Study:

Assessing and Mitigating Privacy Risk Starts at the Top
Privacy is about more than simply complying with the law. From the Information Accountability Foundation, which works with regulators around the globe, to the Direct Marketing Association’s Code of Practice, to white papers issued by law firms working in the field of privacy, the leading voices in the field of information privacy are counseling that good data governance is more than making sure your company doesn’t break the law.

Rather, organizations are now seeing privacy as a risk factor, alongside any number of other factors, that they must consider as they approach the marketplace. As they develop and issue new products and services that collect data or use data, they must consider not just whether what they are doing is legal, but also whether what they are doing might lead to an adverse reaction down the road.

Will the data they’re collecting increase the risk of a data breach? Will this product “creep people out” and lead to reputational or brand damage? Will a regulator take notice and decide what they are doing is unfair or deceptive?

Further, as these risks are identified, what are the pieces that organizations must put in place if they hope to mitigate them? Is it a simple matter of dedicating resources to the privacy team? Staffing up?

The answers we found may surprise you.

Overall, it would seem the first step is simply making the effort. Almost universally, privacy professionals expressed the need for leadership buy-in and engagement. In fact, in smaller firms, the CEO is involved in privacy risk assessment nearly a third of the time. Clearly, privacy is rising to the very top levels of organizational priorities as high-level breaches hit the front pages of the world’s newspapers.

We’ve also found a wide range of investments in risk-mitigating products and services, with relatively low median spends of $30k annually overall, but outlying organizations that are spending many millions a year on services like external privacy counsel, privacy consultancy and IT security services.

The average spend is just under half a million dollars annually for organizations of all shapes and sizes, and that figure doesn’t budge much depending on the size of the organization when we drill down. However, the median spend progresses as you might predict with company size, from just $10k annually in small companies to $100k annually in large corporations.

One other interesting note bubbled up: Privacy programs of all stripes place an emphasis on knowledge of industry events and trends. Let this report be well received in that vein.
The two biggest risks with which organizations concern themselves are both intimately linked and entirely separate in characterization. For companies the world over, the two biggest concerns are a Negative Impact on Brand and Reputation (59 percent very concerned) and a Data Breach (53 percent very concerned).

Clearly, the latter can lead to the former, but in assessing risk, they offer very different challenges. Preventing a data breach means dedicating resources to making sure a discrete action doesn’t happen. Preventing damage to brand and reputation? That can mean preventing a discrete action or it can mean preventing a long-standing and pervasive perception on the part of the marketplace that your organization doesn’t take consumer privacy seriously.

Clearly, mitigating that requires more than just making sure a bad thing doesn’t happen.

Regardless, these two risks are consistently the biggest perceived risks, no matter size or location.

We asked our 347 respondents, all internal privacy professionals, to rate a list of perceived risks on a scale of 1 to 5, with 1 representing zero concern whatsoever, and 5 saying they are very concerned.

We also, for the purposes of this report, asked respondents to identify the size (by number of employees) and location of their companies. We then broke them out by small (< 5,000 employees), medium (5,001 - 25,000 employees) and large (25,000+ employees) to see how risk assessment and mitigation might change as companies grew.
We also broke companies out by whether they are headquartered inside the United States, with its sectorial approach to privacy regulation, or outside the United States, where those working in the field of privacy are generally regulated by omnibus privacy laws, such as those in the EU and Canada.

In the case of identifying risks, we see little differentiation. Brand Impact and Data Breach remain the biggest concerns. However, we see that data breach is a much smaller concern outside of the United States. Within the U.S., larger corporations are much more likely to be concerned than smaller ones about possible class action lawsuits and enforcement actions by regulators.

Those selecting the top box:

- **US:**
  - Brand Impact: 61%
  - Data Breach: 58%
- **Non-US:**
  - Brand Impact: 52%
  - Data Breach: 39%

**Small:**
- Brand Impact: 56%
- Data Breach: 49%

**Medium:**
- Brand Impact: 62%
- Data Breach: 61%

**Large:**
- Brand Impact: 60%
- Data Breach: 53%
- Enforcement Action by Regulator: 26%

**TAKEAWAYS:**

1. The size of the company has little impact on how organizations perceive risk.
2. However, we do see differences between US-based and Non-US companies. Those outside of the United States are less concerned, in general, with data breaches. In fact, just 39 percent of privacy professionals outside the United States listed themselves as very concerned about a data breach.

**Let’s Talk Bottom Line**

So, who are those 35 percent of respondents who say they’re “very concerned” about the bottom line?

In terms of size and geography, they are almost exactly distributed as the rest of the sample, small, medium and large, U.S. and non-U.S.

But does this prioritization of bottom line affect their behavior? According to their self reports, yes.

Across the board, those who pronounced themselves very concerned about bottom line impact were about 10 percent more likely to rate themselves either a 4 or 5 in how their organizations perform on the important factors for mitigating risk. They rated themselves especially higher for their Corporate Training (52 percent vs. 38 percent), Interdepartmental Communication (41 percent vs. 29 percent) and Vendor Management (42 percent vs. 30 percent).

Clearly, when the bottom line is emphasized, the corporation takes notice. In these companies, the CEO is involved in risk assessment 33 percent of the time, vs. 20 percent overall.

