

Ghana's Cybersecurity Paradox: A Nation of Policy Leadership and Pervasive Threats

Executive Summary

Ghana presents a compelling and complex case study in the global cybersecurity landscape, defined by a significant paradox. On one hand, the nation has achieved remarkable success in developing a comprehensive and internationally acclaimed cybersecurity governance framework. This is evidenced by its 'Tier 1: Role Modelling' status in the 2024 International Telecommunication Union (ITU) Global Cybersecurity Index, a distinction held by only a select group of countries worldwide. This achievement is the result of a concerted, multi-year effort to establish a robust legal and institutional bedrock, including the passage of the landmark Cybersecurity Act, 2020 (Act 1038), the creation of the empowered Cyber Security Authority (CSA), and the implementation of a forward-looking National Cybersecurity Policy and Strategy.

On the other hand, this top-tier policy architecture coexists with a pervasive and escalating domestic cybercrime problem. Financial losses from cybercrime are rising sharply, with Ghana losing over GH¢38 million in the 18 months leading up to mid-2025. The country faces a high volume of cyberattacks, and the threat landscape is evolving from common cyberfraud to sophisticated attacks targeting critical infrastructure, leveraging AI-driven deepfakes, and exploiting the nation's rapidly expanding mobile money ecosystem. This on-the-ground reality of pervasive threats starkly contrasts with the nation's celebrated policy readiness.

This report deconstructs this paradox by analyzing its core components. It examines how Ghana's high rankings are a measure of its commitment and the strength of its policy inputs, rather than a direct reflection of security outcomes. The analysis reveals a two-tier cybersecurity ecosystem, where a highly resilient financial sector, driven by strong, sector-specific regulation from the Bank of Ghana, stands in contrast to more vulnerable sectors like healthcare and small-to-medium enterprises (SMEs).

The persistence of cybercrime is traced to systemic challenges, including a significant public awareness gap, a critical shortage of skilled cybersecurity professionals, and persistent enforcement hurdles. The report concludes by evaluating Ghana's future strategies, including plans for specialized cybercrime courts and a national AI governance framework, which demonstrate a maturing understanding of the challenges. Strategic recommendations are provided for government, the private sector, and public education initiatives, focusing on bridging the critical gap between policy and implementation. To secure its digital future, Ghana must now pivot from building its world-class cybersecurity framework to ensuring its effective and universal enforcement on the ground.

Section 1: Ghana's Ascent as a Global Cybersecurity Leader

Ghana's journey in the realm of cybersecurity has been one of rapid and strategic transformation. In less than a decade, the nation has evolved from a position of relative obscurity to being recognized as a continental and global leader in cybersecurity preparedness. This ascent is not accidental but the result of deliberate policy, legislative action, and sustained government commitment, a trajectory best captured by its performance in premier international benchmarks and the acknowledgment of its leadership by global partners.

1.1 Charting the Rankings: From Laggard to 'Role Model'

The most telling metric of Ghana's progress is its dramatic improvement in the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI). The GCI is a trusted global reference that measures the commitment of countries to cybersecurity across five key pillars, providing a snapshot of their preparedness.¹

Ghana's journey began from a low baseline. In the 2017 and 2018 GCI reports, the country registered scores of just 32.6% and 43.7%, respectively, placing it 11th on the African continent.¹ These figures reflected a nascent cybersecurity ecosystem still in the early stages of development. However, the subsequent period saw a monumental leap forward. The 2020 GCI report, released in June 2021, awarded Ghana a score of 86.69%.¹ This propelled the nation to the 3rd position in Africa, trailing only Mauritius and Tanzania, and marked a significant jump to 43rd globally. This achievement was widely seen as direct proof of the government's dedication to developing a secure and resilient cyberspace to support its ambitious digital transformation agenda.¹

The culmination of this progress came with the 2024 GCI report, which introduced a new five-tiered ranking system. Ghana achieved the highest possible classification, 'Tier 1: Role Modelling', with a near-perfect score of 99.27%.² This elite status signifies that Ghana's cybersecurity framework is considered advanced and serves as a benchmark for other nations to emulate.² In this latest assessment, Ghana ranks as the second-highest scoring country in Africa, after Mauritius, and is one of only five African nations and 46 countries worldwide to attain this top tier.² This leadership position stands in stark contrast to other major regional economies like Nigeria and Cameroon, which were placed in the 'Tier 3: Establishing' category, indicating they are still in the process of setting up key cybersecurity initiatives.²

Table 1: Evolution of Ghana's Global Cybersecurity Index (GCI) Ranking (2017-2024)

1.2 The Five Pillars of Success: A Strategic Deconstruction

Ghana's exceptional GCI score is built upon a comprehensive and well-structured approach that addresses all five strategic pillars of the ITU's Global Cybersecurity Agenda (GCA). This demonstrates a holistic strategy that integrates legal, technical, organizational, human, and diplomatic dimensions of cybersecurity.¹

Legal Measures: The cornerstone of Ghana's legal framework is the passage of the landmark Cybersecurity Act, 2020 (Act 1038). This single piece of legislation provided a robust legal basis for regulating the entire cybersecurity ecosystem, from service providers to critical infrastructure, and established clear offenses and penalties for cybercrime.¹

Technical Measures: A key technical achievement has been the development of Ghana's national Computer Emergency Response Team (CERT) ecosystem. This includes the establishment of a national CERT (CERT-GH) to coordinate incident response and the creation of sectoral CERTs for critical industries, enhancing the country's technical capacity to handle threats.¹

Organisational Measures: The government has put in place a sophisticated organizational structure. This includes the revision of the National Cybersecurity Policy and Strategy (NCPS) to provide a clear national direction and the establishment of multi-stakeholder bodies like the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) and the National Cyber Security Technical Working Group (NCSTWG) to ensure a whole-of-government approach.¹ The most significant organizational step was the formal transition of the National Cyber Security Centre (NCSC) into the fully-fledged Cyber Security Authority (CSA), an independent body with regulatory power.¹

Capacity Building: Ghana has demonstrated a persistent commitment to building human capacity and raising public awareness. The institutionalization of the annual National Cyber Security Awareness Month (NCSAM) every October has become a flagship initiative, alongside continuous training programs for law enforcement, public and private sector institutions, and academia.¹

International Cooperation: Recognizing the borderless nature of cyber threats, Ghana has become an active participant in the global cybersecurity community. The country has ratified key international treaties, including the Budapest Convention on Cybercrime and its Second Additional Protocol, and has contributed significantly to the development of the UN Convention on Cybercrimes.² This commitment has positioned Ghana as a regional hub for cybersecurity training, recognized by partners such as the European Union, the Council of Europe, the World Bank, and ECOWAS.²

The high GCI score is not merely a number; it reflects a deliberate and successful effort to build a world-class cybersecurity governance architecture. This architecture is designed to be comprehensive, covering policy, law, technical response, and human factors. However, it is crucial to understand that the GCI primarily assesses the existence and maturity of these frameworks—the inputs and commitments of a nation—rather than the direct outcomes, such as the on-the-ground level of cybercrime or the effectiveness of enforcement. This distinction is fundamental to understanding the paradox at the heart of Ghana's cybersecurity story. The nation has successfully constructed a sophisticated machine for cybersecurity governance; the challenge lies in translating that structural strength into consistent operational security for all its citizens and enterprises.

