2018 WME Privacy Results

Prepared for the BELA Community
July 2018

Contents

- WMEC Benchmark Data Set
- WMEC Ethics Quotient™ Survey Results

World's Most Ethical Companies as Benchmark Data Set

This Report contains data points from Ethisphere's 2018 World's Most Ethical Companies ("WMEC") data set. This data set provides insights into the programs and practices of leading companies from around the world. The dataset referenced through the Report ("WME Honorees") is comprised of 135 companies.

The Benchmark data set is presented to provide a comparative view into the practices of leading companies. For the full list of WMEC companies visit: http://worldsmostethicalcompanies.ethisphere.com/honorees

Privacy

Corporate Governance
Board Training

EQ 3.25. On which topics do directors on your Board receive education or training (separate from the Code)?

Topics	As part of on-boarding or orientation	Education or training on topic included as part of compliance program updates	As part of documented, periodic training initiatives
Anti-trust law	61%	64%	37%
Anti-bribery	59%	79%	44%
Policies regarding confidential information	68%	57%	38%
Policies regarding conflicts of interest	81%	65%	39%
Executive Compensation Trends and Developments	39%	51%	53%
Fiduciary duty	82%	36%	42%
Policies regarding gifts and entertainment	67%	71%	34%
Regulations or trends regarding preventing human trafficking	37%	65%	39%
Risks or regulations regarding information security/cyber security	44%	76%	57%
Policies regarding insider trading	84%	62%	40%
Privacy regulations	45%	77%	39%
Trends and risks regarding the need to protect those who report suspected misconduct	50%	80%	48%
Trends and risks regarding social media	31%	58%	51%
Updates on industry or economic trends or risks	46%	62%	57%
Updates on significant regulatory changes	35%	71%	56%

Program Resources and Structure
Ensure Fulsome Information is Provided to the Audit Committee and Board

EQ 4A.14 Indicate which information your company reports to the Board.

Topics	All Honorees Data
Compliance and ethics program performance	99%
Overview of key initiatives	99%
Hotline and misconduct reporting statistics	100%
Details on misconduct investigations and resolutions	97%
Initiatives and results	98%
Communication initiatives	96%
Program audit findings	97%
Risk assessment findings	98%
Risk mitigation strategy and tactics	97%
Privacy risk assessment and results	86%
Updates relating to the information security plan	93%
Culture of ethics assessment or survey findings	94%
Regulatory and legal updates	98%
Compliance and ethics trends, industry trends, and best practices updates	94%
Code of Conduct updates or revisions	100%
Other	44%

Program Resources and Structure
Consider forming an Audit Committee

EQ 4A.18 Indicate which topics are regularly discussed during the internal compliance and ethics committee

Topics	All Honorees Data
Overall program performance and key program initiatives	96%
Hotline and reporting statistics	95%
Misconduct investigations and resolutions	92%
Compliance and ethics training and communication initiatives	96%
Compliance and ethics program assessment	92%
Compliance and ethics program benchmarking against practices of other companies	92%
Compliance and ethics risk management	96%
Culture of ethics	94%
Significant regulatory and legal updates	97%
Information security	85%
Privacy risk management	83%
Industry trends and best practices updates	95%
Other topics	42%

Written Standards
Written Policies by Risk Topic

EQ 4C.5 Select the risk topics from the list below that are addressed in your company's written policies separate from the Code.

Topics	All Honorees Data
Information security	100%
Gifts and entertainment	99%
Equal employment opportunity	99%
Data privacy	99%
Workplace health and safety	99%
Confidential information	99%
Procurement integrity	98%
Workplace harassment	97%
Social media	97%
Records management	97%
Fair employment	96%
Conflicts of interest	96%
Financial integrity	96%
Non-retaliation	96%
Protecting company assets	95%
Anticorruption	94%

Risk Assessment, Monitoring & Auditing
Risk Topic Review

EQ 4D.5 Which of the following types of risks are reviewed by your company?

