Preparing for GDPR

John Welby

5/20/18

Cybersecurity & Risk Assessment

Information Privacy Programs – Preparing for GDPR

IT structure

- Privacy Office
- Chief Privacy Officer
- Privacy Program
- Where do you start?
  - At the top – the Board of Directors
- Board has a fiduciary duty to secure data
  - How data is protected
- Understand company's current cybersecurity program
- Authorize creation & funding of a Privacy Office

Governance Structure

People

- Chief Privacy Officer ("CPO")
- Desired for CPO to report directly (dotted-line) to CEO and/or General Counsel
  - Helps ensure independence of the CPO
  - Priorities overlap with Legal Department
- Legal
  - May shy away from risk-based decisions
  - Must be pulled into risk-based decision-making process
  - Business needs v. Compliance
  - Partner with CPO
    - Company applying for cyber insurance, etc.
- Marketing
    - Has the pulse of the stakeholders with greatest clarity regarding types of data to collect and repurpose?

Privacy v. Security

Data can be highly secure (i.e. encrypted) but still violate privacy principles

- Example: your company encrypts data end-to-end but your company ***processes data in a manner*** not agreed upon by customers.

Cybersecurity Preparedness

- Breach Response
- CPO and CISO are co-chairs of Incident Response Team
- Do you want CPO to also serve as legal counsel?
  - E.g. CPO/Asst. General Counsel
  - Will "privilege" apply?

Open Source Software ("OSS")

Affects every aspect of our lives

- Communications, transportation, retail, etc.…
- Comes with some risk
- Create an OSS compliance program
- Unmitigated risks balance cost savings?
  - E.g. Equifax Breach – vulnerability in Apache
  - Equifax was in the process of remediating

Open Source Software Management

Open Source Software Audit

- Helps minimize risk of using OSS
- IT, Legal, Risk Management
- Code Scanning
  - Identify OSS used
  - Identify licenses required
  - User obligations
  - Security Vulnerabilities
- Automated Code Scanning Tools
  - Static code analysis
    - Single program analysis
  - Dynamic code analysis
    - How programs interact with other programs and systems
- Record Results

OSS Policy & Guidelines

- Make relevant to audience
  - Engineers & techies – provide enough detail
  - Legal Department
- Identify why you need OSS Policy
  - Perform OSS Audit first
- Identify process for writing policy
- Identify contributors
- Get buy-in from all strata of organization
- Periodic OSS review
- Patching, updates, upgrades done promptly
- Track the process
- Guidance on how to display OSS requests

OSS requires customization for your environment

Key Issues Privacy Office Manages

Inventorying data

- Companies typically don't understand the type of information they process/collect
- Employ data "mapping"
- Document, understand and maintain the lifecycle of sensitive information storage

Vendor management

- "Baking" the privacy and security requirements into 3rd-party agreements and processes
- Very time consuming so, streamline the requirements for 3rd parties hosting confidential information:
  - "80/20 rule" -- 80% of the risk lies with …
  - Investigate 3rd parties' processes
    - SOC reports

What legal regulations must your organization comply with?

- Make a comprehensive checklist
  - 3rd party data storage methods
  - 3rd party transmission of data
  - 3rd party use of data

- Create guidelines/procedures for enforcing company policies and procedures with outside entities
  - Embed your requirements into the contractual framework for external relationships

Cultural Challenges

Change Management

- Impress upon teams the compliance and regulation requirements, customers' desires of how their data is handled

Accepting Risk

- Some technologies are embedded with inherently more risk
- Document the risk
- Document the justification for implementing a specific technology
- Rationale for making decision to move forward with technology – can help "color" that issue

Governance Framework

- Governance structure in place
- Privacy Office is funded and supported by leadership
- Develop baseline policies and procedures
  - Internal & external privacy policies
  - Document privacy statement
  - Maintain/update regularly
- Privacy and Security "baked in" to every initiative
- Privacy events

  National Privacy Day

- Vendor management
- Privacy and Privacy Awareness Checklists ("PAC") Assessments
- Training
- Progression
  - Stay abreast of regulation changes
  - Update policies to reflect changes in law and technology

Blockchain

- Blockchain is a method to share information in a non-centralized but secure way
- Records are distributed across nodes
- Bitcoin is one example of Blockchain technology (permissionless)
- Blockchain is an engine for transcoding processes
  - "defined by what you put around it…"

Why should lawyers care about Blockchain?

- Getting a lot of hype
- Approx. $1.4B in start-up funding in 2016
- More than 2500 patents
- Savings in efficiency gains in financials == $8 - $12B per year

Blockchain Key Concepts

Data Security

- Blockchain uses multiple layers of encryption
- Transactions are encrypted into "blocks"
- Ordered Blocks == "chains"
  - Makes it very hard for bad guys to access
- "Golden Record"
  - Blockchain is an append-only technology
- Records subsequent changes
  - Good for auditing
- "Can't spend a dollar twice"
  - Everyone has the same copy of the information
- Near Real-Time transactions
  - As opposed to current credit card transaction processing times
  - Blockchain and Distributed Ledger Systems
    - "timing matters"
  - Information shared to multiple parties

Blockchain lends itself well to:

- Transactions when parties don't trust each other's changes (i.e. commodity exchanges)
- Rules-based systems (computer systems)
- Where validity matters
- Auditability and Transparency among participants in the system

Permissioned v. Permissionless Systems

- Bitcoin Blockchain == Permissionless system
- Seeing requirements for Permissioned Systems – Gatekeeper effect
    - Banks must be a certain size to participate
    - Healthcare licensing as a factor to participate
- Permissioned systems logically place a virtual security fence around transactions
    - Not just anybody can see your data

Blockchain Use-Cases

- Estonia – public health records
- U.S. – exchange of health information
- Insurance Claims processing
- Art/Jewels – "provenance[1]" of an item is important
- Golden Record – tracks how items changed hands

Where do lawyers come in?

