JS|HELD

PERSPECTIVES

Data Privacy in 2023: Expectations, Responsibilities & Cyber Security Tactics to Safeguard Your Information

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

As more of our lives and work become digitized, an inherent overlap continues to grow between data privacy and cyber security programs. Think of two similarly sized circles: in the past, data privacy and cyber security may have overlapped on the edges, but today, their centers are almost on top of each other. In this article, we begin to look at the data privacy / cyber security relationship, as undoubtedly, the issues are connected, and we can see this trend in industry reactions, publications, and standards.

For example, in 2020, the U.S. National Institute of Standards and Technology (NIST) released the Privacy Framework (PF) and soon after created a crosswalk of controls against the Cyber Security Framework (CSF). In Europe, the General Data Protection Regulation (GDPR) has played a prominent role in pushing data privacy compliance since 2018, influencing cyber security decisions. And today, more non-European Union (EU) jurisdictions are deploying their own federal and regional legislative and regulatory controls, especially those related to personally identifiable information (PII), personal health information (PHI), and consumer protections.

With these trends in motion, do methods exist for data privacy and cyber security initiatives to work together and lower overall risk to the organization? Yes, there are, and we will outline some areas in which the two initiatives can work together. Specifically, we focus on identifying overlap areas and steps that can be taken to create an effective program, all designed to better protect data and reduce cyber risk.

Cyber Security & Data Privacy: Their Differences and Why They Need Each Other

Cyber security controls are generally voluntary, unless external forces demand compliance (e.g., regulatory controls, certification to do business, requirement to notify, etc.). But data privacy tends to be mandatory, through legislation and well-defined regulation. For example:

- Europe has the GDPR, Data Protection Law Enforcement Directive, and proposed legislation such as the Digital Services Act, the Digital Markets Act, and the Artificial Act.
- In the U.S., apart from the common federal laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA) and the Children's Online Privacy Protection Act of 1998 (COPPA), more states are coming out with their own versions of consumer privacy and data security legislation, such as the California Consumer Privacy Act (CCPA) and the New York Department of Financial Services (NYDFS) cyber security regulations.
- Other jurisdictions from across the globe are also expanding their data privacy laws.

But a paradox exists: today's digital demands, coupled with data privacy legislative and regulatory requirements, require cyber security protections. Think about it like this:

- Cyber security controls, from a legislative and regulatory perspective, may be optional; but
- Mandatory data privacy controls, due to digitization, require cyber security controls.

The overlap is therefore immense, though support and implementation of controls, may be very different depending on which perspective you are viewing the problem from.

Is Buy-In for Data Privacy Easier than Cyber Security?

The consequences of failing to comply with data privacy laws are known – fines, civil litigation, market share loss, and shattered confidence and trust. Therefore, as consequences are clear and tangible from a data privacy perspective, enhancements to your cyber security program may garner more support if your information security, data privacy, and risk management leaders can clearly demonstrate the overlap between these separate, but closely related, programs.

It is the **clarity of consequences** – specifically from the data privacy perspective – that become the motivating factor for improvement. So how can these functions work together?

Eliminate Unknown Unknowns

Two data-related questions **must** be answered to build a strong program:

- What rules (e.g., laws, regulations, retention demands, etc.) apply to you?
- What data do you hold?

Depending on the size and complexity of your organization, (e.g., where you operate, what business you are in, what external forces influence your data handling, etc.) answers to these questions may not be clear cut. Here are some quick tips to navigate through each issue:

- **Map requirements by jurisdiction.** Without this analysis, expect blind spots. You can roll the dice and ***assume*** the most stringent requirements, but this route is potentially inefficient, may result in poor return on investment, and miss unique jurisdictional requirements. Expect significant input from various sources (e.g., counsel, security, privacy, business units, and perhaps even vendors).
- **Triage, rank, and prioritize requirements.** Once jurisdictional analysis is complete, continue review from a risk management perspective that will allow for risk prioritization. That means knowing your risk tolerance levels. For example, Jurisdiction X has incredibly strict requirements, but your operations are so limited in that area, the more appropriate ***business decision*** is to take on some risk.
- **Cross reference requirements against data you hold.** This task can be tricky. If your data has not been classified or needs to be reclassified in buckets that align with jurisdictional requirements, you may have a serious blind spot. Once you are capable of performing this task, you should be able to identify gaps that require remediation.
- **Validate data classification procedures.** Well managed data classification can be a life saver due to the many downstream impacts. Classification helps determine segmentation, provenance, residency, and retention requirements, and supports triaging and identification during response.

After completing these tasks, you could, in fact, end up opting for the most stringent requirements, which is not a bad approach, because you at least went through the exercise to ensure no blind spots exist. The additional upside of using the most stringent requirements is that the jurisdictional mapping analysis likely positioned you well for maximum coverage, where only tweaks are required by jurisdiction.

Moreover, this exercise can also identify data you ıneed to retain. Sometimes, your best risk minimization option is to not collect data or destroy data in hand.

Bad Decisions Stem from Bad Information

An additional – and important – issue to keep in mind is the reliability of your analysis. Data uniformity plays a significant role in generating major outputs and maintaining smooth operations (e.g., everyday business, processing and securing data, and facilitating incident response). Therefore, any operation(s) that does not seek data normalization will have difficulty producing the best results. Ask yourself these questions:

- *What data types (e.g., intellectual property, customer, PHI, etc.) do you hold?*
- *Are data types segregated and if so, how?*
- *And most importantly, how confident are you about these responses?*

There is a saying in the computer science world: ***garbage in, garbage out.*** This is the exact situation you want to avoid, because doing so puts you into the position of making decisions. Not only are your data privacy efforts put at risk, but you build inefficiencies into your incident response processes, and, candidly, could be making bad business operation decisions.

Preparing for the Worst

Assuming you have come this far in your data privacy journey, the last pieces of the puzzle are program maintenance and preparation for the breach. Mature organizations will build in processes that can automatically pull data privacy requirements. From a breach perspective, predetermined

escalation matrices, triage paths, and communication flow charts will have been developed and tested to build muscle memory. These are the bedrock principles of strong data privacy ***and*** cyber security programs.

CONCLUSION: CONNECTING DATA PRIVACY TO CYBER SECURITY

In an upcoming two-part mini-series on cyber hygiene, we will examine how a good cyber security program can stem from good data privacy practices. The keys to success in the immediate future will rest in your people, specifically: leadership's ability to demonstrate ***why*** security matters to everyday users, going beyond ***how*** to act securely, and adapting to changing workplace environments.

Acknowledgments

We would like to thank Ron J. Yearwood Jr., and George Platsis for providing insight and expertise that greatly assisted this research.

More About J.S. Held's Contributor

George Platsis, CCISO, is a Senior Director in the Digital Investigations and Discovery unit, which is part of J.S. Held's Global Investigations practice. George has designed and delivered solutions, and led teams, focused on improving breach readiness, designing enterprise-wide and business-unit specific incident response programs, and crafting information estate hardening solutions for a series of Fortune 100 clients in the healthcare, media, financial services, manufacturing, defense, and commercial electronics industries. As part of the Cyber Security practice, George has a lead role in developing and delivering proactive incident response and resilience engagements. He has extensive experience in engineering enterprise-level incident response programs, breach readiness evaluation, business continuity, and disaster recovery. He also leverages past experiences from reactive incident response engagements, complex investigations, and work experience in the security, emergency management, pandemic planning, and bioweapon research fields.

George can be reached at George.Platsis@jsheld.com or +1 321 346 6441.