ISSUE BRIEF

US POLICY

Challenges and Opportunities in Organizational Collaboration on Privacy and Cybersecurity

Author: Amie Stepanovich, FPF, November 2024

FUTURE OF PRIVACY FORUM

Executive Summary

Increasingly, organizations that handle personal data need privacy and cybersecurity teams to collaborate. Collaborative projects often involve shared questions regarding technologies, business practices, and legal compliance.

FPF's Expert Group on Privacy and Cybersecurity has launched a new project to better understand these trends. As an initial step, we surveyed privacy and cybersecurity experts across organizations of varying sizes, sectors, and stages of maturity in terms of their data protection programs.

FPF's early research indicates that incentives for collaboration have expanded both in terms of breadth and frequency in the past year. This, despite our finding that organizational privacy and cybersecurity teams often have systemic differences in both structure and staffing, as well as evidence that structural challenges can hinder effective collaboration. Below, we detail the preliminary findings from our work, including additional elements that are impacting collaboration between privacy and security teams and several factors that can lead to more effective collaboration - e.g. organizational strategy, leadership support, relationship-building, and cross-training.

These findings provide the basis for organizations to consider how their internal structures may influence operations, although more research is needed to further support these findings and to provide a basis to extrapolate recommendations for organizations looking to develop new processes and procedures to increase cross-team cohesion and collaboration.

Challenges and Opportunities in Organizational Collaboration on Privacy and Cybersecurity

Author: Amie Stepanovich, FPF, November 2024

I. Introduction

Most organizations today collect and utilize personal information in a variety of contexts. Personal information may come, directly or indirectly, from users and subscribers as well as employees or contractors or be collected from third party partners. It may be used to provide the central product or service, but also for internal processes or services, including employee services, for advertising or market research, or for secondary services.

One important context in which personal data gets utilized is for the security of the organization and its resources. Those resources may include physical assets, such as hardware and facilities, as well as digital assets, including systems and databases. As such, organizational offices and personnel tasked with security may see different categories and types of personal information both as a tool to carry out their job function as well as an asset that their function is intended to protect.

Security offices are, of course, not the only parts of an organization with an interest in protecting personal information. Another key organizational constituency are the offices and individuals tasked with privacy and/or data protection (collectively referred to herein as "privacy"). Like security units, privacy units often establish organizational policies and practices to govern the processing of personal information, including collection, use, retention, and transfer.

Both security and privacy departments may be required to meet regulatory requirements in the form of national or localized legislation or regulation, including laws passed in different U.S. states and territories where the organization functions. Operational considerations may also be drawn from national and international guidance documents, sectoral “best practices”, or other policy frameworks or materials. Finally, both units may be subject to internal policies and priorities, including commitments related to ethics, human rights, or corporate governance.

Together, complicated governance frameworks alongside department priorities, which sometimes may conflict, have the potential to create tension within organizations. By contrast, when units work together it may not only ameliorate those tensions, but create better, more cohesive, and more efficient organizational workflows.

In 2024, the FPF set out to learn more about how organizations structure their privacy and cybersecurity teams, and specifically about how they think about and/or facilitate cross-team collaboration. As a first step, we have conducted in-depth qualitative interviews with individuals from seven different organizations to discuss their experiences and insights. While this is a small sample set, the organizations represented included a range of different industries, business models, and sizes. However, all of the seven organizations shared a common characteristic in that they process personal data in the course of business. Through analyzing the results of these interviews, FPF has derived ten key takeaways that speak to the internal operation of these critically important teams. These takeaways include:

1. Cybersecurity teams tend to be more established and report to someone with higher seniority than privacy teams
2. Organizations are divided on the extent to which they have, or need to incorporate artificial intelligence specific policies into their operational structures
3. Structurally, organizations tend to house privacy teams in the legal department, whereas the location of cybersecurity teams varies broadly
4. In the last year, the need for collaboration between privacy and cybersecurity teams has expanded both in terms of breadth and frequency
5. While collaboration is generally viewed positively, lack of cross-team collaboration is seen as a pervasive problem, frequently exacerbated by limited or ineffective communication
6. Successful collaboration is fostered by organizational strategy, leadership support, and relationship-building, leading to positive outcomes and long-term strategic benefits
7. Teams often develop structured and strategic plans around activities requiring specific collaboration, while more general cross-team communications tend to be more ad-hoc

8. Internal competition undermines trust between teams and hinders effective collaboration
9. Cross-Training can increase trust and facilitate understanding of when and how to initiate collaboration
10. Leadership support for organizational alignment and coordination is critical to respond to the growth of business imperatives that require cross-team collaboration

FPF is currently considering next steps in this line of inquiry, including how generalizable these experiences may be as well as what lessons organizations may or may not be able to derive from these takeaways. If you would like to share an idea, get involved with our work, or support further research, please contact the Future of Privacy Forum.

