RSAConference2019
San Francisco | March 4–8 | Moscone Center

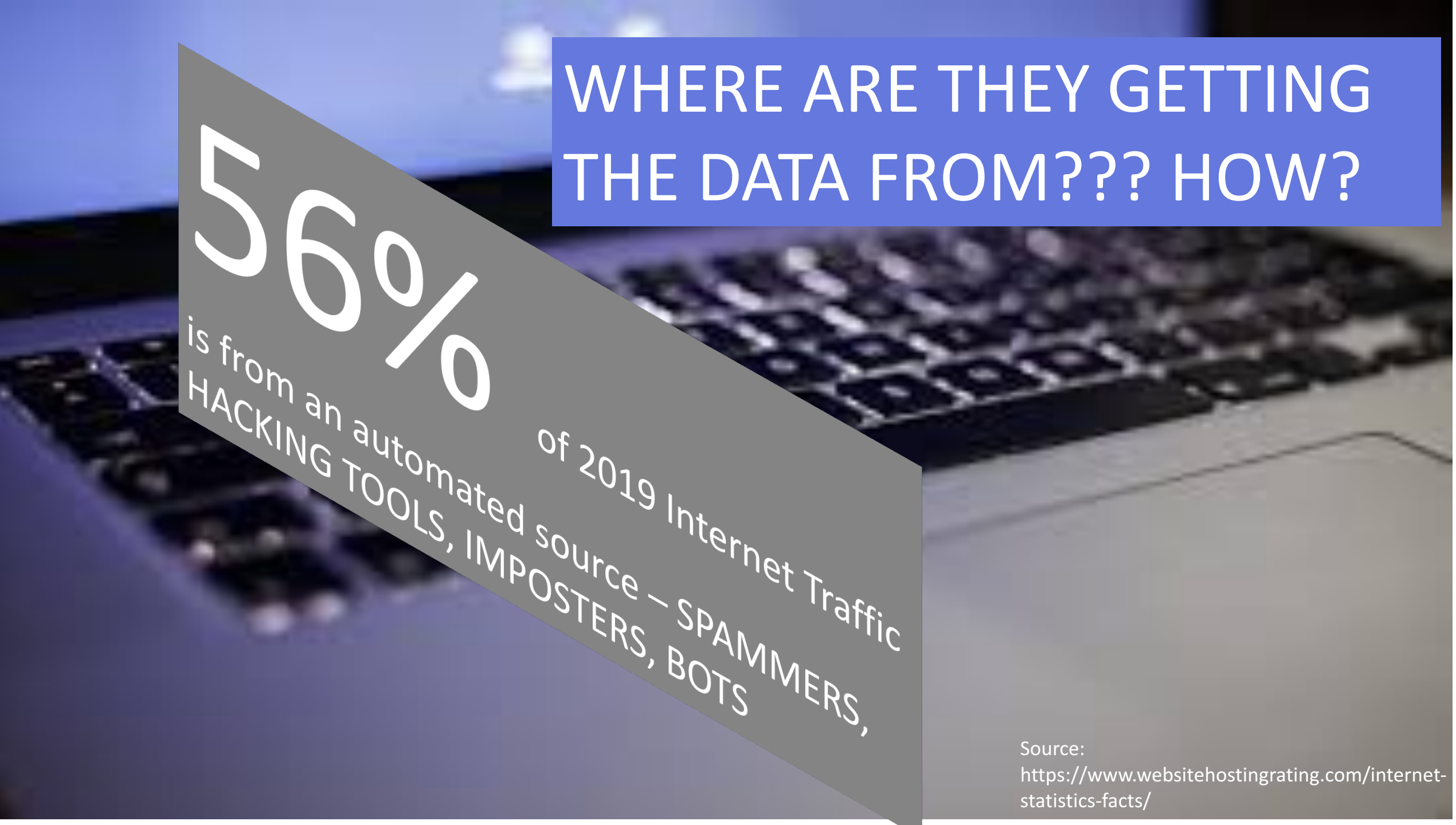
SESSION ID: PRV-T06

Privacy Essentials for Security Professionals

Todd Fitzgerald, CISSP, CISA, CISM, CIPP/US, CIPP/EU, CIPP/CANADA,CIPM, ISO27001, PMP, ITILv3f

Managing Director/CISO
Cybersecurity Leadership Author
CISO SPOTLIGHT, LLC
@securityfitz

WHERE ARE THEY GETTING THE DATA FROM??? HOW?



