HOW IT AND INFOSEC VALUE PRIVACY

iapp | TRUSTe

EXECUTIVE SUMMARY

As a more mature field, information security has long enjoyed larger budgets and more staff than information privacy. As privacy teams have matured and grown, however, their budgets are beginning to be substantive. How do information security and privacy teams work in concert, so that their respective spends can complement one another? Are their priorities aligned? Have firms decided that information privacy investments can enhance information security? What privacy functions are valuable in mitigating a data breach?

These are some of the questions we set out to explore in a survey commissioned jointly by IAPP and TRUSTe and fielded between December 2015 and January 2016, eliciting responses from more than 550 privacy (65 percent) and IT/infosecurity professionals (35 percent).

Our study confirmed the well-documented extent of the cyber-security threat, with 39 percent of companies reporting a significant information incident in the last two years. It also confirmed that companies are increasing their infosecurity and privacy investments alike to help address this growing threat.

Fifty percent of companies have increased the involvement of privacy personnel on their infosecurity teams in the last two years. As they seek to get a better handle on their data and the extent of their corporate risk, they are employing core privacy functions with an IT bent: Forty-two percent increased investment in privacy technology, 41 percent reported both an increased use of privacy impact assessments and data inventory and classification, and 40 percent have increased the use of data retention policies.

In fact, privacy and security professionals alike agree that the most important feature of their information governance regime is communication between the privacy and security teams, many of which are now populated with staff from each discipline. Some 75 percent of IT/infosecurity professionals ranked data minimization and data inventory and mapping as the most important privacy functions in mitigating the risk of a data breach, followed by privacy policies and privacy impact assessments.

> ***"Privacy technology spending is outpacing investment in personnel, as privacy growth maps that of infosecurity over the last 10 years."***

Interestingly, privacy technology spending is outpacing investment in personnel, as privacy growth maps that of Infosecurity over the last 10 years. The study found that 42 percent had increased their spending on privacy-related technology—well ahead of spend on external counsel (34 percent) and external auditors (26 percent).

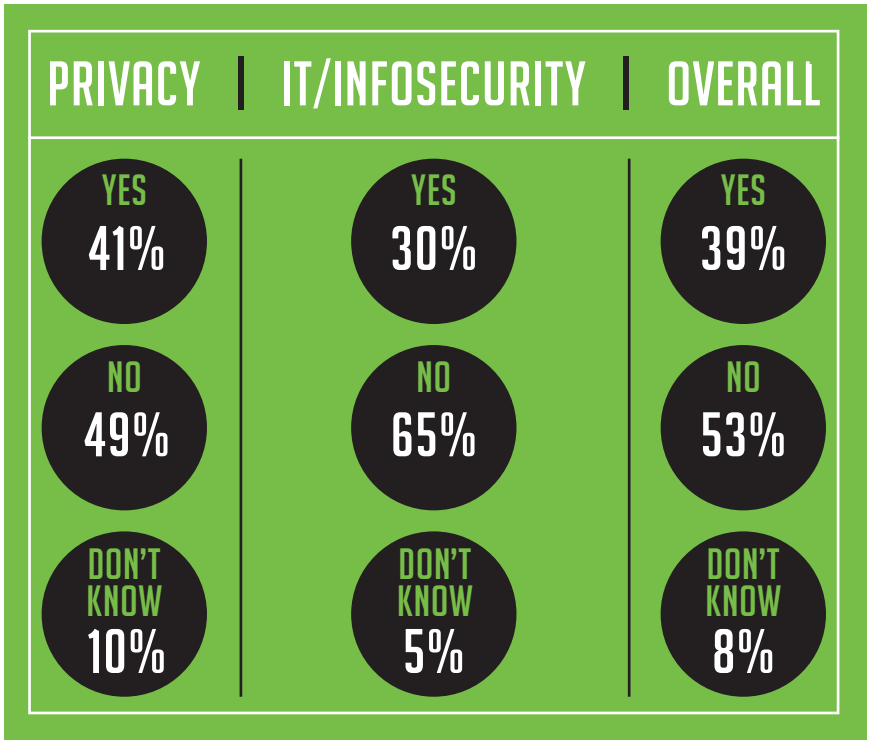
In addition, although regulatory enforcement actions are rare, firms find privacy investments highly important after they occur. While 39 percent of respondents reported a significant cyber incident, the existence of that incident did not seem to move the budget need for privacy. However, when a regulator became involved, suddenly the budget increased and the emphasis on privacy practices became more pronounced.

Perhaps investors and boards should question why companies seem to be waiting for the regulator to call before prioritizing privacy spend.

INFORMATION SECURITY INCIDENTS

Of our 551 respondents, 39 percent had in the past 24 months experienced a significant information security incident, defined as "the unauthorized disclosure of data (intentional or inadvertent), whether or not rising to the level of a 'breach', requiring some organizational response." Among the respondents who identified themselves as serving in a privacy role, 41 percent said they had experienced such an incident in the past two years. By contrast, only 30 percent of respondents who identified themselves as fulfilling information security functions reported experiencing such an incident.

EXPERIENCED AN INFOSECURITY INCIDENT?



This may be a feature of the privacy professionals' broader interpretation of the definition of "information security incident," including their heightened sensitivity to the risks of data leakage under circumstances that might not trigger a traditional security concern.

Although information security incidents were not rare, overall only 14.5 percent of respondents acknowledged experiencing a notice of investigation or formal enforcement action regarding a privacy concern. That number plummeted to only 6 percent when we examined how non-privacy professionals responded. This may, again, be explained by the increased likelihood that privacy respondents would be involved in a response to a regulator, whereas IT and infosecurity staff may have been more removed from the situation, especially if the contact was only an inquiry and did not lead to enforcement action.

NOTIFICATION OF INVESTIGATION?