II. Top Takeaways

The following takeaways were derived from a series of interviews with individuals working on privacy and/or security at a small set of organizations.

Takeaway 1: Cybersecurity teams tend to be more established and report to someone with higher seniority than privacy teams

In a comparison of organizational privacy and cybersecurity teams, cybersecurity teams tend to have been established earlier, to include a larger number of team members, and to report to someone with higher seniority. Respondents most commonly reported that cybersecurity teams were established more than ten years ago, while privacy teams were evenly divided between those that were older than ten years and those that were between 5-10 years old. Further, most respondents reported that their company included 16-50 employees with a privacy function, while most identified more than 100 employees with a cybersecurity function. However, some of that distinction could be accounted for by those with larger teams devoted to cybersecurity incident response and monitoring.

Finally, when asked to identify the senior-most person with responsibility in each area, responses for privacy functions were more likely to indicate a director-level title, whereas the most senior cybersecurity employee was consistently someone at the vice president-level. In addition, cybersecurity leads were more likely to report directly to a CEO, whereas most privacy leads reported to either the company's General Counsel or a Deputy General Counsel.

Takeaway 2: Organizations are divided on the extent to which they have, or need to incorporate artificial intelligence specific policies into their operational structures

Respondents were generally split on the extent to which they had formally adjusted their operational structures to account for AI. Some indicated that their organization had integrated AI into their operations and, in some cases, already had long-standing teams, policies, and processes related specifically to AI. However, on the other hand other respondents reported that few, if any, new steps had been taken to particularly account for AI. In this latter group, there was a still further split between those who indicated their organization was relying on existing governance processes that could already handle the new context and others who had not yet encountered demands around AI that necessitated any special consideration. Interestingly, respondents in each group indicated that they believed that their exact approach was consistent across industry more broadly. This may indicate that AI is being handled similarly within sectors, even as there are many distinct overall approaches.

Takeaway 3: Structurally, organizations tend to house privacy teams in the legal department, whereas the location of cybersecurity teams varies broadly

Without exception, when asked to identify the home department for privacy work within a company, respondents identified their legal team (or a subcomponent). By comparison, in response to a similar question about cybersecurity operations, responses varied broadly, including information technology, finance, or a cybersecurity-specific department. Furthermore, as mentioned previously, privacy teams were much more likely to report to the General Counsel or Deputy General Counsel. Only one respondent indicated that the cybersecurity lead reported to the General Counsel.

Takeaway 4: In the last year, the need for collaboration between privacy and cybersecurity teams has expanded both in terms of breadth and frequency

When respondents were asked to reflect on what issues required the most consistent collaboration between privacy and cybersecurity teams over the past five years, most answers referred to data breaches or other incident-specific investigations (and responses thereto) as well as processes to review and assess third-party vendors. However, when asked to focus instead only on cross-team collaboration over the past year, answers grew both in terms of amount - the number of times collaboration was required - and variance - the number of issues that necessitated collaboration. All told, respondents identified at least thirteen separate areas necessitating significant collaboration in the most recent year, including, but not limited to, responding to increasing regulatory requirements, audits, operationalizing artificial intelligence, and implementation of privacy-enhancing technologies.

Takeaway 5: While collaboration is generally viewed positively, lack of cross-team collaboration is seen as a pervasive problem, frequently exacerbated by limited or ineffective communication

Every respondent was generally positive about the impact of cross-team collaboration, with some highlighting its centrality to the ability of organizations to address broad challenges and meet overall goals. There was also broad agreement across responses of the strong correlation between good communication and successful collaboration. For example, one respondent favorably observed that increased communication often increased collaboration.

However, in discussing specific circumstances of collaboration, respondents individually tended to have a greater number of examples and observations regarding the challenges of cross-team work than its successes. The top cause given for unsuccessful collaboration related to failures in proper communication, either directly or indirectly. In explanation, many respondents spoke to a lack of understanding between teams as a significant barrier to cross-team work. In some cases that lack of understanding was literal; individuals highlighted the distinct terms-of-art and meanings in how privacy and security teams communicated that led to confusion and, in extreme cases, resentment when individuals felt patronized or belittled. In other cases, the lack of understanding stemmed from a lack of engagement - feeling that would-be collaborators were not listening or approaching cross-team issues in a way that could allow a mutual connection to the topic at hand.

