2020 IN REVIEW

Cybersecurity Tech Accord
The voice of the technology industry on international cybersecurity

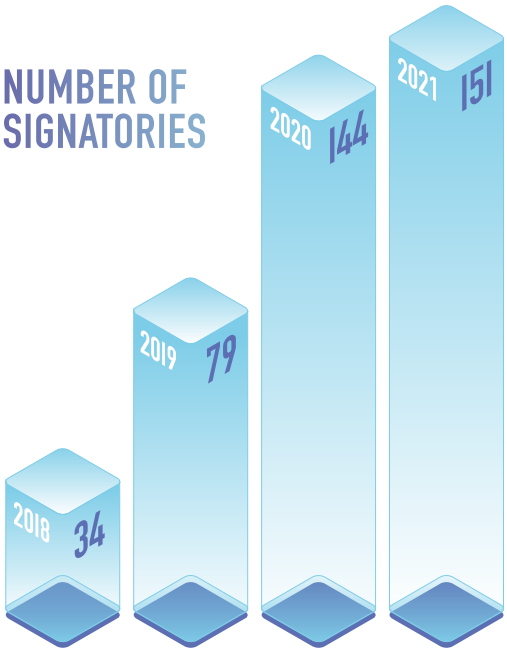
CONTENTS

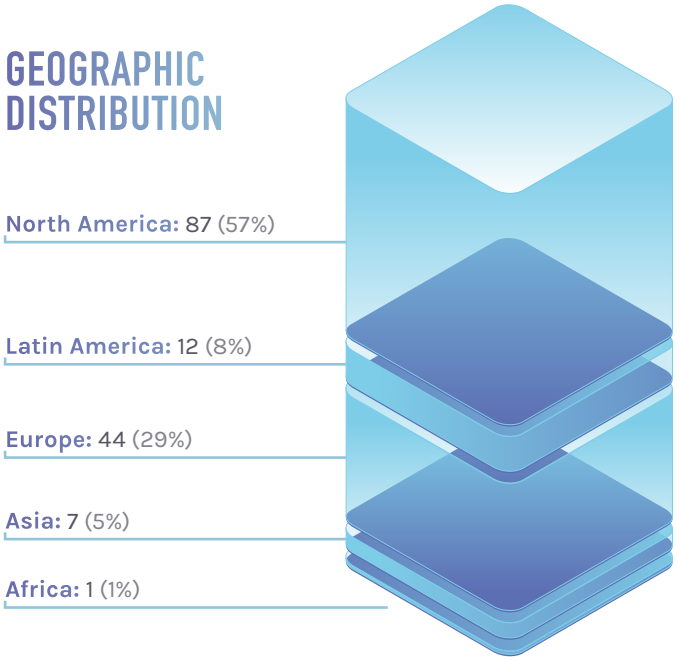
OUR COMMITMENT

A growing coalition to protect technology users and customers everywhere

151 signatories are committed to advancing the mission of the Cybersecurity Tech Accord and are united by common values as reflected in our core principles.

Our growth:





About the Cybersecurity Tech Accord

Founded in 2018, the Cybersecurity Tech Accord is a coalition of over 150 global technology firms committed to advancing trust and security in cyberspace. We firmly believe that protecting the online environment is in everyone's interest and that all stakeholders have a role to play. To this end, we strive to be the industry's voice on peace and security in cyberspace. We are committed to responsible behavior that helps protect and empower our users and customers, thereby improving the security, stability and resilience of our online world.

Our four founding principles:

1. Stronger Defense:
We will protect all of our users and customers everywhere.

2. No Offense:
We will oppose cyberattacks on innocent citizens and enterprises from anywhere.

3. Capacity Building:
We will help empower users, customers and developers to strengthen cybersecurity protection.

4. Collective Response:
We will partner with each other and with likeminded groups to enhance cybersecurity.

A Year In Review:
Letter From The Secretariat

The last year has been a year of reflection for everyone – reflection both on our limitations as well as on our collective resilience and ability to abruptly adapt to changing circumstances and new ways of living amidst a global pandemic. For many of us, digital technology was the lynchpin that allowed us to continue working despite being unable to set foot in a physical office, to learn and connect despite social distancing, and to reduce the spread of COVID-19 by tracking the disease and supporting critical medical advancements. This past year our technology needs increased and evolved more dramatically than ever before, which meant new and more dynamic cyber risk as well.

As the world became more reliant on technology, malicious actors online, with motives ranging from criminal to geopolitical, seized new opportunities to exploit vulnerabilities created by this new reality. Every country in the world **fell victim to at least one COVID-19 themed attack during last year,** as 2020 set new records for the sheer number of sophisticated threats and **significant incidents** overall. Hackers and criminal groups were not alone in taking advantage of this time of upheaval. State actors also became increasingly active in this space. Not only have state-led and -sponsored cyberattacks been on the rise, but the range of targets has also expanded to include now healthcare organizations that are already overwhelmed with COVID-19 patients and even entire technology supply chains. The attack on software company SolarWinds is just one of the most recent and devastating examples to bring attention to a lack of clear boundaries when it comes to state behavior in cyberspace.

Our signatories believe in a collective and unified response to this escalating threat environment, as no single organization, government or individual is equipped to deal with these challenges alone.

