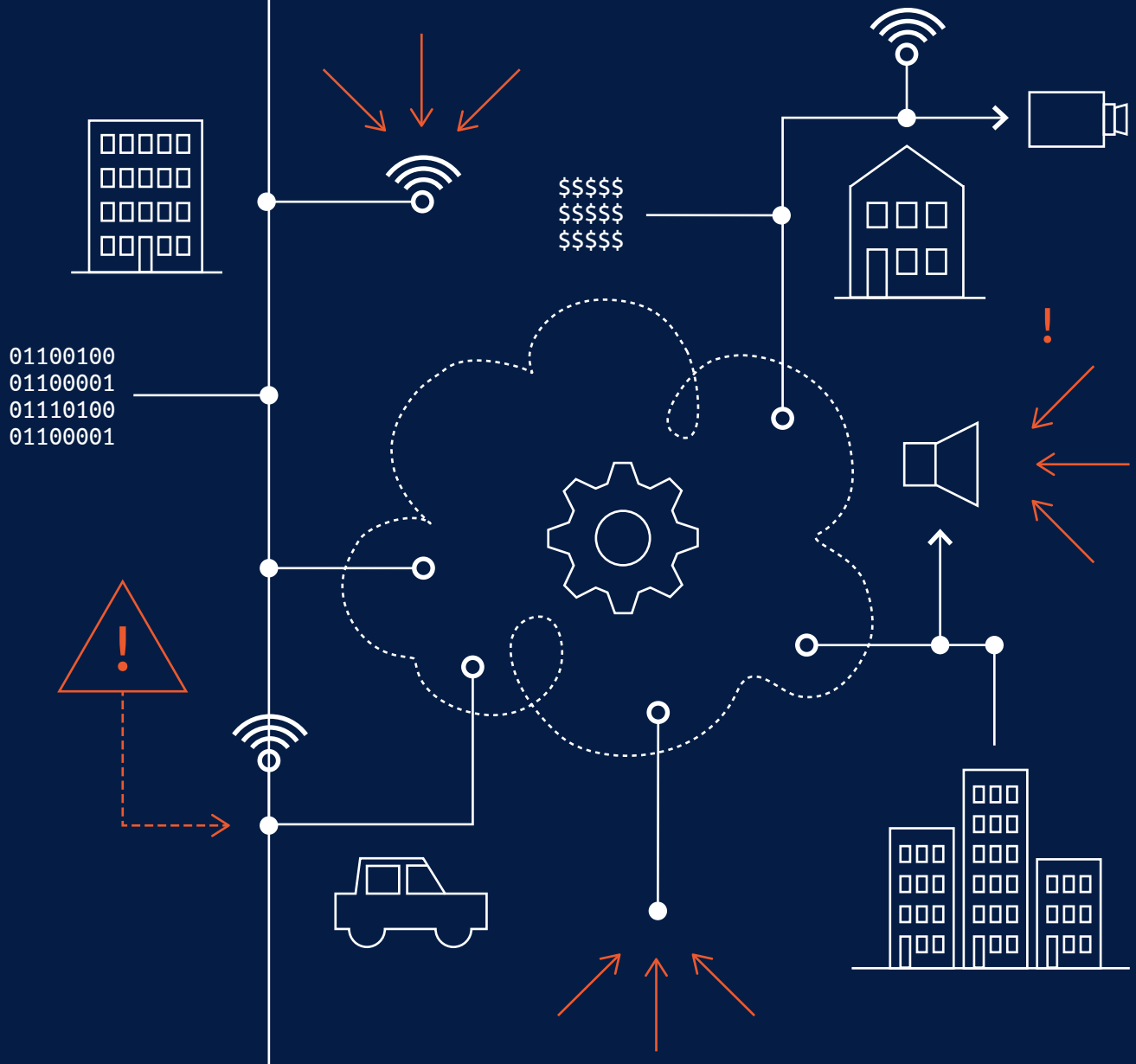
The use cases for connected devices and related technologies include various impactful applications that improve many aspects of people's lives in business, healthcare, education, environmental sustainability, disaster and emergency response, among others. As the connected devices market is expected to continue to grow, more investment will flow into the development of the technology, making devices more available and affordable.[60]

Rapid urbanization – with the world's urban population expected to double by 2050 – means more people are getting better access to digital infrastructure. It also means the provision of such infrastructure will be made easier.[61] As Fanyu Lin, Chief Executive Officer of Fluxus, notes: "Cities have the potential to be the core solution to bridge the digital divide."[62] Digital infrastructure built in high-density cities, where it serves more people and provides them with higher quality of life, is much more cost- and resource-effective than infrastructure built in rural areas. While the urbanization trend helps more people get connected, efforts to develop infrastructure and new connectivity alternatives, such as satellites and community networks, must continue to close the gap in the digital divide.

A lot still needs to be done to bridge this divide. Many people and communities still lack basic access to these technologies, let alone benefit from them. Identifying the key priority area of challenges and solutions is central to ensuring all parts of society can benefit from the technology.

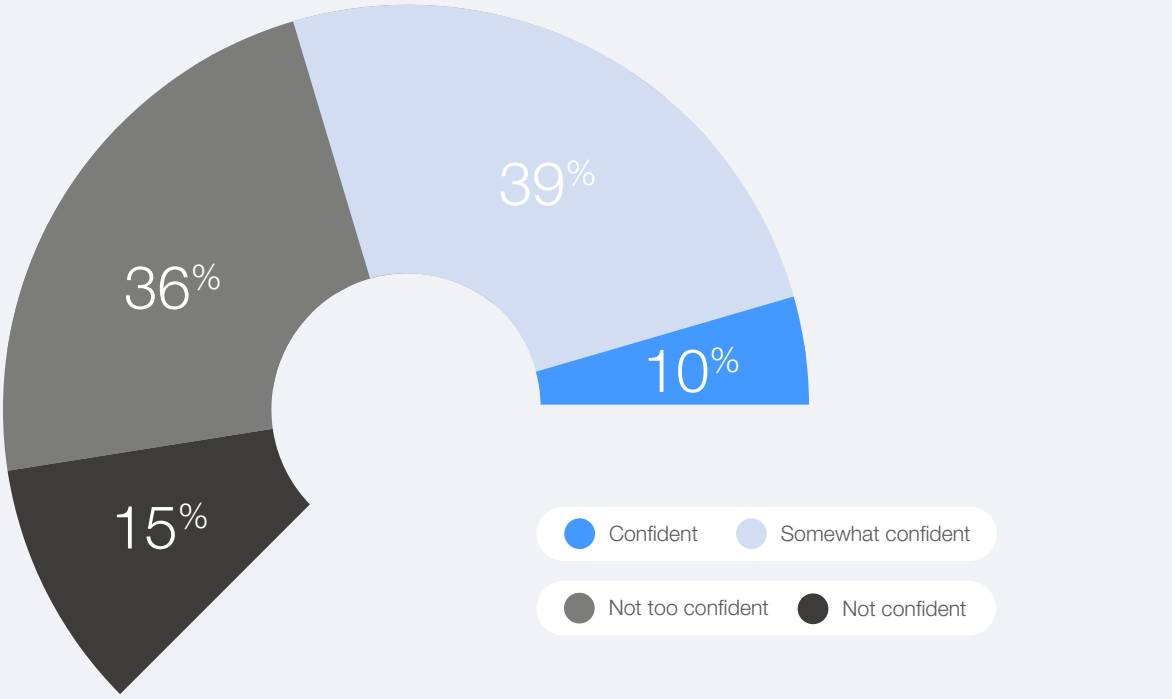
2

Other focus areas



2.1 Environmental sustainability

Figure 5: **User confidence that connected devices and related technologies are environmentally sustainable**



Source: World Economic Forum

Respondents were somewhat divided on whether IoT and related technologies are environmentally sustainable, with 49% confident or somewhat confident and 51% stating otherwise. There is, however, growing confidence in the progress on environmental sustainability of connected devices. In this area, 43% of respondents reported being more confident and somewhat more confident over the last three years, compared to 33% who reported no change and 24% who felt less confident and somewhat less confident.

The optimism is fuelled by the potential that IoT and related technologies has in contributing to attaining the SDGs, such as through smart water meters and air quality monitoring. Analysis shows that over 80% of the current IoT deployments are addressing or have the potential to address the issues detailed in the SDGs.[63] On the other hand, respondents' lack of confidence was attributed to the designed obsolescence of devices, the difficulty to recycle these devices, the energy consumption generated by traffic and data storage, the carbon footprint and uses of raw materials, and costly infrastructure.

While many IoT devices and applications have been designed and geared towards energy efficiency, the current scale of increased connectivity has also created, in turn, an increase in energy consumption. In addition, the trend is to increasingly move from a general-purpose model (e.g. mobiles or computers) to specialization (multiple IoT devices with very particular purposes), which leads to a significant increase in devices owned by households and individuals. The use of certain metals used in devices, such as cobalt and tungsten, contribute to the carbon footprint because these materials are difficult to recycle or reclaim. While IoT and related technologies could be a useful tool in bringing society and businesses closer to the SDGs, current barriers challenge the adoption of sustainable practices. Thus, it is important to evaluate how to best leverage IoT and related technologies for sustainable opportunities and factor in the challenge of making manufacturing in this field more sustainable as well.

