Business Benefits of Investing in Data Privacy Management Programs

January 2023

Contents

I. Foreward

Bojana Bellamy

President, Centre for Information Policy Leadership

Two years ago, CIPL embarked on a data privacy accountability mapping project to understand how 17 leading organizations embedded data privacy accountability into their corporate DNA and what effective and accountable privacy management programs look like. That project raised a new question for us at CIPL – how could we help drive organizations to embrace accountability, that is the key to digital transformation and, ultimately, success in our modern economy and society? This question inspired us to pull the curtain back and explore with CIPL member companies the wide range of tangible business benefits that organizations are experiencing from investing time, money, effort and other resources into building their privacy programs. Now, more than ever, with the increasing privacy and security expectations of regulators, business partners, consumers and investors, it is critical that every organization understand the real value and ROI of accountability for the business bottom line and for long-term sustainability and trust. I am delighted to have partnered with the privacy team at Cisco on this new report that provides insights into how several leading global companies realize value from privacy management programs. I hope that it inspires other organizations to implement accountability to address the data challenges, but also to enable business growth, trust and data-driven innovation.

Harvey Jang

Vice President, Deputy General Counsel & Chief Privacy Officer Cisco Systems, Inc.

It's been over 10 years since I first started working with CIPL and advocating for privacy to be respected as a fundamental human right and managed as a business imperative. Privacy is core to trust and provides a competitive advantage for those who get it right. As privacy professionals, we've known this all along, but "it's not what you know, it's what you can prove." I'm excited about this report as it provides some "proof" and demonstration of positive ROI for investing in privacy programs – much more than compliance and risk avoidance. We hope you find this report useful in support of building and operationalizing privacy in your own organizations. We'll continue to research, measure, and develop additional quantitative evidence in our future studies and reports.

II. Executive Summary

Organizations increasingly recognize that accountability through the implementation of a data privacy management program (DPMP) is essential to operate effectively in the modern digital economy. For many years, the focus of organizations in implementing a DPMP has been mainly to achieve compliance with data protection requirements. Today, many organizations have undergone a shift in understanding and realize that a DPMP is as critical for risk management and compliance as it is for enabling data strategy, building customer trust, winning business, and attracting company investment.

This study by the Centre for Information Policy Leadership (CIPL) and the Privacy Center of Excellence at Cisco explores the business benefits and return on investment (ROI) of DPMPs. In particular, the study demonstrates that organizations are experiencing a wide range of benefits from investing in DPMPs. These include risk management and compliance benefits, as well as positive benefits to use and leverage data more effectively and confidently for responsible innovation. It also demonstrates that investing in a DPMP can give confidence to external stakeholders, including customers, data subjects/users, investors, business partners, and regulators. Moreover, this study highlights that by investing in the elements of accountability, including via the use of a privacy maturity model, organizations can potentially experience substantial financial benefits. Organizations are starting to communicate these benefits to senior leadership and the board, but would like to better understand how to utilize privacy metrics to measure the effectiveness of their privacy programs.

Note that while this report focuses on the specific business benefits that organizations have experienced as a result of investing in DPMPs, such benefits correlate with benefits for a wide range of stakeholders in the data ecosystem, including consumers, regulators, and investors.

Key findings of this study at a glance

- While legal, compliance, and data security concerns have served as traditional drivers for the implementation of DPMPs, there is increasing recognition that accountability through a DPMP can also enable broader innovative uses of data, serve as a competitive edge, and boost trust and confidence in the business as a responsible user of data.

- Risk and compliance benefits, such as avoiding regulatory scrutiny and fines, experiencing fewer breaches, and avoiding damage to reputation, are the most significant benefits experienced by organizations that implement a DPMP. However, there is an increasing trend of organizations experiencing other tangible benefits, including greater agility and innovation, operational efficiency, and making the organization more attractive to investors.

- Over half of CIPL members who participated in this study[1] experienced at least $1 million in benefit from investing in privacy over the past year. Twenty-eight percent experienced over $10 million in benefit.

[1] Throughout this report, any reference to CIPL members refers to the 36 organizations that participated in this study. This represents approximately 45% of CIPL's total membership.

- CIPL members had an average score of 4.13 out of 5 with respect to implementing the seven elements of organizational accountability. The most mature areas of implementation to date are (a) ensuring appropriate leadership and oversight for privacy, (b) putting in place policies and procedures, and (c) ensuring appropriate response and internal enforcement for the DPMP.

- The majority of organizations are using some form of a privacy maturity model to implement accountability, including the CIPL Accountability Framework, ISO standards, Generally Accepted Privacy Principles, and the NIST Privacy Framework, among others.

- Discussions about privacy and how the DPMP is positively impacting the organization will be an increasing area of focus for corporate leadership, including at the board level, in the years ahead. There is great interest and need to understand and build privacy metrics to quantify the value DPMPs bring to their organization.

III. Methodology and Research Questions

In January 2021, CIPL and Cisco launched a survey to measure and understand the business benefits of investing in organizational accountability by implementing DPMPs. The objective of the survey was to:

- Gather a big-picture overview of the many wide-ranging benefits that leading organizations are experiencing as a result of creating and implementing a DPMP.

- Understand how organizational approaches to using data have changed as a result of investing in a DPMP.

- Gain insight into how organizations are communicating about their DPMPs with their corporate leadership and board of directors.

- Inform this report to enable organizations to benchmark the benefits they have reaped to date from their DPMP against their industry peers.

The survey ran from January to March 2021 among CIPL member organizations.[2] A second round of the survey ran from January to February 2022 to give organizations that joined CIPL after March 2021 an opportunity to respond. Approximately 45% of CIPL members (36 organizations) participated in the study. The survey consisted of 12 questions. The full survey is attached as an appendix to this report (see Appendix A). All survey responses were anonymous. However, participants were offered the opportunity to identify themselves for a follow-up interview with CIPL. Of the 36 participants, 14 participated in a follow-up interview with CIPL to elaborate on their responses and provide more quantitative, qualitative, and nuanced data inputs.

[2] https://www.informationpolicycentre.com/membership.html.