The Cybersecurity Tech Accord was launched in April 2018 with 34 global technology companies committed to protecting users and customers everywhere from evolving cyber-threats; three years later, our mission is more important than ever before. Standing up to these evolving and unprecedented challenges, and working together to address them, is core to our principles. To celebrate our anniversary, we're publishing our third annual report, which reflects how our principles have guided our efforts to improve the security, stability, and resiliency of cyberspace from April 2020 through March 2021. This report also demonstrates our signatories' efforts toward creating a safer online world, promoting the principles of the Paris Call Trust and Security in Cyberspace, advancing capacity building through cyber hygiene, and contributing to requests for response from governments and international forums.

We recognize the need to continue in this effort and do our part to not only protect the online environment but also to serve as the industry's voice in favor of greater international political cooperation to mitigate the threats emanating from states and other malicious actors online.

We are excited about our progress made and hope more technology companies will join us in 2021 to help make cyberspace more secure.

Annalaura Gallo
Head Secretariat

Signatory Spotlight:
A discussion with DXC Technology

Adding signatories means gaining new perspectives and fostering collaboration. Mark Hughes, SVP Offerings and Strategic Partners, reflects on DXC Technology's role as a Cybersecurity Tech Accord signatory and the company's commitment to improving the security, stability and resilience of cyberspace.

1. What is the greatest cybersecurity threat that organizations face today?

   We believe recent cyberattacks such as the SolarWinds hack demonstrate key stakeholders' inadequate appreciation and understanding of the extensive interdependencies and gaps vulnerable to exploitation by bad actors. As threat actors become increasingly sophisticated, these stakeholders will urgently need to leverage stronger public-private collaboration. Likewise, more identification and response planning for interdependencies at the company or government segment level is critical.

2. What motivated your company to join the Cybersecurity Tech Accord as a signatory?

   DXC Technology is a global provider of IT services to thousands of commercial and public sector customers who rely on safe and stable IT infrastructure and services every day. Our supply chain and third-party providers of networks, equipment, software, cloud and other services are extensive and vulnerable to cybersecurity attacks. In providing IT services and relying on our providers and partners, DXC's utmost concern is ensuring a safe and secure cyberspace, not only for all these entities to conduct business but also for our customers. We fully support the Cybersecurity Tech Accord's mission and joined to participate in promoting 'a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats.

3. What unique perspective on security challenges do you hope your company can bring to the Cybersecurity Tech Accord?

   DXC is one of the world's largest IT infrastructure providers servicing thousands of customers. We provide a secure and stable infrastructure and services environment every day to support our customers, so we are uniquely positioned to see the impact of malicious cyber events first-hand. Through our work, we have gained deep knowledge and experience in cybersecurity matters and look forward to contributing insights to the Cybersecurity Tech Accord as it develops its future thinking.

4. How does your company live up to the Cybersecurity Tech Accord principles?

   DXC fully supports the Tech Accord's four principles of strong defense, no offense, capacity building, and collective response. Equal protection online is core to our service offerings, and we will continue to support this principle. Likewise, we would never knowingly undermine the security of the online environment as our highest priority is protecting against any efforts to tamper with our services and the greater ecosystem. Finally, we believe cybersecurity is a shared responsibility and that the most effective way to increase the security of cyberspace is through a collective response to address critical challenges. We look forward to participating in crafting our collective response with other Cybersecurity Tech Accord members.

5. Where do you see the Cybersecurity Tech Accord making the biggest impact?

   We believe the efforts of the Cybersecurity Tech Accord member companies, as a growing cohesive and global community, will positively impact the thinking and actions of the worldwide cybersecurity policy community as norms and standards continue to develop.

Mark Hughes
SVP Offerings and Strategic Partners

LIVING UP TO OUR PRINCIPLES

Since the Cybersecurity Tech Accord's inception, our four foundational principles have guided our work and commitments as a group, informing our efforts across initiatives and supporting signatory companies in doing more to improve cybersecurity for users and customers everywhere. While the journey ahead to build a safer cyberspace remains long, and cyber-threats are evolving at great speed, we strongly believe that living up to these principles and continuing to engage in collective action will bring us closer to our common objective of securing our shared online environment.

Principle 1: Stronger Defense

Our signatories believe all users and customers deserve protection online – whether an individual, organization or government – irrespective of their technical acumen, culture, location, or the motive for any malicious attack. To this end, the Cybersecurity Tech Accord signatories strive to design and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability and severity of vulnerabilities.

Creating a safer and more secure online world

Cybersecurity innovation. The Cybersecurity Tech Accord believes the security and stability of our online environment needs fresh thinking and innovation. This is why we **partnered** with the United Nations Office of Disarmament Affairs and the United Nations Envoy on Youth in sponsoring the Apps 4 Digital Peace contest. In 2020, this exciting cybersecurity competition for young innovators concluded with the announcement of the Cybersecurity Tech Accord's top three contest winners. Each **winner**, FSociety, Maktab, and Cyber Teens, was selected for their new and innovative ideas that help limit the use of the internet as a domain of conflict or harm and increase the stability of our online environment.

