



CISA

PUBLICATION

October 2026

Business Email Compromise in Ghana:
Assessing Emerging Threats, Business
Vulnerabilities and Mitigation Strategies



**20
26**

cisaghana.com

Introduction

In June 2025, INTERPOL published the fourth edition of its Africa Cyberthreat Assessment Report. Drawing on data from its private-sector partners, the report found that eleven African countries account for most business email compromise (BEC) activity originating from the continent. It named Ghana, alongside Nigeria, Côte d'Ivoire and South Africa, as a country where that activity is concentrated (INTERPOL, 2025). The finding sits uneasily with Ghana's reputation as a cybersecurity leader. In 2024, the International Telecommunication Union (ITU) placed Ghana in Tier 1, the highest "Role Modelling" category of its Global Cybersecurity Index (Ghana News Agency, 2024).

BEC differs from the ransomware and malware attacks that usually dominate cybersecurity debate. It rarely depends on malicious code. Instead, it relies on a convincing email, a familiar name and a moment of misplaced trust. This makes it a business-process problem as much as a technical one.

This article focuses on Ghana and addresses three questions. What is the nature of BEC, and how is the threat evolving in Ghana? What makes Ghanaian businesses vulnerable? What can firms, financial institutions and the state do about it? Where Ghana-specific data are thin, the article says so, because those gaps are part of the problem.

The Nature of Business Email Compromise

BEC is a form of cyber-enabled fraud. Criminals impersonate a trusted party, such as a chief executive, a supplier or a lawyer. They then persuade an employee to transfer money or sensitive data to accounts they control. According to the FBI, offenders gain access either by deceiving staff or by breaking into genuine business email accounts (Federal Bureau of Investigation [FBI], 2024).

Several variants recur. In CEO fraud, the attacker poses as a senior executive and demands an urgent transfer. In account compromise, an employee's real mailbox is hijacked and used to redirect payments. In false-invoice or "change of bank details" fraud, the criminal poses as a known supplier and supplies a new account number. INTERPOL reports that CEO fraud and bank-detail-change fraud are among the schemes most often reported by African member countries. It also highlights lookalike email domains, fake quotation requests and WhatsApp messages that impersonate known contacts (INTERPOL, 2025).

Consider a typical case. A Ghanaian importer is due to pay an overseas supplier for a container of goods. Days before payment, an email arrives from what appears to be the supplier's finance officer. It says the supplier has changed banks and attaches an invoice with new account details. The sender's address differs from the genuine one by a single

letter. The importer pays. Weeks later, the real supplier asks why it has not been paid, but by then the money has moved on. The scenario is illustrative, but it mirrors the bank-detail-change and lookalike-domain tactics that INTERPOL describes (INTERPOL, 2025).

Most BEC attacks need no malware. Offenders often monitor a compromised or spoofed mailbox for weeks. They learn payment cycles, supplier names and the tone executives use, then strike when a large payment falls due. Some cases involve stolen passwords or network intrusion, but the decisive step is still human: an employee acts on a false instruction (INTERPOL, 2025). Antivirus software and firewalls therefore offer limited protection. Verification procedures, payment controls and staff awareness matter more.

The method is also evolving. INTERPOL's 2026 assessment reports that criminals now use generative artificial intelligence (AI) to write emails that mimic an executive's tone, internal jargon and signature style. Some use free email services to slip past filters designed to catch spoofed company domains (INTERPOL, 2026).

Emerging Threats: BEC Trends in Ghana and Beyond

The global benchmark

The United States publishes the most detailed public data on BEC. In 2025, the FBI's Internet Crime Complaint Center (IC3) received 24,768 BEC complaints, with reported losses of about \$3.05 billion. This was a rise of roughly 16 percent in complaints and 10 percent in losses over 2024 (FBI, 2026). Between October 2013 and December 2023, global exposed losses, which include attempted losses, reached nearly \$55.5 billion across 305,033 incidents (FBI, 2024).

The African picture

INTERPOL's 2025 report describes BEC as a significant and growing threat in Africa, with a sharp rise in both attack volume and financial impact. The finance sector was the most frequently targeted in 2024. Firms engaged in international trade, or with weak security controls, were especially exposed (INTERPOL, 2025). The 2026 edition, covering 2025 data, again ranks BEC as the most financially damaging attack type on the continent. It identifies West Africa as the most active region for BEC detections (INTERPOL, 2026).