1.3 International Recognition and Regional Leadership

Ghana's strategic efforts have not gone unnoticed. The country's rapid progress has been validated by key international development partners, cementing its reputation as a model for other developing nations.

The World Bank has explicitly identified Ghana as a "regional leader for cybersecurity," producing a detailed case study to explore the key milestones and decisions that led to its success so that other countries might learn from its experience.⁹ This recognition is not just based on rankings but on tangible outcomes of a long-term partnership. Since 2006, World Bank projects have provided approximately \$20 million earmarked for cybersecurity in Ghana, support that proved instrumental in establishing foundational elements like the national CSIRT and the CSA itself.¹⁰ This sustained international partnership acted as a powerful accelerator, providing not only funding but also access to global best practices and technical expertise, which allowed Ghana to adopt a mature framework more rapidly than it might have otherwise.

Further burnishing its credentials as an "international champion," Ghana hosted the inaugural Global Conference on Cyber Capacity Building (GC3B) in November 2023, bringing together global leaders to shape the future of cybersecurity development.¹⁰ This leadership role is also reflected in its relationships with its African peers. Nations such as The Gambia, Sierra Leone, and Mozambique have formally approached the CSA seeking collaboration and guidance in developing their own cybersecurity frameworks, viewing Ghana as a continental model to emulate.⁸ This proactive engagement from other countries serves as one of the clearest indicators of Ghana's successful ascent to a position of regional cybersecurity leadership.

Section 2: The Legislative and Institutional Bedrock

The foundation of Ghana's high international standing in cybersecurity is a meticulously constructed set of legal and institutional frameworks. These structures provide the authority, mandate, and strategic direction for all national cybersecurity activities. The centerpiece of this architecture is the Cybersecurity Act, 2020, which created the powerful Cyber Security Authority and set forth a comprehensive national strategy. This deliberate move from an advisory to a regulatory posture has been pivotal in professionalizing the sector and establishing clear rules of engagement for both public and private actors.

2.1 The Cybersecurity Act, 2020 (Act 1038): A Comprehensive Legal Framework

Passed in 2020, the Cybersecurity Act (Act 1038) is the cornerstone of Ghana's legal and regulatory environment for cybersecurity. It replaced a patchwork of older laws, such as the Electronic Transactions Act of 2008, which were no longer adequate to address the modern threat landscape.¹³ Act 1038 provides a single, comprehensive framework designed to regulate cybersecurity activities, protect the nation's digital assets, and align Ghana with international best practices.⁵ The Act's provisions are extensive, creating a proactive and regulatory governance model.

Table 2: Key Provisions and Mandates of the Cybersecurity Act, 2020 (Act 1038)

While the Act is comprehensive, the rapid pace of technological change presents an ongoing challenge. Passed in 2020, the legislation does not explicitly address threats that have since become prominent, such as the malicious use of artificial intelligence and deepfakes.¹⁸ Recognizing this, the government has already signaled its intent to review and amend the Act to ensure it remains responsive to emerging threats, a proactive stance that reflects a mature understanding of the dynamic nature of cybersecurity law.²⁰

2.2 The Cyber Security Authority (CSA): The Engine of Implementation

The Cybersecurity Act, 2020, formally established the Cyber Security Authority (CSA) as the central engine for implementing the nation's strategy.⁵ The CSA's creation on October 1, 2021, marked the culmination of an institutional evolution that began with the small National Cyber Security Secretariat (NCSS) in 2017 and the subsequent National Cyber Security Centre (NCSC) in 2018.⁶ This transition from a secretariat to a full-fledged authority with regulatory power was a critical step, transforming the government's role from advisory to enforcement.

The CSA's mandate is broad and multi-faceted, aiming to achieve the national vision of "A Secure and Resilient Digital Ghana".⁶ Its core functions include ⁶:

Regulation: Overseeing the entire cybersecurity sector, including licensing professionals and service providers, and regulating the owners of Critical Information Infrastructure.

Incident Management: Preventing, managing, and responding to cybersecurity threats and incidents nationwide through its operational arm, the National CERT (CERT-GH).

Development and Awareness: Promoting the development of the cybersecurity industry, creating public awareness of cyber threats, and building national capacity.

Collaboration: Establishing platforms for cross-sector engagement, most notably through the Joint Cybersecurity Committee (JCC), which coordinates the efforts of over 15 public institutions, and collaborating with international agencies to strengthen Ghana's posture.²⁴

Operationally, the CSA has become the public face of Ghana's cybersecurity efforts. It manages the Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC), which has provided a vital channel for citizens and organizations to report threats.¹ It also leads the annual National Cyber Security Awareness Month, a cornerstone of its public education mandate.²⁵ The implementation of a mandatory licensing and accreditation regime for all cybersecurity professionals and businesses since 2023 is one of its most significant regulatory actions, aimed at professionalizing the industry and ensuring a high standard of service delivery.²⁶

2.3 The National Cybersecurity Policy and Strategy (NCPS): The Strategic Blueprint

Guiding the CSA and the nation as a whole is the National Cybersecurity Policy and Strategy (NCPS). The revised version, launched in 2024, serves as a comprehensive five-year roadmap for safeguarding Ghana's digital landscape.⁴ The NCPS is explicitly designed to be a strategic response to both existing and anticipated cyber threats that could undermine the country's progress in digitalization.⁴

The policy is built around five strategic objectives that mirror the ITU's pillars 4:

Build a Resilient Digital Ecosystem.

Secure Digital Infrastructure.

Develop National Capacity.

Deter Cybercrime.

Strengthen Cooperation.

A key tenet of the NCPS is its emphasis on a multi-stakeholder, whole-of-society approach. It recognizes that cybersecurity is a shared responsibility that cannot be shouldered by the government alone.⁴ To this end, the policy formalizes the roles of various collaborative bodies. The Joint Cybersecurity Committee (JCC) serves as the primary vehicle for coordinating efforts across public sector institutions, while the creation of an Industry Forum is intended to facilitate partnership and standard-setting with the private sector.⁴ The CSA is designated as the lead agency responsible for overseeing the implementation of the NCPS, ensuring that the strategic initiatives outlined in the policy are translated into concrete actions with clear timelines and stakeholder responsibilities.²⁸

Section 3: The Pervasive Threat Landscape: A Contradictory Reality

Despite Ghana's internationally recognized achievements in building a robust cybersecurity framework, the nation grapples with a severe and escalating on-the-ground cybercrime problem. This contradictory reality forms the central paradox of its cybersecurity posture. The data on financial losses and incident frequency paints a grim picture, revealing a dynamic and adaptive threat landscape that directly challenges the effectiveness of the country's policy architecture. The nature of these threats has evolved in lockstep with Ghana's own digital transformation, shifting from basic scams to sophisticated attacks on critical economic and social infrastructure.