OVERALL:	YES: 14.5%	NO: 75.5%	DON'T KNOW: 10%
PRIVACY:	YES: 17.27%	NO: 72.70%	DON'T KNOW: 10.03%
IT/INFOSECURITY:	YES: 6.50%	NO: 82.93%	DON'T KNOW: 10.57%

INFORMATION SECURITY INCIDENTS

Interestingly, those who reported a serious security incident were more likely to be in larger firms. Seventy percent of those reporting an incident worked at firms with 5,000 or more employees vs. 56 percent of respondents overall. It's also true that more than half of the 8 percent who didn't know one way or the other worked at firms with 25,000+ employees. That might more accurately be interpreted as "not that I know of, but it seems likely given our size and scope."

Every industry on our list of 29 reported security incidents but for aerospace, capital goods, food markets, and trading companies. The industries most commonly represented were banking, healthcare, insurance, software and services, and telecom.

Those reporting a notice or enforcement action from a regulator tilted even more toward the top. This is unsurprising given the attention regulators generally pay to larger firms. Positive responders were most likely from banking, healthcare, retail and telecom industries.

The relatively small sample size—just 14.5 percent of our total—makes it hard to draw too many inferences about whether the industry make-up is meaningful. Those who received notices are also about six percent more likely to be in Canada, but, again, we can only take that information as directional given the margin of error.

Geography did play a role in security incident reporting as well. Just 29 percent of European companies reported having experienced a cyber incident, though a larger percentage of Europeans than the group as a whole (14 percent) reported not knowing one way or the other.

Similarly, just 9 percent of Europeans reported interaction with a regulator, vs. 14 percent of U.S. respondents and 22 percent of Canadians. Canada has a reputation for active regulators, and it would seem they've earned it. On the other hand, in the context of the recent negotiations over a new international data transfer framework to replace Safe Harbor, it may be interesting to some that EU regulators would appear to be less active than their U.S. counterparts.

COMPOSITION OF THOSE WHO REPORTED AN INCIDENT:

1-250 EMPLOYEES:	7.5%
251-1,000 EMPLOYEES:	6.5%
1,001-5,000 EMPLOYEES:	16%
5,001-25,000 EMPLOYEES:	29%
25,001+ EMPLOYEES:	41%

COMPOSITION OF THOSE WHO REPORTED RECEIVING NOTICE:

1-250 EMPLOYEES:	3%
251-1,000 EMPLOYEES:	7%
1,001-5,000 EMPLOYEES:	12%
5,001-25,000 EMPLOYEES:	24%
25,001+ EMPLOYEES:	54%

HOW DO YOU USE DATA?

We asked our respondents to characterize how their employer works with data, which unveiled some interesting results.

These were their options:

- WE DERIVE REVENUE DIRECTLY FROM SELLING CUSTOMER INFORMATION TO OTHERS (INCLUDING DATA ANALYTICS), E.G., A DATA BROKER
- WE USE AND ANALYZE CUSTOMER INFORMATION AS A COMPONENT OF OUR OVERALL GO-TO-MARKET STRATEGY, E.G., A DATA CONTROLLER
- WE PROCESS INFORMATION, BUT DO NOT SELL OR ANALYZE CUSTOMER INFORMATION, E.G., A DATA PROCESSOR
- WE DO NOT PROCESS, POSSESS OR COLLECT CUSTOMER INFORMATION

Just two percent said their company sells customer data directly. And just six percent said they don't do any collecting or processing of customer data. The rest were relatively evenly split, with 42 percent essentially identifying as "data controllers," as the European definition would apply, and another 34 percent identifying as data processors.

An additional 16 percent of those who answered chose "None of the above."

We'll look at how these different categories of companies handle data differently, but first breaking out these designations based on other factors may offer some interesting findings.

For instance, while the sample is small, companies with fewer than 250 employees (17 percent of our total) are twice as likely to categorize themselves as data brokers and about half as likely to identify as data controllers. They're also more than twice as likely to say they don't have any customer data at all.

Meanwhile, of the 56 percent of respondents who said their companies employ 5,000 or more employees, fewer than two percent said they don't hold customer data. And they were 8 percent more likely to identify as a data controller.

As for geography, we saw no significant difference in the way respondents self-identified other than in Canada, where a full 31 percent self-identified as "none of the above," likely a reflection of the large portion of Canadian privacy professionals in the health care field and other quasi-public posts.

PRIVACY INVESTMENTS

We asked respondents to describe their employers' actions, or investments, with regard to privacy in the past 24 months.

Almost 40 percent of respondents with knowledge of their employers' budget decision (discounting those who chose "don't know") reported that privacy budgets had increased in the last two years, while 60 percent reported increases in information security budgets.

Forty-eight percent of respondents with knowledge reported an increase in the number of employees with privacy duties, and 50 percent said their employer had increased employee training on privacy. In the past two years, 49 percent of respondents reported that their employer had increased the involvement of privacy personnel on information security teams.

With regard to privacy management tools, 41 percent of respondents with knowledge said their employer had increased the use of data inventory/ classification programs and privacy impact assessments, while 33 percent had increased their use of data retention policies.

Ninety percent of our respondents had knowledge of their employers' spending on privacy and information security-related technology tools. Of these, 42 percent of respondents had increased their spending on privacy-related technology while nearly two in three increased their investments in information security-related technology in the past two years.

Spending increases on privacy technology is outpacing spending increases on external services, with 34 percent reporting increased spending on external counsel and 26 percent noting an increase on external auditors.

