The bridge to possible

Ten Tech Policies to Power the Future

The bridge to possible

Cisco's Ten Points

AI and Cybersecurity

1. Leverage AI and cybersecurity to deploy safe and secure infrastructure ...pg.3
2. Remove unsupported and outdated digital devices from critical networks ...pg.4
3. Set rules for government handling of security vulnerabilities ...pg.5

Workforce and Talent Development

4. Empower the next generation with 21st-century digital and AI skills ...pg.6

Government Data Demands

5. Agree on frameworks for government data demands ...pg.7

Connectivity

6. Implement connectivity strategies that bolster networks ...pg.8
7. Allocate sufficient spectrum to reap the full benefits of Wi-Fi ...pg.9

Trade

8. Support free trade and green flows of goods and services ...pg.10
9. Enshrine cross-border data flows in trade and digital agreements ...pg.11

Sustainability

10. Enable the clean and green transition with digital solutions ...pg.12

01 Leverage AI and cybersecurity to deploy safe and secure infrastructure

ISSUE

Global cyberattacks are growing in sophistication, overwhelming defenses that cannot keep up at a human scale. AI has emerged as a key solution that can enhance cybersecurity by analyzing telemetry data to detect anomalies early and efficiently, distinguishing between legitimate and malicious activities in real time, and enabling swift auto-remediation.

AI also introduces new threats, potentially allowing individuals to conduct advanced attacks without needing extensive technical skills. As many organizations rush toward the implementation of AI as part of their business processes, there are potential new threats that arise from the use of the AI system itself. To provide resiliency for applications, there is a need for safe and secure underlying network infrastructure powered by robust AI detection and protection capabilities.

ADDITIONAL CONTEXT

AI's ability to work faster than humans and at network scale is essential to stay ahead of evolving threats. By combining AI and cybersecurity capability with human intelligence, we stand a better chance of shifting the advantage from attackers to defenders—creating a future where technology and infrastructure are more secure.

There needs to be clear principles and guidelines for responsible and inclusive AI use to mitigate the current and emerging risks. These will serve as guardrails to counter security and privacy threats and other concerns such as inaccuracy and bias. Cisco has articulated its Responsible AI Principles—based on transparency, fairness, accountability, privacy, security, and reliability—as governance tenets for developing, deploying, and using AI capabilities.

BEST PRACTICES

Adherence to the latest security research and guidelines—such as those from the National Institute of Standards and Technology (NIST), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Organization for the Advancement of Structured Information Standards (OASIS), and the Open Worldwide Application Security Project (OWASP)—is crucial for organizations to mitigate adversarial risks and align with advanced security practices. Embedding AI-relevant security controls in Secure Development Lifecycle processes is essential—involving supply chain audits, data integrity reviews, and adaptability to threats—to build resilient systems and infrastructure. Data privacy must be prioritized in AI training and operations with robust protections throughout data lifecycles, especially for sensitive information. To counteract AI attacks and misuse, robust moderation tools and comprehensive monitoring are necessary to detect and block malicious prompts and ensure output integrity.

02 Remove unsupported and outdated digital devices from critical networks

ISSUE

Operators of critical infrastructure should be required to remove connected devices from their networks that are no longer subject to software updates by their manufacturers. While exceptions may be justified according to the risk presented, the default policy should be to migrate to a supported product before it reaches end of life.

Multiple governments are adopting legal frameworks or guidance to require critical infrastructure operators to adopt cybersecurity measures and manufacturers to ensure their products are supported. A binding measure on removing obsolete devices would address the gap between the two.

ADDITIONAL CONTEXT

Patching software is a basic tenet of security. Removing end-of-life devices for which updates no longer exist should be low-hanging fruit.

A 2020 NTT study, however, found that 48% of devices on global organizations networks are unsupported or ageing. The problem may be more acute in specific sectors. A Forescout report claims 71% of medical devices were running on obsolete or near-obsolete software in 2019. The real-world impacts can be significant. For example, unpatched and end-of-life software enabled the WannaCry ransomware attack to infect 300,000 machines around the world in 2017.

