RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: AST3-W02

The Data Behind How We Work with Data

Connect to Protect

Sam Pfeifle

Publications Director
International Association of Privacy Professionals
@DailyDashboard

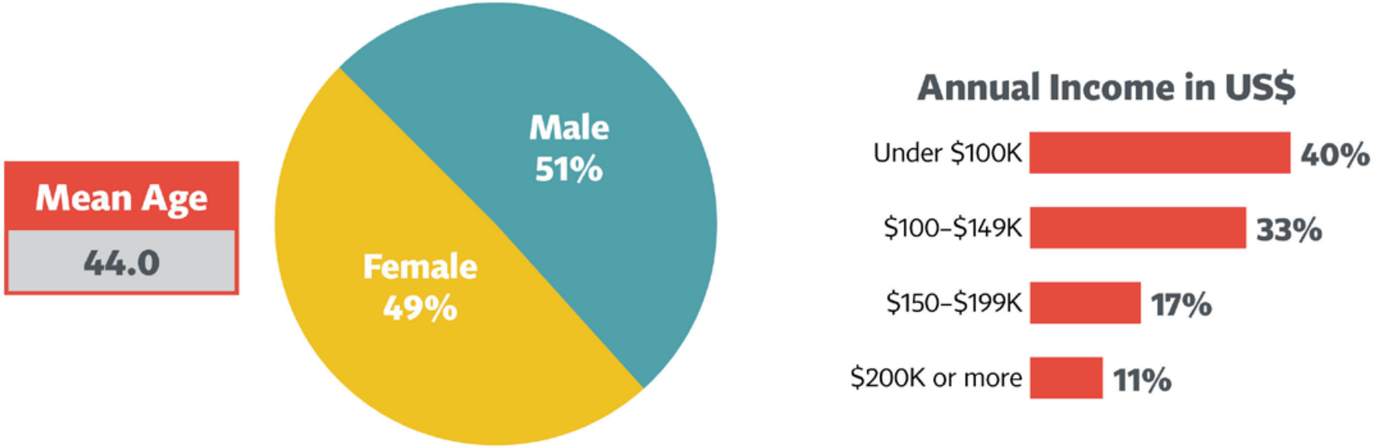
#RSAC

Who Are They?

Privacy professionals are equally split gender-wise, with a mean age of 44

- In addition, 6 in 10 privacy pros have a salary of $100K or more

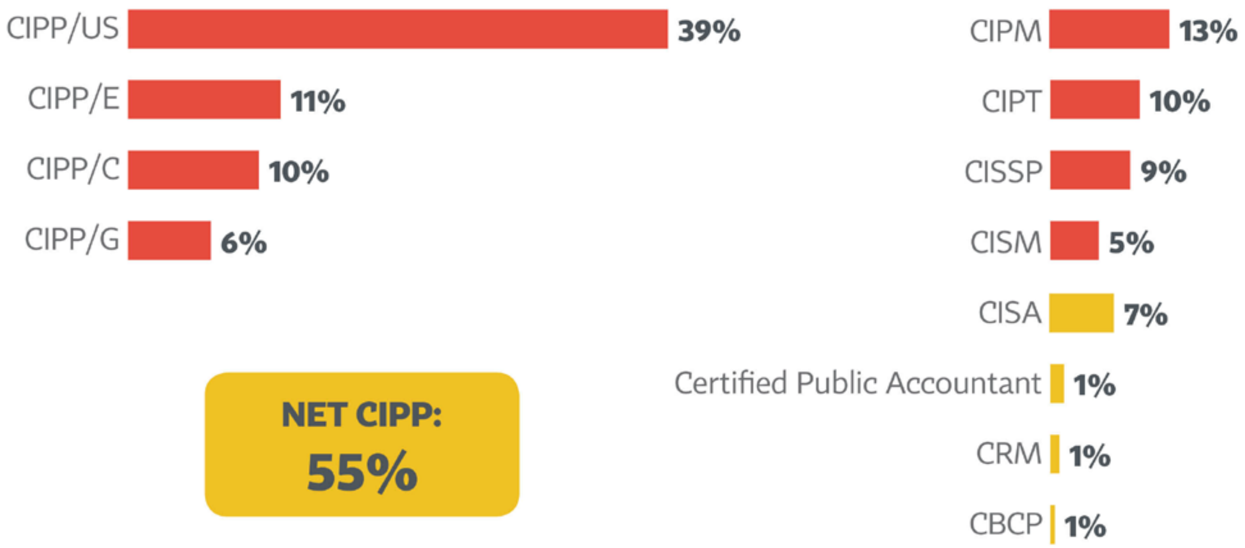
Demographics of Privacy Professionals



Who Are They?

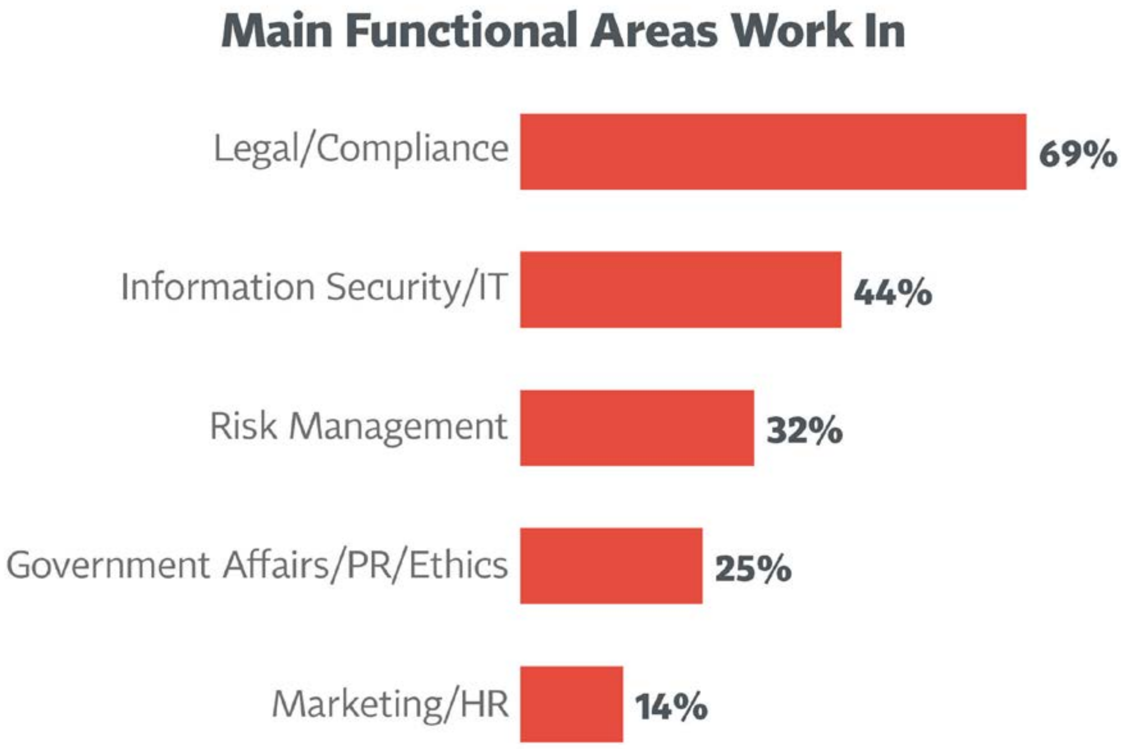
Three-fourths of privacy professionals have some certification, with most having a CIPP

Credentials and Degrees Held by Privacy Professionals



- 24% listed no credential at all
- 23% listed a different credential, Including CCEP, PMP, and CHP

What Do They Do?

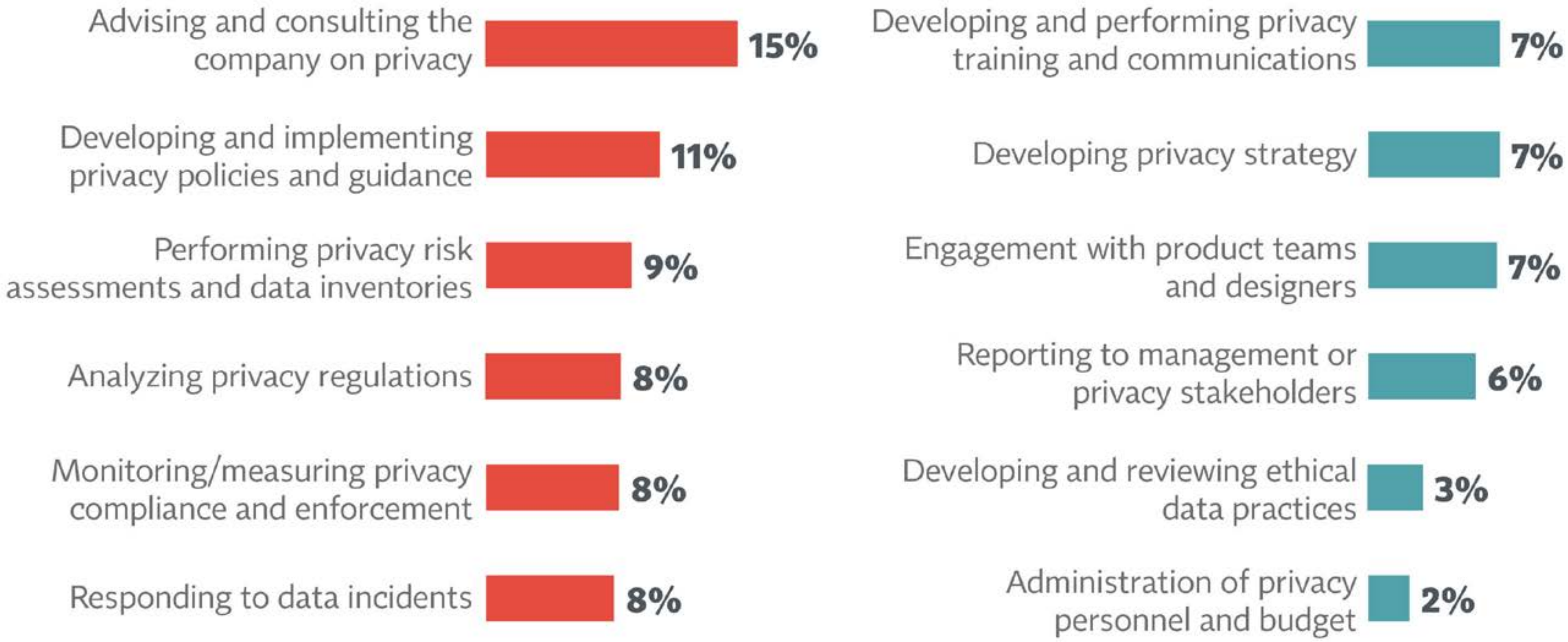


- We are increasingly seeing non-lawyers entering the profession.

