Fraud Tops Ransomware in 2026 as CEOs Reassess Cyber Risk with Global IT

Global IT releases a 2026 cyber risk reality check and executive workshop framework as fraud rises on CEO cyber risk agendas.

Executive leaders reviewing 2026 cyber risk realities, comparing fraud and ransomware in a board□level briefing.

LOS ANGELES, CA, UNITED STATES, February 23, 2026 /EINPresswire.com/ -- Global IT has released “2026 Cyber Risk Reality Check: Fraud vs. Ransomware—How to Align CEO + CISO Priorities,” an executive-focused resource and workshop framework for CEOs, CISOs, CIOs, and CFOs in U.S. enterprises and mid-market organizations, with particular relevance for Los Angeles. Recent global analysis indicates that cyber-enabled fraud has moved ahead of ransomware on many CEO cyber risk agendas for 2026, prompting renewed attention to how leadership teams set priorities, budgets, and board reporting.

> In 2026, boards make better decisions when they treat fraud and ransomware as two signals of the same identity and governance problem, not as competing budget lines.”
>
> *Global IT Communications CISO*

Ransomware has dominated cyber discussions for years, but recent surveys suggest business leaders now report more direct exposure to fraudulent transfers, vendor impersonation, and AI-assisted scams than to large-scale encryption incidents. In the World Economic Forum’s Global Cybersecurity Outlook 2026, CEOs are described as placing cyber-enabled fraud and phishing among their top concerns, while security leaders still tend to highlight ransomware as a primary technical threat, revealing a difference in emphasis between business and security perspectives. The Global IT material examines this divergence and outlines ways organizations can address fraud and ransomware as related outcomes of gaps in identity, governance, and human behavior.

Fraud as a Front-Line Executive Risk
Reports from global cyber risk studies note that a large share of executives say cyber-enabled fraud affected their organizations or peers in recent years, which has made these incidents more visible at the board level. At the same time, data on business email compromise shows significant average losses per incident and growing use of vendor email compromise, where attackers leverage trusted third parties to redirect funds or alter payment details.

Finance and security teams examining cyber‑enabled fraud and business email compromise risks.

Security operations center monitoring ransomware, data theft, and extortion activity across enterprise networks.

“Fraud incidents are often recorded as financial losses long before they are described as security events,” said a Global IT Virtual CISO who advises several mid-market organizations in Southern California. “By the time a fraudulent payment is discovered, boards are already discussing financial impact, yet many of the early warning signs lived in identity access logs, email patterns, or vendor governance processes.”

The Ransomware Paradox in 2026
Industry threat reports continue to document active ransomware groups, shifting extortion techniques, and use of data theft and pressure campaigns alongside or instead of encryption. Analysts tracking AI-related threats have also described sharp increases in AI-assisted scams and impersonation techniques, which can be applied to both fraud and initial access for ransomware operations.

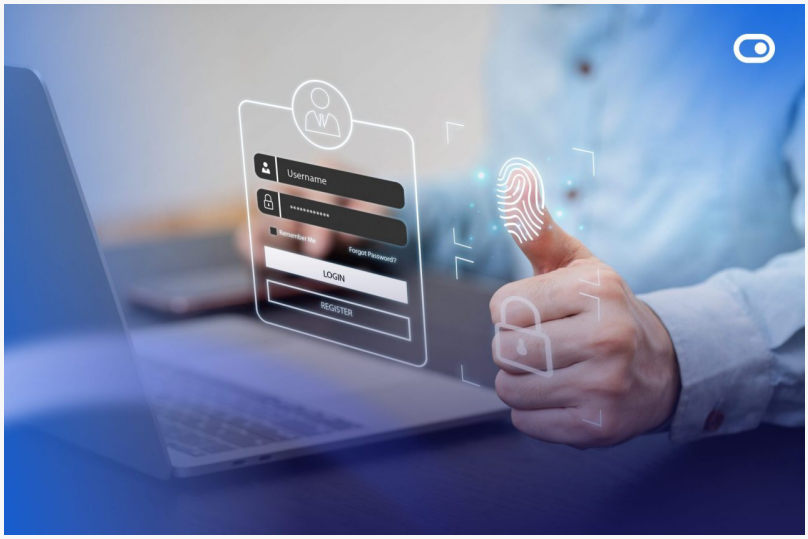
“Many organizations still treat ransomware and fraud as separate categories when they often share entry points and enabling conditions,” said the Director of Cyber Risk & Compliance at Global IT. “The same weaknesses in identity management, email controls, and vendor processes that enable fraudulent payments may also enable lateral movement and data exfiltration.”

