B&FT
Business & Financial Times
SPECIAL PUBLICATION

Cyber Security & IT Survey 2025

TOOLS, FIRMS AND FOUNDERS SHAPING DIGITAL SECURITY IN GHANA

6th October 2025

DATA PROTECTION COMMISSION
VIRTUAL INFOSEC AFRICA
CYBERTEQ
margins ID GROUP
innovaré
apoticaA
CITSYS
McDon Consolidated
iSA
IPMC

B&FT Business & Financial Times
SPECIAL PUBLICATION
MONDAY OCTOBER 6, 2025

Cybersecurity in the mirror

Cybersecurity & IT Survey 2025

After years of growing digital activity, Ghana's cybersecurity now stands before a mirror of accountability. What does it see in its reflection?

The picture reveals two contrasting faces. On one side, there has been clear progress. A decade ago, Ghana had virtually no formal cybersecurity frameworks.

Today, the country boasts a Cyber Security Authority, banks operate Security Operations Centres, and data protection laws are in force. Data centres are emerging across the country, while organisations increasingly embrace cloud solutions. Local innovators are building tools that can stand toe-to-toe with international products.

Yet, the mirror also reflects a harsher reality. Reported cyber incidents rose from 1,317 in 2024 to 2,008 in just the first six months of 2025. In 2024 alone, Ghana lost GH¢23.3 million to cybercrime. By mid-2025, attackers had already siphoned off a further GH¢14.9 million. Data breaches surged by nearly 1,000 percent in early 2024, compromising 1.2 million records.

The skills gap compounds the problem. Ghana requires over 5,000 qualified cybersecurity professionals across different roles, yet critical positions remain unfilled. Small businesses, wrongly assuming that cybercriminals only target large corporations, leave themselves exposed. Many executives still view cybersecurity as an expense rather than an investment in survival.

Two faces of Ghana

By day, Ghana presents itself as a digital success story. Mobile money transactions reached GH¢1.07 trillion. Farmers in Tamale receive instant payments, traders access credit via smartphones, government services are delivered online, and e-commerce reshapes consumer habits nationwide.

But in the shadows, dangers persist. Phishing emails grow more sophisticated, ransomware spreads across borders within seconds, and fraudsters exploit mobile money platforms through social engineering. A major breach of a popular cloud provider last year left several Ghanaian businesses simultaneously exposed. Supply chain attacks threaten to cripple entire industries overnight.

The mobile money ecosystem, processing billions of cedis each month, has become a magnet for cybercriminals. Exploits target both technical vulnerabilities and human behaviour.

Trust hangs by a thread

One successful cyberattack can undo years of progress. The nation's digital transformation depends heavily on public confidence. Citizens must trust that their mobile money is secure, that their personal data will not be compromised, and that online services will not expose them to harm.

Critical questions remain: Are organisations truly compliant with international security standards, or are some certifications merely for show? Are systems independently tested, or left for cybercriminals to probe? Are universities equipping the next generation with cutting-edge cyber skills, or producing graduates from outdated curricula? And do we trust local innovators, or default too easily to foreign vendors despite Ghana's proven record in home-grown fintech?

The people problem

The human element remains Ghana's greatest vulnerability. Universities produce graduates, but too few with specialised skills needed to counter evolving cyber threats. Curricula lag behind the pace of change.

Meanwhile, seasoned professionals are overstretched—serving on multiple boards, consulting for government, and running their own firms simultaneously. This concentration of expertise creates systemic risk: when a few individuals are stretched too thin, the entire ecosystem suffers.

Where we stand

Ghana has achieved a Tier 1 Cybersecurity Nation ranking, but that should not inspire complacency. Systems can be strengthened, people can be trained, and trust can be rebuilt—but only through deliberate effort.

This October, during Cybersecurity Awareness Month, the Business & Financial Times will publish the Cybersecurity & IT Survey 2025. This report will serve as the country's mirror—highlighting companies building resilience, innovators pushing boundaries, regulators enforcing standards, and persistent gaps demanding attention.

The survey will spotlight tools and technologies alongside human stories—successes, mistakes, and lessons that Ghana must absorb before the next wave of attacks. It will showcase home-grown solutions, track emerging threats, and provide a roadmap for fortifying national cyber defences.

For businesses, it offers an opportunity to demonstrate commitment to cybersecurity excellence, to share lessons learned, and to embed best practices. For the nation, it is a call to confront vulnerabilities before they grow into crises.

Looking ahead

The mirror provides clarity—a chance to strengthen cyber posture, rebuild trust, and address uncomfortable truths before they turn into national embarrassments. Each day of inaction carries a price. Every unpatched system, every under-trained employee, and every delayed investment in infrastructure becomes another opportunity for cybercriminals.

The question now is whether Ghana will step forward with resolve or continue staring passively at its reflection. Eventually, the mirror will stop reflecting—it will record. And in that record, history will remember who took action, who looked away, and who helped build the digital trust upon which Ghana's economy and future now depend.

Outdated education fuels cyber skills gap

- expert warns

By Kingsley Webora TANKEH

The Manager of West Africa's first academic Forensic and Cyber Security Laboratory at Wisconsin International University College, Maxwell Amuzu, has said the persistent 'knowledge gap' created by outdated education is crippling Ghana's defence against cybercrime.

He emphasised that the knowledge gap is not due to a lack of graduates, but because their education is often abstract and disconnected from realities of the digital landscape.

Speaking exclusively to Business and Financial Times (B&FT), the digital forensics expert argued that the core issue is education failure.