$30,000 Total
awarded to top three
competition winners

Esteemed panel
of 6 Judges

Winners:
FSociety, Maktab and Cyber Teens

WHOIS data access. As an industry, we understand that speed matters in cybersecurity investigations in order to more effectively defend against malicious actors. Since the Cybersecurity Tech Accord's inception and increasingly over the past year, we have **encouraged** the Internet Corporation for Assigned Names and Numbers (ICANN), as well as the relevant authorities at EU level, to work on a solution that restores third-party access to the WHOIS data – which have previously served as the property records of the internet. Issues like these threaten the security and stability of our shared cyberspace and so we have demanded urgent redress to support strong security measures and accountability online. To this end, the Cybersecurity Tech Accord joined in **signing on to a letter** along with 20 other organizations, calling for swift action to be taken by the European Commissions to restore access to WHOIS. In addition, we **provided feedback** regarding the latest recommendations produced by ICANN's Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data (EPDP). In our feedback, we encouraged ICANN to halt the EPDP proposed policies and related implementations in light of legislative developments in the European Union and in the United States that could be more impactful in helping restore access to WHOIS data.

> "Access to WHOIS data is a critical component to safeguard brand owners and their consumers from financial loss and safety issues. As a Cybersecurity Tech Accord signatory, CSC supports sustainable measures that mitigate digital brand abuse, domain spoofing, domain/DNS hijacking, phishing, and fraud."
>
> **Vincent D'Angelo**
> Global Director, Corporate Development and Strategic Alliances, GSC Global

As the WHOIS data is essential to executing timely cybersecurity investigations and access remains restricted due to the misapplication of the General Data Protection Regulation (GDPR), we will continue to make this a central part of our advocacy efforts in the year ahead.

Coordinated vulnerability disclosure (CVD) policies. We recognize that vulnerability disclosure policies are vital to addressing threats and mitigating potential risks or harm to users. They are at the core of a collaborative approach to cybersecurity, creating a clear process for organizations and individuals to report any known vulnerability to the relevant vendor and trust that it will be addressed expeditiously. In 2019, we committed to having our signatory companies each develop and adopt a policy on vulnerability disclosure. This commitment has persisted while our ranks have grown, and today more than 100 of our signatory companies have adopted a vulnerability disclosure policy, which are available for review on our **website**, to serve as a helpful example for others across the industry. In addition, we have **worked** closely with the OECD Working Party on Security in the Digital Economy, on initiatives including their paper on Responsible Management and Disclosure of Vulnerabilities. We will continue to promote the adoption of CVD policies as a best practice in the next year, to help enable security researchers and ethical hackers to understand how to report vulnerabilities securely.

Understanding perceptions and the shifting landscape

With the rise of sophisticated attacks, organizations today of all sizes find themselves having to defend against advanced threats while conducting business online. Last year, we partnered with the Economist Intelligence Unit on a new study: **"Securing a shifting landscape: Corporate perceptions of nation-state cyber-threats"** to better understand the perceived challenges of nation-state cyber threats, particularly during times of disruption and in the wake of significant incidents. The results revealed an urgent need for a fundamental shift in security planning and effective policy solutions at the national and international levels. They also informed and validated the need for broader inclusion and involvement of the multi-stakeholder community, which aligns with the Cybersecurity Tech Accord's core principles.

As a voice of the technology industry on matters of peace and security in cyberspace, we look forward to leveraging the survey results and our understanding of corporate perceptions to engage in dialogue with multi-stakeholders on the escalating nation-state threats, and advocate for solutions that bring forward recommendations about how to get ahead of these challenges.

Principle 2: No Offense

Our signatories are committed to protecting against efforts to misuse, tamper with, or exploit technology products and services, and will not help any individual or organization use our products and services to launch cyberattacks against customers or users anywhere, or to otherwise knowingly undermine the security of the online environment

Calling for responsible behavior at the United Nations

One of the core tenants of the Cybersecurity Tech Accord is that, as an industry, we are not interested in playing a role in escalating conflict between states and other actors online or engaging in activities that would harm the security of users and customers anywhere. Therefore, we have consistently called on governments to uphold international law in cyberspace and to implement norms for responsible behavior agreed upon by the United Nations (UN). Over the past year, we continued to participate in the multi-stakeholder dialogues that took place alongside cybersecurity discussions at the UN and took every opportunity to contribute our input to the UN's Open-Ended Working Group (OEWG) on ICT in the context of international security. This included participating in live consultations on the OEWG's work, written **contributions**, and responding to **requests for input** from governments participating in the working group. In addition, we joined over 80 international leaders and organizations in signing a **letter** to His Excellency Volkan Bozkir, the new President of the United Nations General Assembly, urging him to make digital trust and security a priority for his presidency.

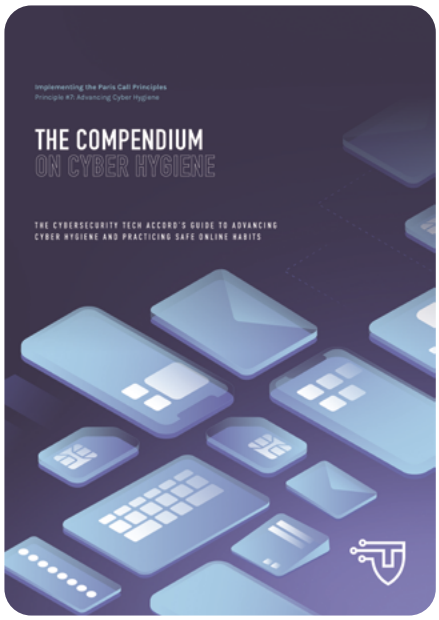
Promoting the Paris Call principles

As an early and vocal supporter of the **Paris Call for Trust and Security in Cyberspace**, the landmark and first-of-its-kind international multi-stakeholder compact on cybersecurity, we continued to commit ourselves to taking forward the agreement's nine principles, focusing on two in particular where our industry has unique expertise.