The survey aimed to answer the following research questions:

- What are the top business benefits that organizations are experiencing from implementing a DPMP?
- How do organizations experiencing such benefits measure against the seven elements of organizational accountability, based on CIPL's Accountability Framework (see Appendix B)?
- What types of privacy maturity models are organizations using to build and implement their DPMP?
- How are organizations communicating and measuring the success of their DPMP?

IV. Study Results and Key Findings

1. Impetus for Implementing a DPMP

Before examining the benefits that result from implementing a DPMP, it is important to understand what drives organizations to create a DPMP in the first place. Traditionally and historically, most organizations start building and implementing a DPMP following a change in leadership, company direction or corporate structure, or in reaction to a data breach or in anticipation of new regulation. A desire to increase operational efficiency and to promote a global, centralized, and consistent approach to data privacy and security compliance is another reason for implementing a DPMP. CIPL members highlighted the following drivers for implementing their DPMPs, both historically and currently:

Traditionally, legal compliance and data security concerns have served as historic drivers to implement a DPMP. However, organizations increasingly recognize that being accountable and having a DPMP can enable a company to use data more broadly, set an organization apart from their competitors, and boost trust and confidence with customers, business partners, investors, regulators, and the public.

- Change in leadership, company direction or corporate structure: The DPMP of many organizations often evolves organically from a change in company leadership, which introduces new perspectives into an organization and an opportunity to re-examine how the organization is using data. This is often also linked to a change in corporate ethos and direction, including the organization's digital transformation. In addition, a change in corporate structure, such as a corporate split, can result in a newly formed company mirroring and adapting an existing program to ensure continued data privacy governance and compliance.

- **Following a breach:** Many DPMP's today have been formed in response to a serious data privacy or security breach. This was either because regulators required the implementation and continuous monitoring of such a program, or due to increased concerns from senior management to rebuild trust and the external perception of the organization as a responsible data steward.

- **Introduction of new regulation:** New and increasing data privacy regulations, including the EU General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA) and Privacy Rights Act (CPRA), Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD) and China's Personal Information Protection Law (PIPL), have prompted companies to create a DPMP, or revise an existing DPMP. Organizations are increasingly becoming aware that there is no alternative but to tackle new data privacy rules proactively via a DPMP to continue to operate in the modern digital economy.

- **Shift from local/decentralized to global/centralized compliance:** Several organizations have created a DPMP out of a desire to increase operational efficiency by tackling data privacy compliance and strategy across all the entities of a corporate group. Often, companies strive to build a consistent global DPMP that can be adapted to the specificities of local compliance, where required, and that straddles across different corporate functions and business units. This enables the company to have a coherent approach to the management of personal data throughout the organization.

While legal compliance and data security concerns have served as traditional drivers to implement a DPMP, there is increasing recognition among organizations that implementing a DPMP can enable a company to use and share data more broadly, including for data-driven innovation. Implementing a DPMP can also provide a competitive advantage by boosting consumer, business partner and investor trust and confidence in the data management capabilities of the business. Importantly, a DPMP also gives regulators increased confidence that the organization is using data in a responsible way. Several CIPL member companies reported that implementing a DPMP was driven by a desire to:

- **Enable broader data use:** Some companies implement a DPMP to fully map their data flows within and outside of the business, operationalize compliance, and respond to incidents in a systematic and repeatable manner. This enables them to free more time and resources to think strategically about how to enable the company's use of data and data-driven innovation.

- **Build a sustainable and trusted business:** The increasing number of data incidents and ubiquitous media attention on data privacy has prompted some companies to implement a DPMP. They do this not only to comply with the law and to minimize the risk of a breach, but also proactively to position the business as a responsible and trusted company that customers, business partners, investors and regulators can feel confident in as it collects, uses, and shares personal data.

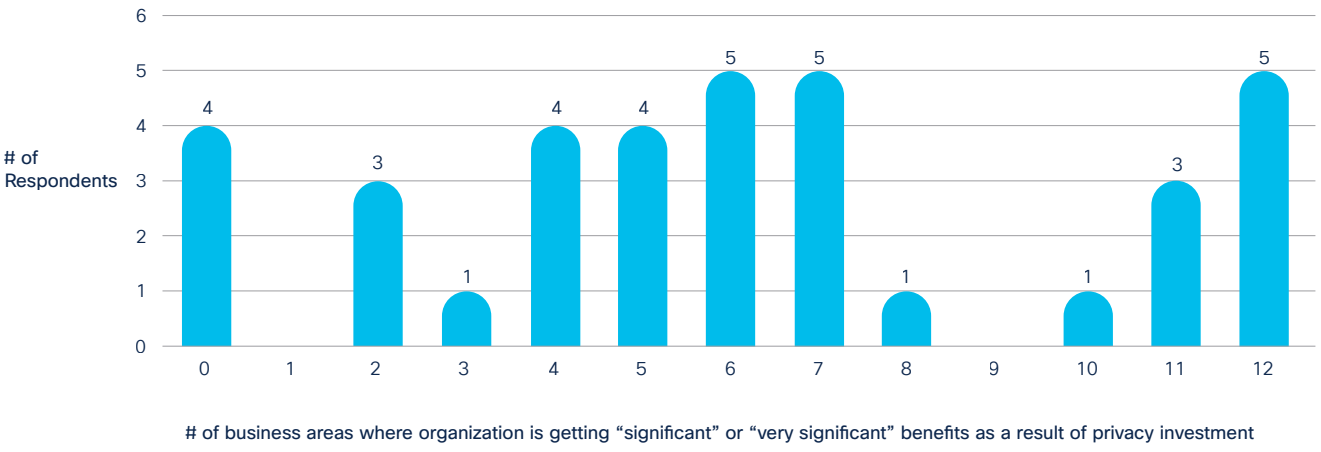
2. Benefits Experienced from Implementing a DPMP

To understand business benefits experienced from privacy-related investments, CIPL asked survey participants to report to what degree they experienced 12 distinct benefits, including "winning deals," "experiencing fewer security breaches," "avoiding damage to reputation," "enabling data innovation," and "making the company more attractive to investors."

One-quarter (25%) of participants identified 10 or more of the 12 areas where their organizations are getting "significant" or "very significant" benefits as a result of investing in privacy. Over three-quarters (78%) of all participants identified at least 4 or more areas of benefit.