Source: https://www.websitehostingrating.com/internet-statistics-facts/

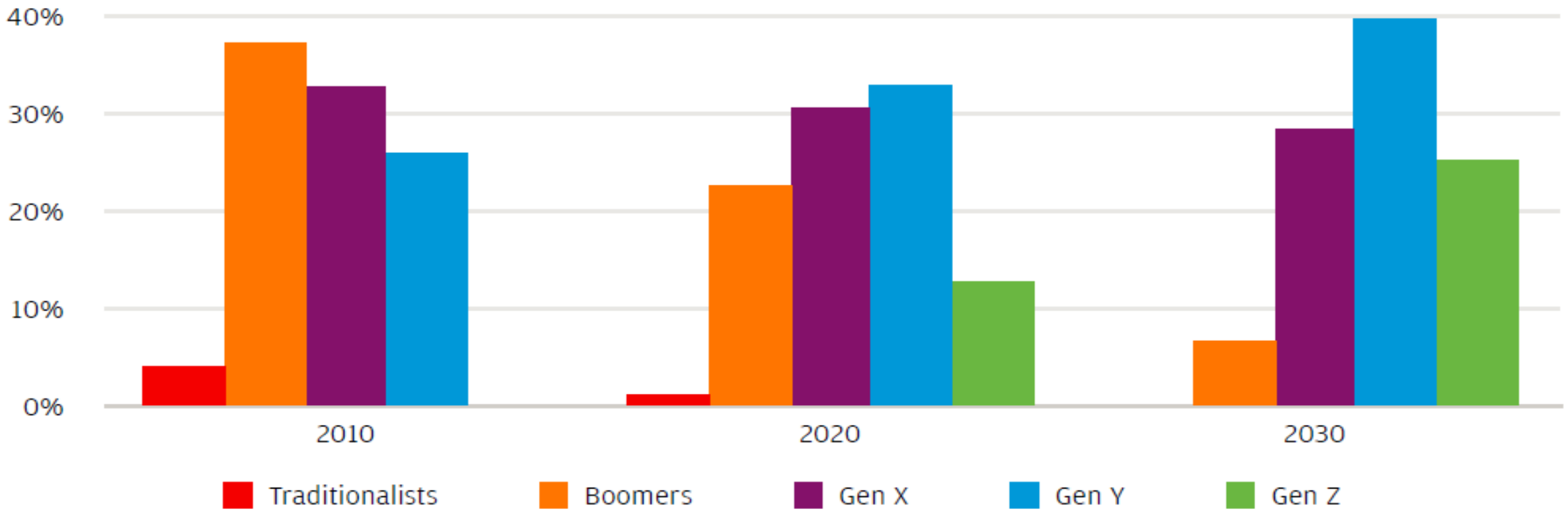
Today We Will Explore …

1. Why Security Professionals should Care About Privacy
2. Privacy Laws and Common Principles
3. The Language of Privacy

RSAConference2019

Why Should Security Officers Care About Privacy?

The Workforce Composition Is Shifting



Source: Deloitte Research/UN Population Division, It's 2008: Do You Know Where Your Talent Is?

Where Is Your Privacy "Line"