3.1 The Scale of the Epidemic: Quantifying the Damage

The statistics on cybercrime in Ghana reveal a problem of epidemic proportions, with a clear and alarming upward trend in both the volume of incidents and the financial cost to the nation. While Ghana has a long history of being a hub for certain types of cybercrime, ranking 7th in a 2008 Internet Crime Survey, the recent data indicates a significant acceleration of the threat.⁷

Between 2016 and 2018, the country lost over US\$200 million to recorded cybercrime cases, establishing the significant economic stakes involved.⁷ More recent and granular data from the Cyber Security Authority (CSA) and law enforcement confirms that the problem is intensifying:

Financial Losses: In 2024, Ghana lost GH¢23.3 million to cybercrime. In just the first half of 2025, this figure reached GH¢14.9 million, representing a 17% increase compared to the same period in the previous year. This puts the total losses over that 18-month period at over GH¢38 million.¹⁸

Incident Volume: The number of reported cyber incidents surged from 1,317 in the first half of 2024 to 2,008 in the first half of 2025—a more than 50% increase.¹⁹ Over the longer term, from 2019 to 2023, a total of 3,804 actual incidents were officially reported to the CSA.³⁵

Attack Frequency: Beyond reported incidents, Ghana is a major target for automated and large-scale attacks. According to a NETSCOUT report, in the first half of 2024, Ghana faced the highest volume of cyberattacks in West Africa, enduring a total of 4,753 Distributed Denial of Service (DDoS) attacks. A significant portion of these attacks (2,759) were aimed at computer-related services businesses and telecommunications carriers.³⁶

Table 3: Reported Cybercrime Incidents and Financial Losses in Ghana (2019-2025)

3.2 Anatomy of Cybercrime in Ghana: From "Sakawa" to Sophisticated Attacks

The threat landscape in Ghana is diverse, ranging from long-established forms of fraud to cutting-edge, technologically advanced attacks. This evolution directly mirrors the country's own digitalization journey, as criminals continuously adapt their methods to exploit new technologies and attack surfaces.

Cyberfraud (The Dominant Threat):

Cyberfraud remains the most prevalent category of cybercrime in Ghana, consistently accounting for more than half of all reported cases and over 90% of the total financial losses.⁷ This broad category includes several distinct types:

Romance Scams and Identity Fraud: This is a long-standing issue where perpetrators create fake online profiles, often on social media and dating sites, to build relationships with victims (frequently older individuals in Western countries) and manipulate them into sending money or gifts.⁷

Commercial Fraud: This includes schemes like fake gold dealerships that target foreign investors with promises of lucrative returns on non-existent gold mines, and estate fraud that targets Ghanaians in the diaspora by selling them fraudulent land and housing blueprints for their retirement.⁷

"Sakawa": Unique to Ghana is the socio-cultural phenomenon of "sakawa," which combines internet-based fraud with West African traditionalist religious rituals. Practitioners seek blessings from priests in the belief that it will improve their success in online scams, indicating a deep-seated social dimension to the problem that goes beyond pure technology.⁷ The persistence of "sakawa" suggests that for some, particularly unemployed youth, cybercrime is perceived as a viable, if illicit, path to wealth, a notion supported by broader regional data showing high unemployment rates among identified cybercriminals.³⁰

Mobile Money and Financial Sector Threats:

The explosive growth of Ghana's mobile money market, which processed transactions exceeding GH¢570 billion in 2024, has created a massive and lucrative target for criminals.³⁸ Attacks on this ecosystem are increasingly sophisticated and include:

Technical Exploits: Techniques such as API manipulation, session hijacking, and the creation of fake mobile payment apps are used to steal credentials or directly redirect funds.³⁸

SIM Swapping: A particularly damaging method where fraudsters use forged identity documents (like the Ghana Card) to obtain a duplicate SIM card for a victim's number. This allows them to take over the victim's mobile money account, intercept one-time passwords, and drain funds before the legitimate owner can regain control.³⁹

Insider Collusion: A critical vulnerability in the system is the role of insiders. There are documented cases of employees within telecommunication companies providing criminals with privileged subscriber information, such as account balances and personal details, to facilitate targeted attacks.³⁹

Emerging and Sophisticated Threats:

As Ghana's digital economy matures, so do its adversaries. Criminals are now leveraging advanced technologies to perpetrate more complex and damaging attacks:

AI and Deepfakes: Malicious actors are using artificial intelligence to create and circulate deepfake videos of prominent figures, including the president and cabinet ministers, falsely endorsing fraudulent investment schemes or medical

products on social media platforms.¹⁸

Ransomware: Attacks have evolved from opportunistic to highly targeted assaults on critical infrastructure. Sectors including banking, healthcare, and energy have faced sophisticated ransomware threats, with attackers employing "double-extortion" tactics where they not only encrypt data but also exfiltrate it and threaten to publish it if the ransom is not paid.³⁸

Supply Chain Attacks: Instead of attacking well-defended organizations directly, criminals are compromising their less secure third-party vendors, such as cloud service providers. A single compromised vendor can provide a backdoor into the systems of dozens of their client organizations, exploiting trusted relationships to bypass defenses.³⁸

Online Impersonation: A growing tactic involves criminals creating fake business profiles on platforms like Google Maps and search listings. These fake profiles redirect unsuspecting users to counterfeit websites designed to harvest credentials, PINs, and one-time passwords, enabling unauthorized access to mobile money and bank accounts.¹⁸

Other Prevalent Crimes:

Beyond financial fraud, other forms of cybercrime are also rampant. Cyberbullying and online blackmail are the second and third most commonly reported types of incidents, accounting for 25% and 14% of cases, respectively.²¹ A unique form of blackmail in Ghana is linked to the country's status as a major global destination for electronic waste. Criminals scavenge discarded hard drives from e-waste dumpsites in search of sensitive personal or corporate data that can be used for extortion.⁷

Section 4: Sector-Specific Analysis: Resilience and Vulnerability

Ghana's national cybersecurity posture is not monolithic. A closer examination reveals a landscape of starkly contrasting maturity levels across different sectors of the economy. While the financial sector has emerged as a model of proactive and resilient cybersecurity governance, other critical areas such as healthcare and the vast small and medium enterprise (SME) sector remain dangerously vulnerable. This uneven development creates systemic weaknesses, as the nation's overall security is only as strong as its most susceptible link. The telecommunications sector, meanwhile, occupies a pivotal position as both a critical line of defense and a primary target for malicious actors.

4.1 The Financial Sector: A Proactive Model of Resilience

The Ghanaian financial sector stands out as a benchmark for effective, sector-specific cybersecurity. This resilience is not a matter of chance but the direct result of proactive leadership and stringent regulation by the Bank of Ghana (BoG). The BoG recognized the systemic risk posed by cyber threats early on and moved decisively to build a collaborative, sector-wide defense mechanism.

The foundation for this was the Cyber & Information Security Directive, issued by the BoG in 2018. This comprehensive directive established a clear framework of protocols and procedures for all regulated financial institutions. Crucially, it mandated that every institution establish its own internal Security Operations Centre (SOC), creating a layered defense system across the industry.⁴¹

The capstone of this strategy is the Financial Industry Command Security Operation Centre (FICSOC), launched in May 2023. FICSOC is a centralized, state-of-the-art command center operated by the BoG, making it one of the few sector-wide SOC's in Africa. Its mandate is to provide real-time, system-wide threat intelligence, monitoring, and incident response coordination for all 23 licensed banks and the central bank itself.⁴¹ Since its launch, FICSOC has already proven its value by helping to mitigate zero-day threats and address multiple vulnerabilities across participating institutions.⁴¹

This model demonstrates a powerful lesson: strong, sector-specific regulation drives maturity. The BoG did not wait for a national crisis to act; it used its regulatory authority to compel investment and collaboration, effectively hardening the entire financial sector against cyber threats. Furthermore, the BoG is actively working to extend this security umbrella to include mobile money operators and smaller financial institutions, recognizing that the actors driving financial inclusion are also critical nodes of vulnerability that must be protected.⁴¹ Under the Cybersecurity Act, the BoG is formally designated as the Sectoral CERT lead for the entire financial industry, solidifying its leadership role.⁴¹

4.2 The Telecommunications Sector: Critical Infrastructure and Key Players

As the providers of the digital backbone for the nation, telecommunication companies in Ghana are central to the cybersecurity ecosystem. They are both critical infrastructure that must be defended and primary targets for criminals seeking to exploit their networks and customer data. The sector is dominated by a few major players.

