Security in Financial Firms

Study finds "surprising disconnect" between IT, Legal and Compliance

---

NEWS PROVIDED BY

Authentic8 ➞

Jan 30, 2020, 12:15 ET

REDWOOD CITY, Calif., Jan. 30, 2020 /PRNewswire/ -- Different priorities and critical communication gaps between IT security teams, compliance professionals, and legal counsel are threatening the regulatory and cybersecurity posture of financial firms, according to new industry research into regulatory compliance and secure web use in the financial sector.

❮   ❯

IT, Compliance, Legal: We Need to Talk. New research about web use and compliance in the financial services sector shows critical communication gaps between the main stakeholders.

The publication, titled Surprising Disconnect Over Compliance and Secure Web Use at Financial Firms, is now available as a Triangle Real Time Research Report. It presents the results of an in-depth survey of senior decision-makers in IT, legal and compliance roles. Conducted by Beacon Technology Partners and sponsored by Silicon Valley-based web isolation solution provider Authentic8, it analyzes the cybersecurity and compliance impact of differing online risk perceptions within the surveyed organizations.

"Financial firms have some of the best-funded IT departments of any industry, that's no secret," says Scott Petry, Co-founder and CEO of Authentic8. "What's perplexing to me, with data breaches and privacy violations at an all-time high, is how deep the divide still runs between IT, compliance and legal professionals in many firms, according to these findings."

The new report quotes practitioners, independent industry observers, and analysts, whom the researchers asked to comment on the survey results. "These three groups are working on the same problem, but they have different views of what the main problem is," said Michele DeStefano, a professor at the University of Miami School of Law.

"Financial firms should move to a flatter organizational structure between those groups," added DeStefano, who co-founded and co-edits the Compliance Elliance Journal. Her recommendation: "IT should be involved in the beginning rather than at the end."

The survey also discovered that "less accessible" IT departments are generally more aware of the risks involved when employees go online than those with higher ratio of IT personnel to serve the employee population.

While this finding applies to financial companies of all sizes, including large organizations with many field offices, the increased awareness does not guarantee a stronger cybersecurity and compliance posture, the survey found.

Instead, some IT departments have developed "tunnel vision" in identifying solutions, according to the research report. Petry says: "The results show that firms often still rely on ineffective traditional perimeter defenses and point solutions, such as anti-virus tools, URL filtering, and VPN, which in turn introduce additional risks."

About Authentic8

Authentic8 is redefining how enterprises conduct business on the web with the Silo web isolation platform. Silo insulates and isolates all web data and code execution from user endpoints, providing powerful, proactive security while giving users full, interactive access to the web. Silo also embeds security, identity, and data policies directly into browser sessions, giving IT complete control over how the web is used. Commercial enterprises and public sector organizations use Silo solutions to provide secure web access, to control web data, apps, and workflows, and to conduct sensitive online research.

SOURCE Authentic8

Related Links

https://www.authentic8.com