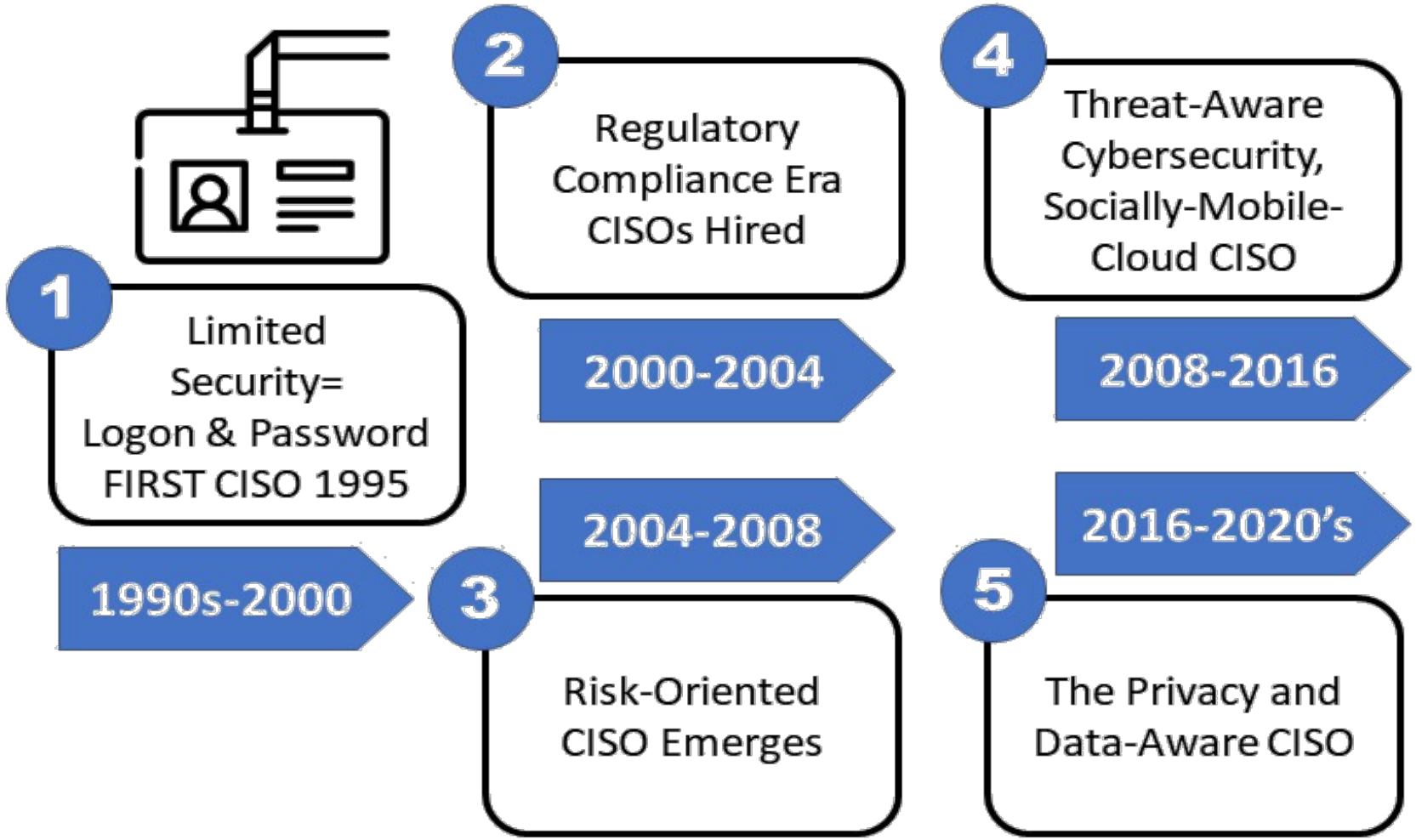
The 2018 CISO Evolution

Leadership
Strategic Thinking
Business Knowledge
Risk Management
Communication
Relationship Management
Security Expertise
Technical Expertise

- Plan path away from operations
- Refine risk management processes to business language
- **Widen vision to privacy, data management and compliance**
- Build support network
- Create focus and attention of business leaders

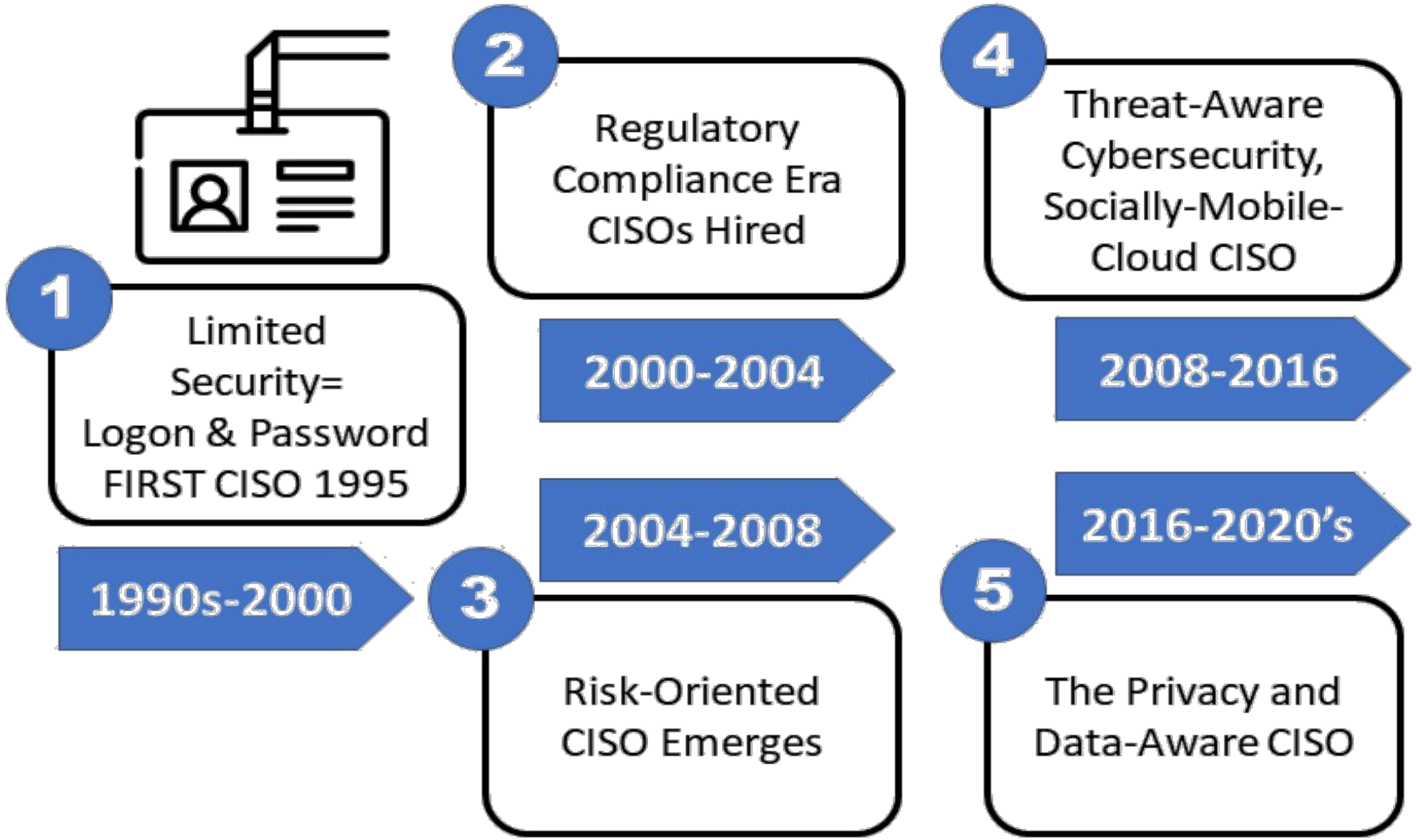
Source: Forrester Research: Evolve to become 2018 CISO or Face Extinction

5 STAGES OF CISO EVOLUTION 1995-2020's



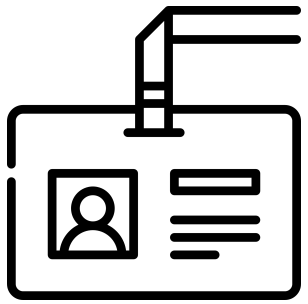
Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