However, this emphasis is not reflected in increased spend on outside risk mitigation. The average spend for these firms is just $200k, and the median is $20k, a full third less than the median spend of the sample as a whole. Nor is there any significant difference in the types of services purchased.
So, we know what companies are concerned about. How do they start evaluating the impact on the organization? Not surprisingly, we again have broad consensus on what factors are linked to extreme business impact: First is the Type of Information Held by the Organization (59 percent very important); second is the Importance of that Personally Identifying Information or Personal Health Information to Business Objectives (39 percent very important), with the Enforcement History of the Regulator coming in third at 28 percent very important.

This may be obvious on its face. If the organization does not collect sensitive information in the first place, there’s less privacy risk. Similarly, if that information is not vital to business objectives, it’s unlikely to be a big concern if that data is compromised in some way.

However, there is a lesson there: Don’t collect information or store information your organization doesn’t need. If the data represents the risk, organizations would be smart to avoid that risk if that data doesn’t also represent significant opportunity.

When looking at our breakout sections, these rankings hold relatively true. Further, as part of this survey we asked outside counsel what factors they thought were most important in evaluating risk to the organization, and their answers lined up nearly identically to those of these inside privacy professionals. While the sample size of these external counsel was not large enough from which to draw significant conclusions, the data does support the validity of our findings overall.
### Highest Overall Perceived Risk Factors:

(as ranked by those selecting top two boxes)

**US:**
- Type of Information - 88%
- Importance of PII to the Business - 81%
- Adverse Experience - 67%
- Enforcement History - 66%

**Non-US:**
- Type of Information - 78%
- Importance of PII to the Business - 71%
- Adverse Experience - 58%
- Enforcement History - 56%

**Small:**
- Type of Information - 82%
- Importance of PII to the Business - 78%
- Adverse Experience - 67%
- Enforcement History - 54%

**Medium:**
- Type of Information - 88%
- Importance of PII to the Business - 75%
- Enforce History - 67%
- Adverse Experience - 67%

**Large:**
- Type of Information - 86%
- Importance of PII to the Business - 81%
- Enforcement History - 71%
- Adverse Experience - 61%

### Takeaways:

1. Small companies are clearly much less worried about enforcement. As companies look to get off the ground in start-up mode, it may be they are more focused on brand and reputation, relatively speaking to enforcement, as they may consider themselves still “under the radar.”

2. Non U.S. companies are less concerned in general about the type of information held and its importance to objectives, which may reflect a deeper history with the handling of sensitive data.
Overall, privacy professionals take two tacks in mitigating risk. First, they emphasize Leadership Buy-In above all else. Trying to mitigate risk is pointless, it would seem, if it is not identified as a priority from the top.

However, second most prominent on privacy professionals’ minds is the technical solution: IT team’s security resources and capabilities paired with their ability to detect incidents.

Combine these with Corporate Training and Education and you get a picture of risk mitigation that places importance on acknowledging the importance of the problem and getting the organization as a whole up to speed.

These four factors are all rated by 80 percent of respondents as important or very important.

The second tier in terms of importance (still rated as important by more than two-thirds) includes Maturity of Program, Vendor Management, Knowledge of Other Incidents and Threats in the Industry, and Data Inventory Program. This isn’t surprising, given how many high-profile breaches involve a third-party vendor and given the importance placed on knowing what type of data is held by the corporation.

It is perhaps surprising that neither the budget or size of the privacy team ranked particularly high, nor did a relationship with regulators. Rather, it was the maturity of the privacy program that was identified as particularly important. Still, in the third tier in importance, but still deemed important by a majority surveyed is Budget of Privacy Team, Physical Location of Data Holdings, Employee Monitoring and Interdepartmental Communications.

At the bottom of priorities is Cyberinsurance, which is clearly not seen as highly important for privacy risk mitigation. As we will see later, however, it is a common spend by companies spending to mitigate risk. Because it is one of the “simpler” things that companies can do to approach risk, it may be commonly used but not particularly highly valued. Also in the bottom tier—and deemed important by less than half of those surveyed—is Size of Privacy Team and Relationship with Regulators.
The importance rankings are very consistent across all sub-groups.

