Who Owns Your Data?

Prof. Scott J. Shackelford JD, PhD
Angie Raymond, JD, PhD

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

Ostrom Workshop

- **Programs**
- – (Environment &) Natural Resource Governance
  – Commons Governance
  – Cybersecurity & Internet Governance
  – Information & Data Governance
  – Political Economy
- **Affiliates** – 300+ in total
- **Working Groups (20+)**
  - Polycentricity
  - Space Governance
  - Artistic Inspiration & the Commons
- **Conferences & Events**
  - Memorial Lectures
  - Smart Cities
  - Workshop on the Ostrom Workshop (WoW)
- **Visiting Scholars**
- **Ostrom Fellowships**
- **Research Awards**
- **Seed Grants**

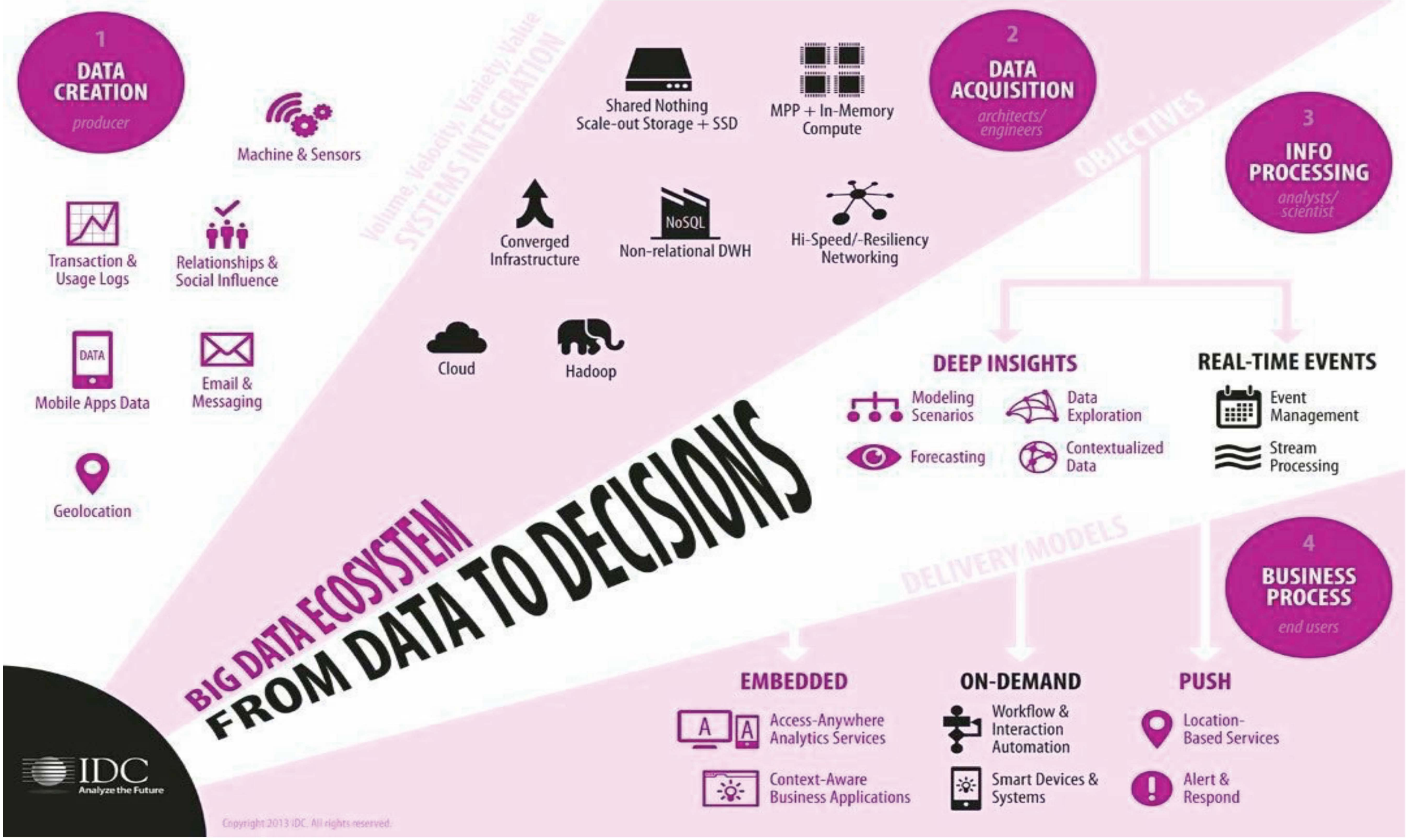
SECTION 1

DATA: WHY IS IT AN ISSUE

Corporations

- Chances are good, you have a ton of data
- And you might have a data management plan, then again - you might have Tom….
- But everyone knows - you want to make

  ‘data driven decisions’