5 STAGES OF CISO EVOLUTION 1995-2020's



Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

5 STAGES OF CISO EVOLUTION 1995-2020's



1 Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2 Regulatory Compliance Era CISOs Hired

2000-2004

3 Risk-Oriented CISO Emerges

2004-2008

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2008-2016

2016-2020's

5 **The Privacy and Data-Aware CISO**

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

The Security Professional Has a New Set of Concerns To Address *Beyond Technology*

- Lack of Global Trust
- Data Location
- New Regulations & Fines
- Breach Notification
- Location Tracking
- Changing Responsibilities

Privacy Concerns Impact Our Daily Lives

Privacy Concerns Impact Our Daily Lives

Source: Several videos in this presentation from personal collection of Eugene Schultz, an unforgettable information security pioneer.

RSAConference2019

Privacy Laws and Common Principles

The Right To Privacy Paper 1890

HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the in-

Warren

Brandeis

"Right to Life"… "Right to Property"… "Right to enjoy life"…"Right to Liberty"

'RIGHT TO BE LET ALONE'

Sectoral Laws In US & Canada

Canada Personal Information Protection and Electronic Documents Act (PIPEDA or PIPED Act)

US Privacy Laws

Fair Credit Reporting Act
Health Information Insurance Portability and Accountability Act (HIPAA)
HITECH
State Breach Notification laws
Gramm-Leach-Bliley Act
Children's Online Privacy Protection Act (COPPA)
1974 Privacy Act /FOIA
Privacy Shield (Safe Harbor Replacement)

Co-Regulatory Approach: Australia "the Privacy Amendment (Notifiable Data Breaches) Act of 2017"

"Only required to notify when there is a data breach likely to result in serious harm to any individual the information relates"

- Kinds of information
- Sensitivity
- Protection (Encryption/Access control)
- Kinds of persons accessing information

22%

Australian Small/Medium Businesses Impacted By Ransomware

Source: Malwarebytes, 2nd Annual State of Ransomware Report: Survey Results for Australia, July 2017


European Union Applies a Comprehensive Data Privacy Approach
1995/98 EU Data Directive
2016 General Data Protection Regulation (Compliance May 2018)

EU General 2016 Data Protection Regulation (GDPR) Changes Privacy in May 2018 By…

- Increased Territorial Scope
- Penalties up to 4% revenue or 20 Million Euro
- Consent must be intelligible and accessible
- Breach notification 72 hours
- Right of access – free copy
- Right to be forgotten
- Data Portability
- Privacy By Design
- Data Protection Officers requirements

Chicago Tribune

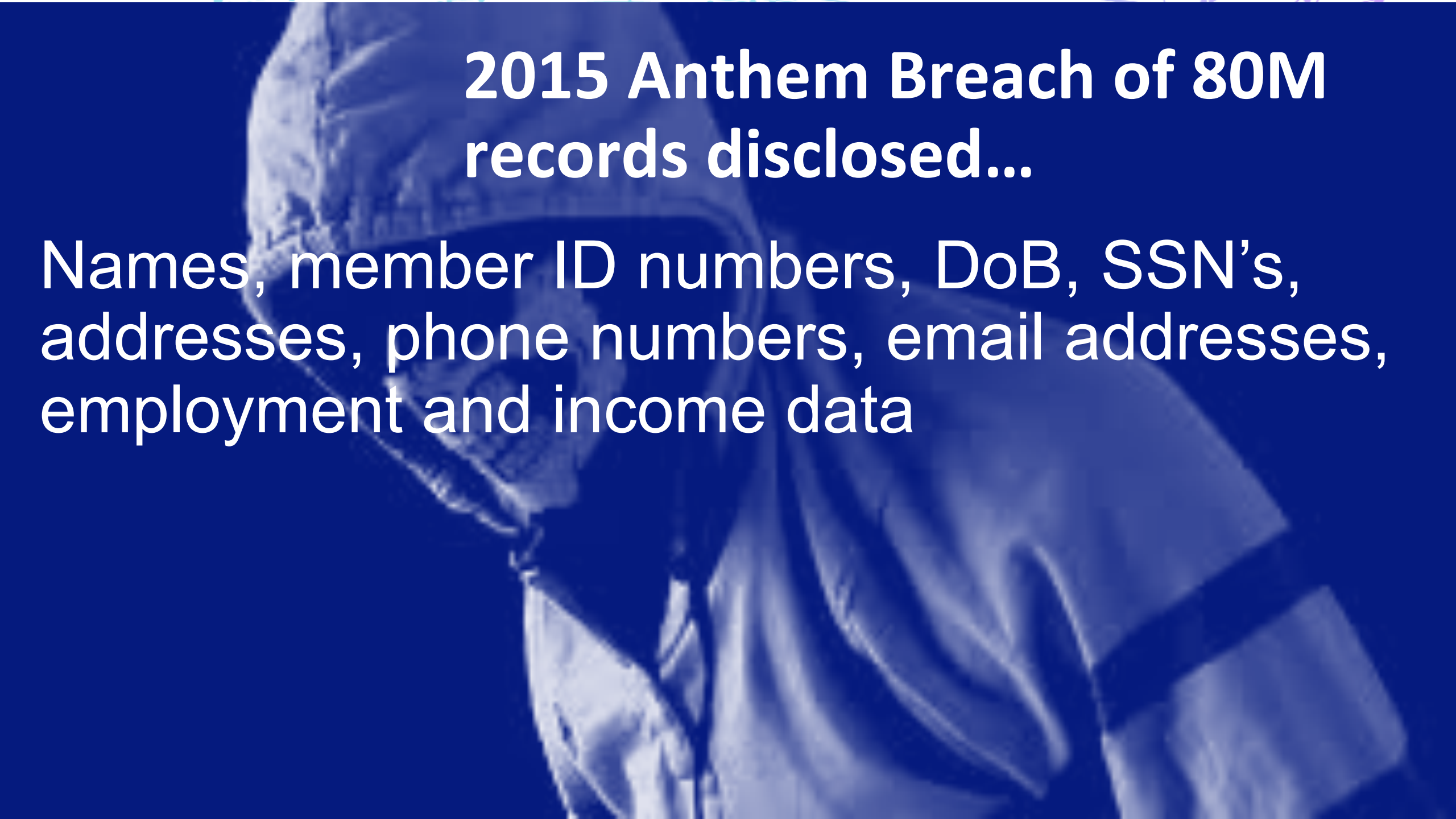
Unfortunately, our site is currently unavailable in most European countries. We are engaged on the issue and committed to looking for a way to support our full range of digital offerings to readers in Europe. We continue to identify technical compliance solutions to provide all readers with our award-winning journalism.