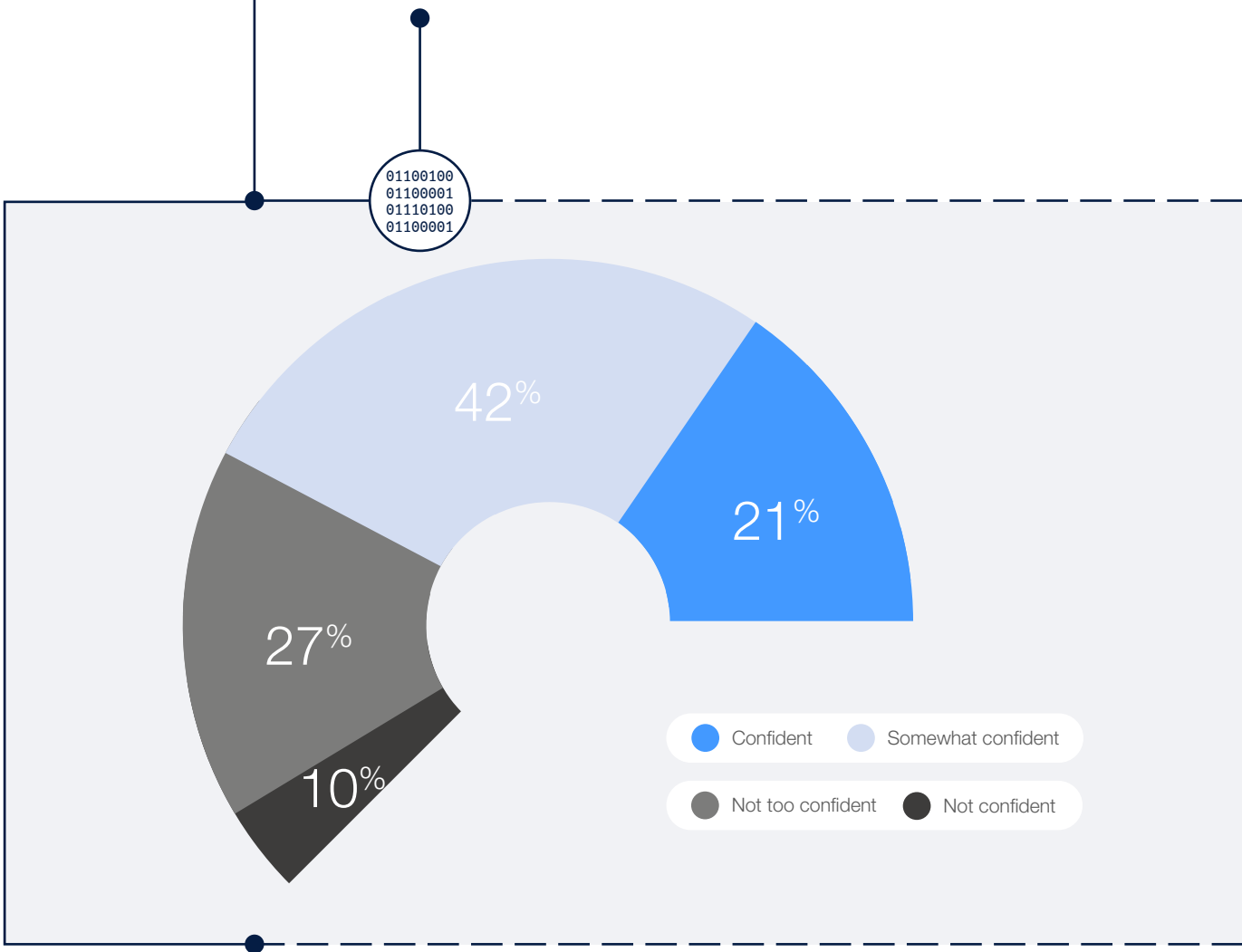
To address these issues, proposed alternatives include the use of IoT devices and applications to help reduce carbon emissions, smart energy meters, smart logistics to find alternative sources of energy to fuel technologies, policies to encourage innovations, and improved recycling practices.

Box 14: **Guidelines for sustainability – The prioritization of sustainability goals**

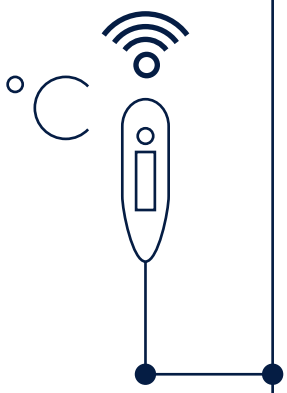
Considering IoT's power to enable digital transformation and its potential to address SDGs through its technologies, the World Economic Forum developed a set of guidelines for sustainability.[64] They were created to encourage the prioritization of sustainability goals as part of the design of commercial projects, while also maximizing social impact and delivering commercial value. They include collaboration models and incentives alignment, business and investment models, and impact measurement.

2.2 Financial and operational feasibility

Figure 6: **User confidence that connected devices and related technologies can be maintained and will provide value throughout their life cycles in the context of rapid technological and social changes**



Source: World Economic Forum



Life-cycle management of IoT and related technologies is essential to avoiding obsolescence of devices and their applications. The shortened life cycle of many connected devices and their respective software – a matter of growing concern – is not only environmentally unsustainable, but it also poses privacy and security risks as well as financial barriers. On average, obsolete devices have twice as many identified vulnerabilities per device compared to those that have aged or to current ones.[65] Incompatibility of software with devices, delays in patches and lack of revisitation to the operating system version all contribute to the growing number of obsolete devices and add to the cost of using these technologies.

Most respondents believed that the issue of obsolescence will be gradually addressed through rapid innovation that allows for maximum scalability, an increase in awareness surrounding the challenges of obsolescence and an improvement in regulations. Most respondents (63%) felt confident or somewhat confident that connected devices and related technologies can be maintained and will provide value throughout their life cycles in the context of rapid technological and social changes. This sentiment is further supported by 62% of respondents who were more confident (20%) or somewhat more confident (42%) that governance practices and developments in technology have changed over the past three years.

On the other hand, 37% of respondents lacked confidence in this area, with 27% and 10% stating to be not too confident and not confident, respectively. Respondents attributed their lack of confidence to the recurrence of "planned obsolescence" practices, where IoT and related technologies often have hardware that cannot be repaired or reused, often having limitations on how many times their software can be updated. Manufacturers benefit from the shortened lifespan of devices as consumers dispose of their devices and must buy new ones.

Respondents also indicated that the lack of interoperability – and failure of governments to intervene and avoid this – as well as the lack of user awareness surrounding the need for software updates and patches has further contributed to their lack of confidence in this area. Proposed solutions to address this governance gap include promoting remote upgrades and maintenance of IoT devices and related technologies, and clear and harmonized guidance for device manufacturers. This must include regulation on repair, refurbishment, resale and the provision of services that encourage individuals to return devices at the end of their life cycles for recycling, as well as standardization and interoperability to ensure ease of patching and updating.

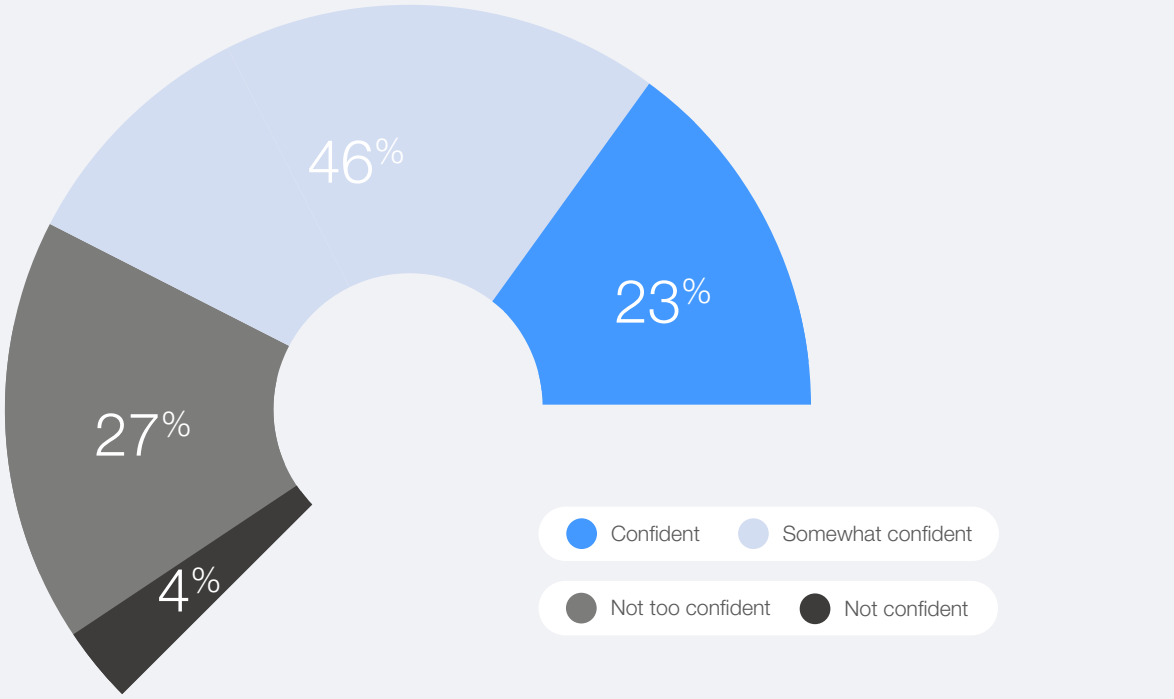
Box 15: **Legislation against "planned obsolescence" – A country takes a step forward**

In 2015, France became the first country to define and outlaw "planned obsolescence", a practice in which manufacturers design a product to become dated or useless within a certain time frame, leading to an increase in its replacement.[66] Furthermore, as of 2020, the French government introduced a durability and repairability rating, in which IoT devices, such as smartphones and electronic and household appliances, will receive a sticker on their packaging to indicate their estimated life span.[67]

In response, users are now advocating for "right-to-repair", arguing that if they own a device, they should be able to repair it themselves or take it to a technician of choice. The objectives of the proponents of right-to-repair include making information (manuals, schematics and software updates) and parts and tools (such as diagnostics tools) available; legalizing the unlocking, adapting or modifying of a device so the owner can install custom software; and accommodating repair in the design.[68]

2.3 Interoperability and system architecture

Figure 7: **User confidence that connected devices and related technologies can operate with each other effectively and efficiently**



Source: World Economic Forum

The interoperability of IoT and related technologies is defined as "the capacity for multiple components within an IoT deployment to effectively communicate, share data and perform together to achieve a shared outcome".[69] About two-thirds (69%) of respondents stated being confident (23%) or somewhat confident (46%) that connected devices and related technologies can operate with one another effectively and efficiently. This is driven by the confidence that it is in the industry's interest to further develop and implement interoperability practices and standards through collaboration and open standards.