Topics	As part of a standalone E&C Risk Assessment	As part of an ERM risk assessment without significant involvement of the E&C Function	As part of an ERM risk assessment without significant involvement of the E&C Function
Financial integrity and fraud	51%	65%	20%
Information technology security	40%	63%	29%
Data privacy laws and regulations relevant to employee, customer, or consumer data	56%	64%	16%
Anticorruption/bribery	68%	59%	7%
Conflicts of interest	69%	49%	9%
Gifts and entertainment	70%	51%	7%
Confidential information	54%	64%	13%
Equal employment opportunity/diversity/discrimination	41%	51%	29%
Procurement integrity/dealing with supplier/supply chain oversight	49%	66%	22%
Workplace health and safety	41%	50%	35%
Workplace harassment	51%	53%	20%
Fair employment/labor standards	40%	49%	33%
Misuse of company assets	51%	59%	18%
Non-retaliation policy and/or whistleblower protections	69%	50%	9%
Intellectual property	42%	55%	27%
Antitrust/competition	54%	58%	15%

Risk Assessment, Monitoring & Auditing
InfoSec Program

EQ 4D.8 Select the following that are included in your company's Information Security Program. Note that the Information Security Program may consist of more than one document or policy. (Multiple select)

Topics	All Honorees
Documented incident response plan	99%
Documentation of processes or procedures to mitigate the company's potential data security risks	98%
Documented regular monitoring and testing of the company's systems	98%
Use of intrusion prevention systems	98%
Documented management oversight and approval of the Information Security Program	97%
Documentation of the company's potential privacy or data security risks (i.e., the results of the risk assessment)	96%
An individual designated as the company's security officer	96%
Documentation of how the company assesses privacy or data security risk (i.e., the process for conducting a risk assessment)	94%
Documented procedures or requirements for selecting third parties that store, process, transmit or access sensitive information on behalf of the company	94%
Documented policy as to how and when data will be destroyed	94%
Documented business continuity management plan	93%
Documented procedures or requirements for due diligence into and contractual language requirements that will be required for engagements with third parties that store, process, transmit or access sensitive information on behalf of the company	92%
Encryption of sensitive data stored on all laptops	92%
Documented policy as to how and when data storage devices such as flash drives may be used	87%
Documentation of laws and regulations applying to the company's information collection, use, storage, sharing, protection, retention and disposal practices	85%
Board approval for the Information Security Program	82%

Training & Communications
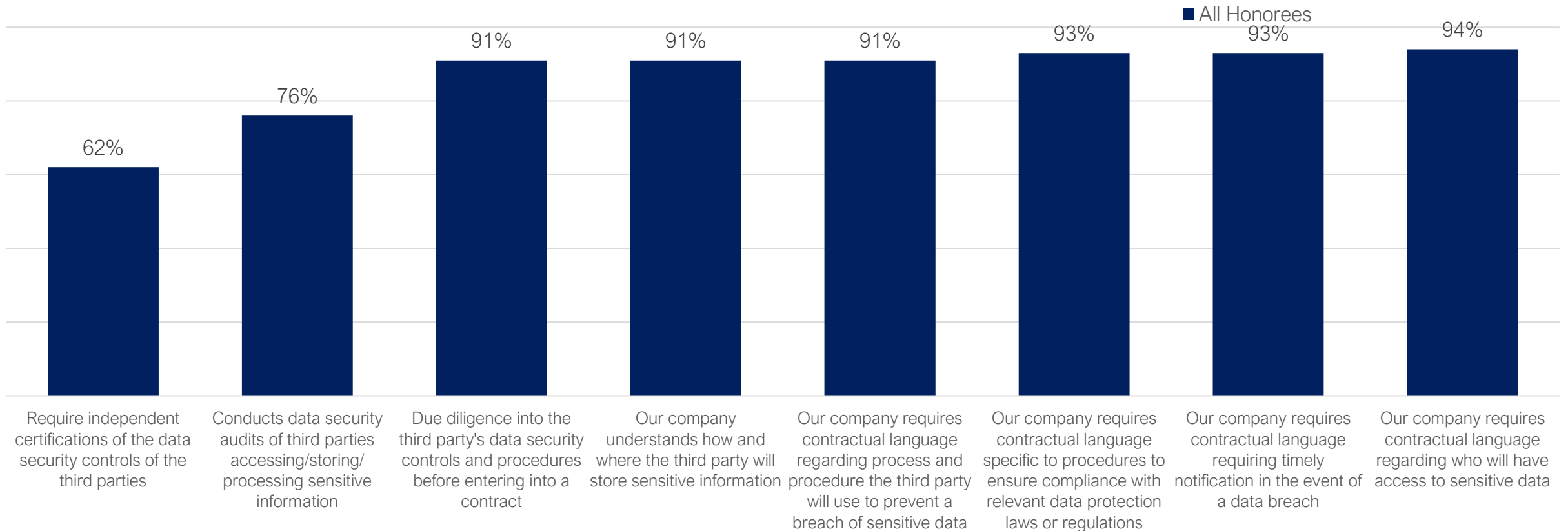## *Adopt Additional C&E Training Best Practices*

EQ 4E.6 Risk-specific training programs administered to employees:

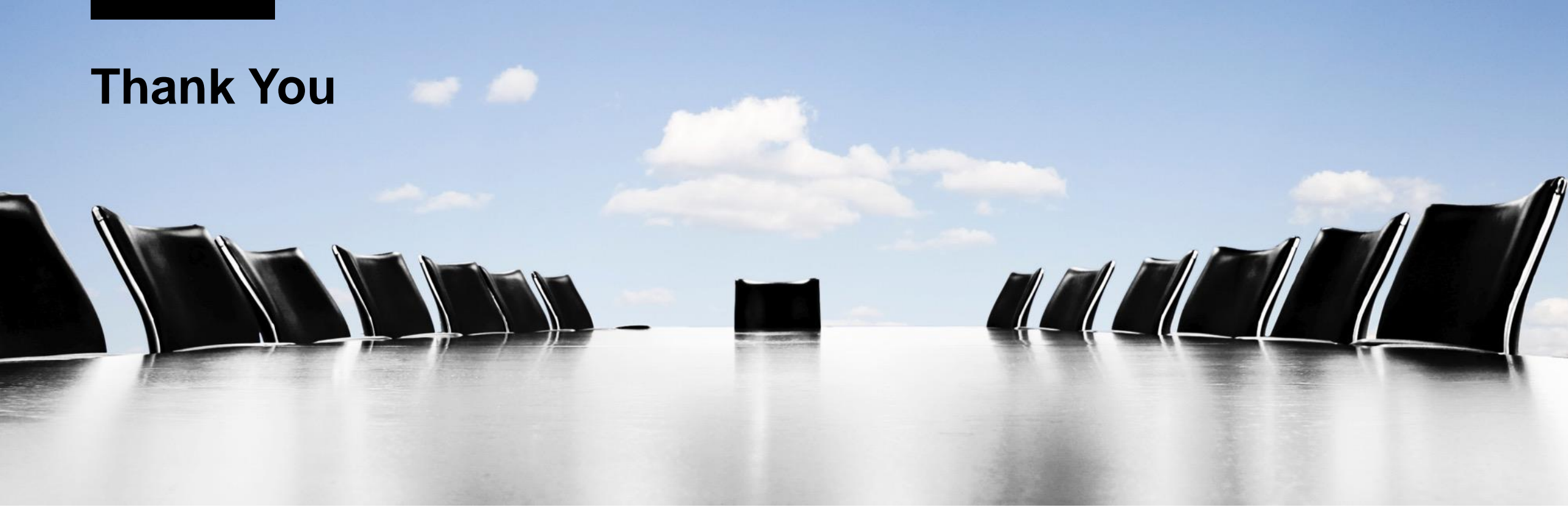| Topics	Training Delivered On-Demand Using Online Modalities	Training Delivered Live Using Online Modalities	Training Delivered Using In-Person Training Sessions
Gifts and entertainment	79%	42%	65%
Workplace harassment	80%	39%	59%
Data privacy laws and regulations	85%	43%	62%
Equal employment opportunity	80%	39%	55%
Information technology security	87%	41%	56%
Non-retaliation policy	76%	37%	64%
Workplace health and safety	81%	42%	70%
Anticorruption	81%	45%	71%
Confidential information	80%	39%	59%
Conflicts of interest	68%	39%	56%
Financial integrity	71%	35%	55%
Procurement integrity	60%	30%	56%
Social media	68%	28%	41%
Insider trading	59%	21%	36%
Political contributions	48%	21%	39%
Antitrust	58%	33%	56%

Risk Assessment, Monitoring & Auditing
Managing Third Party Security Risks

4F.28 Indicate how your company manages privacy and data security risks relating to third parties that store, process, transmit or access sensitive information on behalf of the company. Multiple select)

■ All Honorees

Category	Percentage
Require independent certifications of the data security controls of the third parties	62%
Conducts data security audits of third parties accessing/storing/processing sensitive information	76%
Due diligence into the third party's data security controls and procedures before entering into a contract	91%
Our company understands how and where the third party will store sensitive information	91%
Our company requires contractual language regarding process and procedure the third party will use to prevent a breach of sensitive data	91%
Our company requires contractual language specific to procedures to ensure compliance with relevant data protection laws or regulations	93%
Our company requires contractual language requiring timely notification in the event of a data breach	93%
Our company requires contractual language regarding who will have access to sensitive data	94%

Thank You

Contact Your BELA Director of Engagement:

Sarah Neumann
sarah.neumann@ethisphere.com
(651) 260-8263

Amy Volpe
amy.volpe@ethisphere.com
(917) 796-5114

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®