<table>
<thead>
<tr>
<th>BASE SIZE</th>
<th>OVERALL</th>
<th>US</th>
<th>NON US</th>
<th>LARGE</th>
<th>MEDIUM</th>
<th>SMALL</th>
<th>US SM TO MED</th>
<th>US LARGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
</tr>
<tr>
<td>Leadership Buy In</td>
<td>89%</td>
<td>91%</td>
<td>84%</td>
<td>92%</td>
<td>91%</td>
<td>85%</td>
<td>88%</td>
<td>96%</td>
</tr>
<tr>
<td>Corporate Training and Education</td>
<td>86%</td>
<td>86%</td>
<td>85%</td>
<td>88%</td>
<td>91%</td>
<td>81%</td>
<td>83%</td>
<td>90%</td>
</tr>
<tr>
<td>IT Resources</td>
<td>86%</td>
<td>87%</td>
<td>85%</td>
<td>86%</td>
<td>89%</td>
<td>86%</td>
<td>88%</td>
<td>87%</td>
</tr>
<tr>
<td>IT Ability</td>
<td>84%</td>
<td>86%</td>
<td>80%</td>
<td>85%</td>
<td>81%</td>
<td>85%</td>
<td>86%</td>
<td>87%</td>
</tr>
<tr>
<td>Maturity of Program</td>
<td>74%</td>
<td>75%</td>
<td>71%</td>
<td>84%</td>
<td>72%</td>
<td>64%</td>
<td>66%</td>
<td>87%</td>
</tr>
<tr>
<td>Vendor Management</td>
<td>73%</td>
<td>77%</td>
<td>63%</td>
<td>78%</td>
<td>80%</td>
<td>65%</td>
<td>74%</td>
<td>81%</td>
</tr>
<tr>
<td>Knowledge of Other Incidents &amp; Threats in Industry</td>
<td>68%</td>
<td>70%</td>
<td>65%</td>
<td>65%</td>
<td>64%</td>
<td>73%</td>
<td>72%</td>
<td>68%</td>
</tr>
<tr>
<td>Data Inventory Program</td>
<td>67%</td>
<td>69%</td>
<td>61%</td>
<td>69%</td>
<td>69%</td>
<td>65%</td>
<td>69%</td>
<td>70%</td>
</tr>
<tr>
<td>Budget of Privacy Team</td>
<td>56%</td>
<td>60%</td>
<td>45%</td>
<td>60%</td>
<td>58%</td>
<td>51%</td>
<td>58%</td>
<td>64%</td>
</tr>
<tr>
<td>Physical Location of Data Holdings</td>
<td>56%</td>
<td>57%</td>
<td>53%</td>
<td>57%</td>
<td>47%</td>
<td>58%</td>
<td>54%</td>
<td>60%</td>
</tr>
<tr>
<td>Employee Monitoring</td>
<td>55%</td>
<td>56%</td>
<td>53%</td>
<td>54%</td>
<td>55%</td>
<td>56%</td>
<td>55%</td>
<td>57%</td>
</tr>
<tr>
<td>Interdepartmental Communication</td>
<td>53%</td>
<td>55%</td>
<td>49%</td>
<td>53%</td>
<td>45%</td>
<td>56%</td>
<td>55%</td>
<td>54%</td>
</tr>
<tr>
<td>Size of Privacy Team</td>
<td>44%</td>
<td>46%</td>
<td>39%</td>
<td>56%</td>
<td>47%</td>
<td>29%</td>
<td>36%</td>
<td>59%</td>
</tr>
<tr>
<td>Relationship with Regulators</td>
<td>42%</td>
<td>41%</td>
<td>42%</td>
<td>52%</td>
<td>25%</td>
<td>37%</td>
<td>30%</td>
<td>55%</td>
</tr>
<tr>
<td>Cyberinsurance</td>
<td>35%</td>
<td>37%</td>
<td>30%</td>
<td>32%</td>
<td>36%</td>
<td>38%</td>
<td>40%</td>
<td>34%</td>
</tr>
</tbody>
</table>
### Importance to Mitigating Privacy Risk:

*(ranked by combo of top two boxes)*

<table>
<thead>
<tr>
<th>Overall:</th>
<th>US:</th>
<th>Non-US:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership Buy-In</td>
<td>Leadership Buy-In</td>
<td>Leadership buy-in - 84%</td>
</tr>
<tr>
<td>IT Resources</td>
<td>IT Resources - 87%</td>
<td>IT Resources - 85%</td>
</tr>
<tr>
<td>Corporate Training and Education</td>
<td>Corporate Training &amp; Education - 85%</td>
<td>Corporate Training and Education - 85%</td>
</tr>
<tr>
<td>IT Ability</td>
<td>IT Ability - 85%</td>
<td>IT Ability - 80%</td>
</tr>
<tr>
<td>Vendor Management</td>
<td>Vendor Management - 76%</td>
<td>Maturity of Privacy Program - 71%</td>
</tr>
<tr>
<td>Maturity of Program</td>
<td>Maturity of Program - 75%</td>
<td>Knowledge of Other Incidents and Threats in Industry - 64%</td>
</tr>
<tr>
<td>Data Inventory Program</td>
<td>Data Inventory Program - 68%</td>
<td>Data Inventory Program - 61%</td>
</tr>
<tr>
<td>Knowledge of Other Incidents</td>
<td>Knowledge of Other Incidents - 69%</td>
<td>Physical Location of Data Holdings - 53%</td>
</tr>
<tr>
<td>Budget of Privacy Team</td>
<td>Budget of Privacy Team - 59%</td>
<td>Employee Monitoring - 53%</td>
</tr>
<tr>
<td>Physical Location of Data Holdings</td>
<td>Physical Location of Data Holdings - 57%</td>
<td>Interdepartmental Comm. - 49%</td>
</tr>
<tr>
<td>Employee Monitoring</td>
<td>Employee Monitoring - 55%</td>
<td>Relationship with Regulators - 43%</td>
</tr>
<tr>
<td>Interdepartmental Communication</td>
<td>Interdepartmental Comm. - 54%</td>
<td>Budget of Privacy Team - 45%</td>
</tr>
<tr>
<td>Size of Privacy Team</td>
<td>Size of Privacy Team - 47%</td>
<td>Size of Privacy Team - 40%</td>
</tr>
<tr>
<td>Relationship with Regulators</td>
<td>Relationship with Regulators - 40%</td>
<td>Cyberinsurance - 30%</td>
</tr>
<tr>
<td>Cyberinsurance</td>
<td>Cyberinsurance - 37%</td>
<td>Cyberinsurance - 35%</td>
</tr>
</tbody>
</table>

**TAKEAWAYS:**

- Leadership Buy-In: 89%
- IT Resources: 86%
- Corporate Training and Education: 85%
- IT Ability: 84%
- Vendor Management: 73%
- Maturity of Program: 73%
- Data Inventory Program: 68%
- Knowledge of Other Incidents: 68%
- Budget of Privacy Team: 56%
- Physical Location of Data Holdings: 56%
- Employee Monitoring: 55%
- Interdepartmental Communication: 53%
- Size of Privacy Team: 44%
- Relationship with Regulators: 41%
- Cyberinsurance: 35%
1. Vendor Management is clearly seen as more of an issue in the States than outside. This may reflect the breach prevention culture that has taken root inside U.S. boardrooms following the Target breach of 2013. Following the revelation that it was an HVAC vendor who provided the entry point for malware, there has been heightened focus on vendor management.

