Alex Pessó
Legal and Corporate Affairs Director
Microsoft Chile

Baseline Privacy Legislation

TRANSPARENCY	INDIVIDUAL EMPOWERMENT	CORPORATE RESPONSIBLITY	STRONG ENFORCEMENT
• reasonably informed individual	• empowered to express privacy preferences	• data protected • documented risk assessments	• strong regulator

Baseline Privacy Legislation

Responsibility – Controller/Processor Distinction

- It is important to maintain a distinction in responsibility between a data controller, which determines the means and purposes of processing data, and a data processor, which processes the data on behalf of another organization.
    - A data controller should be primarily responsible for meeting privacy obligations and for providing redress to individuals. So long as a data processor merely processes data on behalf of a data controller, the processor's responsibility should be to follow its data controller's instructions and to assist the data controller in meeting its privacy and security obligations.
- Liability should be allocated among organizations that process data according to their agreement, or barring an agreement, then according to demonstrated fault giving rise to the liability.

Baseline Privacy Legislation

- **Consent and Other Grounds for Processing**

- Consent

  - Consent is an important ground for processing data, and the requirements for obtaining consent should be strong.
  - Consent should not be the only basis for processing data.
  - Providing notice and obtaining consent at the point of data collection is at times either impractical or unnecessary. Individuals can be interrupted and overwhelmed if constantly presented with privacy choices and requests to collect data.

- Legitimate Interest

  - The “legitimate interest” legal ground for processing, which is incorporated into many global privacy laws, is vital for enabling companies to collect data that is necessary to support, deliver and improve a variety of services for the benefit of the data subject, controller or society.

Microsoft’s Privacy Principles

Your data, powering your experiences, controlled by you. [Microsoft Privacy]

Benefits to you

When we do collect data, we will use it to benefit you and to make your experiences better.

Control

We will put you in control of your privacy with easy-to-use tools and clear choices.

Transparency

We will explain what we do with your data in clear, plain language.

Security

We will implement strong security measures to safeguard your data.

Strong Legal Protection

We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.

No content-based targeting

We will not use your email, chat, files or other personal content to target ads to you.

Security

We will ensure that all your data is secure

We spend over $1 billion a year on cybersecurity.

3,500+ security professionals work to secure datacenters and hunt down attackers.

We block more than 5 billion distinct malware threats per month.

