PwC's 2014 Annual Corporate Directors Survey

Trends shaping Governance and the board of the future

IT and cybersecurity oversight

pwc

Table of contents

Please note: Charts may not all add to 100 percent due to rounding

The influence of emerging IT

The influence of emerging technologies and increasing cybersecurity concerns are two trends impacting governance and the board of the future. It's clear that employees' use of their personal mobile devices, computers, and social media as they do their jobs, together with the increased use of cloud computing services are changing the relationship between "old line" IT organizations and the business as a whole. A lot of back office IT infrastructure has been displaced. More and more companies and directors see IT as inextricably wed to corporate strategy and the company's business. IT is now a business issue, not just a technology issue.

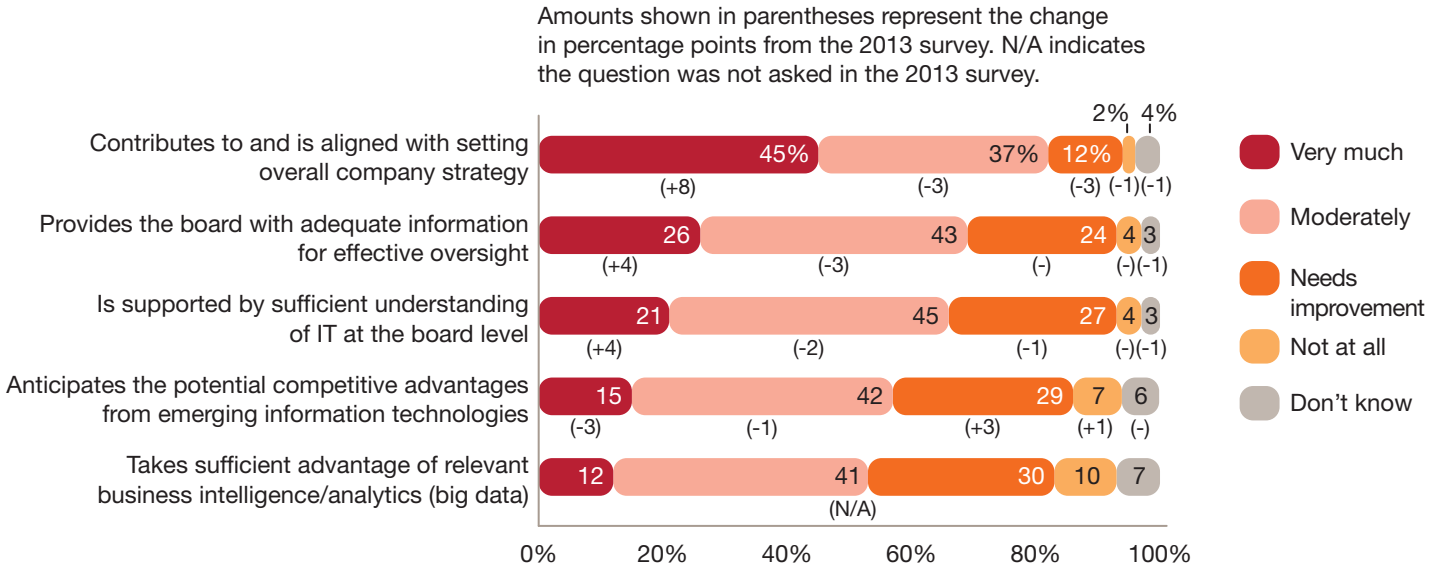
Cybersecurity breaches are regularly and prominently in the news. And directors are increasingly focused on how to provide effective oversight in this area.

IT strategy and risk mitigation

There was a noteworthy year-over-year increase in directors' satisfaction with their company's IT strategy and IT risk mitigation approach. More directors now believe their company's approach very much contributes to, and is aligned with, setting overall company strategy as well as providing the board with adequate information for effective oversight. A greater percentage also believe that their company's approach is supported by a sufficient understanding of IT at the board level. However, there was a decline in the percentage of directors who believe their company's approach "very much" or "moderately" anticipates competitive advantages from emerging information technologies. This may be due to increased awareness of the potential opportunities afforded by using big data and cloud computing as tools.