The importance of keeping technology up to date for security outcomes is recognized by security professionals. Cisco's Security Outcomes Study (2021) surveyed 5100 security and IT staff, who rated a proactive technology refresh study as the number one factor (out of 25) in ensuring a successful security program. In addition, it came out top in subcomponents of a successful program—such as keeping up with business, avoiding major cyber incidents, and a cost-effective security program.

BEST PRACTICES

Various cyber agencies, such as Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. and the National Cyber Security Centre (NCSC) in the UK, recommend removing obsolete products from organizations' networks. Japan's Economic Security Law (2022) takes this further by requiring critical infrastructure operators to submit "introduction plans" for equipment, with detailed policy further specifying this prohibits the use of unsupported devices.

03 Set rules for government handling of vulnerabilities

ISSUE

Some governments are researching, developing, purchasing, and licensing zero-day vulnerabilities and their exploits. Governments should publicly disclose their policies for handling and disclosure of security vulnerabilities, including sufficient safeguards and a presumption towards immediate disclosure and inclusion.

Many countries have adopted Coordinated Vulnerability Disclosure (CVD) policies relating to policies and protections for third-party researchers to identify and communicate vulnerabilities to public and private organizations, and their handling by civil cyber authorities. Only a select few countries, however, provide rules for government exploiting vulnerabilities for their own ends and when to share those vulnerabilities with vendors.

ADDITIONAL CONTEXT

We are concerned governments may be tempted to retain vulnerabilities—rather than disclose them to manufacturers—so that they can be exploited by intelligence or law enforcement communities. This carries substantial economic, reputational, and social risk for companies and individuals, which may not be appropriately accounted for in the decision-making process.

Government security agencies cannot assume that vulnerability information can be retained indefinitely without harm to the public. It may be leaked, stolen, or independently rediscovered. The Heartbleed bug was allegedly known to elements of the intelligence community prior to its public disclosure in 2014. Zero-day vulnerabilities held by the CIA, as well as details of tools to exploit them, found their way into the hands of WikiLeaks as part of the Vault7 leaks. And one study estimated that 15–20% of uncovered vulnerabilities will be independently rediscovered within a year.

BEST PRACTICES

The U.S. Vulnerabilities Equities Process (VEP) was updated in 2017 with the VEP Charter. The UK's Government Communications Headquarters (GCHQ) adopted a VEP process in November 2018. The Dutch government has outlined some of the considerations for use of vulnerabilities to hack devices by intelligence agencies and law enforcement and the means of oversight. How detailed the policy needs to be depends on the existence and level of authorities' offensive cyber capabilities. Even those countries with limited or non-existent programs, however, should bear in mind the benefit of being transparent about that to stakeholders.

04 Empower the next generation with 21st-century digital and AI skills

ISSUE

In the next five years, the World Economic Forum predicts that 23% of jobs globally will evolve due to the transformation of industry—notably through AI and other text, image, and voice processing technologies.

Against the dooming idea that AI will replace jobs, our recent Cisco AI Readiness Index reveals that AI can be a channel for worker growth. AI implementation demands new skills, and even companies who are well-resourced need more (or different) talent to be successful. A top priority for all governments is to build a future-ready workforce.

ADDITIONAL CONTEXT

The advancement of AI and automation necessitates a focus on reskilling and education to enhance human productivity and unlock new capabilities. A joint study by Cisco and Oxford Economics indicates that while some jobs may be lost, others will emerge due to automation's productivity gains. There is, however, a major digital talent shortage impacting industry—leading to loss of growth and profitability, less productivity, increased workload, and lack of innovation and service quality. With 98% of businesses looking at investing in upskilling employees on AI (Cisco AI Readiness Index), there is an urgency to empower citizens and employees with basic digital skills and specialist trainings.

Education systems must adapt through policy reform. Collaboration between governments and businesses is vital, with initiatives like Cisco's Networking Academy providing digital skills training for individuals at any career stage.

The recent launch of the Cisco-led "AI-Enabled ICT Workforce Consortium"—which was catalyzed from the work of the U.S.-EU Trade and Technology Council (TTC) Talent for Growth Task Force—provides an important foundation for understanding the skills needed for tomorrow's jobs and how we can best prepare for those skills.

BEST PRACTICES

While each region may have different levels of maturity and needs, businesses should have access to a global skilled workforce to succeed across borders.