Principle #7:
Support efforts to strengthen an advanced cyber hygiene for all actors.

Principle #8:
Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.

On the second anniversary of the Paris Call, we **launched** new resources intended to help implement and uphold principles #7 and #8.



To support **principle #7**, we released **The Compendium on Cyber Hygiene**, a consolidated and easy-to-use guidebook on best practices for individuals and organizations to improve their cyber hygiene.

The Compendium on Cyber Hygiene

This compendium serves as an easy-to-navigate guidebook on best practices surrounding multifactor authentication, domain name security, email authentication, routing security, virtual private networks, and how to defend against common attack methods like password spray.

To support **principle #8**, we produced a new whitepaper, **No Hacking Back: Vigilante Justice vs. Good Security Online**, to highlight how this principle should be upheld without jeopardizing essential security practices.

No Hacking Back Whitepaper

This whitepaper provides a deep dive into what is considered inadvisable and illegal "hack back" activities versus valuable forward-leaning security practices employed by the technology industry today. It serves as an essential guide for policymakers seeking to better understand the boundaries of industry actions in cyberspace to prevent and deter cyberattacks by criminals, and why "hack backs" are not a suitable way to address the increasing number of threats.

We have been proud to support and promote the Paris Call as an essential agreement to help turn the tide against escalating threats in cyberspace through multi-stakeholder action. Looking ahead, we are pleased to be collaborating further with the Paris Call community as co-chair of its **third working group** on supporting the continuation of UN negotiations on cybersecurity with a robust multi-stakeholder inclusion.

Principle 3: Capacity Building

Our signatories see cybersecurity as a shared responsibility. Together, we work to increase capacity building in every sector and region by improving everyone's ability to act securely and safely online, and by empowering developers, businesses and people that use our technology to better protect themselves. In a connected world, benefits are shared; so, when any individual, organization or government is more secure, we are all more secure.

Protecting users and customers during COVID-19

In 2020, we saw the COVID-19 pandemic purposefully leveraged by malicious actors to take advantage of the most vulnerable users. Signatories such as Panda found evidence of an Advanced Persistent Threat actor (APT) using the pandemic in a spearfishing campaign against public sector entities, while Microsoft fought against human-operated malware and ransomware attacks targeting vulnerable systems. In response to the elevated risk of cyber-threats, our signatories compiled **90 helpful resources** that included tips and suggestions on how to act securely and safely online. **Collectively, the resources focused on:**

Protecting against phishing attacks, scams and disinformation.

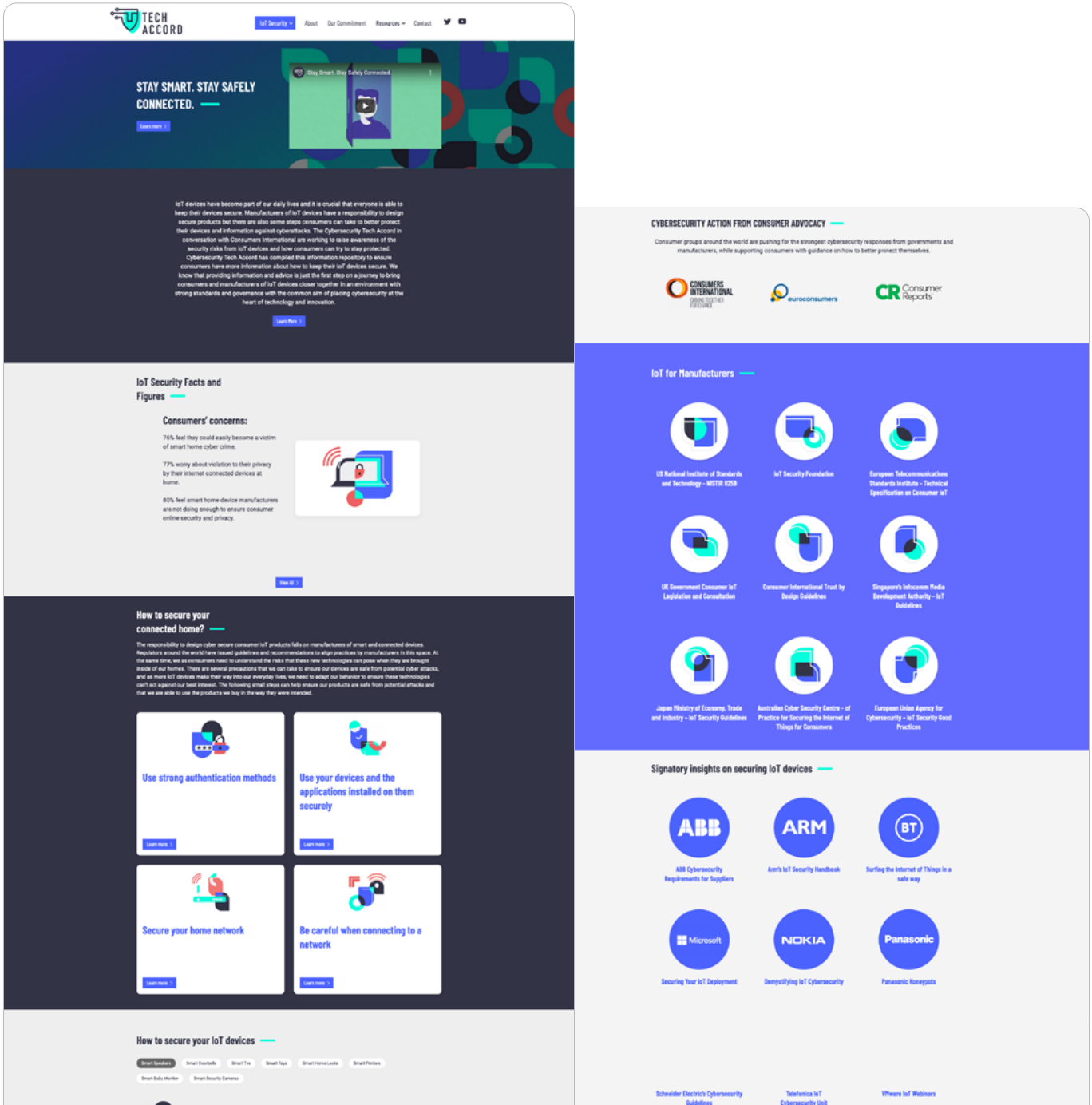
Supporting emergency response.