There is a wide range of perceived benefits from privacy investment among CIPL member companies. One-quarter (25%) of participants identified 10 or more of the 12 areas where their organizations are getting "significant" or "very significant" benefits as a result of investing in privacy. Seventy-eight percent (78%) of participants identified at least 4 or more areas where their organization is getting "significant" or "very significant" benefits from investing in privacy. See Figure 1.

Figure 1: Range of Perceived Benefits from Privacy Investment

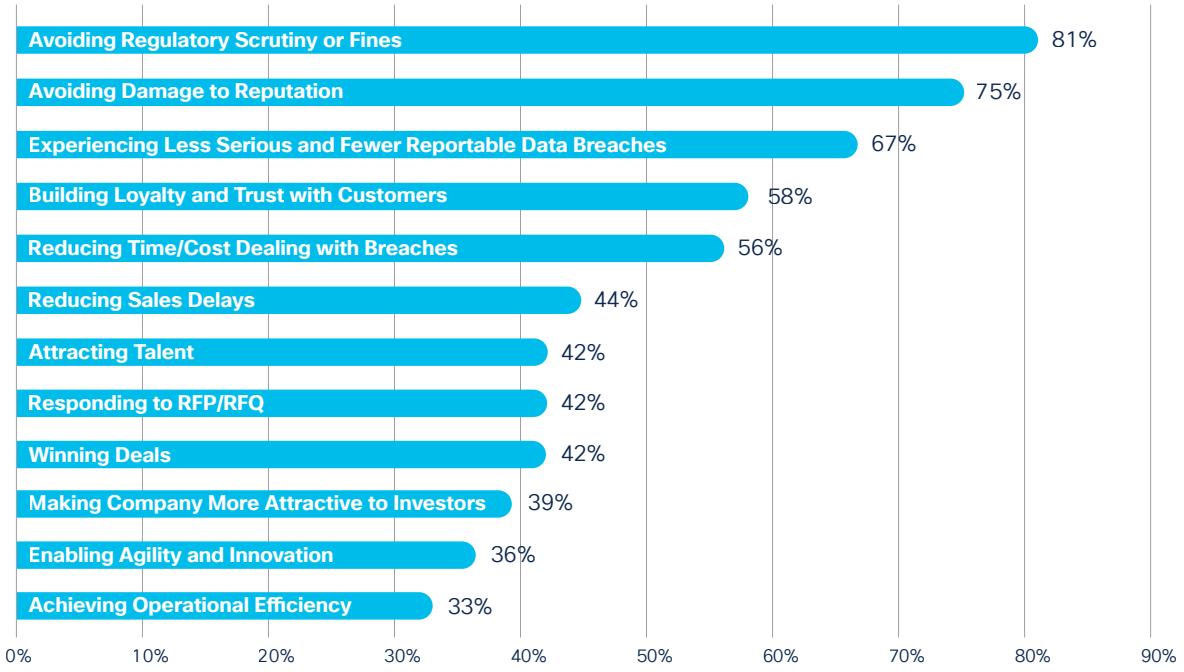


2.1 Most Significant Benefits – Risk and Compliance

CIPL members identified "avoiding regulatory scrutiny or fines" (81%), "avoiding damage to reputation" (75%), and "experiencing less serious and fewer reportable data breaches" (67%) as the top three most significant benefits experienced through their DPMPs. See Figure 2.

Risk and compliance benefits are the most significant benefits experienced by organizations implementing a DPMP. In particular, avoiding regulatory scrutiny or fines, avoiding damage to reputation and experiencing less serious and fewer reportable data breaches.

Figure 2: Percentage Identifying "Significant" or "Very Significant" Benefits from Privacy (in each area)



- Avoiding regulatory scrutiny or fines (81%): Regulatory investigations and fines for non-compliance are top issues for corporate leadership. For some CIPL members, a damaging fine can cost the organization a lot more than the actual amount of the fine. For example, fines can impact share prices, which in turn, impacts investment and confidence in the company. Fines can also serve as a red flag to potential business partners who are weary to engage with a company that was sanctioned for non-compliance with privacy and security requirements, and can also impact consumer confidence in the business and its offerings. By investing in privacy, organizations demonstrate proactive risk management, accountability, and leadership in data protection compliance. This goes a long way with regulators and can serve as a mitigating factor in enforcement and reduce the risk of significant fines and other sanctions.

- **Avoiding damage to reputation (75%):** Organizations are increasingly sensitive to the perceptions of customers, potential customers, employees, government officials, and the media, as a company's reputation is core to its success. A systematic and effective DPMP enables an organization to proactively prevent or reduce privacy- and data-related incidents that could negatively impact an organization's reputation for years. By investing in privacy, an organization demonstrates that it is thinking about data protection risks carefully and that it cares about brand perception and the trust of relevant stakeholders, including consumers and regulators. Several CIPL members reported that they have been able to enhance and preserve their reputation as ethical data stewards through participation in ethics and sustainability evaluations. For example, the Dow Jones Sustainability Indices[3] and Ethisphere[4] rank the world's most ethical companies, including on the topic of data privacy.

- **Experiencing less serious and fewer reportable data breaches (67%):** By investing in privacy, organizations are experiencing a significant reduction in the severity and number of reportable breaches. A DPMP can assist an organization in reducing the number of unnecessary systems processing personal data, reducing unnecessary access to data, and increasing the focus on data minimization, all of which improve the organization's overall security framework. Moreover, by investing in and operationalizing a DPMP, organizations are more prepared to respond quickly when an incident does occur and to manage the impact and the aftermath of a breach.

2.2 Additional Tangible Benefits – Attractiveness to Investors, Agility to Innovate, Operational Efficiency

Over one-third of CIPL members participating in the survey rated "making the company more attractive to investors," "enabling agility and innovation," and "achieving operational efficiency" as significant benefits of investing in a DPMP. While these benefits were experienced by fewer CIPL members, undoubtedly this is an upward trend, and more companies will experience benefits from implementing a DPMP beyond risk management and compliance benefits in the coming years. The results below signal a shift in perspective from viewing a DPMP as solely the cost of doing business to a business enabler that can lead to new business, generate revenue, and enable cost-savings.

Organizations report additional positive benefits from implementing a DPMP, beyond risk management and compliance – making the company more attractive to investors, enabling agility and innovation and achieving operational efficiency.

