Microsoft

National Cybersecurity Policy, Strategy, and Implementation

Amanda Craig

Director, Cybersecurity Policy
Digital Diplomacy
Microsoft

Digital Diplomacy Team

Defending Democracy

Cybersecurity Policy

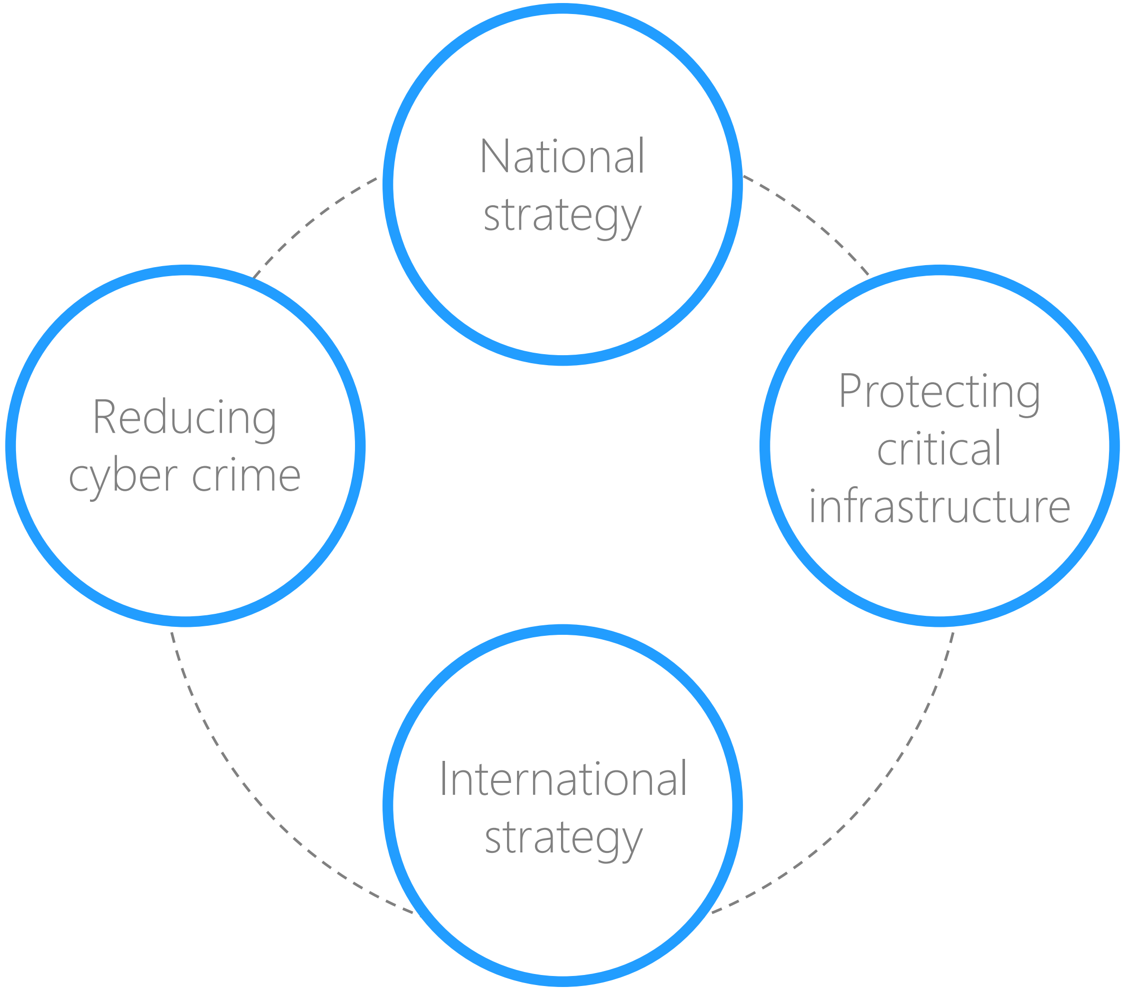
Digital Peace

Microsoft

National Cybersecurity Policy: Foundational Concepts and Areas of Focus

A national cybersecurity policy framework

SECURITY OF GOVERNMENT SYSTEMS



National strategy

Protecting critical infrastructure

International strategy

Reducing cyber crime

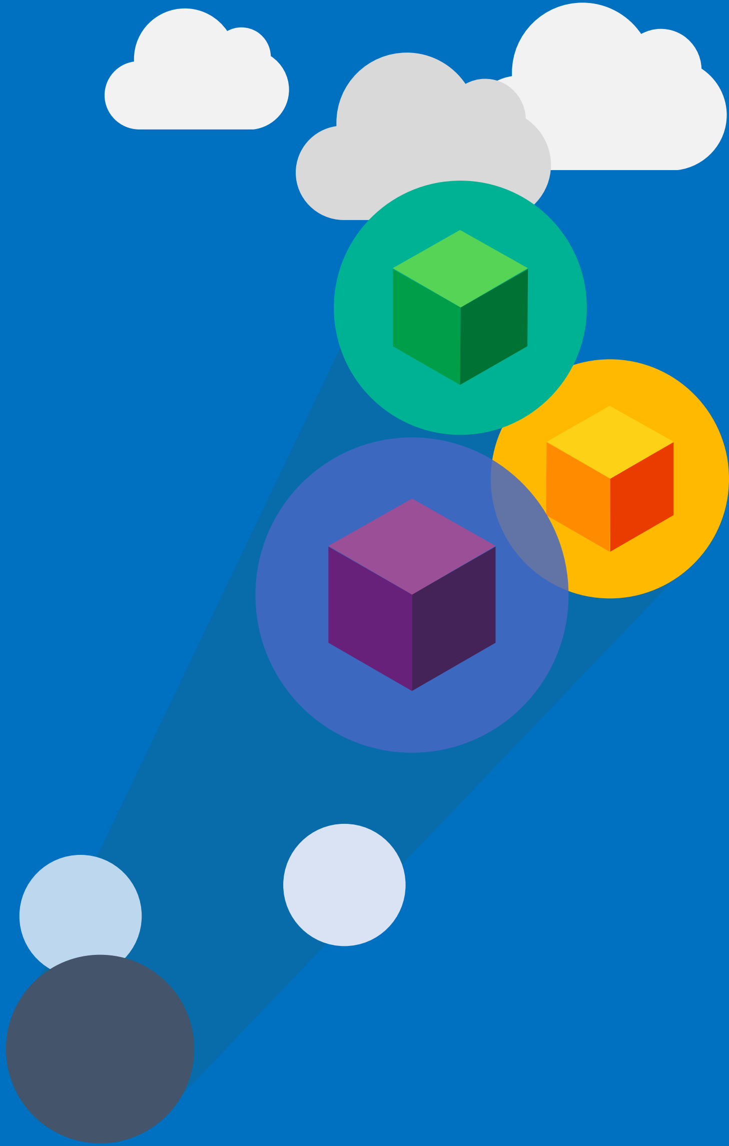
ENTERPRISE SECURITY AND COMPLIANCE

STRENGTHENING SECURITY THROUGH DIGITAL TRANSFORMATION

Microsoft

Cybersecurity Policy Framework:

A practical guide to the development of national cybersecurity policy



Find the paper:

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2rT3a

Microsoft

National Cybersecurity Strategy: Aims, Principles, and Practices

Five aims of a national cybersecurity strategy

Facilitate national dialogue

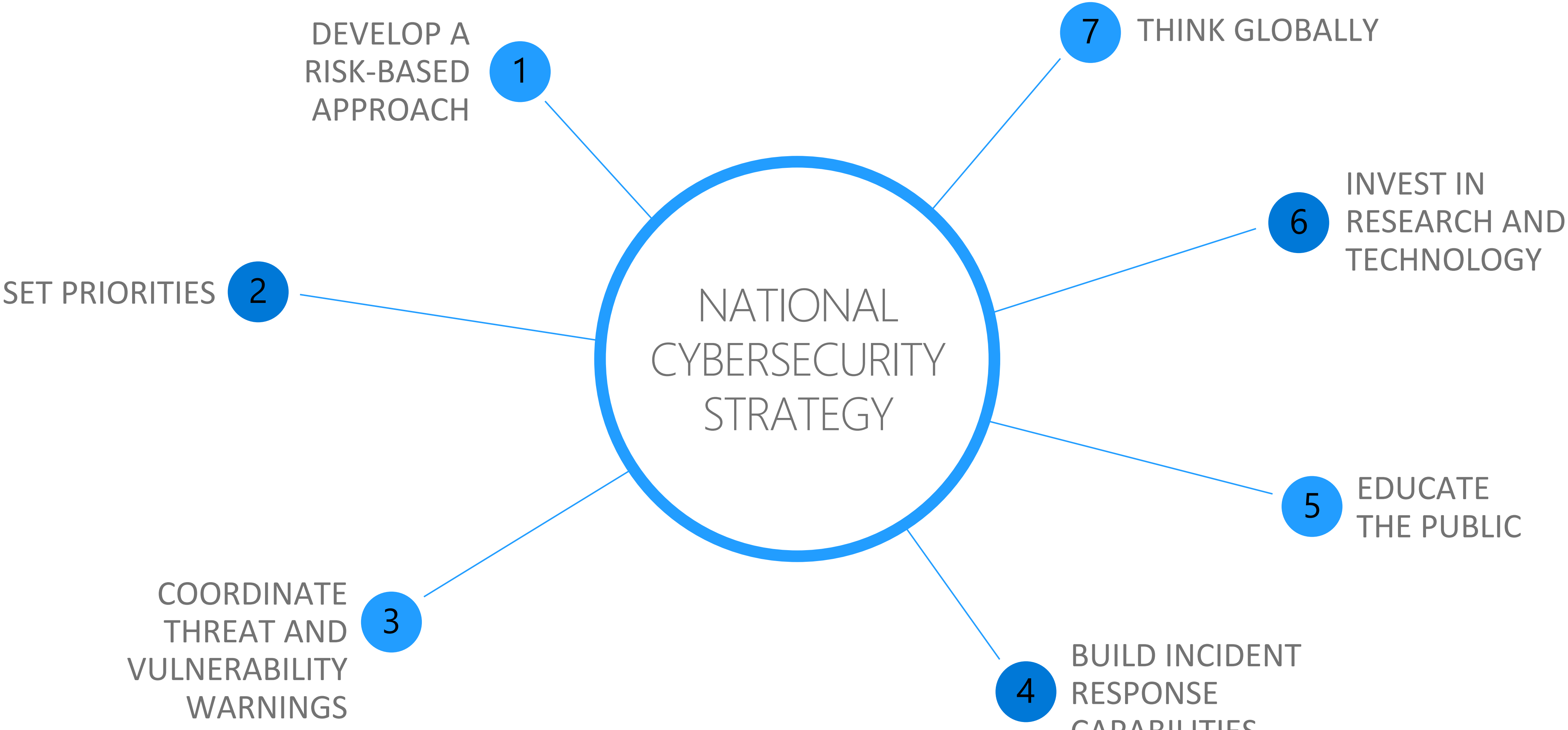
Clarify policies, programs, and priorities

Specify ministry, agency, and department roles

Stipulate goals and metrics to measure progress

Address funding and resource needs

Seven practices to build a national strategy for cybersecurity

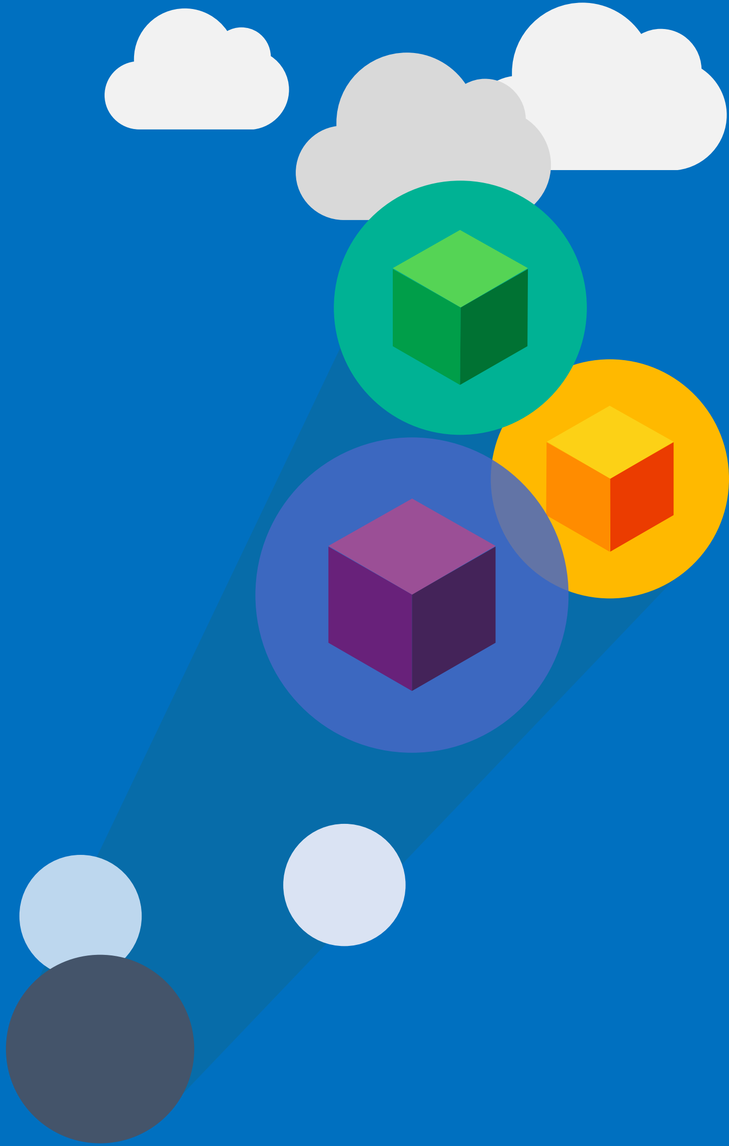

NATIONAL CYBERSECURITY STRATEGY
1 DEVELOP A RISK-BASED APPROACH
2 SET PRIORITIES
3 COORDINATE THREAT AND VULNERABILITY WARNINGS
4 BUILD INCIDENT RESPONSE CAPABILITIES
5 EDUCATE THE PUBLIC
6 INVEST IN RESEARCH AND TECHNOLOGY
7 THINK GLOBALLY

Developing a National Strategy for Cybersecurity:

Foundations for Security, Growth, and Innovation

Find the paper:

http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf



ITU's Guide to Developing a National Cybersecurity Strategy

Lifecycle of a National Cybersecurity Strategy

- Initiation
- Stocktaking and analysis
- Production
- Implementation
- Monitoring and evaluation

Overarching principles

- Vision
- Comprehensive
- Inclusiveness
- Economic and social prosperity
- Human rights
- Risk management
- Policy instruments
- Roles and resources
- Trust environment