Facilitating remote education.

Working from home securely and efficiently.

Keeping IoT devices secure

Everyone, from governments, private organizations, and individual users, needs to play their part to make our online environment more secure. But anyone's ability to act begins with an awareness of the security risks that technology can pose. This is why in 2020, we started a dialogue with **Consumers International** and launched a new initiative, **Stay Smart. Stay Safely Connected**, to raise awareness around the importance of consumer IoT security – for average users as well as manufacturers. The campaign aimed to bring consumers and manufacturers closer together by recognizing that both have critical and distinct roles in protecting IoT products from cyber-threats. While manufacturers have a primary responsibility to design these products to be secure, it is important for consumers to be aware of potential risks and to know the steps they can take to use these products safely.



Promoting cybersecurity awareness across the Commonwealth Nations

As part of our first principle, we took steps to bridge the gap between needs and expertise by producing and releasing a comprehensive **whitepaper**, in collaboration with the **United Kingdom's Foreign & Commonwealth Office (FCO)**, on the state of cybersecurity awareness and associated campaigns across the Commonwealth of Nations. The whitepaper provides industry guidance to support cybersecurity awareness programs and catalogues awareness raising activities throughout the Commonwealth. The report captures a wide array of different approaches, including initiatives from across five continents including some of the world's largest and smallest countries, detailing different approaches to promoting cybersecurity awareness based on respective capacities, needs and cultures. As cybersecurity is a shared responsibility, we are grateful for the opportunity to have partnered with the FCO and the Commonwealth in developing the whitepaper.

Advancing cyber hygiene

As part of our commitment to Principle 7 of the Paris Call on Trust and Security in Cyberspace, we collaborated with like-minded organizations including the **CyberGreen Institute**, the **Global Cyber Alliance** and the **Internet Society**. Together we helped to advance the importance of cyber hygiene by promoting good practices critical to responding to a changing cyber-threat environment. Additionally, we launched a three-part video series to introduce cyber hygiene and highlight basic best practices. We also launched a blog series to educate individuals on how to protect themselves, and businesses on how to adopt security practices to protect customers.

Blogs:

- **The benefits of using a virtual private network (VPN)**
- **Protect against "password spray"**
- **The importance of patching**

Videos:

- **Introducing cyber hygiene**
- **Email security protocol, DMARC**
- **How to protect against DNS threats**

Principle 4: Collective Response

No single company or technology can secure cyberspace alone and our signatories are committed to the idea that we can, and must, achieve more together. As the Cybersecurity Tech Accord, we have formed various partnerships with industry, civil society and security researchers to improve technical collaboration, coordinate vulnerability disclosure, share threats, and minimize malicious code being introduced into cyberspace.

Advancing a multi-stakeholder approach

We frequently collaborate with partners across industries and stakeholder groups to amplify and improve our efforts. This is especially true for our work supporting the implementation of the principles of the Paris Call for Trust and Security in Cyberspace. As the largest ever multi-stakeholder agreement on cybersecurity principles, the Paris Call creates a unique opportunity to work with others to implement the values and commitments of the agreement. To this end, we worked closely with organizations including the CyberGreen Institute, the Global Cyber Alliance and the Internet Society to advance cybersecurity hygiene best practices in accordance with the Paris Call.

Cybersecurity Tech Accord signatories strongly believe that a more robust and secure global routing infrastructure is at the core of a safe internet ecosystem and that it demands shared responsibility and coordinated actions from a community of security-minded organizations. This is why the Mutually Agreed Norms for Routing Security (MANRS), intended to protect this system, was one of the first initiatives that the Cybersecurity Tech Accord endorsed in 2018. Our initial endorsement led to the creation of a working group tasked with investigating how companies beyond network operators and IXPs could contribute to routing security. Initially established as an exploration between the Cybersecurity Tech Accord and the Internet Society, it has since grown in scope and brought in other technology players. In 2020, we announced the development of a **set of six actions** that identify how cloud providers and content delivery networks can further support routing security in alignment with MANRS.