- **Making the company more attractive to investors (39%):** It is encouraging that almost two-fifths of organizations find that by investing in a DPMP, their company becomes more attractive to investors. We are seeing a trend of data privacy and security being increasingly considered in investor decisions and even being linked to Environmental, Social and Governance (ESG) investment. In recent years, we have seen the devastating consequences that can result from data security breaches and the

[3] Dow Jones Sustainability World Index, available at https://www.spglobal.com/spdji/en/indices/esg/dow-jones-sustainability-world-index/#overview.
[4] Ethisphere, available at https://ethisphere.com/.

impact on share prices. For example, Equifax's share price dropped 31% within the two weeks following its highly publicized 2017 data breach. Additionally, Marriott's share price dropped 5.6% following a data breach in 2018 and the UK privacy regulators' launch of an investigation. There also has been an increased focus on data privacy and security in the context of merger and acquisition (M&A) transactions. Investors are increasingly aware of data issues as part of investment considerations. For example, they will often consider the security posture of data-driven organizations and news media coverage of data practices of investment targets. Moreover, no shareholder will want to see their investment spent on bringing an ill-judged acquisition target into compliance after closing. In 2016, Verizon acquired Yahoo! for $350 million dollars less than it originally offered due to two separate data breaches coming to light before the transaction concluded. Yahoo! was also required to pay a $35 million penalty to settle securities fraud charges alleged by the U.S. Securities and Exchange Commission (SEC) and an additional $80 million to settle securities lawsuits brought by unhappy shareholders.

CIPL expects this trend of investor interest in data privacy to continue to grow. Some of the participating CIPL members have even reported that they are engaging in sustainability reporting and evaluations[5], setting up ESG teams within their business, actively briefing investors on data privacy, and responding to an increasing number of investors' questions. We are also seeing the rise of privacy as a board-level issue, particularly because a data breach can have catastrophic consequences on the business' bottom line and investing in a DPMP can mitigate that risk and improve the handling and response to that risk.

- **Enabling agility and innovation (36%):** Just over one-third of participating CIPL members rated "enabling agility and innovation" as a significant benefit of investing in a DPMP, as the systematic and comprehensive approach to data management enables them to unlock the potential of using data responsibly for product and service development and for data-driven innovation. We expect more organizations to experience this benefit in the future. Currently, many organizations are still preparing for the implementation of many new and upcoming privacy laws (such as the California Privacy Rights Act, and other state privacy laws in Virginia, Colorado, Connecticut, Utah, and Brazil's LGPD and China's PIPL). Moreover, some organizations are also evolving their DPMP, or leveraging it to deal with other areas of digital policy, including the responsible use of AI, data sharing, competition law, etc. In other words, organizations are continuously adapting their DPMPs to encompass new realities and often only appreciate the ability to innovate with data once the compliance groundwork has been completed.

- **Achieving operational efficiency (33%):** Just over one-third of participating CIPL members reported that investing in a DPMP has enabled them to automate their privacy workflows and tasks and facilitates more rapid responses to business queries concerning privacy. A DPMP allows organizations to define global controls and standards for use of data across the company and create consistent and timely processes (e.g., risk assessment processes to enable understanding of risk and implementation of mitigating controls). The adoption of compliance technologies also has been useful in this regard. Moreover, by investing in a DPMP, CIPL members facilitated greater collaboration between the different teams in their business, including IT, Information Security, Risk and Compliance, HR, Procurement, Contract Advisory and Solutioning teams, Business Assurance, etc., thereby initiating a more holistic approach to

[5] Id.

organizational data governance instead of the traditional and less-effective siloed approach. Given the constant stream of new data privacy requirements annually, organizations are still actively working on achieving operational efficiency internally. We expect this benefit to become more prevalent as organizations continue to operationalize the new legal requirements through their DPMP's in the coming years.

2.3 DPMP as a Positive Enabler to Use and Leverage Data Responsibly

During CIPL's follow-up interviews with several survey participants, CIPL sought to further explore how implementing a DPMP can serve as a positive enabler to use and leverage data. Even though many companies are still heavily engaged in meeting the compliance and audit objectives of their organization, CIPL found that several members are beginning to realize positive benefits from their DPMP beyond risk management and compliance.

A DPMP is a positive enabler to use and leverage data responsibly by correcting organizations' previously incorrect risk perceptions, increasing the velocity of innovation and bandwidth to think about data use in a strategic way beyond the lens of compliance. A DPMP also serves as a competitive advantage to obtain new business.

- Modified risk perception/tolerance: Investing in a DPMP can change the risk perception of an organization. The more key management and internal stakeholders are familiar with the DPMP, the more confident and competent they become with use of data in a responsible and sustainable way. They also become less risk averse as they better understand the parameters and actual risks of using data. In other words, a DPMP enables organizations to understand and use data more effectively, more responsibly, and for purposes that previously may have been considered out of scope.

- Faster pace of innovation: A DPMP can increase an organization's velocity of innovation. If a company has a robust and rigorous DPMP, it can move faster than companies that lack such a program. A DPMP provides the organization with a roadmap and drives greater consistency, standardized processes, tools, and rules to enable agility in data use and technology.

- Increased strategic bandwidth: A DPMP enables organizations to spend less time thinking about pure compliance issues and more time thinking about how they can use the data they hold to solve real problems in a responsible way. For example, using data to ensure safety, arrive at fair market pricing, and to deliver excellence and high standards of service to customers.

