

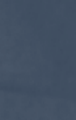
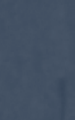


Cybersecurity: Critical Considerations for the Development of the Economy and Digital Society

Angela McKay

Director, Government Security Policy and Strategy

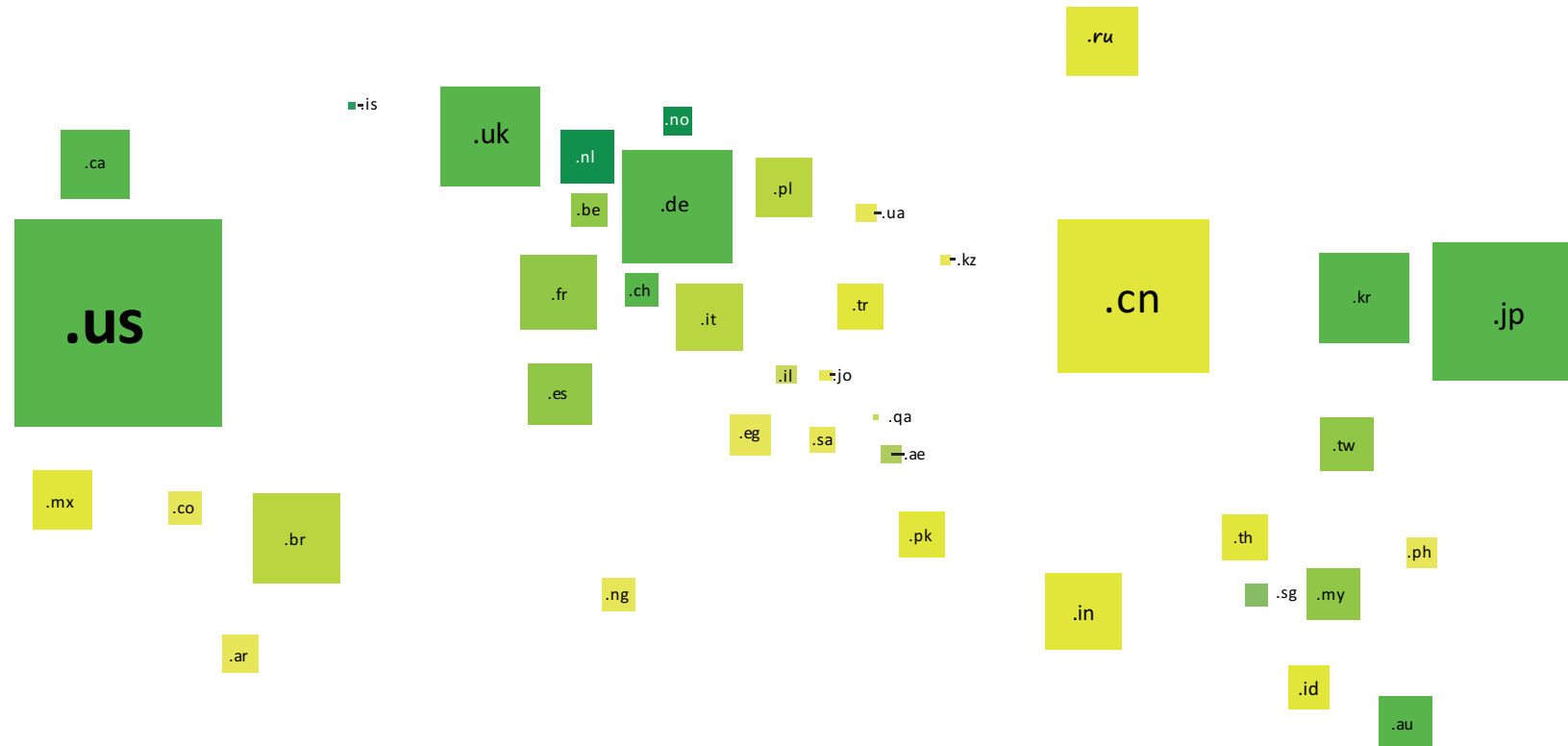
Microsoft



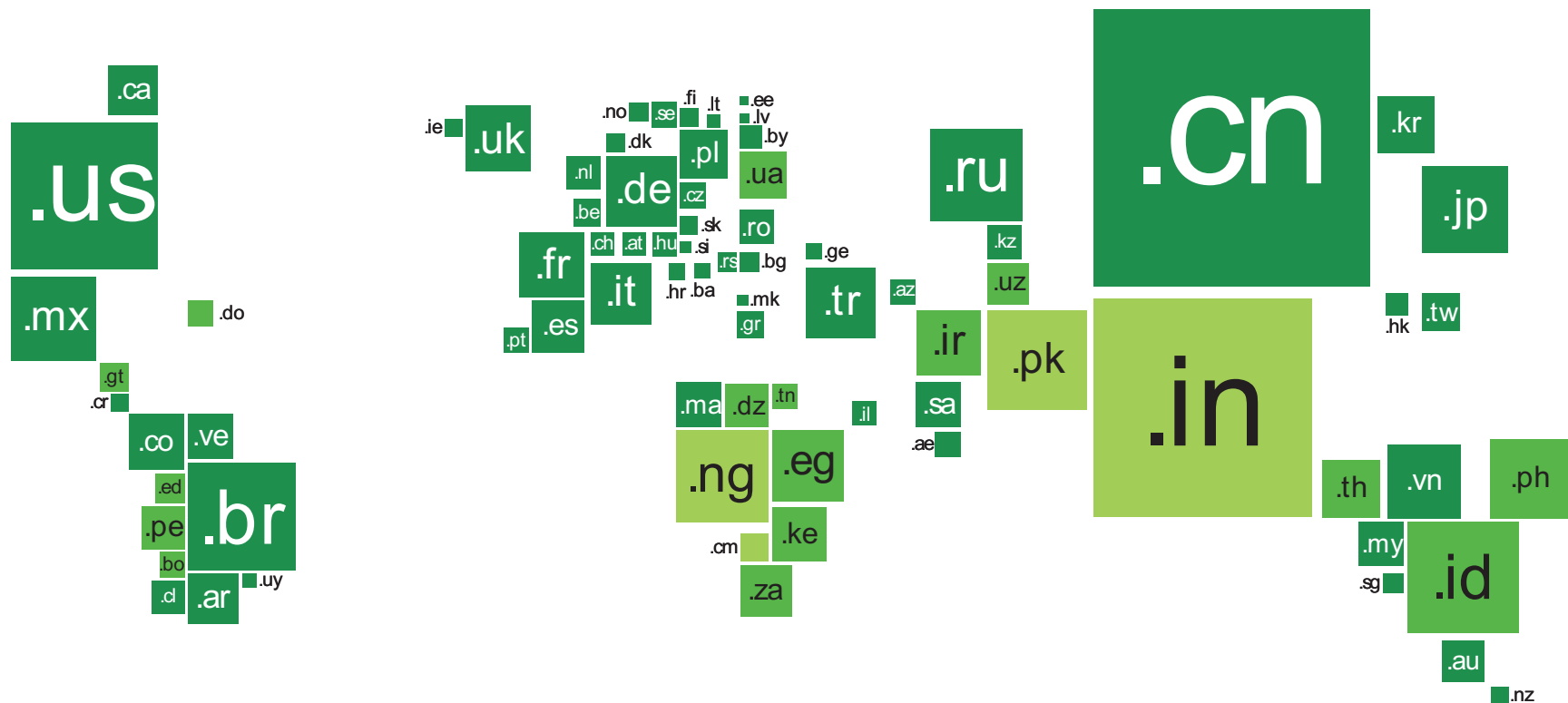
Digital Transformation



Demographic Trends: Internet Users in 2005



Demographic Trends: Internet Users in 2025



Technology Trends

70% 

of CIOs will embrace
a cloud-first strategy
in 2016

50bn

Mobile and IoT connected
devices become ubiquitous



Platform diversity



50x

Data volumes surge



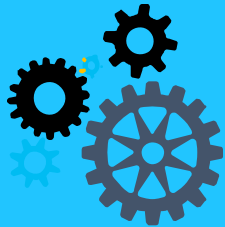
Third Era of Enterprise IT

“Every single industry will be digitally remastered.”