MTN Ghana: With a commanding 61% market share, MTN is the largest operator and a pivotal actor in the digital economy.⁴³ The company has demonstrated a commitment to cybersecurity awareness, hosting its "Business Executive Breakfast" series to educate SMEs on digital threats and running public outreach programs for students and customers during National Cyber Security Awareness Month.⁴⁴ However, its size and prominence also make it a prime target. In April 2025, MTN Group confirmed a data breach that potentially exposed the personal information of 5,700 Ghanaian customers, triggering a formal investigation by the country's Data Protection Commission and underscoring the persistent risks faced even by well-resourced operators.⁴⁸

Telecel (formerly Vodafone Ghana): Telecel operates under the robust global cybersecurity framework of its former parent, the Vodafone Group, which is based on leading industry standards from the US National Institute of Standards and Technology (NIST) and is supported by a global team of over 900 security experts.⁵¹ The company is also active in digital skills development for youth, including providing mentorship in cybersecurity through its participation in the National Girls in ICT initiative.⁵⁴ However, academic research focusing on Vodafone Ghana has pointed to historical challenges, including a lack of cross-firm collaboration on enterprise risk management strategies and concerns about lax enforcement of national policies at the operational level.⁵⁵

AirtelTigo: Now wholly owned by the Government of Ghana, AirtelTigo remains a significant player with a 19% market share.⁴³ As a major provider of mobile money services, it is an integral part of the financial ecosystem and, by extension, a key component of the cybercrime attack surface, though specific public-facing cybersecurity initiatives are less documented.⁴¹

4.3 Vulnerable Sectors: The Soft Underbelly

In sharp contrast to the highly regulated financial sector, several other critical sectors in Ghana exhibit low levels of cybersecurity maturity, creating a "soft underbelly" that poses a systemic risk to the entire nation.

Healthcare: The Cyber Security Authority has issued explicit warnings that the security maturity level of Ghana's health sector is "very low".⁵⁷ A recent assessment of 15 health institutions, including public and private hospitals, uncovered multiple instances of critical-severity vulnerabilities. These included the use of outdated software, a lack of password encryption on sensitive systems, susceptibility to DDoS attacks, and web server misconfigurations.⁵⁷ Such weaknesses not only risk the exposure of sensitive patient data but could also lead to the disruption of critical healthcare services.

Government Services: The government's rapid digitization of public services—such as e-Parliament, e-Justice, and e-Passport systems—has expanded the attack surface for adversaries seeking to disrupt governance or steal citizen data.²⁴ A successful attack on these systems could have far-reaching consequences, affecting millions of citizens simultaneously.³³ The threat is not theoretical; credentials from 35 different government ministries and state-affiliated organizations have already been found circulating on the dark web, exposing them to potential national-level breaches.³¹

Small and Medium Enterprises (SMEs): SMEs are the backbone of the Ghanaian economy but are often the most vulnerable to cyberattacks. Due to significant resource constraints, many SME owners view cybersecurity not as an essential investment but as an "unnecessary expense".³³ This mindset, combined with a lack of in-house technical expertise, makes them attractive and easy targets for cybercriminals. Their vulnerability creates a ripple effect, as SMEs are often part of the supply chains of larger, more secure corporations, providing an insecure entry point for attackers.⁴⁵

This emerging two-tier cybersecurity ecosystem—with a hardened financial core and a soft, vulnerable periphery—is one of Ghana's most significant strategic challenges. Malicious actors can exploit the weaknesses in a low-resilience sector, like a small supplier or a regional hospital, to launch attacks against more secure targets, thereby circumventing stronger defenses. Achieving a truly resilient national digital ecosystem will require a concerted effort to elevate the security posture of these lagging sectors to match the standards set by the nation's leaders.

Section 5: Enduring Challenges and Systemic Gaps

The paradox of Ghana's high policy ranking and its persistent cybercrime problem is rooted in a series of deep-seated, systemic challenges. These gaps exist at the intersection of human behavior, economic realities, and enforcement capacity. While the nation has successfully built an impressive top-down governance structure, its effectiveness is

consistently undermined by bottom-up vulnerabilities. Addressing these enduring challenges is the critical next step in translating Ghana's strategic achievements into tangible, nationwide security.

5.1 The Human Factor: The Weakest Link

Despite significant government efforts, the human element remains the most exploited vulnerability in Ghana's cybersecurity defenses. This manifests in two primary areas: a widespread public awareness gap and a critical shortage of specialized skills.

Public Awareness and Digital Literacy Gaps:

Ghana has institutionalized public awareness initiatives, most notably the annual National Cyber Security Awareness Month (NCSAM).¹ However, evidence suggests a significant disconnect between these campaigns and the actual online behavior of the population. A study by IBM found that human error accounts for as much as 95% of cybersecurity breaches, a statistic that highlights the limits of awareness without behavioral change.⁵⁸

Many users still lack basic cyber hygiene, such as creating strong, unique passwords, utilizing multi-factor authentication, and consistently identifying phishing attempts and other social engineering tactics.¹⁹ This "awareness paradox"—where campaigns exist but risky behaviors persist—indicates that current outreach may not be sufficiently continuous, practical, or culturally resonant to be effective. Academic research on literate mobile money users in Ghana found that while they were generally aware of common threats like impersonation and agent fraud, significant knowledge gaps remained concerning more technical vulnerabilities.⁵⁶ Another study focusing on teenagers revealed that while nearly 75% claimed to be aware of cybersecurity, a mere 1.8% would report a cybercrime incident to the police, suggesting a profound lack of trust in or knowledge of official reporting channels.⁶⁰

The Digital Skills Gap:

Compounding the problem of user vulnerability is an acute shortage of skilled cybersecurity professionals within Ghana. This skills gap is not merely an industry concern; it represents a fundamental threat to national security and economic competitiveness. The demand for cybersecurity experts has surged as organizations across all sectors digitize, but the local supply of qualified talent has failed to keep pace.⁵⁹

This shortage has several negative consequences:

It drives up the cost of security services, making them unaffordable for many SMEs and even some public institutions.⁵⁹

It creates a "brain drain," as the limited pool of trained Ghanaian professionals is often lured by more lucrative opportunities abroad, resulting in a net loss of national capacity.³³

It forces Ghanaian companies to recruit internationally for digital talent, with 70% of those who do so citing a lack of skilled locals as the primary reason.⁶¹

A 2019 report by the International Finance Corporation (IFC) and the World Bank highlighted this broader digital skills deficit in Ghana, noting a significant undersupply of talent relative to market demand.⁶¹ While not focused exclusively on cybersecurity, the report underscores a foundational weakness in the tech talent pipeline that directly impacts the country's ability to build and sustain a robust cybersecurity workforce. Without a sufficient number of trained defenders, Ghana's sophisticated security infrastructure risks being a hollow shell, lacking the human capital needed to operate it effectively.