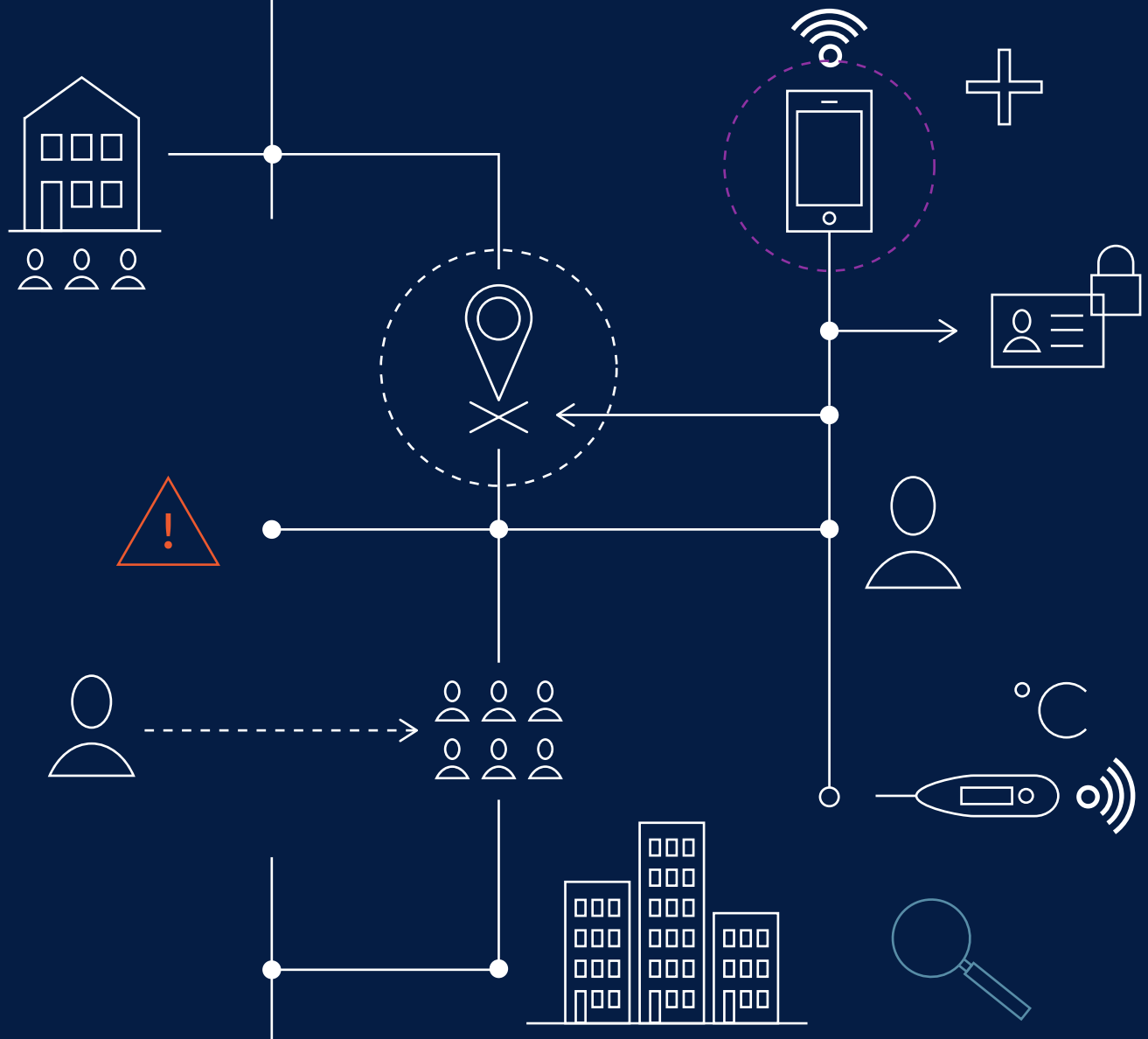
On the other hand, 31% of respondents demonstrated a lack of confidence in the interoperability of connected devices and related technologies, with 27% not too confident and 4% not confident. Given the proprietary nature of many IoT and related technologies solutions that are not API-accessible, interoperability still faces challenges to integrate devices and systems seamlessly. Insufficient requirements and incentives for interoperability across IoT and related technologies as well as the lack of standardization and the dominance of players constitute barriers in this area. To address these challenges and move towards a more integrated system, businesses and industries must improve on standardization by adopting standards and open-source development and converging smart ecosystems through partnerships that deliver a seamless user experience and device connectivity.

Box 16: **Zigbee – An interoperability certification network**

As an initiative from the Connectivity Standards Alliance, Zigbee provides a full-stack solution for smart devices, allowing them to "connect and communicate using the same IoT language with each other" through low-cost and low-energy wireless IoT data solutions.[70] Rather than using point-to-point communication, such as Bluetooth, it uses a mesh network that allows for interoperability of various smart devices. Devices and applications within the Zigbee network span across commercial and residential spaces as well as utilities, and are used in "wireless light switches, home energy monitors, traffic management systems, and other consumer and industrial equipment that require short-range low-rate wireless data transfer."[71]

3

The pandemic effect



The COVID-19 pandemic has made connected devices important in various industries and areas, including healthcare, smart cities and transportation, as governments and businesses navigate service delivery and business continuity and consider health measures and restrictions to curb the spread of the pandemic.

Healthcare

Prior to COVID-19, health trackers, such as smart watches and smart rings, already began to gain popularity. The onset of the pandemic, however, has put these devices in the frontline of combatting the virus by facilitating social distancing, contact tracing and patient monitoring, among others. The use of IoT and related technologies in healthcare was slow and cautious due to regulatory policies related to data security, privacy and approval procedures. Many connected technologies have been deployed through emergency approvals, accelerating the adoption of IoT and related technologies. The U.S. Food and Drug Administration also issued a temporary Emergency Use Authorization (EUA) for the cardiac-focused digital health company Eko, providing it with a certificate for its electrocardiogram low ejection fraction tool to assist clinicians in identifying and assessing cardiac complications due to COVID-19.[72]

Box 17: **Oura Ring – A wearable device for diagnosis and early illness detection**

The Oura Ring is a wearable smart ring that uses sensors to track a variety of health metrics, including sleep, recovery and heart rate monitoring. During the COVID-19 pandemic, the smart device was used to identify signs of the virus through temperature data collection which, in turn, assisted in observing rises in people's temperatures above normal and, consequently, provided early illness detection. A series of studies have found that bio signals from the Oura Ring, including respiratory rate, heart rate, temperature and heart rate variability, were able to detect signals associated with the onset of COVID-19 prior to diagnostic testing.[73]

"X from home"

Owing to the amount of time individuals spent and continue to spend inside their homes, the adoption of smart devices for homes increased. And while numerous companies have shifted back to the office, many have adopted either full work from home or hybrid policies for the workplace. Consequently, individuals have invested in IoT devices and related technologies for their environments. This introduced new features and sensors on existing devices, new home energy management solutions and new features to assist with "x from home", i.e. working from home, shopping from home, studying from home and maintaining health from home.[74] A recent study released by Xiaomi found that 51% of consumers reported having purchased at least one smart device since March 2020.[75]

Business operations

The importance of industrial IoT (IIoT) during the pandemic has led to a potentially significant growth in the area, with a recent McKinsey survey finding that 93% of supply chain and manufacturing professionals intend to focus on smart and resilient solutions.[76] Moreover, the market worth of IIoT is expected to reach $263.4 billion by 2027.[77] Recent developments in IIoT span across remote monitoring, machine health prognostics, smart manufacturing and inventory management. Businesses have leaned on IoT and related technologies to ensure business continuity and resilience throughout the pandemic, implementing technologies of automation and connectivity to tackle the challenges posed by COVID-19. These technologies allowed for businesses to establish social distancing practices, remote asset control, IIoT-enabled inventory management, in-line process automatization and remote assistance, among many others. Using sensors and connected devices, businesses can keep their operations afloat by implementing a plug-and-play mode, while also ensuring employee safety and security. Moving forward, IoT and related technologies can surpass the constraint of managing pandemic scenarios and be leveraged to scale for long-term benefits, such as in energy management and sanitization.