However, the 2026 edition measures the problem differently. Using one vendor's detection data, it traces 70 percent of detected BEC activity to South Africa and 29 percent to Nigeria. Ghana is not singled out in those figures (INTERPOL, 2026). One edition reports where BEC activity is concentrated; the other reports where detected attacks originate. Country rankings should therefore be read as directional, not as a fixed league table.

Ghana's domestic data

Ghana's own figures show a fast-growing fraud problem, but they do not isolate BEC. The Cyber Security Authority (CSA) reported cybercrime losses of GH¢23.3 million in 2024. Reported incidents rose from 1,317 in the first half of 2024 to 2,008 in the first half of 2025. Fraud and impersonation accounted for more than 94 percent of financial losses (Business & Financial Times, 2025). Between January and July 2026, the CSA recorded 3,876 incidents, about 47 percent of which involved online fraud (Ghana News Agency, 2026).

The CSA's Director-General has warned that criminals are increasingly targeting Ghana's digital finance ecosystem through impersonation, payment diversion and BEC (TechAfrica News, 2026). The Bank of Ghana's 2025 Fraud Report adds context. Reported fraud cases across banks, specialised deposit-taking institutions and payment service providers rose by 48 percent, from 16,733 in 2024 to 24,778 in 2025. The total value at risk was about GH¢101 million (Bank of Ghana, 2026). These are not BEC figures, but they show how quickly the attack surface for payment fraud is expanding.

Ghana as an operating base

A further trend concerns offenders rather than victims. United States prosecutors have repeatedly relied on extradition from Ghana in BEC-related cases. In August 2025, three Ghanaian nationals were extradited to New York. They were charged as senior members of a Ghana-based organisation alleged to have stolen more than \$100 million through romance scams and BEC (U.S. Attorney's Office, Southern District of New York, 2025). One of them was sentenced in July 2026 to 85 months in prison (U.S. Attorney's Office, Southern District of New York, 2026).

In a separate case, a Nigerian national arrested in Ghana was extradited to Maryland in August 2024 over a \$7.5 million BEC scheme against two charities (U.S. Attorney's Office, District of Maryland, 2024). He was later convicted and, in August 2026, sentenced to eight years in prison (FBI Baltimore Field Office, 2026). Research also indicates that online fraudsters frequently move from Nigeria to Ghana. It finds that Ghanaian scammers tend to operate independently, unlike Nigerian counterparts often linked to groups such as the Black Axe confraternity (Lazarus & Soares, 2025). Even Black Axe-linked BEC networks appear fluid rather than rigidly hierarchical (Lazarus, 2025).

Vulnerabilities of Ghanaian Businesses

Email-based trade and payments. Many Ghanaian firms buy, sell and pay across borders by email. Importers, exporters and their logistics and finance partners routinely receive invoices and bank details from overseas counterparties. INTERPOL lists import and

export trade, oil and gas, pharmaceuticals, transport and e-commerce among the sectors hit by significant BEC incidents in Africa (INTERPOL, 2025). When a payment instruction arrives only by email, one altered account number can divert the value of an entire consignment.

Small firms with weak controls. Small and medium-sized enterprises (SMEs) face particular risk. Many have no dedicated IT staff, no dual authorisation for payments and no written procedure for changing supplier details. INTERPOL notes that organisations of every size were affected and that weak security controls increased exposure (INTERPOL, 2025). Simple safeguards, such as multi-factor authentication on email accounts, cost little but protect only firms that adopt them.

The human factor. BEC exploits people more than systems. Citing industry research, INTERPOL reports that in Central and West Africa up to 75 percent of human-related cyber incidents were linked to employee behaviour (INTERPOL, 2026). Urgency, deference to seniority and reluctance to question a superior all work in the fraudster's favour. AI-written messages make the deception harder to spot.

Rapid digitisation of payments. Mobile money, online banking and digital payments have widened the attack surface. The Bank of Ghana reports that fraud cases at payment service providers rose by 54 percent in 2025. Value at risk in that segment nearly doubled, from GH¢19 million to GH¢37 million (Bank of Ghana, 2026).

Low recovery and under-reporting. Once money leaves an account, it is hard to recover. Banks and specialised deposit-taking institutions recovered only about GH¢3.7 million, or 5 percent, of GH¢68.2 million at risk in 2025 (Bank of Ghana, 2026). Many victims also stay silent. INTERPOL notes that under-reporting makes precise BEC figures hard to obtain across Africa, and cites fear of reputational damage as one reason (INTERPOL, 2025, 2026). Silence deprives investigators of the intelligence they need.