THOSE WHO REPORTED INCREASES:

	%
SPEND ON INFOSECURITY-RELATED TECHNOLOGY:	66
OVERALL INFOSECURITY BUDGET:	61
EMPLOYEE PRIVACY TRAINING:	53
PRIVACY EMPLOYEES ON THE INFOSECURITY TEAM:	50
NUMBER OF EMPLOYEES WITH PRIVACY DUTIES:	49
SPEND ON PRIVACY-RELATED TECHNOLOGY:	42
USE OF DATA INVENTORY AND CLASSIFICATION:	42
USE OF PRIVACY IMPACT ASSESSMENTS:	41
USE OF DATA RETENTION POLICIES:	40
OVERALL PRIVACY BUDGET:	39
SPEND ON EXTERNAL PRIVACY COUNSEL:	34
SPEND ON EXTERNAL PRIVACY AUDIT:	26

ROLE OF PRIVACY IN MITIGATING THE RISK OF A SECURITY INCIDENT

We asked respondents about the importance of a number of privacy functions to mitigating the risk of an information security breach. Perhaps reflecting a global effort to get privacy and IT/infosecurity in better communication, respondents identified the communication between privacy and infosecurity teams as most vital in risk mitigation, followed by inclusion of privacy team members on incident response teams, and the very existence of breach response teams.

It would seem that infosecurity teams are eager to know which data is most in need of protecting and which data, when lost, poses the most risk to the enterprise's well being. Data minimization and data inventory and mapping were ranked highest in risk mitigation by IT/Infosecurity teams.

Finally, corporate training, long a hallmark of any privacy team's responsibilities, rounds out the top four answers, all identified by a majority of respondents.

HIGHEST OVERALL PERCEIVED IMPORTANCE

(AS RANKED BY THOSE SELECTING 4 OR 5, IMPORTANT OR VERY IMPORTANT):

	%
COMMUNICATIONS BETWEEN PRIVACY AND SECURITY DEPTS.	91
CORPORATE TRAINING AND EDUCATION ON PRIVACY	87
ROLE OF PRIVACY PROFESSIONAL ON THE INCIDENT RESPONSE TEAM	85
DATA BREACH RESPONSE TEAMS	84
MATURITY OF PRIVACY PROGRAM	81
PRIVACY WORKING GROUP	60
BUDGET OF PRIVACY TEAM	57
RELATIONSHIPS WITH REGULATORS	53
PRIVACY CERTIFICATION, INDIVIDUALS	49
SIZE OF PRIVACY TEAM	43
OUTSIDE PRIVACY COUNSEL	37
PRIVACY CERTIFICATION, ORGANIZATIONAL	32

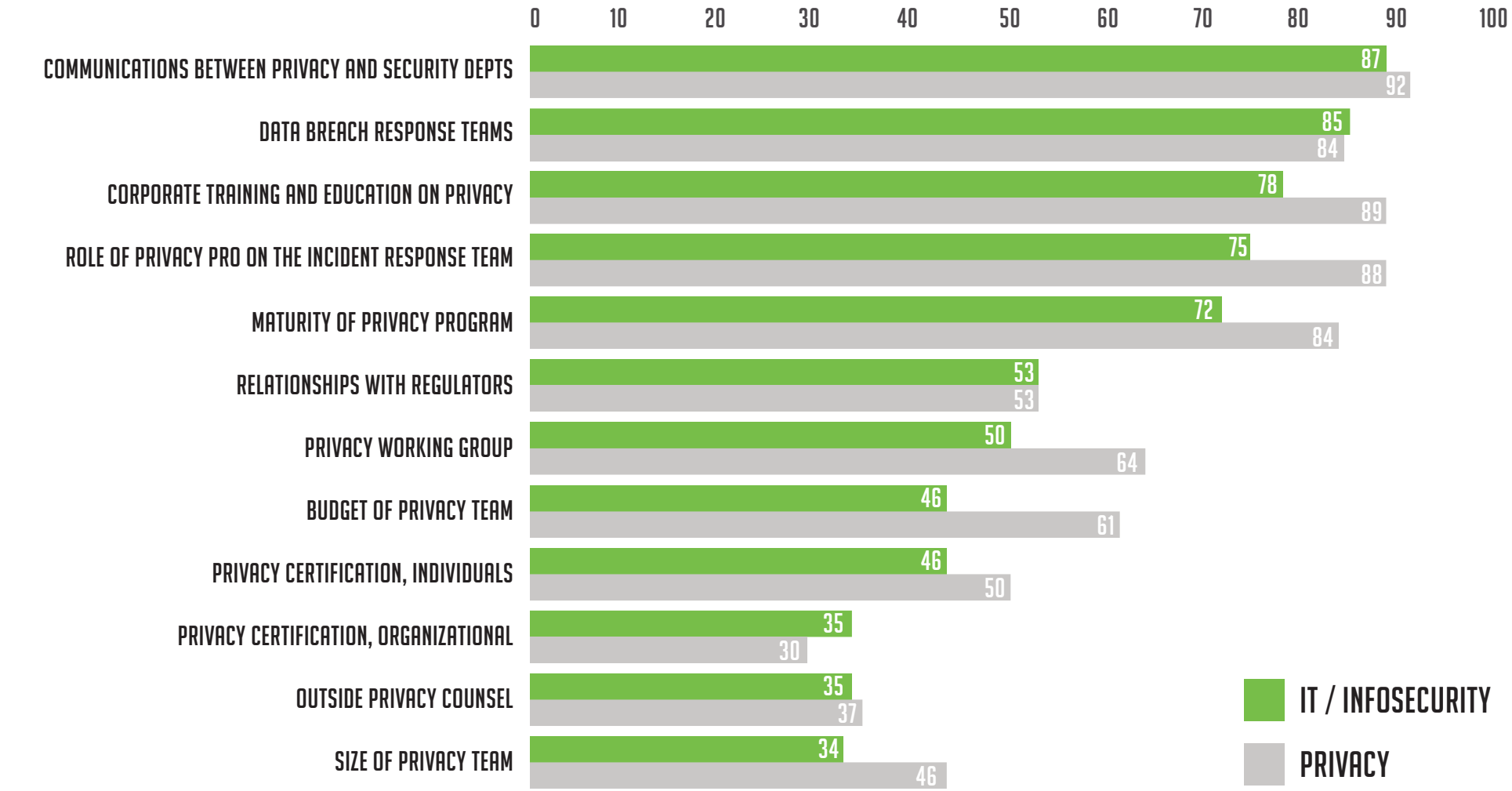
	%
DATA INVENTORY/MAPPING	74
SPEND ON INFORMATION SECURITY-RELATED TECH	74
PRIVACY IMPACT ASSESSMENTS	71
DATA RETENTION POLICIES	68
EMPLOYEE MONITORING	55
SPEND ON PRIVACY-RELATED TECHNOLOGY	57
WEBSITE TRACKER SCANNING	45