Two years into the pandemic, supply chain disruptions continue and will likely endure.[78] These disturbances have caught the attention of C-suite executives as the leadership now considers these disruptions to be the biggest threat to the growth of businesses and economies. The crisis generated by COVID-19 has made companies prioritize business continuity by building resilience and flexibility over focusing on innovation and restructuring. One of the hardest-hit areas was the supply chain for smart appliances,

including chip assembly, chip fabrication and smart components. In lieu of this challenge, supply chain workarounds have now become a standard, and many companies have produced alternatives, from buying warehouses when requiring more space to making their own containers, chartering vessels and buying e-commerce fulfilment operators.

Built environment

Strict lockdown measures transformed the way built environments are navigated. The importance of IoT and related technologies increased due to how buildings needed to operate throughout the pandemic to adapt to social distancing practices, such as smart heating, ventilation and air-conditioning systems to adhere to health standards, strict cleaning requirements and occupancy monitoring. The adoption by many of working from home, and consequently the decrease in building occupancy, is an opportunity for businesses to invest in smart building technologies to reduce potential operational costs while also becoming more sustainable.

COVID-19 transformed many parts of urban life, with a decrease in traffic and public transit usage, a rise in internet connectivity, a decrease in pollution and a disruption in supply chains. Leading smart cities that had already invested in IoT and related technologies prior to the pandemic were better prepared to deal with COVID-19. More sensors have been installed in smart cities since the onset of the pandemic, using multiple IoT applications and devices, such as thermal cameras, surveillance, drones and phone apps.[79] Governments that were able to deploy existing technologies and integrate them with innovative approaches demonstrated success in mitigating the risks of COVID-19 while using IoT and related technologies.

Box 18: **Big data analytics, new technology and proactive testing – The response to COVID-19 in Taiwan[80]**

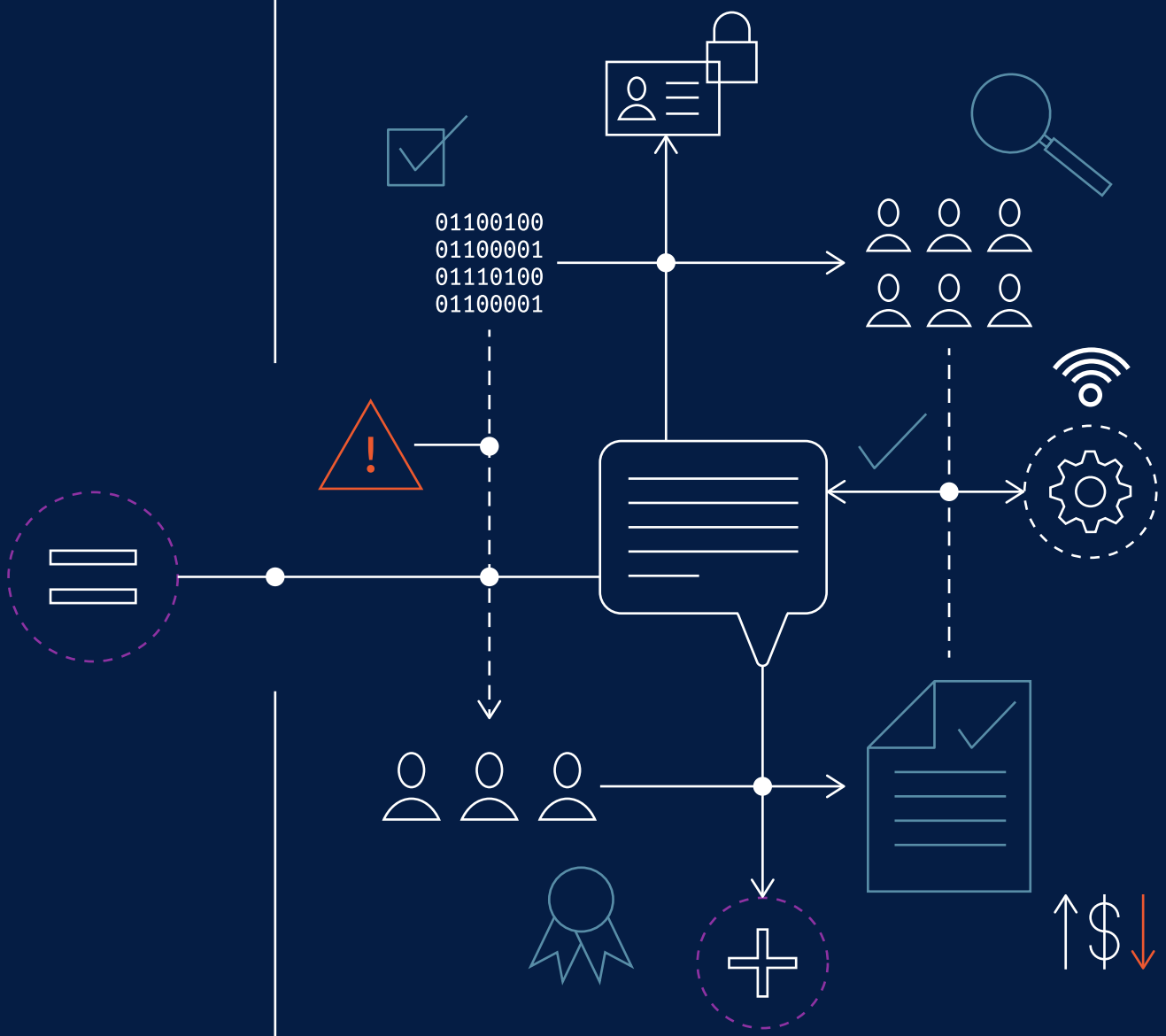
Through prompt action and preparedness to tackle the COVID-19 pandemic, Taiwan leveraged the use of IoT and related technologies to curb the spread of the virus. The government combined its national health insurance database with its immigration and customs database, generating real-time alerts during clinical visits based on travel history and clinical symptoms to help identify cases of contamination. Additionally, it used new forms of technology, including QR-code scanning and online reporting of travel history and health symptoms, to classify the risk of infections of travellers based on flight origin and travel history.

The pandemic spurred many changes in the field of transportation, including cabin sensing and analytics as well as smart logistics. This led to an increase in adoption of decentralized fleet management, ultraviolet C-based light cleaning and in-cabin environment control.

As society moves towards online channels, businesses and governments have responded by greatly accelerating digital transformation, spurring the adoption of these developments in personal lives, the public sphere and the market. Innovations allowed for an increased use of IoT and related technologies that improved quality of life for individuals and drew governments nearer to citizens, allowing the former to provide better services, and provided businesses with insights and solutions to address challenges within their industries due to the pandemic. Fanyu Lin notes that the pandemic "put the IoT ecosystem at the centre of the global stage. Because the dependence on IoT has increased dramatically during this period, benefits become more obvious, and the risk becomes also exposed."[81]

Nonetheless, the increase in usage of IoT and related technologies leads to questions about security, privacy and civil liberty. While tools such as contact tracing and thermostats served as important means for public health communication and containing the spread of the virus, these applications also collected sensitive data information which, in turn, has raised concern about the potential of data leaks, surveillance and misuse. Therefore, while these devices have proven to be an asset in mitigating the risks of the pandemic, they have an impact on privacy and security. Modern approaches to contact tracing and containing the spread of viruses, however, are being conducted with user consent placed at the forefront of the applications. To curb the spread, Google and Apple announced a joint effort to develop a system to enable contact tracing through a Bluetooth-based approach, where users must opt-in to participate.[82] User privacy, security and consent should be at the forefront of such development, while also allowing for interoperability between the systems.