He indicated that many new professionals enter the field with textbook knowledge but lack the investigative mindset and practical skills to counter real-world threats.

"The reason most people finish up with cybersecurity and they don't know what to do or they cannot even prevent some threats is a matter of depth. Technology is constantly changing," he added.

He noted that to build a resilient digital future for Ghana, cybersecurity education must evolve from teaching theory to churning our practitioners capable of outthinking ever-evolving adversaries.

He lamented the lack of investment in cybersecurity infrastructure and learning materials.

"Most of our educational institutions don't have the equipment or resources, so they teach in abstracts. But in our lab, we give practical examples and a real feel of the environment and tools before they even go out."

Mr. Amuzu maintained that cybersecurity is not just about penetration or hacking but has a vast spectrum of roles including prevention, threat-hunting and digital forensics.

"The wrong education is just introducing people to the classroom, telling them pen-testing is done this way and then throwing them into the environment to learn on their own.

The kind of education I'm talking about becomes a use-case, an illustration immersing people into that kind of thinking," he stressed.

His lab is designed as a solution to this problem. He satisfied that students are immersed in a simulated cyber ecosystem to build the skills required for detecting, diagnosing and averting cyber attacks.

They use Virtual Reality to practice being expert witnesses in court, learning how to make digital evidence admissible.

They also work in isolated virtual machines to dissect live malware and hunt for vulnerabilities in real-time. "You have to become that person.

You have to take that form," he noted, emphasising that cybersecurity is a lifestyle of constant curiosity. "It's more or less like a skill set that becomes your personal everyday life," he added.

Mr. Amuzu acknowledged the Cyber Security Authority's efforts to register professionals and streamline the sector. However, he stressed that closing the knowledge gap requires a fundamental overhaul of training methodology across the board.

Cyber capacity building and digital financial inclusion ...a critical analysis of prevailing approaches

By Desmond ISRAEL Esq.

In the rush to bank the unbanked, Africa has become a global laboratory for financial inclusion. Mobile money, digital wallets, and fintech platforms are transforming the lives of millions who were once outside the formal financial system. But this digital leap comes with a shadow — rising cyber threats. Every digital payment, every mobile transaction, every new fintech app expands not just access, but attack surfaces.

As digital financial services proliferate, the security infrastructure meant to protect them often lags. Nowhere is this mismatch more visible than in developing countries like Ghana, where the same innovations that promise financial empowerment also open the door to exploitation. Bridging this gap requires more than regulation. It demands a rethinking of how we build cyber capacity — who it's for, how it's done, and what "capacity" truly means in a rapidly shifting digital economy.

The Double-Edged Sword of Digital Inclusion

Digital financial inclusion is, by most measures, a success story. In Ghana, mobile money penetration stands at over 40%. Across Africa, more than 500 million mobile money accounts have been opened. The continent leads the world in transaction volumes and innovation models, from pay-as-you-go solar to community savings platforms built on basic phones.

But the very traits that make digital financial services accessible — simplicity, speed, scale — also make them vulnerable. Social engineering scams, SIM swap fraud, identity theft, and phishing attacks have all surged in step with adoption. Fintech startups, often lean and under-resourced, struggle to meet basic cybersecurity hygiene standards. Users, many of whom are new to digital systems, are rarely equipped to recognize threats or defend themselves.

In this context, cyber capacity building cannot be treated as a backend concern for IT departments. It is a frontline issue, critical to trust, usability, and resilience in the digital finance ecosystem.

The Flawed Status Quo: Overbuilt for Governments, Underdesigned for Users

Most current models of cyber capacity building follow a familiar pattern. International partners, often from the Global North, fund national-level programs focused on building incident response teams (CSIRTs), drafting cybersecurity strategies, or conducting high-level policy workshops. These are important, but they largely orbit government ministries and a handful of elite agencies.

Meanwhile, the private sector — especially fintechs and mobile network operators — is left to fend for itself. User education is an afterthought. And local cybersecurity ecosystems, including startups, academia, and civil society, are often excluded from both design and delivery.

The result is a system that looks strong on paper but is brittle in practice. In Ghana, for example, while the Cyber Security Authority has taken commendable steps toward building institutional frameworks and issuing directives, enforcement is uneven, and alignment between regulation and innovation is patchy. Many fintechs, particularly in the early stage, operate below the cybersecurity radar — too small to be noticed, too fast-moving to be regulated in time.

A cyber breach in this environment is not just a technical failure. It erodes trust in digital systems, deters adoption, and sets back financial inclusion gains by years. And the damage is disproportionately borne by those least able to absorb it: low-income users, rural entrepreneurs, and women-led microbusinesses.

Lessons from Global Practice: Scale, Scope, and Sustainability

Some countries have managed to square the circle. Singapore's Cyber Security Agency, for instance, runs a multi-layered approach that pairs national strategy with deep engagement across industry and citizens.

Brazil's central bank mandates strict cybersecurity protocols for financial institutions but also provides toolkits and training for smaller players. Rwanda has adopted a community-based approach, working with local tech hubs to deliver grassroots digital hygiene programs.

Three lessons stand out. First, cyber capacity building must be multi-tiered — national strategy alone is not enough. It must extend down to the operational level of service providers, and further still to the end users. Second, it must be inclusive.

Fintech founders, product designers, user researchers, digital rights advocates — all have roles to play in shaping secure ecosystems. Third, it must be continuous. Threats evolve, platforms change, behaviors shift. One-off training or donor-funded workshops won't cut it.

Africa's Strategic Crossroads: Build or Buy Security?