Directors with longer tenure are more likely to believe the company's IT strategy and IT risk mitigation approach contributes to and is aligned with overall company strategy.

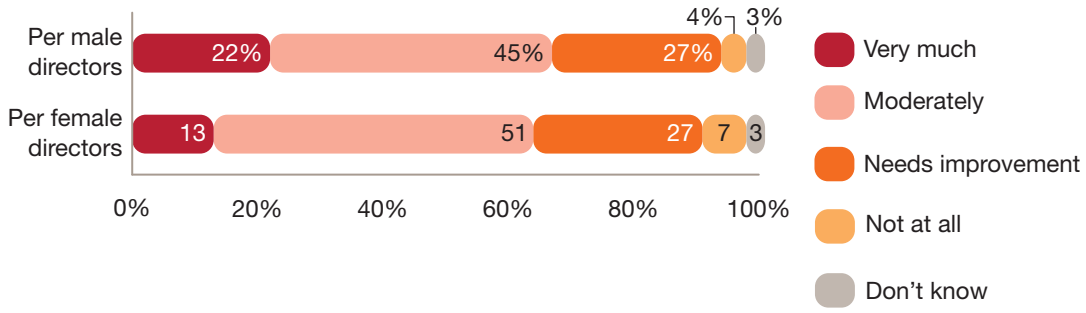
Do you believe your company's IT strategy and IT risk mitigation approach:



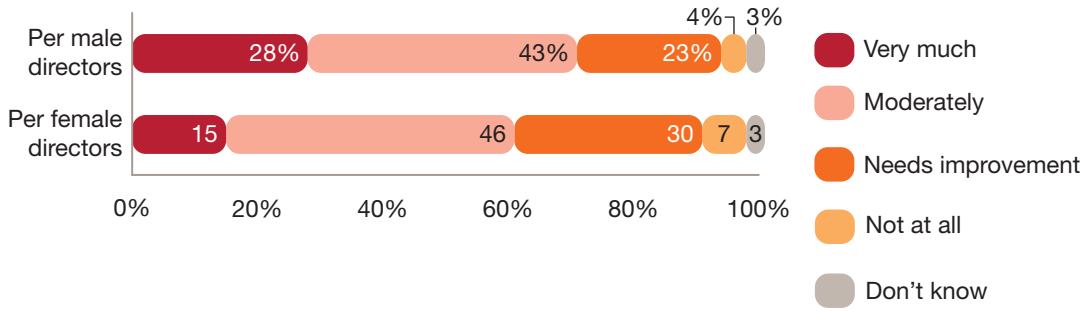
Female directors are more skeptical about whether their company's IT strategy and IT risk mitigation approach is supported by a sufficient understanding of IT at the board level and whether the approach provides the board with adequate information for effective oversight.

Do you believe in your company's IT strategy and IT risk mitigation approach:

Is supported by sufficient understanding of IT at the board level



Provides the board with adequate information for effective oversight



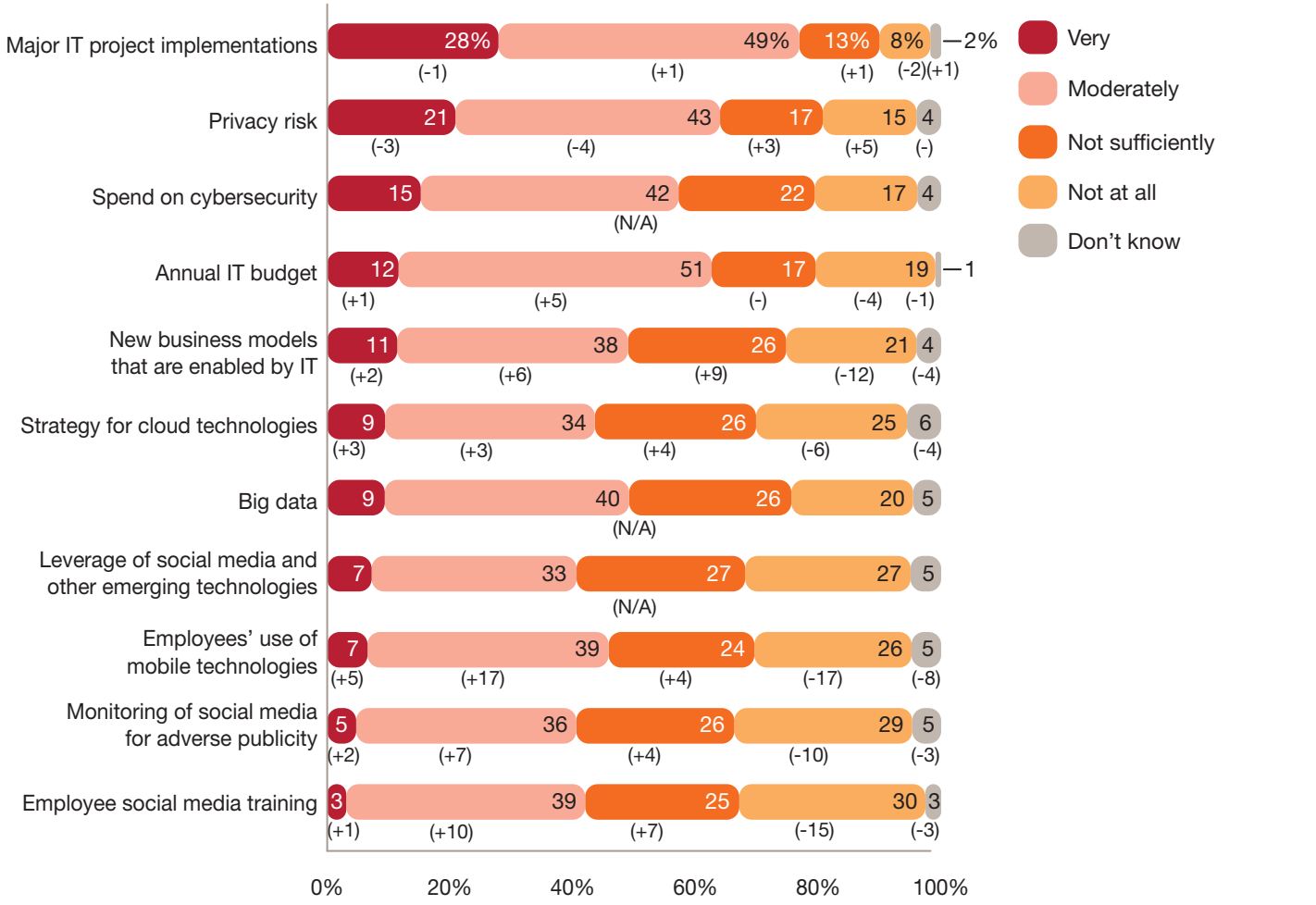
IT oversight beyond the basics

During the last two years directors indicated high levels of engagement with traditional IT areas like overseeing the annual IT budget and the status of major IT project implementations. They are now also indicating an increased focus on certain less-traditional IT areas such as social media and employee use of mobile technologies. Forty-one percent of directors say they are now at least "moderately" engaged in overseeing the company's monitoring of social media for adverse publicity—compared to only 32% in 2012. There was also an 11 percentage point increase in directors who say they are at least "moderately" engaged in overseeing employee social media training and policies. Similarly, 46% of directors say they are now at least "moderately" engaged in overseeing employee use of mobile technologies (compared to 24% two years ago). This increased focus may be recognition by directors of the importance of these emerging technologies on their companies.

On the flip side, directors recognize that big data and cloud technologies could use more attention—over a quarter say they are not sufficiently engaged in these areas. And, only 53% of directors indicate their company's IT strategy and IT risk mitigation approach even "moderately" takes sufficient advantage of big data.

How engaged is your board or its committees with overseeing/understanding the following?