Conclusion

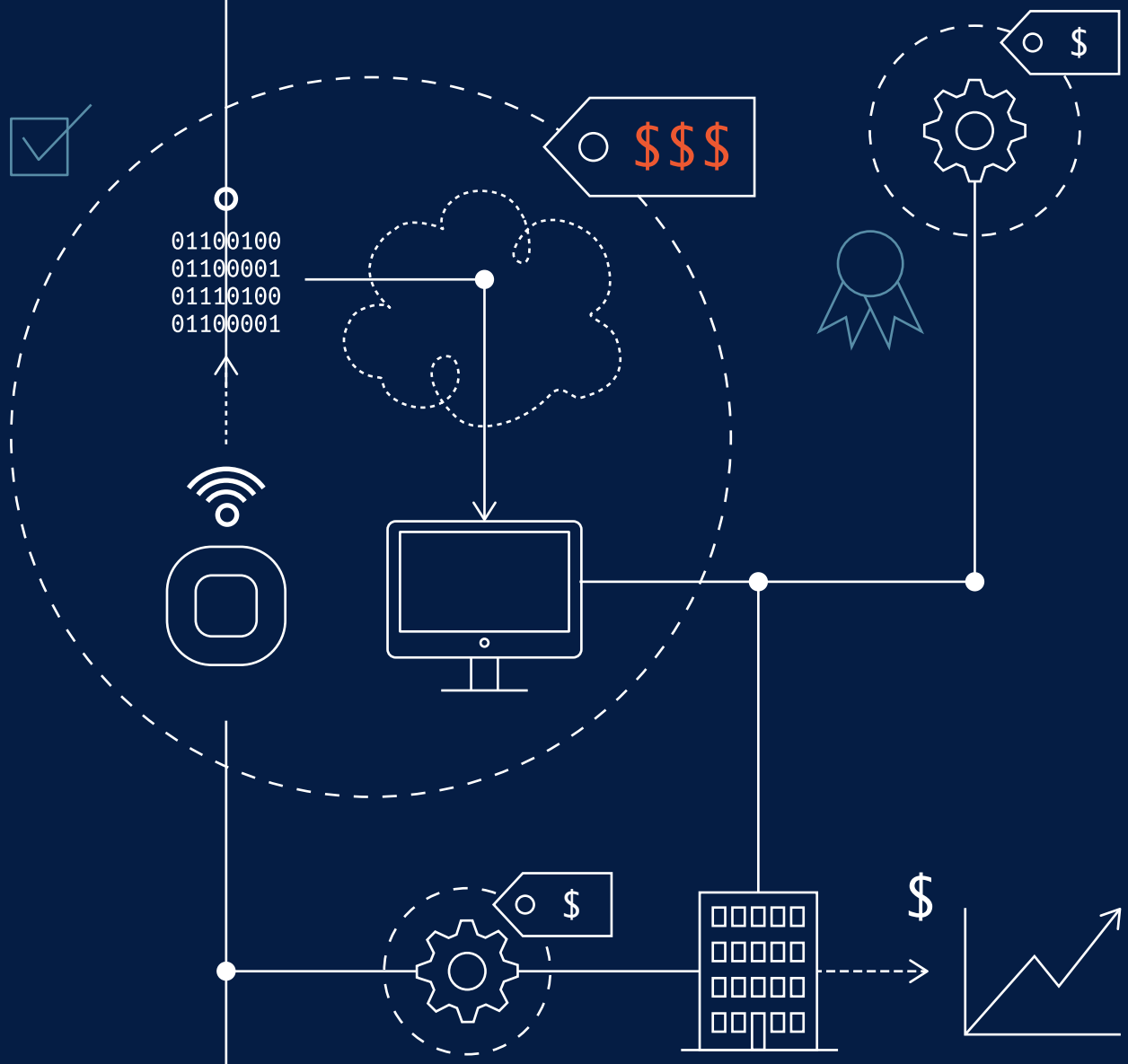


A path towards a more sustainable and inclusive IoT

The role of IoT and related technologies continues to affect the way people work and live. This digital transformation presents the opportunity to shape a future that is more sustainable, inclusive and prosperous for all. These developments, however, are not withstanding new risks and challenges in governance. Published at the onset of COVID-19, the *State of the Connected World 2020 Edition* shed light on the importance of IoT and related technologies in providing solutions to the challenges of a novel pandemic, requiring consumers, businesses and governments to adapt and innovate. Technologies deployed for contact tracing, social distancing, telehealth, automation of manufacturing and services, remote working and learning, among many others, enabled the world to effectively respond to the crisis and mitigate its risks. The role of IoT and related technologies in collecting and providing data to curb the spread of the disease, however, emphasized existing concerns regarding security, privacy, interoperability, economic sustainability and equity.

The *State of the Connected World 2023 Edition* highlights the current governance gaps in the realm of IoT and related technologies, what developments or changes can be observed from its previous publication and paths forward to address those gaps and the associated risks. In response to the findings of this report, the World Economic Forum has identified the principal areas of opportunity for collective action from businesses and governments, especially those pertaining to ethics, security and accessibility. The full potential of IoT and related technologies remains untapped and, as the world becomes increasingly connected and digitized, the systemic challenges must be acted upon, requiring the commitment of the various stakeholders within the ecosystem.

Appendices



Appendix A: Methodology[83]

A governance gap is defined as the difference between the potential risks posed by a technology and society's efforts to safeguard itself against these risks. Those efforts include laws, industry standards and self-governance approaches designed to achieve the greatest potential benefit of that technology for society as a whole.

The IoT governance gaps identified in this report are based on the expert perceptions of a wide range of IoT industry stakeholders. They have been analysed across the following impact areas:

Ethics and integrity: The ability of IoT devices and systems to safeguard the privacy of users and engender trust that personal information will be collected, stored and used for agreed purposes in an ethical and responsible manner

Cybersecurity: The ability of IoT devices, applications and systems to maintain a safe and secure development, deployment and operational environment

Equal access: The ability of IoT devices and systems to fairly benefit and protect societal stakeholders irrespective of geographic, socio-economic or other factors

Environmental sustainability: The ability of IoT devices and systems to be environmentally sustainable throughout their life cycle

Obsolescence (financial and operational feasibility): The ability of IoT devices and systems to be financially and operationally sustainable throughout their life cycles in the context of rapid technological and social changes

Interoperability and system architecture: The ability of IoT devices and systems to interact effectively with each other to execute tasks in an efficient and cost-effective manner

The research consisted of quantitative and qualitative approaches, including surveys, interviews and desktop research.

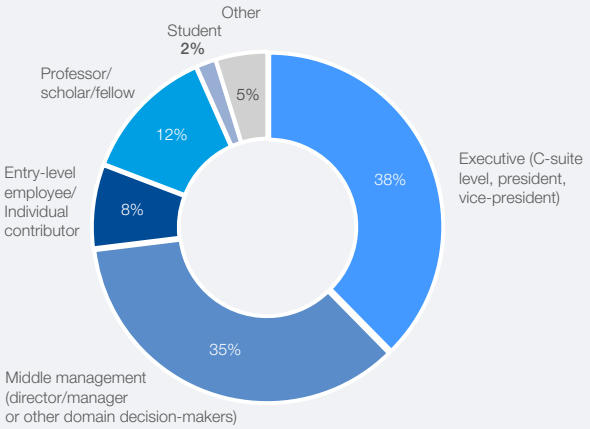
Quantitative research
The State of the Connected World survey, distributed to IoT experts in the private and public sectors and to private citizens in civil society, asked them to assess both the risks associated with IoT and the current level of society's ability to safeguard against harm from these risks. (See Appendix B for demographic information on survey respondents.) A total of 271 responses, received from around the globe, were used to calculate and identify current perceived levels of confidence in governance gaps and change in confidence in connected technologies and related governance practices over the last three years. The data collected was ranked into three top areas of impact according to governance gaps where most respondents indicated being "not too confident" or "not confident".

Qualitative research
In addition to the quantitative data, the survey respondents were asked to provide qualitative responses on examples of risk and governance measures as input to the qualitative research. More than 25 interviews were conducted with global IoT experts to capture further insights on IoT risks and governance. Finally, extensive desktop research was conducted on current governance measures around the globe. Taken together, the results of the quantitative analysis and the input from qualitative research allowed to identify and prioritize the key IoT governance gaps described in this report.

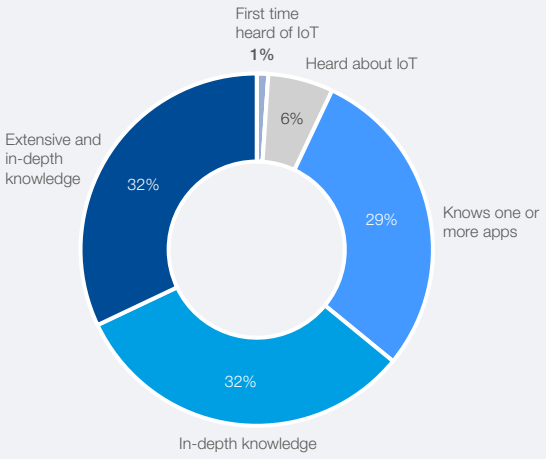
271 responses were received.