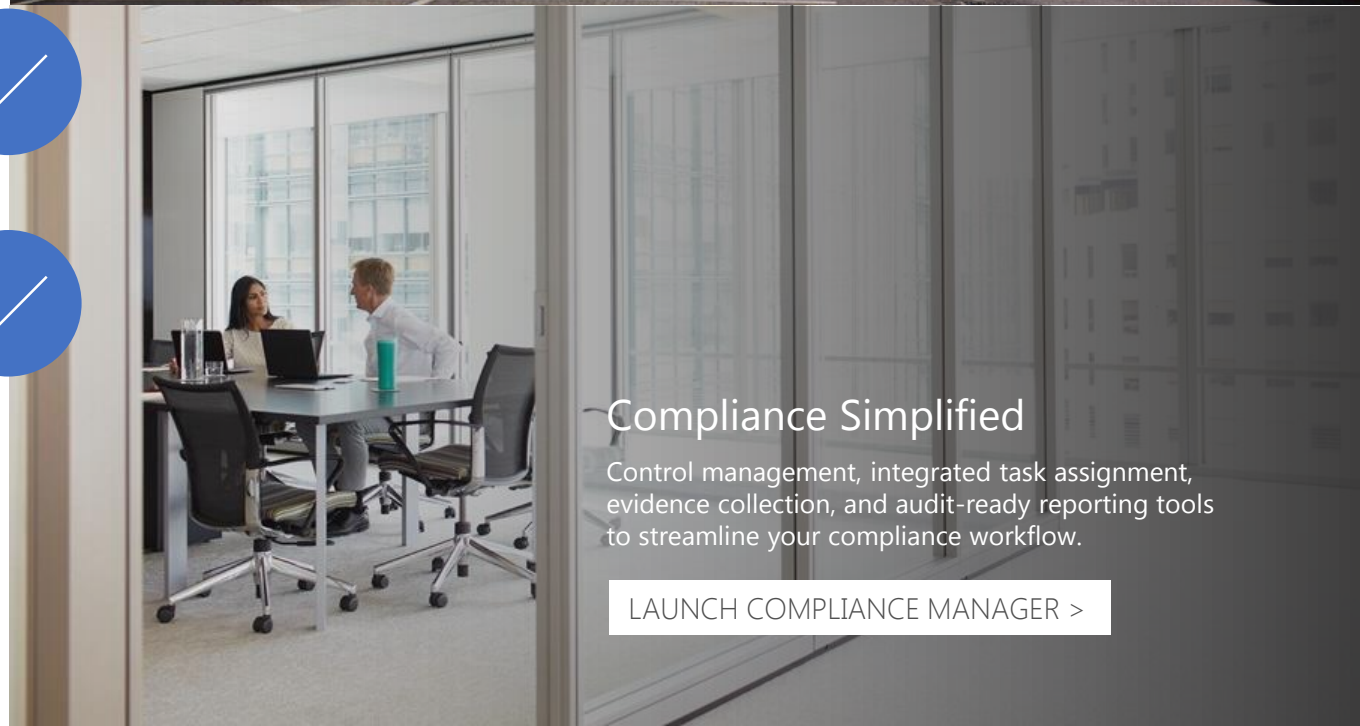
Transparency

We will be transparent about the collection and the uses of data

We provide geographic locations where customer data is stored.

We publish the number of legal demands for customer data that we receive from law enforcement agencies.

We provide visibility into what we do with customer data, how we protect it, and how they are in control.



Compliance

We will manage your data in accordance with the law of the land

We have the most comprehensive compliance coverage in the industry.

We committed to sharing our experiences in complying with complex regulations.

We make several resources available to help our customers along their Compliance journey.

Global

- ☑ ISO 27001:2013
- ☑ ISO 27017:2015
- ☑ ISO 27018:2014
- ☑ ISO 22301:2012
- ☑ ISO 9001:2015
- ☑ ISO 20000-1:2011
- ☑ SOC 1 Type 2
- ☑ SOC 2 Type 2
- ☑ SOC 3
- ☑ CSA STAR Certification
- ☑ CSA STAR Attestation
- ☑ CSA STAR Self-Assessment
- ☑ WCAG 2.0 (ISO 40500:2012)

US Gov

- ☑ FedRAMP High
- ☑ FedRAMP Moderate
- ☑ EAR
- ☑ DFARS
- ☑ DoD DISA SRG Level 5
- ☑ DoD DISA SRG Level 4
- ☑ DoD DISA SRG Level 2
- ☑ DoE 10 CFR Part 810
- ☑ NIST SP 800-171
- ☑ NIST CSF
- ☑ Section 508 VPATs
- ☑ FIPS 140-2
- ☑ ITAR
- ☑ CJIS
- ☑ IRS 1075

Industry

- ☑ PCI DSS Level 1
- ☑ GLBA
- ☑ FFIEC
- ☑ Shared Assessments
- ☑ FISC (Japan)
- ☑ APRA (Australia)
- ☑ FCA (UK)
- ☑ MAS + ABS (Singapore)
- ☑ 23 NYCRR 500
- ☑ HIPAA BAA
- ☑ HITRUST

Regional

- ☑ Argentina PDPA
- ☑ Australia IRAP Unclassified
- ☑ Australia IRAP PROTECTED
- ☑ Canada Privacy Laws
- ☑ China GB 18030:2005
- ☑ China DJCP (MLPS) Level 3
- ☑ China TRUCS / CCCPPF
- ☑ EN 301 549
- ☑ EU ENISA IAF
- ☑ EU Model Clauses
- ☑ EU – US Privacy Shield
- ☑ GDPR
- ☑ Germany C5
- ☑ Germany IT-Grundschutz workbook
- ☑ India MeitY
- ☑ Japan CS Mark Gold
- ☑ Japan My Number Act
- ☑ Netherlands BIR 2012
- ☑ New Zealand Gov CC Framework
- ☑ Singapore MTCS Level 3
- ☑ Spain ENS
- ☑ Spain DPA
- ☑ UK Cyber Essentials Plus
- ☑ UK G-Cloud
- ☑ UK PASF