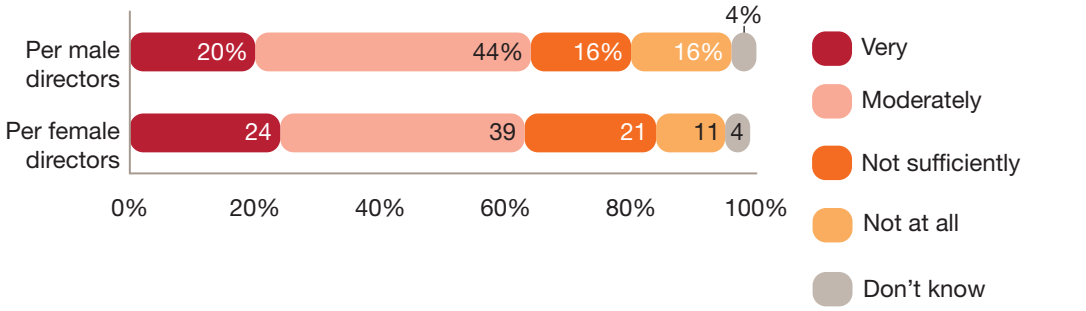
Amounts shown in parentheses represent the change in percentage points from the 2012 survey. N/A indicates the question was not asked in the 2012 survey.



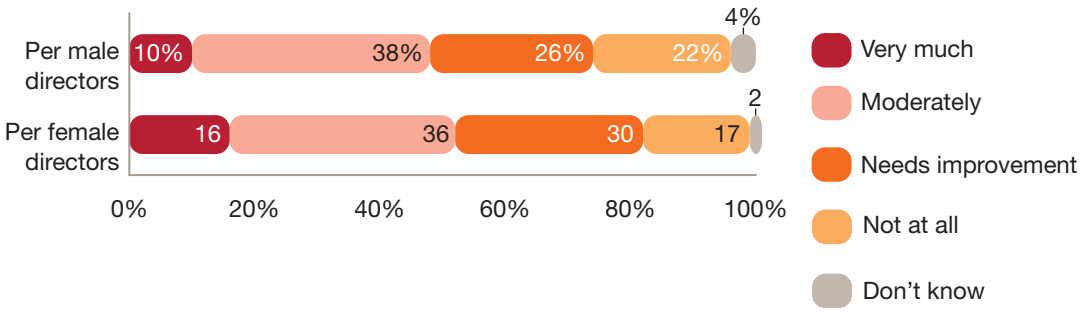
Female directors indicated their boards have higher levels of engagement with oversight of the risk of loss of customer data and with new business models enabled by IT. They also generally expressed a desire to focus more attention on most IT issues.

How engaged is your board or its committees with overseeing/understanding the following?

Risk of compromising customer data (privacy)