Chicago Tribune, Los Angeles Times block European users due to GDPR

Europe's strict new privacy regulations took effect on Friday, but even with the two-year grace period to become compliant, not everyone was ready.

Copyright © 2018, Chicago Tribune


DATA BREACH



2015 Anthem Breach of 80M records disclosed…

Names, member ID numbers, DoB, SSN's, addresses, phone numbers, email addresses, employment and income data


$115 Million Lawsuit Settlement (June 2017)
$38 Million Went To Lawyers
Settlement with Department Health & Human Services for $16 Million


UNDER GDPR, THE “FINE” POTENTIALLY COULD BE…
$3.6 BILLION

Organization for Economic Co-operation and Development (OECD) 8 Privacy Principles

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

#1: Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

#2: Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

#3: Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

#4: Use Limitation Principle

- Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9
- except:
  a) with the consent of the data subject; or
  b) by the authority of law.


RGYCOMMERCE.HOUSE.GOV
CNBC


RGYCOMMERCE.HOUSE.GOV | @
OMMERCE
CNBC
Mr. Zuckerberg

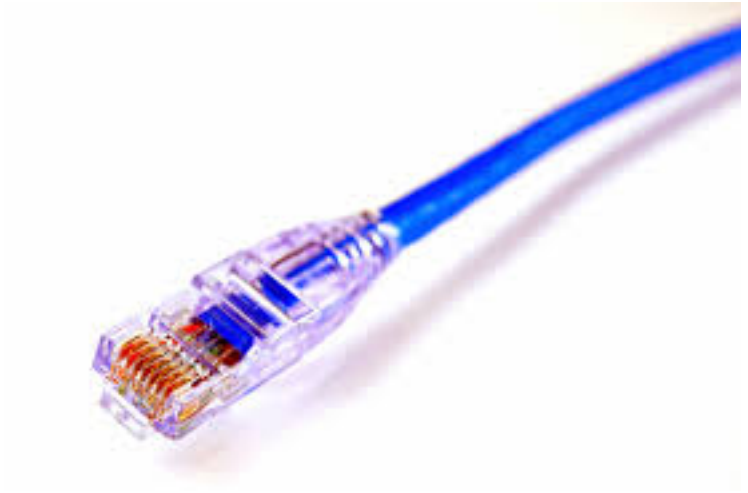
Source: CNBC


RGYCOMMERCE.HOUSE.GOV | @
OMMERCE
CNBC
Mr. Zuckerberg

#5: Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

#6: Openness Principle



There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

#7: Individual Participation Principle

Right to obtain confirmation DATA STORED	REASONABLE MANNER, COST and FORM	Ability to challenge denials
REASONABLE TIME	If denied, be provided a reason	Right to erase, rectify complete, or amend information

#8: Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

RSAConference2019

The Language of Privacy

Personal Information Elements

Sources of Personal Information

Public Records	Publicly Available	Nonpublic
• Real estate • Criminal • Varies State/National/Local level	• Names and addresses • Newspapers • Search engines • Facebook/Twitter	• Medical records • Financial information • Adoption Records • Company customers • Employee database