ROLE OF PRIVACY IN MITIGATING THE RISK OF A SECURITY INCIDENT

When we filtered for answers submitted by respondents who identified themselves as fulfilling privacy functions versus those who fulfill information security or information technology (non-privacy) functions, the results were slightly different.

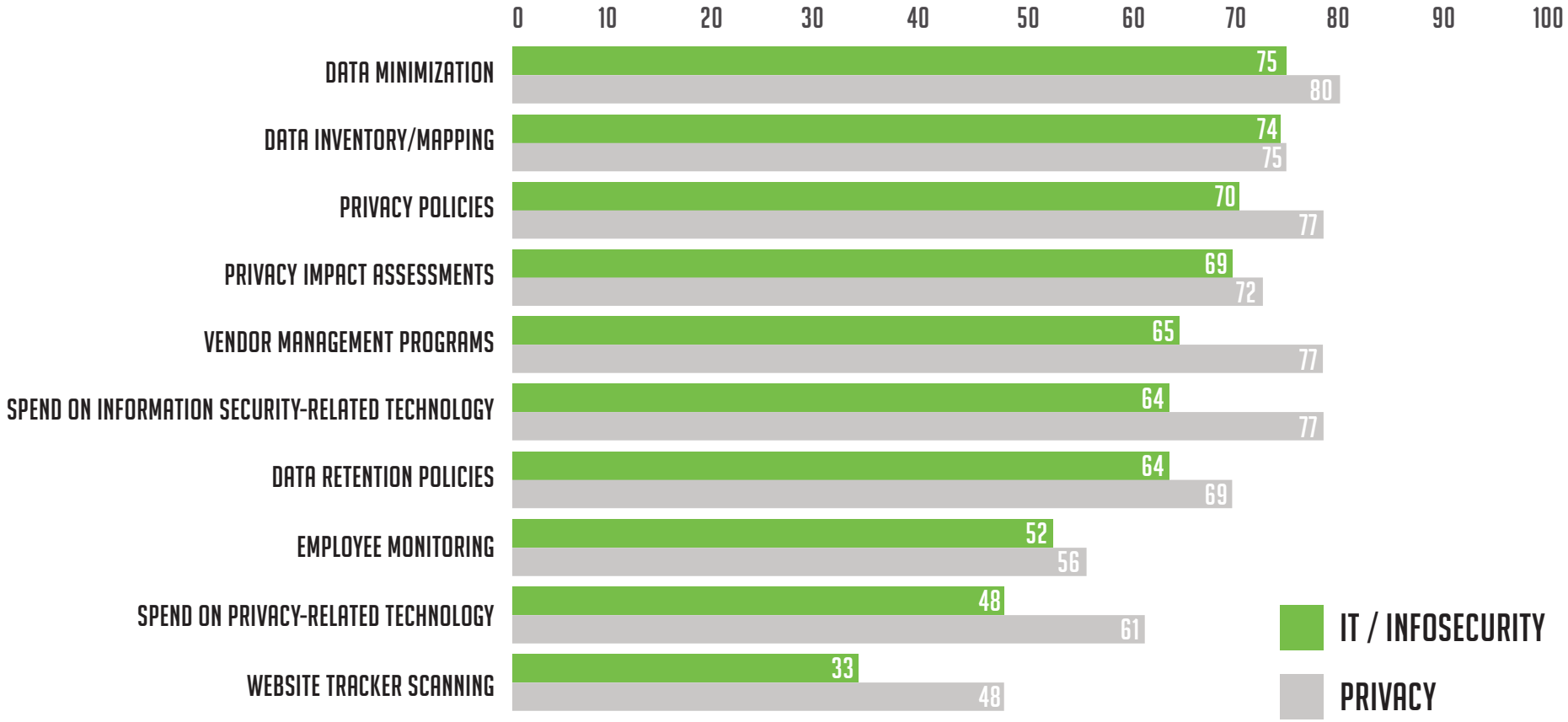
Those in IT and infosecurity functions, perhaps predictably, were less likely to value corporate training and education and the size and budget of the privacy team. However, it would seem that communication between privacy and security departments as well as the existence of well-rounded incident response teams are some things the entire organization can agree on.

HIGHEST OVERALL PERCEIVED IMPORTANCE (AS RANKED BY THOSE SELECTING 4 OR 5):



ROLE OF PRIVACY IN MITIGATING THE RISK OF A SECURITY INCIDENT

HIGHEST OVERALL PERCEIVED IMPORTANCE (AS RANKED BY THOSE SELECTING 4 OR 5):



WHERE PEOPLE SIT

DEPARTMENT	DISCIPLINE'S REPRESENTATION		
	PRIVACY	INFOSEC	IT
INFORMATION TECHNOLOGY	42%	76%	-
INFORMATION SECURITY	52%	-	71%
LEGAL	95%	43%	26%
PRIVACY	-	46%	33%
REG COMPLIANCE / ETHICS	92%	51%	57%
HUMAN RESOURCES	82%	40%	34%
PHYSICAL SECURITY	42%	73%	53%
RECORDS MANAGEMENT	71%	49%	41%
FINANCE / ACCOUNTING	52%	54%	50%
PROCUREMENT	44%	55%	57%
MARKETING/ PR	67%	37%	47%
GOVERNMENT AFFAIRS	78%	29%	31%

CROSS POLLINATION

We also asked our respondents to tell us the extent to which information privacy, security and technology personnel can be found throughout their organization, including in each other's departments.