Good practice focus areas

- Governance
- Risk management
- Resilience
- Critical infrastructure
- Capacity building
- Legislation/regulation
- International cooperation

Find the 2018 paper: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

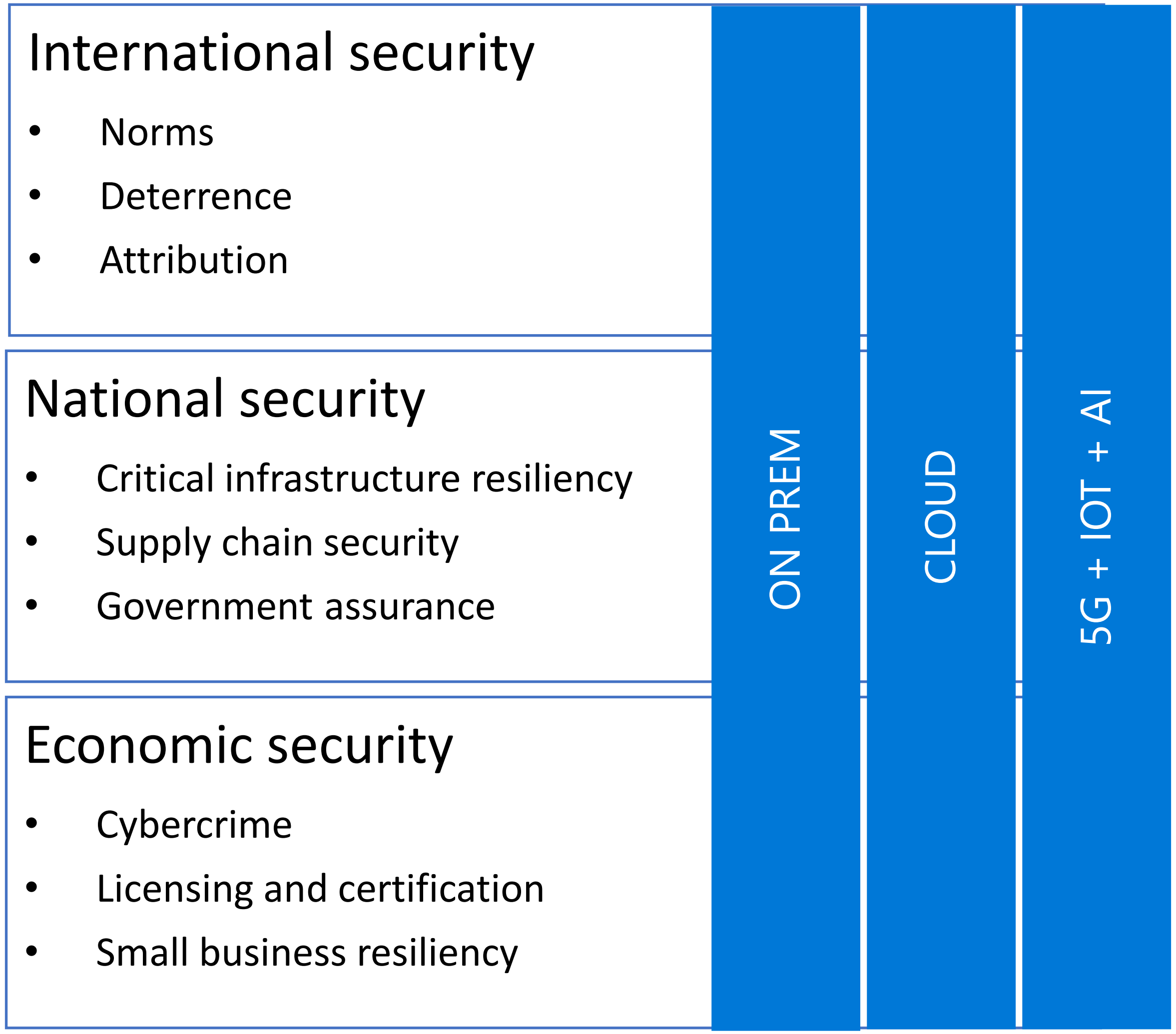
Watch for a 2021 update!

Microsoft

Cybersecurity and Digital Transformation

Changing cybersecurity policy landscape

INFORMATION SHARING	INCIDENT REPORTING	SECURITY BASELINES
SOFTWARE ASSURANCE	IDENTITY MANAGEMENT	BLOCKCHAIN
SECURITY TELEMETRY	RISK MANAGEMENT	WORKFORCE DEVELOPMENT
VULNERABILITY DISCLOSURE	ZERO TRUST APPROACHES	INCIDENT RESPONSE



International security

- Norms
- Deterrence
- Attribution

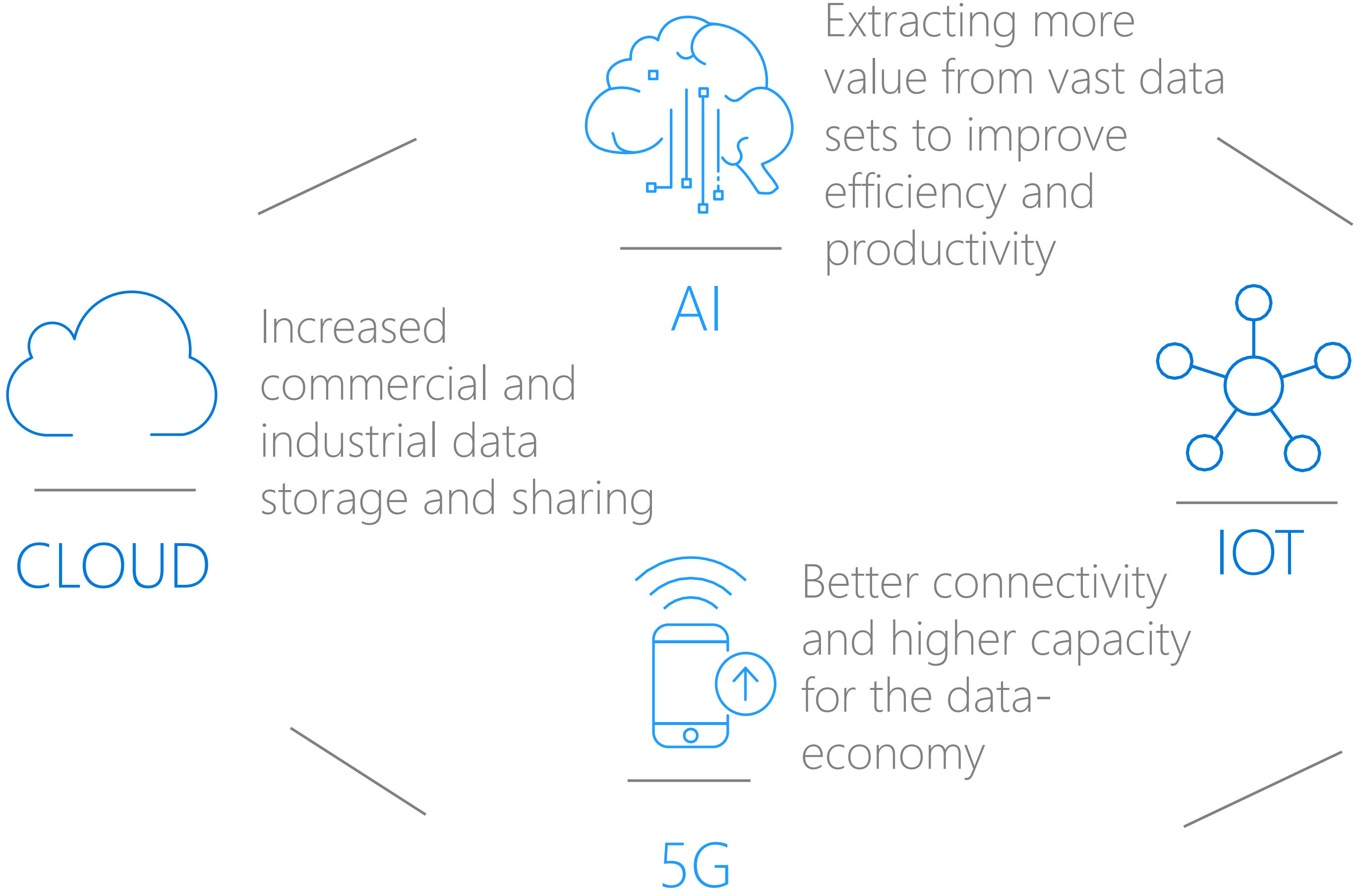
National security

- Critical infrastructure resiliency
- Supply chain security
- Government assurance

Economic security

- Cybercrime
- Licensing and certification
- Small business resiliency

Cloud is foundational to digital transformation



CLOUD

Increased commercial and industrial data storage and sharing

AI

Extracting more value from vast data sets to improve efficiency and productivity

IOT

More connected devices creating and sharing data

5G

Better connectivity and higher capacity for the data-economy

Resilience and cybersecurity of critical infrastructure, strategic business assets, and consumer products are further enablers of digital transformation.

Effective policy approaches

Process

Open, transparent, and iterative

Principles

Risk based, outcomes focused, resiliency focused

Perspective

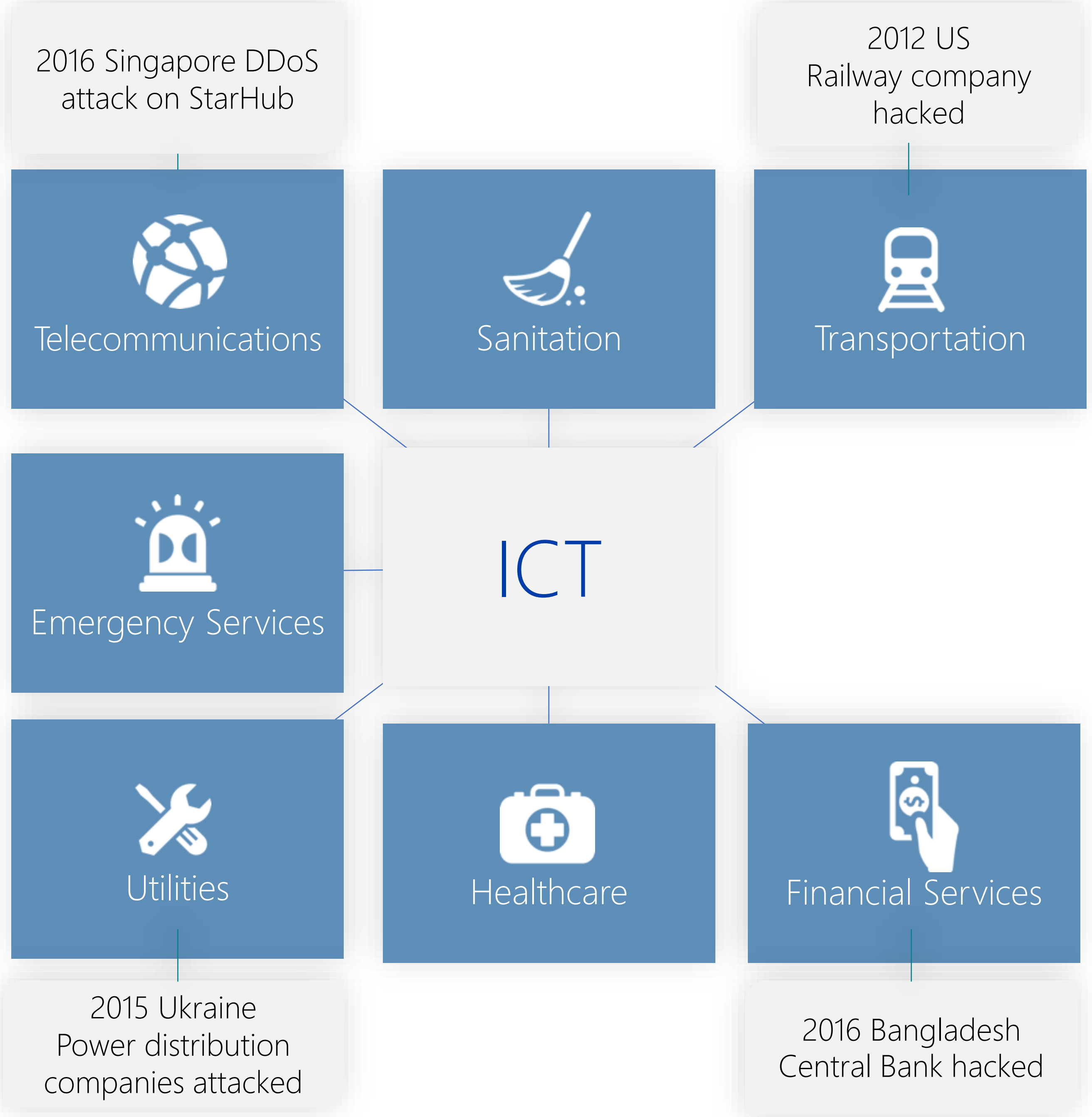
Consistent and interoperable globally

Protecting critical infrastructure:

Security baselines

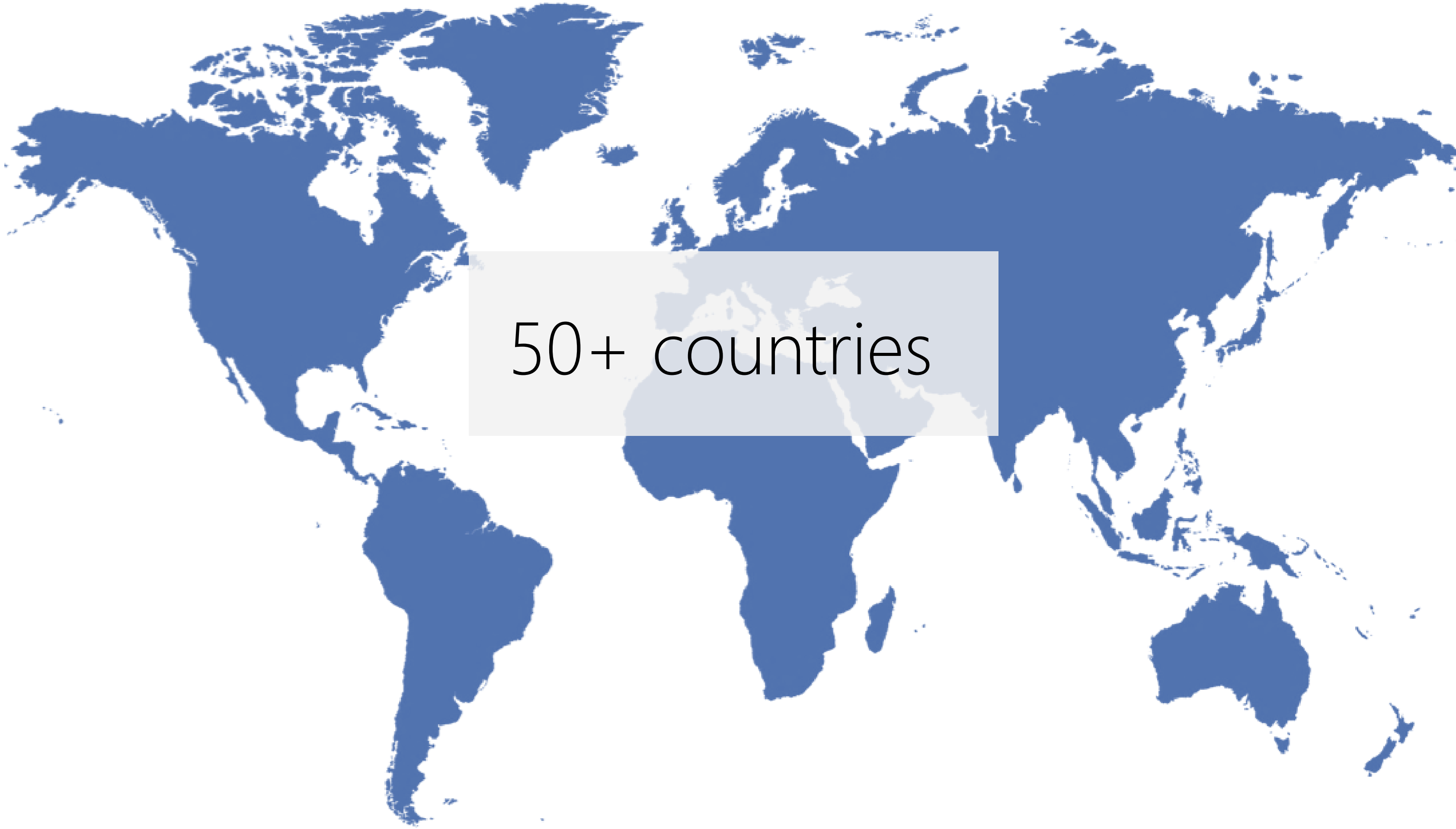
Protecting critical infrastructure is increasingly important

Without appropriate safeguards, the proliferation of connected devices and big data will make critical infrastructure more vulnerable to a serious cyberattack.