Appendix B: 2023 State of Connected World survey demographics

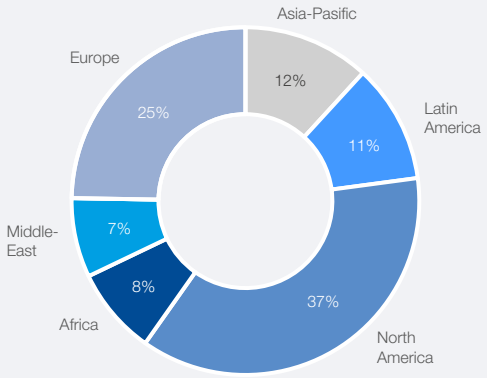
Employment level of respondents



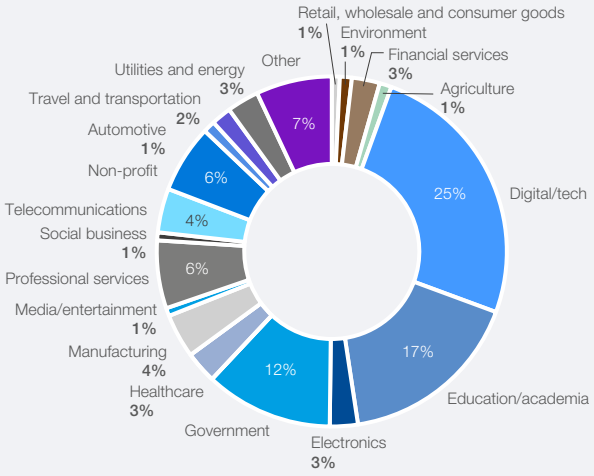
Level of knowledge about IoT



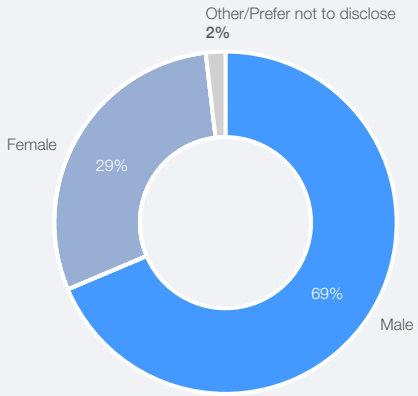
Region of respondents



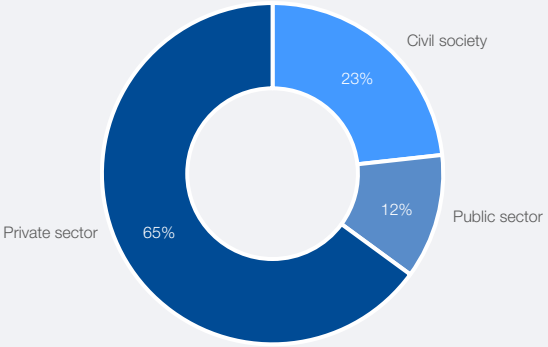
Sector of employment of respondents



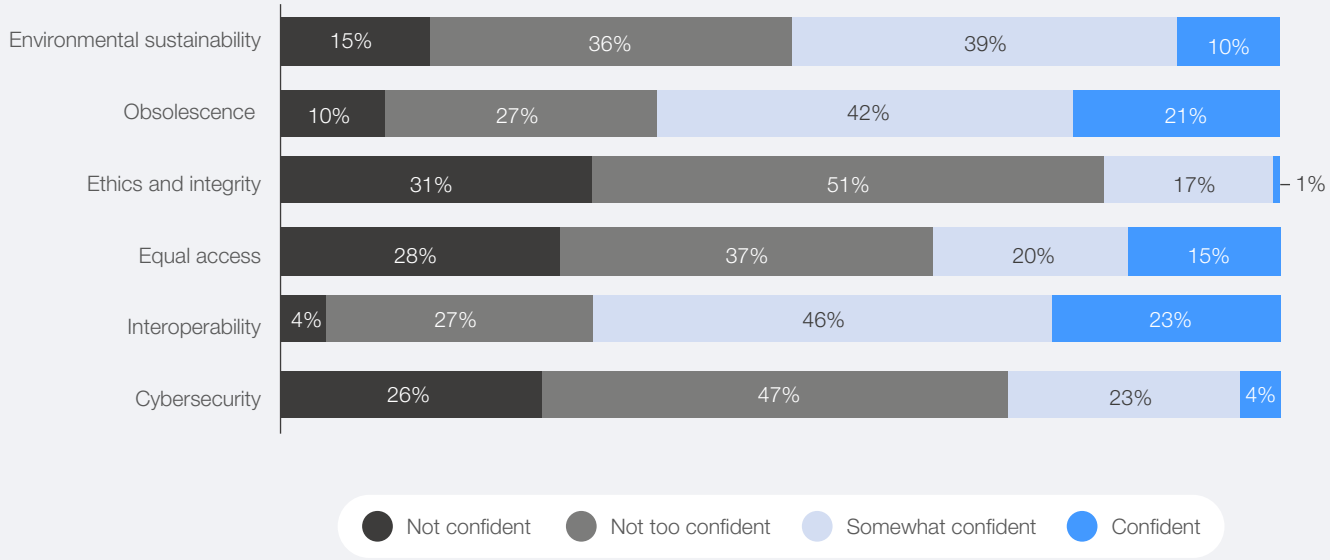
Gender of respondents



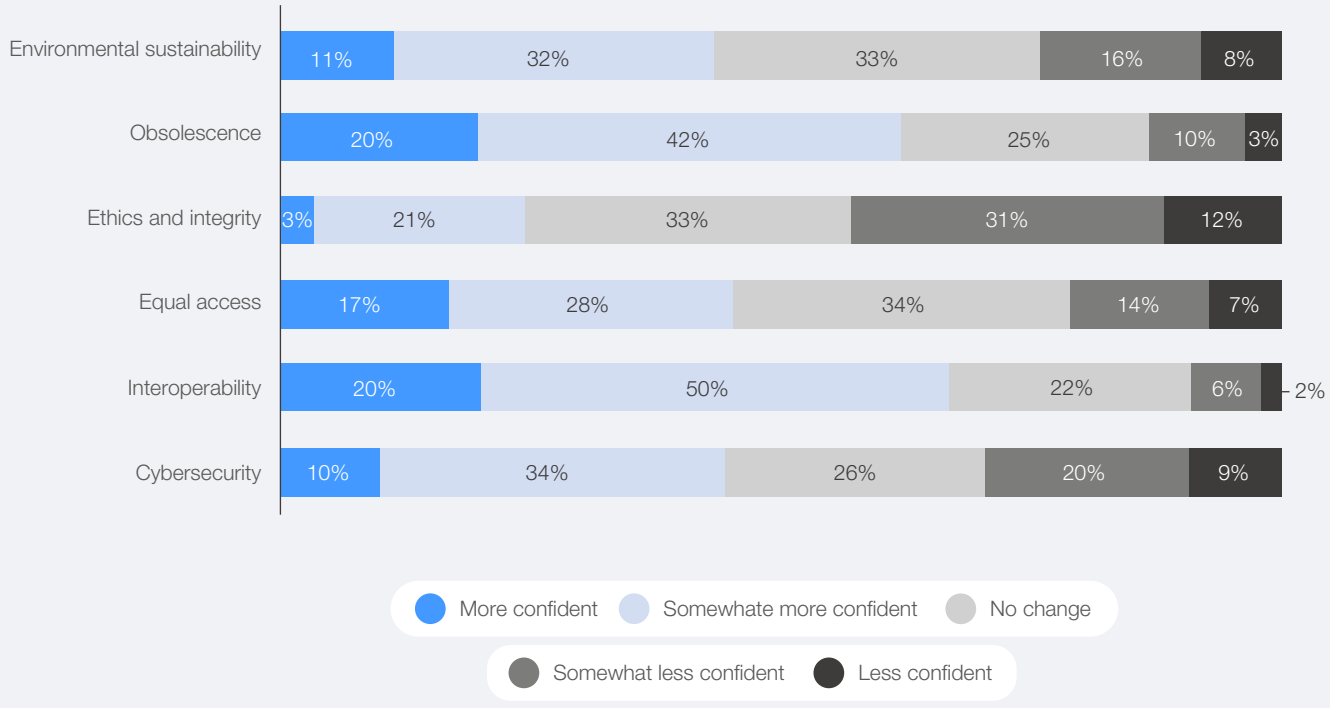
Sector categories of respondents



Confidence in governance gap



Change in confidence over past three years



Contributors

Lead authors

Giovanna Antoniazzi
Early Careers Programme, Urban Transformation, World Economic Forum LLC

Saiful Salihudin
Platform Curator, Urban Transformation, World Economic Forum LLC

Main contributors

Tushaar Bhaat
Founder and Managing Director, Convaise, Germany

Obakeng Hlatshwayo
Senior Project Manager, Centre for the Fourth Industrial Revolution South Africa

Boipelo Jarvis
Fellow, Centre for the Fourth Industrial Revolution South Africa

Karen Lightman
Executive Director, Carnegie Mellon University, USA

Acknowledgements

Council on the Connected World

This Insight Report benefited from the input, guidance and review of the experts and stakeholders on the World Economic Forum Council on the Connected World.

Review Committee

José M. Alonso
Chief Executive Officer, World Wide Web Foundation, USA

Cristina Colom
Director, Digital Future Society, Mobile World Capital Barcelona, Spain

Scott Harden
Chief Technology Officer, Innovation, Schneider Electric, France

Ntsibane Ntlatlapa
Head, Centre for Fourth Industrial Revolution South Africa

Josh Siegel
Assistant Professor, Michigan State University, USA

Council Members

José M. Alonso
Chief Executive Officer, World Wide Web Foundation, USA

Shahid Ahmed
Group Executive Vice-President, New Ventures and Innovation, Nippon Telegraph and Telephone, Japan

Anousheh Ansari
Chief Executive Officer, XPrize Foundation, USA

Alicia Asin
Chief Executive Officer, Libelium, Spain

Madeline Carr
Professor of Global Politics and Cybersecurity, Department of Computer Science, University College London, UK

Harsh Chitale
Chief Executive Officer, Digital Solutions Division, Signify, Netherlands

Cristina Colom
Director, Digital Future Society, Mobile World Capital Barcelona, Spain

Jackline Conca
Undersecretary of Innovation and Digital Transformation of Brazil

Thulani Dlamini
Chief Executive Officer, Council for Scientific and Industrial Research (CSIR), South Africa

Ken Hu
Deputy Chairman, Huawei Technologies, People's Republic of China

Farnam Jahanian
President, Carnegie Mellon University, USA

Chris Johnson
Head, Global Enterprise Business, Nokia, Finland

Gilbert Kamieniecky
Head, Private Equity Technology, Investcorp International, USA

Mohamed Kande
Vice-Chair and Leader, US and Global Advisory, PwC, USA

Vimal Kapur
President and Chief Executive Officer, Honeywell Performance Materials and Technologies, USA

Anton Kotov
Chief Strategy Officer and Chief Digital Officer, Electrification, ABB, Switzerland

Helena Leurent
Director-General, Consumers International, UK

Fanyu Lin
Chief Executive Officer, Fluxus, USA

Jeff Lorbeck
Senior Vice-President, Qualcomm, USA

Adrian Lovett
Chief Executive Officer, Development Initiatives, Kenya

Jacqueline Lu
President and Co-Founder, Helpful Places, Canada

Stella Ndabeni-Abrahams
Minister of Small Business Development of South Africa

Peter Nicoletti
Field Chief Information Security Officer, Check Point Software Technologies, USA

Mariam Nouh
Vice-President, Economies of the Future, King Abdulaziz City for Science and Technology (KACST), Saudi Arabia

Julie Owono
Executive Director, Internet Sans Frontières, France

Maria Paz Canales
Executive Director, Derechos Digitales, Chile

Nadège Petit
Chief Innovation Officer, Schneider Electric, France

Victor Pineda
President, World Enabled, USA

Tobin Richardson
President and Chief Executive Officer, Connectivity Standards Alliance, USA

Aarthi Subramania
Group Chief Digital Officer, Tata Sons, India

Åsa Tamsons
Senior Vice-President and Head, Business Area Technologies and New Businesses, Ericsson, Sweden

Michele Turner
Senior Director, Google Smart Home Ecosystem, Google, USA

Kristel Van der Elst
Chief Executive Officer, The Global Foresight Group, Canada

Beau Woods
Cyber Safety Innovation Fellow, Atlantic Council, USA

Andrew Young
Associate Director and Group Chief Innovation Officer, Sino Group, Hong Kong SAR

Additional acknowledgements

The World Economic Forum and the Council on the Connected World acknowledge the many experts and representatives from companies large and small, industry associations, academia, government and civil society who participated in the report interviews, surveys and workshops. Special thanks go to the Centres for the Fourth Industrial Revolution for their dedication and support to help bring this initiative to life.