To the extent departments had personnel representing privacy, information security, or information technology, here is how each discipline is represented:

Firstly, given the relative importance placed on vendor management, the third highest tactical priority, it's fair to ask if more procurement teams ought not to have privacy representation. Also, given physical security's often large stockpile of PII—everything from biometric data to location data from card keys to video surveillance—it's perhaps surprising to see so little representation for privacy there.

Alternately, given the high importance placed on communications between teams, we may see increasing numbers of legal teams taking on infosecurity and IT professionals to make sure they're consulting on policy and privacy by design.

BROKERS, CONTROLLERS, PROCESSORS, AND OTHERWISE

But what about the priorities of those different types of companies we mentioned earlier—brokers, controllers, processors, and those with only employee data?

First, the margins. Just 2 percent and 6 percent of respondents identified as brokers or those without data, respectively. So the data can only be taken as anecdotal, at best. However, the data does seem to align with common sense. Those without consumer data holdings prioritize the privacy team 10 percent less than average, and are 15 percent less likely to value relationships with regulators.

In fact, they didn't report a single cyber incident or interaction with a regulator from their ranks.

They're also 8 percent less likely to have increased their privacy budget and 12 percent less likely to have increased their privacy headcount. They're almost 20 percent less likely to have increased the use of privacy impact assessments.

And, as you might expect they value employee monitoring almost 20 percent more than average.

On the flip side, the small number of brokers we identified were simply more status quo than any of our other categories, in that everything has basically remained the same in terms of privacy investment over the past two years. With consumer data so central to their business model, it may be they already have significant privacy programs in place. Broker Acxiom, for example, is largely thought to have been the first company to anoint someone with the title of chief privacy officer, back in the 1990s.

Most instructive, though, is looking at the difference between controllers and processors. The controllers tend to be larger companies, with 43 percent reporting more than 25,000 employees vs. just 32 percent of processors. It's no surprise, then, that those respondents working for data controllers are also about 9 percent more likely to have reported a security incident, and 25 percent more likely to have received notice from a regulator, a full 67 percent of the total.

We've already seen that larger companies get more regulatory activity and are more likely to report a security incident. Still, there may be some question as to whether processors are outside the public eye (and that of regulators).

It should also be no surprise, as we'll see in our next section on the effect of regulator activity vs. the effect of a security incident, that data controllers are 7 percent more likely to have increased the number of employees dedicated to privacy, and 9 percent more likely to have increased the emphasis put on data inventory, classification, and minimization, along with data retention policies.

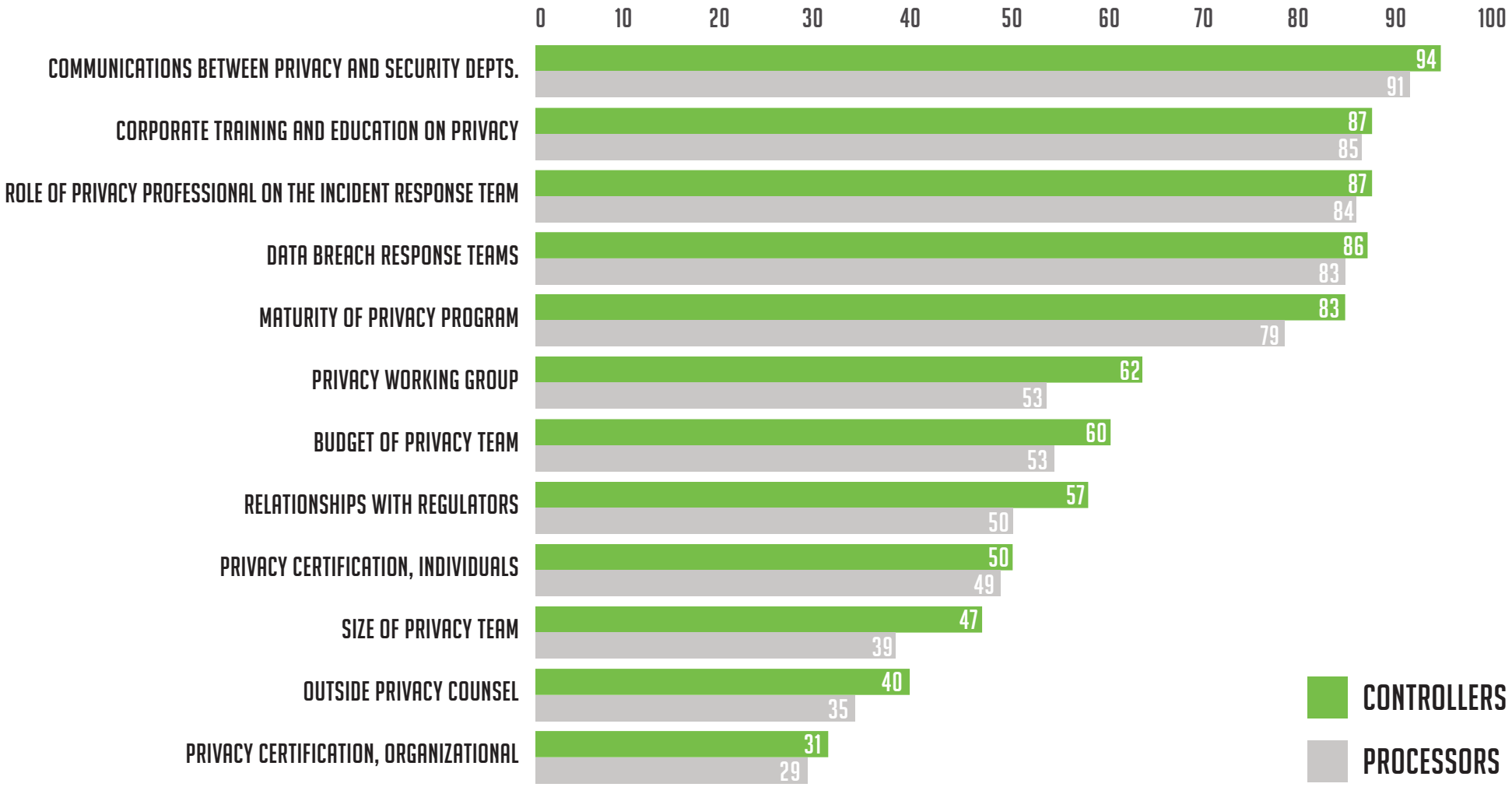
On the other hand, perhaps reflecting that processors are playing catch-up in the privacy operations game, they are 7 percent more likely to have increased their use of privacy impact assessments.

