RESEARCH NEWS STORY

March 11, 2022

***Turning Vulnerability to Strength*: Corporate Governance's Role in Cybersecurity**

Cyber-attacks are a looming threat to most firms today, but what can board members and policy makers do about it? A new study provides some answers.

In the modern technological era, cybersecurity has risen to importance across the board. The corresponding rise in cyber-attacks on organizations have prompted firms to take a more active approach to mitigating these risks. In this regard, a recent article summarizes the research on corporate governance and the need for IT expertise to oversee cyber risks. It also provides implications for practice, policy, and researchers.

Cybersecurity currently ranks third among the top key strategic risks cited by institutional investors and represents more than $35 trillion assets under management. Given the rapid growth in cyber-crime recently, regulators worldwide have begun to introduce legislation to protect consumer data and privacy.

Yet, governance surveys suggest that boards are not sufficiently prepared to address cybersecurity risks, with 77% of organizations operating with limited cybersecurity, and 87% lacking sufficient resources or a plan to prevent a cyber breach. With the rise of cybersecurity breaches, most companies have recognized the need for IT expertise at the board or senior management level to reduce a firm's chances of a disastrous cybersecurity breach.

Echoing this sentiment, a comprehensive academic review published in *Current Issues in Auditing* takes a closer look at the present and future roles that governance may play in regulating cybersecurity risk. The authors of this review, Caroline C Hartmann, Associate Professor at Texas A&M University - Commerce, and Jimmy Carmenate,
Clinical Assistant Professor, School of Accounting, Florida International University, have gathered empirical data which suggests that IT expertise, such as knowledge of systems implementation and technology transformation, can improve a board's fiduciary duties towards their firm and help mitigate cyber threats.

"We highlight the struggles of the board and other committees in keeping up with the technological advances that make organizations vulnerable to attacks", says Prof Hartmann, who uses this paper to teach a corporate ethics course at the university.

Traditionally, research in this field focuses on information sharing, investments in cybersecurity, the role of internal audit, disclosure of cybersecurity activities, and effects of security breaches. There is a gap in understanding what enables governing bodies in successfully addressing cybersecurity risks and security breaches, and this new study aims to bridge this gap by reviewing and summarizing the latest evidence to inform senior executives and policymakers on best practices.

The researchers believe that there is potential for IT expertise to be used as a governance tool to combat cyber-attacks. After examining aspects of a board's cyber risk oversight capacity, as well as audit committee and management involvement in cybersecurity risks, they suggest that an organization is best prepared for cybersecurity breaches if board members themselves have IT expertise, if the audit committee or a separate risk committee advises on cybersecurity, or if the organization appoints IT experts in senior management positions such as Chief Information Officer (CIO) or Vice President of IT.

In practice, adopting suitable approaches in cybersecurity risk management based on the unique cybersecurity environment and specific needs of a firm can be challenging. *"Firms have begun appointing technology experts and creating board-level IT committees to help the board manage its IT and cybersecurity risk oversight responsibilities"* comments Prof Carmenate on the nature of corporate governance in cybersecurity research.

The study's implications also extend to policy makers and regulatory bodies to bear the consideration that IT expertise, and perhaps even specifically cybersecurity expertise, may be a necessary mandate at the board or senior management level for successful cybersecurity risk oversight for a firm. Currently, federal regulations in the US only require firms to disclose cybersecurity risks and the board's role in cyber risk oversight but provide no guidance on how these risks should be addressed.

"This paper provides practitioners and business owners with relevant information on how to strengthen their boards and governance mechanisms to ensure they are adequately prepared for the frequent changes and risks that technological advances bring forth", concludes Prof Hartmann.

They hope that this work may help organizations have an integrated approach to preparing for, detecting, and responding to cyber incidents.

Reference

Authors	Caroline C Hartmann[1], Jimmy Carmenate[2]
Title of original paper	Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research
Journal	*Current Issues in Auditing*
DOI	https://doi.org/10.2308/CIIA-2020-034
Affiliations	1. Texas A&M University - Commerce 2. Florida International University

Cybersecurity is a relatively new and unfamiliar responsibility for the board of directors in a firm. In a new review, researchers provide insights on the role that governance mechanisms have to play in mitigating cybersecurity risks.
Image courtesy: Shutterstock

About Professor Caroline C Hartmann

Caroline Hartmann, DBA, CPA, is an Associate Professor of Accounting at Texas A&M University - Commerce. Her educational qualifications include a DBA, Accounting, from Kennesaw State University in 2015, and MS, Accounting, from American University, in 1995. Her research interests include corporate governance, fraud, business ethics, and corporate social responsibility. Prior to her academic career, she served as a Chief Financial Officer and Auditor for some of the Big 6 accounting firms. She is a member of the American Institute of Certified Public Accountants (AICPA) and the American Accounting Association (AAA).