Endnotes

1. World Economic Forum in collaboration with the Global Internet of Things Council and PwC, *State of the Connected World 2020 Edition*, Insight Report, December 2020.
2. Consumers International and the Internet Society, "The trust opportunity: Exploring consumers' attitudes to the Internet of Things", 1 May 2019, https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf (accessed 9 November 2022).
3. Matt Burgess, "How GDPR Is failing", *WIRED*, 23 May 2022, https://www.wired.com/story/gdpr-2022/ (accessed 9 November 2022).
4. Consumers International and the Internet Society, op. cit.
5. Kate Kaye, "Ad trackers continue to collect Europeans' data without consent under the GDPR, say ad data detectives", Digiday.com, 4 October 2021, https://digiday.com/media/ad-trackers-continue-to-collect-europeans-data-without-consent-under-the-gdpr-say-ad-data-detectives/ (accessed 9 November 2022).
6. Emilie Scott, "The trouble with informed consent in smart cities", International Association of Privacy Professionals, 28 February 2019, https://iapp.org/news/a/the-trouble-with-informed-consent-in-smart-cities/ (accessed 9 November 2022).
7. Mark Smith and Jacquelyn Palmer, "ANALYSIS: Three Years Later, GDPR Compliance Still a Challenge", Bloomberg Law, 21 July 2021, https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-three-years-later-gdpr-compliance-still-a-challenge (accessed 9 November 2022).
8. Ben Wolford, "What is GDPR, the EU's new data protection law?", GDPR.EU, https://gdpr.eu/what-is-gdpr/ (accessed 9 November 2022).
9. The World Bank, "Population, total – European Union", https://data.worldbank.org/indicator/SP.POP.TOTL?locations=EU (accessed 9 November 2022).
10. User Centrics, "Brazil's General Data Protection Law/Lei Geral de Proteção de Dados (LGPD) – an overview", 14 March 2022, https://usercentrics.com/knowledge-hub/brazil-lgpd-general-data-protection-law-overview/#:~:text=The%20General%20Data%20Protection%20Law,effect%20on%20August%2016%2C%202020 (accessed 9 November 2022).
11. Personal Data Protection Commission Singapore, "PDPA Overview", https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act#:~:text=What%20is%20the%20PDPA%3F,Banking%20Act%20and%20Insurance%20Act (accessed 9 November 2022).
12. State of California Department of Justice, "California Consumer Privacy Act (CCPA)", https://oag.ca.gov/privacy/ccpa (accessed 9 November 2022).
13. Bloomberg Law, "China Personal Information Protection Law (PIPL) FAQs", 6 April 2022, https://pro.bloomberglaw.com/brief/china-personal-information-protection-law-pipl-faqs/ (accessed 9 November 2022).
14. Cookiebot, "POPIA – South Africa's Protection of Personal Information Act: Enforcement update July 2021", 2021, https://www.cookiebot.com/en/popia (accessed 29 November 2022).
15. Interview with Farnam Jahanian on 26 August 2022.
16. See Tech Policy Design Lab, "Collaborating to build a safer, more empowering online world for everyone", https://techlab.webfoundation.org/about (accessed 9 November 2022).
17. Butlr, "Butlr People Sensing Platform: Anonymous spatial intelligence in real time", 2022, https://www.butlr.io/technology (accessed 9 November 2022).
18. Publicis Sapient, "The Data Collection and Consent Survey", https://www.publicissapient.com/insights/data-collection-and-consent-survey-IPSOS-research?utm_source=google&utm_medium=PR&utm_campaign=CDPIpsosResearchGlobal2020PR (accessed 9 November 2022).
19. Meta, "Introducing Privacy Center", 7 January 2022, https://about.fb.com/news/2022/01/introducing-privacy-center (accessed 9 November 2022).
20. KPMG, "Corporate data responsibility: Bridging the consumer trust gap", August 2021, https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2021/corporate-data-responsibility-bridging-the-consumer-trust-gap.pdf (accessed 9 November 2022).
21. World Economic Forum, "Unlocking the Shared Value of Smart City Data: A Protocol for Action", White Paper, June 2022, https://www.weforum.org/whitepapers/unlocking-the-shared-value-of-smart-city-data-a-protocol-for-action (accessed 10 November 2022).
22. Alex Najibi, "Racial Discrimination in Face Recognition Technology", Science in the News, 24 October 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology (accessed 9 November 2022).

23. World Economic Forum, *A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations*, Insight Report, Revised November 2022, https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf (accessed 10 November 2022).
24. Kaspersky, "Kaspersky Security Bulletin 2021. Statistics", https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_eng.pdf (accessed 9 November 2022).
25. Thought Lab, "Cybersecurity Solutions for a Riskier World", https://thoughtlabgroup.com/cyber-solutions-riskier-world/ (accessed 9 November 2022).
26. Cybersecurity Ventures, "Boardroom Cybersecurity 2022 Report", https://www.secureworks.com/resources/rp-boardroom-cybersecurity-report (accessed 9 November 2022).
27. Verified Market Research, "Global Consumer IoT Market Size by Type, by Application, by Geographic Scope and Forecast", August 2022, https://www.verifiedmarketresearch.com/product/consumer-iot-market/ (accessed 9 November 2022).
28. Office of the Victorian Information Commissioner, "Internet of Things and Privacy – Issues and Challenges", April 2021, https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-of-things-and-privacy-issues-and-challenges/#:~:text=The%20passive%20nature%20of%20many,not%20want%20their%20information%20collected (accessed 9 November 2022).
29. Steve Morgan, "Cybercrime to cost the world $10.5 trillion annually by 2025", *Cybercrime Magazine*, 13 November 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021 (accessed 9 November 2022).
30. Ciaran Martin, "Out-of-Control Cybercrime Will Cause More Real-World Harm", *WIRED*, 2 February 2022, https://www.wired.com/story/cyber-criminals-physical-harm/ (accessed 10 November 2022).
31. Forbes, "Fallout: The Reputational Impact of IT Risk", Forbes Insights, 2014, https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf (accessed 10 November 2022).
32. Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)", https://www.cisa.gov/circia (accessed 10 November 2022).
33. European Commission, "Cyber Resilience Act", 15 September 2022/updated 5 November 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (accessed 10 November 2022).
34. Cyber Security Agency Singapore, "Cybersecurity Labelling Scheme (CLS)", https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls (accessed 10 November 2022).
35. BitSight Technologies, "7 Cybersecurity Frameworks That Help Reduce Cyber Risk", 15 August 2022, https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk (accessed 10 November 2022).
36. National Cyber Security Centre, "Cyber Aware: Take your email security to another level", https://www.ncsc.gov.uk/cyberaware/home (accessed 10 November 2022).
37. South African National CSIRT, Cybersecurity Hub, Computer Security Incident Response Teams, 2016, https://www.cybersecurityhub.gov.za (accessed 29 November 2022).
38. Arm, "Arm Morello Program", https://www.arm.com/architecture/cpu/morello (accessed 10 November 2022).
39. Madeline Carr, et al., "Are smart home and wearable devices secure? A global consensus on 5 security must haves", World Economic Forum, Agenda, 15 February 2022, https://www.weforum.org/agenda/2022/02/5-security-must-haves-for-internet-connected-consumer-products (accessed 10 November 2022).
40. Ibid.
41. Datashield, "Why User Education is #1 in Cyber Resilience", https://www.datashieldprotect.com/blog/why-user-education-is-important-cybersecurity-resilience (accessed 10 November 2022).
42. National Institute of Standards and Technology, "Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software", updated 24 May 2022, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0#:~:text=By%20February%206%2C%202022%2C%20in,a%20consumer%20software%20labeling%20program (accessed 10 November 2022).
43. Deborah George, "IoT Manufacturers – What You Need to Know About California's IoT Law", *The National Law Review*, 28 January 2020, https://www.natlawreview.com/article/iot-manufacturers-what-you-need-to-know-about-california-s-iot-law (accessed 10 November 2022).
44. The World Bank, *The Internet of Things – The New Government to Business Platform: A Review of Opportunities, Practices, and Challenges*, 2017, https://documents1.worldbank.org/curated/pt/610081509689089303/pdf/Internet-of-things-the-new-government-to-business-platform-a-review-of-opportunities-practices-and-challenges.pdf (accessed 10 November 2022).
45. OECD, "One year of SME and entrepreneurship policy responses to COVID-19: Lessons learned to 'build back better'", 8 April 2021, https://www.oecd.org/coronavirus/policy-responses/one-year-of-sme-and-entrepreneurship-policy-responses-to-covid-19-lessons-learned-to-build-back-better-9a230220 (accessed 10 November 2022).