For many African governments, the dilemma is whether to build local cyber capacity or rely on external tools and frameworks. It's tempting to outsource security to big tech providers or foreign consultants — they offer polished platforms, quick deployments, and seemingly bulletproof compliance checklists.

But long-term, this approach is risky. It breeds dependency, limits contextual adaptation, and stifles local industry growth. Instead, countries like Ghana should prioritize strategic investment in domestic capacity: training cybersecurity professionals, funding local innovation, and creating platforms for public-private collaboration.

A Ghanaian fintech shouldn't have to choose between growth and security. It should have access to affordable, context-aware cybersecurity tools and advisory services.

Regulators,, must resist the urge to copy andpaste frameworks from the EU or the U.S. without considering fit. What works in Brussels won't necessarily work in Kumasi or Tamale. Policies must reflect local usage patterns, infrastructure gaps, and linguistic realities.

Continued on page 26

The Real IPMC

Two Decades of Technological Innovation

When the name IPMC comes to mind for many Ghanaians, they associate it with classrooms, certification courses, and tech training.

For almost twenty years, the institution has established a strong reputation as the hub where aspiring professionals acquire coding skills, become proficient in software applications, and obtain qualifications that enhance their job prospects. However, this viewpoint, although correct, reveals only part of the narrative.

Beneath the training centers and examination rooms exists a distinct identity: that of a quiet force building the digital foundation for Ghana's leading businesses.

"Individuals notice the training arm due to its visibility," remarks Mr. Amardeep, the quiet CEO whose vision has directed IPMC since its beginning. "Our genuine influence unfolds in boardrooms and server rooms nationwide." We are the ones that sustain businesses, assist them in growing, and provide the resources needed to compete globally.

It's a daring assertion, yet the proof is clear. Enter the headquarters of any prominent manufacturing company, retail chain, or financial institution in Ghana, and you're likely to discover IPMC's influence on the systems that keep things running smoothly.

IPMC Ebizframe ERP Software

IPMC's main product, Ebizframe ERP, serves as the unseen force behind many of the nation's well-known brands, overseeing tasks from inventory handling in warehouses to compliance submissions with the Ghana Revenue Authority.

What distinguishes Ebizframe in a saturated enterprise software market is not only its thoroughness but also its flexibility to address the specific challenges of functioning in Ghana. The system effortlessly manages multi-currency transactions, copes with the intricacies of local tax regulations, and produces the required reports that satisfy auditors and appease regulators. For businesses growing in West Africa, the platform's capacity to unify data from various jurisdictions while upholding compliance regulations in each has been extremely beneficial.

However, Mr. Amardeep, is quick to emphasize that compliance and accounting, although essential, only serve as the groundwork. "Any good ERP system can monitor transactions," he states. "The true worth lies in how you utilize that knowledge." This philosophy powers the sophisticated functionalities integrated into ebizframe, attributes that convert raw data into competitive edge.

The flexi reports feature enables companies to analyze data in numerous formats, generating tailored dashboards that address the unique inquiries of each executive. A CFO can track cash flow trends throughout subsidiaries instantly.

A procurement director can determine which suppliers reliably meet deadlines and which ones fail to do so. A sales manager can identify new market trends weeks ahead of rivals.

These insights gain even greater significance when combined with the system's workflow automation features. Purchase requisitions that previously stalled for days waiting for various signatures now advance through approval processes automatically, activated by set rules and limits. The decrease in processing time is not quantified in hours but in percentages, with certain clients indicating a cycle time enhancement of sixty percent or greater. Contract approvals, budget approvals, expense refunds all the bureaucratic hurdles that hinder organizational progress are eliminated.

By digitizing data collection at all touchpoints, from warehouse receiving areas to customer service desks, Ebizframe removes the transcription mistakes and information gaps that hinder manual processes.

The unified communication channels ensure that when exceptions arise, the appropriate individuals are promptly alerted via the channels they regularly utilize, be it email, SMS, or in-app messaging.

For Mr. Amardeep, these represent not merely technical attributes but catalysts for a core transformation in the operations of Ghanaian businesses. "We assist companies in transitioning from addressing past issues to predicting future possibilities," he clarifies.

The investment returns are evident in both measurable and nuanced ways: lower carrying costs due to optimized inventory levels, enhanced cash collection through improved receivables management, stronger negotiating power from data-supported supplier assessments, and the assurance that arises from decisions grounded in facts instead of intuition.

IMPC Raptech AI

Even though Ebizframe has grown into a market leader, IPMC has not become complacent with its achievements. The launch of Raptech AI indicates the company's acknowledgment that the forthcoming competitive landscape is within machine intelligence.

While conventional systems inform companies about past events and their reasons, Raptech AI explores what will occur in the future and the actions that should be taken. The system gathers operational data, sales trends, supply chain activities, customer actions, market indicators, and reveals insights that human analysts could take weeks to find, if they notice them at all.

A distributor utilizing Raptech AI could find that the demand for particular products consistently peaks three days following payday dates in specific areas, allowing for proactive inventory placement. A producer could detect subtle relationships between production line factors and defect rates, averting quality problems before they arise.

A retailer may discover that specific product pairings lead to higher basket values, guiding promotional tactics and store designs. These are not theoretical situations but the types of predictive insights that are currently assisting IPMC's clients in staying ahead of market changes.

Artificial intelligence may seem theoretical until you witness it identifying a supply chain issue a month ahead of when it would have led to stock shortages," Mr. Amardeep notes. "That's the moment when business leaders realize this is not science fiction." "It's survival of the fittest."

