ETHISPHERE

INSIGHTS INTO CYBERSECURITY

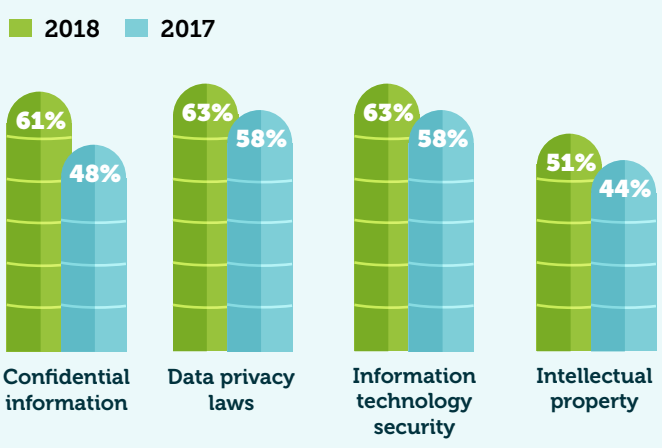
from THE WORLD'S MOST ETHICAL COMPANIES

Ethisphere, as the global leader in defining and advancing the standards of ethical business practices, features data and insights on Cybersecurity from companies featured among the 2018 World's Most Ethical Companies (WME) data set.

Breaking Cybersecurity Out of the IT Silo

WME Honorees understand cybersecurity is no longer just the domain of the IT department and should be part of broader Enterprise Risk Management (ERM) discussions. With increased involvement of the Ethics and Compliance function, ERM programs frequently include confidential information, data privacy laws, IT security and intellectual property as part of the overall ERM program.

Risk types reviewed by Honorees as part of an ERM process with significant involvement of the E&C function



Addressing Third Party Risk

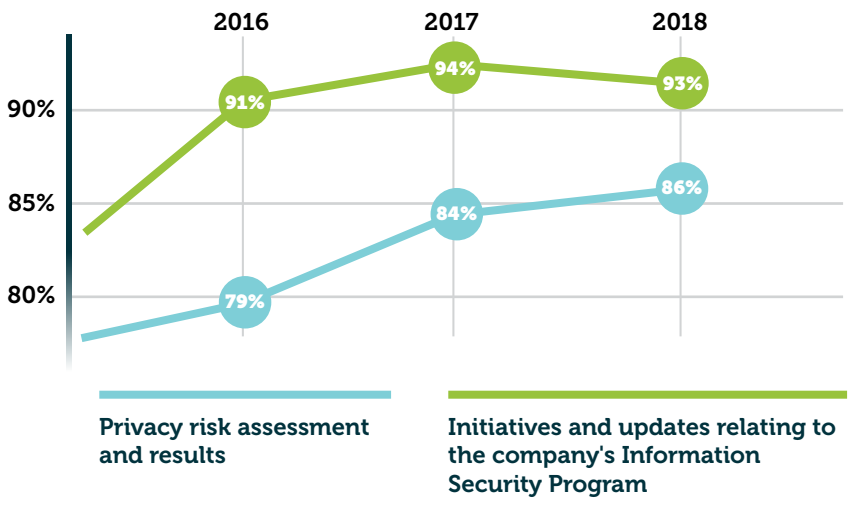
To help mitigate third party data security risks, **84 percent** of WME Honorees consider data security practices as part of the Ethics and Compliance due diligence process. Additionally, **76 percent** of WME Honorees conduct data security audits of third parties that access and store sensitive information on behalf of the company.

Engaging with Boards

WMEs recognize the importance of engaging and training the Board on cyber readiness, data security, and privacy standards. During programmatic updates to the Board, **68 percent** of WME Honorees provide Board Directors education on cybersecurity and **53 percent** provide education on privacy regulations.

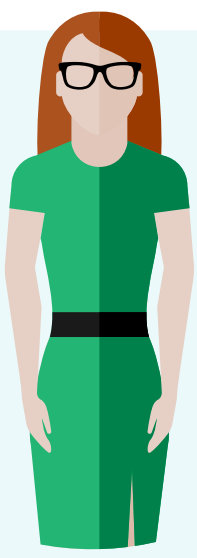
Reporting on Cybersecurity

Ethisphere has observed an increase in Honorees reporting updates about the organizations' information security program and privacy risk assessments to the Board of Directors. This speaks to the heightened attention cybersecurity matters now garner at the highest levels of organizational stewardship.



Training Employees

Honorees are increasingly providing their employees with the necessary education to combat modern-day cybersecurity risks. This includes robust, targeted, and risk-specific training programs on topics such as protecting confidential information and information technology security, among other topics.



Confidential information
2018 - 81% **2017 - 73%**

Data privacy laws
2018 - 86% **2017 - 74%**

Information technology security
2018 - 88% **2017 - 78%**

Intellectual property
2018 - 56% **2017 - 44%**

Records management and retention
2018 - 59% **2017 - 52%**

Learn how Ethisphere and CREATe Compliance can help you assess, benchmark and improve your cybersecurity program.

info@ethisphere.com 888-229-3207

www.ethisphere.com

CREATe Compliance
An ETHISPHERE Business

Top Five Steps to Becoming More

CYBER SECURE

CREATe Compliance, an Ethisphere business, works with global companies to assess and improve cybersecurity programs. Based on this experience, here are the top five steps companies can take to improve the "people, processes and technology" fundamentals required for effective cybersecurity risk management and information security.

1 Take a cross-functional approach.

Cybersecurity is no longer just the domain of the information technology (IT) department. Prevention and the response to breaches should involve a variety of roles throughout an organization, from legal and compliance teams to risk managers, communications, IT and human resources.

2 Consider cyber threats as part of broader enterprise risk management (ERM) programs.

A risk-based approach helps to focus resources on top priorities. An analysis of threats and consequences of a breach can inform decisions.

3 Identify your most critical information.

What and where are your company's crown jewels? It's important to identify your most valuable information, know where it's located and who has access to it. Then put appropriate controls in place to protect it.

4 Address insider and third party risk.

Insiders – employees, contractors, consultants, business partners and other third parties – are the most likely source of a cyber breach and they are also your first line of defense. Make sure you have policies in place, training, and processes for on-boarding and off-boarding, among other actions.

5 Align with external standards and best practices.

When reporting to senior management, a useful approach is to reference established guidance and standards, such as the NIST Cybersecurity Framework – a voluntary, flexible approach consisting of standards, guidelines, and best practices.

Learn how Ethisphere and CREATe Compliance can help you assess, benchmark and improve your cybersecurity program.

info@ethisphere.com 888-229-3207

www.createcompliance.com