2. Budget is seen as more of a necessity in the United States. This would seem to agree with research done by the likes of Deirdre Mulligan and Kenneth Bamberger in their 2010 paper, “Privacy on the Books and on the Ground,” and upcoming book Privacy on the Ground, showing that while the EU may have a long-standing history with privacy, the work of privacy is often done in EU firms by relatively low-level data protection officers who are under-funded and not integrated into the business as a whole. Whereas many U.S.-based global firms have privacy teams that are more strategic and well funded.

**TAKEAWAYS:**

**SMALL:**
- Leadership Buy-In - 85%
- IT Resources - 85%
- Corporate Training and Education - 81%
- IT Ability - 85%
- Vendor Management - 65%
- Maturity of Program - 64%
- Data Inventory Program - 65%
- Knowledge of Other Incidents - 74%
- Budget of Privacy Team - 52%
- Physical Location of Data Holdings - 59%
- Employee Monitoring - 56%
- Interdepartmental Communication - 56%
- Size of Privacy Team - 31%
- Relationship with Regulators - 37%
- Cyberinsurance - 39%

**MED:**
- Leadership Buy-In - 90%
- Corporate Training and Education - 91%
- IT Resources - 89%
- IT Ability - 81%
- Vendor Management - 80%
- Maturity of Program - 72%
- Data Inventory Program - 69%
- Knowledge of Other Incidents - 64%
- Budget of Privacy Team - 58%
- Employee Monitoring - 55%
- Physical Location of Data Holdings - 47%
- Interdepartmental Communication - 44%
- Size of Privacy Team - 47%
- Cyberinsurance - 36%
- Relationship with Regulators - 25%

**LARGE:**
- Leadership Buy-In - 93%
- Corporate Training and Education - 88%
- IT Resources - 86%
- IT Ability - 86%
- Vendor Management - 84%
- Maturity of Program - 78%
- Data Inventory Program - 68%
- Knowledge of Other Incidents - 66%
- Budget of Privacy Team - 59%
- Employee Monitoring - 54%
- Physical Location of Data Holdings - 57%
- Interdepartmental Communication - 54%
- Size of Privacy Team - 56%
- Cyberinsurance - 36%
- Relationship with Regulators - 52%
TAKEAWAYS:

1. Maturity of the Program clearly becomes more and more important as the size of the organization grows. The tasks become increasingly more complicated and it’s increasingly difficult to monitor everything that’s going on in the organization.

2. Similarly, Size of the Privacy Team gets increasing emphasis as organizations grow. The budget likely gets similarly increasing emphasis, though the margin of error in this study makes the trend we see here less than statistically significant.

3. Perhaps surprisingly, the expected need for Cyberinsurance goes progressively down, though it is less than statistically significant considering the sample size. Why might this be? Maybe as programs become more mature, they realize that Cyberinsurance is no kind of panacea.

4. We see a much bigger emphasis on Relationship with Regulators as companies grow, as well. This makes sense, as large companies are much more likely to have privacy-focused policy people who make a relationship with regulators their actual priorities.

5. When staying within the U.S. and looking at Large vs. a combination of Small and Medium organizations, Leadership Buy-in, Maturity of Privacy Program, Size of Privacy Team, Relationship with Regulators and Vendor Management were all significantly more likely to be deemed important by larger organizations, so these trends would seem to be more prominent inside the U.S. than outside.

---

The Curious Case of Cyberinsurance

Isn’t insurance inherently designed to mitigate risk? Why, then, do privacy professionals rate it so low in importance in our survey?

Scott Godes, a partner with Barnes & Thornberg who specializes in cyberinsurance consultation, has some ideas.

It all depends on how you view risk, he theorizes. “If you consider mitigating risk to be limited to avoiding a problem in the first place,” he said, “then many people likely don’t view cyberinsurance as a way of avoiding a problem.” Rather, he said, they may simply view it as a way of offloading the financial implications of something happening.

When you consider that damage to brand and reputation in the marketplace are seen as the big risks privacy professionals are looking to address, cyberinsurance doesn’t necessarily address that. Nor can it prevent a data breach.

“Some policies do offer you an opportunity to work with security firms as a way to make sure your security is as good as possible,” Godes said by way of caveat, “but, typically, it’s just a financial backstop.”

Further, he said, a good cyber policy should offer the opportunity to work with PR firms trained in data breach response, so that may mitigate some risk to the brand, after all. Especially if a company is savvy about its policy choices.

“Cyberinsurance differs from carrier to carrier, policy to policy,” said Godes. “The best scenario involves all of the stakeholders in the company—risk managers, in-house counsel, the privacy team and others—taking a close look at the policy and conferring so that the terms being offered are the ones best aligned with what your company needs.”
What Do They Do Well and Where Are the Gaps?