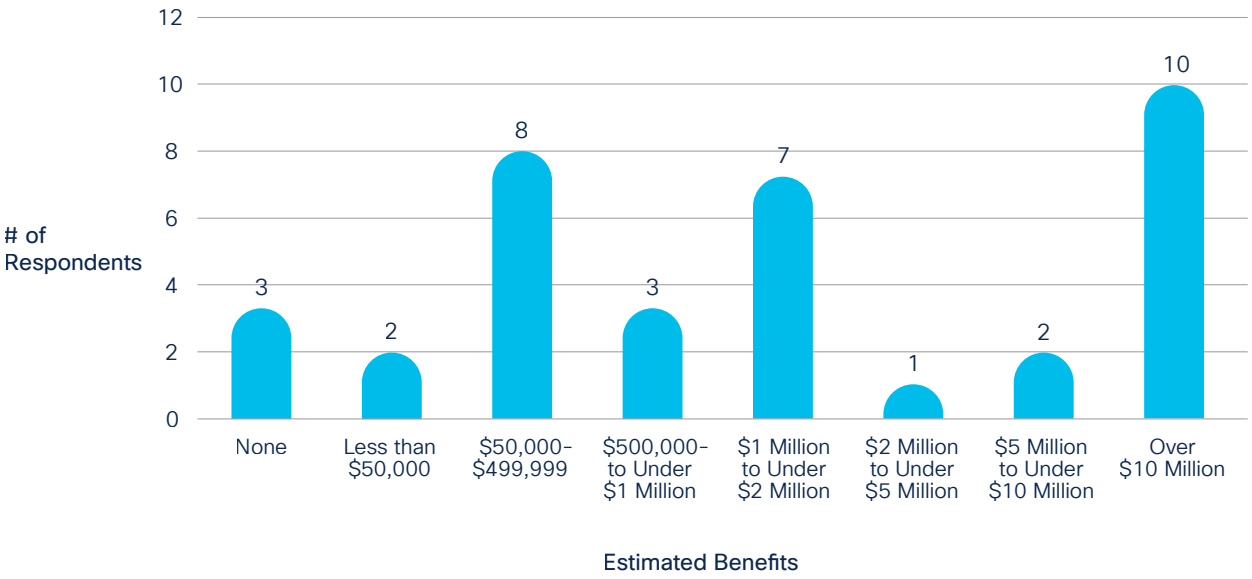
- Competitive advantage: A DPMP gives organizations an edge in attaining new business, especially organizations that are acting as business service providers and processors in B2B transactions. For example, it enables organizations to quickly respond to queries from prospective customers regarding how it addresses privacy and security concerns, including compliance with the GDPR and other key national data privacy laws. One CIPL member also

reported that had it not obtained privacy certifications,[6] it would have missed opportunities to gain a significant amount of business from its clients. Another CIPL member noted that implementing a privacy compliance program changed the company perspective entirely from one of a reactive perspective towards privacy compliance to one of treating privacy as a competitive edge. The organization views privacy as a means for the organization to become the most trusted place for consumers to provide their data because of the value they get back.

2.4 Quantifying Benefits Experienced from Privacy-related Investments

After identifying the areas of benefit experienced, CIPL asked survey participants to consider how much, in monetary terms, their organization benefited from privacy-related investments over the past year. We instructed participants to include cost savings, efficiency gains, and revenue benefits as part of this calculation. See Figure 3.

Figure 3: Quantified Privacy Benefits



[6] Data privacy certifications are not only a stamp of approval that an organization has met certain privacy requirements but can also serve as a mechanism to enable accountable privacy compliance programs.

- Fifty-six percent of CIPL members who participated in this study experienced at least $1 million in benefit from investing in privacy over the past year. Twenty-eight percent experienced over $10 million in benefit.

- Only 8% of CIPL members reported not experiencing any monetary benefit from their privacy investments. This finding does not necessarily mean monetary benefits are not occurring in these organizations as a result of investing in privacy. Some organizations have not yet collated enough data to identify and/or measure what such savings might be.

- More generally, there is additional work to be done in how organizations measure and quantify the benefit of a DPMP consistently and systematically over time. These metrics would be particularly useful for internal C-suite and Board reporting.

Clearly, investing in privacy is more than investing in improved compliance; it can have positive impact on the business' bottom line.

3. Organizational Accountability

3.1 How Organizations Rank Across the Seven Elements of Accountability

Organizational accountability is a cornerstone of modern data protection, delivering effective data privacy and protection for individuals, and driving sustainable and responsible business practices in an increasingly digital world. This study sought to understand how organizations experiencing the benefits outlined in Section 2 of this report measure against the seven elements of organizational accountability reflected in CIPL's Accountability Framework (see Appendix B). The seven elements of accountability include (i) leadership and oversight; (ii) risk assessment; (iii) policies and procedures; (iv) transparency; (v) training and awareness; (vi) monitoring and verification; and (vii) response and enforcement.

The average self-reported score of CIPL members on implementing the seven elements of accountability is 4.13 out of 5. This is significantly higher than the 3.68 average score among all companies surveyed in Cisco's 2021 Data Privacy Benchmark Study.

Many of these elements form the basis of accountable compliance programs for several other regulatory and corporate compliance areas, including anti-corruption, export control, corporate fraud and white-collar crime, anti-money laundering, and healthcare.[7] CIPL has highlighted these elements in the privacy arena for many years.[8]

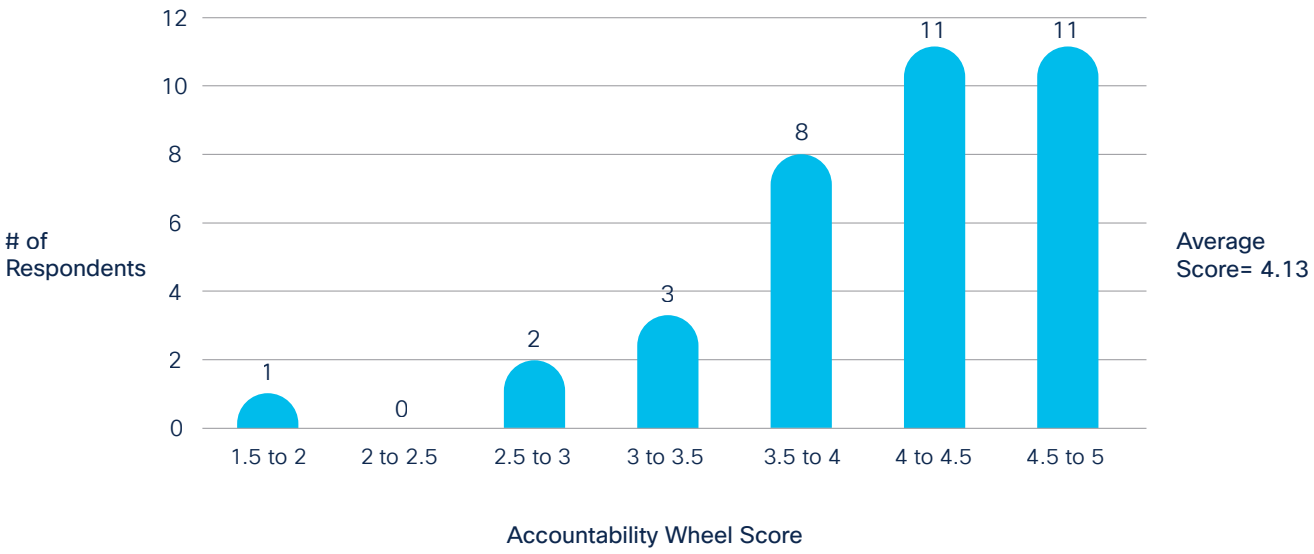
[7] See CIPL White Papers on "Organizational Accountability – Existence in US Regulatory compliance and its Relevance for a US Federal Privacy Law", 3 July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_-_existence_in_us_regulatory_compliance_and_its_relevance_for_a_federal_data_privacy_law__3_july_2019_.pdf and "Organizational Accountability - Past, Present and Future, 30 October 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organisational_accountability_%E2%80%93_past_present_and_future__30_october_2019_.pdf.