IPMC Data Centers

At the foundation of all these software solutions lies IPMC's most essential but least noticeable service: the Data centre services. In a time when the availability of information is crucial for business continuity, the organization runs facilities built around three essential principles: security, reliability, and scalability.

These are not converted warehouse areas with air conditioning units attached. They are specially designed facilities featuring backup power systems, biometric security measures, fire suppression systems, and network structures that guarantee that if one link fails, the traffic automatically diversifies through other options.

For companies weary of overseeing their server rooms, contending with generator malfunctions, cooling system failures, and the ongoing struggle to scale infrastructure with growth, IPMC's data center services provide freedom.

Colocation setups enable businesses to retain oversight of their equipment while delegating the environmental intricacies.

Cloud hosting solutions offer enhanced flexibility, enabling businesses to adjust computing resources upwards or downwards according to real-time requirements instead of worst-case scenarios. Disaster recovery solutions guarantee that if a catastrophe impacts a company's main site, essential systems can be rapidly restored from secure backups stored in geographically distinct locations.

Looking forward, Mr. Amardeep anticipates IPMC's role growing even more as Ghana's digital transformation speeds up. New features are being developed. Collaborations with international tech leaders are being established. The footprint of data centres is expanding. All of this is directed at making sure that Ghanaian companies get top-notch technology solutions locally.

Mr. Amardeep reflects, "Two decades ago, we began teaching individuals on computer usage." "Today, we're establishing the technological base that supports Ghana's economy."

Tomorrow, we will assist companies in utilizing technologies that are yet to be created. The goal remains the same, supporting Ghanaian businesses, but the range continues to grow.

The real IPMC, it turns out, has been hiding in plain sight all along, not behind classroom doors, but inside the systems quietly powering the nation's economic transformation.

Cybersecurity risk exposure for Ghanaian Businesses

The way forward

By Ben TAGOE

In less than two decades ago, Ghana's digital transformation has accelerated at an extraordinary pace. From mobile money innovations reshaping financial inclusion, to cloud platforms powering small businesses, technology has become the backbone of our economy. Yet, alongside this progress has come a sobering reality: the cyber threats confronting Ghana are growing in scale, sophistication, and impact.

Hence, cybersecurity in Ghana is no longer a technical afterthought. It is now a boardroom issue, a national development issue, and a matter of public trust. To fully understand where Ghana stands, we must trace how far we have come, confront the challenges still ahead, and explore what businesses whether large and small must do to secure their futures.

The early years of Ghana's digital expansion were marked by fragmentation. Organizations were left to fend for themselves, adopting ad hoc measures often only after a breach had occurred. Banks, telcos, and government institutions developed their own silos of protection, but there was no unified national framework to anchor cybersecurity efforts.

The first real turning point came in 2018, when the Bank of Ghana issued its Cyber and Information Security Directive. This was the first time a regulator formally imposed mandatory standards for cybersecurity within a critical sector.

The directive required financial institutions to establish governance structures, appoint CISOs, adopt policies aligned with international standards, and implement monitoring and incident reporting frameworks. It forced banks and financial institutions to take cybersecurity beyond mere IT best practices, embedding it in governance and compliance. This directive laid the groundwork for sectoral regulation and signaled that cybersecurity had matured into a matter of systemic risk that demanded regulatory oversight.

Momentum built further with the establishment of the Cyber Security Authority (CSA). For the first time, Ghana had a national body responsible for coordinating incident response, driving awareness campaigns, and guiding policy. The CSA enacted the Cybersecurity Act, 2020 (Act 1038) which provides a framework for regulating the industry, protecting critical information infrastructure (CII), and enforcing compliance across sectors. Together, the Bank of Ghana directive and Act 1038 marked Ghana's shift from reactive, fragmented responses, to a structured, regulated, and nationally coordinated cybersecurity regime.

Fast-forward to 2023 and 2024, and Ghana's cybersecurity ecosystem looks markedly different. Regulation, oversight, and awareness have advanced significantly, and the country is being recognized internationally as a leader in cyber capacity building.

The CSA's licensing and accreditation regime has been one of the most visible reforms. By the end of 2023, more than 1,200 service providers, establishments, and professionals had registered under the scheme. Unprecedented, Ghana has created a legitimate marketplace for cybersecurity services, where businesses and professionals are vetted and held accountable. This move not only legitimizes the industry, but also builds trust between providers and the organizations that rely on their expertise.

The financial sector remains at the center of the cyber threat landscape. The Bank of Ghana's 2024 Fraud Report paints a sobering picture: while the number of fraud cases in banks fell by 26%, from 969 in 2023 to 716 in 2024, the value at risk rose by 19%, climbing from GH¢63 million to GH¢75 million. Forgery and document manipulation alone accounted for GH¢53.5 million, compared to just GH¢7.5 million the year before.

This sevenfold increase illustrates how fraudsters are refining their tactics, focusing on fewer but higher-value exploits. Payment Service Providers (PSPs), which power Ghana's booming digital economy, recorded 15,673 fraud cases in 2024, up from 14,655 in 2023. As digital transactions increase in volume and value, so too does their attractiveness to fraudsters, underscoring the tension between innovation and risk.

Fraud remains the most visible threat. The fact that only GH¢3 million — about 4% of the GH¢83 million at risk in 2024 was recovered underscores a critical weakness in enforcement and legal processes. Lengthy court proceedings and the abandonment of cases mean that fraudsters often face minimal consequences. Without stronger deterrence, the incentive for cybercrime remains high.