> ***"There may be some question as to whether processors are outside of the public eye."***

BROKERS, CONTROLLERS, PROCESSORS, AND OTHERWISE

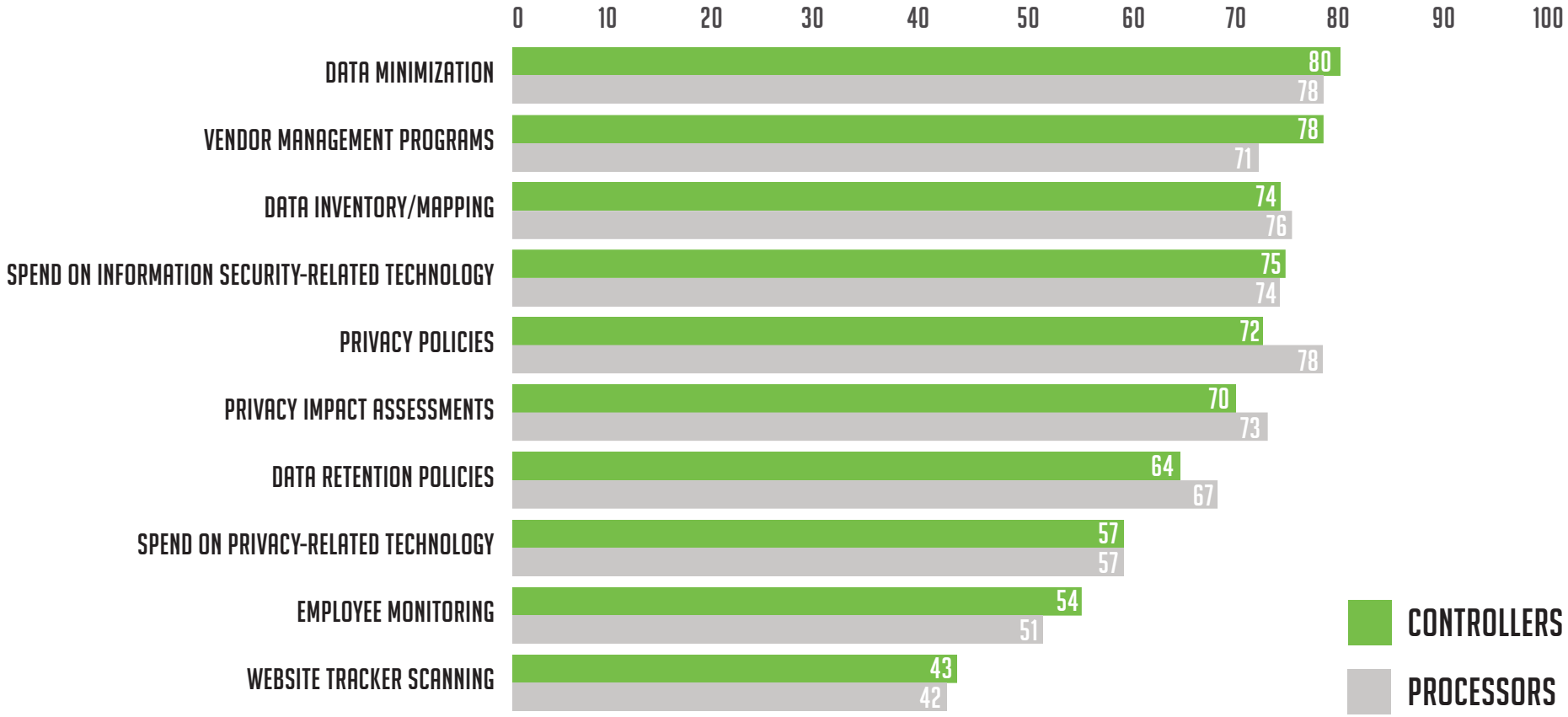
In looking at their attitudes toward mitigating a breach, we see a similar emphasis on privacy practices among controllers. They value more highly the privacy budget, the maturity of the privacy program, the privacy working group, outside privacy counsel, a vendor-management program, and relationships with regulators (reflecting their greater likelihood of experiencing regulatory interaction).

HIGHEST OVERALL PERCEIVED IMPORTANCE (AS RANKED BY THOSE SELECTING 4 OR 5):



BROKERS, CONTROLLERS, PROCESSORS, AND OTHERWISE

HIGHEST OVERALL PERCEIVED IMPORTANCE (AS RANKED BY THOSE SELECTING 4 OR 5):



IMPACT OF A BREACH VS. REGULATOR INVOLVEMENT

As part of our survey, we sought to find out whether a serious data security incident or some kind of enforcement activity, everything from a notice of investigation to an actual enforcement action, affected the way companies handled data. Alternatively, we wondered whether we might see a difference between the data-handling attitudes of those who'd experienced a negative data experience and those who reportedly hadn't.