46. Emiliana Vegas, “School closures, government responses, and learning inequality around the world during COVID-19”, Brookings, 14 April 2020, https://www.brookings.edu/research/school-closures-government-responses-and-learning-inequality-around-the-world-during-covid-19 (accessed 10 November 2022).

47. Alliance for Affordable Internet, “Mobile Broadband Pricing”, 17 May 2022, https://a4ai.org/research/mobile-broadband-pricing (accessed 10 November 2022).

48. European Commission, “Statement by Executive Vice-President Margrethe Vestager on the initial findings of the Consumer Internet of Things Sector Inquiry”, June 2021, https://ec.europa.eu/commission/presscorner/detail/en/speech_21_2926 (accessed 10 November 2022).

49. Matt Leonard, “Declining Price of IoT sensors means greater use in manufacturing”, Supply Chain Dive, 14 October 2019, https://www.supplychaindive.com/news/declining-price-iot-sensors-manufacturing/564980 (accessed 10 November 2022).

50. International Telecommunication Union, “Facts and Figures 2021: 2.9 billion people still offline”, 29 November 2021, https://www.itu.int/hub/2021/11/facts-and-figures-2021-2-9-billion-people-still-offline (accessed 10 November 2022).

51. The World Bank, “Report: Universal Access to Sustainable Energy Will Remain Elusive Without Addressing Inequalities”, 7 June 2021, https://www.worldbank.org/en/news/press-release/2021/06/07/report-universal-access-to-sustainable-energy-will-remain-elusive-without-addressing-inequalities#:~:text=Since%202010%2C%20more%20than%20a,fragile%20and%20conflict%2Daffected%20settings (accessed 10 November 2022).

52. Interview with Greg Hrebek on 26 August 2022.

53. The World Bank, “Achieving Broadband Access for All in Africa Comes with a $100 Billion Price Tag”, 17 October 2019, https://www.worldbank.org/en/news/press-release/2019/10/17/achieving-broadband-access-for-all-in-africa-comes-with-a-100-billion-price-tag (accessed 10 November 2022).

54. Calum Handforth and Seth Tan, “Public-private collaboration key to connecting the unconnected”, United Nations Development Programme, 7 May 2021, https://www.undp.org/policy-centre/singapore/blog/public-private-collaboration-key-connecting-unconnected (accessed 10 November 2022).

55. See Will Burnfield, “How Can Public-Private Partnerships Increase Affordable Internet Access?”, Alliance For Affordable Internet (A4AI), 12 November 2015, https://a4ai.org/news/how-can-public-private-partnerships-increase-affordable-internet-access (accessed 10 November 2022).

56. See GSMA, “Principles for Driving the Digital Inclusion of Persons with Disabilities”, https://www.gsma.com/mobilefordevelopment/principles-for-driving-the-digital-inclusion-of-people-with-disabilities (accessed 10 November 2022).

57. Simon Hill, “Here’s What the ‘Matter’ Smart Home Standard Is All About”, *WIRED*, 4 October 2022, https://www.wired.com/story/what-is-matter (accessed 10 November 2022).

58. See EDISON Alliance [website], https://www.edisonalliance.org/home (accessed 10 November 2022).

59. Alliance for Affordable Internet (A4AI), “Meaningful Connectivity — unlocking the full power of internet access”, https://a4ai.org/meaningful-connectivity (accessed 10 November 2022).

60. GlobeNewswire, “With 10.10% CAGR, IoT Devices Market Size Worth USD 2724.42 Million by 2028 | Global IoT Devices Industry Trends, Share, Value, Analysis & Forecast Report by Facts & Factors”, 1 September 2022, https://www.globenewswire.com/en/news-release/2022/09/01/2508413/0/en/With-10-10-CAGR-IoT-Devices-Market-Size-Worth-USD-2724-42-Million-by-2028-Global-IoT-Devices-Industry-Trends-Share-Value-Analysis-Forecast-Report-by-Facts-Factors.html#:~:text=Key%20Insights%20from%20Primary%20Research,US%24%202%2C724.42%20Million%20by%202028 (accessed 10 November 2022).

61. The World Bank, “Urban Development”, 6 October 2022, https://www.worldbank.org/en/topic/urbandevelopment/overview#:~:text=Today%2C%20some%2056%25%20of%20the,people%20will%20live%20in%20cities (accessed 10 November 2022).

62. Interview with Fanyu Lin on 26 August 2022.

63. World Economic Forum, “Internet of Things: Guidelines for Sustainability”, January 2018, https://www3.weforum.org/docs/IoTGuidelinesforSustainability.pdf (accessed 11 November 2022).

64. Ibid.

65. Gigi Onag, “Surge in obsolete network devices pose cybersecurity risk”, FutureIoT, 12 June 2020, https://futureiot.tech/surge-in-obsolete-network-devices-pose-cybersecurity-risk (accessed 11 November 2022).

66. BBC, “Apple investigated by France for ‘planned obsolescence’”, 8 January 2018, https://www.bbc.com/news/world-europe-42615378 (accessed 11 November 2022).

67. Darrel Moore, “France confronts ‘planned obsolescence’ with repairability rating”, Circular, 19 October 2020, https://www.circularonline.co.uk/news/france-confronts-planned-obsolescence-with-repairability-rating (accessed 11 November 2022).

68. Thorin Klosowski, “What You Should Know About Right to Repair”, Wirecutter, 15 July 2021, https://www.nytimes.com/wirecutter/blog/what-is-right-to-repair (accessed 11 November 2022).

69. Mary K. Pratt, “IoT interoperability standards complicate IoT adoption”, IoTAgenda.com, 19 April 2021, https://www.techtarget.com/iotagenda/tip/IoT-interoperability-standards-complicate-IoT-adoption (accessed 11 November 2022).

70. Connectivity Standards Alliance, “Zigbee: The Full-Stack Solution for All Smart Devices”, https://csa-iot.org/all-solutions/zigbee (accessed 11 November 2022).

71. Pratik Sonawane, Manali Gurav and Riyaj Kazi, “Environmental Parameters Monitoring Using WSN”, National Conference on Information, Communication and Energy Systems and Technologies 2019, *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 5, no. 7, March-April 2019.

72. Laura Lovett, “Eko lands EUA for device that helps detect coronavirus patients with cardiac complications”, MobiHealthNews, 14 May 2020, https://www.mobihealthnews.com/news/eko-lands-eua-device-helps-detect-coronavirus-patients-cardiac-complications (accessed 11 November 2022).

73. Oura, “Can Researchers Use Oura To Spot Signals Associated with COVID-19?”, 2 March 2022, https://ouraring.com/blog/detect-covid-19 (accessed 11 November 2022).

74. Muhammad Umair, et al., “Impact of COVID-19 on IoT Adoption in Healthcare, Smart Homes, Smart Buildings, Smart Cities, Transportation and Industrial IoT”, *Sensors*, vol. 21, no. 11, 1 June 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8199516 (accessed 11 November 2022).

75. CISION PR Newswire, “New survey finds 70% of consumers improved home during COVID-19, more than half used smart devices”, Xiaomi, 6 January 2021, https://www.prnewswire.com/news-releases/new-survey-finds-70-of-consumers-improved-home-during-covid-19-more-than-half-used-smart-devices-301201817.html (accessed 11 November 2022).

76. Knut Alicke, Richa Gupta and Vera Trautwein, “Resetting supply chains for the new normal”, McKinsey & Company, 21 July 2020, https://www.mckinsey.com/capabilities/operations/our-insights/resetting-supply-chains-for-the-next-normal (accessed 11 November 2022).

77. GlobeNewswire, “Industrial IoT (IIoT) Market Worth $263.4 Billion by 2027 – Market Size, Share, Forecasts, & Trends Analysis Report with COVID-19 Impact by Meticulous Research®”, 30 September 2021, https://www.globenewswire.com/news-release/2021/09/30/2306043/0/en/Industrial-IoT-IIoT-Market-Worth-263-4-Billion-by-2027-Market-Size-Share-Forecasts-Trends-Analysis-Report-with-COVID-19-Impact-by-Meticulous-Research.html (accessed 11 November 2022).

78. Tarek Sultan, “5 ways the COVID-19 pandemic has changed the supply chain”, The Davos Agenda/World Economic Forum, 14 January 2020, https://www.weforum.org/agenda/2022/01/5-ways-the-covid-19-pandemic-has-changed-the-supply-chain/ (accessed 11 November 2022).

79. Absalom E. Ezugwu, et al., “A Novel Smart City-Based Framework on Perspectives for Application of Machine Learning in Combating COVID-19”, *BioMed Research International*, vol. 2021, https://www.hindawi.com/journals/bmri/2021/5546790 (accessed 11 November 2022).

80. See C. Jason Wang, et al., “Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing”, *Journal of the American Medical Association*, vol. 323, no. 14, pp. 1341-42, 3 March 2020, https://jamanetwork.com/journals/jama/fullarticle/2762689 (accessed 11 November 2022).

81. Interview with Fanyu Lin on 26 August 2022.

82. Apple, “Apple and Google partner on COVID-19 contact tracing technology”, 10 April 2020, https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology (accessed 11 November 2022).

83. See World Economic Forum in collaboration with the Global Internet of Things Council and PwC, *State of the Connected World 2020 Edition*, Insight Report, December 2020.

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