Insider threats compound the problem. In 2024, 365 staff members from various financial institutions were implicated in fraud cases, up from 274 the previous year. Cash theft and suppression accounted for three-quarters of these cases. Alarmingly, only 155 staff were dismissed, meaning more than half of the implicated employees remained in the system. Weak disciplinary frameworks, insufficient vetting, and a culture of leniency create fertile ground for insider fraud.

Small and Medium-sized Enterprises (SMEs) represent another pressing concern. As the backbone of Ghana's economy, SMEs are critical to growth, but they are increasingly becoming the low-hanging fruit for cybercriminals. Many SMEs lack dedicated IT staff or security budgets, and their dependence on digital platforms makes them particularly vulnerable to phishing, ransomware, and business email compromise. A single breach can wipe out trust, disrupt operations, and even collapse a small enterprise.

Ben TAGOE

The writer is Chief Executive Officer of Cyberteq

The skills and resource gap adds to the challenge. Cybersecurity is resource-intensive, requiring investment in tools, people, and processes. But many organizations are constrained by budgets, and Ghana's pool of skilled professionals is limited. Brain drain is a constant risk as trained cybersecurity talent seeks opportunities abroad.

Finally, the human factor remains a persistent vulnerability. Phishing, SIM-swap scams, and social engineering attacks succeed because end users often lack awareness. While awareness campaigns like the National Cyber Security Awareness Month (NCSAM) have gained traction, building a culture of digital safety across millions of users takes time.

Every business, regardless of size or sector, is now a prime target for cyberattacks. The truth remains one, it is no longer a question of if an organization will be targeted, but when. The financial industry, attackers exploit forgery, impersonation, and payment channel manipulation. In healthcare, the threat often comes in the form of ransomware that locks critical patient data and disrupts lifesaving services.

The education sector is increasingly targeted by phishing scams and data breaches, as schools and universities store vast amounts of personal and research data. Energy and utility providers face risks of sabotage and disruption to critical infrastructure, while retail and e-commerce companies must contend with payment fraud and data theft from online platforms. Even government and public institutions are not exempted; phishing, malware, and denial-of-service attacks can bring essential services to a halt.

The reality is that the nature of the attack may differ by industry, but the underlying message is the same: no organization is safe. Every sector has vulnerabilities that cybercriminals are eager to exploit, and every business whether in finance, health, education, energy, retail, or government must recognize that it is a target.

For Ghanaian businesses, cybersecurity must be reframed not as a compliance obligation but as a business enabler. The survival of an organization increasingly depends on its ability to safeguard its data, systems, and reputation.

This means embedding cybersecurity into governance at the highest levels. Boards and executives must treat it as a strategic risk, not a technical issue. Technical, physical and administrative controls are non-negotiable. Staff must be continuously trained, not only to recognize phishing emails but also to understand their role as custodians of trust.

Third-party risk management

Continued on page 19

McDon Consolidated

Who we are

In a landscape where cyber threats grow more sophisticated by the day, McDon Consolidated stands out as a builder of resilient, intelligent systems that protect, empower, and scale. From Insurance firms to schools, law firms, and SMEs, McDon delivers secure, intuitive platforms that help organizations thrive in the digital age.

From Vision to Impact

McDon Consolidated was incorporated in 2020 with a bold mission: to build secure, scalable digital systems that empower business around the globe to thrive in a connected world. What began as a lean team of innovators in Accra has grown into a multi-award-winning tech firm with global reach and local relevance.

The company's early breakthroughs came in SMEs and insurance, where McDon's custom CRM & Workflow platforms helped clients digitize operations, improve client engagement, and meet compliance standards with confidence.

Over time, McDon expanded its portfolio to serve SMEs across diverse industries—from real estate and healthcare to fashion, transport, schools, professional services and agro-business.

Today, McDon Consolidated is recognized across Africa, Europe, and North America for its commitment to clarity, security, and transformation. With DigitCRM and DigitInsure CRM at the core, McDon continues to invent the digital future—one business at a time.

Flagship Platforms

DigitInsure CRM

A specialized tailored CRM for Insurance firms, DigitInsure CRM streamlines digital policy selling(firest premium) & renewal, policy management, client onboarding, backoffice workflow automation, complaints management, cliams & refunds managment, customer service, payment integration and compliance.

With embedded cybersecurity protocols and intuitive departmental & branches workflows, it helps Insurers build trust and operate with confidence. Your business in your palm. Your clients in your care.

DigitCRM

A flexible, industry-tailored CRM platform designed for SMEs across sectors. DigitCRM supports: Schools, Real estate firms, Homecare providers, Law firms, Professional service firms, Hospitals, Transport businesses, Agro-enterprises, Media houses, Fashion retailers, Wholesale distributors, E-commerce brands, Advertising agencies.

It enables secure client engagement, workflow automation, invoice & receipt, and mobile access—making it a powerful tool for growth and operational clarity. Your business in your palm. Your brand in their hearts.

Beyond CRM

- Custom CRM for Law Firms, Secure client portals, document automation, case citations and references, compliance tracking, and integrated bookkeeping.
- Web & Mobile apps Development, Full-Stack Development, e-Commerce platforms, and Ai & BotTech solutions with embedded security protocols.
- Business Process Modeling & Reengineering, Solution Architecture Design & Redesigning for resilience, clarity, and control.
- Cloud hosting, VPS Hosting, Shared Hosting and Dedicated Hosting
- Business Application Services: Quickbooks and Saga Accounting (Bookkeeping, Invoicing, payroll, inventory, tax compliance, financial reporting)

Global Recognition

McDon's commitment to excellence has earned it accolades across Africa, Europe, and North America:

- *Best Insurance CRM Service Provider 2025 – MEA Markets (Africa)*
- *CRM Platform of the Year 2024 – CorporateLiveWire (Europe)*
- *Excellence Award for Web & App Development Services 2024 – New World Report (North America)*
- *Best Business Management CRM Solution Provider 2024 – New World Report (North America)*
- *Best Full-Service CRM Platform 2023 – New World Report (Canada)*

These honors reflect McDon's global footprint and its ability to deliver secure, scalable solutions that meet the highest standards of innovation and trust.