2016 Singapore DDoS attack on StarHub
2012 US Railway company hacked
Telecommunications
Sanitation
Transportation
Emergency Services
ICT
Utilities
Healthcare
Financial Services
2015 Ukraine Power distribution companies attacked
2016 Bangladesh Central Bank hacked

Governments recognize the importance of protecting critical infrastructure from cyber threats

Critical infrastructure cyber risks are typically thought of as risks to information systems, that, if exploited, could negatively impact national security, economic well-being, or public safety to a significant degree.



50+ countries

The approach and substance of security baselines are key

Approach

Leverage diverse expertise by utilizing an open, collaborative and iterative development process that engages various stakeholders

Substance

Facilitate decision-making by bridging risk management understanding within and between organizations

Manage risks efficiently through a risk-based and prioritized set of baseline practices

Enable innovation by driving toward desired security outcomes rather than prescriptive requirements

Leap forward by leveraging best practices

Support economic growth by realizing economic and security benefits with efficiency

BEST PRACTICE:

Provide a single document or reference point that creates a common language on risk management and desired security outcomes within and between organizations

A common language for an emerging field like cybersecurity enables more communication, shared learning, informed investments, and continuous improvement:

Within an organization

- Creates shared understanding and more effective prioritization and management of risk
- Creates continuity in security strategy, planning and investments
- Drives continuous improvement

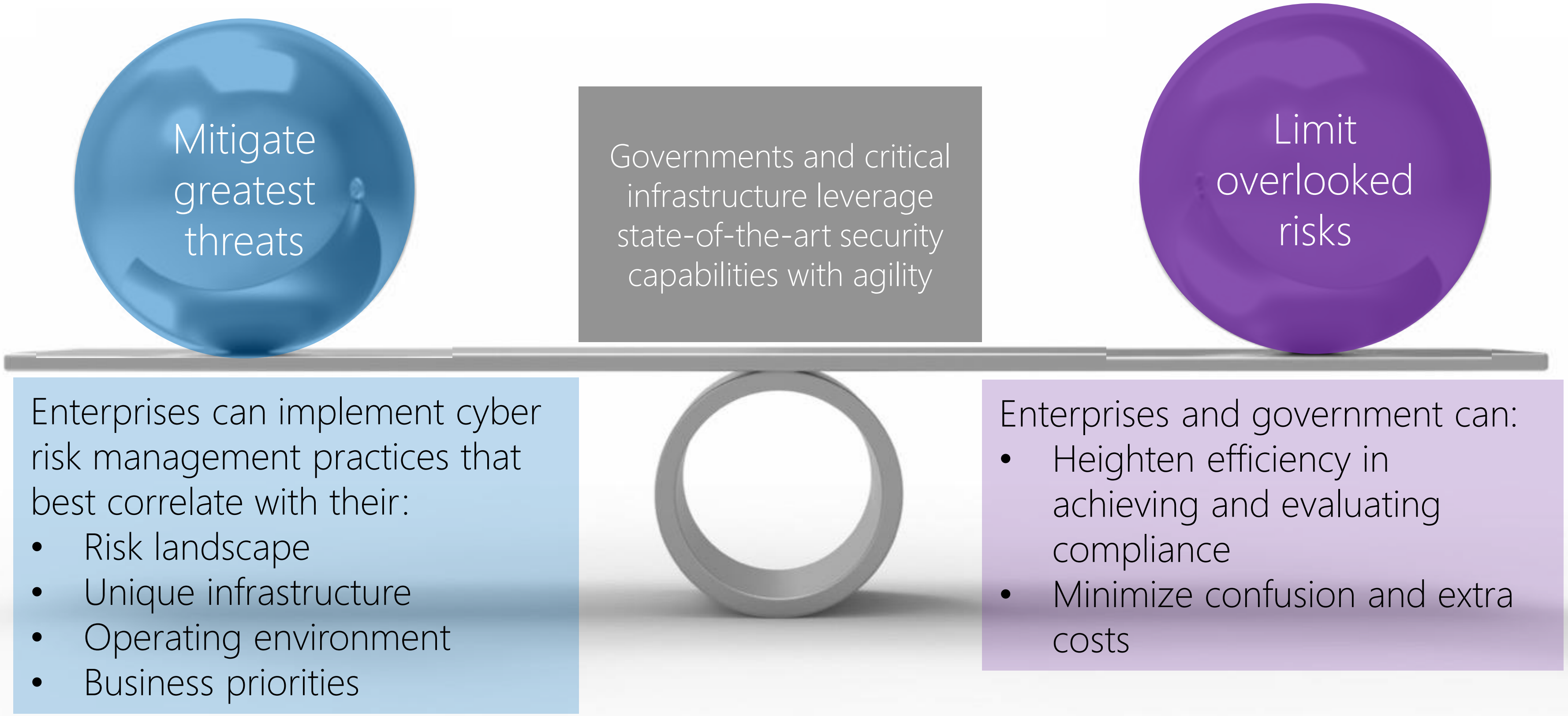
Between or across multiple organizations

- Enables buyers to request or require security information in a more consistent manner
- Enables suppliers to share meaningful information on risk management practices

BEST PRACTICE:

Focus on a risk-based and prioritized set of baseline practices

Governments should focus on the most important risks as they develop their approaches:



Mitigate greatest threats

Governments and critical infrastructure leverage state-of-the-art security capabilities with agility

Limit overlooked risks

Enterprises can implement cyber risk management practices that best correlate with their:

- Risk landscape
- Unique infrastructure
- Operating environment
- Business priorities

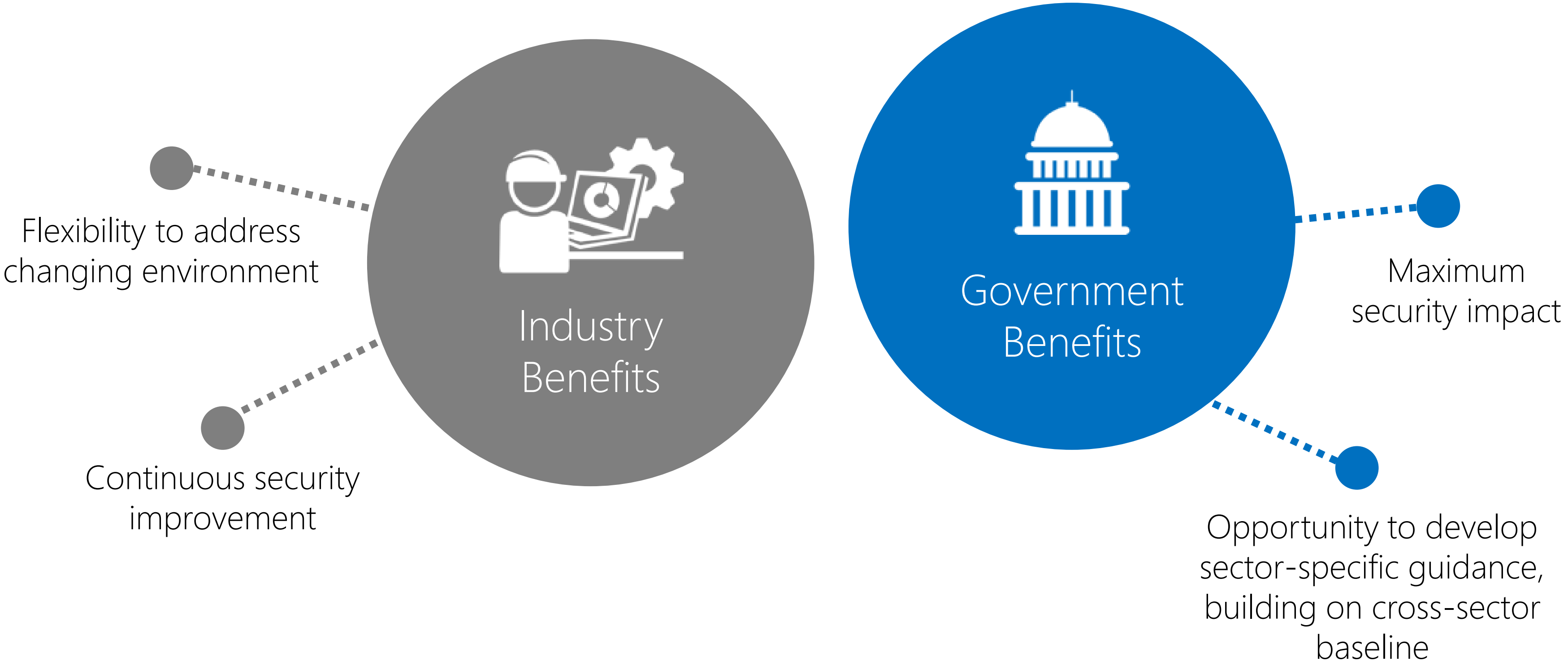
Enterprises and government can:

- Heighten efficiency in achieving and evaluating compliance
- Minimize confusion and extra costs

BEST PRACTICE:

Focus on desired security outcomes

When governments articulate what organizations should aim to achieve rather than how they should implement security:



Industry Benefits

Flexibility to address changing environment

Continuous security improvement

Government Benefits

Maximum security impact

Opportunity to develop sector-specific guidance, building on cross-sector baseline

BEST PRACTICE:

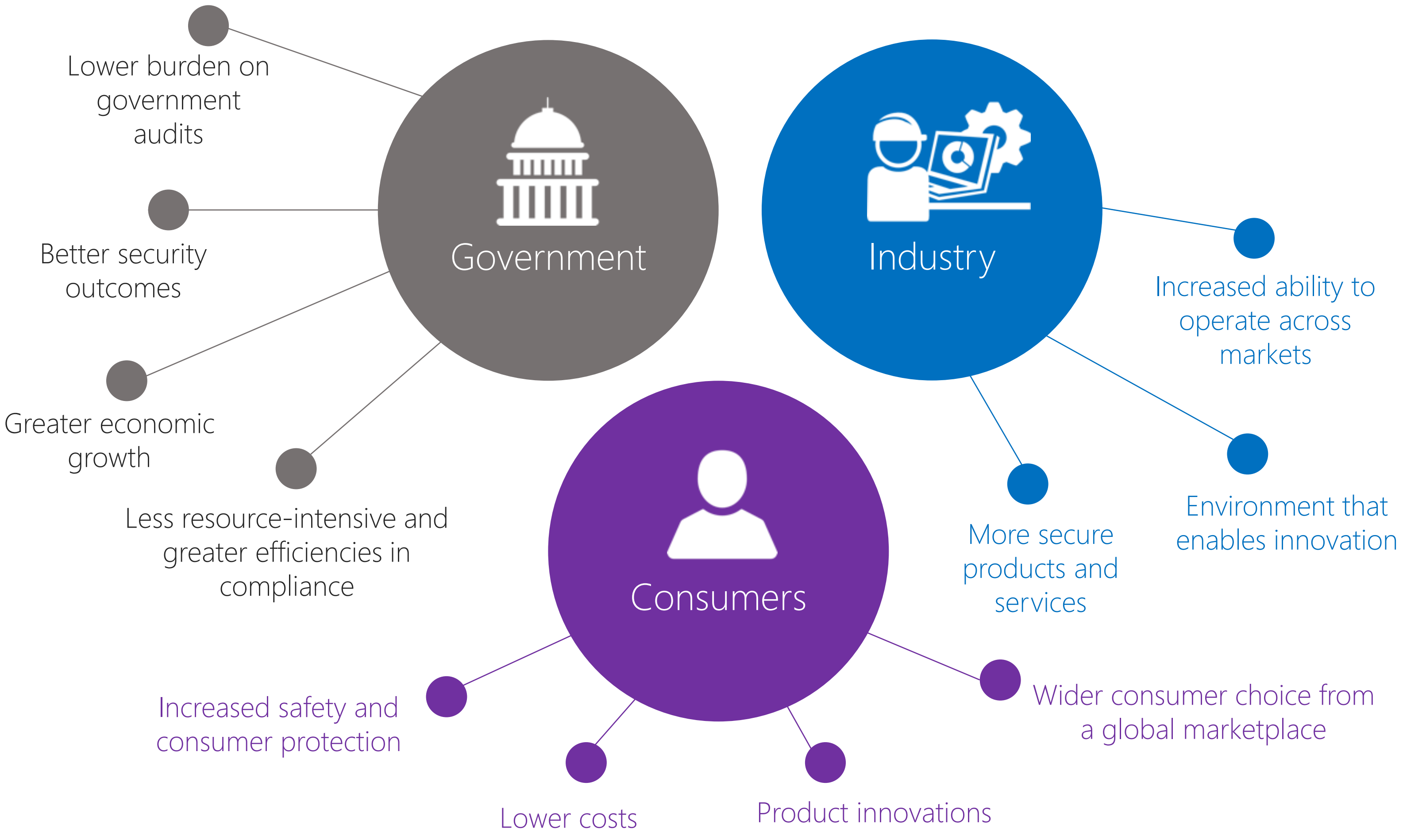
Leverage existing reference points with widespread support

Utilizing tried and tested methods provides governments with a valuable starting point:

- Raise the level of ecosystem cybersecurity
- Allow shared learning and exchange across governments
- Gain enormous efficiencies rather than building out a set of risk management practices from scratch

BEST PRACTICE:

Security baselines should support economic growth while maximizing security outcomes


Government
Lower burden on government audits
Better security outcomes
Greater economic growth
Less resource-intensive and greater efficiencies in compliance
Industry
Increased ability to operate across markets
More secure products and services
Environment that enables innovation
Consumers
Increased safety and consumer protection
Lower costs
Product innovations
Wider consumer choice from a global marketplace

Risk based and prioritized practices

Security baselines typically define a set of common security requirements that aim to help organizations manage cybersecurity risk.