Countries like Singapore and the U.S. have implemented strategies to upskill and reskill their workforce at all levels, while other countries such as Sweden or Canada have taken a more specialized approach. The Singapore strategy includes initiatives to build a pipeline of AI researchers; an expansion of the AI practitioner workforce through investment in training, scholarships, and international internships; and support for mid-career professionals transitioning to AI roles.

In the context of the U.S.-EU TTC, both governments have rightly identified skills as an area for cooperation, and the TTC Talent for Growth Task Force serves as a catalyst for innovative skills approaches. Organizations such as the World Economic Forum have set up a growing network of countries and partners to start a "reskilling revolution".

05 Agree on frameworks for government data demands

ISSUE

For reasons of expedience and efficiency, certain governments—including the EU and the U.S.—consider it necessary to enable law enforcement authorities (LEAs) to make demands directly to tech companies for data related to criminal investigations, regardless of location of data. This should be conducted under a government-to-government framework that provides legal certainty for entities from which the data is sought, that addresses potential conflicts in law, and that creates safeguards to protect the fundamental rights of the individuals to whom the data relates.

ADDITIONAL CONTEXT

Over the last decades, LEAs have become increasingly interested in electronic evidence to supplement physical evidence in criminal investigations. In a world where international data flows are the norm, the relevant data does not necessarily sit within national borders. As a result, the nature of access demands has led to a dynamic whereby the data may be subject to laws of multiple jurisdictions. Where such demands are made unilaterally, without proper concern for the legal framework in the other jurisdiction, this can put companies in a position where to comply with one law is to breach the law elsewhere.

The risk of unauthorized foreign government data access is one of the primary drivers for the emergence of strict data sovereignty controls on the location, operation, and ownership of cloud services provided to public sector and regulated customers. Such sovereign architectures offer customers greater control over the cloud environment but significantly increase cost, restrict availability and features, limit innovation, and can be detrimental to security. As such, it is a far better policy approach to relieve such tensions through government frameworks.

BEST PRACTICES

The OECD adopted the first intergovernmental agreement on common approaches for safeguarding privacy and other human rights when accessing personal data for law enforcement and national security purposes—providing a strong baseline for signatory countries to build on. Both the EU (e-Evidence Regulation) and the U.S. (CLOUD Act) have adopted foundational legislation for bilateral agreements.

The U.S.-UK Data Access Agreement entered into force in October 2022, followed in January 2024 by an agreement with Australia.

06 Implement connectivity strategies that bolster networks

ISSUE

As policymakers look to digital infrastructures to enable the applications of the future, they should adopt a bold industrial vision for the backbone of the Internet. There's no digital transformation without networks.

We need a combination of expertise and specialization of Internet stakeholders and technologies—not only 5G/6G, FTTH, Wi-Fi, and satellites but also technologies supporting the ecosystem (e.g., data centers or cloud solutions). All are playing a critical role in meeting public policy goals on digital infrastructure, transformation, skills, sustainability, and security.

Therefore, similarly to the U.S. CHIPS Act and the EU Chips Act, governments should build new, open, and collaborative alliances for connectivity to incentivize innovative partnerships and address the broadband needs of businesses and citizens. In addition, they should review telecom rules and regulations with the goal to identify reforms that can enable more creative and cross-border business models and services, better leverage existing public funding, and move them one step further toward spectrum coordination and harmonization.

ADDITIONAL CONTEXT

Deployment of broadband globally is uneven and often fails to keep up with the latest technologies and market needs. In the last decade, the financial health of telecom operators and their ability to invest in networks and new services has been impacted by lack of harmonization, stringent rules, little flexibility on government aid, and difficulties to scale up solutions.

As enterprises embrace cloud-based applications and digital platforms to transform how they operate and engage with their customers, they should be able to operate more freely in this new and different landscape to replicate their earlier success of selling traditional connectivity services—notably through Network-as-a-Service (NaaS), edge cloud, managed security services, and the green and digital transformation. All of which can help them monetize their investments in the networks.

BEST PRACTICES

With the $42.5 billion broadband infrastructure funding included in the U.S. Infrastructure Investment and Jobs Act, the U.S. has adopted a bold vision for broadband planning, digital inclusion, and deployment projects.