As a reminder, for the purposes of the survey, we defined a "significant information security incident" as the unauthorized disclosure of data (intentional or inadvertent) whether or not rising to the level of a "breach," requiring some organizational response. Respondents were also reminded that all responses would be kept anonymous and only analyzed in the aggregate.

We've already seen the percentages for those who answered that they did, in fact, have a security incident (39 percent) or receive notice from a regulator (14.5 percent), but how did these experiences change behavior?

For those reporting a security incident, it is perhaps most striking how similar their answers are to the general population. And where there is a difference, that difference is perhaps counterintuitive. In fact, while the differences are within the margin of error, respondents who experienced a security incident are slightly less likely to have increased their privacy budget, training efforts, privacy headcount, or privacy involvement on infosec teams.

However, they are slightly more likely to have increased their spend on privacy technology and they are 8 percent more likely to have increased spend on information security technology.

Similarly, in terms of their opinions on how to best manage breach risk, they are largely in lock-step with the general population. For no factor do we see a statistically significant difference, and in only four areas do we find a five-percent or greater difference that could be called a directional indication.

HOW ATTITUDES IN IMPORTANCE FOR MITIGATING BREACH RISK CHANGE FOLLOWING A CYBER INCIDENT (PERCENT OF THOSE SELECTING 4 OR 5, GENERAL POPULATION LISTED FIRST):

SIZE OF PRIVACY TEAM	43%	48%	^ +5%
MATURITY OF PRIVACY PROGRAM	81%	86%	^ +5%
PRIVACY CERTIFICATION, INDIVIDUALS	49%	42%	v -7%
PRIVACY CERTIFICATION, ORGANIZATION	31%	26%	v -5%

IMPACT OF A BREACH VS. REGULATOR INVOLVEMENT

The top-level tactics for those experiencing a security incident remain essentially the same: communicate between teams, train employees and executives, and make sure there's a privacy professional on the incident response team.

We see a different story for those who have received notification or enforcement action, however.

Significantly, if we back out those respondents without budget knowledge, we find those who've interacted with regulators to be more likely to have increased privacy spend (47 percent vs. 39 percent) while having the exact same likelihood of increasing infosecurity spend (60 percent vs. 60 percent).

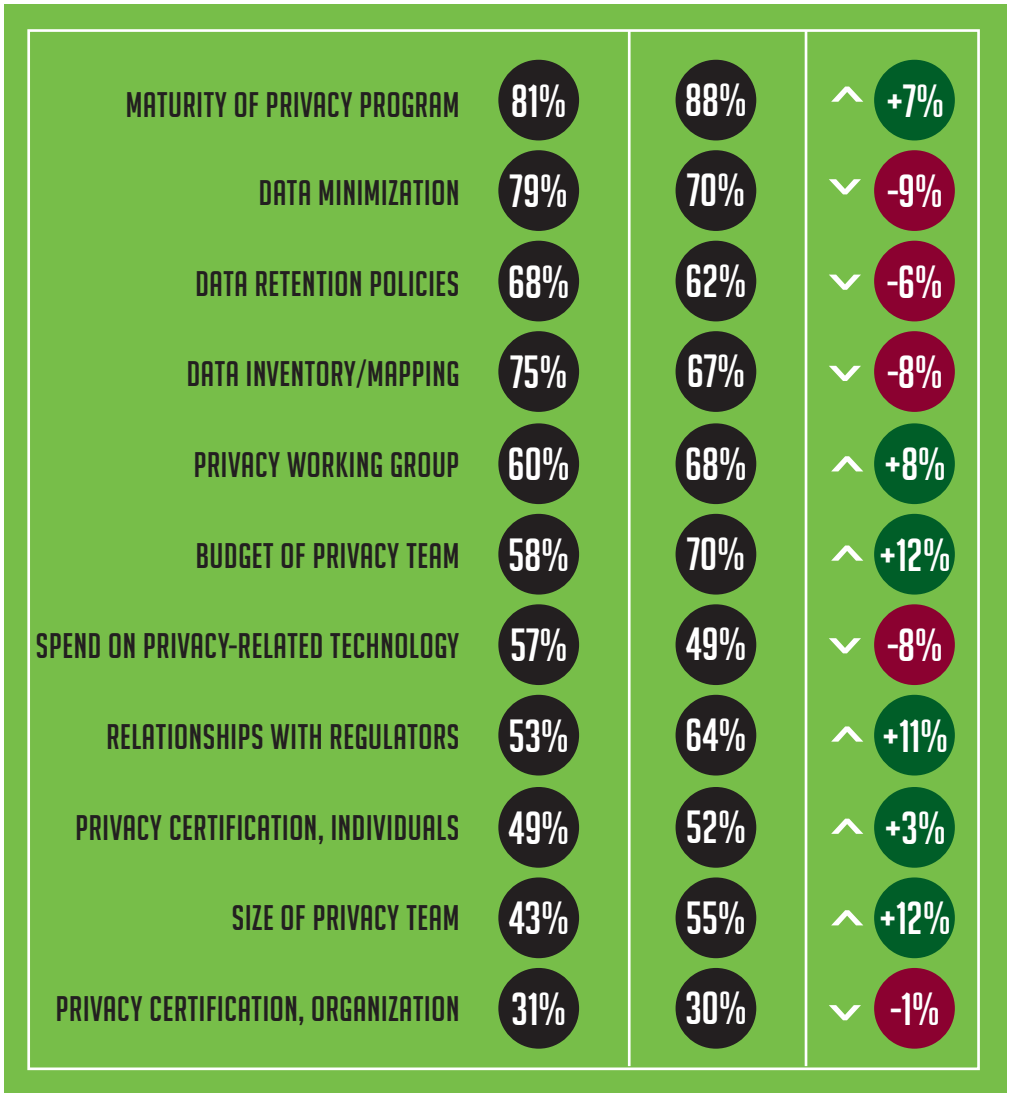
It is perhaps intuitive that a cyber incident would lead to increased technological spend, while an interaction with a regulator would lead to increased spend on the likes of external counsel in the privacy budget, but we didn't find a statistical difference in external counsel spend here; those with regulator interaction are actually slightly more likely both to have increased and to have decreased their counsel spend (rather than simply keep it the same).