[8] See https://www.informationpolicycentre.com/organizational-accountability.html.

Survey participants were asked to rank to what extent they had implemented each of the seven elements of accountability on a 5-point Likert scale, ranging from "having little in place" on the lower end to "having a majority in place" on the higher end.

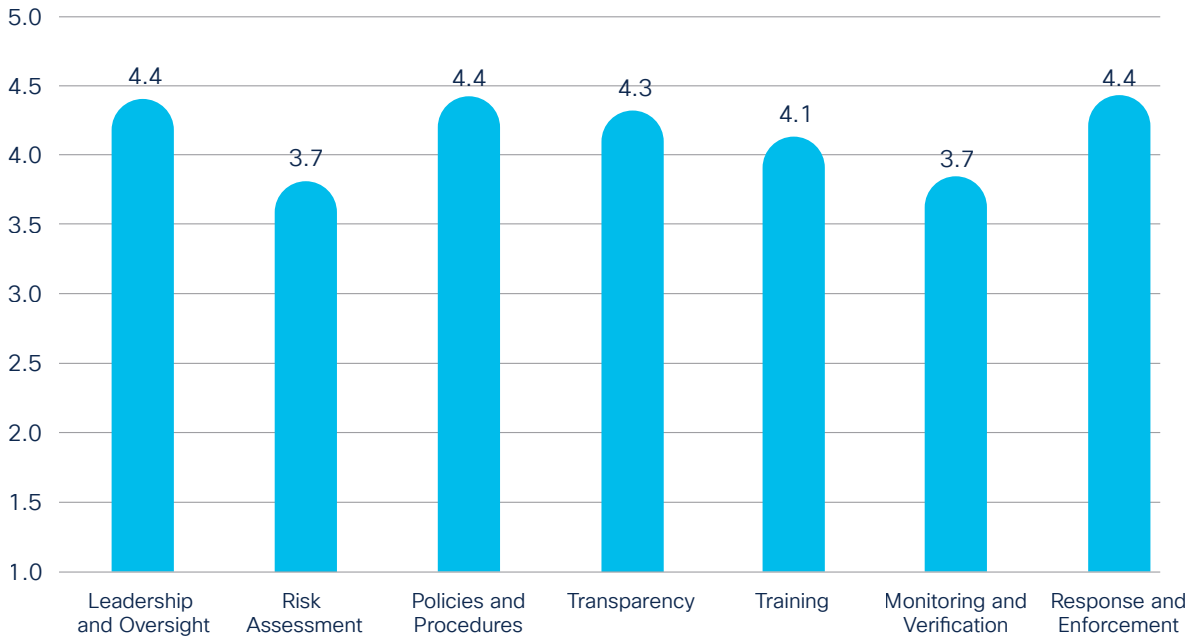
The average self-reported score on the seven elements of accountability is 4.13 out of 5. Over 60% of participating CIPL members had an average score of 4 or above.

Figure 4: Average Accountability Wheel Scores (across all 7 elements)



"Leadership and oversight," "policies and procedures," and "response and enforcement" ranked as the areas of highest implementation, each averaging 4.4 out of 5. "Risk assessment" and "monitoring and verification" ranked as the areas of lowest implementation, but were still quite high at 3.7 out of 5. See Figure 5.

Figure 5: Average Score on Accountability Wheel Elements



The average 4.13 score among participating CIPL members is significantly higher than the 3.68 average score among all companies surveyed in Cisco's 2021 Data Privacy Benchmark Study.[9] This difference may be due to the fact that Cisco's study surveys a broader spectrum of companies in many countries. CIPL member companies are, by default, a self-selecting group, consisting of some of the most sophisticated and advanced organizations that have been proactively building, implementing, and refining their DPMP for many years and embedding data privacy accountability into their corporate DNA and culture.

[9] Cisco 2021 Data Privacy Benchmark Study, available at https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf.

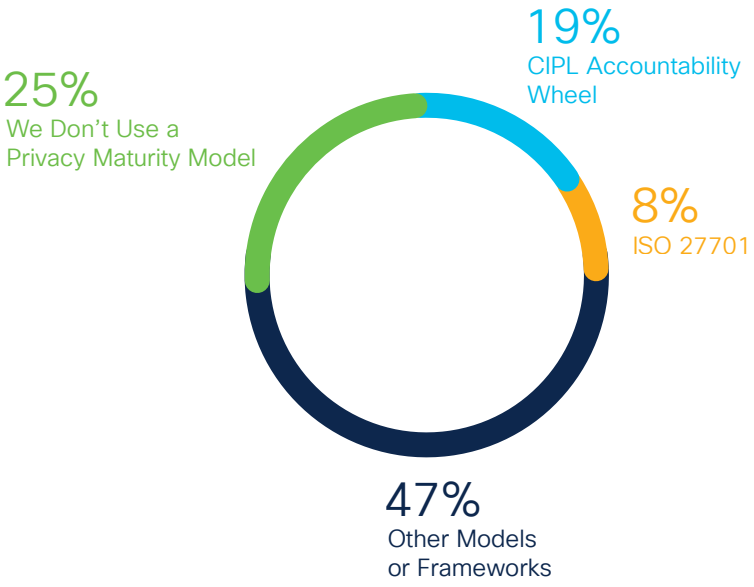
3.2 Privacy Maturity Models

There are a variety of privacy maturity models that organizations can utilize to implement accountability in a systematic and consistent way, which deliver effective accountability and enable the responsible use of data. This study sought to understand the privacy maturity models that organizations are using, if any, to experience the benefits reported from implementing a DPMP and to enable higher levels of implementation across the seven elements of accountability.