Takeaway 6: Successful collaboration is fostered by organizational strategy, leadership support, and relationship-building, leading to positive outcomes and long-term strategic benefits

While collaboration is viewed favorably in general, and often seen as unsuccessful in practice, examples given of instances of successful collaboration provided insight into ways to foster a collaborative environment. For instance, respondents named clearly defined roles and responsibilities, both for relevant teams as well as for specific individuals, most frequently as the driver of successful collaborations. On the flip side, collaboration itself was identified as a challenge in cases where individuals were unsure of their role or teams felt like their contributions were not valued.

Successful collaboration is also frequently supported by broader organizational strategy, including encouragement from leadership as well as the establishment of platforms for collaboration, cross-team exercises, or combined training.

In cases where respondents reported cases of successful collaborations, they also shared that the results of that collaboration can facilitate broader organizational improvements, including the identification of systemic gaps in organizational process and the pursuit of important long-term strategic shifts. Successful collaborations were also said to help establish positive relationships between team members that increased respect for what each individual could bring to a collaborative process and form the basis for future cross-team projects.

Takeaway 7: Teams often develop structured and strategic plans around activities requiring specific collaboration, while more general cross-team communications tend to be more ad-hoc

When projects, either short- and long-term, were determined to require specific cross-team collaboration, respondents indicated that teams would attempt to develop structured, strategic approaches to the work. This could include consideration of clear understanding of roles and responsibilities, formulation of cross-functional teams, and creation of processes to respond to identified circumstances necessitating specific collaboration.

However, while failures in communication were frequently connected to unsuccessful instances of collaboration, methods and means for communicating between teams were not generally approached with the same level of strategic thinking. For instance, when asked about tools for communication, most respondents provided information on general office tools or resources, including e-mail, messaging, or direct interactions, but not necessarily with regard for the strengths or weaknesses of any particular tool in a particular context. By contrast, some responses did include reference to formal committees or regular meetings set up to ensure necessary, comprehensive communication that included all relevant team members.

Takeaway 8: Internal competition undermines trust between teams and hinders effective collaboration

Second only to communication, trust was frequently identified as a key component for successful collaborations. Unfortunately, several responses identified experiencing a lack of trust directly related to the need (or perceived need) to compete internally across teams for important resources. Some resources identified by respondents as inciting competition included headcount, budget, leadership attention and/or recognition, or professional development opportunities, such as public speaking or ability to contribute to responses to press inquiries.

Respondents identified that a competitive dynamic frequently led to assertions of uneven control over issues, processes, or partnerships and, in some cases, the creation of overlapping or redundant processes, such as separate teams contracting with distinct vendors for the same work. In these instances, respondents reported significant inefficiencies as well as organizational decisions that lacked cohesion or failed to account for the full context of an issue. Notably, respondents also raised that this was a compounding problem, where the behaviors facilitated by the lack of trust would themselves further degrade trust between the teams.

Takeaway 9: Cross-Training can increase trust and facilitate understanding of when and how to initiate collaboration

In general, privacy teams were described as more heavily on the “legal” side of an organization, while cybersecurity was often described as highly “technical”. However, several respondents raised that the frequent areas of overlap required not only professionals working on either side to have basic understanding of the other, but also to establish appreciation and respect for the expertise on topics on which they were less familiar. A key tactic for establishing a general baseline of shared knowledge was to host cross-trainings that included individuals working across both topics. In addition to building a broader shared literacy and lexicon, which necessarily supported a more efficient identification of issues where one team may need to bring expertise from another, shared training also frequently increases cross-team trust, which benefits the organization more broadly.

Takeaway 10: Leadership support for organizational alignment and coordination is critical to respond to the growth of business imperatives that require cross-team collaboration

Respondents largely championed the need for organizational leadership to support and actively promote increased alignment and collaboration between privacy and cybersecurity teams. Where leadership openly regards one team as more valuable or important than another, respondents often reported internal discord. However, in cases where leadership establish common goals, endorse collaborative processes, and address challenges comprehensively, respondents expressed feeling more empowered to address the increasing number of mutual challenges impacting both teams and the organization more broadly.

III. Conclusion

The above takeaways represent the results of very preliminary research into the aspects of organizational collaboration between privacy and cybersecurity teams. These takeaways may not apply to all organizations or all teams, and more work will be needed to determine what, if any, recommendations may be able to be drawn from these insights. If you have comments, suggestions, or would like to get involved in FPF's Privacy and Cybersecurity Expert Group, please reach out to info@fpf.org for more information.

FUTURE OF PRIVACY FORUM

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005

info@fpf.org | FPF.ORG