—Mark Raskino, VP & Gartner Fellow

Era 1: IT Craftsmanship

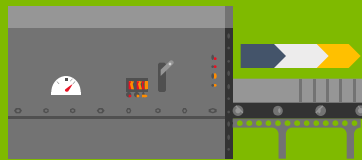
Technology focus



Sporadic automation and innovation; frequent issues

Era 2: Industrialization

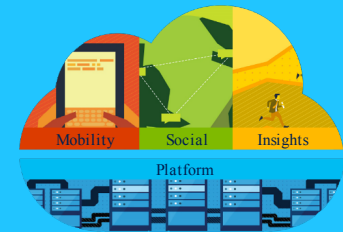
Process focus



Services and solutions; efficiency and effectiveness

Era 3: Digitalization

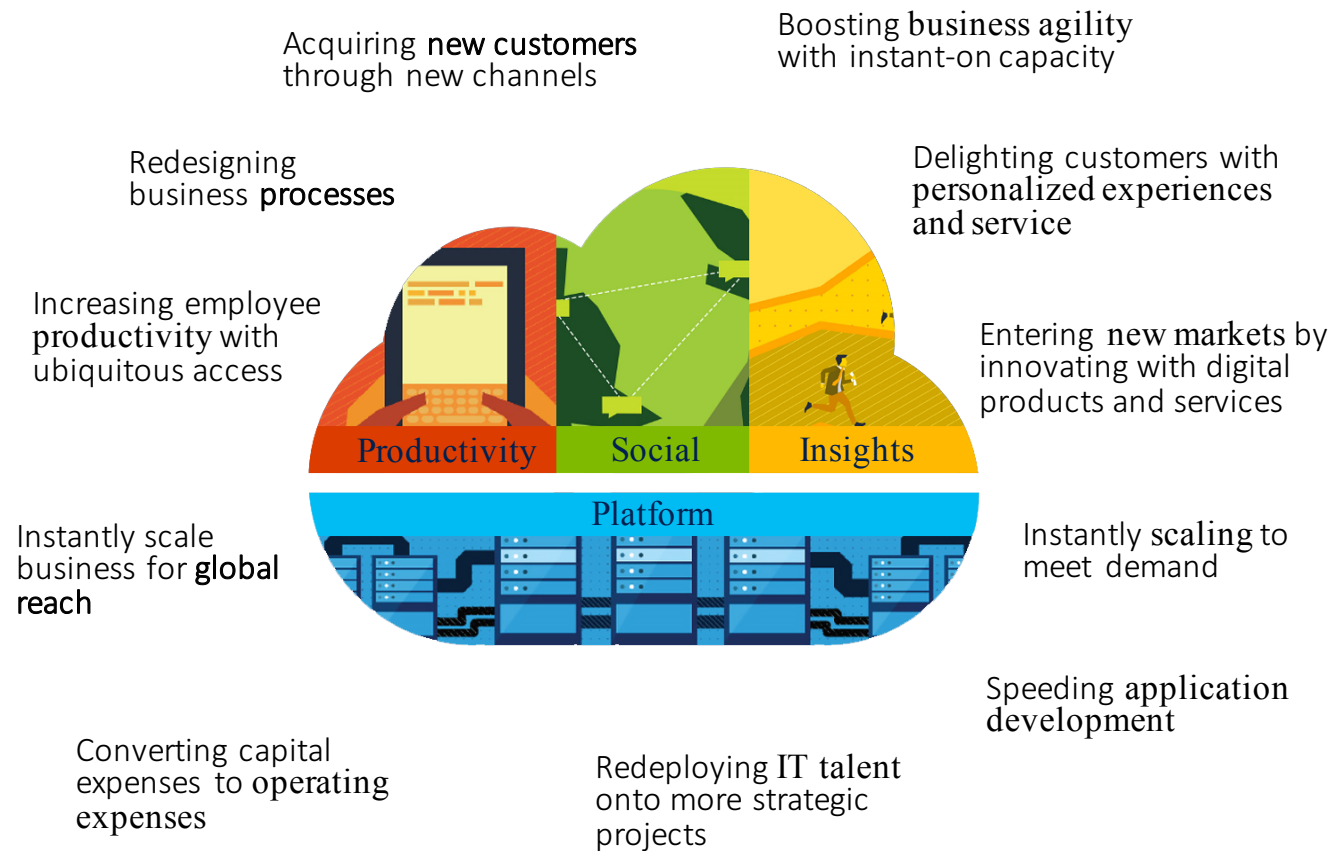
Business model focus



Digital business innovation; new types of service

Today

Cloud as Enabler of Digital Transformation



Speed



2 weeks
to deliver new services vs. 6-12
months with traditional solution

Case Study: HarperCollins Publishers

Scale



Scale from **30,000 to 250,000**
site visitors instantly

Case Study: Autocosmos

Economics



75% less cost
compared to on-premises

Microsoft Azure BI Team, STMG Proof Points Central

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