5.2 Economic and Enforcement Hurdles

The economic consequences of cybercrime extend far beyond the direct financial losses, creating second-order effects that threaten Ghana's entire digital transformation agenda. These economic pressures are exacerbated by persistent challenges in law enforcement and regulation.

Economic Impact of Cybercrime:

The most insidious impact of rampant cybercrime is the erosion of trust, which is the bedrock of any digital economy.

Damage to Investor Confidence: Ghana has positioned itself as a regional technology hub to attract foreign investment. However, persistent and high-profile cybercrime could undermine this reputation, making international businesses hesitant to establish local operations and invest in the country's digital infrastructure.¹⁸ The CEO of the Ghana Investment Promotion Centre has warned that cybersecurity is not just a technical issue but an "economic imperative" central to maintaining investor confidence.¹⁸

Erosion of Consumer and Business Trust: The constant threat of fraud deters both consumers and businesses from fully embracing digital platforms. Studies on e-commerce in Ghana show that concerns about cybercrime, including fraud and identity theft, are significant barriers to adoption and negatively affect users' intention to make purchases online.⁶³ This stifles the growth of the local digital economy and discourages SMEs from digitizing their operations for fear of falling victim to scams.¹⁹

Enforcement and Regulatory Gaps:

Despite a strong legal framework on paper, its practical application faces significant hurdles.

Prosecution Challenges: Law enforcement agencies face difficulties in successfully prosecuting cybercrime cases, partly due to challenges in collecting and preserving electronic evidence in a manner that is admissible in court under existing acts.⁷

Weak Public-Private Cooperation: A critical gap exists in the collaboration between law enforcement and the private sector, particularly telecommunication companies. Officials from the Economic and Organised Crime Office (EOCO) have reported that their investigations are often hampered by weak cooperation from telcos, who may delay action on fraud reports or be reluctant to share information about system vulnerabilities for fear of damaging their market reputation.³⁹

Regulatory Vacuum in Fintech: The fintech sector, especially the mobile money ecosystem, has grown so rapidly that regulatory frameworks have struggled to keep pace. This has created gaps in the oversight of mobile money providers and other fintech firms, leaving them and their customers exposed.³⁹

Section 6: The Future Trajectory: Strategy, Innovation, and Recommendations

Recognizing the gap between its policy achievements and the on-the-ground reality, Ghana's government is charting a forward-looking course aimed at strengthening its defenses, closing systemic loopholes, and preparing for the next wave of technological change. The planned initiatives—from judicial reforms to a national AI strategy—demonstrate a maturing understanding of the multifaceted nature of cybersecurity. This final section evaluates these future strategies and provides actionable recommendations for key stakeholders to help bridge the critical policy-implementation gap and secure Ghana's digital future.

6.1 Forward-Looking Government Initiatives: Strengthening the Framework

The government's planned initiatives show a strategic intent to address the core weaknesses identified in the current ecosystem: enforcement, funding, and cross-sector coordination.

Legislative and Judicial Reforms: Acknowledging that the threat landscape evolves faster than legislation, the Ministry of Communication, Digital Technology and Innovations has initiated a review of the Cybersecurity Act, 2020, to ensure it can effectively tackle emerging threats like AI-driven manipulation.²⁰ Perhaps the most significant planned reform is the collaboration with the Attorney-General's Office and the Ministry of Justice to establish specialized courts dedicated solely to cybercrime. This move is designed to accelerate the prosecution of offenders and build judicial expertise in handling complex electronic evidence, directly addressing a major enforcement bottleneck.²⁰

Financial and Structural Enhancements: To combat the chronic underfunding that has limited defensive capabilities, particularly in the public sector and for SMEs, the government plans to establish a Cybersecurity Fund. As outlined in the Cybersecurity Act, this fund will provide a sustainable financing mechanism for national cyber initiatives, capacity building, and the protection of critical infrastructure.⁵⁸ Structurally, there are plans to expand the successful sectoral CERT model beyond finance and telecoms to other critical sectors, including energy, health, academia, and transport, thereby raising the security baseline across the entire economy.⁶⁸

Strengthening International Cooperation: The government has reaffirmed its commitment to working with global partners to combat transnational cybercrime. President John Mahama has pledged to enhance cooperation with agencies like the FBI to track, arrest, and prosecute offenders involved in romance scams and other financial crimes, utilizing extradition treaties where necessary.²⁰ A Joint Cyber Security Committee has also been established to

formalize collaboration with international security partners, ensuring a unified approach to protecting Ghana's cyberspace.⁵⁸

These planned reforms indicate that Ghana's leadership has correctly diagnosed the primary obstacles to effective cybersecurity. The focus on a dedicated fund addresses resource constraints, the specialized courts target the enforcement gap, and the expansion of sectoral CERTs aims to correct the uneven maturity across the economy. Together, these initiatives represent a shift toward reinforcing the operational capacity needed to give the country's legal and policy frameworks real teeth.

6.2 Securing Emerging Technologies: The Next Frontier

In a remarkably proactive move, Ghana is not only working to solve today's cybersecurity problems but is also laying the groundwork to govern the technologies of tomorrow. By developing a national strategy for artificial intelligence and other emerging technologies before their widespread adoption, Ghana is attempting to "leapfrog" the reactive regulatory posture that has challenged many developed nations.

National AI Strategy: The government has unveiled a comprehensive National AI Strategy that aims to guide the ethical, inclusive, and secure deployment of artificial intelligence across key sectors, including healthcare, agriculture, education, and public administration.⁷⁰ A key component of this strategy is the digitization of essential national datasets to ensure that AI models are trained on local data, reflecting Ghanaian cultural nuances and preventing the reinforcement of foreign biases.⁷² A presidential directive has been issued requiring all government agencies to adopt AI tools by 2026 to improve efficiency and service delivery.⁷¹

Emerging Technologies Bill: To provide a legal foundation for this strategy, an Emerging Technologies Bill is being drafted for submission to Parliament. This legislation is set to cover AI, blockchain, and robotics, and aims to strike a careful balance between fostering innovation and ensuring robust regulation. The bill will establish clear ethical standards, data protection requirements, and accountability frameworks for the use of these technologies.⁷⁰ By creating a predictable and safe regulatory environment, the government aims to build public trust and attract high-quality foreign investment into its burgeoning tech sector.

This forward-looking approach to tech governance is highly strategic. However, its ultimate success is contingent on resolving the foundational cybersecurity weaknesses that persist today. An advanced AI ecosystem built upon a foundation of low public awareness, a significant skills gap, and weak enforcement would create vulnerabilities of a far greater magnitude.

6.3 Strategic Recommendations: Closing the Policy-Implementation Gap

To translate its world-class policy framework into effective, on-the-ground security, Ghana must prioritize closing the gap between strategy and execution. The following recommendations are targeted at key stakeholders to address the systemic challenges identified in this report.

For Government and Regulators:

Pivot from Framework Development to Rigorous Enforcement: The primary focus must now shift from creating new policies to ensuring the existing ones are enforced. The Cyber Security Authority should be empowered with increased budgetary and human resources to conduct regular, mandatory audits and compliance checks on all designated Critical Information Infrastructure, with meaningful penalties for non-compliance.

Replicate the Bank of Ghana's Regulatory Model: The BoG's proactive, directive-led approach to securing the financial sector should be used as a blueprint for other critical sectors. Sector-specific regulators, particularly in healthcare and energy, must be mandated and resourced to develop and enforce similar binding cybersecurity directives for their licensees.

