



Digital Risk Management Survey Finds Most Companies Improperly Resourced to Address Cybersecurity

Updated 03 October 2018

The cyber risk landscape is quickly evolving, but organizations are slow to catch up with the new threat landscape, according to the 2018 State of Digital and Social Media Risk Management survey. Organizations are still organized to focus primarily on more traditional cyber risk management, are not updating their processes and policies or investing in tools and technologies to comprehensively address the latest- and fastest-growing threats coming from digital and social media.

While there has been a rise in organizations investing in tools and technologies to specifically identify and address social media risks, this still represents a minority, and companies are not organized or properly resourced to comprehensively address cyber security in a digital world. Only a small fraction of companies have a fully mature, optimized, resourced program to comprehensively address and manage today's cyber risk landscape. These were among the key findings of a survey of more than 250 companies across a wide range of industries to track how they perceive and manage digital and social media risks today.

“Cyber criminals are looking for every possible way to exploit an enterprise. As security teams protect against these emerging digital threats, relevancy and automation are key to filtering out noise and delivering actionable threat detection in real-time,” said Dan Nadir, Vice President of Digital Risk, Proofpoint.

“The 2018 State of Digital and Social Media Risk Management,” now in its second year, was conducted by JEM Consulting & Advisory Services, a Silicon Valley-based management consultancy focused on digital and social media. The study, sponsored by Proofpoint, highlights trends and best practices for digital and social media risk management and provides a useful resource for teams responsible for managing the growing number and types of digital and social media risks in their organizations.

This year’s survey also asked about General Data Protection Regulation (GDPR) compliance, and discovered that many organizations either overestimate their GDPR compliance or underestimate the need to comply. Respondents were asked about their GDPR-readiness. Forty-one percent of respondents said they were ready and 38 percent said they would be ready. Nine percent said they didn’t believe that GDPR was relevant to them and three percent were not aware of GDPR. Only nine percent of respondents said they were not ready to comply with GDPR by the deadline. Yet, more than a quarter of respondents did not have a data protection or privacy program or any programs to educate their employees about data security, privacy and data protection policies and risk mitigation just a few weeks prior to the May 25th GDPR-compliance deadline.

Cyber risks are ever evolving and cyber risk management must evolve as well to truly ensure security, privacy and data protection. Organizations can improve their digital risk management by focusing on people, process and technology. Senior leadership and boards need to better understand the evolving cyber risk landscape and the importance of protecting their organizations from digital and social media risks in addition to more traditional cyber threats.

Additional findings from this research will be made available through a forthcoming edition of *SNCR 2020: Exploring New Communications Tools and Technologies*.

AUTHORS



Jennifer McClure
**Distinguished Principal
Fellow, Marketing &
Communications Center**
The Conference Board

The Conference Board is the Member-driven think tank that delivers *Trusted Insights for What's Ahead*[®]. Founded in 1916, we are a nonpartisan, not-for-profit entity holding 501(c)(3) tax-exempt status in the United States.

© 2025 The Conference Board, Inc.