PRIVACY ESSENTIALS FOR SECURITY PROFESSIONALS

Todd Fitzgerald,
CISSP,CISM,CISA,CGEIT,CRISC,PMP,ISO27000,CIPP/US,CIPP/E,CIPP/C,CIPM,ITITv3f
Managing Director/CISO
CISO Spotlight, LLC
@securityfitz
tfitzgerald@cisospotlight.com Linkedin.com/in/toddfitzgerald
Whose Lookin’ At Yur Stuff?

- 84% American Users don’t know how to secure email
- 41% of children’s profiles visible to all
- 56% Millennials will share location for coupons

Stats Source: Brandongaille.com, 29 Profound Internet Privacy Statistics, May 26, 2017
Today's Agenda

1. Why Should Security Officers Care About Privacy?
2. The Language of Privacy
3. Privacy Laws and Common Principles
4. Privacy Program Design
1. What Is The Phishing Threat Today?

WHY SHOULD SECURITY OFFICERS CARE ABOUT PRIVACY?
We all have our Privacy “Line”
The Fortune 1000 Is Investing in Privacy and Values Relationships To Information Security

Other Functions Seen as “Very Important” for Privacy Collaboration: Top Mentions

<table>
<thead>
<tr>
<th>Function</th>
<th>Mentioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security</td>
<td>76%</td>
</tr>
<tr>
<td>Legal</td>
<td>62%</td>
</tr>
<tr>
<td>Information technology</td>
<td>62%</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>14%</td>
</tr>
<tr>
<td>Government affairs</td>
<td>14%</td>
</tr>
<tr>
<td>Marketing</td>
<td>14%</td>
</tr>
<tr>
<td>Corporate ethics</td>
<td>14%</td>
</tr>
<tr>
<td>Human resources</td>
<td>14%</td>
</tr>
</tbody>
</table>

Source: Benchmarking Privacy Management and Investments of the Fortune 1000, IAPP 2014 Research
The 2018 CISO Evolution

- 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

<table>
<thead>
<tr>
<th>Leadership</th>
<th>• Plan path away from operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Thinking</td>
<td>• Refine risk management processes to business language</td>
</tr>
<tr>
<td>Business Knowledge</td>
<td>• Widen vision to privacy, data management and compliance</td>
</tr>
<tr>
<td>Risk Management</td>
<td>• Build support network</td>
</tr>
<tr>
<td>Communication</td>
<td>• Create focus and attention of business leaders</td>
</tr>
<tr>
<td>Relationship Management</td>
<td>Source: Forrester Research: Evolve to become 2018 CISO or Face Extinction</td>
</tr>
<tr>
<td>Security Expertise</td>
<td></td>
</tr>
<tr>
<td>Technical Expertise</td>
<td></td>
</tr>
</tbody>
</table>

Source: Forrester Research: Evolve to become 2018 CISO or Face Extinction
The New CISO will Need to Know Privacy

1. **Non Existent Security=Logon & Password**
   - FIRST CISO 1995

2. **Regulatory Compliance Era**
   - Must hire security officer
   - 1990s-2000

3. **The "Risk-oriented" CISO emerges**
   - 2000-2003
   - 2004-2008
   - 2008-2014

4. **The Privacy and Data-aware CISO**
   - 2015-20+

5. **The Threat-aware Cybersecurity, Socially-Mobile CISO**
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.
PRIVACY LAWS AND COMMON PRINCIPLES
"Right to Life"... "Right to Property"... "Right to enjoy life"..."Right to Liberty"

‘RIGHT TO BE LET ALONE’

Warren

Brandeis

The Right To Privacy Paper 1890
<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1890</td>
<td>&quot;The Right to Privacy&quot; Warren and Brandeis</td>
</tr>
<tr>
<td>1947</td>
<td>Article 12 of Universal Declaration of Human Rights</td>
</tr>
<tr>
<td>1966</td>
<td>US Freedom of Information Act</td>
</tr>
<tr>
<td>1970</td>
<td>Fair Credit Reporting Act</td>
</tr>
<tr>
<td>1974</td>
<td>US Privacy Act</td>
</tr>
<tr>
<td>1978</td>
<td>France Data Protection Act</td>
</tr>
<tr>
<td>1980</td>
<td>Organization for Economic Cooperation and Development (OECD)</td>
</tr>
<tr>
<td>1981</td>
<td>Council of Europe Convention on the Protection of Personal Data</td>
</tr>
</tbody>
</table>
**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