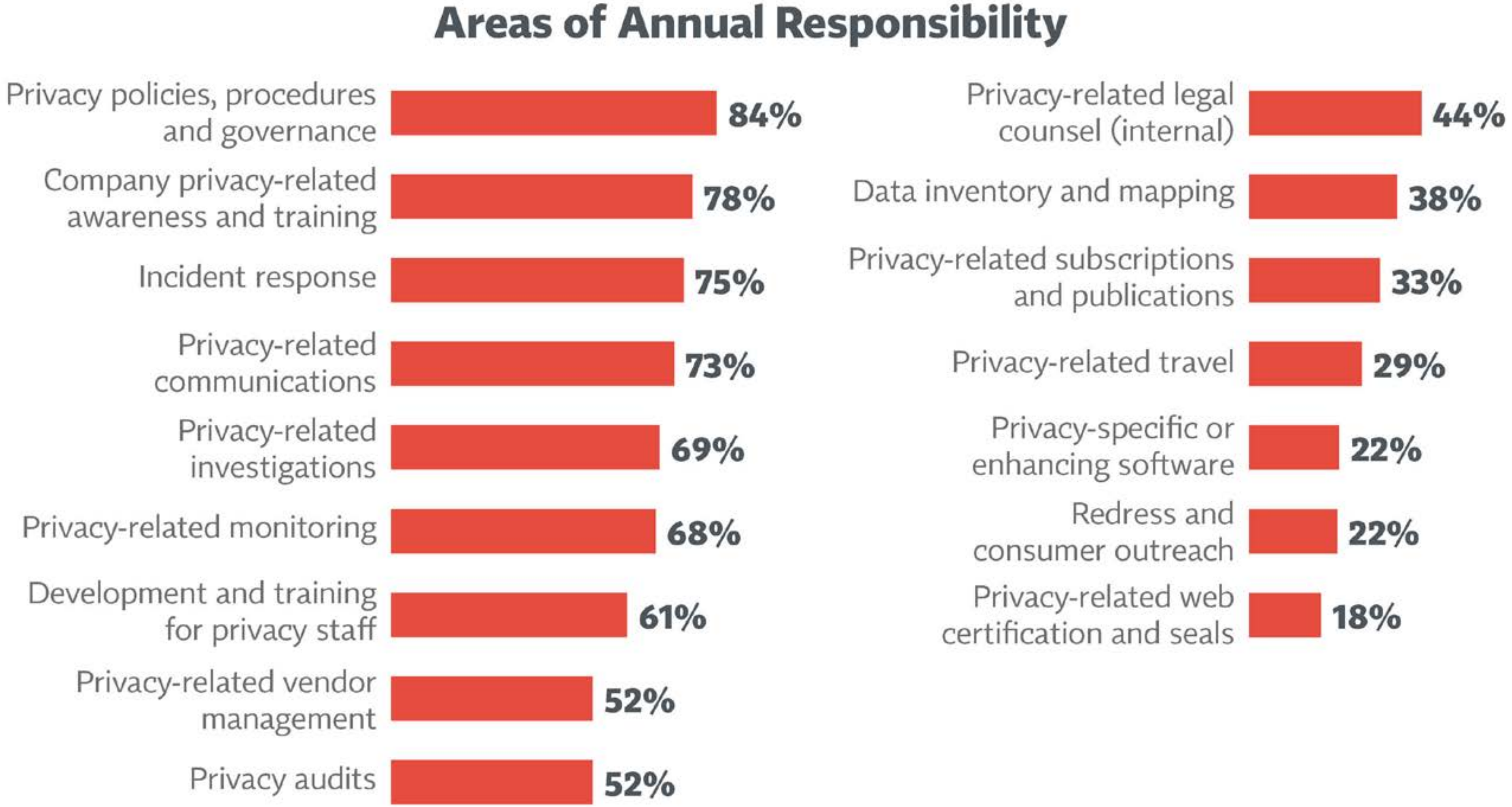
- We are seeing more operational privacy pros being embedded in more diverse areas of the organization

What Do They Do?

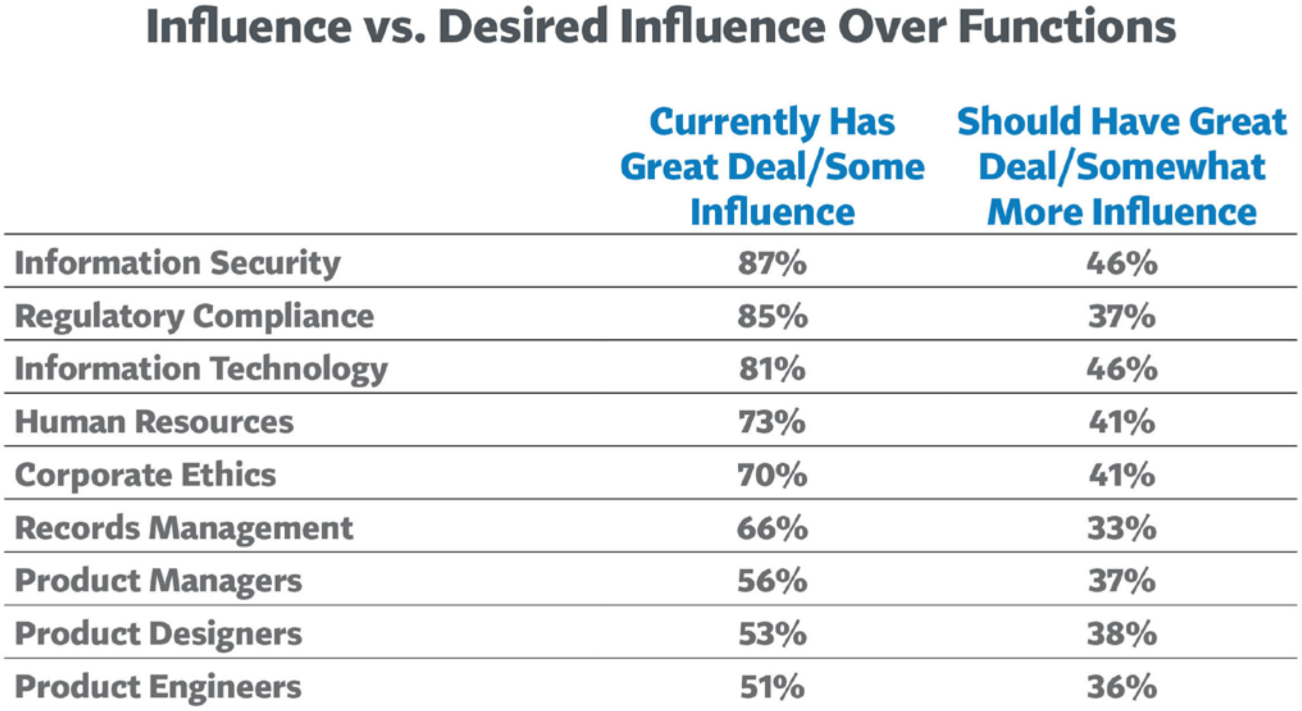
Mean Percent of Privacy Work Per Area



What Do They Do?



What Do they Do?