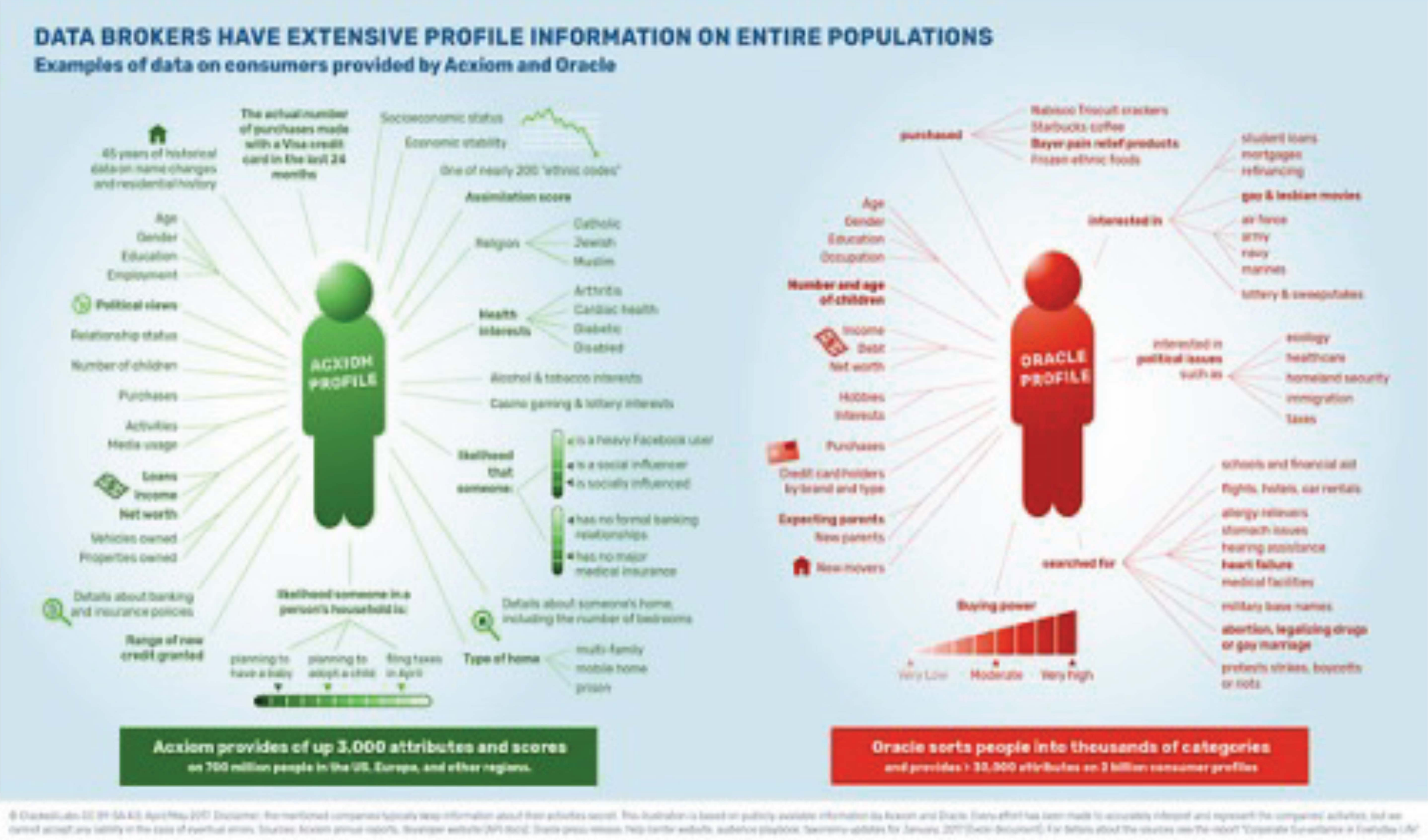

1
DATA CREATION
producer
Machine & Sensors
Transaction & Usage Logs
Relationships & Social Influence
DATA
Mobile Apps Data
Email & Messaging
Geolocation
Volume, Velocity, Variety, Value
SYSTEMS INTEGRATION
Shared Nothing Scale-out Storage + SSD
MPP + In-Memory Compute
2
DATA ACQUISITION
architects/ engineers
Converged Infrastructure
NoSQL
Non-relational DWH
Hi-Speed/-Resiliency Networking
Cloud
Hadoop
OBJECTIVES
3
INFO PROCESSING
analysts/ scientist
DEEP INSIGHTS
Modeling Scenarios
Data Exploration
Forecasting
Contextualized Data
REAL-TIME EVENTS
Event Management
Stream Processing
BIG DATA ECOSYSTEM
FROM DATA TO DECISIONS
DELIVERY MODELS
4
BUSINESS PROCESS
end users
EMBEDDED
A
A
Access-Anywhere Analytics Services
Context-Aware Business Applications
ON-DEMAND
Workflow & Interaction Automation
Smart Devices & Systems
PUSH
Location-Based Services
Alert & Respond
IDC
Analyze the Future

So….

- Its not REALLY (usually) about who owns the data. It's about:
  - WHO has CONTROL of the data
  - WHAT RESPONSIBILITY goes with that control
  - (and sometimes, it might be about who owns it….)

SECTION 2

DATA 101



DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle

Acxiom provides of up 3.000 attributes and scores
on 700 million people in the US, Europe, and other regions.

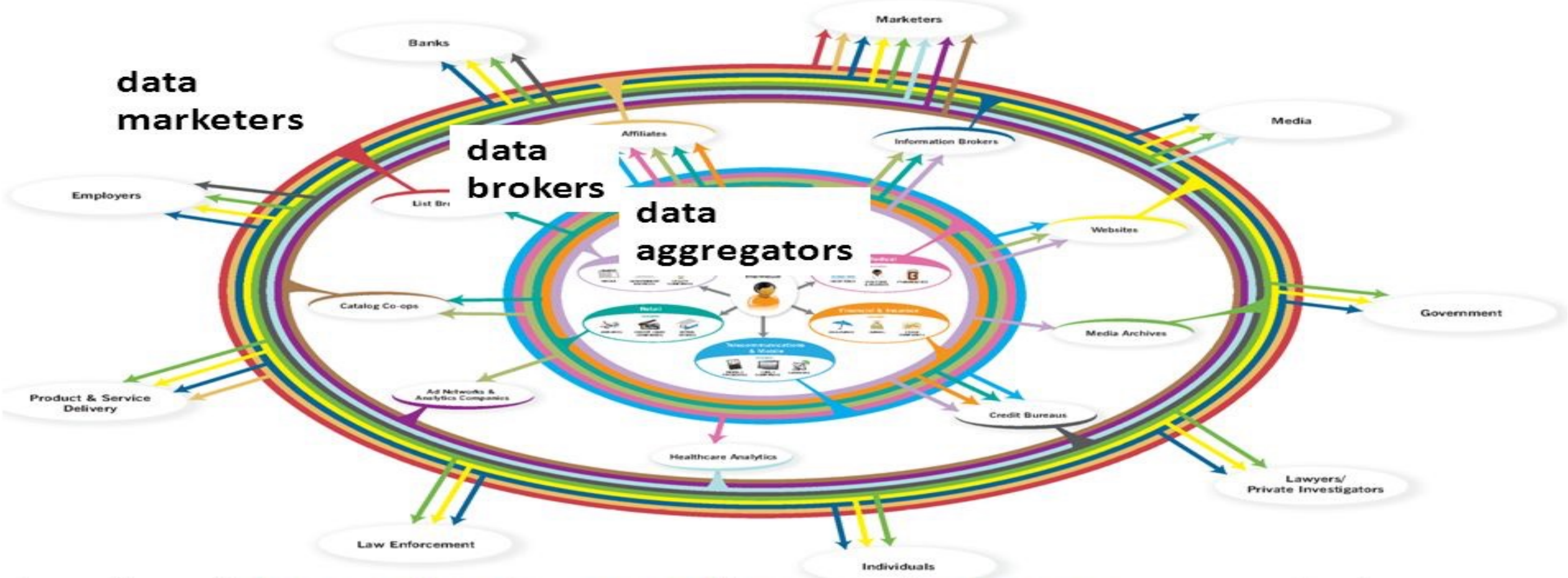
Oracle sorts people into thousands of categories
and provides > 30,000 attributes on 2 billion consumer profiles

© CrackedLabs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information by Acxiom and Oracle. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Acxiom annual reports, developer website (API docs); Oracle press release, help center website, audience playbook, taxonomy updates for January 2017 (Oracle document). For details about the sources see the report "Corporate Surveillance in Everyday Life"

DATA is EVRYWHERE

Emerging Data Subjects

http://www.ftc.gov/bcp/workshops/privacyroundtables/personalDataEcosystem.pdf



A series of data stewards , custodians , and curators are producing, consuming and brokering data products forming a far more **complex value making chain** than in traditional enterprise or scientific contexts

Sometimes-

- Sometimes, it might be about who owns it….
- Because- if you OWN it- you can
  - sell it,
  - license it,
  - share it,
  - limit its use,
  - And, of course it then often time HAS VALUE

And there are LAWS: FEDERAL LAW

- The United States doesn’t have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA.

As with the national laws, there are state-level laws that carve out coverage of individual aspects of data privacy. Missouri has ebook privacy rules. The Illinois Biometric Information Privacy Act (BIPA) gives people privacy rights over their biometric data, such as their fingerprint or face scans. When it comes to data-breach notifications, it's particularly hard to know your rights, with at least 54 different laws that vary by region.

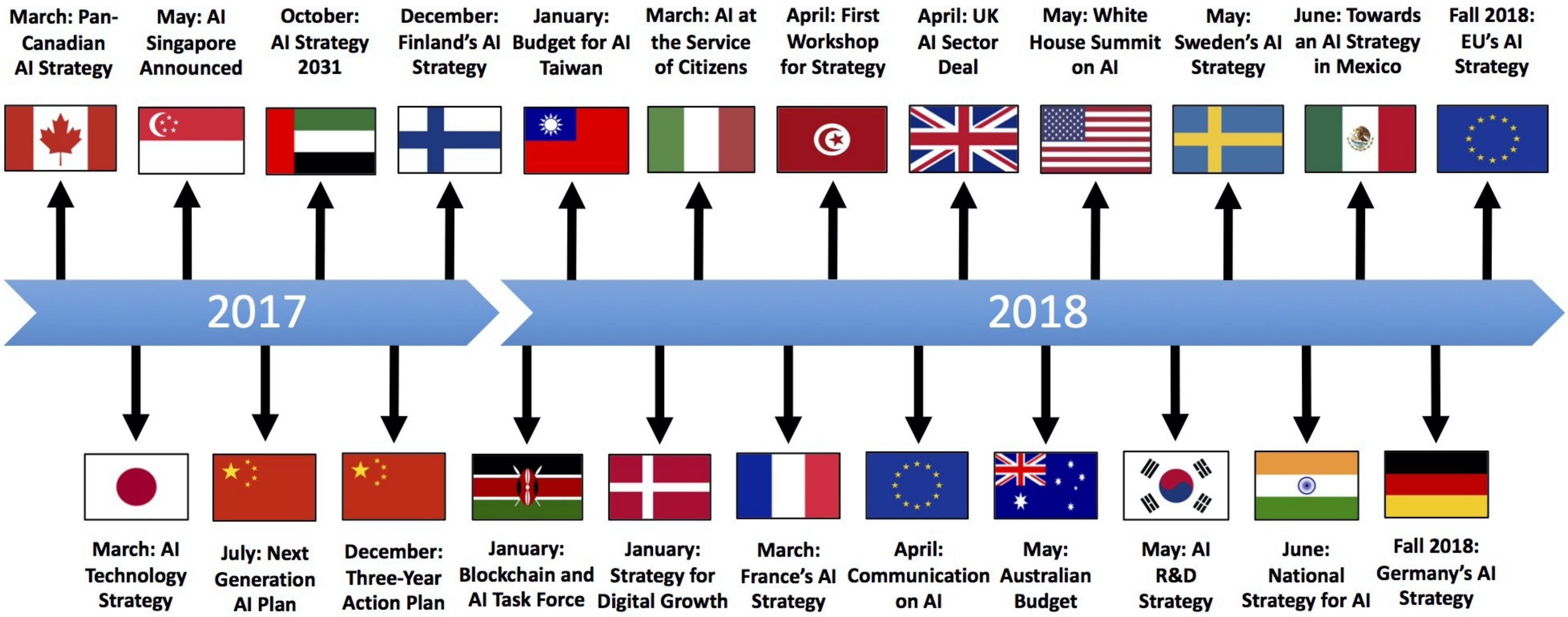
But note:

