August 2021

Privacy Compliance Newsletter

Check out ID's Privacy Compliance webpage, where you can find up-to-date thought leadership and download the most recent version of this newsletter.

PRIVACY HAPPENINGS

IAPP: The Privacy Advisor Podcast

Jedidiah Bracy's **podcast interviews** of some of the privacy world's most interesting people regarding current topics such as:

- Rep. DelBene on what it will take to pass US privacy legislation
- April Doss on US surveillance, global data flows and Big Tech after the Russia investigation
- Analyzing Virginia's new privacy law with Odia Kagan
- Is a 'multilateral privacy treaty' the answer to 'Schrems II'?
- Many others

The Death of the Third-Party Cookie

Safari and Firefox block third-party cookies by default to protect users' privacy. Google Chrome announced they will join them by 2022. Is this really the death of the third-party cookie? Should advertisers panic? Google is working on a browser-based tracking model. Publishers and brands are developing ad models relying on their own first-party data.

See what may replace third-party cookies.

Transnational Codes for Cloud Service Providers Approved Under the GDPR

The GDPR introduced the possibility of compliance for controllers and processors through an approved code of conduct. The first codes have been approved by the European Data Protection Board (EDPB) and relate to cloud computing. The approved codes of conduct are:

- EU Data Protection Code of Conduct for Cloud Service Providers (the EU Cloud Code)
- Cloud Infrastructure Service Providers in Europe (CISPE Code)

Click here for details provided by **OneTrust DataGuidance.**

WHAT IS YOUR PRIVACY COMPLIANCE MATURITY?

This quiz will help determine your data privacy posture and give you tools and tips to gaining compliance.

Take the quiz!

SPOTLIGHT:
CYBER TALENT CRUNCH VS PRIVACY RISK

"Hackers gain access . . ." seems to be the lead story of many news outlets the past few months. These stories describe criminals hacking into computer systems and demanding money for the safe return of the stolen data. Recently these attacks have impacted our supply chain and our daily lives. The **Washington Post reports these crimes have resulted in** " . . . missed chemotherapy appointments and delayed ambulances, lost school days, and transportation problems." The ransomware attack on Colonial Pipeline led to gas shortages; JBS meat processing led to worries about meat shortages; Baltimore County Public Schools were forced to halt classes; and the ticketing process of Martha's Vineyard ferry service was disrupted to name just a few.

Corporate America should invest more in cybersecurity you say. **"The only hitch: There's a massive, longstanding labor shortage in the cybersecurity industry"** reports CNN. According to a 2020 survey by (ISC)2, there are about 879,000 US cybersecurity professionals in the workforce and an unfilled need for another 359,000. Globally, the gap is estimated to be over 3 million with some believing closer to **3.5 million**. From 2013 to 2021, there has been a 350% growth in open cybersecurity positions.

The need for cyber talent and the number of unfilled positions won't be resolved quickly. Nowhere is the workforce-skill gap more pronounced than in cybersecurity.

What to do in the meantime

Just hiring more cybersecurity experts – if you can find them -- won't solve all the hacking threats. Winning the battle will take a comprehensive playbook including plays, strategies, and a proactive defense. Look to your privacy program to quarterback a proactive strategy on two fronts.

Get in shape

Just as two-a-days are a staple of football to get in shape for the season, there are two privacy principles that make your organization better prepared to reduce the effects of a data breach:

- privacy risk management
- data retention

Privacy Risk Management: establish control over personal information

Step 1: Scout the Landscape
You'll need an understanding of the personal data your organization is collecting, where it's stored, how it's being used and if it is shared. You're right, this step describes the foundation of every strong privacy program – a data map. If your organization collects sensitive or personal customer data for marketing campaigns or to improve customer experience, for example, how this data is stored and secured is essential. With a data map, the flow of data across your organization is visible allowing you to see potentially risky processes.

Step 2: Conduct Privacy Risk Assessments – aka Data Protection Impact Assessments (DPIA) or Privacy Impact Assessments (PIA)
Privacy Risk Assessments serve as early warning systems that detect access or security problems. These systems ensure your organization is accurately measuring and managing customer risk (not just organization risk) and is compliant with global data protection regulations.

Regulations like the CCPA and GDPR don't specify data protection technologies or make process recommendations. Neither do they offer risk assessment templates. Best practices shared by the IAPP state risk identification must to be a part of any business process using personal or sensitive data as well as any system design. A risk-based approach should be your guide through the entire lifecycle of data.

Benefits of adding Privacy Risk Assessments in your playbook include:

- Enhance information for informed decision making
- Avoid costly or embarrassing mistakes in privacy compliance
- Reduce revenue loss arising from customer abandonment of products and services due to mistrust
- Provide evidence your organization is working to minimize its privacy risks

These benefits attempt to alleviate the costly and embarrassing consequences of a data breach. The average total cost of a data breach in 2019 was $3.92M (from IBM Security and Ponemon Institute: 2019 Cost of a Data Breach Report). This report also indicates lost business is the largest contributor. The average cost of lost business was $1.42M or 36% of the total average cost. Not all costs are immediate. The report goes on to say about one-third of data breach costs occurred more than a year after the breach incident. Thus, data breaches impact your organization for years. Your organization's financial and brand well-being is worth the effort to identify data processing risk and establish business workflows to mitigate them.

Data Retention: If you don't have it, they can't take it

In last month's newsletter, we reviewed why organizations can't ignore their obligations related to the data retention requirements of regulations like the GDPR. Privacy regulation requirements and threats of cyber incidents should incentivize businesses to implement proper information governance programs that include strong data retention policies for all content. **(Click here if you missed this article)**

Data is the lifeblood of the organization. It must be available for use to meet business objectives, but it must be secured as it flows across your organization. Privacy Risk Assessments intercept vulnerabilities. With this information, informed decisions can be made regarding risk remediation and necessary mitigation workflows. Informed decisions can also be made regarding how much risk is tolerable when balancing business objectives with protecting consumer trust and brand reputation.

With focus on a risk-based approach teamed up with strong retention policies for all content, your organization will be in shape to run interference against those hackers.