The UK's Wireless Infrastructure Strategy is another successful example that prioritizes close engagement with industry and local bodies across the country, bridges and coordinates priorities across government departments, removes practical barriers to investment and innovation, and explores potential market consolidation.

In Singapore, the government plans to upgrade its nationwide broadband network to 10 Gbps with through $74 million investment. By 2028, more than 500,000 households would be able to benefit from 10 Gbps speeds. The upgrade is planned in anticipation of data-intensive tools such as AI, VR, and smart homes.

07 Allocate sufficient spectrum to reap the full benefits of Wi-Fi

ISSUE

Cisco's connectivity goals are simple. We want to securely connect everything to make anything possible. Our vision is a "network of networks" focusing on customer and application needs, rather than favoring one technology over another.

While 5G remains the preferred technology for wide-area coverage, Wi-Fi 6 and 7 continue to be favored for indoor use due to their much lower deployment costs.

With the emergence of hybrid work and new applications, indoor connectivity relies on high-quality Wi-Fi. The Wi-Fi ecosystem is mature, with enterprise and consumer access points and clients readily available. While there has been some progress with mobile use in the band, actual mobile operations are years away.

With billions of new wireless devices crowding spectrum bands every year, this scarce resource must be properly managed. To power the digital economy, governments should allocate the entire 6 GHz band for unlicensed use (i.e., Wi-Fi) and allow indoor use as an immediate measure.

ADDITIONAL CONTEXT

Approximately 90% of indoor traffic overall and up to 80% of mobile traffic are carried indoors on Wi-Fi. With the rapid growth of FTTH broadband networks, we know that additional Wi-Fi spectrum will be badly needed within only a few years.

Should the 6 GHz band be opened to Wi-Fi, the global economic value of Wi-Fi could reach $4.9 trillion in 2025—driven by a boost in IoT development, the growing adoption of augmented and virtual reality use cases, and the increasing importance of free Wi-Fi.

Governments should open the full band, not just the lower part. The difference between 500 and 1200 MHz for Wi-Fi is shown in the number of users and applications that will be able to operate advanced applications simultaneously. This will affect not only large-scale operations like factories and warehouses but also schools and homes. It is the difference between only four to eight students in a classroom using AR/VR and the entire class doing so simultaneously.

BEST PRACTICES

Today, countries representing 40% of global GDP (U.S., Korea, Canada, Saudi Arabia, etc.) have allocated the 6 GHz entire band for Wi-Fi. The U.S. and Canada will begin standard power Wi-Fi 6 GHz operations in 2024.

Next to ongoing studies looking at hybrid sharing, governments could also explore spectrum sandboxes (i.e., isolated testing environments)—such as the pilot outlined in UK regulator Ofcom's spectrum roadmap—to better understand the potential benefits.

08 Support free trade and green flows of goods and services

ISSUE

The plurilateral Information Technology Agreement (ITA) was one of the most successful agreements for businesses and consumers. By cutting tariffs on trade across millions of ICT products and their components, the ITA has supported the development and diversification of ICT global value chains and facilitated greater adoption of ICT products, which has helped bridge the digital divide and equipped businesses for their digital transformation goals.

Governments should look at facilitating the trade of green goods and services at bilateral and international level, notably via:

- A Circular Economy Trade Agreement in the World Trade Organization (WTO) with electronic customs facilitation of e-waste, distribution and repair services;
- An Information Technology Agreement for energy efficient products, building upon the past work of the Environmental Goods agreement;
- Alignment on Digital Product Passport standards across the globe, balancing transparency with strong intellectual property right protections.

ADDITIONAL CONTEXT

Energy- and resource-efficient technologies and services are critical to the transition to a low-carbon economy and to adapt to climate change.

The WTO simulations indicate that by cutting tariffs and applying a 25% reduction in the *ad valorem* equivalent of non-tariff barriers on energy-related environmental goods and environmentally preferable products, new trade opportunities would be created for businesses estimated at $116 billion for energy-related goods and at $10 billion for environmentally preferable products. This would result in a 0.8% global GDP increase relative to the baseline in 2030 while also reducing CO2 emissions.