- 'Rules of the Road'
    - Similar to contracts
- Compliance
    - Companies must live within regulations

[1] Art is accompanied by documentation, commonly known as provenance, that confirms its authenticity. Good provenance leaves no doubt that a work of art is genuine and by the artist whose signature it bears.

GDPR Data Transfer Regulations

- International data transfer processing restrictions of GDPR based on EU Privacy Directive of 1995
    - Equivalent Regulation:
        - Safe Harbor → EU/US Privacy Shield
        - EU Model Clauses
- Data transfer mechanisms look very similar to 1995 regulation
- New Notice Requirements for Data Transfer Mechanisms in Privacy Statements
    - Transferring customers' data internationally
        - Document your data transfer mechanisms you are using
        - Notify data subjects of whether you're transferring data internationally and if you are
        - Is destination country a country that the EU Commission "finds adequate?"
            - "Adequacy" == privacy laws of destination country are essentially equivalent to GDPR, or
        - Must notify data subjects what:
            - Data transfer mechanisms used
            - Reference the appropriate safeguards you have in place
            - Tell data subjects where they can find information on the data transfer mechanisms
- Monetary fines can be extreme for violations
- Failure to comply (processing or transferring of any data outside EU) can be subject to a fine of:
    - €20M, or:
    - A sliding scale up to 4% total worldwide turnover
        - How big company is
        - How egregious the breach
        - Duration of the violation

Five Options for Data Transfer Mechanisms

Only eleven countries are "adequate" to transfer data:

Canada	Argentina
New Zealand	EU territories (e.g. Isle of Man)

1. Binding Corporate Rules ("BCRs")
    - Enshrined in GDPR
    - Pertinent to intra-group transfers only
    - Takes approx. 18 months to get
    - > $100,000 in compliance tools to get up and running
    - Previously approved BCRs will remain in place until repealed and replaced

2. Model Clauses
    - Contractual clauses related to data transfers
    - Companies can add to data transfer agreements or Master Service Agreements ("MSAs") with vendors and data processor in other countries

3. Certifications
    - Reviewed by EU Commission Supervisory Authority

4. Codes of Contact
    - Reviewed by EU Commission Supervisory Authority

5. Consent
    - Even consent has been made more difficult:
    - Individuals must respond actively, orally or in writing and knowingly

Latest GDPR News

Privacy Shield has been challenged in at least two court cases:

- Cases will take a year or two to make it to the European Court of Justice
- First review of Privacy Shield just completed
    - European Commission found it "adequate"
        - If using Privacy Shield now, keep using it
- Review of Model Clauses has been challenged to the Irish High Court and they sent the case to the European Commission
    - Review and ruling will take a year or two
        - Keep using Model Contracts/Clauses

United States Department of Justice Guidance on Bug Bounty Programs

Issued a framework for a vulnerability disclosure program for online systems

https://www.justice.gov/criminal-ccips/page/file/983996/download

Background

1. Build secure software by continually finding and fixing software vulnerabilities ("bugs").
2. Framework targets companies using 3rd parties (ethical hackers) to find security holes in networks and software.

Examples

1. 2010 – Google started
2. 2017 – DOD, "Hack the Air Force"
    - 207 bugs found in online system
    - 17 yr.-old took home the most money for discovering most bugs
3. "Hack the Pentagon"
4. "Hack the Army"

Potential Issues w/ Ethical Hacking

1. Ethical hacking can cause inadvertent problems:
    - Sensitive information can be inadvertently disclosed to the wrong parties

2. Companies are doing these security assessments informally with no boundaries or guidelines

Ethical Hacking Focus

1. Clearly define methods 3rd parties can and can't use to disclose security vulnerabilities.
2. Clearly define who report is released and who has access

Four-Step Program

1. Design the "bug" program:
   - What's fair game for 3rd party to access/hack
   - Clearly define restrictions on methods and techniques used by 3rd parties:
     - Don't run during business hours
     - Don't use social engineering
     - Specify type of bugs 3rd parties are permitted to go after
2. Plan for administering the program
   - Reporting procedure
   - POC for reporting vulnerabilities
   - Action/remedies taken for:
     - Good-faith mistakes
     - Bad-faith mistakes/damage caused
     - Malicious activities
3. Prepare a policy that accurately and unambiguously captures the organization's intent
   - A formal policy
     - Authorized activities
     - Scope of systems and data subject to the data disclosure program
       - Very detailed and precise
     - Define protocols and restrictions on handling sensitive data
     - Specify consequences of violating policies
       - Share with 3rd parties
   - Implement the Program
     - Make disclosure policy easily accessible and widely available
       - Internally & Externally
     - Encourage employees to follow policy
     - Instruct 3rd parties as to requirement to adhere to policy

Consequences of Not Following Privacy Policy

Background

The Computer Fraud and Abuse Act ("CFAA")

- Anti-hacking statute prohibiting unauthorized access to computers and networks
- Civil and criminal penalties

The Department of Justice's ("DOJ") focus is for organizations to be mindful of irresponsibly bringing in 3rd parties for ethical hacking.

DOJ is likely to continue to expand CFAA

Summary

1. Clearly define boundaries for parameters of vulnerability (ethical hacking) assessments.
2. Create contracts and policies in clear and unambiguous terms.
3. Perform due diligence BEFORE bringing in a 3rd party ethical hacker.

(American Bar Association, 2017)

American Bar Association. (2017, November 9). Podcast - Ascending Stars of ABA SciTech:Hot Topics in 60 minutes. Washington, DC, United States of America. Retrieved May 19, 2018, from https://www.americanbar.org/groups/science_technology/publications/podcasts.html