- These laws restrict the way you
  - Gather,
  - Use,
  - Share,
  - Aggregate,
  - Store, and
  - Retain
- THEY DON'T CARE IF YOU OWN IT- it's about you CONTROLING IT

SECTION 3

A Modern USE: AI Strategies and Themes

National AI Policies & Strategies in 2018



March: Pan-Canadian AI Strategy

May: AI Singapore Announced

October: AI Strategy 2031

December: Finland's AI Strategy

January: Budget for AI Taiwan

March: AI at the Service of Citizens

April: First Workshop for Strategy

April: UK AI Sector Deal

May: White House Summit on AI

May: Sweden's AI Strategy

June: Towards an AI Strategy in Mexico

Fall 2018: EU's AI Strategy

2017

2018

March: AI Technology Strategy

July: Next Generation AI Plan

December: Three-Year Action Plan

January: Blockchain and AI Task Force

January: Strategy for Digital Growth

March: France's AI Strategy

April: Communication on AI

May: Australian Budget

May: AI R&D Strategy

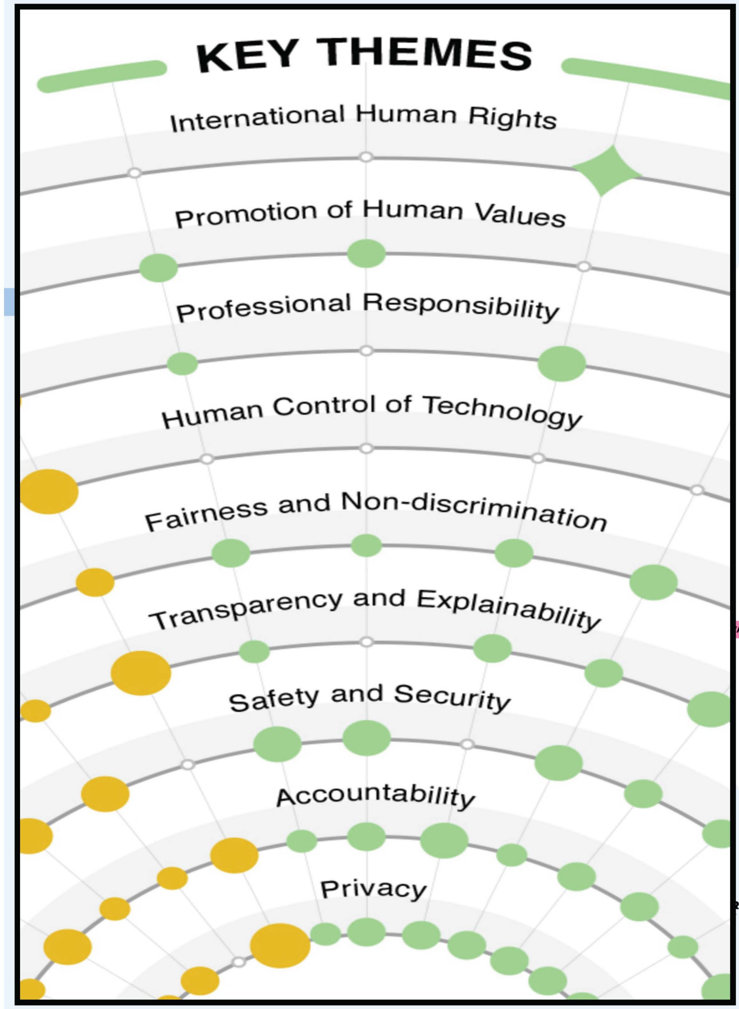
June: National Strategy for AI

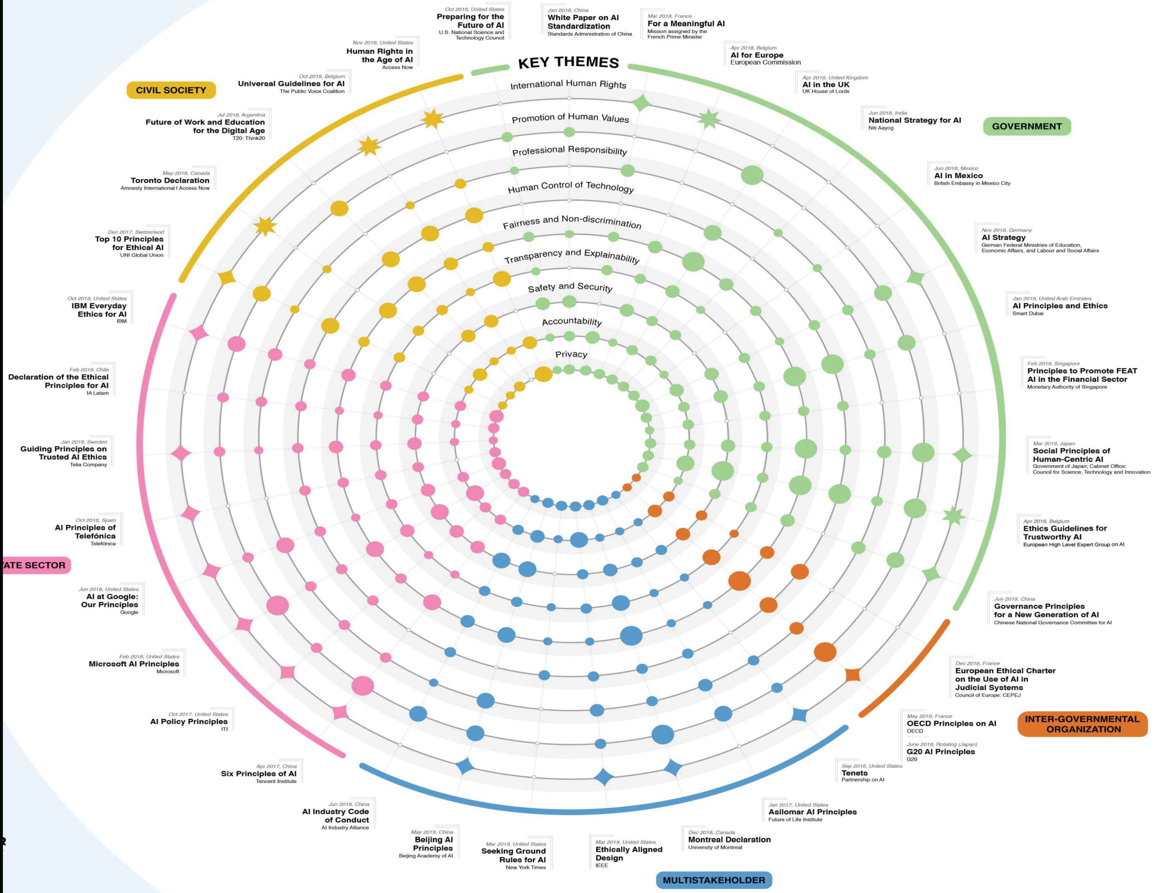
Fall 2018: Germany's AI Strategy

Source: Tim Dutton, "An Overview of National AI Strategies," Medium (2018), https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd

National AI Policies & Strategies Today

Source: OECD.AI (2020), powered by EC/OECD (2020), STIP Compass database, https://oecd.ai.