McDon Consolidated – *Inventing the Digital Future with Your Business*

CEO's Profile:

Chief Executive Officer, McDon Consolidated

DonDaddy N. Kyeremateng is the visionary CEO & CTO of McDon Consolidated Ltd, a fast-rising Software Company in Canada and Ghana CRM solutions provider serving African SMEs, Schools and Insurers.

With over two decades of experience spanning IT infrastructure, Generative Ai & Application Development, and the Insurance industry, DonDaddy has positioned McDon as a trusted partner in safeguarding business continuity and client trust across the continent.

Key Achievements:

Founded McDon Consolidated to address the cybersecurity and CRM needs of underserved African markets.

Developed DigitInsure CRM and DigitCRM, two flagship platforms tailored for Insurance and SMEs sectors.

Led McDon's expansion into Ghana, Nigeria, and Kenya, with a growing footprint in North America.

Championed mobile-first cybersecurity, making enterprise-grade protection accessible to SMEs and startups.

Recognized for thought leadership in digital trust, data protection, and strategic onboarding.

Advised Insurance firms on digital transformation, claims automation, and customer experience optimization.

DonDaddy's leadership blends technical depth with strategic foresight, making him a standout figure in Africa's digital transformation journey—especially in sectors where trust, compliance, and operational resilience are paramount.

Unlocking Business Growth:

Why Africa Must Embrace CRM Technology

In today's hyper-connected global economy, Customer Relationship Management (CRM) systems have become the backbone of modern business success.

From New York to Tokyo, companies rely on CRM platforms to streamline operations, enhance customer engagement, and drive exponential growth. Yet, across much of Africa, the adoption of CRM remains surprisingly low—not due to lack of need, but lack of awareness.

What Is CRM and Why Does It Matter?

CRM stands for Customer Relationship Management. It refers to software tools that help businesses manage interactions with current and potential customers. CRM is more than just software—it's a strategic approach to managing customer relationships, automating workflows, and improving internal collaboration. It empowers businesses to:

- Track leads and customer data.
- Automate sales and supports processes & boosts operational efficiency
- Generate real-time analytics for smarter decisions.
- Foster seamless communication across departments.
- Enhances customer satisfaction.
- Higher retention rates, Increase referrals
- Better upselling and cross-selling opportunities

In advanced economies, CRM is a standard tool for scaling businesses. It's no coincidence that the most competitive companies in the world are also the most digitally organized.

CRM Complements Core Business Systems

Operational efficiency today demands more than just robust core systems. While ERP platforms in manufacturing, accounting engines in finance, underwriting systems in insurance, and booking tools in hospitality form the backbone of sector-specific operations, they often fall short in managing customer relationships and front-office agility.

That's where CRM comes in—not as a luxury, but as a strategic necessity. CRM integration bridges the gap between transactional systems and customer engagement, enabling unified data flows, personalized service delivery, and faster decision-making across departments and branches

In Western markets, it's standard practice to integrate CRM with core systems to:

- Centralize customer data across departments.
- Personalize communication and service delivery.
- Automate follow-ups, reminders, and client engagement.
- Improve forecasting and decision-making with real-time insights.

CRM doesn't replace your core system—it enhances it. It fills the gap between transactional operations and relationship-driven growth. That's why companies in sectors like healthcare, real estate, education, insurance, and logistics all use CRM to stay competitive.

The Data Speaks: Africa's CRM Gap

The global CRM adoption rate is staggering—91% of companies worldwide use CRM systems, according to Grand View Research. In contrast, CRM spending per employee in Africa averages just $2.35, highlighting a massive underutilization of digital tools.

This gap is more than a statistic—it's a missed opportunity. Consider this:

- SME Survival Crisis: Up to 90% of African SMEs fail within five years, often due to poor customer management and lack of structured sales tracking (African Development Bank).
- CRM ROI: Businesses using CRM report a 29% increase in sales, 32% boost in forecasting accuracy, and up to 30x return on investment (Nucleus Research).

These figures make a powerful case: CRM isn't just a tool—it's a growth engine and a survival strategy.

McDon Consolidated: Africa's CRM Trailblazer

Recognizing this gap, McDon Consolidated, a forward-thinking software company based in Canada and Ghana, has developed two CRM products tailored specifically for the African business ecosystem.

DigitCRM

DigitCRM is a smart, mobile-friendly CRM platform tailor-made for SMEs and enterprises across industries—from retail and real estate to professional services to healthcare and education. It offers:

- Lead and client management.
- Automated invoicing and secure payments.
- Workflow optimization and cross-departments & branches collaboration.
- Advanced analytics and reporting.
- A self-service portal for customers.
- Ideal for remote, hybrid, or in-office working environments.

DigitCRM was designed to meet Africa's business realities head-on, empowering companies with tools that are not just functional, but contextually intelligent.