Accelerate Judicial and Law Enforcement Capacity Building: The establishment of specialized cybercrime courts should be fast-tracked. This must be accompanied by a continuous training program for judges, prosecutors, and police investigators on the nuances of handling electronic evidence, digital forensics, and the technical aspects of modern cybercrime.

For the Private Sector (especially Telcos and Financial Institutions):

Establish a Formalized Public-Private Threat Intelligence Sharing Platform: Move beyond ad-hoc cooperation to create a trusted, formalized mechanism for real-time, bi-directional sharing of threat intelligence and incident data between major private sector actors (telcos, banks), the CSA, and law enforcement agencies like EOCO. This will help overcome the current reluctance to share information and enable a more coordinated national response.

Invest Strategically in the Local Talent Pipeline: To combat the brain drain and fill the critical skills gap, leading tech companies should form strategic partnerships with Ghanaian universities and training institutions.⁷⁵ This should involve co-developing curricula, funding specialized cybersecurity labs, offering robust internship programs, and creating competitive, long-term career paths within Ghana to retain top talent.

For Public Education and Awareness:

Evolve from Annual Campaigns to Continuous, Targeted Education: The NCSAM is a good foundation, but it is not enough. A continuous, multi-channel public education strategy is needed. This strategy should use culturally relevant messaging in local languages and target the most vulnerable populations (e.g., the elderly, rural mobile money users, and youth) through channels they trust, such as community radio, local leaders, and mobile-first content.

Integrate Cyber Hygiene into the National Education Curriculum: In collaboration with the Ministry of Education, fundamental cybersecurity principles—such as password hygiene, identifying phishing, and understanding digital privacy—should be embedded into the national school curriculum from the primary level upwards to build a generation of digitally resilient citizens.

Works cited

Ghana's cybersecurity development ranked third in africa - CSA || News, accessed October 11, 2025, https://www.csa.gov.gh/csa_rank.php

Ghana Ranked tier 1 Status in Latest ITU Global Cybersecurity Index, accessed October 11, 2025, <https://moc.gov.gh/2024/09/16/ghana-ranked-tier-1-status-in-latest-itu-global-cybersecurity-index/>

Ghana to strengthen national Cybersecurity Agency - African Wireless Communications, accessed October 11, 2025, <https://www.africanwirelesscomms.com/news-details?itemid=8998>

Ghana Launches National Cybersecurity Policy and ... - CSA || News, accessed October 11, 2025, <https://www.csa.gov.gh/ghana-launches-national-cybersecurity-policy-and-strategy.php>

Ghana's Cybersecurity Act 2020 (Act 1038) - Digital Watch Observatory, accessed October 11, 2025, <https://dig.watch/resource/ghanas-cybersecurity-act-2020-act-1038>

CSA - Ministry of Communication, Digital Technology and Innovations, accessed October 11, 2025, <https://moc.gov.gh/csa/>

Cybercrime in Ghana - Wikipedia, accessed October 11, 2025, https://en.wikipedia.org/wiki/Cybercrime_in_Ghana

African countries call on Ghana's Cyber Security Authority (CSA) for collaboration and support - CSA || News, accessed October 11, 2025, https://www.csa.gov.gh/csa_and_some_african_countries.php

Ghana : A Case Study in Strengthening Cyber Resilience (English) - World Bank Documents, accessed October 11, 2025, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099111623162584046>

ghana - World Bank Documents, accessed October 11, 2025, <https://documents1.worldbank.org/curated/en/099111623162584046/pdf/P17785201f69be0150909902c3a7202107e.pdf>

The Inspiring Ghana Cybersecurity Results Story - A Case Study in Strengthening Cyber Resilience - CSA || News, accessed October 11, 2025, <https://www.csa.gov.gh/the-inspiring-ghana-cybersecurity-results-story.php>

Enhancing Cyber Resilience in Developing Countries - World Bank, accessed October 11, 2025, <https://www.worldbank.org/en/results/2025/01/29/enhancing-cyber-resilience-in-developing-countries>

Ghana National Cyber Security Policy & Strategy, accessed October 11, 2025, <https://afyonluoglu.org/PublicWebFiles/strategies/Africa/Ghana%202014%20National%20Cyber%20Security%20Policy%20and%20Strategy-EN.pdf>

Ghana National Cyber Security Policy & Strategy - ITU, accessed October 11, 2025, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf

Ghana's Cybersecurity Act - Facia.ai, accessed October 11, 2025,
<https://facia.ai/knowledgebase/ghanas-cybersecurity-act/>

Cybersecurity Act, 2020 1 Act 1038 ARRANGEMENT OF SECTIONS ..., accessed October 11, 2025,
<https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf>

cybersecurity act, 2020 - Atuguba & Associates, accessed October 11, 2025,
<https://atugubaassociates.com/file/Cybersecurity%20Act,2020%20Act,1038.pdf>

Ghana Faces Rising Cyber Threats Despite Digital Progress, accessed October 11, 2025,
<https://www.newsghana.com.gh/ghana-faces-rising-cyber-threats-despite-digital-progress/>

Cybercrime: Ghana's Growing Digital Weak Spot - Imani Africa, accessed October 11, 2025,
<https://imaniafrica.org/2025/09/cybercrime-ghanas-growing-digital-weak-spot/>

Ghana To Advanced Collaboration With Global Partners To Fight Cybercrime – Mahama, accessed October 11, 2025,
<https://businessdayghana.com/ghana-to-advanced-collaboration-with-global-partners-to-fight-cybercrime-mahama/>

Ghana loses GH¢23.3m to Cybercrime in 2024, GH¢ 14.9m in just six months, accessed October 11, 2025, <https://www.gbcghanaonline.com/general-news/ghana-loses-gh%C2%A223-3m-to-cybercrime-in-2024-gh%C2%A2-14-9m-in-just-six-months/2025/>

Minister Launches 2025 National Cyber Security Awareness Month and Calls for Safer, More Accountable Digital Space, accessed October 11, 2025, <https://moc.gov.gh/2025/09/03/minister-launches-2025-national-cyber-security-awareness-month-and-calls-for-safer-more-accountable-digital-space/>

CSA || About Us - Cyber Security Authority, accessed October 11, 2025, <https://www.csa.gov.gh/about-us.php>

Ghana Claims Top Spot in African Cybersecurity Rankings, Minister Announces, accessed October 11, 2025,
<https://techafricanews.com/2025/07/02/ghana-claims-top-spot-in-african-cybersecurity-rankings-minister-announces/>

Fighting Cybercrime, a shared responsibility – CSA Director-General - CSA || News, accessed October 11, 2025,
<https://www.csa.gov.gh/fighting-cybercrime-a-shared-responsibility-csa-director-general>

CSA || Licensing and Accreditation - Cyber Security Authority, accessed October 11, 2025,
https://www.csa.gov.gh/licensing_and_accreditation

Ghana Cybersecurity Services Licensing - International Trade Administration, accessed October 11, 2025,
<https://www.trade.gov/market-intelligence/ghana-cybersecurity-services-licensing>

Ghana's National Cybersecurity Policy and Strategy (NCPS) | Digital Watch Observatory, accessed October 11, 2025,
<https://dig.watch/resource/ghanas-national-cybersecurity-policy-and-strategy-ncps>