The following chart illustrates well the clear gap between where privacy professionals would like to be and where they find themselves today. While they were not reticent about placing very high rankings on the importance of a number of factors in mitigating privacy risk, they were very reluctant to rate themselves very highly at all on their organizations’ performance.

Overall, just a very few factors were rated by even a majority of respondents as either excellent or a notch below.

In fact, respondents in general rate themselves poorly on 10 of the 15 categories.
Looking specifically at those eight categories deemed most important (those where more than 60 percent of respondents selected one of the top two boxes), just four of them were even moderately rated for performance: Leadership Buy-In, IT Resources, IT Ability and Knowledge of Other Incidents and Threats in the Industry. This means for the remaining highly important categories (including Corporate Training and Education, Maturity of Program, Vendor Management and Data Inventory), we see a clear gap between desired and actual performance.

This is perhaps not surprising. Privacy remains a young field and we know that many privacy professionals started up the privacy programs they now head just a few short years ago. However, this is stark data showing the relative immaturity of the industry and its potential for growth, expansion and improvement.

Further, while Leadership Buy-in, and the IT teams, are both rated relatively highly (emphasis on relatively), Size and Budget of the Privacy Team are two of the three lowest-rated items. It’s fair to wonder how these two things can co-exist: On the one hand, privacy pros feel they do, indeed, have leadership buy-in. On the other hand, they do not appear to feel that their privacy team is appropriately resourced.

A full 37 percent of respondents rated their budget as either “totally insufficient” or just above that. While only 24 percent rated their budget as either excellent or just below that. Perhaps this is simply indicative of the natural human inclination toward wanting more resources put toward any important job, but there would appear to be reason to expect a growth in privacy investment in the short term if the leadership buy-in is as-reported.

Further, when you contrast the importance professionals place on maturity with the very mediocre way they rate themselves, there’s a clear gap there. They know they have a ways to go yet and the evidence supports them.

Finally, Vendor Management and Data Inventory would seem to be the two operational tasks that privacy programs need to focus on going forward. Understanding how data enters and exits the organization is essential to mitigating risk and not many privacy professionals are highly confident in their abilities to track data through their organizations.

Worst-performing categories:

(Percent responding in bottom two boxes)

- Size of Privacy Team - 49%
- Budget of Privacy Team - 37%
- Data Inventory Program - 36%
- Vendor Management - 31%
- Employee Monitoring - 30%
- Relationship with Regulators - 27%
- Interdepartmental Communication - 27%
In the following chart, we plot U.S. companies vs. non-U.S. companies, comparing both the level of importance they place on factors for mitigating risk and their performance on those factors:

**US vs Non US Companies:**

**Important and performing poorly**
- Corporate Training and Education
- Vendor Management
- Maturity of Program
- Data Inventory Program
- Physical Location of Data Holdings
- Size of Privacy Team
- Budget of Privacy Team
- Cyberinsurance

**Important and performing well**
- Leadership Buy-In
- IT Resources
- IT Ability
- Knowledge of Other Incidents and Threats in the Industry

**Not Important and performing poorly**
- Interdepartmental Communication
- Employee Monitoring
- Relationship with Regulators

**Moderate Importance (50%-60%)**
- Key:
  - ○ = US
  - ▢ = Non US
  - ■ = Moderate Performance and/or Moderate Importance (50%-60%)
What Do They Do Well and Where Are the Gaps?

### US Companies:

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>Non US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership Buy-In</td>
<td>91%</td>
<td>84%</td>
</tr>
<tr>
<td>Corporate Training and Education</td>
<td>86%</td>
<td>85%</td>
</tr>
<tr>
<td>IT Resources</td>
<td>87%</td>
<td>85%</td>
</tr>
<tr>
<td>IT Ability</td>
<td>86%</td>
<td>80%</td>
</tr>
<tr>
<td>Maturity of Program</td>
<td>75%</td>
<td>71%</td>
</tr>
<tr>
<td>Vendor Management</td>
<td>77%</td>
<td>63%</td>
</tr>
<tr>
<td>Knowledge of Other Incidents and Threats in Industry</td>
<td>70%</td>
<td>65%</td>
</tr>
<tr>
<td>Data Inventory Program</td>
<td>69%</td>
<td>61%</td>
</tr>
<tr>
<td>Budget of Privacy Team</td>
<td>60%</td>
<td>45%</td>
</tr>
<tr>
<td>Physical Location of Data Holdings</td>
<td>57%</td>
<td>53%</td>
</tr>
<tr>
<td>Employee Monitoring</td>
<td>56%</td>
<td>53%</td>
</tr>
<tr>
<td>Interdepartmental Communication</td>
<td>55%</td>
<td>49%</td>
</tr>
<tr>
<td>Size of Privacy Team</td>
<td>46%</td>
<td>39%</td>
</tr>
<tr>
<td>Relationship with Regulators</td>
<td>41%</td>
<td>42%</td>
</tr>
<tr>
<td>Cyberinsurance</td>
<td>37%</td>
<td>30%</td>
</tr>
</tbody>
</table>

While there are small regional differences, those differences are largely within the margin of error. What we see is further confirmation that certain issues are global: Corporate Training and Education is clearly a concern for privacy professionals, followed by Vendor Management, Maturity of Program and Data Inventory.
Where the real performance differences lie is in size of company:

(ranked by percent selecting top two boxes)