New business models that are enabled by IT



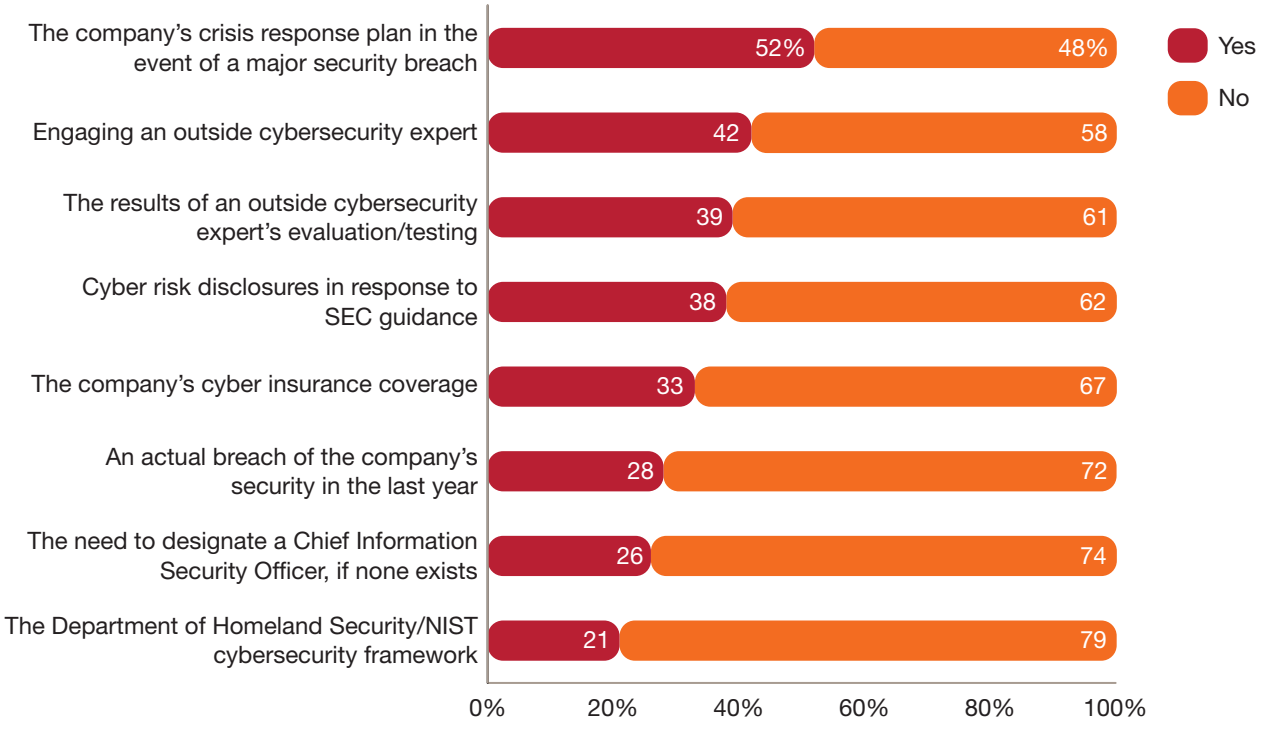
The Achilles' heel of IT—cybersecurity

The increasing complexity of directors' IT oversight roles, a number of recent high-profile data breaches and the new Department of Homeland Security/NIST cybersecurity framework all contribute to our next major governance trend—the spotlight on cybersecurity is getting brighter. We believe this trend will grow in prominence as directors say they want to allocate more time and attention to this area. Almost two-thirds of directors want at least "some" increased focus on IT risks like cybersecurity.

Boards concerned about cybersecurity

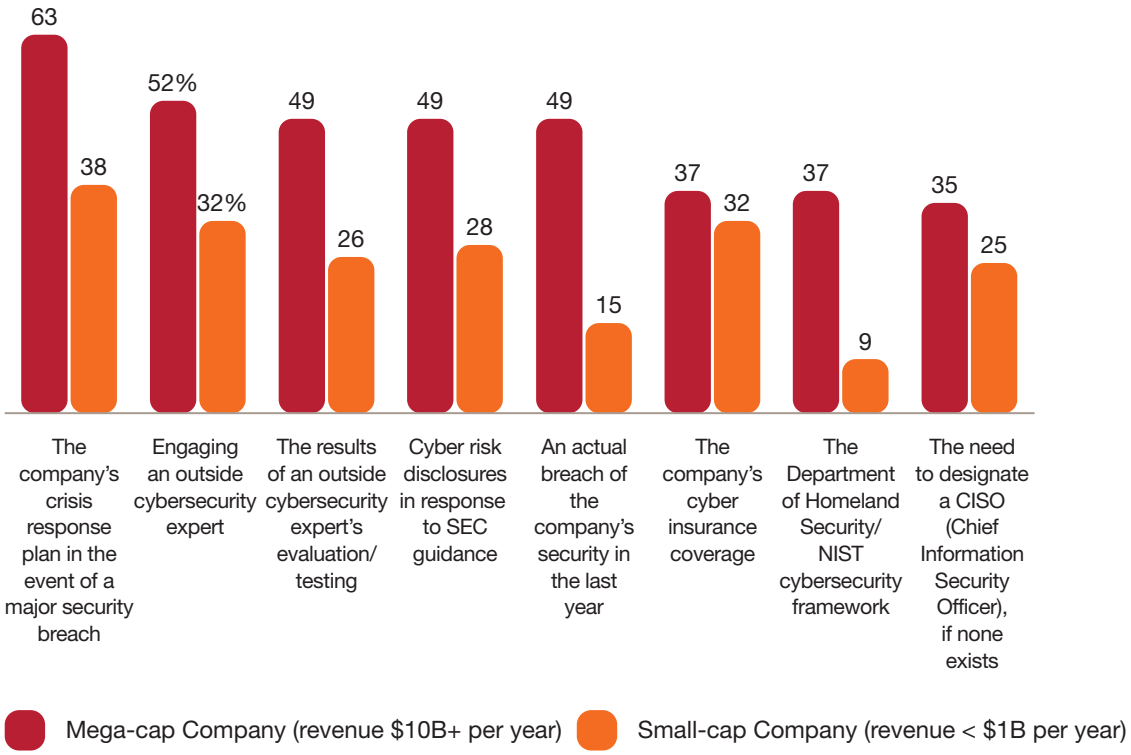
Cybersecurity breaches are at an all-time high. However, nearly half of directors have not discussed the company's crisis response plan in the event of a breach and 67% have not discussed the company's cybersecurity insurance coverage. Directors may want to consider adding these topics to their board agendas.