Enforcement capacity and the Tier 1 paradox. Ghana's legal framework is strong on paper. Its score of 99.27 percent in the 2024 Global Cybersecurity Index placed it among Africa's top performers. The Cybersecurity Act, 2020 (Act 1038) is widely cited as a model law. Yet the CSA itself acknowledged that capacity development was the one pillar where Ghana did not score highly (Ghana News Agency, 2024). In Sumsb's 2024 Global Fraud Index, Ghana was among the African countries assessed as most vulnerable to digital fraud (Sumsb, 2024).

The gap is best explained as one between legal architecture and operational capacity. The statutes exist. What has lagged is investigative throughput, digital forensics and prosecutorial follow-through. The extradition cases show that international cooperation works. They also show that the most serious BEC cases linked to Ghana are prosecuted

abroad rather than at home. The draft Cybersecurity (Amendment) Bill, 2025 seeks to close part of this gap. It would empower the CSA to investigate and arrest and, on the authority of the Attorney-General, to prosecute cybercrime (Cyber Security Authority, 2025). Critics warn that placing regulatory, investigative and prosecutorial powers in one body could weaken checks and balances (GhanaFact, 2025).

Conclusion

BEC in Ghana is best understood as a governance and business-process problem, not only a technical one. The evidence points to three conclusions. First, Ghana is repeatedly named as a centre of BEC activity, although rankings shift with how the problem is measured. Second, Ghanaian businesses are exposed through email-based trade, weak payment controls, limited staff awareness and a fast-digitising payment system. Third, Ghana's strong laws have not yet been matched by domestic investigative and prosecutorial capacity.

No single statute or index score will solve BEC. Firms that verify before they pay, banks that can stop fraudulent transfers quickly, and a justice system that prosecutes at home as readily as it extradites will make the difference. Until then, Ghana risks remaining two things at once: a role model on paper and a recurring name in BEC case files. The recommendations below set out practical steps.

Recommendations: Mitigation Strategies

For businesses

Verify every payment change through a second channel. Confirm any new or altered bank details by telephone, using a number already on file, never one supplied in the email itself.

Separate duties for payments. Require two authorised officers to approve large, urgent or first-time payments, and hold payments to newly changed accounts until they are verified.

Secure email accounts. Enable multi-factor authentication, monitor for suspicious mail-forwarding rules and deploy domain authentication standards (SPF, DKIM and DMARC) to make spoofing harder.

Use licensed providers. When outsourcing IT or security services, engage providers licensed or accredited by the CSA, as the Authority has urged financial institutions and merchants to do (Graphic Online, 2026).

Train and empower staff. Give finance and procurement teams regular, realistic training, including examples of AI-written messages. Make it normal to question an urgent instruction, even from a senior executive.

Report immediately. Notify the bank at once to attempt a recall, then report to the CSA and the Police. Speed improves the chance of recovery.

For banks and payment service providers

Strengthen transaction safeguards. Flag large first-time transfers to new beneficiaries, check that account names match payee details where possible, and agree rapid inter-institution protocols for freezing suspected fraudulent funds.

For government and regulators

Publish BEC-specific data. The CSA and the Bank of Ghana should report BEC incidents and losses as a separate category, by sector, so that policy can be targeted.

Build domestic enforcement capacity. Expand digital forensics and financial-intelligence capacity in the Economic and Organised Crime Office, the Ghana Police Service's Cybercrime Unit and the CSA, so that extradition becomes the exception rather than the main route to accountability.

Preserve checks and balances. As the Cybersecurity (Amendment) Bill advances, keep investigative and prosecutorial functions accountable through clear separation or judicial oversight.

Deepen international cooperation. Sustain joint operations with INTERPOL and partner agencies. Operation Sentinel, which targeted BEC, digital extortion and ransomware across 19 African countries in late 2025, led to 574 arrests and shows what coordinated action can achieve (INTERPOL, 2026).

Reach SMEs and young people. Extend CSA awareness campaigns to SMEs and exporters. Alongside enforcement, support diversion and rehabilitation programmes for young offenders, building on INTERPOL's pilot work in this area (INTERPOL, 2026).

