Summary of Paper: Linking Cybersecurity and Accounting: An Event, Impact, Response Framework

What is this Study About?

Cybersecurity breaches pose significant threats to an organization's operations, financial performance, and stakeholder trust. In light of the increasing prevalence and severity of these events, the researchers present an "Event, Impact, Response Framework," which is designed to help both practitioners and researchers better assess cybersecurity threats, understand their impact, and develop effective response strategies.

What are the major findings of the study?

The study highlights the crucial role of accounting professionals in identifying, measuring, and tracking the costs associated with cybersecurity events, as well as in ensuring appropriate disclosure of such events to investors and other stakeholders. The researchers point out the existing gaps in knowledge and practice regarding how cybersecurity can be incorporated into accounting and financial reporting. Moreover, the framework underscores how accounting professionals can use cybersecurity research findings to potentially enhance risk assessment, impact analysis, and response planning.

Why is the study important?

These findings underscore the growing interconnection between cybersecurity and accounting and emphasize the need for accountants to broaden their skill set to include cybersecurity risk management. By proposing a structured framework, the researchers not only help address the current challenges in managing cybersecurity risks but also set the stage for future studies on this topic. The insights are particularly valuable for informing policy development, enhancing corporate governance, and fostering a culture of proactive risk management within organizations, ultimately contributing to the resilience and integrity of financial reporting in the digital age.