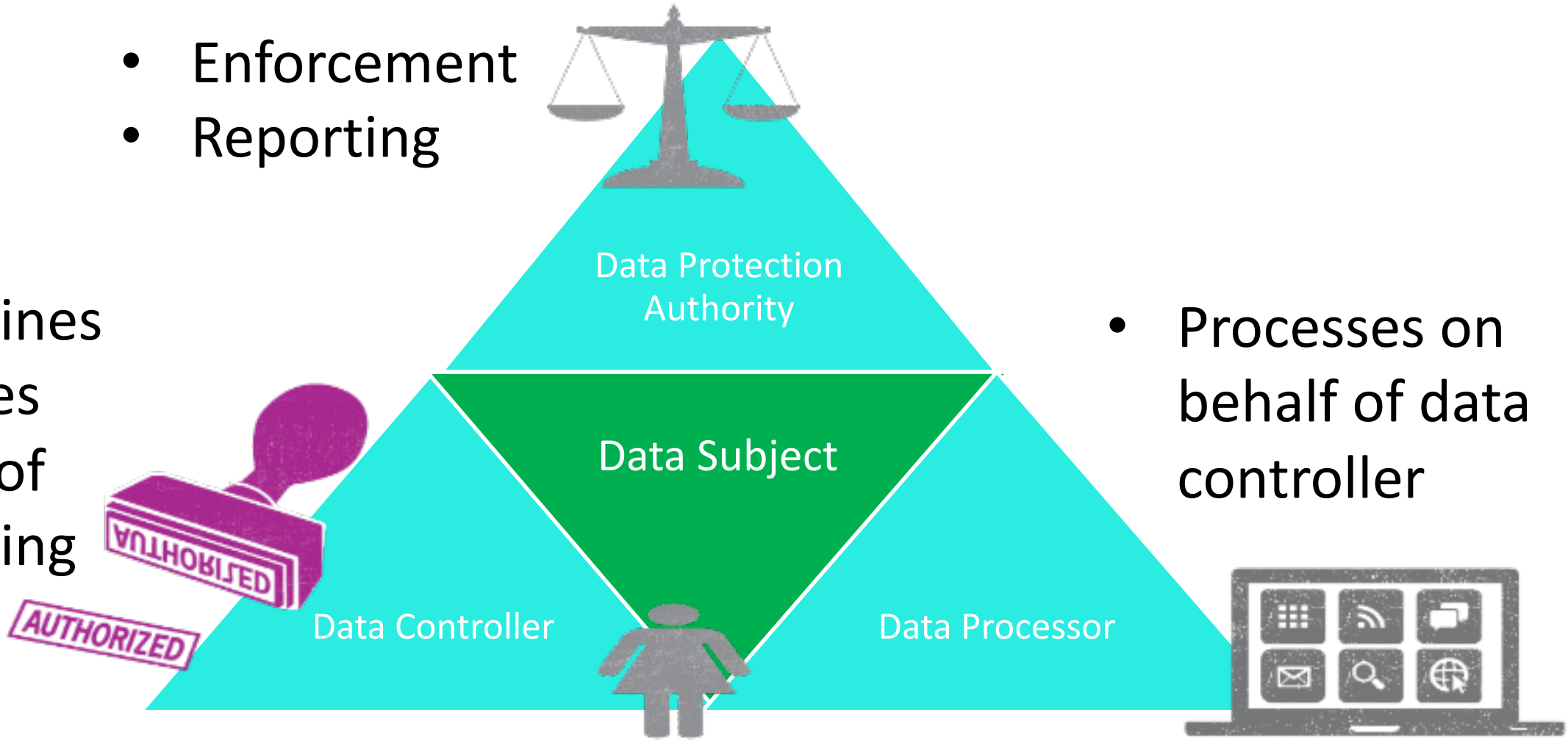
Sensitive Personal Information

- Racial or Ethic Origin
- Political opinion
- Religious or philosophical beliefs
- Trade-union membership
- Health or sex life
- Offenses or criminal convictions

- Social Security Number
- Financial Information
- Driver's License Number
- Medical Records