Budget and Control Considerations for 2026
The 2026 Cyber Risk Reality Check material discusses how organizations can review cyber-related

budgets without reducing their focus on ransomware resilience. It emphasizes controls that influence both fraud and ransomware exposure, such as consolidated identity platforms, phishing-resistant multifactor authentication for higher-risk roles, and stronger access governance around finance and vendor systems.

“Organizations that align security, finance, and IT around shared control objectives often find they can address multiple risk scenarios with the same investments,” said the CFO of a Los Angeles–based healthcare organization that collaborates with Global IT on cyber risk initiatives. “Financial workflows, identity systems, and recovery capabilities all influence how fraud and ransomware incidents unfold.”

The guidance highlights three practical areas for 2026 planning:



Identity and finance teams aligning access controls, MFA, and payment verification to reduce fraud and ransomware exposure.


Executives participating in a cyber risk workshop on fraud, ransomware, and board‑level metrics.

Emphasizing identity and access controls that reduce the impact of both fraud and ransomware incidents.

Embedding verification steps and dual controls in payment and vendor processes to address business email compromise and related fraud scenarios.

Incorporating combined fraud and ransomware scenarios into incident response exercises and resilience testing.

Metrics for Boards and Committees

Several recent reports note that boards are seeking clearer views of cyber risk in financial and operational terms, rather than detailed technical metrics. The Global IT framework suggests that organizations identify a concise set of recurring measures that connect cyber activity to business impact and resilience.

“Board-level reporting tends to be most effective when it focuses on trends and outcomes rather than on individual tools or alerts,” said an independent board director and former CIO who advises multiple California organizations. “Metrics that link identity, fraud attempts, and recovery capabilities provide a more integrated picture of risk than isolated technical indicators.”

The resource describes examples of metrics boards may request, including:

Documented fraud losses and near-miss incidents by category over time.

Ransomware readiness indicators, such as tested recovery times and backup verification results for critical systems.

Identity and access-related measures, including multifactor authentication adoption and investigation of anomalous access events.

Training and simulation outcomes for executives, finance, and operations regarding fraud and phishing campaigns.

Scenario: Combined Fraud and Extortion in a Regional Firm
The Global IT material includes a scenario involving a professional services organization in the Los Angeles area that relies on multiple cloud platforms and a distributed workforce. In the scenario, an attacker manipulates vendor communications to redirect payments, then uses the same access to obtain sensitive data and apply extortion pressure, without relying solely on encryption. The example is used to illustrate how finance controls, identity management, and incident response planning can influence both financial losses and continuity of operations.

What the 2026 Cyber Risk Reality Check Includes
The 2026 Cyber Risk Reality Check from Global IT is structured as a set of materials that support executive discussions and board engagement. The components include:

A thought leadership article outlining how fraud and ransomware priorities are shifting in 2026 and how executives can interpret recent research.

A one-page brief for board and committee packets summarizing key decision points and example metrics.

A suggested LinkedIn post series structure tailored to CEOs, CISOs, CIOs, and CFOs who need to communicate cyber risk themes to broader stakeholders.

A cyber-enabled fraud prevention checklist that reflects controls relevant to Los Angeles cybersecurity and fraud prevention, including identity, email, and finance process measures.

A ransomware readiness scorecard format aligned with contemporary threat behaviors and resilience expectations.

A template for summarizing cyber risk governance information in board reports.

Availability and Regional Focus
Global IT is making the 2026 Cyber Risk Reality Check materials available as part of its advisory work with organizations in Los Angeles and other regions. The company also conducts executive risk alignment workshops that convene CEOs, CISOs, CIOs, and CFOs to review fraud and ransomware exposure, budget choices, and board reporting practices using the framework. Sessions are being scheduled with mid-market and enterprise organizations across 2026.

Organizations interested in learning more about the 2026 materials or workshop format can contact Global IT through the details below or via the company's website.

About Global IT
Global IT is a Los Angeles–based provider of managed IT, cybersecurity, cloud, and compliance services for mid-market and enterprise organizations in California and the surrounding region. Its services include Los Angeles managed IT services, Managed IT services Los Angeles, Managed firewall services in Los Angeles, and IT risk management as a service for clients in sectors such as healthcare, financial services, professional services, and manufacturing.

Press Team
Global IT Communications, Inc
+1 213-403-0111
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
Other