Span a wide range of operational and risk management activities:

Identify **Protect** **Detect** **Respond** **Recover**

Cross-sector security baselines enable interoperability and allow for a narrow set of sector-specific requirements as necessary.

The NIST Cybersecurity Framework: The Approach

The U.S. National Institute of Standards and Technology (NIST) has led the development and evolution of a risk-based cybersecurity framework for critical infrastructure, outlining a set of industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks.

Version 1.0 was published in February 2014, and Version 1.1 was published in April 2018.

Developing and Evolving the Framework

involved significant public-private partnership and global participation

The National Institute of Standards and Technology (NIST) hosted numerous workshops and public consultations to inform its efforts to develop and evolve the Framework. As such, the process reflected the following principles:

Open

Collaborative

Iterative

The NIST Cybersecurity Framework: **The Substance**

The U.S. National Institute of Standards and Technology (NIST) has led the development and evolution of a risk-based cybersecurity framework for critical infrastructure, outlining a set of industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks.

Version 1.0 was published in February 2014, and Version 1.1 was published in April 2018.

The Framework comprises three parts: **Core**, Tiers and Profiles

The Framework Core

*A set of **cybersecurity activities, desired outcomes, and applicable references** that are common across critical infrastructure sectors.*

Five functions	Categories	Informative References
Identify	• Asset management • Business Environment • Governance • Risk assessment • Risk management strategy • Supply chain risk management	Specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. E.g.: ISO/ IEC 27001:2013 NIST SP 800-53 CCS CSC 2 ISA 62443-2-1:2009
Protect	• Identity management and access control • Awareness and training • Data security • Information protection processes and procedures • Maintenance • Protective technology	
Detect	• Anomalies and events • Security continuous monitoring • Detection processes	
Respond	• Response planning • Communications • Analysis • Mitigation • Improvements	
Recover	• Recovery planning • Improvements • Communications	

The NIST Cybersecurity Framework: **The Substance**

The U.S. National Institute of Standards and Technology (NIST) has led the development and evolution of a risk-based cybersecurity framework for critical infrastructure, outlining a set of industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks.

Version 1.0 was published in February 2014, and Version 1.1 was published in April 2018.

The Framework comprises three parts: Core, **Tiers** and Profiles

The Framework Implementation Tiers

provide context on how an organization views cybersecurity risk and the processes in place to manage that risk

The Four Tiers grow in terms of rigor and sophistication in cybersecurity risk management practices and the extent to which they inform and complement business needs.

Tier 1: Partial

Tier 2: Risk informed

Tier 3: Repeatable

Tier 4: Adaptive

The NIST Cybersecurity Framework: The Substance

The U.S. National Institute of Standards and Technology (NIST) has led the development and evolution of a risk-based cybersecurity framework for critical infrastructure, outlining a set of industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks.

Version 1.0 was published in February 2014, and Version 1.1 was published in April 2018.

The Framework comprises three parts: Core, Tiers and **Profiles**

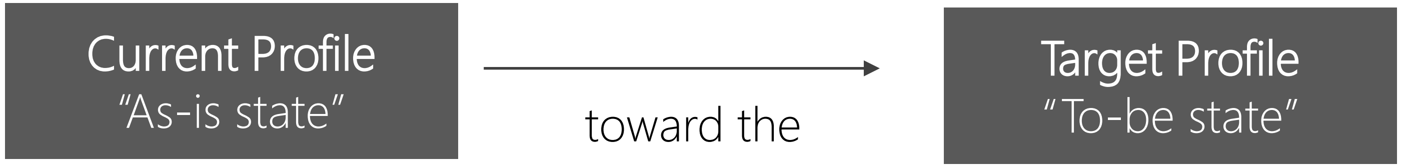
A Framework Profile

represents the outcomes, based on business needs, that an organization has selected from the Framework Core

Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).

To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important.

The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation.



Current Profile
"As-is state"

toward the

Target Profile
"To-be state"

ISO/IEC 27103 and 27101 - Cybersecurity Framework Guidelines: **The Approach**

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1 Subcommittee (SC) 27 has developed ISO/IEC 27103, which builds on best practices for a cybersecurity framework by integrating international ISO and IEC standards as references that support implementation of cybersecurity activities.

ISO/IEC 27013 was approved in October 2017 and published in February 2018.

ISO/IEC 27101 is under development.

Developing ISO/IEC 27103 and ISO/IEC 27101

involved public and private sector experts in a global, multilateral forum

ISO/IEC JTC 1 SC 27 study group participants contributed to the development of the reference, providing input and edits during ISO and IEC meetings and calls, and national bodies had the opportunity to influence and vote on whether it was approved. As such, the process reflected the following principles:

Global

Collaborative

Iterative

ISO/IEC 27103 - Cybersecurity and ISO and IEC Standards: **The Substance**

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1 Subcommittee (SC) 27 has developed ISO/IEC 27103, which builds on best practices for a cybersecurity framework by integrating international ISO and IEC standards as references that support implementation of cybersecurity activities.

ISO/IEC 27013 was approved in October 2017 and published in February 2018.

ISO/IEC 27103

*A set of **cybersecurity activities, desired outcomes, and applicable international references** that are common across critical infrastructure sectors.*

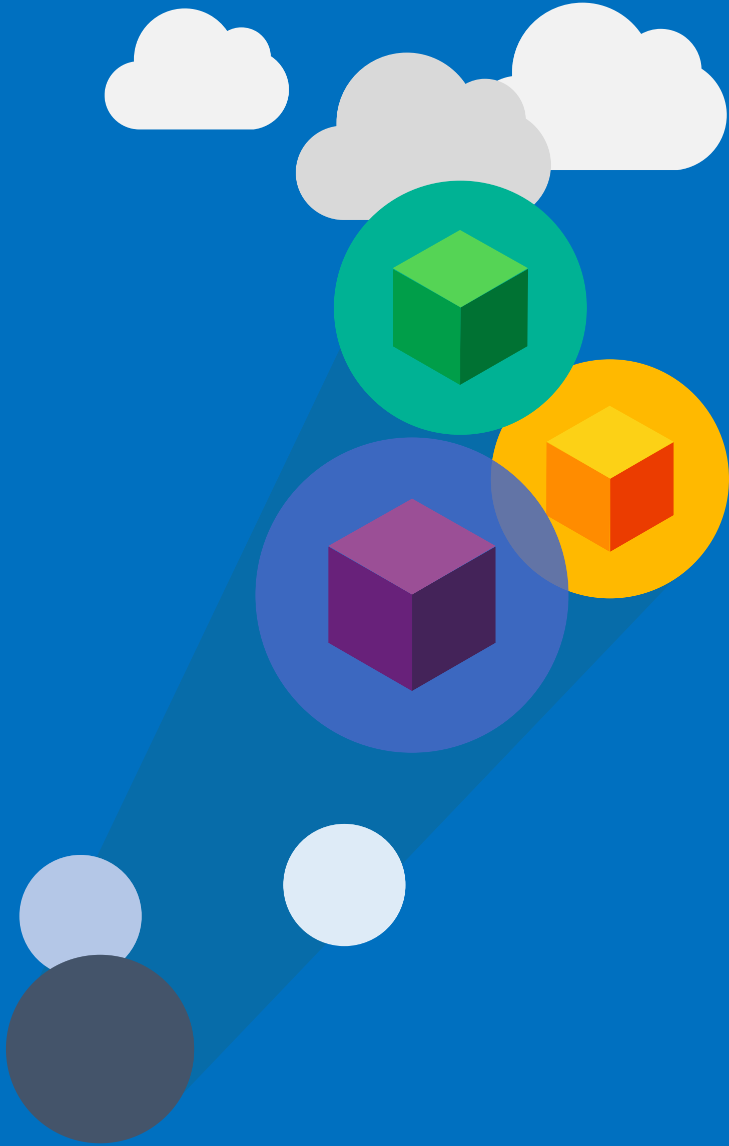
Five outcomes	Categories	References
Identify	• Asset management • Business Environment • Governance • Risk assessment • Risk management strategy	Specific sections of international standards that are relevant across sectors and that illustrate methods to achieve the outcomes associated with each category (as well as each subcategory). E.g.: ISO/ IEC 27001 and 27002 ISO/IEC 20243 ISO/IEC 27035 ISO/IEC 29147 and 30111 ISO 31000 IEC 62443
Protect	• Access control • Awareness and training • Data security • Information protection processes and procedures • Maintenance • Protective technology	
Detect	• Anomalies and events • Security continuous monitoring • Detection processes	
Respond	• Response planning • Communications • Analysis • Mitigation • Improvements	
Recover	• Recovery planning • Improvements • Communications	

Microsoft

Risk management for cybersecurity: Security Baselines

Find the paper:

http://download.microsoft.com/download/4/6/0/46041159-48FB-464A-B92A-80A2E30B78F3/MS-riskmanagement-securitybaselines-WEB.pdf

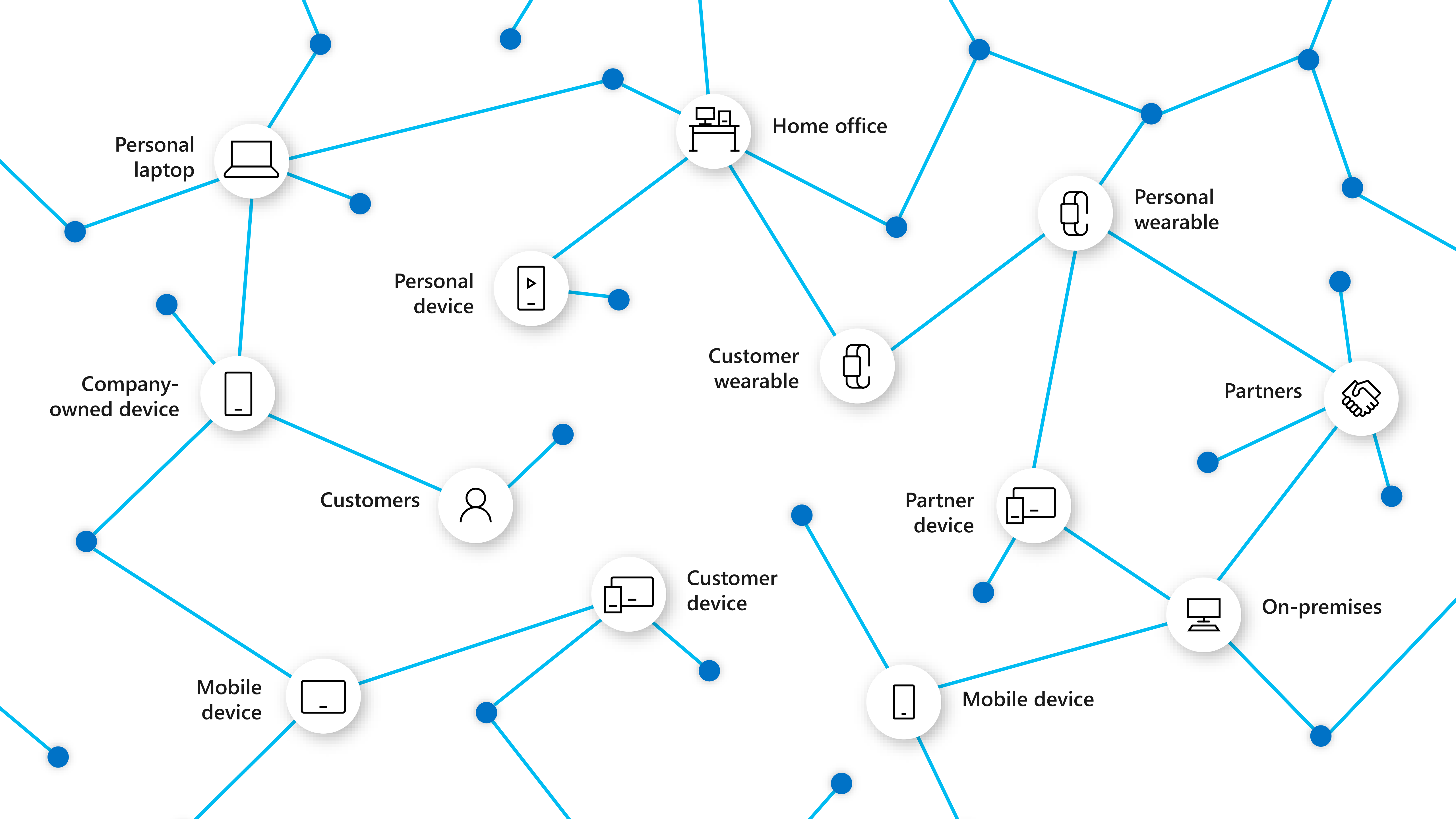


Microsoft

Thank you!