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

<table>
<thead>
<tr>
<th>Right to obtain confirmation DATA STORED</th>
<th>REASONABLE MANNER, COST and FORM</th>
<th>Ability to challenge denials</th>
</tr>
</thead>
<tbody>
<tr>
<td>REASONABLE TIME</td>
<td>If denied, be provided a reason</td>
<td>Right to erase, rectify complete, or amend information</td>
</tr>
</tbody>
</table>
A data controller should be accountable for complying with measures which give effect to the principles stated above.
THE LANGUAGE OF PRIVACY
Privacy Language Can Be Foreign To Business Environment...
Source: Several videos in this presentation from personal collection of Eugene Schultz, an unforgettable information security pioneer.
EU Defines Personal Data

- "Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

- Sensitive Personal Data or 'special categories of personal data' are generally prohibited from processing (some exemptions).

- De-Identified (non-personal) data – laws generally do not apply after identifying elements removed.
Personal Information Elements

- Name
- Gender
- Age
- DOB
- Marital Status
- Citizenship
- Nationality
- Languages Spoken
- Veteran Status
- Disabled Status
- IP Address
- Demographics
Sensitive Personal Information

EUROPE

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

UNITED STATES

• 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
Privacy Policy and Notice

- **Privacy Policy** – Internal statement directing employees

- **Privacy Notice** - statement to data subject for collection, use, retention and disclosure of information

- Contracts, application forms, web pages, terms of use, Icons, signs, brochures

**PRIVACY NOTICE**
- Initially, periodically
- Clear and conspicuous
- Accurate and complete
- Readable, plain language

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training
Example Privacy Policy – How the Information is Used

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
  • Log information

We may associate your device identifiers or phone number with your Google Account.

Device information

We collect device-specific 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:
Privacy Consent

OPT-OUT
- Processed unless data subject objects
- Box pre-checked to accept or check box to opt-out

OPT-IN
- Information processed only if data subject agrees
- Active affirmation
OPT-IN or OPT-OUT?

A. DO YOU WANT TO RECEIVE ADDITIONAL INFORMATION?
   - YES ☑ NO

B. ☐ CHECK BOX IF YOU DO NOT WANT TO RECEIVE MORE INFORMATION

C. DO YOU WANT TO RECEIVE ADDITIONAL INFORMATION?
   - YES ☐ NO

D. ☑ PLEASE SEND MORE INFORMATION ABOUT YOUR PRODUCTS
PRIVACY PROGRAM DESIGN
Privacy Information Life Cycle

- **Collection**
  - Limits
  - Lawful and fair means
  - Consent
  - Identified purpose
  - Proportionate

- **Use**
  - Purposes identified in notice
  - Implicit or explicit consent

- **Retention**
  - Retain only as long as necessary for purpose
  - Securely dispose, destroy, return

- **Disclosure**
  - Rights maintained on transfer of data
  - New purposes subject to consent
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
FINAL THOUGHTS/NEXT STEPS
Data+Privacy+Security+Risk= New Focus

Regulatory Compliance Era
Must hire security officer


Non Existent
Security=Logon & Password
FIRST CISO 1995

The Threat-aware
Cybersecurity, Socially-Mobile CISO

The 'Risk-oriented" CISO emerges

The Privacy and Data-aware CISO
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
Resources to Further Information Security Program (Available in RSA Book Store)

Steps To Build An Information Security Program

CISO Leadership Skills To Lead Program – Insight by Industry Experts & Pioneers

2 Books Available To BUILD and LEAD your Information Security Program

SIGNING IN RSA BOOKSTORE

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training
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 EU Data Protection Directive 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
Will This Be Your Security Program’s Future?
Will This Be Your Security Program’s Future?
Thank You Very Much For Your Participation!

Todd Fitzgerald, CISSP, CISM, CISA, CGEIT, CRISC, CIPP/US/E/C, CIPM, PMP, ISO27001, ITILv3f
Managing Director/CISO
CISO Spotlight, LLC
Deerfield, IL
Linkedin.com/in/toddfitzgerald
tfitzgerald@cisospotlight.com