References

Asiama, A. A. (2026). Pathways of intention: Narratives of future withdrawal from cyber fraud among Ghanaian youth. *Journal of Developmental and Life-Course Criminology*, 12, Article 17. <https://doi.org/10.1007/s40865-026-00306-y>

Bank of Ghana. (2026). *Banks, SDIs and PSPs 2025 fraud report*. Financial Stability Department. <https://www.bog.gov.gh/wp-content/uploads/2026/07/FRAUD-REPORT-2025.pdf>

Business & Financial Times. (2025, September 9). GH¢15m lost to cyberfraud in first-half 2025. <https://thebftonline.com/2025/09/09/gh%E2%82%B515m-lost-to-cyberfraud-in-first-half-2025/>

Cyber Security Authority. (2025). *Cybersecurity (Amendment) Bill, 2025* [Draft for public consultation]. [https://www.csa.gov.gh/resources/Cybersecurity%20\(Amendment\)%20Draft%20Bill%202025%20final%2015102025.pdf](https://www.csa.gov.gh/resources/Cybersecurity%20(Amendment)%20Draft%20Bill%202025%20final%2015102025.pdf)

FBI Baltimore Field Office. (2026, August 28). *Nigerian national sentenced to federal prison in connection with business email compromise scam*. Federal Bureau of Investigation. <https://www.fbi.gov/contact-us/field-offices/baltimore/news/nigerian-national-sentenced-to-federal-prison-in-connection-with-business-e-mail-compromise-scam>

Federal Bureau of Investigation, Internet Crime Complaint Center. (2024, September 11). *Business email compromise: The \$55 billion scam* (Public Service Announcement I-091124-PSA). <https://www.ic3.gov/PSA/2024/PSA240911>

Federal Bureau of Investigation, Internet Crime Complaint Center. (2026). *2025 internet crime report*. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

GhanaFact. (2025). Draft 2025 Cybersecurity Bill: CSA's new functions, police powers & other major amendments. <https://ghanafact.com/draft-2025-cybersecurity-amendment-bill-csas-new-functions-police-powers-cyber-hygiene-other-major-amendments/>

Ghana News Agency. (2024, September 16). Ghana ranked Tier 1 in latest ITU Global Cybersecurity Index. <https://gna.org.gh/2024/09/ghana-ranked-tier-1-in-latest-itu-global-cybersecurity-index-2/>

Ghana News Agency. (2026, September). Online fraud accounts for 47% of Ghana's cyber incidents – CSA. <https://gna.org.gh/2026/09/online-fraud-accounts-for-47-of-ghanas-cyber-incidents-csa/>

Graphic Online. (2026, September). Cybersecurity is a duty owed to every customer – CSA boss. <https://www.graphic.com.gh/business/business-news/cybersecurity-is-a-duty-owed-to-every-customer-csa-boss.html>

INTERPOL. (2025). *INTERPOL Africa cyberthreat assessment report 2025* (4th ed.). https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf

INTERPOL. (2026). *INTERPOL African cyberthreat assessment report 2026*. <https://www.interpol.int/Media/Documents/Publications/Cybercrime/African-Cyberthreat-Assessment-Report-2026>

Lazarus, S. (2025). Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the “Black Axe” confraternity. *Deviant Behavior*, 46(4), 456–480. <https://doi.org/10.1080/01639625.2024.2352049>

Lazarus, S., & Soares, A. B. (2025). From business centres to hustle kingdoms: Historical perspectives on innovative models of deviant education. *International Annals of Criminology*, 62(3–4), 449–468. <https://doi.org/10.1017/cri.2025.1>

Sumsub. (2024, November). *Sumsub launches Global Fraud Index, revealing top risks and insights for Africa* [Press release]. https://www.einpresswire.com/article_pdf/758103126/sumsub-launches-global-fraud-index-revealing-top-risks-and-insights-for-africa

TechAfrica News. (2026, September 2). Ghana Cyber Security Authority launches 2026 awareness month to strengthen digital finance security. <https://techafricanews.com/2026/09/02/ghana-cyber-security-authority-launches-2026-awareness-month-digital-finance/>

U.S. Attorney’s Office, District of Maryland. (2024, August 30). *Nigerian national extradited from Ghana to face charges for an alleged \$7.5 million business email compromise scheme involving two charitable organizations*. <https://www.justice.gov/usao-md/pr/nigerian-national-extradited-ghana-face-charges-alleged-75-million-business-email>

U.S. Attorney’s Office, Southern District of New York. (2025, August 8). *Ghanaian nationals extradited for roles in criminal organization that stole more than \$100 million through romance scams and other fraud*. <https://www.justice.gov/usao-sdny/pr/ghanaian-nationals-extradited-roles-criminal-organization-stole-more-100-million>

U.S. Attorney’s Office, Southern District of New York. (2026, July 28). *Ghanaian national sentenced to 85 months in prison for stealing more than \$10 million via romance scams*. <https://www.justice.gov/usao-sdny/pr/ghanaian-national-sentenced-85-months-prison-stealing-more-10-million-romance-scams>.