Stratos Cyber

EXECUTIVE BRIEFING MEMO TEMPLATE

(AI-Phishing & Impersonation Threat – August 2025)

OVERVIEW

Generative AI has industrialized phishing, transforming it from a nuisance attack into a sophisticated fraud vector. Global reporting confirms that AI-enhanced phishing campaigns have risen over 1,000% since 2024, and synthetic voice impersonation is now present in more than 14% of executive-targeted fraud cases. While verified cases in the Caribbean are still emerging, the structural realities of our region — reliance on email approvals, hierarchical trust, and high executive visibility — mean institutions here are acutely vulnerable.

WHY THIS MATTERS TO BOARDS

The use of AI in phishing and impersonation directly affects governance, not just IT operations.

- **Financial Risk:** Misrouted payments, fraudulent wire transfers, and manipulated vendor accounts.
- **Compliance Risk:** Failures to safeguard sensitive or regulated data under ISO/IEC 27001, GDPR, or local data protection laws (e.g., Jamaica's Data Protection Act, Trinidad's Data Protection Act, Barbados' DPA).
- **Reputational Risk:** Loss of public trust following disclosure of executive impersonation or synthetic voice fraud.
- **Operational Risk:** Disruptions to HR, finance, and IT workflows from unauthorized access or fraudulent approvals.

Stratos Cyber

REGIONAL RELEVANCE

- The Central Bank of The Bahamas issued a public warning in April 2025 regarding AI-generated deepfake scams impersonating officials.
- CARICOM IMPACS has flagged AI-powered phishing and social engineering as emerging regional threats.
- According to ICT Pulse, AI-enhanced phishing campaigns are already targeting SMEs across Latin America and the Caribbean.

BOARD ACTION POINTS

- **Approve a Secondary Validation Policy:** Mandate a second channel (phone, in-person, secure app) for all high-risk requests.
- **Commission AI-Phishing Simulations:** Require annual training that tests executives and staff against realistic AI-crafted lures.
- **Mandate Executive Exposure Audits:** Reduce unnecessary online publication of executive bios, signatures, and voice recordings that can be used to train AI impersonators.
- **Integrate AI-Impersonation Scenarios into Incident Response:** Ensure the organizational playbook includes workflows for deepfake audio, synthetic communications, and impersonation fraud.
- **Implement Digital Brand Protection Services:** Adopt monitoring and takedown capabilities to detect fraudulent domains, fake social media profiles, and impersonation sites that exploit the organization's name, executives, or branding.

Stratos Cyber

GUIDANCE FOR INTERPRETING THE HEATMAP

The risk heatmap below applies standard classifications of Critical, High, Medium, and Low, aligning with international governance frameworks (ISO 27005, COSO ERM, NIST CSF). It is designed to inform the board's oversight role by highlighting where cyber threats intersect with institutional resilience, financial stewardship, and regulatory accountability.

- **Critical Risks** represent exposures with both high likelihood and high potential impact. These require immediate governance attention, explicit board ownership, and allocation of resources. They should appear on the board's risk register and remain standing agenda items until mitigated or transferred.
- **High Risks** are material exposures that can significantly disrupt operations or undermine compliance if realized. They require executive action within the current planning cycle, and the board should require regular reporting on progress and assurance from management that controls are being applied.
- **Medium Risks** should be managed by management within established operational risk frameworks, but the board should require quarterly visibility to ensure these do not escalate into higher categories.
- **Low Risks** are exposures with limited business impact or likelihood. They should be acknowledged within the enterprise risk register but can be overseen under the organization's routine risk management practices without additional board intervention.

The board's role is not to design controls, but to ensure that:

1. Critical and High risks are resourced and governed at the appropriate level, with accountability clearly assigned.
2. Management provides independent assurance (through audit, compliance, or third-party review) that mitigations are functioning.
3. Risk appetite statements are updated to reflect the evolving threat landscape, ensuring cyber resilience remains aligned with strategic objectives.

Stratos Cyber

RISK HEATMAP

Threat Vector	Likelihood	Impact	Overall Risk
AI-generated phishing emails	High	High	Critical
Deepfake executive voice notes	Medium	High	High
Vendor impersonation (AI-crafted RFPs/invoices)	Medium	Medium	Medium
Repackaged credentials + AI-tailored lures	High	Medium	High

Stratos Cyber

CONCLUSION

AI-phishing is not a technical anomaly. It is a governance issue that challenges the very basis of institutional trust.

Boards must act decisively by mandating verification policies, commissioning readiness exercises, and embedding AI-phishing into organizational risk frameworks.

Stratos Cyber recommends treating this as a standing board agenda item until maturity in trust architecture is demonstrably achieved.

Stratos Cyber

ABOUT US

Stratos Cyber is a leading innovator in cybersecurity, dedicated to helping businesses navigate an ever-evolving digital threat landscape.

Headquartered in Canada with a global reach, we specialize in delivering tailored security solutions that empower organizations to safeguard their digital assets, maintain compliance, and build resilience against future threats.

With a strong focus on innovation and governance, we leverage cutting-edge technology and a proactive approach to ensure our clients thrive in today's connected world.

Email

info@stratos-cyber.com

Telephone

+1 514 299 2015

Website

www.stratos-cyber.com