Final Version - Towards Ghana's National Policy On Cyber Security | PDF - Scribd, accessed October 11, 2025,
<https://www.scribd.com/document/874650534/Final-Version-Towards-Ghana-s-National-Policy-on-Cyber-Security>

Cyber Law and Security - Lessons for Law Enforcement.pptx - Center for Strategic and Defence Studies, accessed October 11, 2025, <https://csdsafrica.org/wp-content/uploads/2021/09/Cyber-Law-and-Security-Lessons-for-Law-Enforcement.pptx-compressed.pdf>

Ghana Loses GH¢23.3m to Cybercrime in 2024, GH¢14.9m in 2025 First Half – Sam George, accessed October 11, 2025, <https://managingghana.com/2025/09/15/ghana-loses-ghc23-3m-to-cybercrime-in-2024-ghc14-9m-in-2025-first-half-sam-george/>

Ghana Loses GH¢38 Million to Cybercrime, accessed October 11, 2025,
<https://www.newsghana.com.gh/ghana-loses-gh%E2%82%B538-million-to-cybercrime/>

Expert Warns Outdated Software Leaves Ghana Vulnerable to Hackers, accessed October 11, 2025,
<https://www.newsghana.com.gh/expert-warns-outdated-software-leaves-ghana-vulnerable-to-hackers/>

Ghana Launches Cybersecurity Awareness Month 2025 to Tackle Online Threats, accessed October 11, 2025, <https://techafricanews.com/2025/09/04/ghana-launches-cybersecurity-awareness-month-2025-to-tackle-online-threats/>

Collaborative Efforts Needed to Fight Cybercrime - Cyber Security Authority - CSA || News, accessed October 11, 2025, <https://www.csa.gov.gh/collaborative-efforts-needed-to-fight-cybercrime-cyber-security-authority>

Ghana Faces Highest Volume of Cyberattacks in West Africa, NETSCOUT Reports, accessed October 11, 2025, <https://techafricanews.com/2024/11/06/ghana-faces-highest-volume-of-cyberattacks-in-west-africa-netscout-reports/>

Nigeria, Ghana, Guinea most targeted for cyber attacks - SAMENA Daily News, accessed October 11, 2025, https://www.samenacouncil.org/samena_daily_news?news=103021

5 Critical Cyber Security Threats Facing Ghanaian Businesses in 2025 - Acity Journal, accessed October 11, 2025, https://blog.acity.edu.gh/acity_blog/5-critical-cyber-security-threats-facing-ghanaian-businesses-in-2025/

Mobile money robberies: Inside Ghana's rising cybercrime wave ..., accessed October 11, 2025, <https://thefourthestategh.com/2025/10/mobile-money-robberies-inside-ghanas-rising-cybercrime-wave/>

Cybersecurity: A pillar for safeguarding ghana's critical infrastructure, accessed October 11, 2025, <https://thebftonline.com/2025/09/01/cybersecurity-a-pillar-for-safeguarding-ghanas-critical-infrastructure/>

Cybersecurity for Financial Inclusion: Lessons from Ghana, accessed October 11, 2025, <https://www.afi-global.org/opinion/cybersecurity-for-inclusive-finance-lessons-from-ghana/>

CYBER & INFORMATION SECURITY DIRECTIVE - Bank of Ghana, accessed October 11, 2025, <https://www.bog.gov.gh/wp-content/uploads/2019/09/CYBER-AND-INFORMATION-SECURITY-DIRECTIVE.pdf>

Ghana - Information and Communications Technology (ICT), accessed October 11, 2025, <https://www.trade.gov/country-commercial-guides/ghana-information-and-communications-technology-ict>

MTN Ghana Leads Conversation On Cybersecurity And Digital Transformation For SMEs, accessed October 11, 2025, <https://www.businessghana.com/site/news/business/295220/MTN-Ghana-Leads-Conversation-On-Cybersecurity-And-Digital-Transformation-For-SMEs>

MTN Moves To safeguard Ghana's SMEs sector against Cyber-attacks, accessed October 11, 2025, <https://www.telecomschamber.org/industry-news/mtn-moves-to-safeguard-ghana-s-smes-sector-against-cyber-attacks/>

Driving Cybersecurity Awareness Initiatives in Ghana | - MTN Group, accessed October 11, 2025, <https://www.mtn.com/case-study/driving-cybersecurity-awareness-initiatives-in-ghana/>

MTN Ghana holds cybersecurity awareness at Labone Senior High ..., accessed October 11, 2025, <https://www.modernghana.com/news/1188270/mtn-ghana-holds-cybersecurity-awareness-at-labone.html>

MTN Ghana Data Breach Impacts 5700 Customers, Investigation Underway, accessed October 11, 2025, <https://dailysecurityreview.com/security-spotlight/mtn-ghana-data-breach-impacts-5700-customers-investigation-underway/>

MTN Ghana Data Breach: 5,700 customers potentially affected, accessed October 11, 2025, <https://www.ghanaweb.com/GhanaHomePage/business/MTN-Ghana-Data-Breach-5-700-customers-potentially-affected-1981776>

MTN Hit by CyberAttack, Urges Vigilance Among Users - Ecofin Agency, accessed October 11, 2025, <https://www.ecofinagency.com/telecom/2504-46688-mtn-hit-by-cyberattack-urges-vigilance-among-users>

Cyber Security Factsheet 2025 - Vodafone IR, accessed October 11, 2025, <https://investors.vodafone.com/~media/Files/V/Vodafone-IR/documents/our-purpose/vodafone-cybersecurity-factsheet-2025.pdf>

Cyber security - Vodafone.com, accessed October 11, 2025, <https://www.vodafone.com/about-vodafone/how-we-operate/consumer-privacy-and-cyber-security/cyber-security>

2024 Cyber Security Factsheet - Vodafone.com, accessed October 11, 2025, <https://reports.investors.vodafone.com/view/578448872>

Telecel Ghana Hosts 100 Girls for 2025 National Girls in ICT Open ..., accessed October 11, 2025, <https://telecel.com.gh/explore-telecel/foundation/articles/telecel-ghana-hosts-100-girls-for-2025-national-girls-in-ict-open-day>

Cyber Risk Posture Of Ghanaian Telecommunication Companies: A Case Study Of Vodafone Ghana - UGSpace, accessed October 11, 2025, <https://ugspace.ug.edu.gh/items/aa73ae9a-af3f-428d-a619-331a6d633ca5>

Exploring Cybersecurity Awareness among Literate Mobile Money Users in Ghana - Simple search, accessed October 11, 2025, <https://his.diva-portal.org/smash/get/diva2:1999285/FULLTEXT01.pdf>

Ghana's health sector low in cybersecurity maturity – CSA cautions - CSA || News, accessed October 11, 2025, <https://www.csa.gov.gh/ghana-s-health-sector-low-in-cybersecurity-maturity-csa-cautions.php>

Ghana Moves to Strengthen Digital Security with New Fund and Joint Cyber Committee, accessed October 11, 2025, <https://techafricanews.com/2025/10/02/ghana-moves-to-strengthen-digital-security-with-new-fund-and-joint-cyber-committee/>

INSTITUTE OF ICT PROFESSIONALS GHANA - IIPGH - Ghana's Cybersecurity Journey: Confronting the Challenges of a Multi-Layered Defense, accessed October 11, 2025, <https://iipgh.org/ghanas-cybersecurity-journey-confronting-the-challenges-of-a-multi-layered-defense/>