Industry

- ☑ 21 CFR Part 11 (GxP)
- ☑ MARS-E
- ☑ NHS IG Toolkit (UK)
- ☑ NEN 7510:2011 (Netherlands)
- ☑ FERPA
- ☑ CDSA
- ☑ MPAA
- ☑ DPP (UK)
- ☑ FACT (UK)
- ☑ SOX

microsoft.com/en-us/trustcenter/compliance/complianceofferings

Cybersecurity In The News, In The Boardroom

Cost (USD) of cybercrime to global economy by 2022

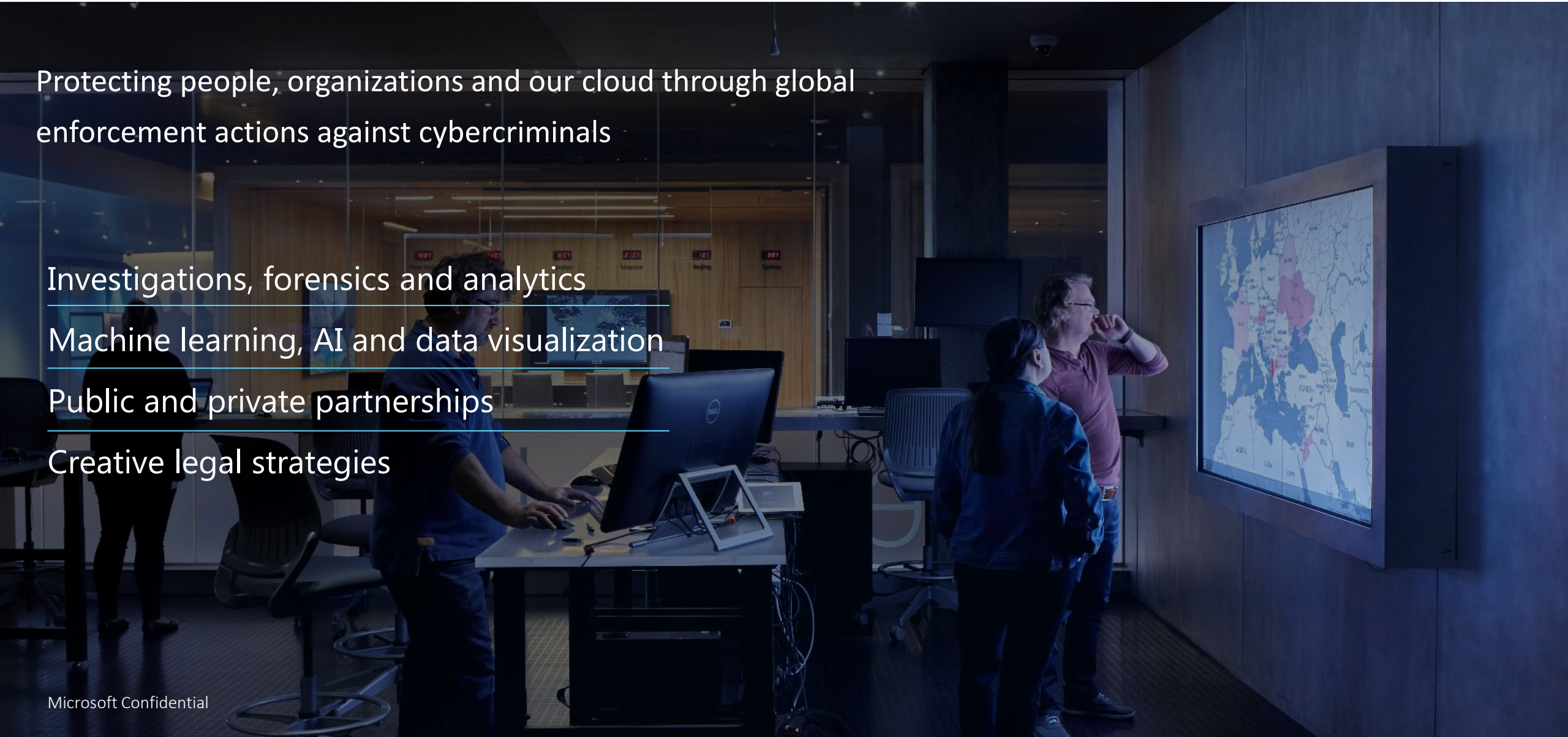
Growth in ransomware families in 12 months

1.6M Average cost of a spear-phishing attack

99 DAYS Median number of days between infiltration and detection

200% Business email compromise increase in six months

Digital Crimes Unit: Leading the fight against crime



Protecting people, organizations and our cloud through global enforcement actions against cybercriminals

- Investigations, forensics and analytics
- Machine learning, AI and data visualization
- Public and private partnerships
- Creative legal strategies