KEY THEMES
International Human Rights
Promotion of Human Values
Professional Responsibility
Human Control of Technology
Fairness and Non-discrimination
Transparency and Explainability
Safety and Security
Accountability
Privacy


KEY THEMES
International Human Rights
Promotion of Human Values
Professional Responsibility
Human Control of Technology
Fairness and Non-discrimination
Transparency and Explainability
Safety and Security
Accountability
Privacy
CIVIL SOCIETY
GOVERNMENT
ATE SECTOR
INTER-GOVERNMENTAL ORGANIZATION
MULTISTAKEHOLDER
Oct 2016, United States
Preparing for the Future of AI
U.S. National Science and Technology Council
Jan 2018, China
White Paper on AI Standardization
Standards Administration of China
Mar 2018, France
For a Meaningful AI
Mission assigned by the French Prime Minister
Apr 2018, Belgium
AI for Europe
European Commission
Apr 2018, United Kingdom
AI in the UK
UK House of Lords
Jun 2018, India
National Strategy for AI
Niti Aayog
Jun 2018, Mexico
AI in Mexico
British Embassy in Mexico City
Nov 2018, Germany
AI Strategy
German Federal Ministries of Education, Economic Affairs, and Labour and Social Affairs
Jan 2019, United Arab Emirates
AI Principles and Ethics
Smart Dubai
Feb 2019, Singapore
Principles to Promote FEAT AI in the Financial Sector
Monetary Authority of Singapore
Mar 2019, Japan
Social Principles of Human-Centric AI
Government of Japan; Cabinet Office; Council for Science, Technology and Innovation
Apr 2019, Belgium
Ethics Guidelines for Trustworthy AI
European High Level Expert Group on AI
Jun 2019, China
Governance Principles for a New Generation of AI
Chinese National Governance Committee for AI
Dec 2018, France
European Ethical Charter on the Use of AI in Judicial Systems
Council of Europe: CEPEJ
May 2019, France
OECD Principles on AI
OECD
June 2019, Rotating (Japan)
G20 AI Principles
G20
Sep 2016, United States
Tenets
Partnership on AI
Jan 2017, United States
Asilomar AI Principles
Future of Life Institute
Dec 2018, Canada
Montreal Declaration
University of Montreal
Mar 2019, United States
Ethically Aligned Design
IEEE
Mar 2019, United States
Seeking Ground Rules for AI
New York Times
May 2019, China
Beijing AI Principles
Beijing Academy of AI
Jun 2019, China
AI Industry Code of Conduct
AI Industry Alliance
Apr 2017, China
Six Principles of AI
Tencent Institute
Oct 2017, United States
AI Policy Principles
ITI
Feb 2018, United States
Microsoft AI Principles
Microsoft
Jun 2018, United States
AI at Google: Our Principles
Google
Oct 2018, Spain
AI Principles of Telefónica
Telefónica
Jan 2019, Sweden
Guiding Principles on Trusted AI Ethics
Telia Company
Feb 2019, Chile
Declaration of the Ethical Principles for AI
IA Latam
Oct 2019, United States
IBM Everyday Ethics for AI
IBM
Dec 2017, Switzerland
Top 10 Principles for Ethical AI
UNI Global Union
May 2018, Canada
Toronto Declaration
Amnesty International I Access Now
Jul 2018, Argentina
Future of Work and Education for the Digital Age
T20: Think20
Oct 2018, Belgium
Universal Guidelines for AI
The Public Voice Coalition
Nov 2018, United States
Human Rights in the Age of AI
Access Now

“Automation outcomes are not pre-determined but are shaped by the policies and choices we make.”

Michel Servoz, The Future of Work? Work of the Future! On how Artificial Intelligence, Robotics and Automation are Transforming Jobs and the Economy in Europe, EU Comm’n, at 3 (2019).

Current AI Governance Efforts

National & Regional

- United States
- European Union
- China
- Singapore
- Others (41)

International

- OECD
- G20
- UN
- World Economic Forum

Private Initiatives

- Companies
- Academia
- Non-profit
- Civil Society
- Collaborations

Private Sector Initiatives	
Accenture	Ethical Framework for Responsible AI and Robotics
Google	Google’s AI Principles
IBM	Everyday Ethics for Artificial Intelligence; Principles for Trust and Transparency
Intel	AI Public Policy Principles
Microsoft	Microsoft AI Principles
Academic Initiatives	
Harvard University	Ethics and Governance of Artificial Intelligence
Peking University, Tsinghua University	Beijing AI Principles (published in collaboration with the Chinese Academy of Sciences and others)
Stanford University	100 Year Study on AI
University of Montreal	Montreal Declaration for A Responsible Development of AI
University of Oxford	Government AI Readiness Index
Nonprofit and Collaborative Initiatives	
ACM	Statement on Algorithmic Transparency and Accountability
FATML	Principles for Accountable Algorithms and a Social Impact Statement for Algorithms
Future of Life Institute	Asilomar AI Principles
IEEE	Ethically Aligned Design; Ethical Aspects of Autonomous and Intelligent Systems
OpenAI	OpenAI Charter
Partnership on AI	Tenets of the PAI to Benefit People and Society
Public Voice Coalition	12 Universal Guidelines for the Development of AI

Survey of AI Principles

Google's AI Principles	Beijing AI Principles	IEEE
Be socially beneficial.	Do good	Human rights
Avoid unfair bias.	For humanity	Well-being
Safety	Be responsible	Data Agency
Accountability	Control risks	Effectiveness
Privacy by Design	Be ethical	Transparency
Scientific Excellence	Be diverse and inclusive	Accountability
Availability	Open and share	Awareness of Misuse
		Competence

SECTION 4

A Modern Issue: Cybersecurity

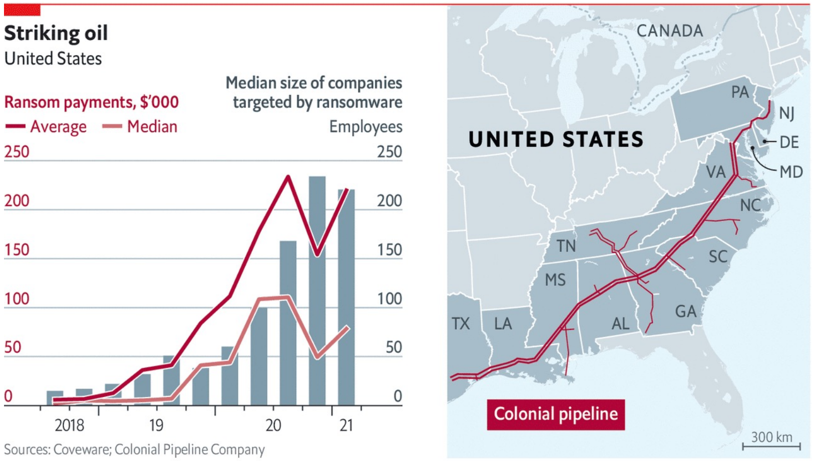
Defining the Cyber Threat

To Companies

- Cyber Attacks are **Costly** – ransomware cost per incident was $178,254 in 2020 (Gartner)
- **Widespread** – Phishing attacks increased by 11% during the pandemic (Verizon)
- **Easy** – malware is freely accessible on both the common and deep web for as little as $70 (TechRepublic)
- **Expanding** – Internet of (Every)thing

To Countries

- Fear of "Electronic Pearl Harbor" (overblown?)
- Protecting critical national infrastructure