DigitInsure CRM

DigitInsure CRM is a specialized tailored-made CRM and workflow system designed to support the unique operational needs of various Insurance segments. It offers:

- Tailored policy management modules for life, health, pensions, group business and general insurance including brokers
- Automated claims processing, premium & renewal collection, and complaint resolution customized to each product line
- Real-time collaboration between agents and back-office staff, with sector-specific workflows
- Mobile access for distribution teams to issue invoices and receipts on the go - speed to digital selling
- A self-service portal for

Continued on next page

ISA®

INFORMATION SECURITY ARCHITECTS

No. 8 Lomo Adawu Street, La – Accra | P. O. Box OS 3082, Osu – Accra |
+233550330753 +233264284133 +233244430935 | business@isa.com.gh

Why Ghana's Financial Sector is Pioneering Cyber Resilience

A Sector Under Siege

The financial services sector has become the bellwether of cybersecurity maturity in Ghana, often leading the way for other industries.

Banks and financial institutions face constant cyber threats, strict regulatory oversight, and high customer expectations. These pressures have forced them to invest heavily in security, adopt advanced practices, and nurture talent positioning finance as the natural driver of national cyber resilience.

Globally, banks are the most targeted organizations. A 2024 Mandiant report showed the financial industry accounted for 17.4% of all cyberattacks more than any other sector.

In Africa, the threat surge is particularly steep, with organizations facing over 2,100 cyberattacks per week on average in 2023. Banks are doubly vulnerable practically because they hold sensitive data and money, and they are quick adopters of digital channels, cloud platforms, and fintech services. This expands their attack surface, making them magnets for phishing, fraud, ransomware, and state-backed attacks.

But with high risk comes high awareness. As Moody's analysts put it, financial institutions' long experience with cyber threats has given them a "heightened awareness" that translates into superior investment, governance, and talent acquisition.

Regulation as a Driver

A second reason banks lead in cybersecurity is regulatory pressure. In Ghana, the Bank of Ghana's Cyber & Information Security Directive compels banks to establish SOCs, implement incident reporting, and maintain governance frameworks.

In parallel, the Cybersecurity Act and the Cyber Security Authority's guidelines for Critical Information Infrastructure (CII) reinforce minimum standards across the sector. These requirements leave little room for complacency. One Ghanaian bank, facing a regulatory deadline to operationalize a Security Operation Center (SOC), turned to Managed Detection and Response (MDR) services to meet compliance quickly.

Within weeks, the MDR provider deployed sensors, integrated logs into its hybrid cloud and on-premises SIEM and provided 24/7 threat monitoring effectively spinning up SOC capabilities without the long delays of building in-house. The bank met its deadline, avoided penalties, and gained an advanced operation capable of real-time detection and rapid response.

Benefits of MDR

The MDR approach ultimately delivered far more than regulatory compliance. By enabling continuous, round- the-clock monitoring, it ensured that gaps in detection were effectively closed and potential threats could be spotted before escalating into serious incidents.

Beyond vigilance, the presence of dedicated analysts meant that whenever suspicious activity was identified, responses were immediate, often within minutes. This rapid intervention limited damage, preserved business continuity, and provided the bank with a level of agility that would have been difficult to achieve internally.

Equally significant was the infusion of external expertise through the MDR service. The bank gained access to advanced threat intelligence and insights into emerging attack patterns that its internal team might not have been able to identify alone. This augmented intelligence placed the institution ahead of the curve, strengthening its defensive posture against sophisticated adversaries.

Moreover, the structured reports generated by the MDR system simplified the audit process, providing regulators with clear evidence of the bank's compliance efforts. These reports not only reassured authorities but also gave management confidence in the robustness of its security operations.

Taken together, these advantages highlight how financial institutions are pioneering the use of security-as-a-service models. By embracing MDR, they are not simply meeting compliance obligations but setting new standards in agility, intelligence, and accountability—approaches that other sectors are only beginning to explore.

People at the Center

Technology is only part of the story. Banks recognize that skilled people remain the backbone of resilience. Yet Africa faces a severe cybersecurity talent shortage. Cisco's 2024 study highlighted that while demand is surging, training programs remain limited.

Financial firms have stepped up by supporting capacity-building initiatives. For example, Information Security Architects (ISA) runs its Information Systems Vulnerability Management (ISVM) training since 2018, through which more than 50 individuals have learned practical vulnerability management skills. Many of the trainees have gone on to become analysts, auditors, and penetration testers in Ghana's workforce.

This human investment extends to partnerships. In the MDR case, the external analysts worked closely with the bank's IT staff, transferring knowledge and building local capacity. The blend of external expertise with in-house upskilling illustrates how financial institutions can close skill gaps while securing their systems.

Beyond technical training, banks are also leaders in security awareness campaigns for their general workforce, running phishing drills, executive workshops, and secure coding sessions. This helps cultivate a security-first culture that ripples across supply chains and vendors.

A Model for Other Industries

The financial sector's progress has knock-on effects for the wider economy. By demanding robust security from vendors, banks indirectly raise standards across SMEs and service providers. Through industry groups like the Ghana Association of Banks, banks share lessons on compliance automation and incident handling effectively setting the pace for other industries such as telecoms, e-commerce, and government.

Many of today's cross-sector standards, like PCI-DSS and ISO 27001, originated in finance. Similarly, banking CERTs and information-sharing networks have served as models for sectoral collaboration. In Ghana, the sector's leadership has already begun influencing parallel initiatives in critical information infrastructure.

Conclusion

Ghana's financial institutions are not just protecting themselves; they are trailblazing a path to national cyber resilience. Their heightened exposure, regulatory obligations, and proactive investments have made them the most mature sector in cybersecurity.