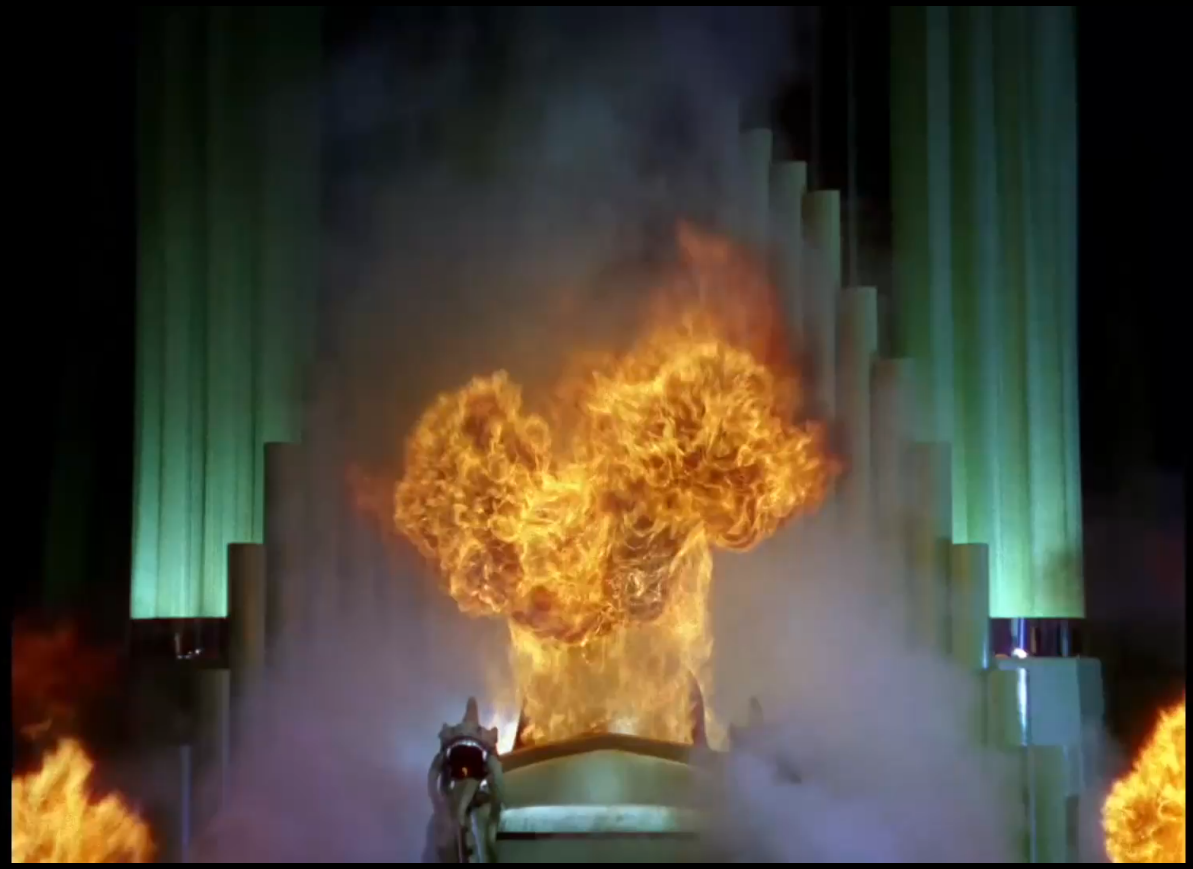
Data Protection Roles

- Enforcement
- Reporting

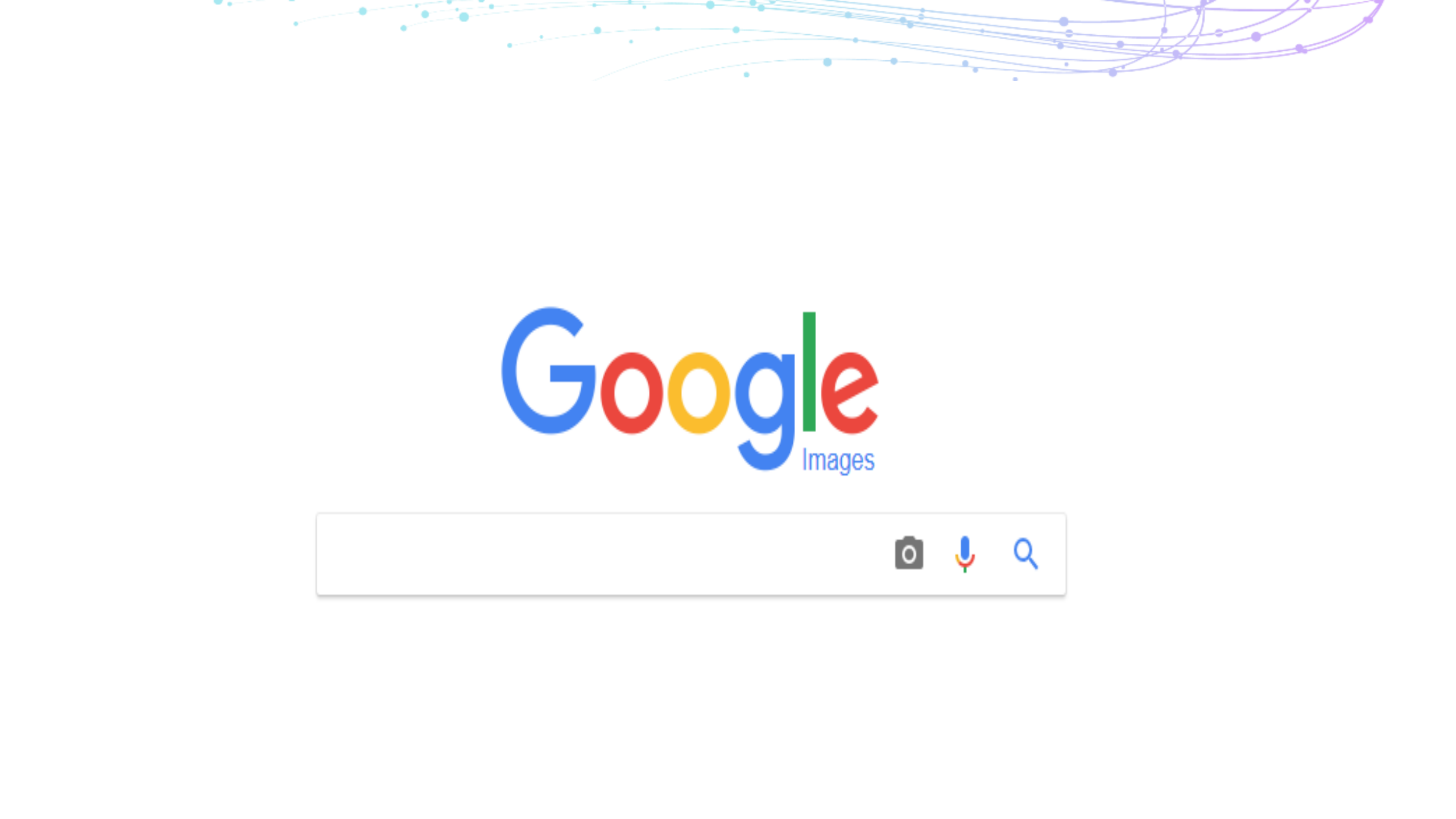


- Determines purposes
- Means of processing

- Processes on behalf of data controller



Where do we go when we need information ?