Understanding cyber safety behavior among teenagers in Ghana - ResearchGate, accessed October 11, 2025, https://www.researchgate.net/publication/353352954_Understanding_cyber_safety_behavior_among_teenagers_in_Ghana

A New Study Explores Digital Skills in Sub-Saharan Africa - International Finance Corporation, accessed October 11, 2025, <https://www.ifc.org/content/dam/ifc/doc/mgrt/digital-skills-report-flyer-5-22-19-web.pdf>

Digital Skills in Sub-Saharan Africa Spotlight on Ghana, accessed October 11, 2025, <https://www.ifc.org/content/dam/ifc/doc/mgrt/digital-skills-final-web-5-7-19.pdf>

Experiences and perceptions of cybercrime victims in Ghana: The ..., accessed October 11, 2025, <https://www.tandfonline.com/doi/full/10.1080/2331186X.2023.2285623>

Culture and Cybersecurity 's Role in the Continual Usage of E-Commerce Platforms in Sub-Saharan Africa: Perspectives from Ghana | Advances in Consumer Research, accessed October 11, 2025, <https://acr-journal.com/article/culture-and-cybersecurity-s-role-in-the-continual-usage-of-e-commerce-platforms-in-sub-saharan-africa-perspectives-from-ghana-873/>

Understanding the Impact of Cybercrime on E-commerce practices in Ghana | Request PDF, accessed October 11, 2025, https://www.researchgate.net/publication/342014708_Understanding_the_Impact_of_Cybercrime_on_E-commerce_practices_in_Ghana

CYBER-CRIME AND ITS EFFECTS ON E-COMMERCE TECHNOLOGIES - Conscientia Beam, accessed October 11, 2025, <https://archive.conscientiabeam.com/index.php/104/article/download/2520/3885>

Ghanaian justice and security officials better equipped to protect victims of cybercrime, accessed October 11, 2025, <https://thecommonwealth.org/news/ghanaian-justice-and-security-officials-better-equipped-protect-victims>

Ghana Plans Cybercrime Court as Arrests Top 100, accessed October 11, 2025, <https://www.newsghana.com.gh/ghana-plans-cybercrime-court-as-arrests-top-100/>

C-IN-C LAUNCHES CYBER SECURITY AWARENESS MONTH - Ghana Armed Forces, accessed October 11, 2025, <https://gafonline.mil.gh/news/c-in-c-launches-cyber-security-awareness-month>

Ghana's AI Ambitions: Strategy and Emerging Tech Bill Take Shape ..., accessed October 11, 2025, <https://360mozambique.com/world/africa/ghanas-ai-ambitions-strategy-and-emerging-tech-bill-take-shape/>

Ghana Outlines National AI Roadmap, Emerging Technologies Bill in Development, accessed October 11, 2025, <https://techafricanews.com/2025/09/29/ghana-outlines-national-ai-roadmap-emerging-technologies-bill-in-development/>

Ghana to Develop National AI Strategy Initiative Amid Digital Transformation Push, accessed October 11, 2025, <https://moc.gov.gh/2025/05/02/ghana-to-develop-national-ai-strategy-initiative-amid-digital-transformation-push/>

Ghana Unveils National AI Strategy, Preps Emerging Tech Bill at ENJOY AI 2025, accessed October 11, 2025, <https://www.techinafrica.com/ghana-unveils-national-ai-strategy-preps-emerging-tech-bill-at-enjoy-ai-2025/>

Ghana Unveils National AI Strategy, Plans Emerging Tech Bill - iAfrica.com, accessed October 11, 2025, <https://iafrica.com/ghana-unveils-national-ai-strategy-plans-emerging-tech-bill/>

Top 10 Cybersecurity Training Companies in Ghana - Edoxi, accessed October 11, 2025, <https://www.edoxi.com/studyhub-detail/top-cybersecurity-training-companies-ghana>

Diploma in Cyber Security | Japhson Institute of Technology, accessed October 11, 2025, <https://japhsoninstitute.edu.gh/cyber-security.html>

Certificate Programme in Cyber Security - KAIPTC, accessed October 11, 2025, <https://www.kaiptc.org/academic-programmes/short-courses/certificate-programme-in-cyber-security/>

Year of Report	GCI Score (%)	Africa Rank	Global Rank	Key Milestones/Contributing Factors
2017	32.6%	11th	-	Initial stages of formal cybersecurity development; National Cyber Security Secretariat (NCSS) established.
2018	43.7%	-	-	Transition to National Cyber Security Centre (NCSC); launch of National Cyber Security Awareness Month (NCSAM).
2020	86.69%	3rd	43rd	Passage of the comprehensive Cybersecurity Act, 2020 (Act 1038); revision of the National Cybersecurity Policy and Strategy; development of the national CERT ecosystem.
2024	99.27%	2nd	-	Achieved 'Tier 1: Role Modelling' status; full operationalization of the Cyber Security Authority (CSA); enhanced protection of Critical Information Infrastructure (CII); strengthened international cooperation, including ratification of the Second Additional Protocol to the Budapest Convention.

Provision Area	Key Mandates/Regulations	Responsible Body/Entities	Penalties/Enforcement
Cyber Security Authority (CSA)	Establishes the CSA as the primary regulatory body for all cybersecurity activities in Ghana.	Cyber Security Authority (CSA)	The CSA is empowered to issue directives, set standards, and impose administrative penalties.
Critical Information Infrastructure (CII)	Mandates the designation, registration, and protection of CII. Owners must report incidents and undergo periodic security audits.	CSA, Owners of CII (e.g., banks, telcos, energy companies)	Unauthorized access to CII is punishable by heavy fines and imprisonment.
Licensing & Accreditation	Requires all cybersecurity service providers (CSPs), establishments (CEs), and professionals (CPs) to be licensed or accredited by the CSA.	CSA, Cybersecurity Professionals and Businesses	Operating without a license can lead to fines, revocation of business permits, and criminal charges.
Incident Reporting	Mandates the reporting of cybersecurity incidents to the relevant CERT within 24 hours of detection.	All organizations and CII owners	Failure to report incidents can result in administrative penalties.
Child Online Protection	Criminalizes the creation, possession, and distribution of indecent images of children, as well as cyberstalking and online grooming of minors.	Law Enforcement, CSA	Penalties range from 5 to 25 years of imprisonment.
Investigatory Powers	Grants law enforcement agencies the power to obtain production orders for subscriber information and interception warrants for traffic and content data.	Law Enforcement Agencies	Service providers must comply with lawful orders.

Provision Area	Key Mandates/Regulations	Responsible Body/Entities	Penalties/Enforcement
International Cooperation	Mandates the CSA to collaborate with international bodies and establishes a 24/7 point of contact to facilitate global cooperation in tackling cybercrime.	Cyber Security Authority (CSA)	The Act supports global enforcement and allows for the blocking of illegal content.

Year/Period	Number of Reported Incidents	Direct Financial Losses (GH¢)	Key Threat Categories (% of incidents in H1 2025)
2019-2023 (Aggregate)	3,804	-	-
2024 (Full Year)	-	23.3 million	-
H1 2024	1,317	-	-
H1 2025	2,008	14.9 million	Online Fraud (36%), Cyberbullying (25%), Online Blackmail (14%), Unauthorized Access (12%), Information Disclosure (9%)