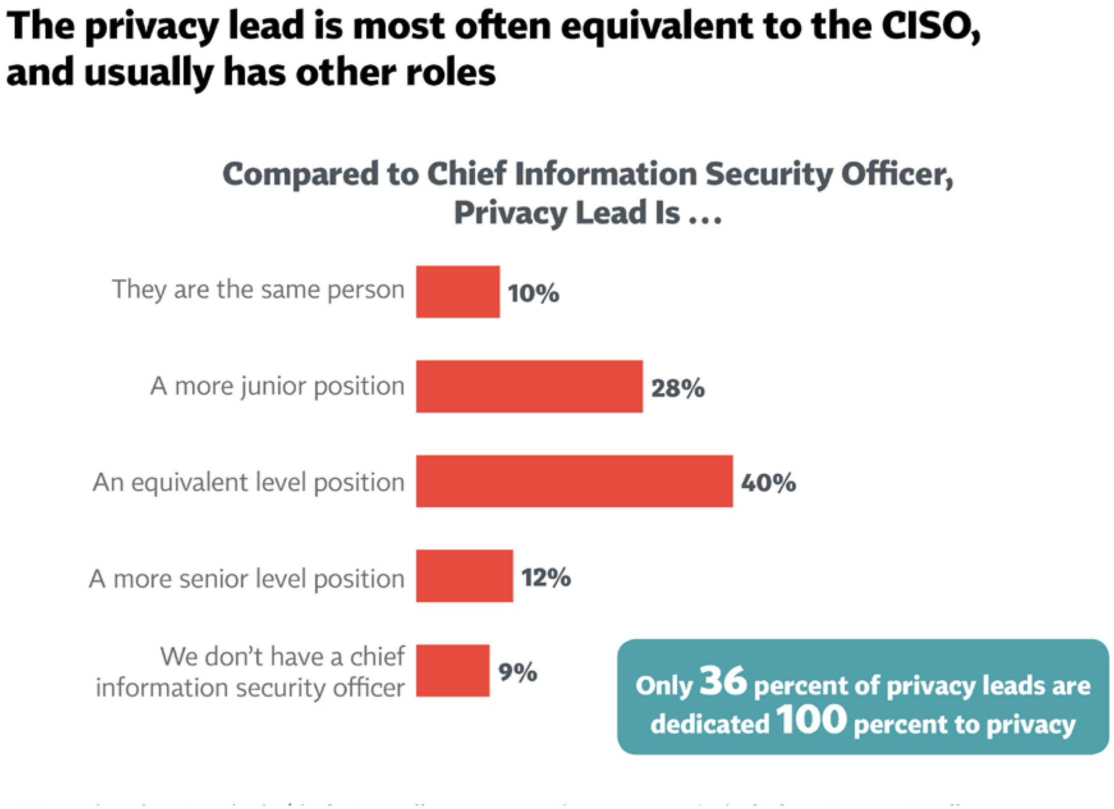


Influence vs. Desired Influence Over Functions

	Currently Has Great Deal/Some Influence	Should Have Great Deal/Somewhat More Influence
Information Security	87%	46%
Regulatory Compliance	85%	37%
Information Technology	81%	46%
Human Resources	73%	41%
Corporate Ethics	70%	41%
Records Management	66%	33%
Product Managers	56%	37%
Product Designers	53%	38%
Product Engineers	51%	36%

- As we'll see later IT, Infosec, and Privacy are intimately linked within the organization.

What Do they Do?



The privacy lead is most often equivalent to the CISO, and usually has other roles

Compared to Chief Information Security Officer, Privacy Lead Is . . .

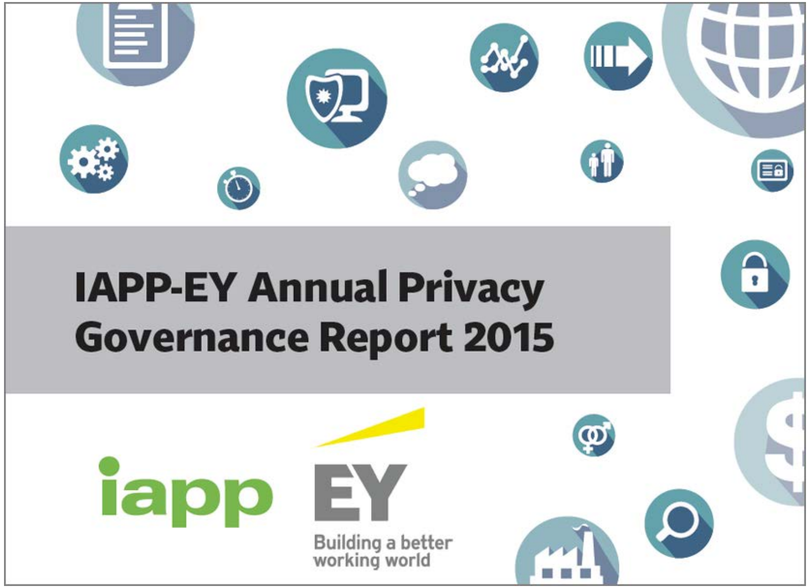
Only 36 percent of privacy leads are dedicated 100 percent to privacy

Operational Conclusions and Applications

- Privacy handles a wide variety of tasks and is organized in many different ways

- Companies need to begin defining clearly what is, and what is not, privacy

- Privacy is getting deep within organizations; those with privacy as just a compliance role may be behind the times



IAPP-EY Annual Privacy Governance Report 2015

iapp

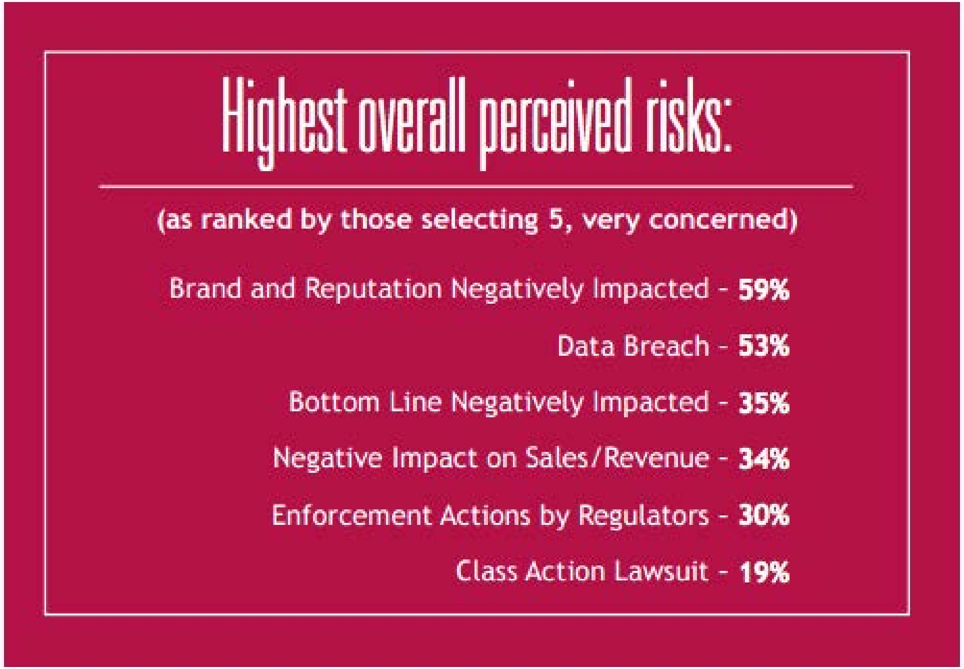
EY

Building a better working world

https://iapp.org/media/pdf/resource_center/IAPP-EY_Privacy_Governance_Report_2015.pdf

The Biggest Risks

- Brand vs. Breach
- Who’s Watching the Bottom Line?
- Will Regulator Risk Increase?



Highest overall perceived risks:

(as ranked by those selecting 5, very concerned)

Brand and Reputation Negatively Impacted - **59%**

Data Breach - **53%**

Bottom Line Negatively Impacted - **35%**

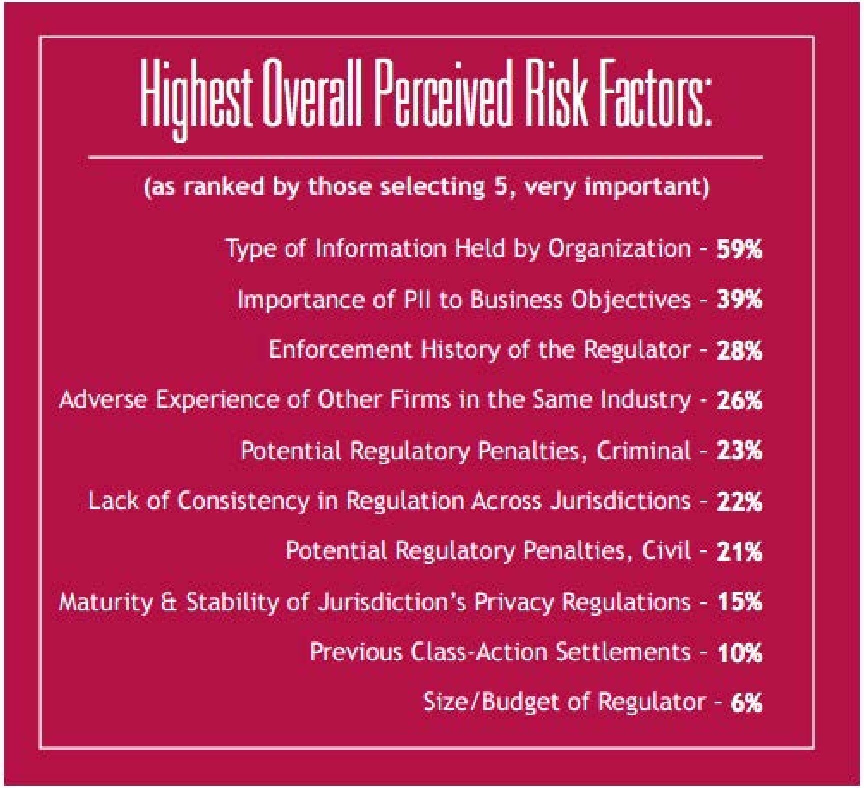
Negative Impact on Sales/Revenue - **34%**

Enforcement Actions by Regulators - **30%**

Class Action Lawsuit - **19%**

Biggest Risk Factors

- PII Is King
- Risk in the Post Safe Harbor Age
- Enforcement History Becoming More Robust



Highest Overall Perceived Risk Factors:

(as ranked by those selecting 5, very important)