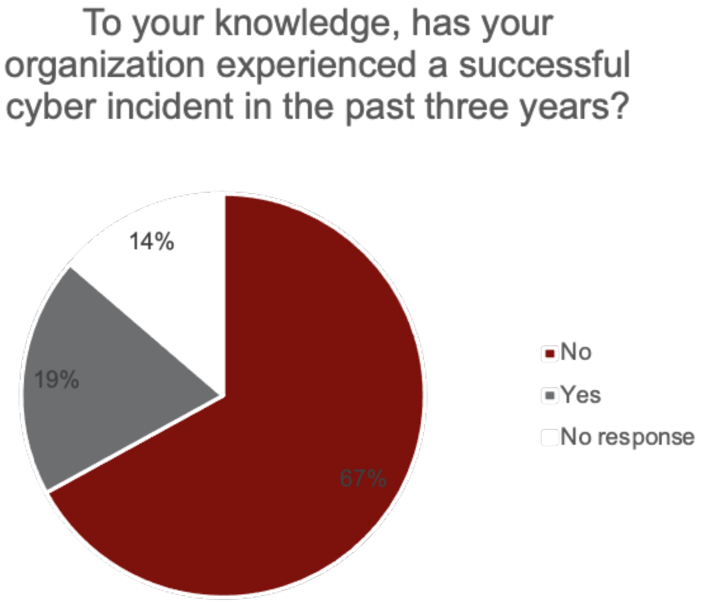
Striking oil

United States

Sources: Coveware; Colonial Pipeline Company

The Economist

State of Hoosier Cybersecurity 2020 Snapshot

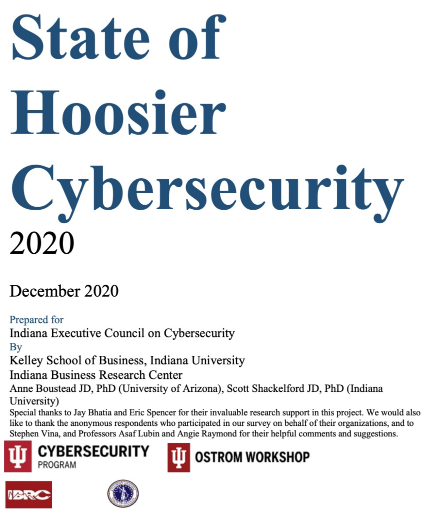


To your knowledge, has your organization experienced a successful cyber incident in the past three years?

- *Fewer organizations in critical infrastructure sectors reported successful cyber attacks than non-critical infrastructure organizations*
  - *About 13% of critical infrastructure organizations reported successful attacks*
  - *About 28% of non-critical infrastructure organizations reported successful attacks*

Most Indiana Organizations Report Taking Steps to Prevent Cyber Incidents

- *Just over 91% of organizations surveyed said they had taken some steps to prevent cyber incidents*
- *Slightly more critical infrastructure organizations said they had taken steps to prevent cyber incidents, when compared to non-critical infrastructure organizations*
  - *About 94% of critical infrastructure organizations reported taking cyber incident prevention steps*
  - *About 88% of non-critical infrastructure organizations reported taking cyber incident preventions steps*



State of Hoosier Cybersecurity

2020

December 2020

Prepared for
Indiana Executive Council on Cybersecurity
By
Kelley School of Business, Indiana University
Indiana Business Research Center
Anne Boustead JD, PhD (University of Arizona), Scott Shackelford JD, PhD (Indiana University)

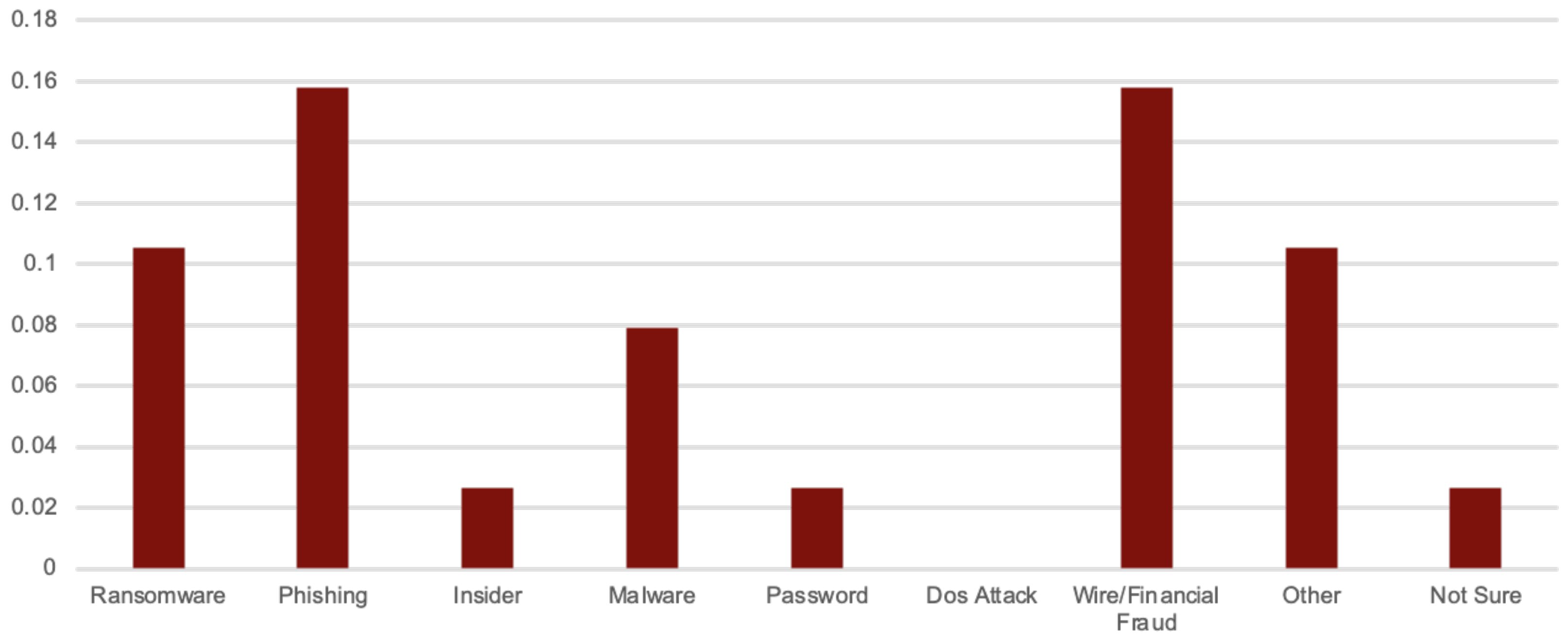
Special thanks to Jay Bhatia and Eric Spencer for their invaluable research support in this project. We would also like to thank the anonymous respondents who participated in our survey on behalf of their organizations, and to Stephen Vina, and Professors Asaf Lubin and Angie Raymond for their helpful comments and suggestions.

