New Cyber Risk Forecast: AI-driven attacks erode email controls and drive financial loss

AI-driven attacks reduce control effectiveness and sharply increase financial exposure

MOUNT AIRY, NC, UNITED STATES, May 18, 2026 /EINPresswire.com/ -- New Cyber Risk Forecast Warns AI-driven Attacks are Eroding Business Email Controls and Driving Non‑Linear Financial Loss

> Businesses face more effective, financially damaging attacks because they are indistinguishable from legitimate communications and can trigger multiple financial transactions.”
>
> *Charlene Deaver-Vazquez*

CyberRiskModels.com released a new report showing that artificial intelligence is changing the pattern of business email compromise (BEC) attacks and accelerating financial losses through multiple financial transactions.

The report, “New Cyber Risk Forecast: AI Is Eroding BEC Controls and Driving Non-Linear Financial Loss,” finds that AI-driven strategy increases likelihood of attack slightly but it’s the financial exposure that can increases dramatically, as much as nine times under typical conditions.

“AI-driven attacks are changing the playbook on email compromise,” said Charlene Deaver-Vazquez, founder of CyberRiskModels.com. “Businesses face more effective, financially damaging attacks because they are indistinguishable from legitimate communications and can trigger multiple financial transactions.”

The analysis shows that AI-generated phishing and BEC campaigns are reducing the effectiveness of existing controls. Attacks are becoming more credible and context-aware, making them more difficult for employees to distinguish from legitimate communications.

The report identifies a shift to a hybrid “spray-to-target” attack model. In this approach, threat actors begin with broad outreach and escalate to targeted interactions after a recipient engages. Once that transition occurs, attacks move from pattern-based detection to conversation-based manipulation, reducing the effectiveness of traditional email security measures.

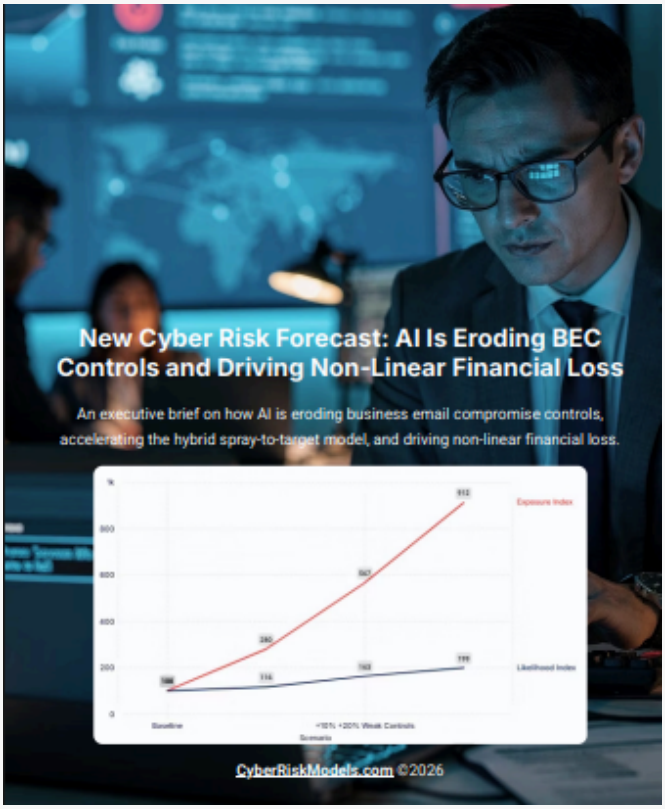
This increased effectiveness is possible because in recent years, cybercriminals have used public data to map organizational processes that allow them to develop transaction-focused scenarios

tied to real workflows.

The report also highlights a key structural change in how risk develops. While attack likelihood may increase gradually, financial exposure grows more rapidly due to a combination of reduced control effectiveness and the potential for multiple financial actions within normal business operations.

These conditions can allow a single compromise to result in multiple payments or transactions, increasing total losses.

CyberRiskModels.com said the most critical gap is at the execution layer — the point at which financial decisions are carried out. At that stage, outcomes depend less on detection technology and more on whether organizations enforce verification processes before funds are moved.



New Cyber Risk Forecast on AI-Driven Email Attacks

Recommended controls include independent verification using known contact paths, dual approval processes and delays for payment changes.

“The decisive factor is not whether the attack reaches the business,” Deaver-Vazquez said. “It is whether the organization enforces verification at the moment of financial action.”

The report concludes that BEC should be treated as a business process risk rather than a standalone cybersecurity issue. Organizations need to shift their focus from prevention and detection to controls embedded in financial workflows.

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

More information is available at https://cyberriskmodels.com.

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

Charlene Deaver-Vazquez

CyberRiskModels.com
+1 301-346-3752
Charlene@cyberriskmodels.com
Visit us on social media:
LinkedIn