Type of Information Held by Organization - **59%**

Importance of PII to Business Objectives - **39%**

Enforcement History of the Regulator - **28%**

Adverse Experience of Other Firms in the Same Industry - **26%**

Potential Regulatory Penalties, Criminal - **23%**

Lack of Consistency in Regulation Across Jurisdictions - **22%**

Potential Regulatory Penalties, Civil - **21%**

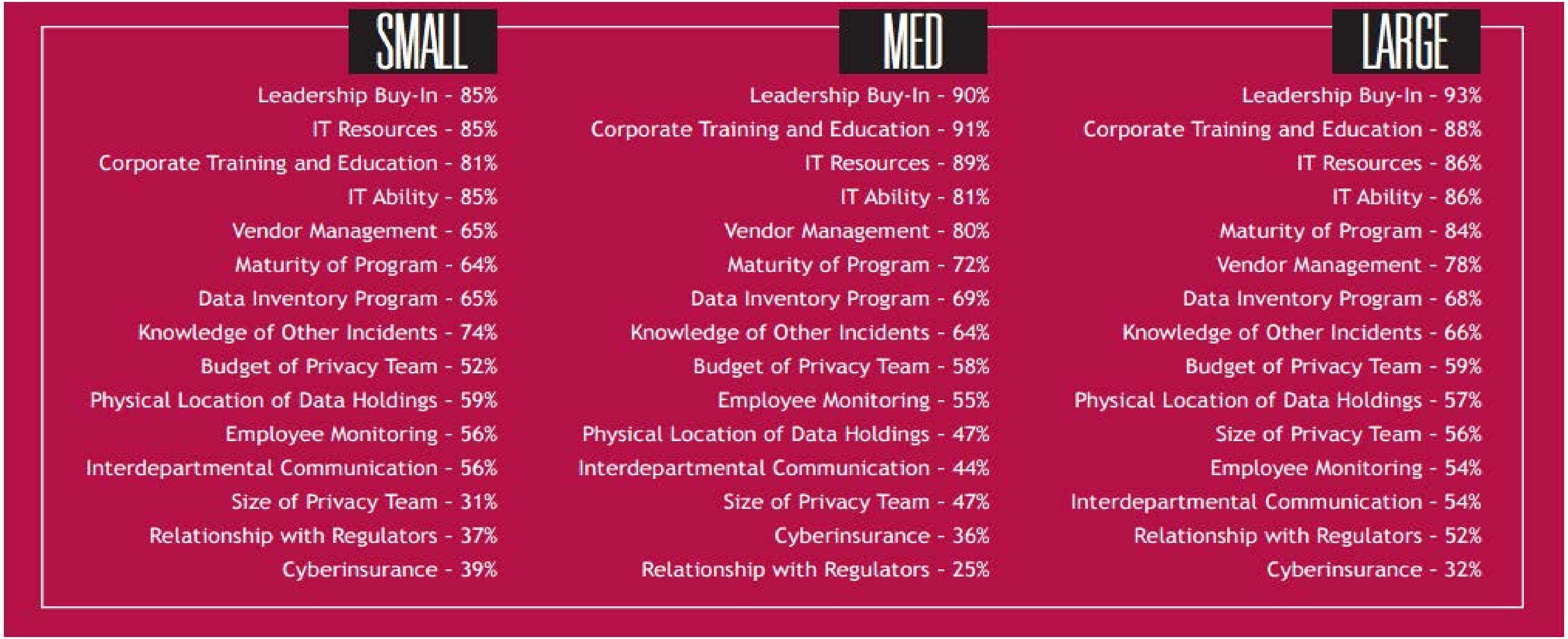
Maturity & Stability of Jurisdiction's Privacy Regulations - **15%**

Previous Class-Action Settlements - **10%**

Size/Budget of Regulator - **6%**

Mitigating Risk

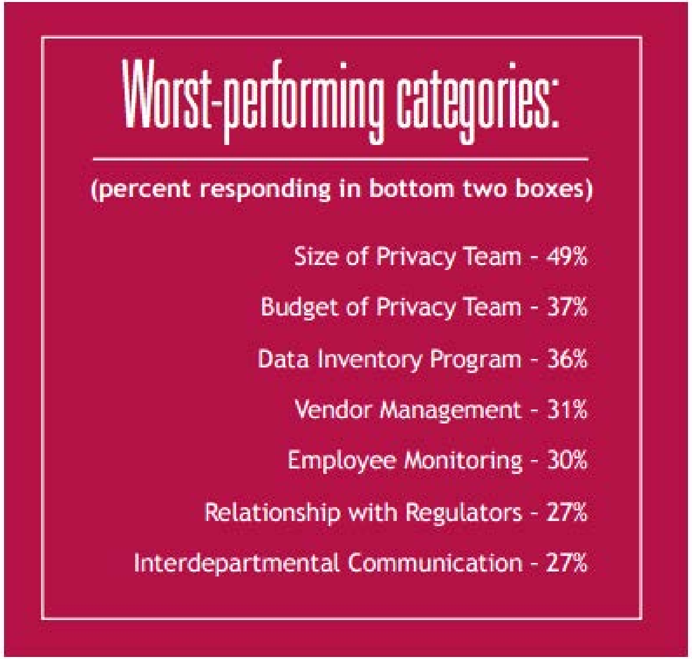
- What if Leadership Won’t Buy In?
- Working with IT
- Curious Case of Cyberinsurance



SMALL	MED	LARGE
Leadership Buy-In - 85%	Leadership Buy-In - 90%	Leadership Buy-In - 93%
IT Resources - 85%	Corporate Training and Education - 91%	Corporate Training and Education - 88%
Corporate Training and Education - 81%	IT Resources - 89%	IT Resources - 86%
IT Ability - 85%	IT Ability - 81%	IT Ability - 86%
Vendor Management - 65%	Vendor Management - 80%	Maturity of Program - 84%
Maturity of Program - 64%	Maturity of Program - 72%	Vendor Management - 78%
Data Inventory Program - 65%	Data Inventory Program - 69%	Data Inventory Program - 68%
Knowledge of Other Incidents - 74%	Knowledge of Other Incidents - 64%	Knowledge of Other Incidents - 66%
Budget of Privacy Team - 52%	Budget of Privacy Team - 58%	Budget of Privacy Team - 59%
Physical Location of Data Holdings - 59%	Employee Monitoring - 55%	Physical Location of Data Holdings - 57%
Employee Monitoring - 56%	Physical Location of Data Holdings - 47%	Size of Privacy Team - 56%
Interdepartmental Communication - 56%	Interdepartmental Communication - 44%	Employee Monitoring - 54%
Size of Privacy Team - 31%	Size of Privacy Team - 47%	Interdepartmental Communication - 54%
Relationship with Regulators - 37%	Cyberinsurance - 36%	Relationship with Regulators - 52%
Cyberinsurance - 39%	Relationship with Regulators - 25%	Cyberinsurance - 32%

But Companies Are Struggling

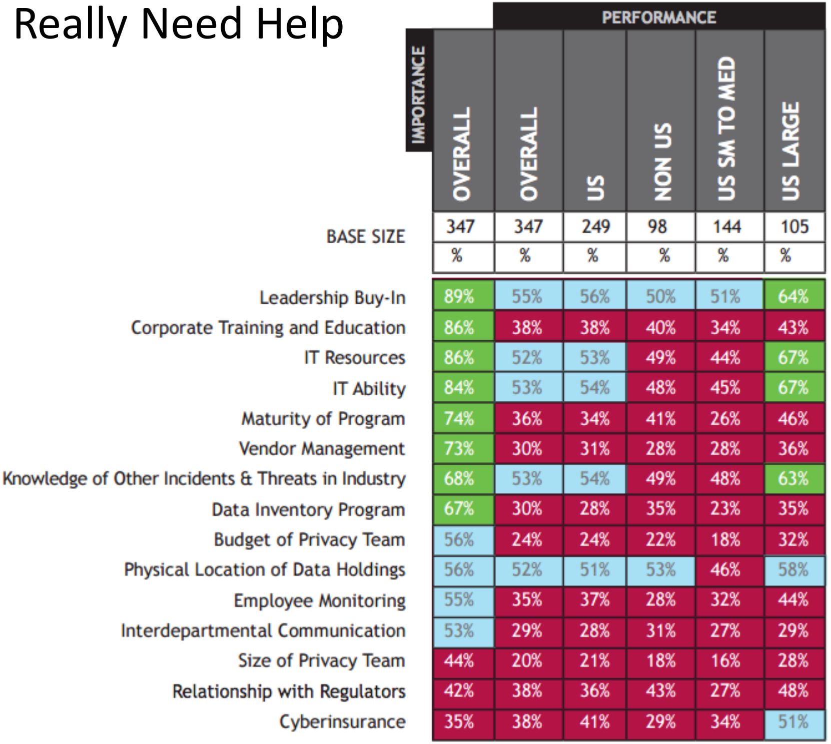
- Mind the Gaps
- Where's the Money?
- SMEs Really Need Help



Worst-performing categories:

(percent responding in bottom two boxes)

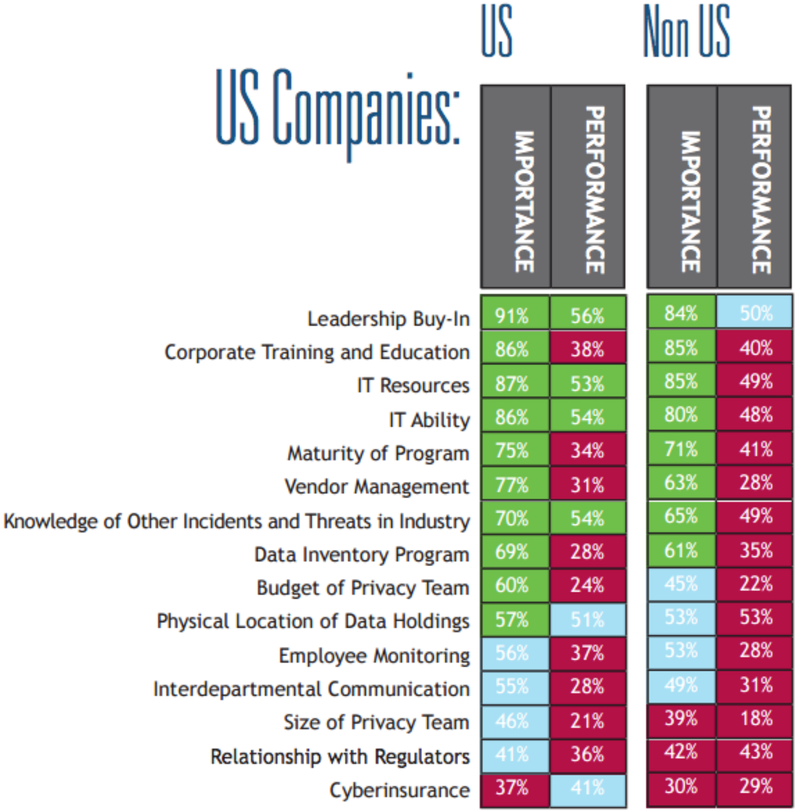
Size of Privacy Team - 49%
Budget of Privacy Team - 37%
Data Inventory Program - 36%
Vendor Management - 31%
Employee Monitoring - 30%
Relationship with Regulators - 27%
Interdepartmental Communication - 27%