Economic and Societal Transformation

Job Creation
through
Innovation

Democratization
of Computing

Social Inclusion

Increased Agility

Cost Savings

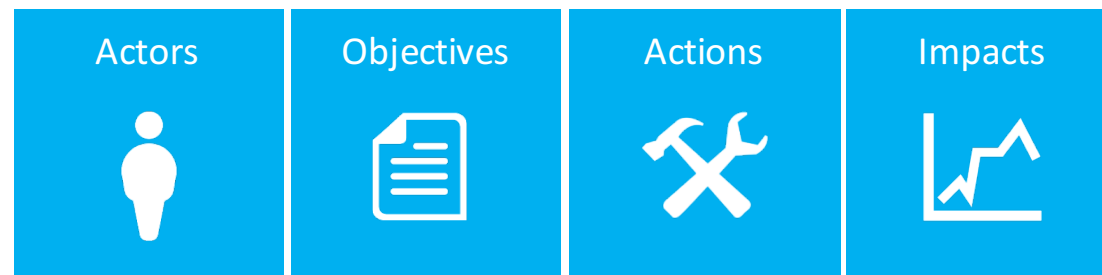
Security



Cyber Risks and Response



Cyber Risk Environment

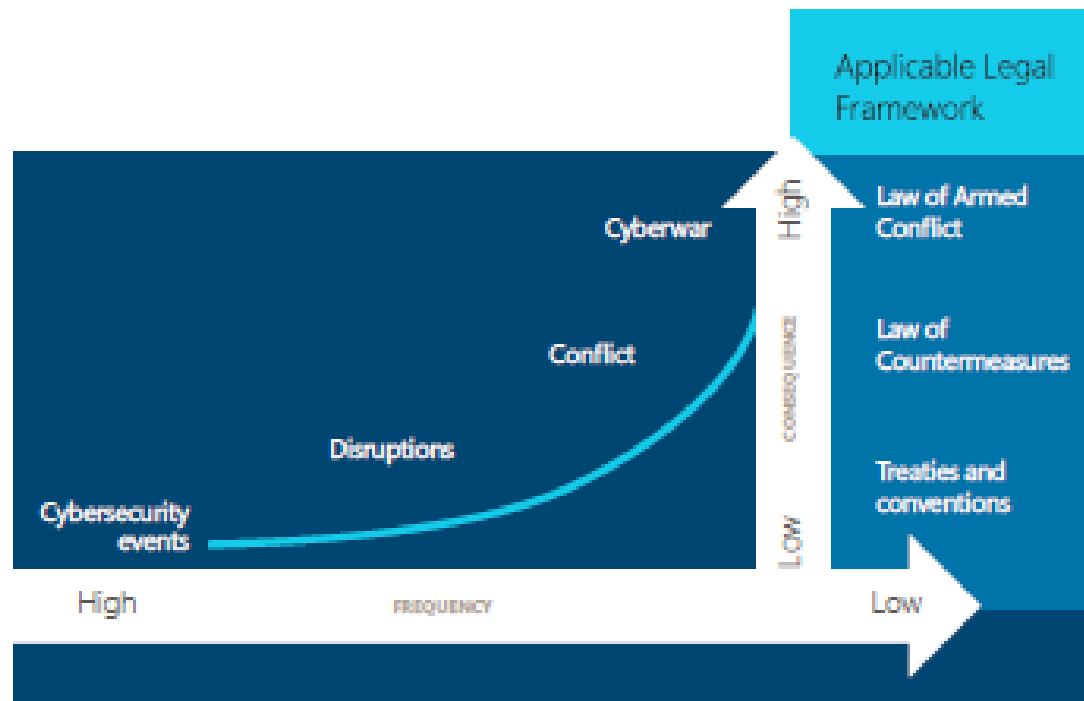


Many methods of attack

Permissive environment

Increasing consequences

Escalating Conflict



Dependence and Risks Drive Public Policy

Systems



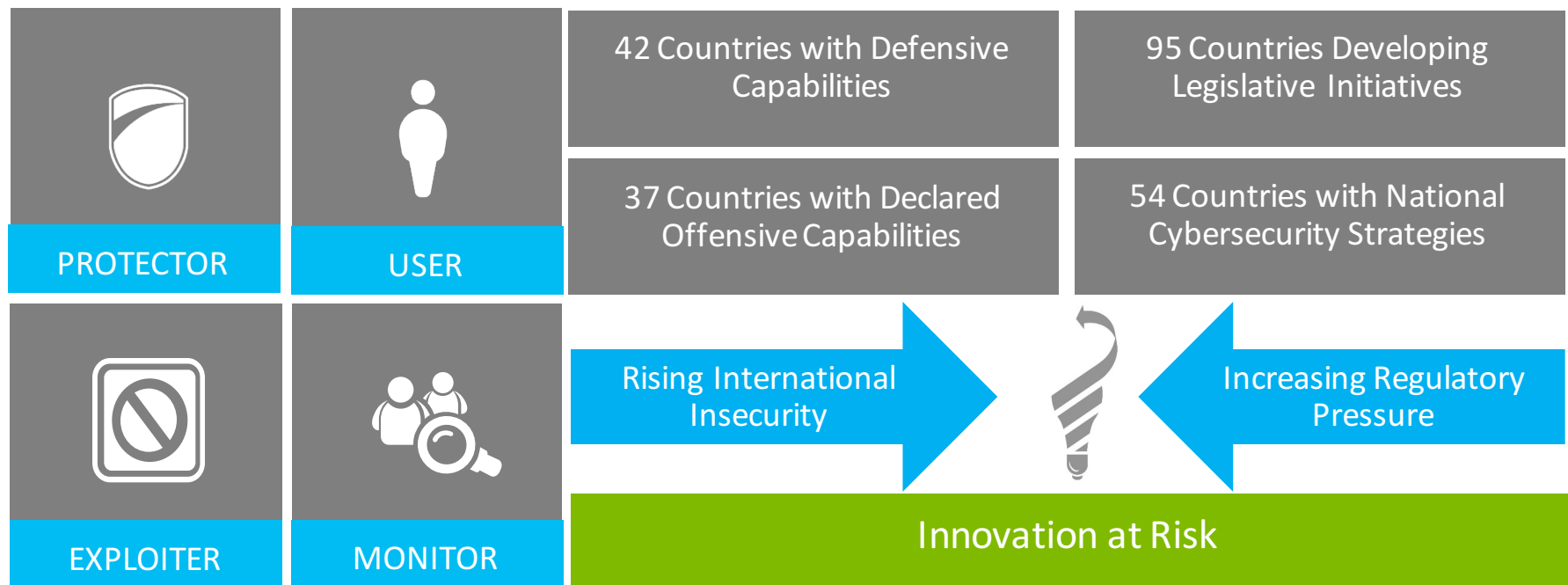
Societies



Sovereignty



Governments' Roles and Regulatory Pressures



Policy Topics at Play

Security of
Government
Systems

Operational
Security and
Controls

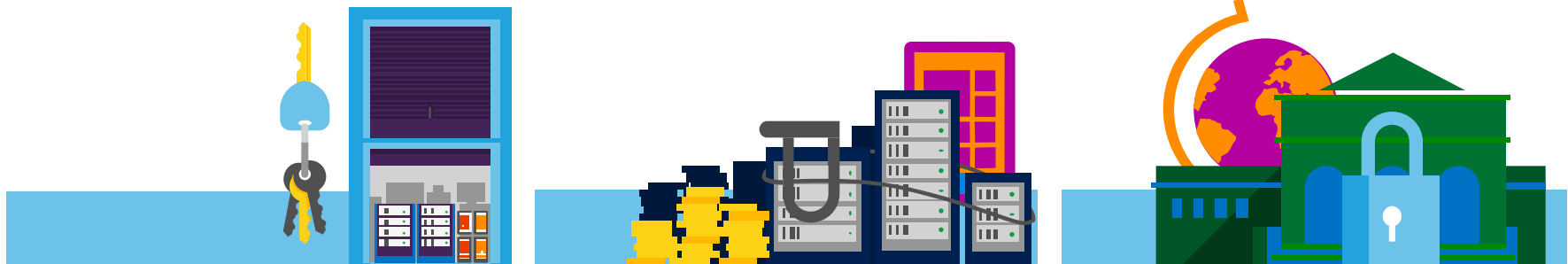
Data Security
and Access

Incident
Reporting and
Information
Sharing

Audit and
Compliance

Cloud
Certification

Enterprise Security
and Compliance



Policy Principles