Microsoft

Cloud computing security

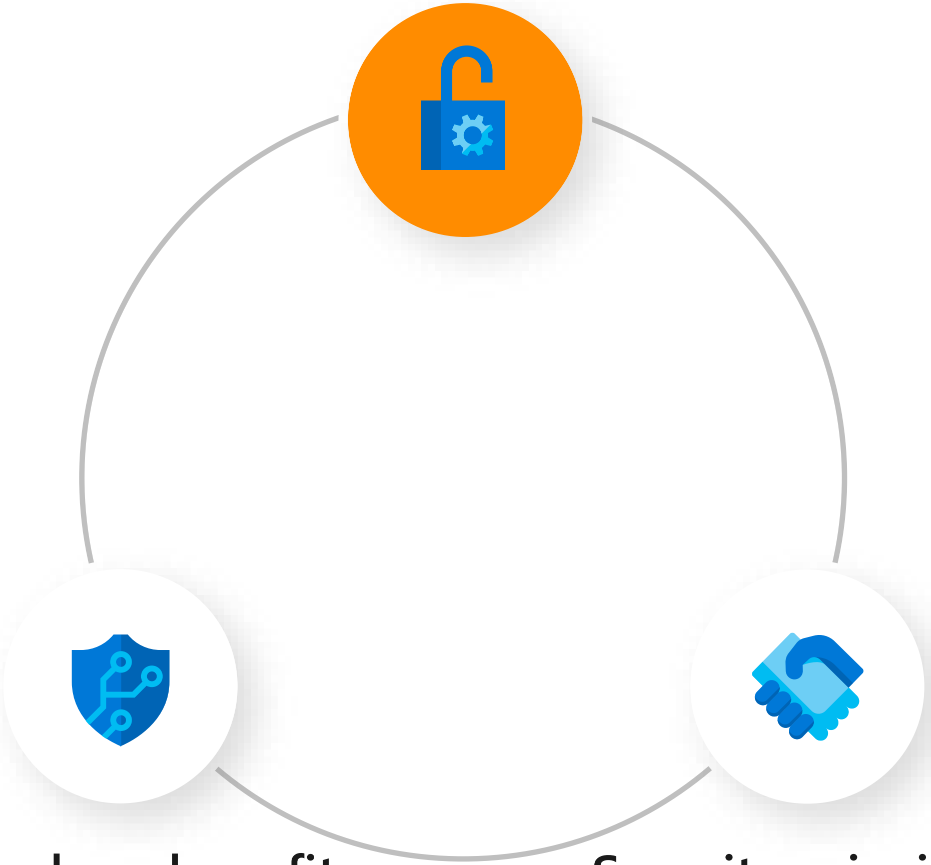

Personal laptop
Home office
Personal wearable
Personal device
Customer wearable
Company-owned device
Partners
Customers
Partner device
Customer device
On-premises
Mobile device
Mobile device

Cloud 101

Agenda

Technology benefits

Security principles



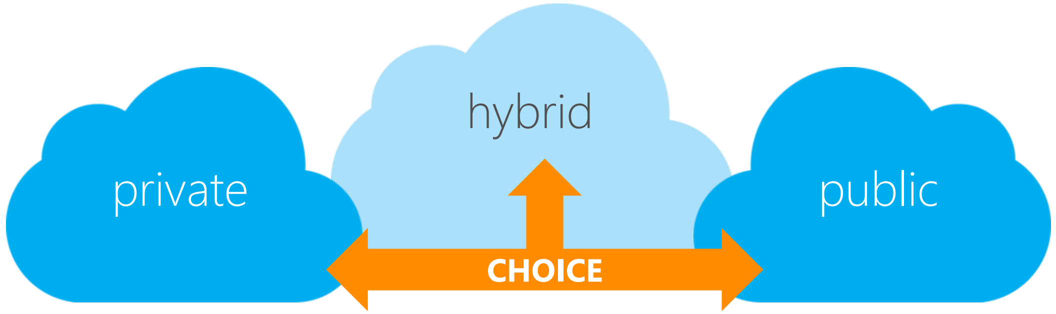
Overview

Technology benefits

Security principles

What do we mean, when we say cloud?

Deployment models



private

hybrid

public

CHOICE

Environment operated solely for a single organization; it may be managed by that organization or by a cloud service provider.

Public or private environments remain unique entities but are bound together with on-premises ICT by common technology that enables data and application portability.

Multi-tenant environments in which cloud service providers own and make available to the general public their cloud infrastructure, including storage and applications.

Service models

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Cloud is becoming integral to government transformation

Start with a trusted & resilient foundation ☑ Reshape how you engage with citizens

Leverage economies of scale and expertise ☑ Enable more productive work

Use the cloud to drive future technology uptake ☑ Enable domestic IoT economy

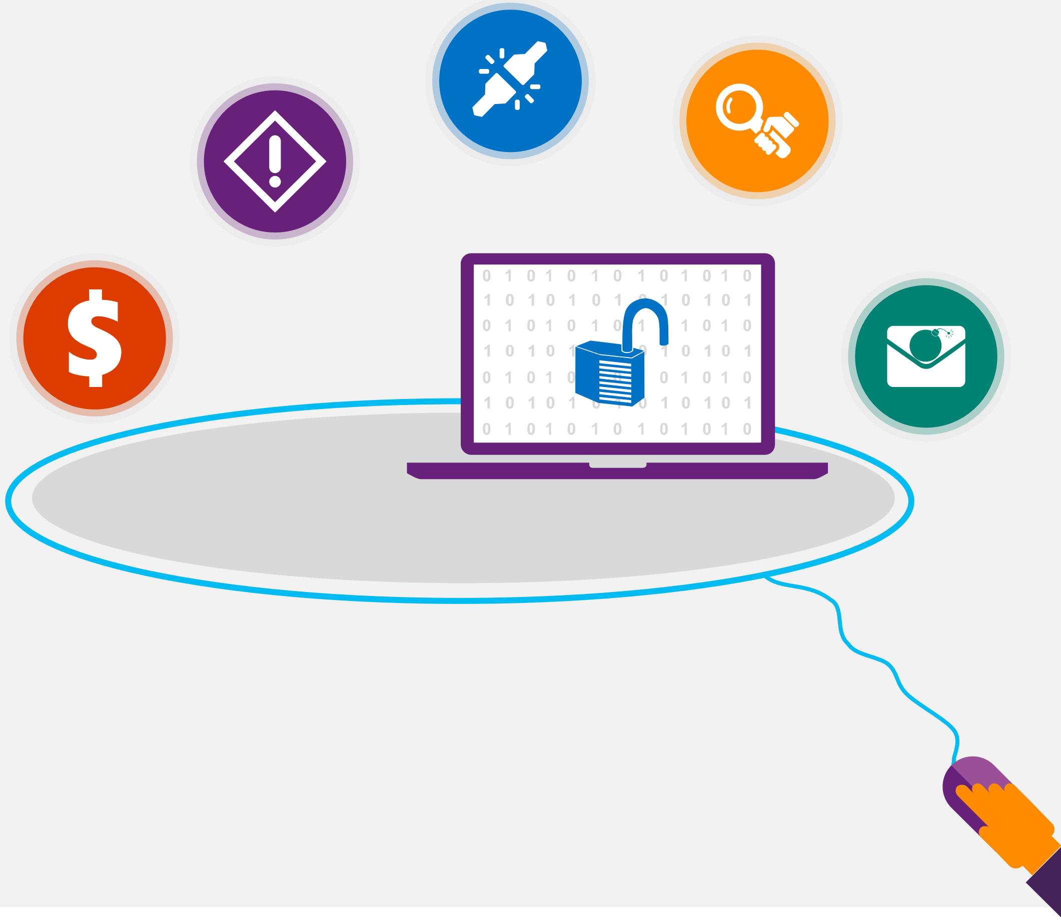
Yet security concerns persist

Cybercrime extracts between 15% and 20% of the value created by the Internet.[1]

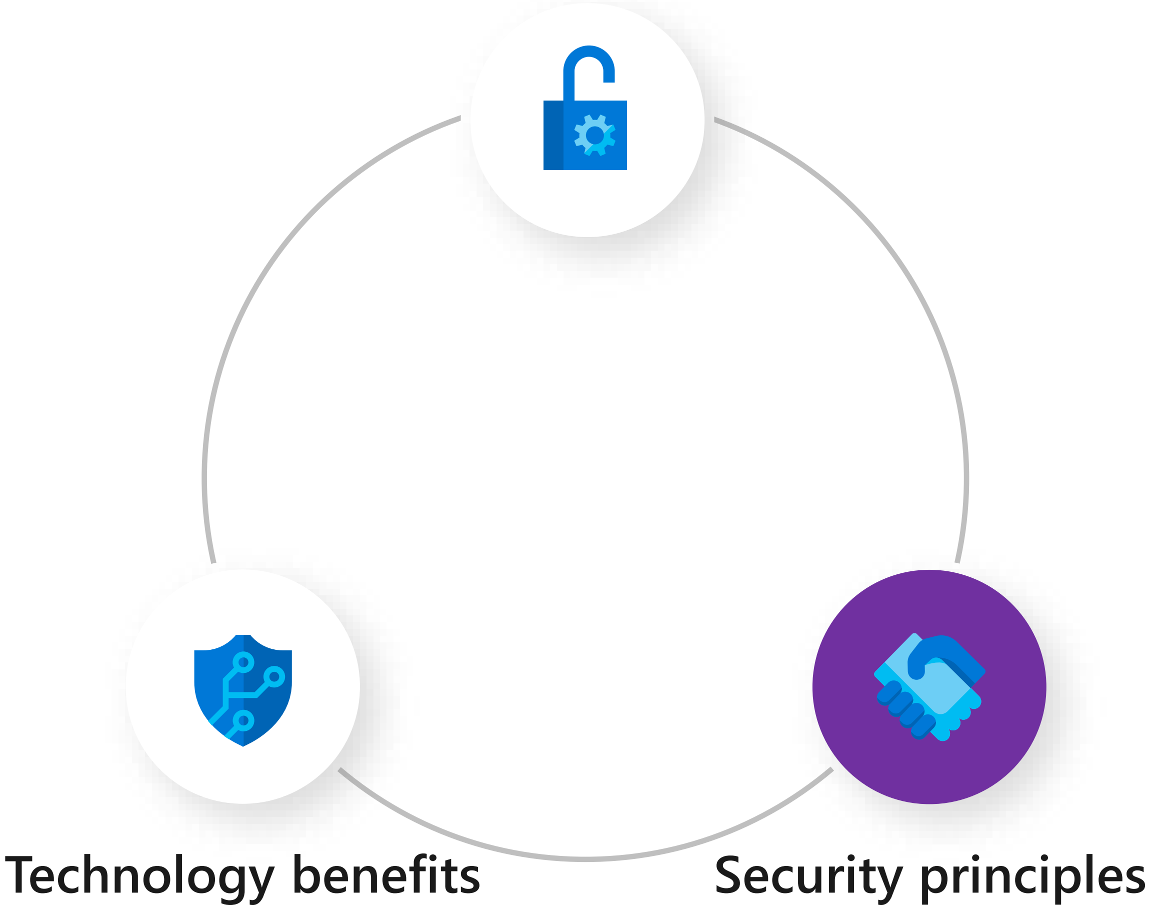
In the UK, 81% of large corporations and 60% of small businesses reported a cyberbreach in the past year.[2]

Total financial losses attributed to security compromises increased 34% in 2014.[3]

Impact of cyber attacks could be as much as $3 trillion in lost productivity and growth.[4]



Cloud 101



Technology benefits

Security principles

Cloud security principles

Innovative

Cloud policies should set a clear path toward innovating and advancing the security and resiliency of their government services.

Flexible

Cloud policies should be flexible and should enable governments to select the most suitable cloud types for delivering their services in a secure and resilient manner.

Data aware

Cloud policies should demonstrate data awareness by ensuring that assessments, categorization, and protection of data are commensurate with risk.

Risk-based

Cloud policies should prioritize the assessment, management, and reduction of risk in the delivery of cloud services for governments.

Standard-based

Cloud policies should leverage global standards as the basic requirements for increasing security and resiliency in government cloud services.

Transparent

Cloud policies should establish transparent and trusted processes for developing compliance requirements and for evaluating the security and resiliency of cloud services.

Microsoft

Cloud security principles

Innovative

Flexible

Data aware

Risk-based

Standard-based

Transparent

Cloud policies should set a clear path toward innovating and advancing the security and resiliency of their government services.

While the pace at which governments incorporate new technologies must be responsive to the realities of their environments, Microsoft encourages governments to take a forward-leaning approach, empowering organizations to move to the cloud when appropriate by adopting a “cloud first” policy.

Transport for London is *innovative*, using open data to provide bike rental information and developing a contactless payment system on the resilient foundation of public cloud services.

Cloud security principles

Innovative

Flexible

Data aware

Risk-based

Standard-based

Transparent

Cloud policies should be flexible and should enable governments to select the most suitable cloud types for delivering their services in a secure and resilient manner.

Government entities should retain sufficient flexibility as they develop and implement their cloud security policies and evaluate various cloud deployment and service models, ensuring that they can apply their knowledge and hands-on experience to make the best decisions for their environments.

Australia's newest cloud policy is *flexible*, enabling government departments to make implementation decisions, including regarding when their data can be moved to offshore cloud environments.

Cloud security principles

- Innovative
- Flexible
- **Data aware**
- Risk-based
- Standard-based
- Transparent

Cloud policies should demonstrate data awareness by ensuring that assessments, categorization, and protection of data are commensurate with risk.

Governments should take a conscious approach to data governance as part of their cloud policies, categorizing their systems and data by sensitivity and business impact, which will enable them to realize optimizations and compliance efficiencies that might not be possible when all data is assigned the same value.

The UK has developed *data-aware* cloud policies, simplifying its security classification system to three levels and recognizing that the vast majority of its data can be marked “Official,” a low level of sensitivity.

Microsoft

Cloud security principles

- Innovative
- Flexible
- Data aware
- **Risk-based**
- Standard-based
- Transparent

Cloud policies should prioritize the assessment, management, and reduction of risk in the delivery of cloud services for governments.

Governments should assess risks in cloud and in on-premises technologies, determining how their risk profiles may improve by migrating to the cloud as well as what net new risks must be managed, and should distinguish between common and unique risks, easing later risk management decisions.

The Security Assurance Framework for Evaluation outlines how governments can take a *risk-based* approach, assessing and determining how to treat risks in cloud environments.

Microsoft

Cloud security principles

- Innovative
- Flexible
- Data aware
- Risk-based
- **Standard-based**
- Transparent

Cloud policies should leverage global standards as the basic requirements for increasing security and resiliency in government cloud services.

Because many governments share common risks and cloud computing is based on aggregation and scale to drive down costs, governments should leverage global standards as the basis of their cloud security certifications, enabling greater efficiency, lower costs, and more market competition.

The UK is utilizing a *standards-based* approach to cloud certifications, leveraging ISO 27001 to create an efficient, consistent, and reusable mechanism for cloud security assessments.

Microsoft

Cloud security principles

- Innovative
- Flexible
- Data aware
- Risk-based
- Standard-based
- **Transparent**

Cloud policies should establish transparent and trusted processes for developing compliance requirements and for evaluating the security and resiliency of cloud services.