**SMALL**
- Leadership Buy-In - 53%
- Physical Location of Data Holdings - 53%
- Knowledge of Incidents - 44%
- IT Ability - 42%
- IT Resources - 41%
- Corporate Training - 36%
- Cyberinsurance - 33%
- Relationship with Regulators - 32%
- Employee Monitoring - 31%
- Vendor Management - 29%
- Maturity of Privacy Program - 27%
- Interdepartmental Communication - 27%
- Data Inventory - 26%
- Budget of Privacy Team - 20%
- Size of Privacy Team - 16%

**MED**
- Knowledge of Incidents - 50%
- IT Resources - 45%
- Leadership Buy-In - 44%
- IT Ability - 44%
- Physical Location of Data Holdings - 41%
- Corporate Training - 33%
- Maturity of Privacy Program - 33%
- Cyberinsurance - 29%
- Employee Monitoring - 28%
- Vendor Management - 25%
- Relationship with Regulators - 27%
- Data Inventory - 25%
- Interdepartmental Communication - 23%
- Budget of Privacy Team - 16%
- Size of Privacy Team - 13%

**LARGE**
- IT Resources - 66%
- IT Ability - 66%
- Knowledge of Incidents - 63%
- Leadership Buy-In - 61%
- Physical Location of Data Holdings - 56%
- Corporate Training - 43%
- Relationship with Regulators - 49%
- Cyberinsurance - 47%
- Maturity of Privacy Program - 46%
- Employee Monitoring - 41%
- Data Inventory - 35%
- Vendor Management - 34%
- Interdepartmental Communication - 32%
- Budget of Privacy Team - 30%
- Size of Privacy Team - 27%
What Do They Do Well and Where Are the Gaps?

TAKEAWAYS:

1. Larger firms, as we’ve seen in other studies, have more mature privacy programs that are better resourced. Global, multinational firms led the charge for data privacy in the early days of the late 1990s.

2. Medium-sized firms are clearly just coming around to privacy, with underfunded teams that are not particularly confident. However, these firms are likely already dealing with complex data flows, so the need for a more mature program is likely particularly striking.

3. Data Inventory and Vendor Management are clearly issues in organizations of every size and shape.

4. Corporate Training would seem to be the next most pressing issue, across the board, especially when considering the importance privacy professionals place on it for mitigating risk.

To illustrate the effects of size more starkly, we again plot importance against performance, this time contrasting small- and medium-sized companies against their larger brethren:
The larger firms separate themselves with confidence in their performance on Leadership Buy-In, IT Ability and Resources, Knowledge of Other Incidents in their Industry and the Physical Location of Data Holdings.

By contrast, small and medium companies in the United States only muster moderate performance in Leadership Buy-In and rate themselves poorly in every other category.
Who’s Evaluating Risk?

We asked participants in the survey to select all of the participants in privacy risk evaluation, allowing them to select as many choices as they’d like. What we found is that evaluating risk is most commonly a team effort, with 68 percent saying the whole privacy team is involved in evaluating risk. The next most-common participants are the General Counsel and the Chief Compliance Officer:

Significantly, roughly a third use outside counsel to help with risk evaluation, with 20 percent going all the way up to the CEO and 15 percent involving the corporate board of directors.

1. The General Counsel is clearly more involved in the privacy risk process in the United States. This may be because compliance is more difficult to discern in the U.S., where there may not be any specific law governing how data can be used. While in the EU understanding of the law may move deeper into the organization.

2. The CISO is more involved in privacy in the U.S. than outside. This may reflect what we’ve already seen is a greater emphasis on data breach prevention in the U.S. as part of the privacy program.
1. Not surprisingly, the CEO is much more likely to be involved in evaluation privacy risk at smaller companies. This may simply be a reflection of pure organizational size and the ability of a CEO at a smaller company to be more hands on in more aspects of the organization. But it may also reflect what we’ve already seen is a greater emphasis on privacy as it pertains to a smaller company’s brand and reputation.

2. As companies grow, privacy becomes a much more collaborative affair, with more voices involved in privacy risk assessment and mitigation. The most surprising part of these results may be that we don’t see a statistically significant increase in involvement by a Chief Risk Officer in the larger firms. Perhaps this means privacy hasn’t yet risen to the level of other significant risks dealt with by large corporations on a regular basis.

3. Though not statistically significant, we do see a directional trend indicating companies are more likely to rely on outside counsel as they grow. Likely, this is a function of the growing complexity that companies face as they enter more jurisdictions, but it is also likely a function of increased team size and budget and simply the ability to hire outside counsel as they grow.
This is the classic case where statistics can be deceiving. Looking simply at the mean, you’ll find the average spend by any privacy program on outside risk mitigation is $498,513.50.

However, this is greatly influenced by outliers. The median spend for all companies is just $30k.

The range here is vast. One the low end, plenty of companies reported zero spend on outside privacy risk mitigation. On the high end, more than handful of companies reported spends in the eight figures.

This would seem to reflect outside forces at work. First, those companies with sensitive data that is vital to business interests certainly have a vested interest in making sure the data is secure and well managed. While, on the other hand, companies that essentially have only employee data to manage have little incentive to spend on outside privacy mitigation services.

Second, those companies that have had an incident or those going through a process like qualifying for binding corporate rules for data transfer to and from the EU have much greater costs than your average firm.

Thus, we see that average spend by small companies is $479,098.40, nearly double the $249,779.80 average spend of medium-sized companies. Yet, if we look at median spend, we find a more predictable $15,000 spend for small companies and $25,000 for medium firms.

For large-sized companies, the average is $624,179.70, with a median of $100,000.