Innovative



Flexible



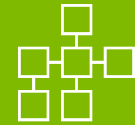
Data aware



Risk based



Standards
based



Transparent

Beyond Regulation



median # of days **attackers are present** on a victim network **before detection**



Average cost of a data breach to a company

15%

increase YoY

Security



level issue

Impact of cyber attacks could be as much as **\$3 trillion** in lost productivity and growth

Job security

Customer loyalty

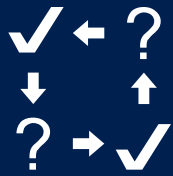
Implications

Brand reputation

Civil liability

Intellectual property

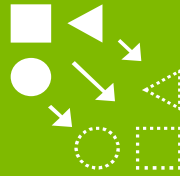
Complexities for the Private Sector in the Digital Age



Loss of trust in
products and
services



Complicated
response cycles
and operational
uncertainties



Distorted threat
models



Reciprocity costs
from state
actions



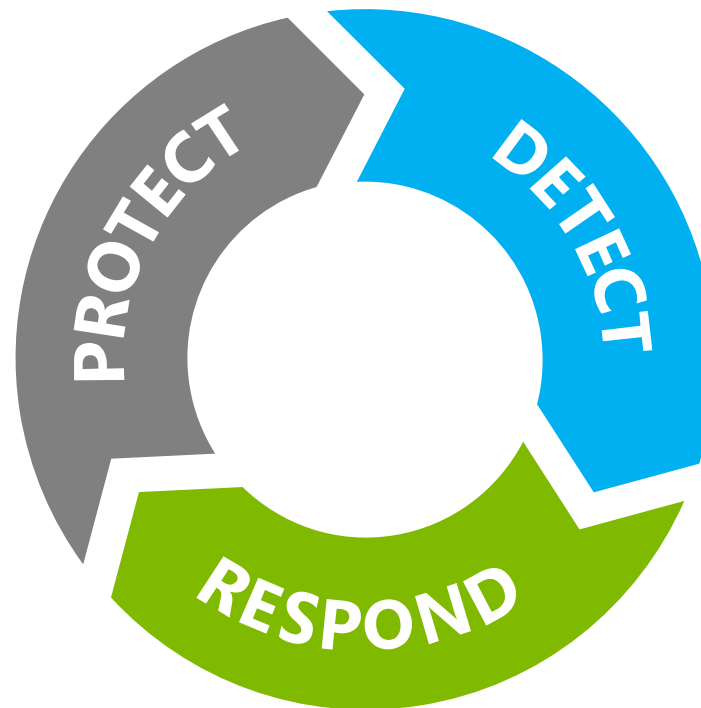
Regulatory costs
from dynamic
compliance
environment

Enterprise Risk Management

Continuous risk management is the key to advancing persistent security.

Innovating in response to attacks and incidents develops and grows sustained capabilities.

Cultural adaptation is required in the face of rapidly changing threats.



Due Diligence for Cybersecurity

Integrated, holistic approach
beyond just IT

Dedicated staff and budget

Governance

Standards,
Controls, and
Compliance

3rd Party Risks

Audit

Continuous
improvement

Collective Security



Microsoft Commitment to Cybersecurity

We have built a culture of strong privacy principles and leading security practices

We invest deeply in building a trustworthy computing platform and security expertise

We proactively fight cybercrime and advocate extensively for policies and action that enhance cybersecurity