	IMPORTANCE	PERFORMANCE				
	OVERALL	OVERALL	US	NON US	US SM TO MED	US LARGE
BASE SIZE	347	347	249	98	144	105
	%	%	%	%	%	%
Leadership Buy-In	89%	55%	56%	50%	51%	64%
Corporate Training and Education	86%	38%	38%	40%	34%	43%
IT Resources	86%	52%	53%	49%	44%	67%
IT Ability	84%	53%	54%	48%	45%	67%
Maturity of Program	74%	36%	34%	41%	26%	46%
Vendor Management	73%	30%	31%	28%	28%	36%
Knowledge of Other Incidents & Threats in Industry	68%	53%	54%	49%	48%	63%
Data Inventory Program	67%	30%	28%	35%	23%	35%
Budget of Privacy Team	56%	24%	24%	22%	18%	32%
Physical Location of Data Holdings	56%	52%	51%	53%	46%	58%
Employee Monitoring	55%	35%	37%	28%	32%	44%
Interdepartmental Communication	53%	29%	28%	31%	27%	29%
Size of Privacy Team	44%	20%	21%	18%	16%	28%
Relationship with Regulators	42%	38%	36%	43%	27%	48%
Cyberinsurance	35%	38%	41%	29%	34%	51%

U.S. vs. the World

- U.S. Sample Is Bigger
- More IAPP Firms are U.S.-Based
- Still, There's Something There



US Companies:

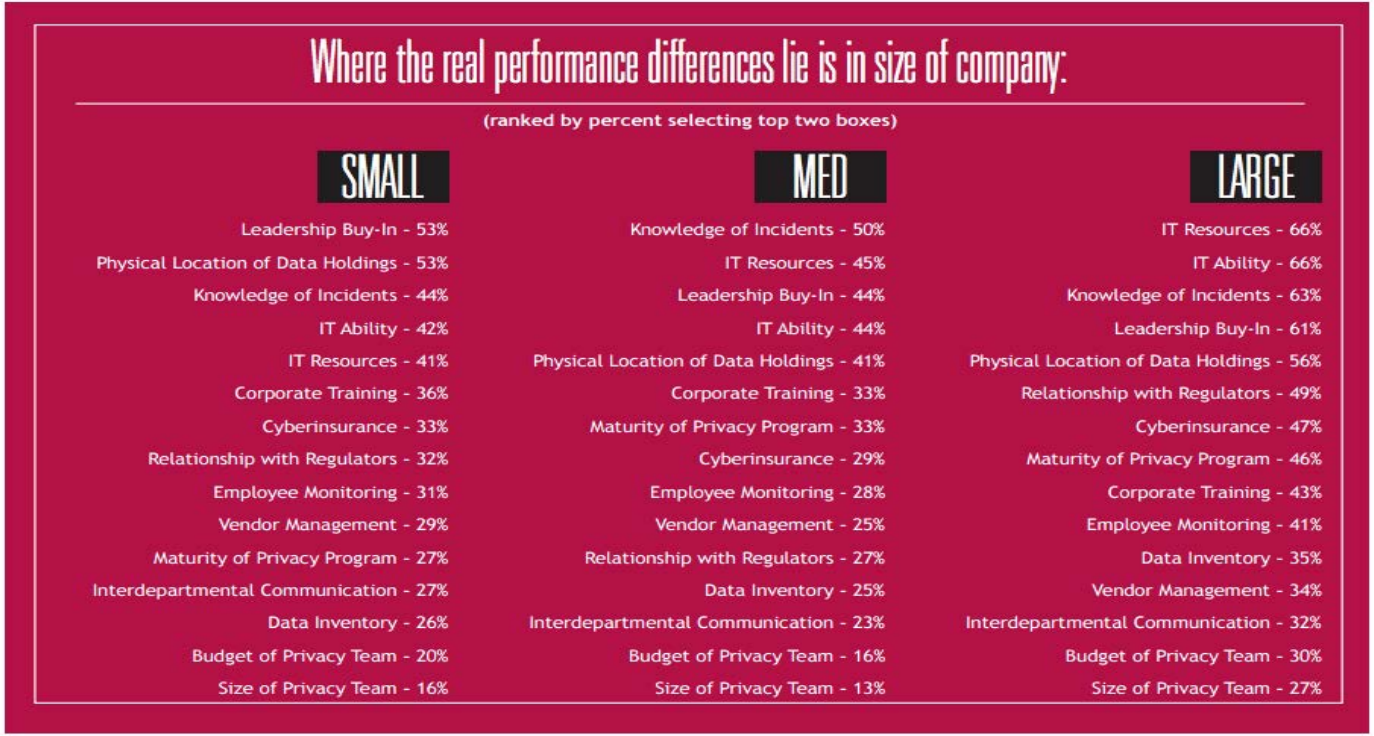
	US		Non US	
	IMPORTANCE	PERFORMANCE	IMPORTANCE	PERFORMANCE
Leadership Buy-In	91%	56%	84%	50%
Corporate Training and Education	86%	38%	85%	40%
IT Resources	87%	53%	85%	49%
IT Ability	86%	54%	80%	48%
Maturity of Program	75%	34%	71%	41%
Vendor Management	77%	31%	63%	28%
Knowledge of Other Incidents and Threats in Industry	70%	54%	65%	49%
Data Inventory Program	69%	28%	61%	35%
Budget of Privacy Team	60%	24%	45%	22%
Physical Location of Data Holdings	57%	51%	53%	53%
Employee Monitoring	56%	37%	53%	28%
Interdepartmental Communication	55%	28%	49%	31%
Size of Privacy Team	46%	21%	39%	18%
Relationship with Regulators	41%	36%	42%	43%
Cyberinsurance	37%	41%	30%	29%

Size Matters

- The Maturity Curve

- Working with IT

- Working with the Regulator



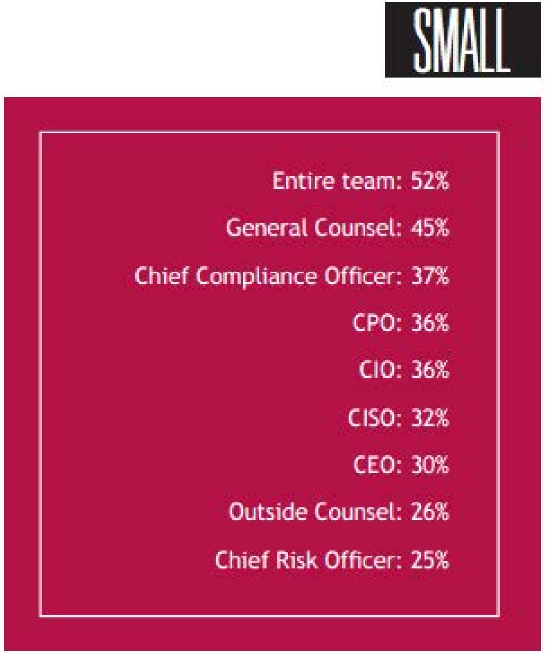
Where the real performance differences lie is in size of company:

(ranked by percent selecting top two boxes)

SMALL	MED	LARGE
Leadership Buy-In - 53%	Knowledge of Incidents - 50%	IT Resources - 66%
Physical Location of Data Holdings - 53%	IT Resources - 45%	IT Ability - 66%
Knowledge of Incidents - 44%	Leadership Buy-In - 44%	Knowledge of Incidents - 63%
IT Ability - 42%	IT Ability - 44%	Leadership Buy-In - 61%
IT Resources - 41%	Physical Location of Data Holdings - 41%	Physical Location of Data Holdings - 56%
Corporate Training - 36%	Corporate Training - 33%	Relationship with Regulators - 49%
Cyberinsurance - 33%	Maturity of Privacy Program - 33%	Cyberinsurance - 47%
Relationship with Regulators - 32%	Cyberinsurance - 29%	Maturity of Privacy Program - 46%
Employee Monitoring - 31%	Employee Monitoring - 28%	Corporate Training - 43%
Vendor Management - 29%	Vendor Management - 25%	Employee Monitoring - 41%
Maturity of Privacy Program - 27%	Relationship with Regulators - 27%	Data Inventory - 35%
Interdepartmental Communication - 27%	Data Inventory - 25%	Vendor Management - 34%
Data Inventory - 26%	Interdepartmental Communication - 23%	Interdepartmental Communication - 32%
Budget of Privacy Team - 20%	Budget of Privacy Team - 16%	Budget of Privacy Team - 30%
Size of Privacy Team - 16%	Size of Privacy Team - 13%	Size of Privacy Team - 27%

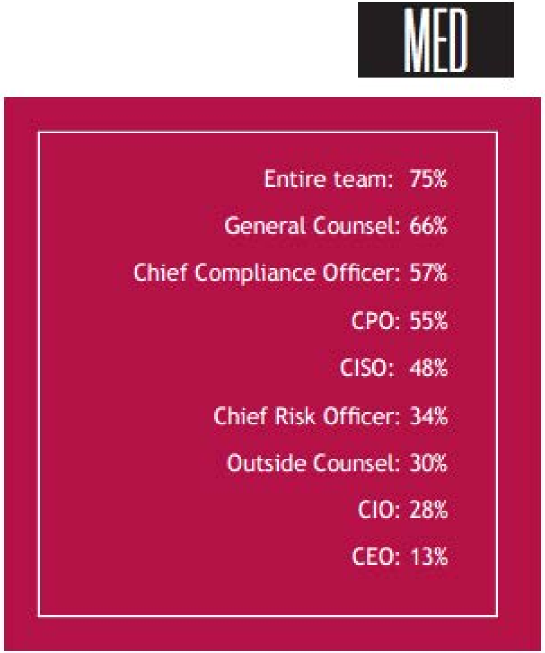
Who’s Doing the Assessing?