Google
Images


YouTube

GOOGLE Privacy Policy – How the Information is Used

- Which ads you find more useful
- People who matter most to you online
- Videos you like
- Language you speak
- We may associate your phone number with your device
- We Automatically collect and store “certain” information in our server logs

Privacy Policy
Last modified: December 19, 2014 (view archived versions)
There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we’re using information and the ways in which you can protect your privacy.
Our Privacy Policy explains:
What information we collect and why we collect it.
How we use that information.
The choices we offer, including how to access and update information.
We’ve tried to keep it as simple as possible, but if you’re not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long time user, please do take the time to get to know our practices – and if you have any questions consult this page.
Information we collect
We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you’ll find most useful, the people who matter most to you online, or which YouTube videos you might like.
We collect information in two ways:
Information you give us. For example, many of our services require you to sign up for a Google Account. When you do, we’ll ask for personal information, like your name, email address, telephone number or credit card. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.
Information we get from your use of our services. We collect information about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or you view and interact with our ads and content. This information includes:
Device information
We collect devicespecific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.
Log information
When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:

GOOGLE FINED 50 MILLION EUROS BY FRENCH REGULATOR CNIL UNDER NEW GDPR LAW (JAN 2019)

Privacy By Design – 7 Principles

1. Proactive/ Preventive
2. Privacy By Default
3. Embedded In Design
4. Positive-Sum Not Zero-Sum
5. End-End Lifecycle Protection
6. Visibility/Transparency
7. Respect for Users

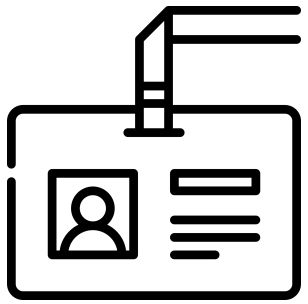
RSAConference2019

Final Thoughts

Today We Explored…

- Why Privacy should be Important to the security officer
- 8 information OECD Privacy Principles
- Global laws impacting privacy
- Building a program through Privacy By Design Principles
- Understanding the data elements and language of privacy

THE CISO "PRIVACY FOCUS" IS HERE



1 Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2 Regulatory Compliance Era CISOs Hired

2000-2004

3 Risk-Oriented CISO Emerges

2004-2008

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2008-2016

2016-2020's

5 **The Privacy and Data-Aware CISO**

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

Apply What You Have Learned Today

- Next week you should:
  - Schedule a meet n greet with the privacy officer or legal dept.
- In the first three months following this presentation you should:
  - Read the General Data Protection Regulation (GDPR) and any local laws
  - Visit the International Association of Privacy Professionals (IAPP) website at www.privacyassociation.org
  - Examine your organization's privacy policies
- Within six months you should:
  - Go forward with a privacy certification
  - Drive an assessment project (with the privacy officer) to determine where the privacy gaps are
  - Begin educating the workforce on privacy principles with regional meetings

In The End, Privacy Is All about TRUST….

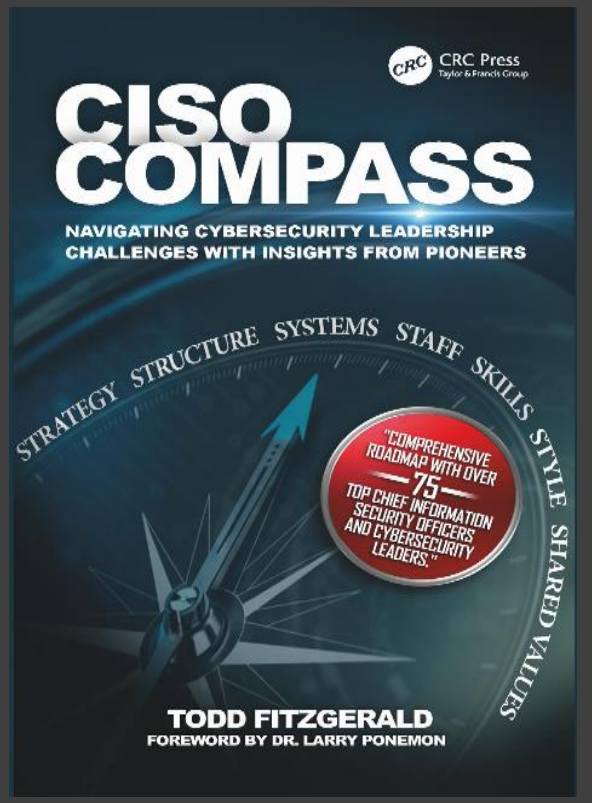
In The End, Privacy Is All about Establishing TRUST….

THANK YOU!!! ANY QUESTIONS?

Todd Fitzgerald CISSP, CISA, CISM, CIPP/US, CIPP/EU, CIPP/CANADA,CIPM, ISO27001, PMP, ITILv3f, Cybersecurity Leadership Author

LINKEDIN.COM/IN/TODDFITZGERALD

AMAZON.COM/AUTHOR/TODDFITZGERALD



CISO SPOTLIGHT, LLC

Trusted Cybersecurity and Privacy Training

RSAConference2019