



SEC Reports Widely Divergent Levels of Cybersecurity Preparedness

Feb 6, 2015

Reading Time : **1 min**

By: Natasha G. Kohne, Jo-Ellyn Sakowitz Klein, David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

Not surprisingly, nearly all broker-dealers (88 percent) and investment advisers (74 percent) reviewed had experienced cyber attacks, including fraudulent emails and malware. As a general rule, most broker-dealers (93 percent) and investment advisers (83 percent) had written information security policies in place. Many of these based their security framework on published cybersecurity risk management standards, such as those published by the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) and the Federal Financial Institutions Examination Council (FFIEC). It is no surprise that third-party risk assessments, reporting and information sharing, and cybersecurity insurance are the most discussed topics in this review.

[Click here](#) to read the full alert.

Categories

Cybersecurity, Privacy & Data Protection

Compliance

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.