CYBERSECURITY PROGRAM

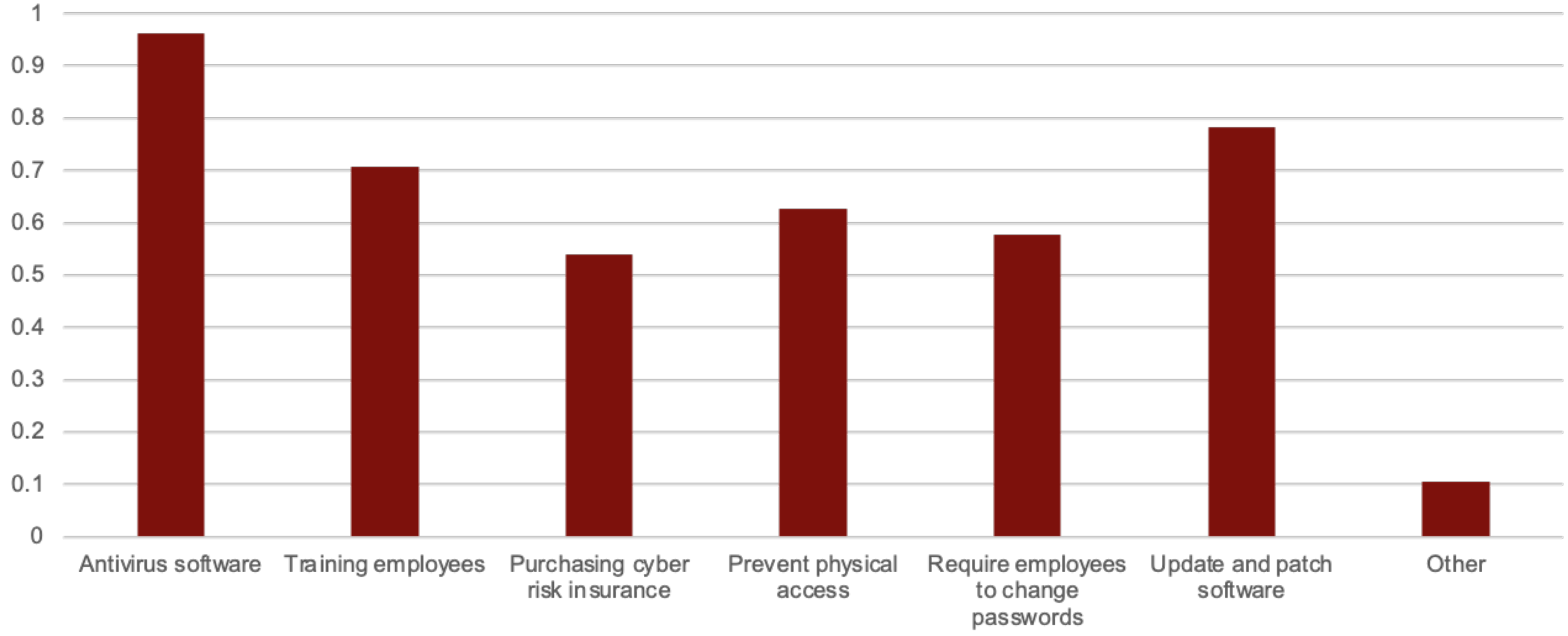
OSTROM WORKSHOP

IBRC

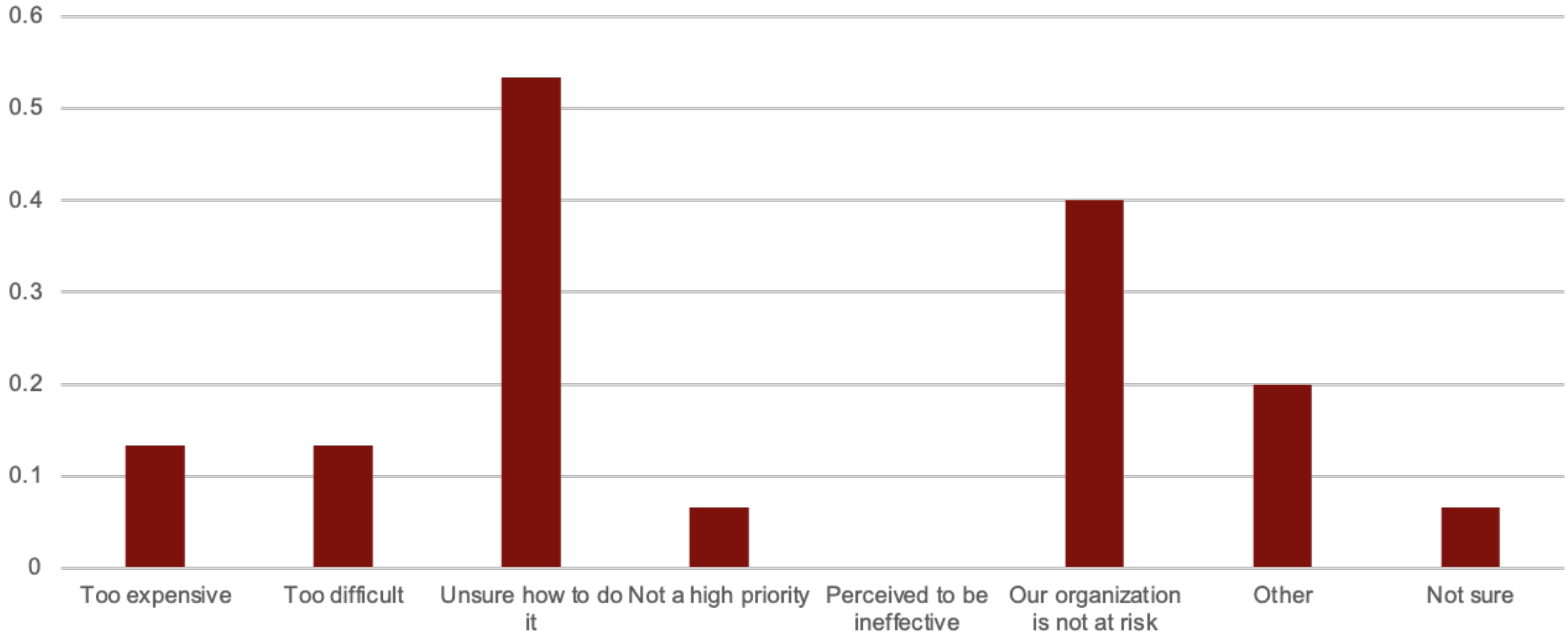
Type of Attacks Experienced



Steps Taken to Prevent Cyber Incidents



Reasons why organizations did not take preventative steps

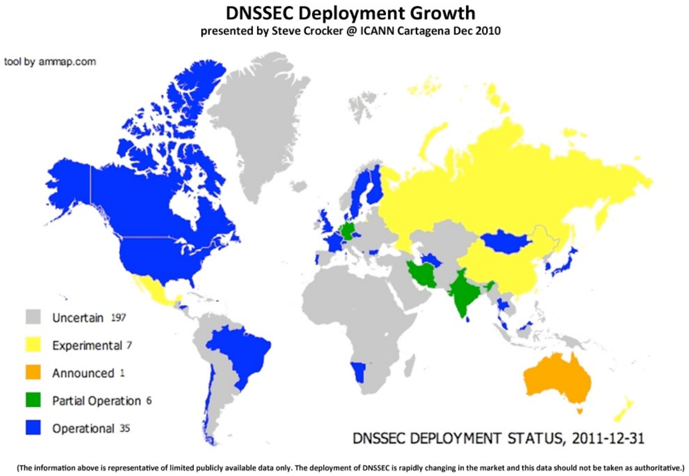


Managing Cyber Attacks

Technical Vulnerabilities

- Hardware
  - Secure Supply Chains
  - "Trust but Verify"
- Protocols
  - Ex: DNS
  - Importance of DNSSEC
- Code
  - Improving Accountability
  - Liability Issues
- Users

*Source: www.aronsonblogs.com


DNSSEC Deployment Growth
presented by Steve Crocker @ ICANN Cartagena Dec 2010
tool by ammap.com
Uncertain 197
Experimental 7
Announced 1
Partial Operation 6
Operational 35
DNSSEC DEPLOYMENT STATUS, 2011-12-31
(The information above is representative of limited publicly available data only. The deployment of DNSSEC is rapidly changing in the market and this data should not be taken as authoritative.)

*Source: www.techbyte.pl

Private-Sector Cybersecurity Best Practices

- **Summary**: Be *proactive* and invest in built-in cybersecurity best practices from the inception of a project.
- **Technology**
  - Encrypt Data (at rest and in transit)
  - Biometrics & Deep Packet Inspection
- **Investments**
  - Average: >10-15% of IT budgets
  - Cybersecurity as CSR
- **Organization**
  - CISO Savings
  - Audit Training Programs & Penetration Testing

*Source: www.wizilegal.com

> *"[T]he cyber threat cannot be eliminated; rather, cyber risk must be managed."*

Former Director of National Intelligence James R. Clapper
Worldwide Cyber Threats Testimony, Sep. 10, 2015

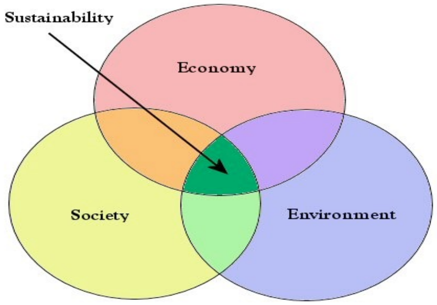
Throwing Money at the Problem

- **U.S. Private Sector Spending on Cybersecurity** - $102 billion by 2020 (a 38% increase from 2016)
- **U.S. Public Sector Spending on Cybersecurity** - $28 billion in 2016 (compared to $7.5 billion in 2007)
- **How much is too much?** According to the Gordon-Loeb theory, the optimal amount is *37% of the projected loss*.

Copyright Lisa Benson

Investigating Analogies: Cybersecurity as Social Responsibility

- **Problems**: Is there a tragedy of the cyber commons? Putting it another way, is there a market failure here? Where does cost-benefit analysis fall short?
- **Idea**: Measure impact of a firm's operation on the broader Internet ecosystem.
- **Some Applicable Tools**:
  - Integrated Reporting
  - Certificate Programs
  - Environmental Law Analogies
- **Drawbacks**?



*Source: *www.keepoklahomabeautiful.com*

Why is Deterring Ransomware Attacks So Challenging?