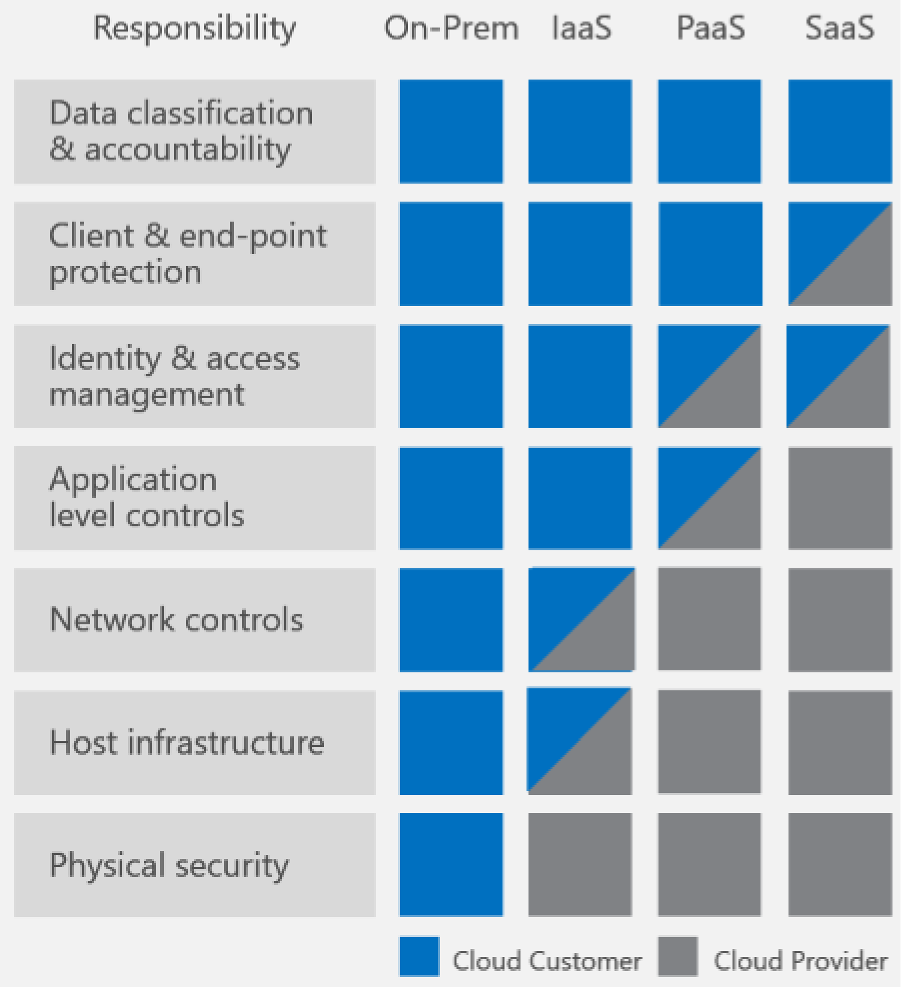
Governments should leverage the expertise and perspectives of all relevant stakeholders when developing cloud requirements, enabling them to establish clear, comprehensive, and easily adoptable compliance frameworks, and utilize clear evaluative criteria in assessing cloud providers.

The U.S. National Institute of Standards and Technology (NIST) developed its Cybersecurity Framework through a *transparent* process, resulting in greater clarity for and faster uptake by providers.

One final point…

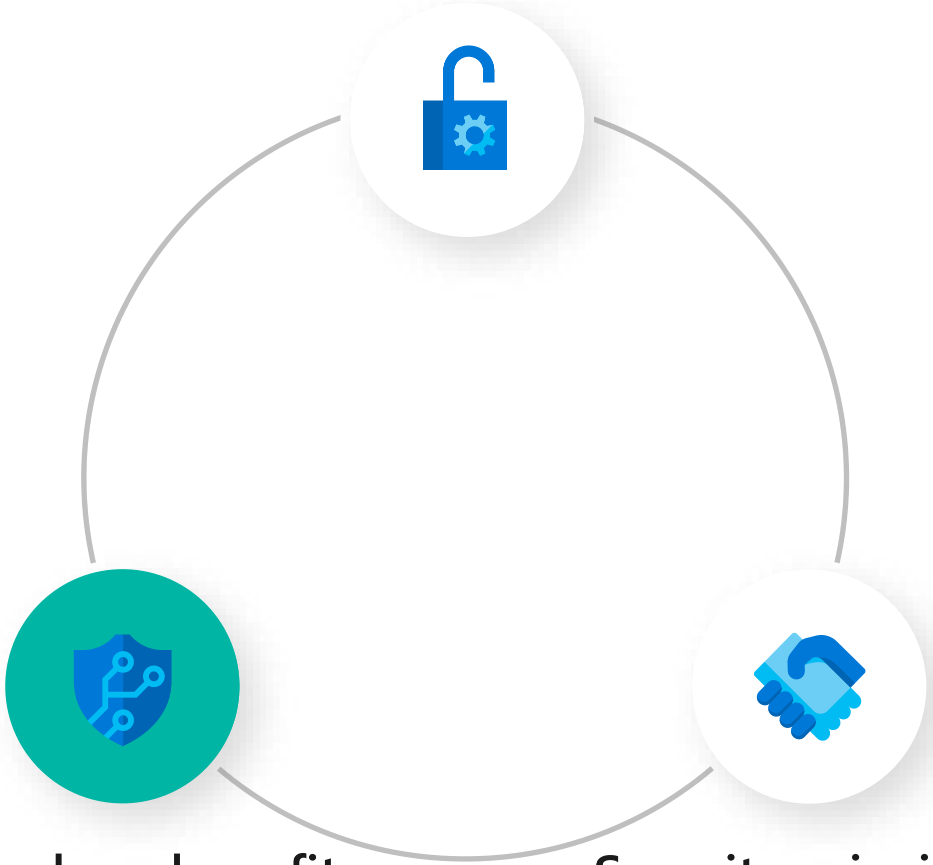
Security responsibilities

The various cloud services require different levels of customer engagement and **responsibility for security**.



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◩
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	◩	⬛	⬛
Host infrastructure	🟦	◩	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud Customer ⬛ Cloud Provider



Cloud 101

Technology benefits

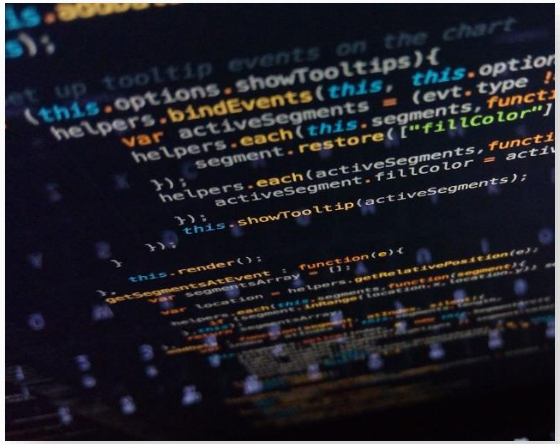
Security principles

Key challenges and concerns

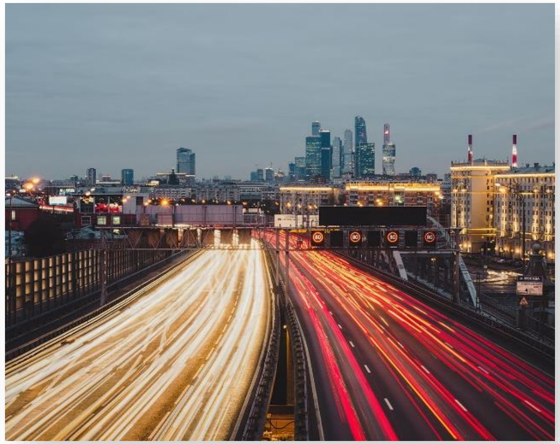
TOPIC	AREA OF CONCERN
Cybersecurity Defending against highly-resourced, persistent adversaries and online fraud	• Sophisticated attacks • Cost • Brand reputation/customer trust/retention • Vendor management • Data protection • Adaptive access control
Digital Transformation Adapting to disruptive technologies and competing with new vendors that use hi-tech (digital natives)	• Cloud • Innovative customer experiences • Deployment configurations • Trusted partners
Compliance Maintaining compliance	• Regulatory compliance • Data integrity, privacy, compliance • 3rd party/partner compliance

The era of flux and transformation

Everyone is now in the technology business

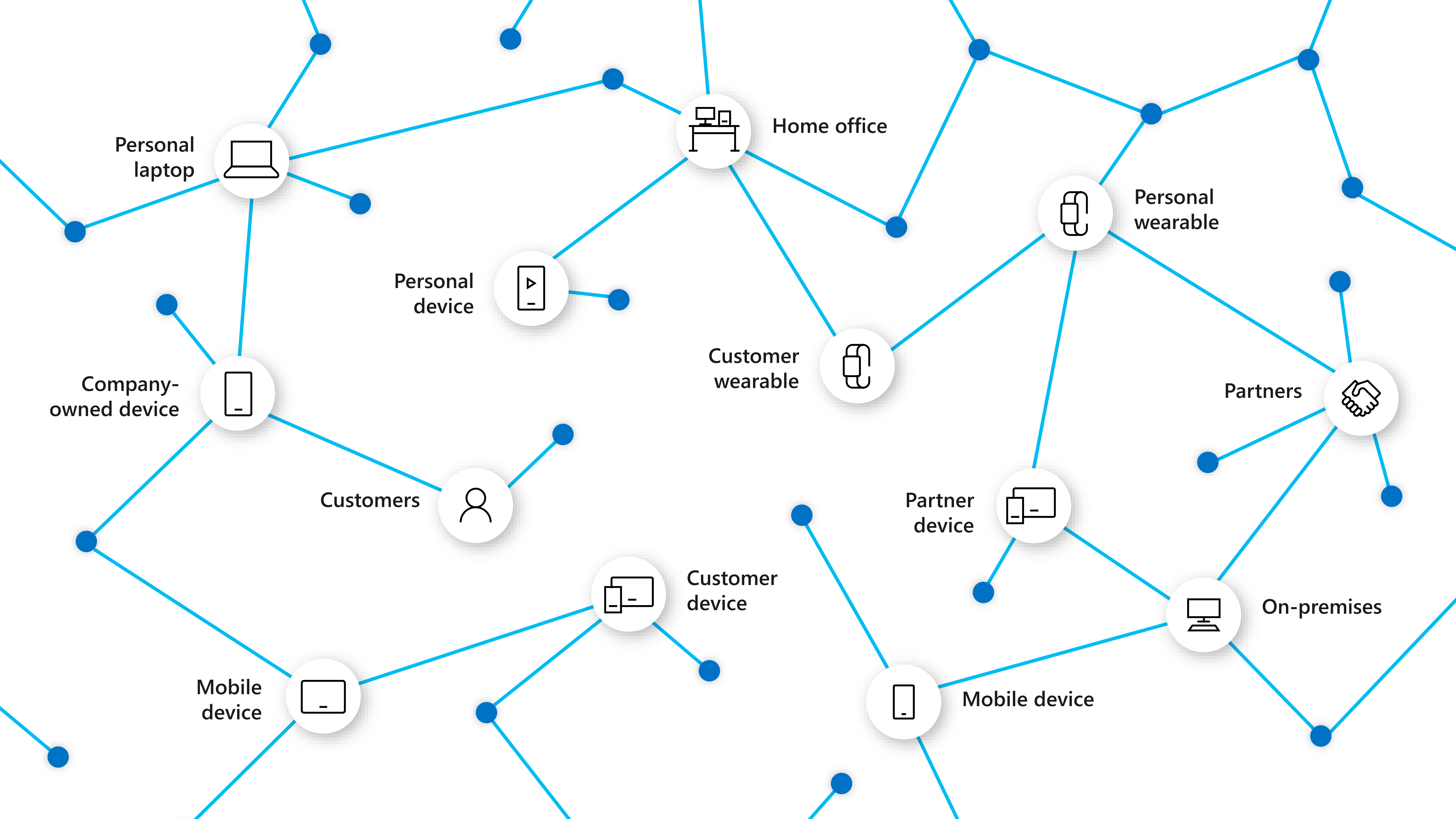


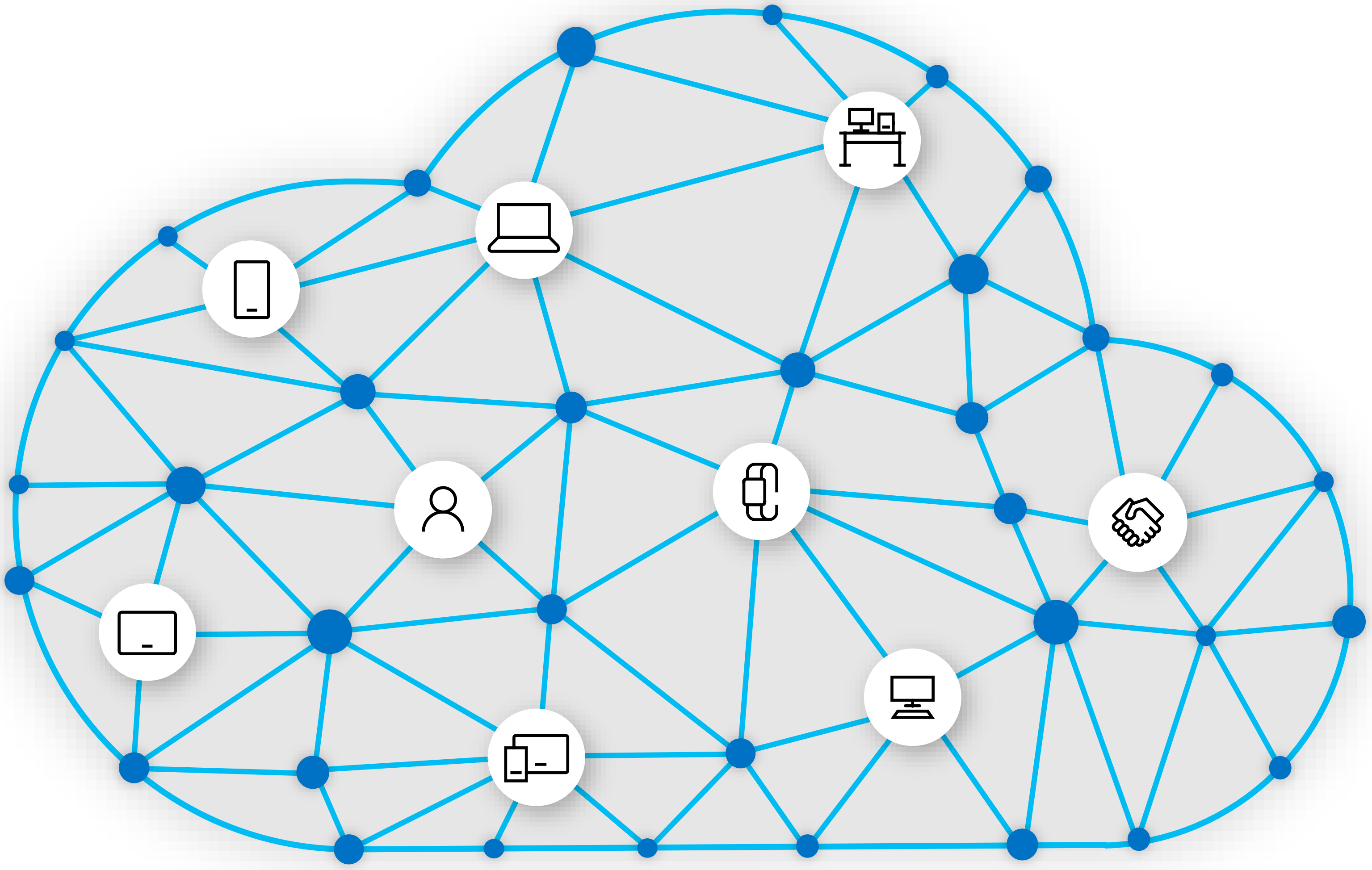
Conventional security tools have not kept pace