Compliance

Risk management

Cybersecurity

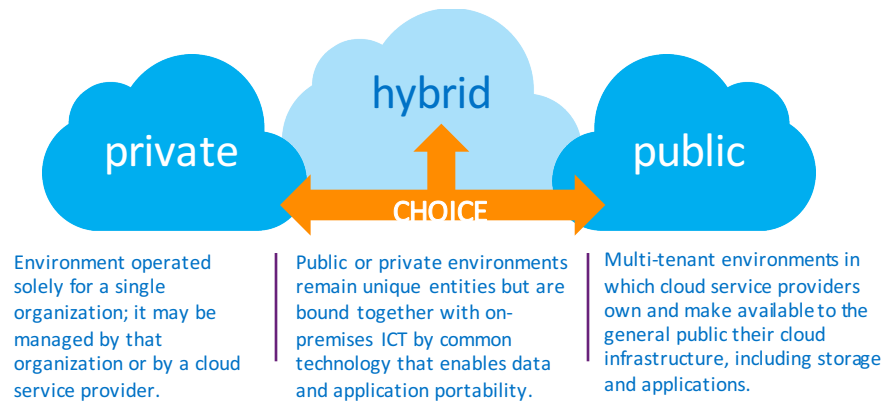
Transparency

Governance

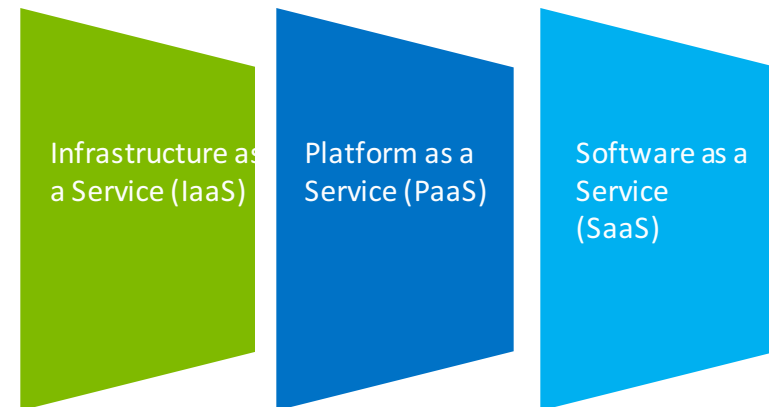
Advocacy

Risk Informed Choice

Deployment models



Service models



Trusted Cloud Principles

Commitment to principles worthy of your organization's trust

Security



The confidentiality, integrity, and availability of your data is protected.

Privacy & Control



No one is able to use your data in a way that you do not approve.

Compliance



Your data is stored and managed in compliance with applicable laws, regulations and standards.

Transparency



You have visibility into how your data is being handled and used.

Synergistic Roles

Private Sector

- ✓ Manage risks to systems and data
- ✓ Exchange information to enable ecosystem risk management
- ✓ Enable greater control, demonstrate compliance, be transparent
- ✓ Coordinate vulnerability handling
- ✓ Provide technical expertise to governments on cybersecurity challenges
- ✓ Help identify critical infrastructure functions that would create unacceptable impacts, and should not be subject to offensive actions
- ✓ Catalyze action to define cybersecurity norms

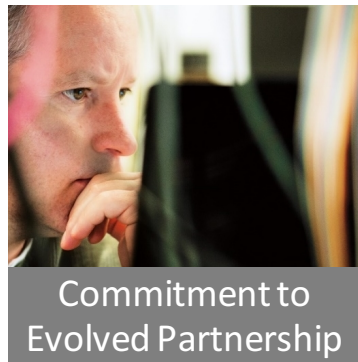
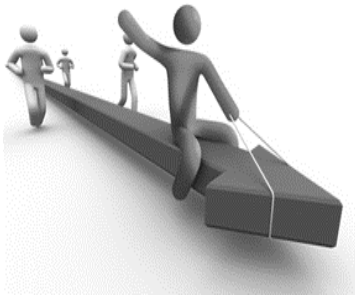
Public Sector

- ✓ Harmonize risk management requirements
- ✓ Exchange information to enable ecosystem risk management
- ✓ Create agile regimes for compliance that leverage existing standards
- ✓ Publish a vulnerability handling policy
- ✓ Engage with private sector to understand technical challenges, esp. potential consequences of actions
- ✓ Increase transparency on defensive and offensive capabilities and criteria for use
- ✓ Define and implement cybersecurity norms

Efficient and Effective Partnership



Advancing Persistent Security Together



Commitment to
Evolved Partnership

Synergistic roles

Risk management, information sharing,
vulnerability handling,
critical infrastructure protection,
norms

Timely,
demonstrable results

Transparency



Multi-stakeholder



Converging Interests



Innovative



Microsoft