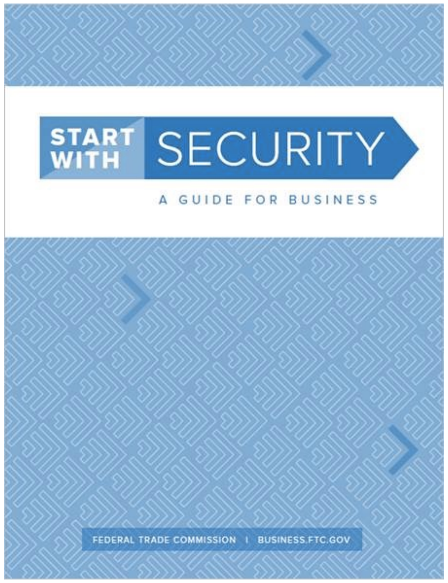
- **U.S. Federal Efforts**
  - Federal Trade Commission
  - NIST Cybersecurity Framework
  - Role of CISA
  - Recent Exec Orders
  - Cryptocurrency & IoT Regulation
- **State-Level Efforts**
  - States of Emergency & New State Laws ("Reasonableness")
- **Civil Society**
  - Consumer Reports Digital Standard

© Randy Glasbergen
glasbergen.com

"I can't see your future, but I found your bank files, Social Security number and all of your company passwords."

FTC Cybersecurity Best Practices

1. Start with Security
2. Compartmentalize Access to Data
3. Require Secure Passwords & Authentication
4. Store/Transmit Personal Info Securely
5. Segment & Dynamically Monitor Networks
6. Secure Remote Access
7. Cybersecurity-Awareness Training
8. Ensure Security of Service Providers
9. Regularly Update Security Practices
10. Secure Paper, Physical Media & Hardware



START WITH SECURITY

A GUIDE FOR BUSINESS

FEDERAL TRADE COMMISSION | BUSINESS.FTC.GOV

Negligence and the NIST Cybersecurity Framework

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

*Source: *welivesecurity.com*

- **2013 State of the Union Address**
  - Focus on cyber threats to nation's critical infrastructure
- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity**
  - Increase information sharing
  - Ensure privacy and civil liberties protections
  - Develop a voluntary Cybersecurity Framework
- CISA Ransomware Role & Resources

The Wider View: Global Approaches to Securing Critical Infrastructure

What is ‘Critical Infrastructure?’

- How is it defined? Is this evolving?
- What regulatory requirements come along with the designation?
- What powers should governments have in protecting critical infrastructure? Are these too narrow, or too broad?
- If everything is ‘critical,’ is anything?

EU Cybersecurity Policy

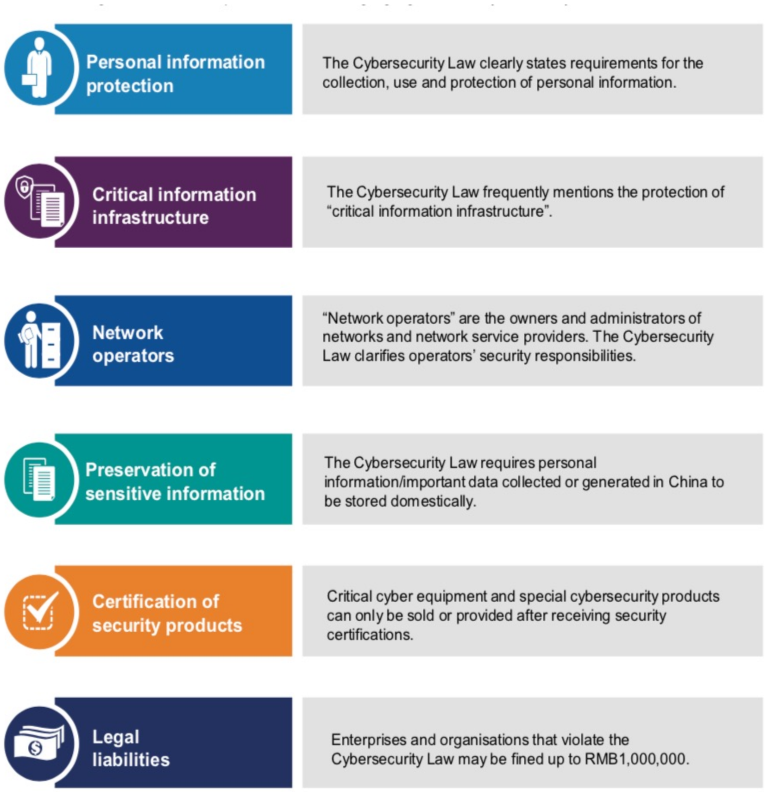
- **National Cybersecurity Initiatives**
  - Ex: UK
- **New EU Cybersecurity Strategy (Feb. 2013)**
  - Notify national authorities of "significant" cyber attacks
  - Regulate CNI as well as Internet companies
  - Impose liability even with outsourcing
- **NIS Directive / General Data Protection Reg.**

GDPR Top-10 Operational Impacts

1. Cybersecurity & Data Breach Requirements
2. Mandatory Data Protection Officer
3. Consent
4. Cross-Border Data Transfers
5. Profiling
6. Data Portability
7. Vendor Management
8. Pseudonymization
9. Codes of Conduct & Certifications
10. Consequences of Non-Compliance

**Source: IAPP*

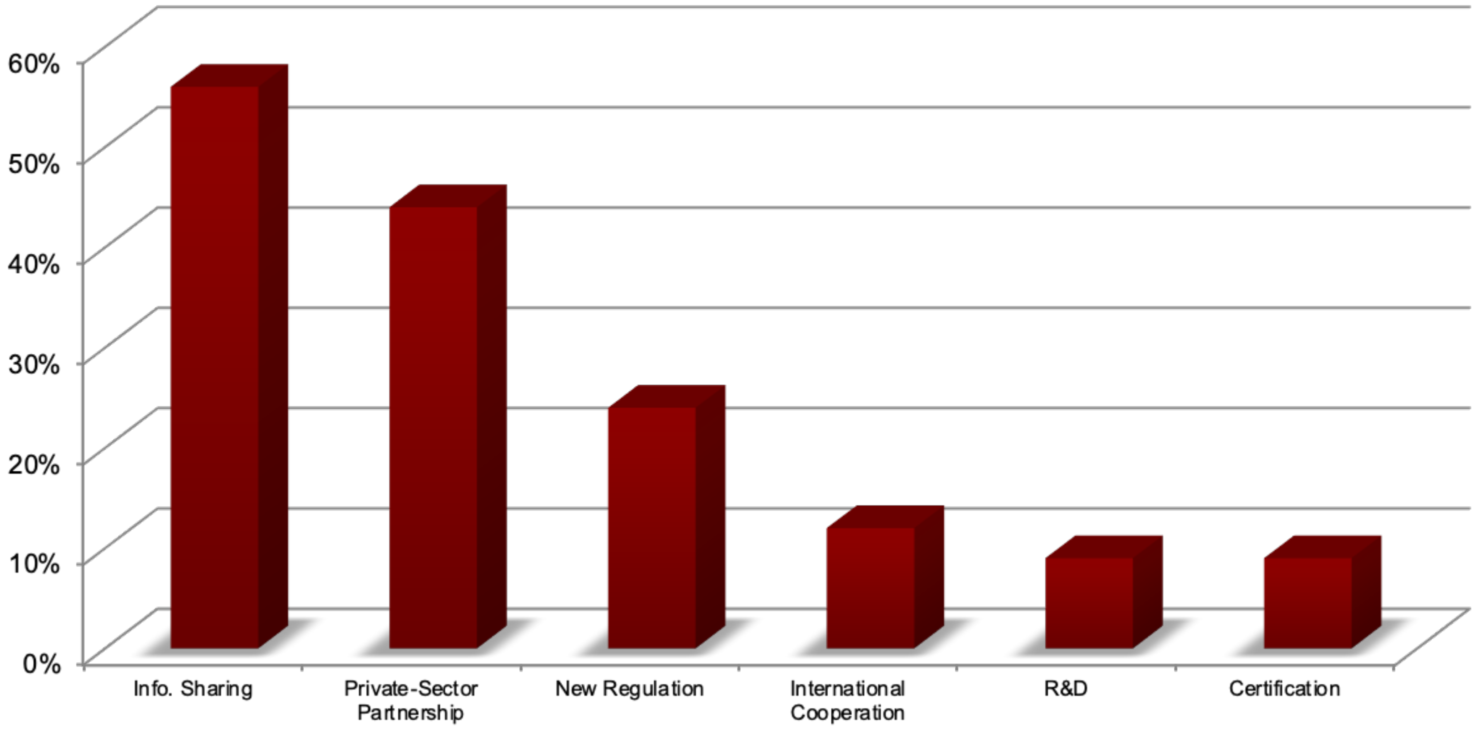
Highlights of China’s Cybersecurity Law



Personal information protection	The Cybersecurity Law clearly states requirements for the collection, use and protection of personal information.
Critical information infrastructure	The Cybersecurity Law frequently mentions the protection of “critical information infrastructure”.
Network operators	“Network operators” are the owners and administrators of networks and network service providers. The Cybersecurity Law clarifies operators’ security responsibilities.
Preservation of sensitive information	The Cybersecurity Law requires personal information/important data collected or generated in China to be stored domestically.
Certification of security products	Critical cyber equipment and special cybersecurity products can only be sold or provided after receiving security certifications.
Legal liabilities	Enterprises and organisations that violate the Cybersecurity Law may be fined up to RMB1,000,000.