Security professionals alone can't fill the gap

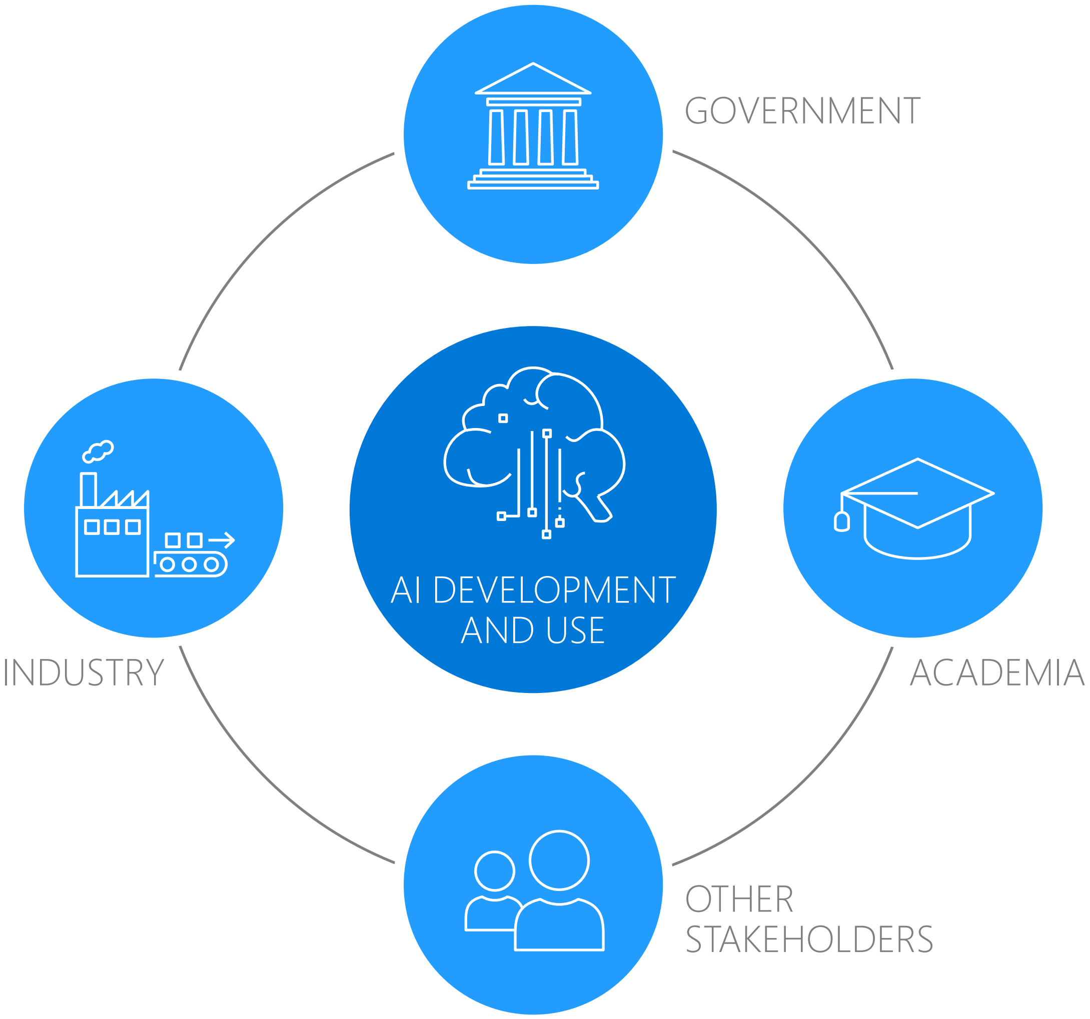
Regulatory requirements and costs are increasing


Personal laptop
Home office
Personal wearable
Personal device
Customer wearable
Company-owned device
Partners
Customers
Partner device
Customer device
On-premises
Mobile device
Mobile device



5. Artificial Intelligence (AI) & Digital Transformation

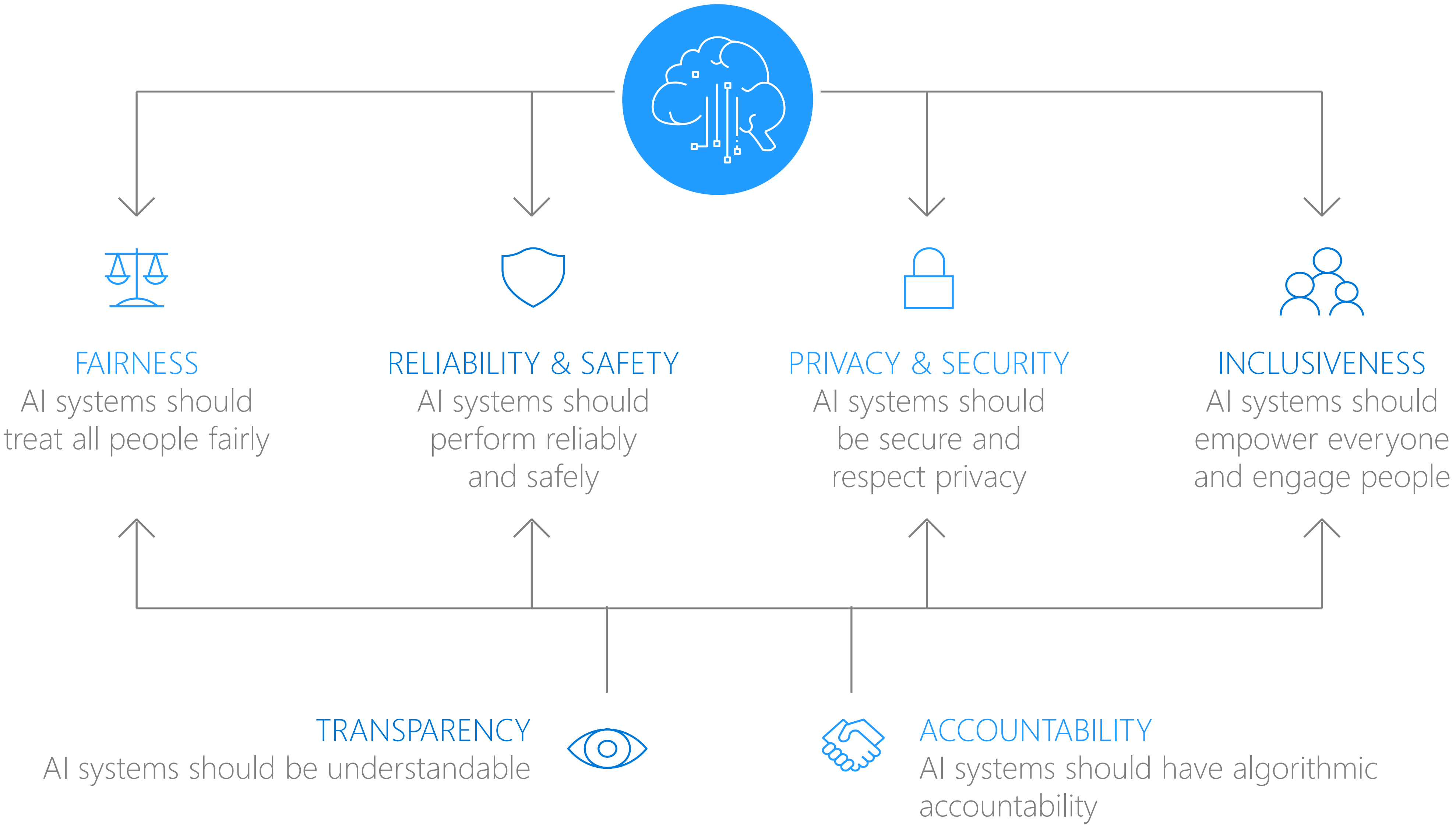
Microsoft and responsible AI innovation



Recommend sustained constructive multi-stakeholder engagement on AI technology to:

- Maximize benefits
- Protect individuals and society
- Define high-level ethical and moral principles
- Support foundational standards helping businesses adopt practices consistent with principles

Microsoft AI principles



FAIRNESS
AI systems should treat all people fairly

RELIABILITY & SAFETY
AI systems should perform reliably and safely

PRIVACY & SECURITY
AI systems should be secure and respect privacy

INCLUSIVENESS
AI systems should empower everyone and engage people

TRANSPARENCY
AI systems should be understandable

ACCOUNTABILITY
AI systems should have algorithmic accountability

Microsoft

PARTNERSHIP ON AI

Founded Sept 2016

Develop and share best-practice methods and approaches in the research, development, testing, and fielding of AI technologies

Advance public understanding of AI across varied constituencies, including on core technologies, potential benefits, and costs

Provide an open and inclusive platform for discussion and engagement on the future of AI, and to ensure that key stakeholders have the knowledge, resources, and capacity to participate

Identify and foster aspirational efforts in AI for socially benevolent applications

Existing frameworks already apply

- AI is already governed by many national, regional and sector-specific laws and regulations
- For example, the EU GDPR requirements already apply whether a solution uses AI or not
- In most cases, existing laws are adequate
- When the use of AI raises new concerns not addressed by existing frameworks new guidance should be considered
- Policy makers should consult with industry, academia, governments and other stakeholders to avoid new actions from inhibiting the responsible use and deployment of AI

New frameworks are in development

Microsoft

The EU will propose a new regulatory framework for AI in early 2021

Our suggestions are that it should:

- Incentivize AI stakeholders to adopt governance standards and procedures
- Leave space for positive uses of AI by keeping down the cost of compliance
- Differentiate types of harm as risks to safety and fundamental rights require different rules
- Clarify which requirements apply to which actors
- Rely on existing laws and regulatory frameworks as much as possible

Healthy development of standards

Microsoft

- Transparent processes
- Open participation
- Bottom-up approach
- Standardization of foundational concepts and management practices discourages the use of standards as a barrier to market access
- Support different ethical and legal regimes
- Promote economic growth and augmenting human capabilities with AI

Standards are one of many tools

Microsoft

New regulations and policies create a need to ensure compliance with certain norms

Standards are often critical in supporting assurance practices

Many tools can help realize policies and regulations

- Standards
- Open Source Software
- Codes of conduct
- Self-attestation
- Operational guidelines

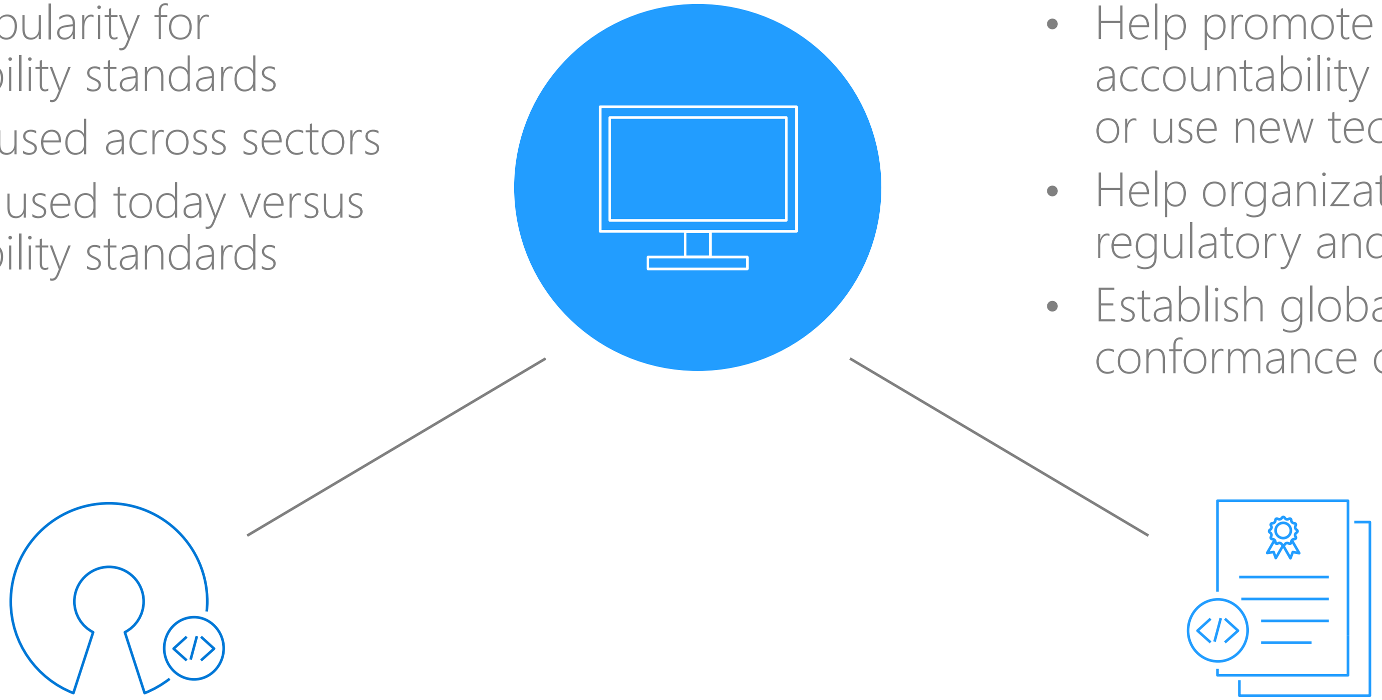
Standards versus open source software

Open Source Software

- Gaining popularity for interoperability standards
- Frequently used across sectors
- Commonly used today versus interoperability standards

Traditional Standards

- Help promote trust and accountability for orgs that produce or use new technologies like AI
- Help organizations meet AI related regulatory and policy requirements
- Establish globally accepted conformance criteria

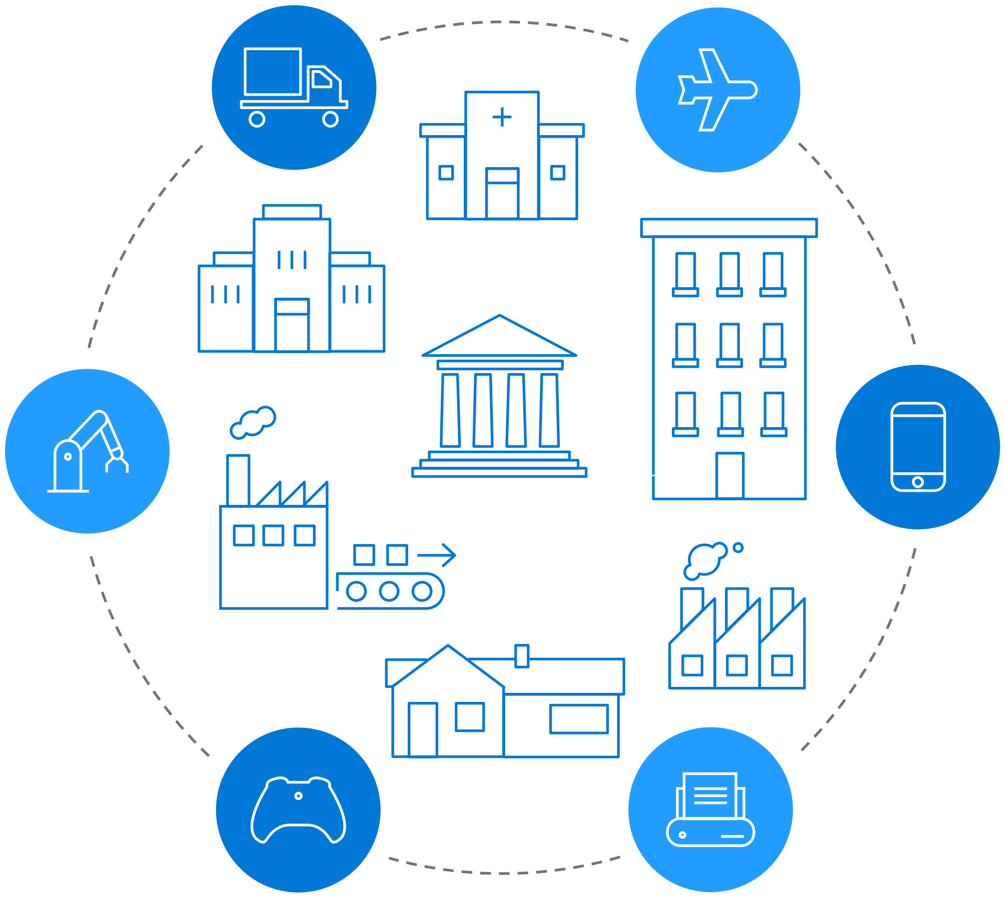


Microsoft

6. Internet of Things (IoT) security

What is the Internet of Things?

