(IRRCi) indicates that while companies must disclose significant cyber risks, those disclosures rarely provide differentiated or actionable information. The report examines key cybersecurity threats to corporations and provides information to investors struggling to evaluate investment risk, business mitigation strategies and the quality of corporate board oversight.

Isaac M. O'Bannon • Jul. 31, 2014

A new report from PwC US and the Investor Responsibility Research Center Institute (IRRCi) indicates that while companies must disclose significant cyber risks, those disclosures rarely provide differentiated or actionable information. The report examines key cybersecurity threats to corporations and provides information to investors struggling to evaluate investment risk, business mitigation strategies and the quality of corporate board oversight.

"Cybersecurity has moved from the back office to the corporate board room because it poses a deep threat to a company's bottom line and reputation," said Jon Lukomnik, executive director of the Investor Responsibility Research Center Institute (IRRCi). "The reality today is that virtually every company is reliant on information and technology, so not one company or sector is left out."

Lukomnik added, "The severity of the gap between the magnitude of cybersecurity threat and the lack of steps boards have taken to address the risks is a key issue for investors and policy makers alike. In recent weeks both Securities and Exchange Commissioner Luis Aguilar and Treasury Secretary Jack Lew have made public comments regarding cybersecurity issues." Lukomnik explained, "Even when Boards do act, investors often feel in the dark on cybersecurity. First, it's dynamic and highly technical. Second, companies can be reluctant to disclose details on threats because they are concerned about providing hackers with a roadmap to vulnerabilities."

What Investors Need To Know About Cybersecurity: How to Evaluate Investment Risks was

The report suggests that investors focus on corporate preparedness for cyber attacks, engage with highly-likely targets to better understand corporate preparedness, and demand better and more actionable disclosures (though not at a level that would provide a cyber-attacker a roadmap to make those attacks).

"The consequences of poor security include lost revenue, compromised intellectual property, increases in costs, impact to customer retention, and can even contribute to C-level executives leaving companies," said Nocera. "This paper can help investors ask the 'right' questions to assess the level of risk they may be facing."

The study suggests investors ask the following key questions:

- Does the company have a Security & Privacy executive who reports to a senior level position within the company?
- Does the company have a documented cybersecurity strategy that is regularly reviewed and updated?
- Does the company perform periodic risk assessments and technical audits of its security posture?
- Can senior business executives explain the challenges of cybersecurity and how their company is responding?
- What is the organization doing to address security at its business partners?
- Has the company addressed its sector-based vulnerability to cyber attack?
- Does the organization have a response plan for a cyber incident?

The study also outlines common motivations for cyber-attacks, by industry sector, based on PwC experience:

The full report is available here. A webinar to review the findings and respond to questions is scheduled for Wednesday, August 20, 2014 at 2 PM EDT. Register here.