FOR IMMEDIATE RELEASE

New Analysis Shows DFS Cybersecurity Guidance Improves Control Execution—but Leaves a Critical Gap in Measurable Risk Reduction

Mount Airy, N.C., May 2026 — CyberRiskModels.com released a new report analyzing the impact of recent New York Department of Financial Services (DFS) cybersecurity guidance, finding that while the recommendations improve control execution, they do not fully address how risk exposure is changing in a heightened threat environment.

The report,*"The Cyber Risk Gap: What DFS Guidance Reduces—and What It Doesn't,"* shows that DFS-aligned actions can strengthen control effectiveness and reduce the probability of certain attack outcomes, but material residual risk remains due to non-linear changes in threat behavior and attack impact.

"DFS guidance reinforces controls that organizations already have—but it doesn't answer the most important question: how much risk is actually reduced," said Charlene Deaver-Vazquez, founder of CyberRiskModels.com. "In today's environment, improving controls does not translate directly to reduced impact."

The analysis shows that the guidance primarily drives **more consistent and disciplined execution** of existing controls such as multi-factor authentication, vulnerability management, monitoring, and third-party oversight, rather than introducing new capabilities. This improvement increases resistance to attack impact, but not enough to offset accelerating threat conditions.

A key finding in the report is that cyber risk is increasingly **non-linear**. Control effectiveness can erode unevenly under pressure, while attack impact expands disproportionately—particularly in AI-driven attack scenarios that can make controls ineffective.

The report highlights a growing "scenario gap" between control-focused guidance and business-level decision-making. While DFS provides a strong defensive framework, it does not quantify:

- How exposure is changing under current threat conditions
- Which attack scenarios are becoming more likely or more severe
- What level of residual risk remains after controls are strengthened
- Which actions will materially reduce business impact

To address this gap, CyberRiskModels.com applied a scenario-based modeling approach that measures how control effectiveness, threat conditions, and business characteristics interact to determine actual exposure. The findings show that even with improved controls, high-

impact risks such as ransomware and business email compromise remain elevated due to persistent likelihood and expanding attack pathways.

“Executives don’t make decisions based on whether a control exists—they make decisions based on potential business loss,” Deaver-Vazquez said. “Without quantifying how threats and controls interact at the scenario level, organizations are operating without a clear view of residual risk.”

The report concludes that organizations must move beyond control maturity and adopt **continuous, scenario-based risk measurement** to understand how changing conditions affect exposure. In a heightened threat environment, this includes accounting for AI-driven attack methods, geopolitical influences, and the compounding effects of control degradation.

CyberRiskModels.com provides monthly cyber risk forecasts designed to help organizations assess likelihood, financial impact, and response strategies in changing threat conditions.

Download the report here:
https://d1yei2z3i6k35z.cloudfront.net/14814792/6a199d36588ba8.76711119_The-Cyber-Risk-Gap-What-DFS-Guidance-Reduces-and-What-It-Doesnt.pdf

More information: https://cyberriskmodels.com

Media Contact:
Charlene Deaver-Vazquez
CyberRiskModels.com
Charlene@CyberRiskModels.com