Almost one-fifth (19%) of participants reported using the CIPL Accountability Framework (see Appendix B) with over half (55%) of the participants using alternative similar models or homegrown frameworks. Alternative privacy maturity models being utilized include the American Institute of CPAs' (AICPA) Privacy Management Framework, ISO 27001, 27701 and 10012, TrustArc-Nymity integrated Privacy and Data Governance Accountability Frameworks, Generally Accepted Privacy Principles, NIST Privacy Framework, and the Canadian Accountability Model issued by Canadian Privacy Regulators in 2012.

One-quarter (25%) of participants are not using any privacy maturity model. These organizations may be achieving data privacy and security compliance through more ad-hoc processes and do not seem to be using a fixed or organized framework. Given the increasing complexity and volume of data privacy and security requirements, use of a more formal framework to organize compliance policies, procedures, and controls may be more desirable for these organizations in the long run and would more clearly demonstrate privacy accountability efforts internally and externally. See Figure 6.

Figure 6: Privacy Maturity Models



4. Communicating and Measuring the Experienced Benefits and Effectiveness of a DPMP

During CIPL's follow-up interviews with several survey participants, CIPL asked whether the participants have communicated the benefits they have experienced to senior leadership and the board, and whether these conversations have influenced any further changes to their DPMP. CIPL also asked participants to detail the types of metrics they use to measure the effectiveness of their DPMP. Measuring effectiveness of a DPMP enables organizations to understand how the DPMP is actually delivering on compliance and generating reported benefits.

CIPL expects that discussions around privacy and how the DPMP is positively impacting the business will be an increasing area of focus for corporate leadership in the years ahead, especially considering its potential to impact the business bottom line, company reputation, investment, and competitiveness in the marketplace.

4.1 Communicating the Experience Benefits and ROI of a DPMP

To date, the majority of senior management and board-level discussions concerning privacy have focused mostly on risk, legal, and compliance issues. This includes updates on the privacy program, how it has been deployed, significant data events and incidents, potential regulatory changes, resources, and budget. Nevertheless, we are beginning to see an increasing trend of organizations discussing privacy with top management in the context of a broader data strategy and how the DPMP can create value for the company itself as well as for customers. Moreover, there are increasing conversations around public trust and data use, as well as dialogues related to data and Environmental, Social, and Governance (ESG) issues emerging at the senior executive and board levels. CIPL expects that discussions around privacy and how the DPMP is positively impacting the business will be an increasing area of focus for corporate leadership in the years ahead, especially considering its potential to impact the business bottom line, company reputation, investment, competitiveness, and ultimately sustainability in the marketplace.[10] Moreover, the DPMP is likely to play an increasing role as part of an organization's mission to be purpose-driven and as it considers the impact of its data activities on wider society and social good.

[10] In 2022, CIPL launched a new project on Data-Smart Corporate Boards, which seeks to reorient corporate perceptions of data beyond the realm of risk and compliance. The project aims to elevate data as a board-level issue by highlighting data as a critical business asset.

4.2 Metrics to Measure the Effectiveness of a DPMP

To add color to discussions with senior leadership and the board, and to internally measure the effectiveness of a DPMP, CIPL members have been developing and using a variety of metrics to measure the success of their DPMP, its effectiveness in achieving the outcomes and objectives identified by the organization, and to identify areas for program improvement. By monitoring the performance of the DPMP in this way, organizations are able to provide some Key Performance Indicators (KPIs) to corporate leadership to highlight how the DPMP is actually delivering on compliance and generating reported benefits.

The types of performance metrics CIPL members have been tracking to date include:

- Number of security incidents
- Incidents by cause
- Number of data subject rights requests
- Education and training session attended, programs deployed, and materials distributed
- Number of users with reduced access to data systems
- Number of issues discovered by privacy scanning tools
- Number of vendors reviewed and cleared from a privacy standpoint
- Time saved negotiating with customers as a result of the DPMP
- Number of Privacy Impact Assessments performed
- Number of privacy reviews, escalations, and positive or negative outcomes
- Number of complaints
- Number of letters/inquiries from regulators
- Number of privacy staff
- Total privacy budget
- Number of products/services utilizing personal data
- Number of business processes using consumer vs. employee data

Several participants reported that there is still more work to be done to determine the right KPIs to measure the performance and effectiveness of their DPMPs and to benchmark against the efforts of their industry peers. CIPL intends to conduct further benchmarking work on privacy metrics in the future. We also believe there is scope for organizations to further explore methods of quantifying, in monetary terms, the value and ROI that a DPMP brings to an organization, in addition to cost savings as a result of avoiding data breaches, privacy litigation, etc.

V. Appendix A: Survey Questions

CIPL Survey on Business Benefits of Privacy Programs

Thank you for participating in this CIPL survey. It should take you less than 10 minutes to complete.

Implementing and investing in a privacy management program can bring significant business benefits to organizations, their customers and shareholders. The Centre for Information Policy Leadership (CIPL) is undertaking research into the specific benefits that organizations are experiencing as a result of efforts to implement a data privacy management program into their business. The aggregate results will be shared with the CIPL membership and other participants in the form of a white paper on the topic. This survey is being conducted in partnership with the Privacy Center of Excellence team.

We will use the information that you provide for the purpose of writing the white paper and to contact you in the event you would be interested in having a follow-up call with CIPL about your responses. Unless you provide contact information for a follow-up interview, your response will be anonymous.

If you have any questions about this survey please contact Michelle Marcoot at mmarcoot@HuntonAK.com.

Question 1: Is your organization a member of the Centre for Information Policy Leadership (CIPL)?

- Yes
- No

Question 2: How much would you estimate your organization spends overall on its privacy management program and compliance (internal and external spend)?