Our approach to collective action is based on our four principles for how all signatory companies will behave when it comes to cybersecurity. We will need to continue to have a global and collaborative response, bringing together the resources, technology and collective will of our companies around the world to protect people, strengthen products and systems and oppose those who exploit weaknesses.

2020 BY THE NUMBERS

New Signatories in 2020:

10

CRAYONIC

DXC.technology

EATON

Greenlight Cyber Security

LogRhythm

Moback

NEC

REDSEAL

SECURE SOFT

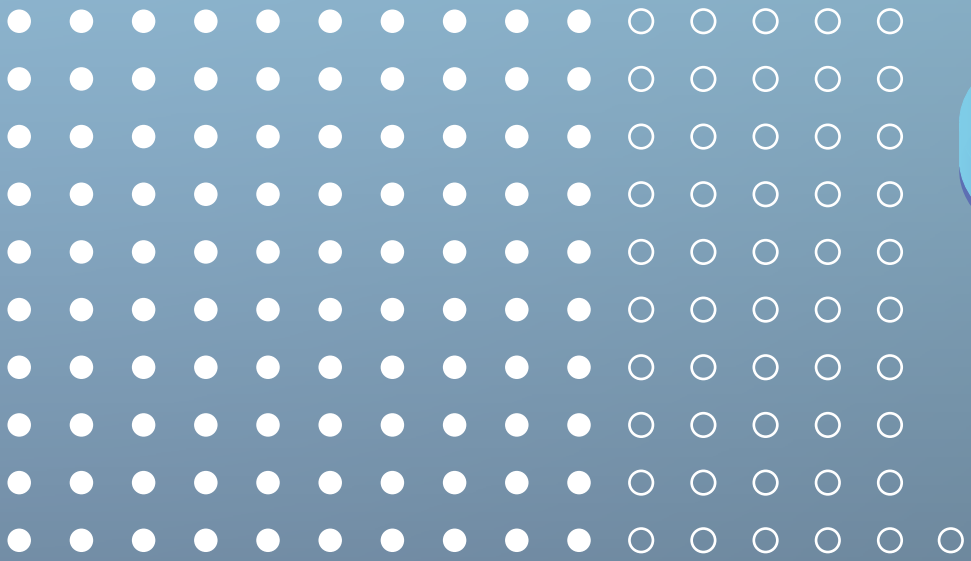
wallencore

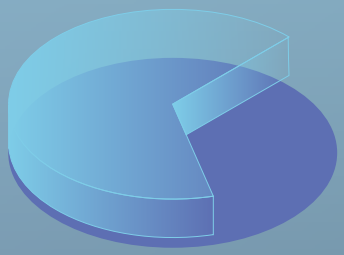
GEOGRAPHIC DISTRIBUTION

% of New Signatories

PERCENTAGE OF SIGNATORIES WITH CVD POLICIES

100 out of
151 Signatories





66.2% OF SIGNATORIES

LAUNCHED INITIATIVES IN A DIALOGUE/PARTNERSHIP WITH

9 Organizations

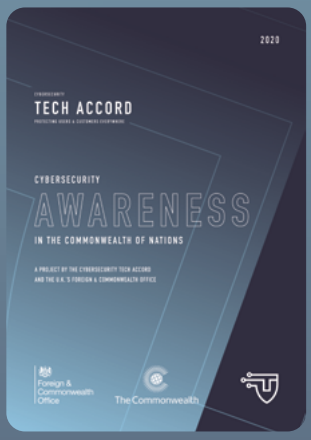
- United Nations Office of Disarmament Affairs
- United Nations Envoy on Youth
- Consumers International
- Internet Society
- Organisation for Economic Co-operation & Development (OECD)
- French Ministry for Europe and Foreign Affairs
- UK's Foreign & Commonwealth Office
- Cyber Peace Foundation
- The Economist Intelligence Unit

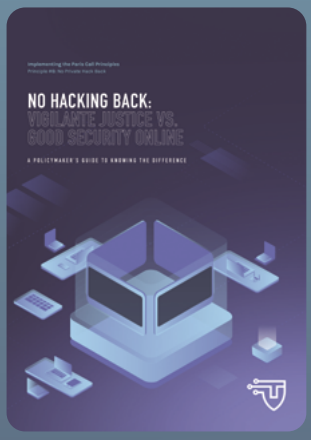
EVENTS HOSTED/ATTENDED 4

- **50th World Economic Forum →**
- **UNIDIR Operationalizing Cyber Norms: Multi-stakeholder Approaches to Responsible Vulnerabilities Disclosure →**
- Apps 4 Digital Peace Awards Ceremony
  Virtual Award Ceremony Registrants: 144
- **Paris Call Working Group on supporting the UN negotiations with a strong multi-stakeholder approach – Kick-off meeting →**

CYBERSECURITY CAMPAIGNS 4

- Cyber hygiene **Three-Part Video Series →** & **Three-Part Blog Series →**
- **Stay Smart. Stay Safely Connected Consumer IoT →**
- Support of **Global CyberPeace Challenge →**
- GCA Twitter Chat