Turning to priorities for risk mitigation, we see a similar inclination. Those who've had regulator interaction are more likely to place emphasis on privacy budget, the size of the privacy team, and the maturity of the privacy program. They also move in the opposite direction in terms of individual privacy certification, valuing it more highly than those who've had the cyber incident.

As you might infer, they also value the relationship with the regulator much more highly, and they are more likely to value the privacy working group, perhaps perceiving a need to communicate better throughout the organization.

Some of the tactical efforts they value less, however. Data minimization, inventory, mapping, and retention all drop slightly, while remaining relatively high overall.

HOW ATTITUDES IN IMPORTANCE FOR MITIGATING BREACH RISK CHANGE FOLLOWING INTERACTION WITH A REGULATOR (PERCENT OF THOSE SELECTING 4 OR 5, GENERAL POPULATION LISTED FIRST):



CONCLUSION

We know the privacy profession is growing. We know that focus on privacy practices is working its way deeper into organizations around the globe. What we see in these findings, however, is that there is also growing realization that breach prevention is more than just good security.

Largely, privacy has been called in after the breach has happened—to handle notification and remediation, perhaps to identify the value of the data that has been lost. However, we see clear evidence that the infosec and IT communities are cottoning on to the fact that privacy can be of help before an incident. Privacy is perceived as adding value by contributing data classification and minimization help, establishing good policy, and communicating thoroughly so that organizations understand the value of the information they have and can better plan how to protect it and allocate resources.

It is also perhaps instructive for organizations to look at the disparity between the reaction to a cyber incident and the reaction to interaction with a regulator. While one is not necessarily triggered by the other, it's clear that companies are doing more to change their behavior when a regulator is involved.

With the general understanding that regulators are under-resourced and don't have the ability to investigate every incident, let alone become aware of every incident, one wonders whether organizations are cognizant of the bullets they may be dodging.

> ***"It's clear that companies are doing more to change their behavior when a regulator is involved."***

Their own IT staffs know that throwing their tech spend at security isn't the only—or even the best—way to prevent damaging breaches.

The next question is: Has that message made it to the c-suite?

NOW, LET'S HEAR HOW IT WORKS IN PRACTICE:

KEVIN HAYNES –
CHIEF PRIVACY OFFICER, THE NEMOURS FOUNDATION

KEVIN HAYNES –
CHIEF PRIVACY OFFICER, THE NEMOURS FOUNDATION

"I learned early in my role in privacy that very few cases are black and white. Very few situations are yes or no, zero or one. It's not binary," observes Kevin Haynes, Chief Privacy Officer for The Nemours Foundation, which provides health care services for children.

Kevin paid his way through college working in information technology, including as an information security specialist. He later served as Chief Information Security Officer (CISO) for a variety of organizations and also held that role at Nemours.

"When the former CPO retired, I was asked if I wanted the position. It interested me because I was looking for a change from IT, and I wanted to work more closely with people and business issues. I believed my background in security and IT would be a great benefit in privacy," Haynes said.

Indeed it was. At first, Haynes thought it would be possible to be both CISO and CPO. But that grand idea quickly faded as he began to appreciate the differences between the information security and privacy responsibilities, as well as the differences in function and mindset.

"In security," he said, "you're either secure or not, you have control or not. But privacy is not just about control, and not just the process or technology. It's about the information, the people represented by the information. In privacy, we look at incidents, but then we go one step further to ask what information was revealed. Is there a risk of harm to the person or her reputation?"

Haynes finds that procedures, frameworks and tools he deployed as a CISO are still useful to him as CPO, where he conducts risk assessments, privacy impact assessments, and self-assessments, working with software applications and other tools. Access controls also remain very important because of the particular regulations that apply in health care.

He finds crucial to his success as CPO the close working relationship he shares with the CISO. They meet at least weekly, so that nothing is ever lost or missing in their communication. Kevin knows that his ability to understand his colleague's job is a significant advantage to their collaborative relationship.

"Nonetheless, I see the two roles as completely different functions. I initially thought both roles could be consolidated. I've now learned that there's no way you can do both jobs effectively," Haynes said. "The expertise and discipline required for the CISO and CPO functions are different. I used to think privacy would be easy—that it would be just reporting and interviewing people. But the responsibility of the privacy officer is different from that of a CISO. The CPO and CISO share common ground, like risk assessments and information protection controls.

"One core difference," he continued, "is that whereas the CISO is working on improving technology and educating people on how best to take advantage of the technology, the privacy side spans every element of information access from the phone calls people take, to access to electronic records, to state law complexity. There are also very few resources available for privacy professionals in terms of frameworks, standards and principles compared to the guidance available to security professionals."

Different does not mean incompatible, however, it just means the privacy and security personnel need to communicate regularly and work as a team.

"Consider the issue of access controls, for example," Haynes said. "An information security professional is going to think about whether the user is responsible for the area of interest, whether they are authorized to get into the app. When I think about whether someone can access an app, I'm also worried about what content they can see. We just need to make sure we're in tune with each other."