**Source: KPMG*

Critical Infrastructure Dimension Summary Chart



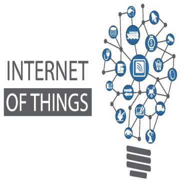
Proposing a National Cybersecurity Safety Board

- Idea: Why not create an NTSB for cyber attacks?
- Op-Ed Version: https://theconversation.com/what-cybersecurity-investigators-can-learn-from-airplane-crashes-91177

MAKING TRANSPORTATION SAFER
NATIONAL TRANSPORTATION SAFETY BOARD
1967
2017
YESTERDAY ★ TODAY ★ TOMORROW

Fixing an Internet of Broken Things

1. *Deeper cooperation both within and between IoT sectors*
2. *Develop standards for IoT devices using the NIST CSF and CPS as guides*
3. *Promote flexible, guidance-driven frameworks to promote resilience, including in supply chains*
4. *Use government contracting as a mechanism to promote cybersecurity due diligence*
5. *Boost FTC and SEC resources to go after bad actors and enforce reporting requirements*

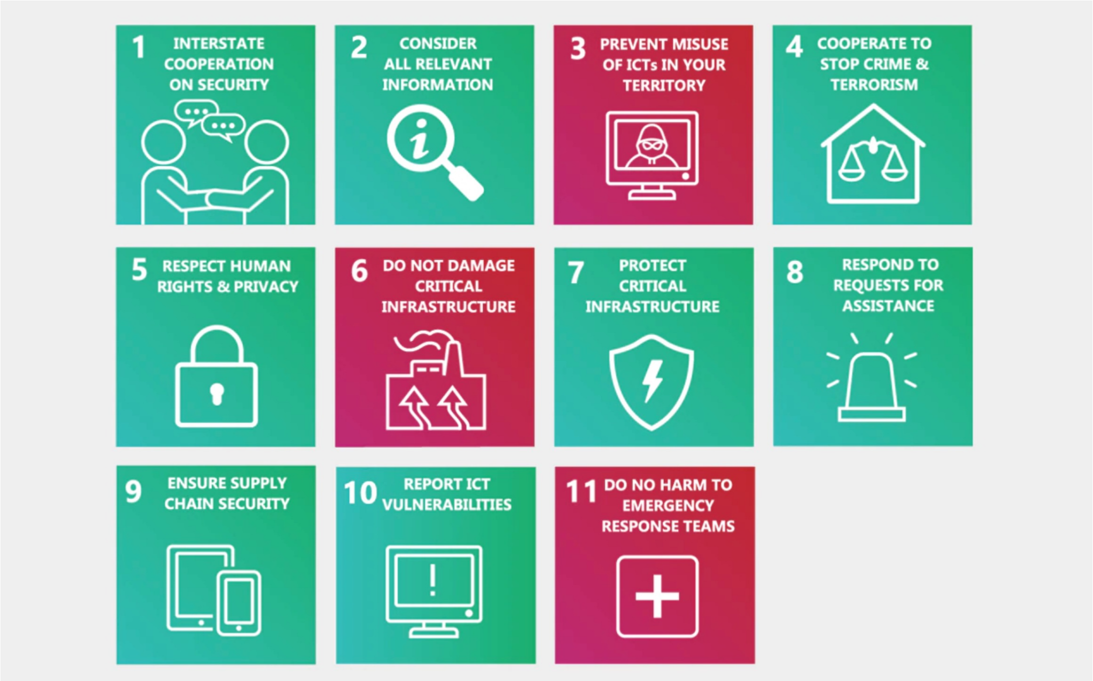


Unpacking "Cyber Peace"

Vatican's Pontifical Academy of Sciences Erice Declaration on Principles for Cyber Stability and Cyber Peace

1. All governments should recognize that **international law guarantees individuals the free flow of information and ideas**; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.
2. All countries should work together to **develop a common code of cyber conduct and harmonized global legal framework**, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.
3. All users, service providers, and governments should work to ensure that **cyberspace is not used in any way that would result in the exploitation of users**, particularly the young and defenseless, through violence or degradation.
4. Governments, organizations, and the private sector, including individuals, should implement and maintain **comprehensive security programs based upon internationally accepted best practices** and standards and utilizing privacy and security technologies.
5. Software and hardware developers should strive to develop **secure technologies that promote resiliency** and resist vulnerabilities.
6. Governments should actively participate in **United Nations' efforts to promote global cyber security and cyber peace** and to avoid the use of cyberspace for conflict.

Recognized Cyber Norms



1 INTERSTATE COOPERATION ON SECURITY

2 CONSIDER ALL RELEVANT INFORMATION

3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY

4 COOPERATE TO STOP CRIME & TERRORISM

5 RESPECT HUMAN RIGHTS & PRIVACY

6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE

7 PROTECT CRITICAL INFRASTRUCTURE

8 RESPOND TO REQUESTS FOR ASSISTANCE

9 ENSURE SUPPLY CHAIN SECURITY

10 REPORT ICT VULNERABILITIES

11 DO NO HARM TO EMERGENCY RESPONSE TEAMS

Key Stakeholders, Organizations & Initiatives

Stakeholders

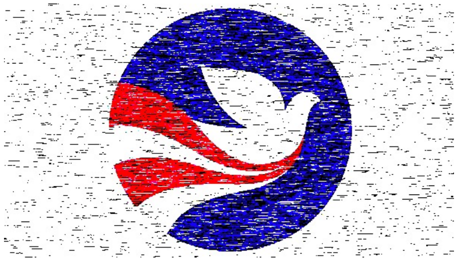
- UN
- Governments
- Think Tanks
  - Atlantic Council
  - Brookings
- Companies
  - Microsoft
  - Raytheon
- Foundations
- Civil Society
- Academia
- Users

Organizations

- Cyber Peace Initiative
- Cyberpeace Institute
- Cybersecurity Tech Accord
- Online Trust Alliance
- Global Commission on the Stability of Cyberspace
- Cyber Peace Foundation

Initiatives

- UNGGE
- G7
- G20
- Paris Call
- Christchurch Call
- ITU Global Cybersecurity Index



Cyber Peace Goals

Framework

	Category A	Category B	Category C	Category D	Category E
Guarantee Universal Internet Access	Access Quality Cybersecurity Education	Spread Cyber Hygiene	Defend Intellectual Property	Reduce Inequality	Empower Diverse Communities and Voices in Internet Governance
Defend Electoral Processes	Protect Privacy	Define Enforceable Cyber Norms	Protect Children and at-risk Groups Online	Safeguard Critical Infrastructure	Promote Lifecycle Security and Corporate Social Responsibility
Counter the Spread of Disinformation	Support Cybersecurity Frameworks & Best Practices	Encourage the Growth of Just, Resilient Institutions	Clarify Legal Standards and Cybersecurity Expectations	Deepen Collaborations to Fight Cybercrime, Terrorism, and Cyber Conflict	

Thank you!

Scott Shackelford, JD/PhD

sjshacke@indiana.edu

Angie Raymond, JD/PhD

angraymo@indiana.edu

That's all Folks!
dwrs4.me