- Bringing in Outside Counsel
- CISO v. CPO
- Team Effort



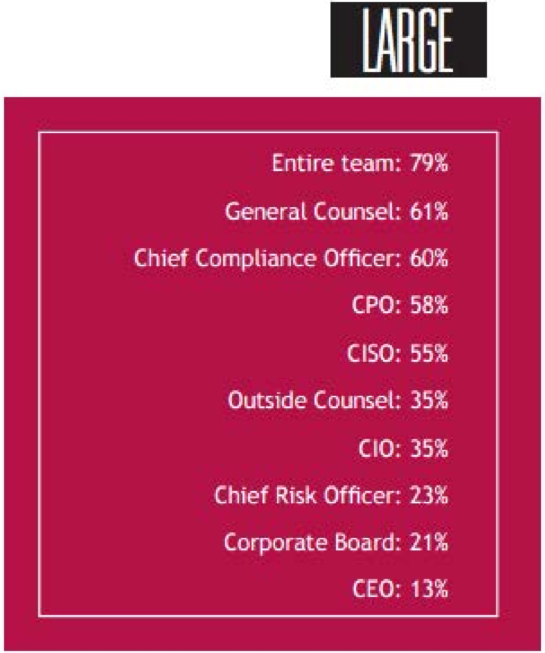
SMALL

Entire team: 52%
General Counsel: 45%
Chief Compliance Officer: 37%
CPO: 36%
CIO: 36%
CISO: 32%
CEO: 30%
Outside Counsel: 26%
Chief Risk Officer: 25%



MED

Entire team: 75%
General Counsel: 66%
Chief Compliance Officer: 57%
CPO: 55%
CISO: 48%
Chief Risk Officer: 34%
Outside Counsel: 30%
CIO: 28%
CEO: 13%



LARGE

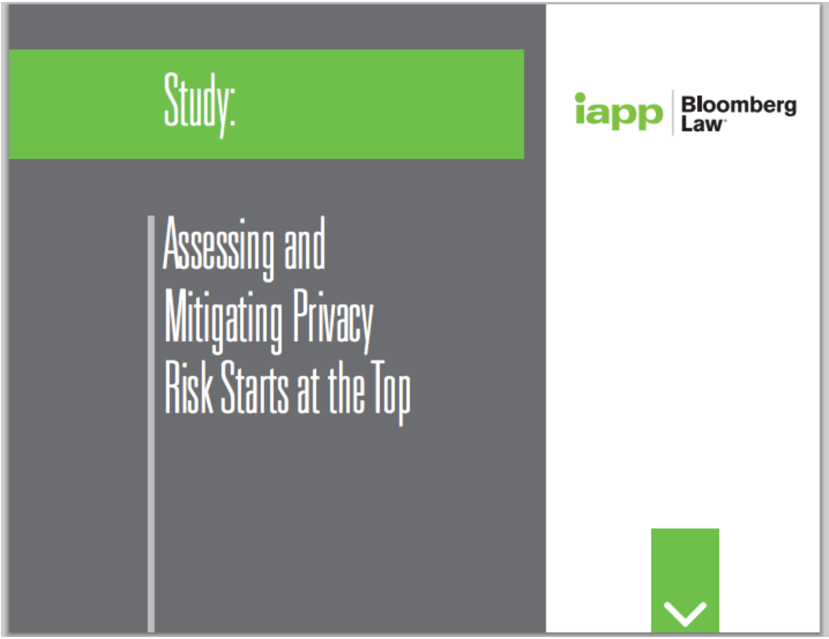
Entire team: 79%
General Counsel: 61%
Chief Compliance Officer: 60%
CPO: 58%
CISO: 55%
Outside Counsel: 35%
CIO: 35%
Chief Risk Officer: 23%
Corporate Board: 21%
CEO: 13%

Risk Conclusions and Applications

- Privacy is a young profession and operation; without executive buy-in it will not be an asset to the company

- How will risk evolve with budget and staff? Most agree throwing money at the problem won't work. Has to be tactical.

- Prepare for the EU General Data Protection Regulation and understand global privacy.



Study:

Assessing and Mitigating Privacy Risk Starts at the Top

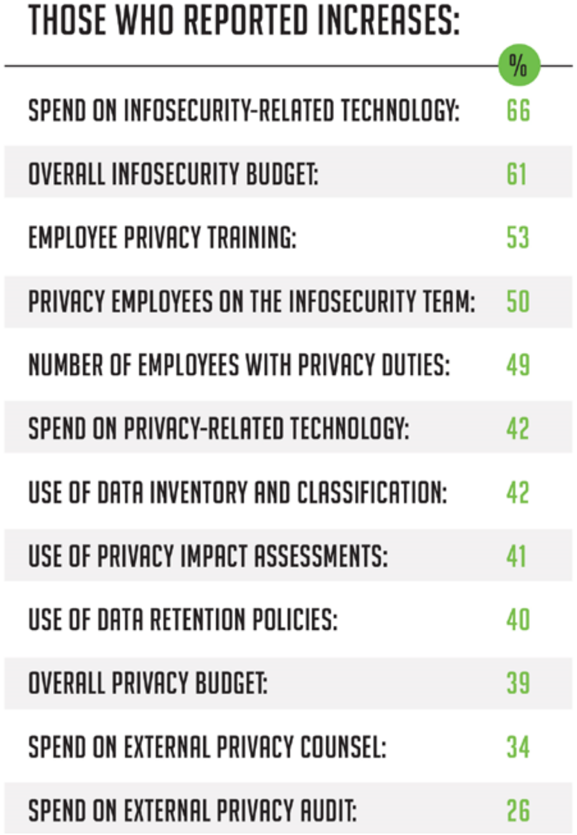
iapp | Bloomberg Law

https://iapp.org/resources/article/study-assessing-and-mitigating-privacy-risk-starts-at-the-top

How IT and Infosec Value Privacy

- Half of all companies have increased the number of privacy pros on the infosecurity team

- Investment in privacy tech is running ahead of external spend on audit and counsel



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

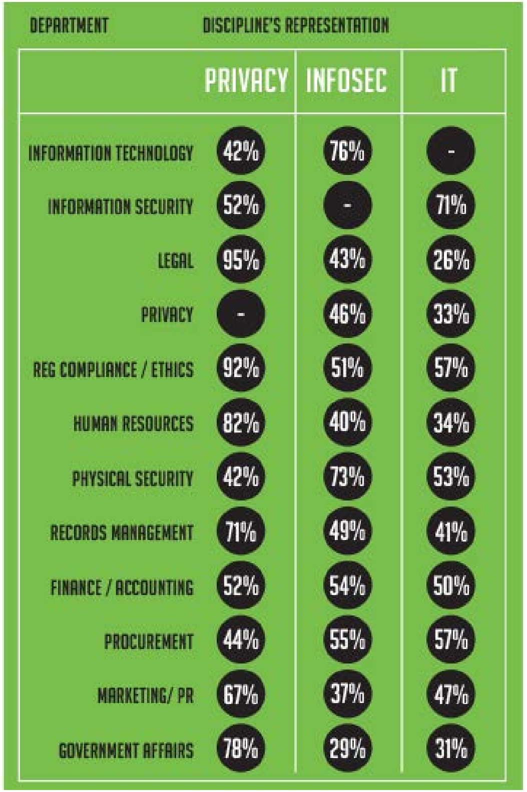
- The Privacy Venn diagram

- More about people than budget

And That Collaboration Is Only Increasing

- Half of all infosec teams now have privacy team members

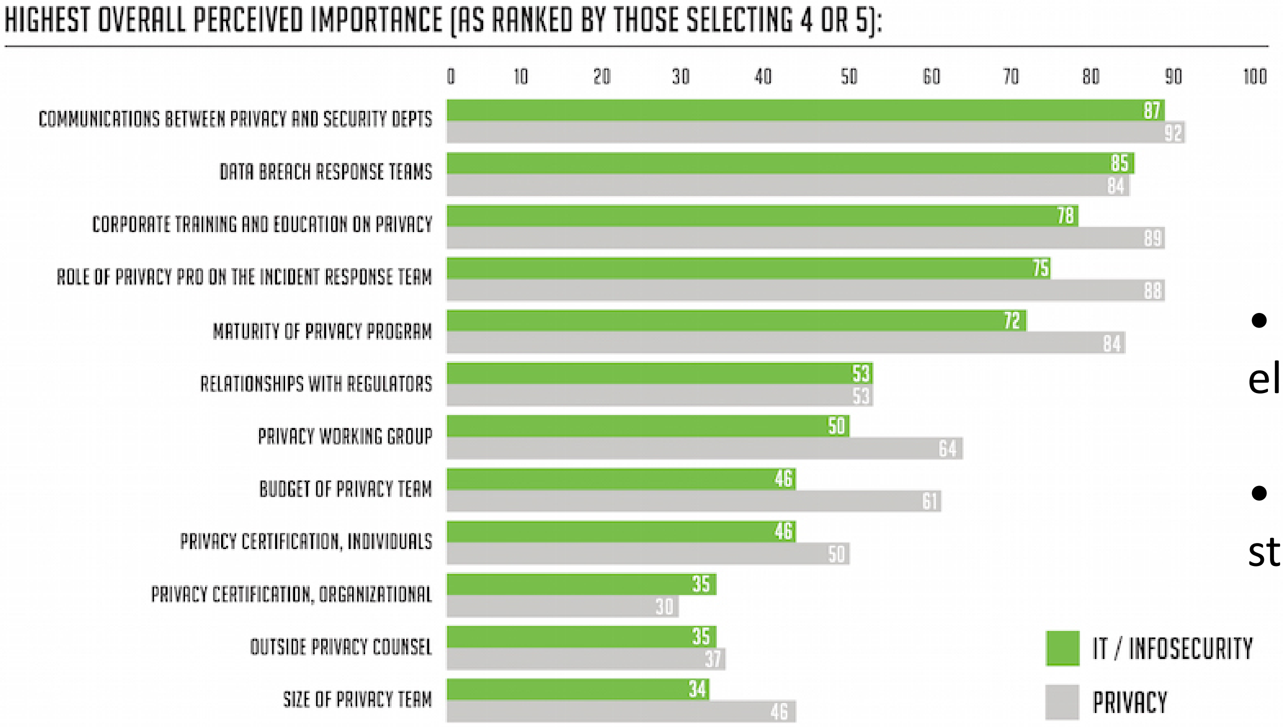
- And vice versa



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%

- Could government affairs use more infosec professionals now that security is becoming more of a policy issue?