BEST PRACTICES

As governments consider trade agreements with other countries, they should identify methods that can better enable the flow of green goods and services. Currently, only two trade agreements in the world—negotiated by New Zealand with the Separate Customs Territory of Taiwan, Penghu, Kinmen, and Matsu and the United Kingdom—have explicitly removed tariffs on a list of specific environmental goods. We have also seen recent regional efforts, such as the U.S.-Canada-Mexico Agreement (USCMA), address potential non-tariff measures on environmental goods and services.

09 Enshrine cross-border data flows in trade and digital agreements

ISSUE

The digital economy has been a driver of economic growth in countries around the world, and organizations of all sizes and industries depend on the movement of data to thrive. This need for efficient and effective cross-border data flows will only accelerate in the era of AI and as other innovations emerge. However, some governments have called for a policy of data localization—believing that keeping data onshore will provide better security and protection. The reality is that the ability for data to be secured has little to do with the location of the data but with the practices of the data custodian.

ADDITIONAL CONTEXT

The disruption of cross-border data flow would negatively impact the economic development of a country—with the cost of data localization outweighing perceived benefits. Allowing the free flow of data will not only allow domestic companies to access best-in-class services available globally but also enable such companies to reach a regional and global market for their own products and services. The ability to analyze data across borders allows greater visibility of threats and fraudulent behavior—providing better protection against bad actors for both consumers and businesses. A diversity of data storage locations across geographical boundaries ensures greater resiliency against disruption and attacks.

BEST PRACTICES

The government of Japan proposed the Data Free Flows with Trust Initiative (DFFT) as a new model for global data governance. The goal: support the free flow of data across borders while ensuring trust in privacy and security. Japan has infused the DFFT into new trade agreements, such as the U.S.-Japan Digital Trade Agreement and the Japan-UK Comprehensive Economic Partnership Agreement. The DFFT is committed to build on existing and emerging data governance models, including the Global Cross Border Privacy Rules (CBPR) Forum. The CBPR system is a voluntary, multilateral, and enforceable global privacy certification that companies can use to demonstrate compliance with internationally recognized data privacy principles. The U.S. remains committed to the OECD DFFT and Global CBPR work even as it continues to evaluate its approach to digital trade issues. Other countries—including the EU, the UK, and many countries in Asia—continue to pursue digital trade agreements. For example, the EU-UK Trade and Cooperation Agreement includes a specific “cross border data flows” provision.

10 Enable the clean and green transition with digital solutions

ISSUE

Technology is a crucial enabler for the sustainability transition and for optimizing value chains. Innovation enables us to rethink business models in ways that are digital and low carbon but also that improve individual wellbeing and create opportunities for communities.

The European Union put the twin green and digital transition at the heart of European recovery with NextGenEU, while the U.S. Inflation Reduction Act made targeted investments in clean energy. However, there remains ample room for improvement in aligning the green, energy, and digital agendas in a way that catalyzes industrial success and fosters positive social impact through thoughtful regulation and incentives.

It is now time to support the deployment of the enablers of the green and digital transition across industry verticals (e.g., agriculture, manufacturing, health care, transportation, etc.). Efforts such as public-private partnerships, incentives and tax systems that encourage clean investments, and responsible deregulation can accelerate this work.

ADDITIONAL CONTEXT

Our 2023 Cisco Broadband survey revealed that 65% of consumers in Europe, the Middle East, and Africa are now concerned about the carbon footprint of their broadband—with young people the most concerned.

This supports a wider market trend that shows widespread consumer awareness around the environmental impact of the products they use and a demand for companies to step up and mitigate their impact on the planet.

The green and digital transformation is a dual challenge that the public and private sectors must come together to solve by creating, developing, enabling, and investing in technology solutions to reduce carbon emissions.

Governments have an important role to play in defining the standards around science-based targets, transparent ESG management, and reporting. In doing so, they should not lose sight of critical aspects—such as local incentives and interoperability at the international level—to help businesses scale up their sustainability ambitions.

BEST PRACTICES

The European Commission and Parliament have been the first to launch a green digital coalition, gathering 30+ tech companies to develop the key performance indicators, methodologies, and solutions to help enable industry verticals. Governments should continue to support adoption of solutions which can help businesses to become greener and also compliant with sustainability-related regulation.

Ten Tech Policies to Power the Future