**TAKEAWAYS:**

1. The large portion of privacy spend on outside risk mitigation vendors is coming from U.S. headquartered firms. The average spend outside the U.S. is drastically influenced by one firm reporting a $50,000,000 annual spend, which is clearly an outlier.

2. The spend increases predictably from small to large firms when looking at the median. $100,000 remains a very small amount for a firm with 25,000+ employees ($4 per employee at the low end), however, and we should expect this to increase.
Does the CEO Influence Spend?

Want to find a subset of our respondents with an even higher mean spend on outside privacy products and services than non-U.S. corporations? Then look at those who say the CEO is involved in the risk-mitigation deliberations.

While just 21 percent said the CEO is involved, those companies represent a relatively large amount of privacy spend, with an average outlay of $983,289.

Again, however, the median spend is far lower, just $10k, which makes sense considering that small firms are much more likely to have the CEO involved and small firms have the lowest median spend.

It’s all about the outliers here: 11 of the companies with seven-figure or more spends are among this group, which is 31 percent of the total amount of seven-figure spends. In fact, much of the mean number comes from that same $50 million outlier in the mix. Back that out, and the average drops all the way under $350k.

They are also more likely to spend on IT security services. A full 54 spent on IT security last year, vs. just 42 percent of the general population. On the other hand, just 42 percent spent on outside counsel vs. 53 percent of all respondents. This mirrors the spending habits of small companies in general, however, so it may simply be a factor of most of these involved CEOs heading up small companies.

Not surprisingly, the most common spend by privacy departments is on outside privacy counsel, with 53 percent employing outside counsel. This is followed by IT Security Services (45 percent), Outside Privacy Consultants (36 percent) and Cyberinsurance (34 percent), which is the fourth most common spend, despite professionals indicating it’s relatively low in importance for risk management.

Notably, 23 percent spent funds on software for privacy risk mitigation, which may be surprising for those who think privacy pros don’t often use technological solutions.
What Are They Spending on?

TAKEAWAYS:

1. As we saw above, non-U.S. companies are less likely to spend on outside counsel. Four in 10 firms still bring in counsel for help in risk mitigation, but it’s clearly a much more common practice in the U.S. It’s interesting, however, to see that more non-U.S. companies have identified a “Breach Coach,” which is a lawyer or consultant specifically dedicated to organizing breach response. Especially considering that non-U.S. firms have expressed they are less likely to be worried about a breach in the first place, this would indicate that the idea of a breach coach is more entrenched outside of the United States.

2. Similarly, as we would expect from the way that non-U.S. firms have characterized it, Cyberinsurance is a less likely spend for non-U.S. firms.

3. IT is a priority around the globe. We see very consistent spend on IT consulting services and IT forensics services regardless of geography.

TAKEAWAYS:

1. Clearly, small firms are less likely to spend on privacy mitigation in general, including on outside privacy counsel. It is most likely that internal counsel is working on privacy risk alongside the privacy team, as we saw in the earlier data. If anyone is working on privacy risk at all, that is.

2. While not statistically significant due to sample size, we see a directional indication that the percentage of firms spending on cyberinsurance drops as the firms increase in size. As we’ve seen that privacy professionals don’t value cyberinsurance highly for risk mitigation, this may reflect that as privacy teams mature, they see cyberinsurance as less necessary or less effective for risk mitigation.

3. The highest priority for small companies is brand and reputation, but we see that, when actually spending money on outside vendors, there is a directional indication that breach prevention through appropriate security is a top priority for small firms, though the sample isn’t large enough to say this with statistical certainty. If they’re going to spend on one thing outside the building, security may be it.
How Law Firms View Risk for the Organizations They Work with

We have now seen that, even in the smallest companies, working with outside counsel is an investment that organizations are consistently making for privacy and risk-assessment services. Roughly a third of the companies surveyed involved outside counsel in assessing privacy risk at their organizations, and over half (54%) employed outside privacy counsel for privacy-risk-assessment services. On average, law firms surveyed provide nearly half of their privacy clients with either risk-assessment and/or risk-mitigation services.

So, what are outside counsel telling them, and how do they view privacy risk differently from their counterparts inside organizations? Further, how do law firms ensure that they are able to provide appropriate risk assessment and mitigation services?

In this portion of the report, we look at how law firms prioritize risk, and how those law firms organize themselves to provide valuable services to their clients.

How do their concerns align with those of internal privacy pros?

In general, external counsel sees the world relatively similarly to their internal counterparts, just looking at the percentages of responses marked “very important”:

**Law Firms:**
- Data Breach: 55%
- Brand and Reputation Negatively Affected: 55%
- Bottom Line Negatively Affected: 29%
- Enforcement Action by Regulators: 26%
- Class Action Lawsuit: 22%
- Negative Impact on Sales/Revenue: 19%

**Corporations:**
- Data Breach: 53%
- Brand and Reputation Negatively Affected: 59%
- Bottom Line Negatively Affected: 35%
- Enforcement Action by Regulators: 30%
- Class Action Lawsuit: 19%
- Negative Impact on Sales/Revenue: 34%

Those internal privacy professionals are likely more aligned with their businesses’ interest, and so it makes sense that they would pay more attention to, and be more aware of risk to, the bottom line and sales and revenue factors.
How does external counsel view factors for risk evaluation? Yet again, external counsel is in relative lockstep with inside privacy professionals, identifying the type of information held by an organization and the importance of that information to business objectives as most important to evaluating risk.