It’s the Most Important Thing They Do…

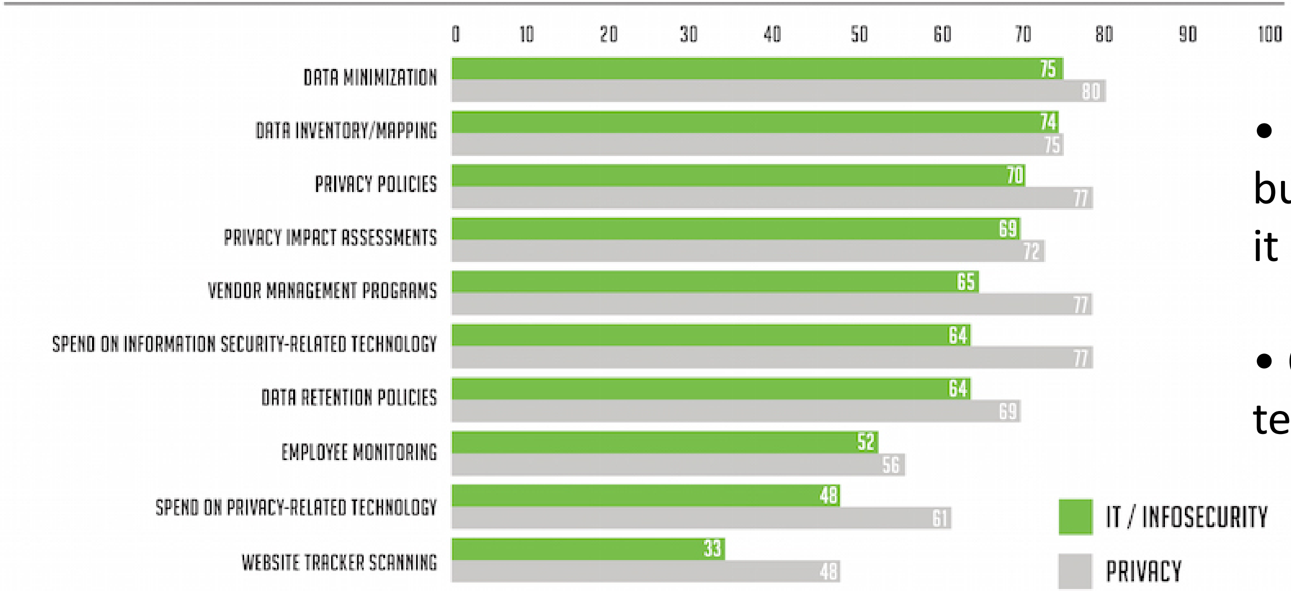


HIGHEST OVERALL PERCEIVED IMPORTANCE (AS RANKED BY THOSE SELECTING 4 OR 5):

- Communication trumps all else – how to do?
- Privacy working group is a start

It’s the Most Important Thing They Do…

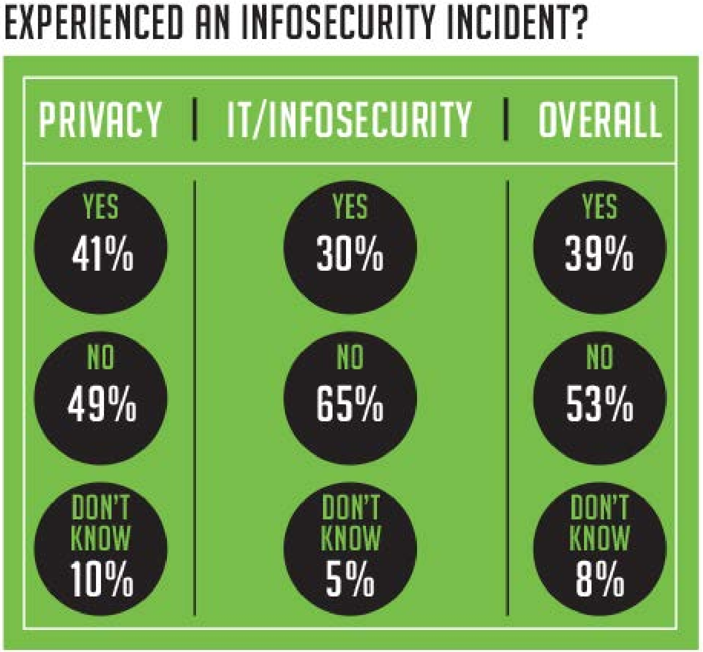
HIGHEST OVERALL PERCEIVED IMPORTANCE (AS RANKED BY THOSE SELECTING 4 OR 5):



- Privacy pros want tech, but feel they’re not getting it from IT?

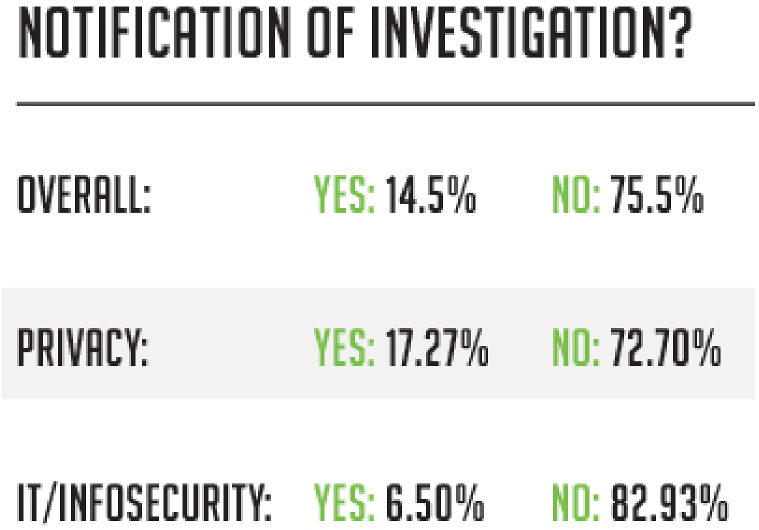
- Or does IT know best that tech can’t solve everything?

How Do Opinions Change When Bad Things…



EXPERIENCED AN INFOSECURITY INCIDENT?

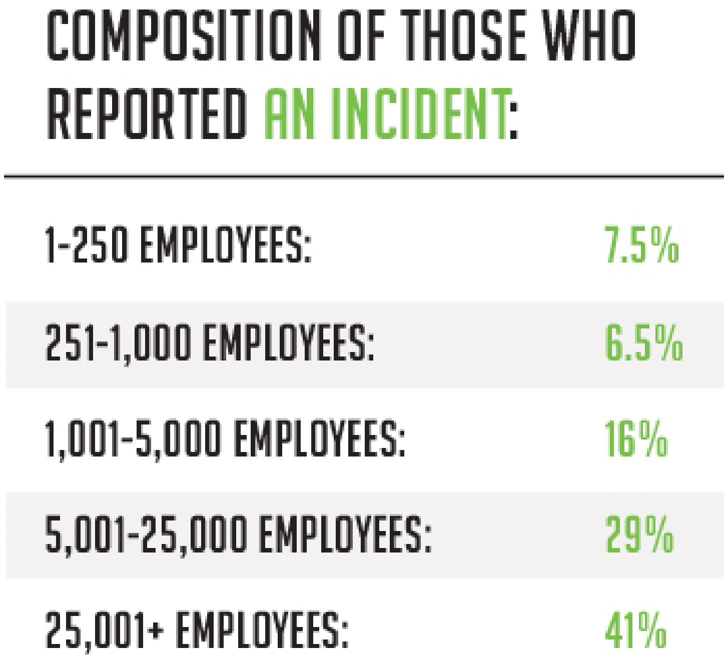
PRIVACY	IT/INFOSECURITY	OVERALL
YES 41%	YES 30%	YES 39%
NO 49%	NO 65%	NO 53%
DON'T KNOW 10%	DON'T KNOW 5%	DON'T KNOW 8%



NOTIFICATION OF INVESTIGATION?