WHITEPAPERS/ POLICY BRIEFS 3

CONSULTATION RESPONSES PROVIDED 8

- Cybersecurity Tech Accord Letter to OECD Scoping Paper on Digital Security of Products
- Cybersecurity Tech Accord Comments on OECD Work on Responsible Management and Disclosure of Vulnerabilities
- Cybersecurity Tech Accord submission to Australian consultation on responsible state behavior in cyberspace
- Cybersecurity discussions at the United Nations: Let drafting begin!
- Cybersecurity Tech Accord Comments on OECD Work on Digital Security
- Tech Accord reflections and comments on Geneva Dialogue background document
- Calling on the UN General Assembly to prioritize digital trust and security
- Cybersecurity Tech Accord Response: Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2

THREE YEARS OF OUR SHARED COMMITMENT

FROM 34 TO 151

The Cybersecurity Tech Accord's journey to becoming the industry's voice on peace and security online

OUR CORE PRINCIPLES

- Strong Defense
- Strong Offense
- Capacity Building
- Collective Response

APRIL

Cybersecurity Tech Accord Launch

Global technology companies sign the Cybersecurity Tech Accord, to defend customers everywhere from attacks by cybercriminals and state actors.

AUGUST

Routing Security Norms

Endorses Mutually Agreed Norms for Routing Security to increase resilience and security.

Campaign on Restoring WHOIS Access

Calls on ICANN to expedite solutions for legitimate third-party access to WHOIS data.

SEPTEMBER

Coordinated Vulnerability Disclosure Call

Supports Global Forum on Cyber Expertise (GFCE) call for industry adoption of coordinated vulnerability disclosure (CVD) policies.

OCTOBER

Capacity Building Webinars

Launches series with Global Forum on Cyber Expertise (GFCE) on cybersecurity best practices.

Support for DMARC

Endorses Domain-based Message Authentication, Reporting & Conformance (DMARC), with the Global Cyber Alliance (GCA).

NOVEMBER

Paris Call Supporter

Endorses the Paris Call for Trust and Security in Cyberspace, a landmark multistakeholder agreement.

DECEMBER

UN High Level Panel on Digital Cooperation

Calls for UN's Panel on Digital Cooperation to sign Paris Call, oppose cyberattacks anywhere and empower users to defend themselves.

2019

FEBRUARY

GSCS Singapore Norm Package

Welcomes new norms from the Global Commission on the Stability of Cyberspace. Calls on Commission to address cyber hygiene.

APRIL

Recommendations on Confidence Building

Publishes recommendations supporting the Organization of American States (OAS) on adopting confidence-building measures for cyberspace.

JULY

Civil Society Collaboration

Announces consultative workshops with civil society to identify and collaborate on peace and security online.

OCTOBER

Cybersecurity Awareness Promotion

Announces consultative workshops with civil society to identify and collaborate on peace and security online.

JANUARY

Apps 4 Digital Peace Contest

Launches Apps 4 Digital Peace contest with the UN Office of Disarmament Affairs.

2020

DECEMBER

Participation in UN OEWG

Joins the UN Open-Ended Working Group's dialogue on responsible state behavior and delivers statements of multi-stakeholder collaboration.

Commitments in Action

Begins publishing case study examples of signatory "Commitments in Action," showcasing cybersecurity best practices by leading companies.

MARCH

MANRS Adoption by Cloud Providers

Partners with In ternet Society to develop actions allowing cloud providers and Content Delivery Networks (CDN) to help secure large hubs of the Internet from routing problems.

MAY

Consumer IoT Security Initiative

Launches "Stay Smart. Stay Safely Connected" campaign with Consumers International on risks and best practices for consumer IoT products.

APRIL

CISO Blog Series

Launches blog series asking signatories: "What keeps your CISO up at night?"

NOVEMBER

Cyber Hygiene Compendium

Releases a compendium of cyber hygiene practices in support of Paris Call principle #7.

Hack Back Whitepaper

Publishes "No Hacking Back: Vigilante Justice vs.Good Security Online" whitepaper, supporting Paris Call principle #8.

JULY

Contribution to Geneva Dialogue

Provides feedback to the Geneva Dialogue's background document to support stability of the digital environment.

2021

FEBRUARY

Report on State-Sponsored Attacks

Releases survey report, with the Economist, on state-sponsored cyber-attacks on business.