In fact, their responses are remarkably similar across the board, lending further credence to the reliability of our data.

What does external counsel believe are the most important factors for their clients as they look to mitigate risk? Mostly the same things as their potential clients. However, they are even more likely to rate Leadership Buy-In and Knowledge of Other Incidents as important. As these external counsel are likely to have worked with a number of companies on risk evaluation and mitigation, this emphasis seems instructive.

**Most Important Factors for Risk Evaluation**

*(those checking the top box, law firms listed second)*:

- Type of Information Held by Organization: 59% vs. 55%
- Importance of PII to Business Objectives: 39% vs. 36%
- Enforcement History of Regulator: 28% vs. 24%
- Adverse experience: 26% vs. 28%
- Potential Regulatory Penalties Criminal: 23% vs. 16%
- Lack of Consistency in Regulation across Jurisdictions: 22% vs. 21%
- Potential Regulatory Penalties Civil: 21% vs. 19%
- Maturity and Stability of Jurisdiction’s Privacy Regulation: 15% vs. 19%
- Previous Class Action Settlements: 10% vs. 12%
- Size and or Budget of Regulator: 6% vs. 7%

**Top Risk Mitigation Factors**

*(ranked by those answering with top two boxes, law firms listed second)*:

- IT Ability: 84% vs. 79%
- IT Resources: 86% vs. 78%
- Corporate Training and Education: 85% vs. 76%
- Leadership Buy-In: 89% vs. 74%
- Vendor Management: 73% vs. 70%
- Budget of Privacy Team: 56% vs. 64%
- Maturity of Program: 73% vs. 62%
- Data Inventory: 68% vs. 57%
- Knowledge of Other Incidents: 68% vs. 55%
- Employee Monitoring: 55% vs. 52%
- Interdepartmental Communication: 53% vs. 50%
- Physical Location of Data Holdings: 56% vs. 48%
- Cyberinsurance: 35% vs. 42%
- Size of Team: 44% vs. 38%
- Relationship with Regulators: 35% vs. 36%
Interestingly, a third of respondents (33%) said that a Relationship with Regulators was either not important at all, or just a notch above. And this aligned exactly with those responding to the small importance of the Size of the Privacy Team. If you look at the directionally indicative extra emphasis that lawyers put on privacy team budget, it might be fair wonder if external counsel is saying, “Let us handle that for you.”

What Makes a Good External Counsel?
So, what are the factors that affect whether external counsel can be effective in providing risk-assessment and mitigation services to their clients?

Quite simply, it comes down to the commitment of leadership to providing resources to the privacy team and the experience and skills of the lawyers doing the work themselves. Lawyers put relatively less emphasis on pure numbers of partners and associates, and seemed to put less stock in having In-House Expertise in Non-Legal Areas like IT or Public Relations and Number of Global Offices.

And How Do they Rate Themselves?
Law firms surveyed feel they are well equipped to provide quality privacy counsel to their clients as they rate themselves well on what they deem as most important—specifically Leadership Buy-in, Experience of Privacy-Focused Partners, Training of Privacy-Focused Lawyers and Dedicated Privacy Team.

They rate themselves moderately on Number of Privacy-Focused Lawyers, but that also received relatively low importance ratings.

Finally, they rate themselves poorly for categories deemed unimportant: In-house, Non-Legal Expertise and Number of Global Offices.

Factors for Successful Client Services

- Leadership Buy-In: 75%
- Experience of Privacy-Focused Partners: 62%
- Training of Privacy-Focused Lawyers: 60%
- Dedicated Privacy Team: 54%
- Number of Privacy-Focused Lawyers: 47%
- In-House, Non-Legal Expertise: 38%
- Number of Global Offices: 22%
How Law Firms View Risk for the Organizations They Work with

Rating 4 or 5

<table>
<thead>
<tr>
<th>Importance</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership Buy-In</td>
<td>75%</td>
</tr>
<tr>
<td>Experience of Privacy-Focused Partners</td>
<td>62%</td>
</tr>
<tr>
<td>Training of Privacy-Focused Lawyers</td>
<td>60%</td>
</tr>
<tr>
<td>Dedicated Privacy Team</td>
<td>54%</td>
</tr>
<tr>
<td>Number of Privacy-Focused Lawyers</td>
<td>47%</td>
</tr>
<tr>
<td>In-House Non-Legal Expertise</td>
<td>38%</td>
</tr>
<tr>
<td>Number of Global Offices</td>
<td>22%</td>
</tr>
</tbody>
</table>

TAKEAWAYS:

1. If anything, external counsel feels that privacy-risk-assessment and mitigation is a niche business and that it’s important to have Leadership Buy-In, counsel with experience and dedication to the privacy field. While it may be important in some areas of the law to be able to throw hours and bodies at an issue, that would not seem to be the case with privacy.

2. It seems that external counsel are confident in their ability to deliver in the categories they deem as most important.

3. There would seem to be job opportunity for lawyers looking to get into the privacy field. While external counsel doesn’t necessarily feel that pure numbers of experienced lawyers is hugely important, neither do they feel their firms are especially well staffed. Similarly, while not much stock was put in non-legal expertise, neither do firms carry much of that non-legal expertise on staff. As we see internal privacy professionals saying brand and reputation are vital above all else, and saying that IT Security and Corporate Training and Education are paramount, it would seem to make sense for law firms to bone up on these non-legal areas or to at least have on hand a suite of business partners who can be on call to provide services to their clients.