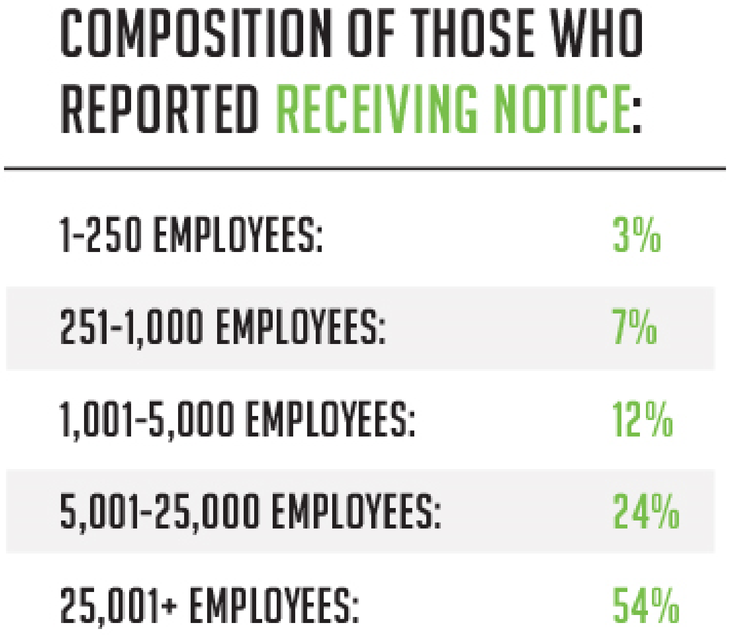
OVERALL:	YES: 14.5%	NO: 75.5%
PRIVACY:	YES: 17.27%	NO: 72.70%
IT/INFOSECURITY:	YES: 6.50%	NO: 82.93%

How Do Opinions Change When Bad Things…



COMPOSITION OF THOSE WHO REPORTED AN INCIDENT:

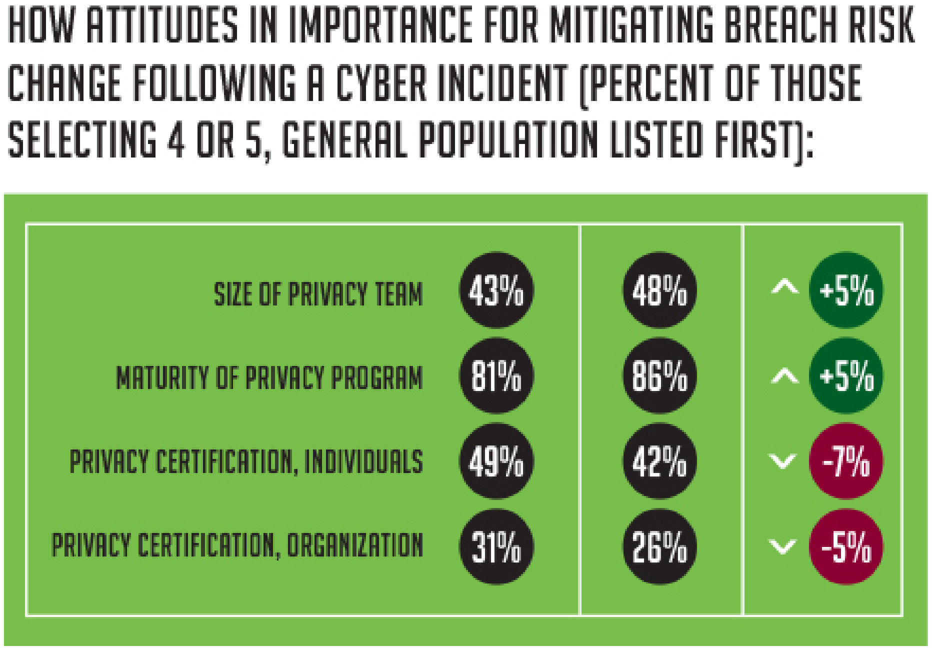
1-250 EMPLOYEES:	7.5%
251-1,000 EMPLOYEES:	6.5%
1,001-5,000 EMPLOYEES:	16%
5,001-25,000 EMPLOYEES:	29%
25,001+ EMPLOYEES:	41%



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 Opinions Change When Bad Things…



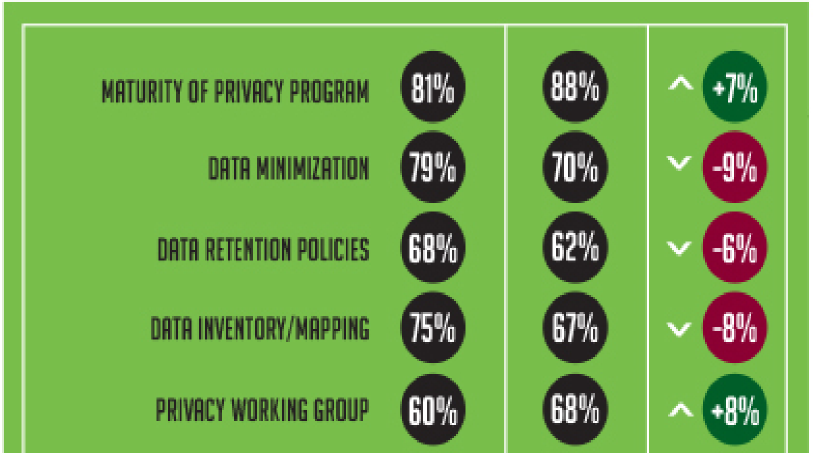
HOW ATTITUDES IN IMPORTANCE FOR MITIGATING BREACH RISK CHANGE FOLLOWING A CYBER INCIDENT (PERCENT OF THOSE SELECTING 4 OR 5, GENERAL POPULATION LISTED FIRST):

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

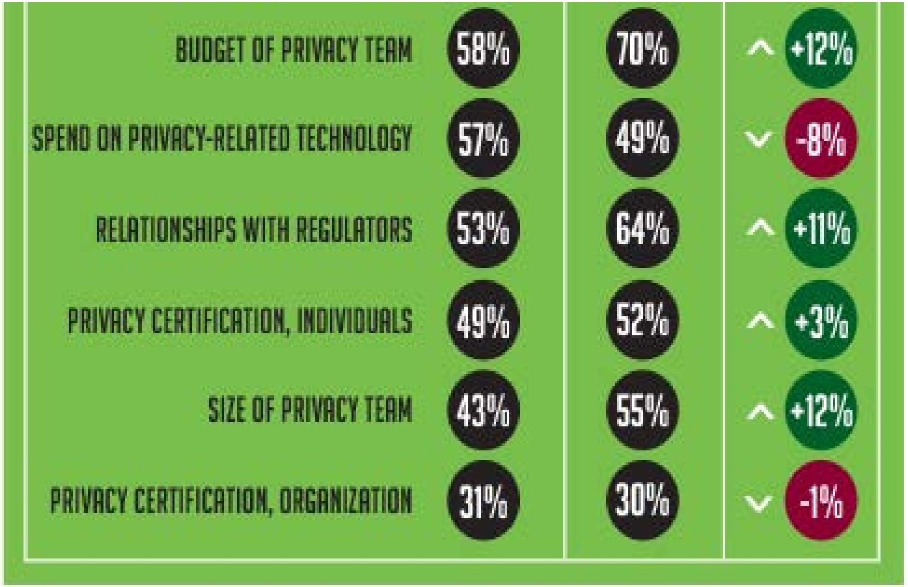
- Priorities change almost not at all
- The only change in action was an increase in security tech spending

How Do Opinions Change When Bad Things…

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):



MATURITY OF PRIVACY PROGRAM	81%	88%	↑ +7%
DATA MINIMIZATION	79%	70%	↓ -9%
DATA RETENTION POLICIES	68%	62%	↓ -6%
DATA INVENTORY/MAPPING	75%	67%	↓ -8%
PRIVACY WORKING GROUP	60%	68%	↑ +8%

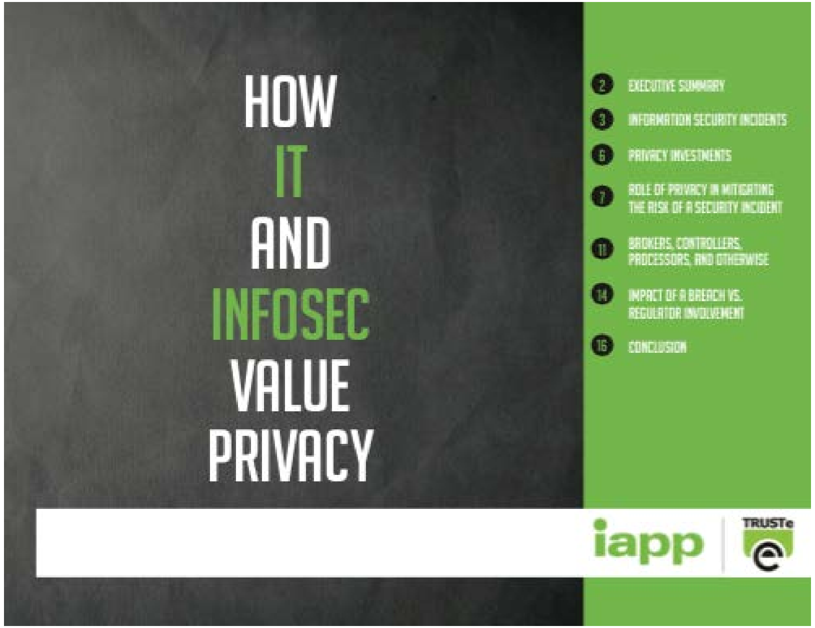


BUDGET OF PRIVACY TEAM	58%	70%	↑ +12%
SPEND ON PRIVACY-RELATED TECHNOLOGY	57%	49%	↓ -8%
RELATIONSHIPS WITH REGULATORS	53%	64%	↑ +11%
PRIVACY CERTIFICATION, INDIVIDUALS	49%	52%	↑ +3%
SIZE OF PRIVACY TEAM	43%	55%	↑ +12%
PRIVACY CERTIFICATION, ORGANIZATION	31%	30%	↓ -1%

How Do Opinions Change When Bad Things…

- When the regulator comes calling, we see a new emphasis on privacy operations
- Breaches are about more than the data lost
- Sound policy before and after a breach can keep a notice from becoming a full investigation

Applying IT and Infosec Findings



HOW IT AND INFOSEC VALUE PRIVACY

iapp | TRUSTe

https://iapp.org/resources/article/how-it-and-infosec-value-privacy/

Make the privacy opps easier: Get out of the Word file era

Get your people talking: Populate your working group; build your teams

Train your organization: Budgets and teams are small; make everyone part of the team

Sam Pfeifle @DailyDashboard
IAPP
sam@iapp.org