Note that you should not include security spending in your estimate. This would likely be your overall budget for privacy, and may include costs of staff, tools, internal and external counsel, consultants, etc.

- Up to $250,000
- $250,000 to $499,999
- $500,000 to under $1 Million
- $1 Million to under $2 Million
- $2 Million to under $5 Million
- Over $5 Million (Please specify how much _____)

Question 3: What is the budget of your organization's privacy office specifically (excluding headcount)? Please select only one answer.

- Up to $100,000
- $100,000 to $249,999
- $250,000 to $499,999
- $500,000 to $999,999
- Over $1,000,000 (Please specify how much _____)

Question 4: For the purposes of the previous question, what types of expenses do you include in the privacy office budget?

(Please specify_____)

Question 5: To what extent are the following statements true about your organization's data privacy program? Please select only one answer in each row.

We have established Leadership & Oversight for data protection and privacy, including buy-in and support from management (e.g., privacy team in place, regular reporting to management and the Board)	We have little in place (roughly 0-20% complete) We are working on it and have made some progress (roughly 20-40% complete) We have made significant progress, but we still have a significant way to go (roughly 40-60% complete) We have a majority of this in place (roughly 60-80% complete) We have all or nearly all in place and are continuously improving (roughly 80-100% complete)
We have implemented controls to identify and manage privacy risks (e.g., weighing risks of using information, periodic reviews of privacy program, adapting the program to changing levels of risk)	We have little in place (roughly 0-20% complete) We are working on it and have made some progress (roughly 20-40% complete) We have made significant progress, but we still have a significant way to go (roughly 40-60% complete) We have a majority of this in place (roughly 60-80% complete) We have all or nearly all in place and are continuously improving (roughly 80-100% complete)

We maintain written privacy policies and procedures aligned to legal requirements and industry best practices (e.g., concrete processes and controls that are followed by the organization)	We have little in place (roughly 0-20% complete) We are working on it and have made some progress (roughly 20-40% complete) We have made significant progress, but we still have a significant way to go (roughly 40-60% complete) We have a majority of this in place (roughly 60-80% complete) We have all or nearly all in place and are continuously improving (roughly 80-100% complete)
We are transparent about our privacy practices (e.g., published information about rights of individuals with respect to their data, easily accessible dashboards and portals)	We have little in place (roughly 0-20% complete) We are working on it and have made some progress (roughly 20-40% complete) We have made significant progress, but we still have a significant way to go (roughly 40-60% complete) We have a majority of this in place (roughly 60-80% complete) We have all or nearly all in place and are continuously improving (roughly 80-100% complete)
We provide ongoing privacy training to personnel responsible for handling personal data (e.g., data privacy is embedded in the culture of the organization and is a shared responsibility)	We have little in place (roughly 0-20% complete) We are working on it and have made some progress (roughly 20-40% complete) We have made significant progress, but we still have a significant way to go (roughly 40-60% complete) We have a majority of this in place (roughly 60-80% complete) We have all or nearly all in place and are continuously improving (roughly 80-100% complete)
We regularly monitor internal compliance with our privacy program, policies and procedures (e.g., regular internal and external audits and improvement plans)	We have little in place (roughly 0-20% complete) We are working on it and have made some progress (roughly 20-40% complete) We have made significant progress, but we still have a significant way to go (roughly 40-60% complete) We have a majority of this in place (roughly 60-80% complete) We have all or nearly all in place and are continuously improving (roughly 80-100% complete)

We have implemented effective response and enforcement procedures (e.g., for responding to inquiries, complaints, data breaches, and internal non-compliance)	We have little in place (roughly 0-20% complete) We are working on it and have made some progress (roughly 20-40% complete) We have made significant progress, but we still have a significant way to go (roughly 40-60% complete) We have a majority of this in place (roughly 60-80% complete) We have all or nearly all in place and are continuously improving (roughly 80-100% complete)

Question 6: How much has your organization experienced the following benefits as a result of your privacy-related investments?

Please select only one answer in each row.

Avoiding damage to reputation	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Enabling data agility and innovation	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Enabling our organization to win deals we otherwise would not have won	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit

Achieving operational efficiency	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Reducing any sales delays due to privacy concerns from customers/ prospects	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Avoiding regulatory scrutiny or fines	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Reducing the time and the cost of dealing with data breaches	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Building loyalty and trust with our consumers and/or business customers	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit

Attracting and retaining talent for our organization	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Helping to differentiate our organization and better respond to Requests for Proposal (RFP) and Requests for Quote (RFQ) from business clients and customers	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Experiencing less serious and fewer reportable data security breaches	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit
Making our company more attractive to investors	No benefit Minor benefit Moderate benefit Significant benefit Very significant benefit

Question 7: From the selections you have made in the previous question, please rate what you consider to be the three most significant areas of benefit. Please rank up to three by clicking on the choices in order of your preference.

Question 8: For your responses in the previous question, please tell us more about how your privacy program helped you to experience these benefits, with reference to any particular quantitative and/or qualitative examples.

Question 9: In considering the benefits from your privacy-related investments, how much (in monetary terms) would you estimate your organization benefitted over the past year? Please include cost savings, efficiency gains, as well as revenue benefits.

Please select only one answer.

- None
- Less than $50,000
- $50,000 – $499,999
- $500,000 to under $1 Million
- $1 Million to under $2 Million
- $2 Million to under $5 Million
- $5 Million to under $10 Million
- Over $10 Million

Question 10: Do you currently use a privacy maturity model or framework to organize your privacy management program? Please select only one answer.

- CIPL Accountability Wheel
- ISO 27701
- Other (Please specify)
- We don't use a privacy maturity model

Question 11: What 1-2 benefits would be most helpful for you to have, that you don't yet have today (perhaps due to the inability to measure, investment needed, etc.)?

_____

_____

Question 12: Would you be willing to have a short follow up call with CIPL to discuss your responses?

Please select only one answer.

- Yes (Please provide your name, organization, title and email address. A CIPL representative will be in touch with you).
- No

VI. Appendix B: CIPL Accountability Framework

Figure 7: CIPL Accountability Framework – Universal Elements of Accountability

VII. About the Centre for Information Policy Leadership

CIPL is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/.

VIII. About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more on The Newsroom and follow us on Twitter.