Microsoft



Definition:

There is no agreed general definition for the Internet of Things

Defining Characteristics:

Connects a device to a network or the Internet and the physical world

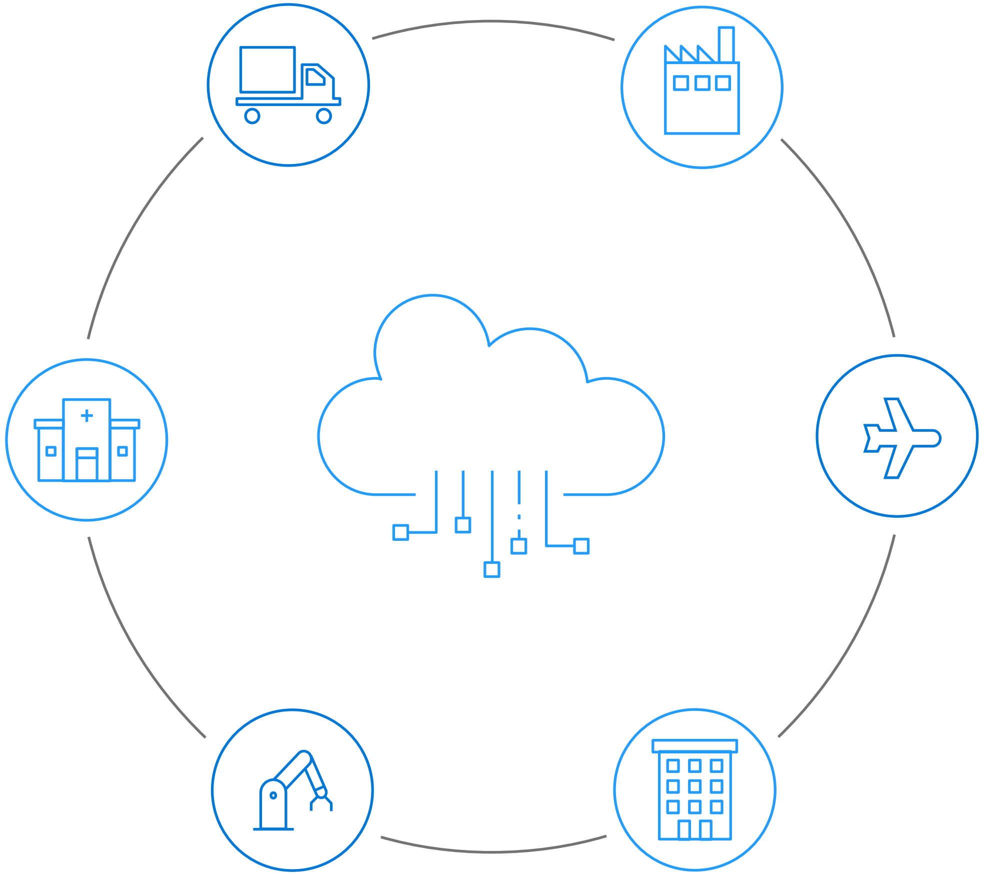
Examples:

- Sensors -> Collect data
- Actuators -> Control the physical world
- Embedded Systems -> Dedicated function
- Legacy -> Connecting any existing widget to the Internet

The potential for IoT

Microsoft

- A fourth industrial revolution for manufacturing
- Real-time collection of large volumes of data
- Input to use for AI and Machine Learning
- Predictive maintenance based on embedded sensors
- Continuous feedback loops
- Medical devices
- New methods of connectivity (5G, satellite, etc.)
- So much more…



Risks

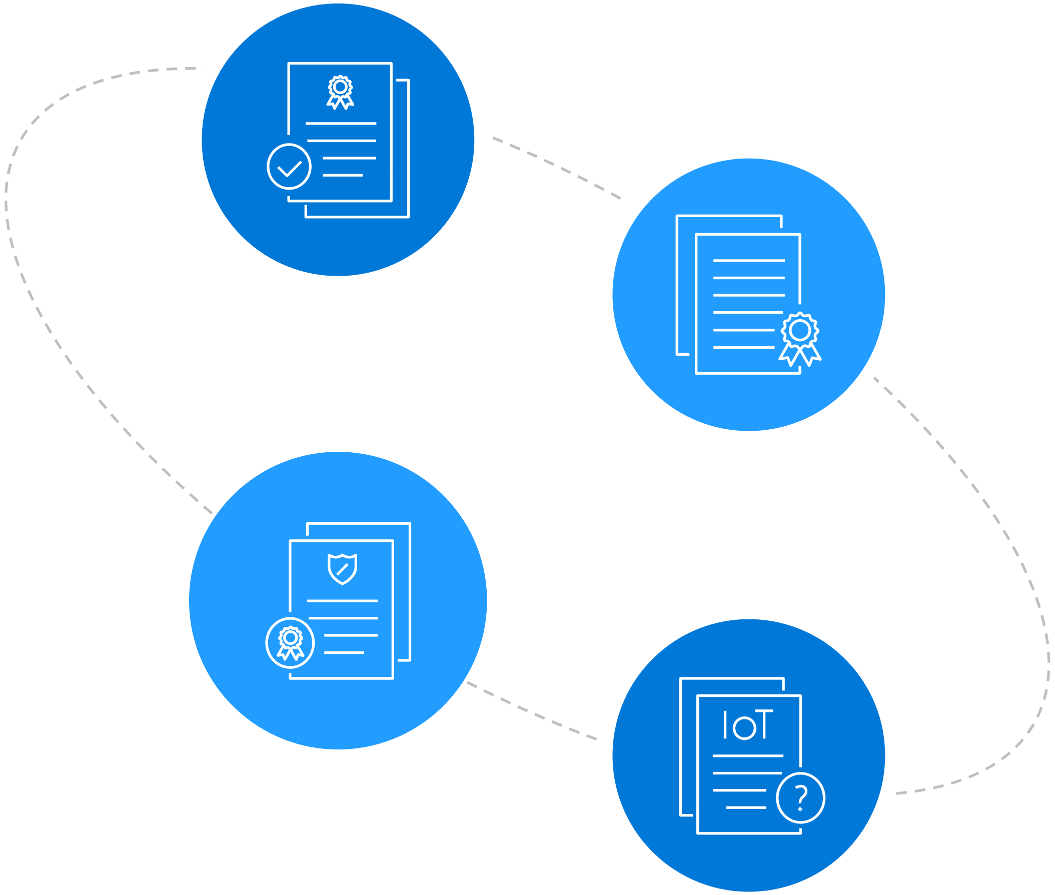
- IoT devices are online
- Will be attacked due to vulnerabilities
- IoT devices are numerous
- Security practices are not prioritized or well-known
- Compromise can be hard to detect

Not just the risk of losing the data on the device:

- Steppingstone for attacking other devices
- Physical world actions impacting safety
- Inaccurate sensor data makes bad decisions

Standards

Microsoft



- Past decade - everyone on the IoT bandwagon
- New and existing organizations generating lots of IoT content
- Fragmentation
- Problems adapting traditional security to IoT
- New low resource security techniques are developing and being adopted
- Promising signs of unification efforts with core security features emerging

NIST IR 8259

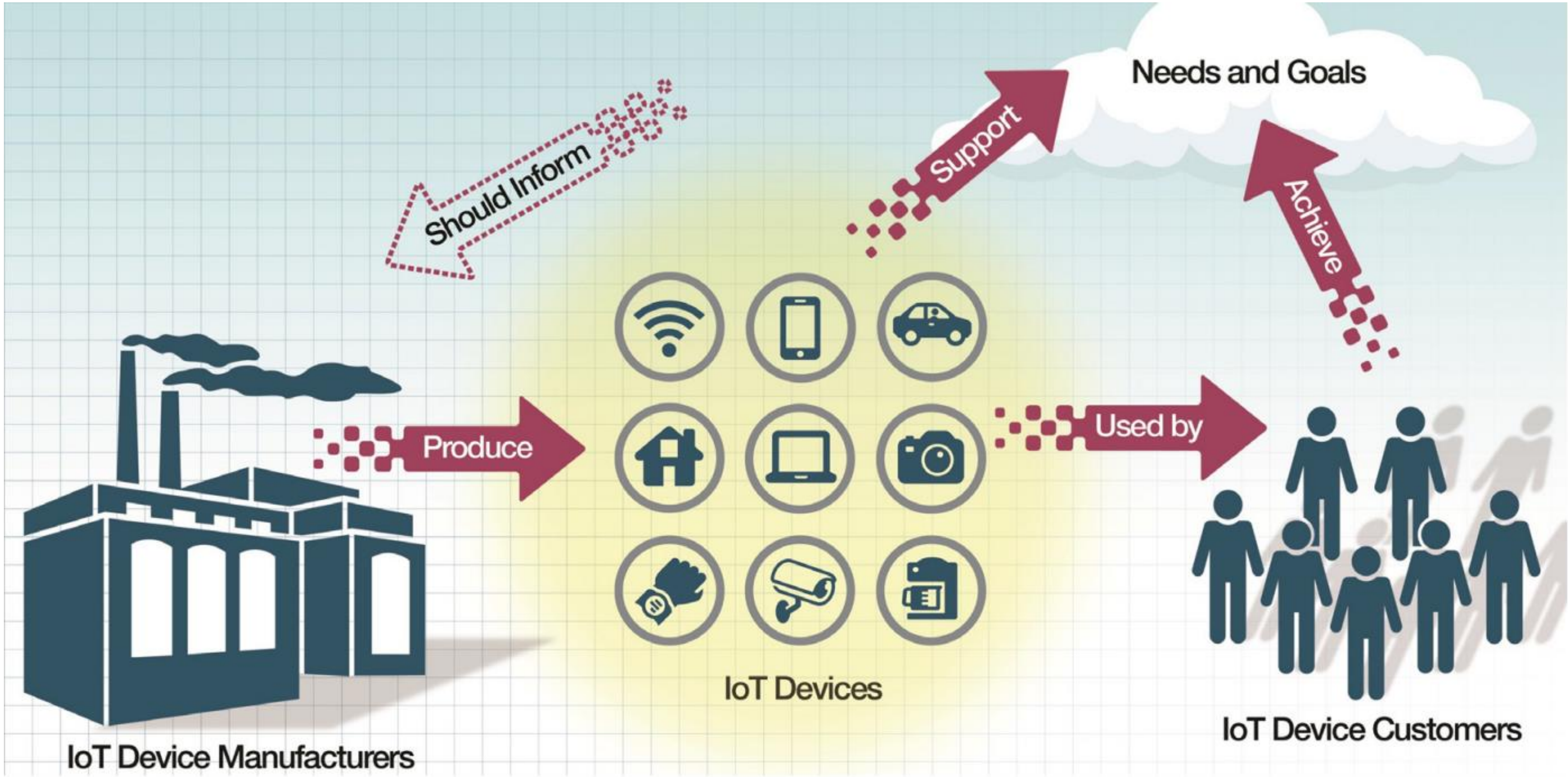


Figure 2: Connections Between IoT Device Manufacturers and Customers Around Cybersecurity[1]

[1] U.S. National Institute of Standards and Technology: Foundational Cybersecurity Activities for IoT Device Manufacturers (NIST IR 8259)

NIST IR 8259A: Core Baseline

- **Device Identification:** Uniquely identified logically and physically
- **Device Configuration:** Software can be reconfigured by authorized entities
- **Data Protection:** Protects the confidentiality and integrity of data it stores and transmits
- **Logical Access to Interfaces:** Restricts logical access to its local and network interfaces (including protocols and services used)
- **Software Update:** Software can be updated using a secure and configurable mechanism
- **Cybersecurity State Awareness:** Can report cybersecurity state to authorized entities (e.g., the owner)

Source: U.S. National Institute of Standards and Technology: IoT Device Cybersecurity Capability (NIST IR 8259A)

ETSI EN 303 645

- European standard with 13 requirements for consumer IoT devices
- Basis for increasing number of policy initiatives

Source: ETSI EN 303 645 V2.1.1: Cyber Security for Consumer Internet of Things: Baseline Requirements

- Keep software updated
- Make it easy for users to delete user data
- Validate input data
- Make systems resilient to outages
- Communicate securely
- Minimize exposed attack surfaces
- Examine system telemetry data
- Securely store sensitive security parameters
- Make installation and maintenance of devices easy
- No universal default passwords
- Ensure software integrity
- Ensure that personal data is secure
- Implement a means to manage reports of vulnerabilities

Regulatory trends and concerns

- Protecting the Internet from IoT devices
- Encouraging industrial competitiveness through IoT adoption
- Data localization
- Procurement recommendations for government use
- Risk in critical infrastructure
- Protecting consumers
- Privacy protection
- Device certification and labeling
- Device lifecycles

Microsoft

Thank you!

Amanda Craig – amcraig@microsoft.com
Chelsea Smethurst – chelseas@microsoft.com
Rachel Azafrani – rachelaz@microsoft.com
Rob Spiger – rob.spiger@microsoft.com