With regard to cybersecurity issues, has your board or its committees discussed:



Mega-cap company directors are three times more likely than small-cap directors to have discussed an actual breach of their company's security in the last year. This may be because the largest companies have greater resources available to dedicate toward detection capabilities. And, mega-cap company directors are four times more likely than small-cap companies to have discussed the Department of Homeland Security/NIST framework.

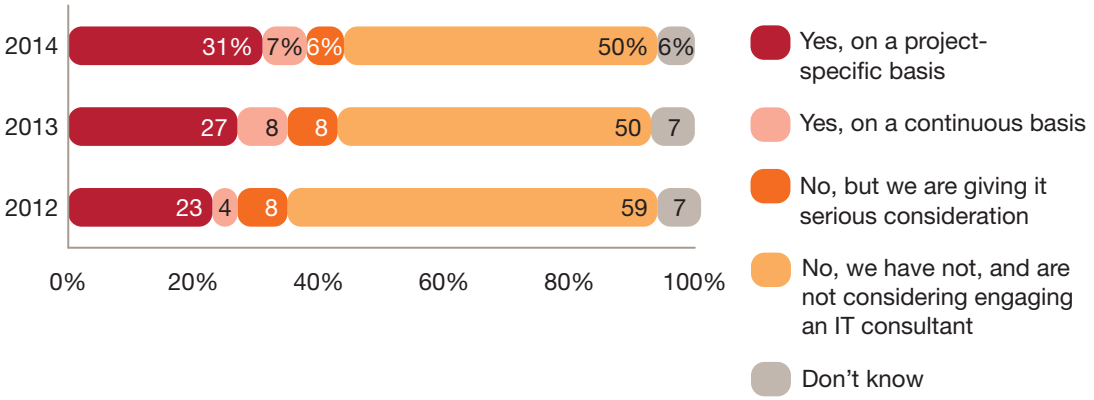
With regard to cybersecurity issues, has your board or its committees discussed:



Thirty-eight percent of directors now say their boards use external IT consultants—compared to 27% in 2012. In the last twelve months, 42% of directors say they discussed engaging an outside cybersecurity expert, and nearly four in ten actually reviewed the results of an outside cybersecurity expert's evaluation and testing of their company's systems.

Mega-cap company directors are 20 percentage points more likely than small-cap company directors to say their board has engaged an outside expert to help them fulfill their IT oversight responsibilities—perhaps not surprising, as directors from the largest companies may believe the higher value of their intellectual property and the volume of private data they retain makes their company more of a target.

During the last 12 months, has your board or its committees engaged an outside consultant to advise on IT strategy, opportunities, or risks?



www.pwc.com

To have a deeper conversation about how this subject may affect your business, please contact:

Mary Ann Cloyd
Leader, Center for Board Governance
PwC
(973) 236 5332
mary.ann.cloyd@us.pwc.com

Don Keller
Partner, Center for Board Governance
PwC
(512) 695 4468
don.keller@us.pwc.com

Paul DeNicola
Managing Director, Center for Board Governance
PwC
(973) 236 4835
paul.denicola@us.pwc.com

©2014 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP, a Delaware limited liability partnership, or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate legal entity. This proposal is protected under the copyright laws of the United States and other countries. NY-15-0065-3