MARCH

CVD Policy Milestone

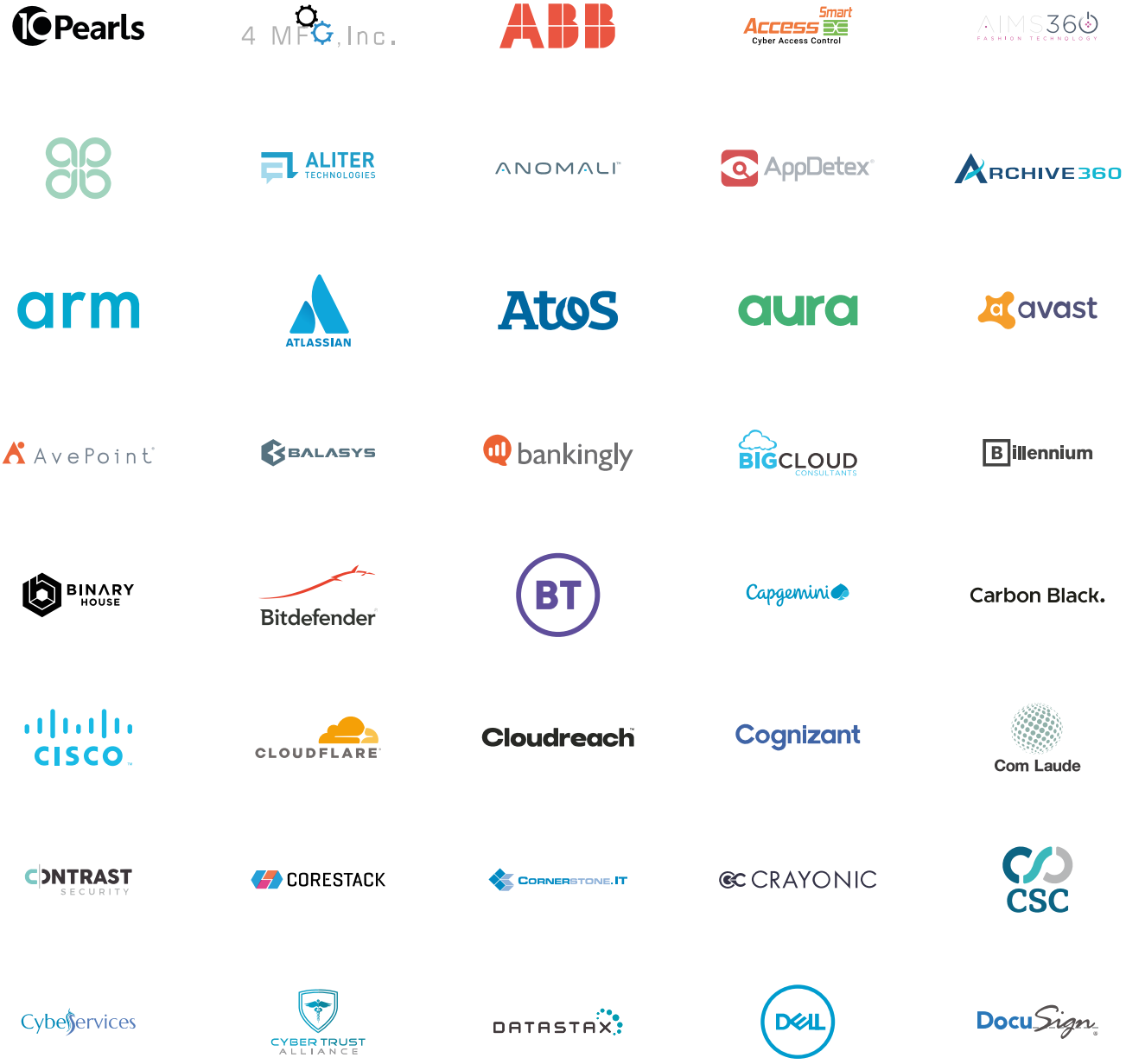
100 Tech Accord signatories adopt CVD policies.

Co-Chairs Paris Call Working Group

Joins French Ministry of Foreign Affairs' initiative to chair the Paris Call working group on multistakeholder inclusion in UN cyber dialogues.

TECH ACCORD SIGNATORIES

We welcome others who share our commitment to the Cybersecurity Tech Accord principles to get involved and join this effort. For more information, visit **www.cybertechaccord.org** or contact our secretariat at **info@cybertechaccord.org**




DOGTOWN MEDIA

DOMAINTOOLS

DXC.technology

EATON

ebrc

entel

ePrivacy

eset
ENJOY SAFER TECHNOLOGY

Exeltek

eye/o

facebook

fastly

FIREEYE

Flowmon
Driving Network Visibility

FRAMEWORK
SECURITY

F-Secure

G DATA

Gigamon

GitHub

GitLab

Globant

Greenlight
Cyber Security

GREYCORTEX

gtd

guardtime

HCS
Business Solutions
working smarter with IT

HITACHI
Inspire the Next

[H]matix

hp

Hewlett Packard
Enterprise

IMPERVA

indra
minsait

INFINIT
CONSULTING

integrity
partners

International
SOFTWARE SYSTEMS

intuit

JUNIPER
NETWORKS

KOOLSPAN

kpn

LaSalle Consulting Partners

LawToolBox.com

LinkedIn

LIREX.COM
IT INNOVATIONS

LogRhythm

Madison Computer Works

MarkMonitor
Protecting brands in the digital world

MediaPRO

mercado libre

Microsoft

Moback

NEC

NetApp

nielsen

NOKIA

NORTHWAVE

NTT
onShore SECURITY
ORACLE
orange
Panasonic
panda
pango
pax8
percipient.ai
predica.
PROFESSIONAL OPTIONS
QOMPLX:
Associates
REDSEAL
Resecurity
reveal
Rockwell Automation
RSA
SAFE PC CLOUD
safetica
salesforce
SAP
Schneider Electric
Scitum
secucloud
SECURE SOFT
SecurityScorecard
SHARP
SILENT BREACH
SONDA
SSRD
STACKPATH
STRATA Information Technology
stripe
StrongConnexions
swisscom
SWITCHFAST
Synack
TADGROUP
TANIUM
TIM
Telefónica
telelink
tenable
ThreatModeler
TREND MICRO
UNISYS
US Licensing Group
US Medical IT
VALIDY
vmware
VU
wallencore
WCA TECHNOLOGIES
WIPFLI
WISeKey


PASS1234

FOR INFORMATION ON THE CYBERSECURITY TECH ACCORD,
PLEASE EMAIL INFO@CYBERTECHACCORD.ORG