By embracing innovations like MDR, embedding governance into their structures, and fostering talent through training, they provide both a shield for their customers and a template for others to follow.

As cyber threats escalate, the financial sector's role as a pace-setter is invaluable. By sharing experiences and supporting the ecosystem, banks are helping shape a digital future that is not only secure for themselves but also safer for Ghana's broader economy.

Bridging Ghana's Cybersecurity Skills Gap: Building Local Talent for a Secure Future

In Ghana and across Africa, cybersecurity has become a central pillar of economic resilience. Yet, while threats rise rapidly, the availability of skilled professionals has not kept pace. This mismatch creates a skills gap that threatens not only businesses but also national security. Closing this gap is no longer a matter of choice — it is an urgent necessity. The good news is that local initiatives and industry-driven programs are beginning to shift the landscape, providing both inspiration and a practical roadmap.

Understanding the Gap

Global studies have repeatedly warned of cybersecurity workforce shortages, but the African context is particularly acute. A 2024 Cisco report estimated that Africa needs millions of cybersecurity professionals in the coming years, yet structured training pathways remain limited.

In Ghana, the demand is especially high in the financial sector, where regulatory compliance and relentless attacks create a constant need for skilled defenders. Banks and regulators need SOC analysts, incident responders, and data protection officers, but too few graduates leave school with the required practical skills. This shortage has real consequences: organizations take longer to detect breaches, over-rely on external consultants, and struggle with compliance.

ISA's Contribution:

Training as a Launchpad

One of the most effective approaches to bridging the gap has been industry-led training. Information Security Architects (ISA), for example, runs its Information Systems Vulnerability Management (ISVM) program, designed to give learners practical skills in identifying and managing vulnerabilities.

Over 250 participants have completed the training, including university graduates, junior IT officers, and even professionals transitioning from unrelated fields. Many of them have since entered the workforce as security analysts, penetration testers, and compliance officers. For these individuals, ISVM training became a career launchpad giving them hands-on exposure that a traditional classroom could not provide.

This highlights a key truth: bridging the skills gap is not just about producing degrees but about creating pathways into real-world practice.

Challenges to Retention

Yet, building talent is only half the battle. Retaining it is equally difficult. Ghanaian firms often lose trained staff to multinational companies, international organizations, or even foreign markets offering higher pay.

This "cybersecurity brain drain" is a global phenomenon, but it hits emerging markets harder. Businesses in Ghana need to think creatively about retention — offering career progression, competitive benefits, and continuous learning opportunities. Equally, public policy could explore incentives to keep talent local, such as subsidies for cybersecurity apprenticeships or national service placements in critical infrastructure sectors.

The Role of Industry-Academia Partnerships

Another piece of the puzzle lies in closer collaboration between universities and industry. Academic programs often focus heavily on theory, while industry needs hands-on practitioners. Initiatives like guest lectures, internship pipelines, and co-designed curricula can close this gap.

Financial institutions, for example, can sponsor university labs or SOC simulations, while universities can embed compliance and digital forensics into IT courses. Such partnerships not only build skills but also ensure graduates are job-ready.

Why Local Content Matters

Critically, Ghana must avoid over-reliance on imported training. While global certifications are valuable, local content

ensures relevance to Ghana's regulatory and threat landscape. Training that integrates Ghana's Data Protection Act,Cybersecurity Act, and sector-specific directives equips professionals to solve local problems. ISA's work reflects this approach: programs contextualize global frameworks (ISO 27001, NIST) within Ghana's environment. This mix of global best practices and local realities is what creates effective defenders.

A Path Forward

To truly bridge the cybersecurity skills gap, Ghana requires a multi-layered and deliberate strategy that goes beyond isolated interventions. One critical step is the expansion of industry-led practical training programs that focus on producing job-ready professionals. These initiatives must provide hands-on exposure to real-world tools, threats, and compliance requirements so that graduates are not only theoretically competent but immediately useful to employers. Another important layer involves skills transfer through partnerships.

Collaborations between companies and external service providers, such as MDR engagements, allow in-house teams to learn directly from seasoned experts. This approach not only provides immediate protection but also ensures that local staff gain the competence to manage future incidents, thereby creating sustainable capacity within organizations.

Addressing the challenge of retention is equally vital. Ghana needs clear career pathways and retention policies that make it attractive for skilled professionals to stay in-country. Competitive incentives, opportunities for growth, and a supportive work culture can help curb the migration of talent to foreign markets or multinational corporations.

Equally essential is industry-academia collaboration. Universities and training institutions must work hand in hand with industry leaders to align curricula with market needs. This will ensure that graduates emerge with both the theoretical foundation and the applied skills demanded by employers. Initiatives such as joint research, internships, and guest lectures can serve as bridges between classroom learning and industry realities.

Finally, there must be a strong commitment to developing local content. While global certifications and frameworks are valuable, training that integrates Ghana's own regulatory requirements and threat landscape will make professionals more effective. Contextualizing global best practices within local realities ensures that cybersecurity strategies are relevant, sustainable, and tailored to the nation's unique challenges.

Conclusion

The cybersecurity skills gap in Ghana is real, but it is also solvable. Programs like ISVM prove that with targeted, practical training, individuals can quickly step into vital roles. MDR collaborations show how skills transfer can happen on the job. And human stories demonstrate that bridging the gap isn't just about statistics — it's about giving people futures while protecting national assets.

If Ghana continues to blend local content, industry leadership, and human-centered strategies, it can turn today's skills shortage into tomorrow's competitive advantage. The result would not only be safer businesses but also a stronger digital economy powered by Ghanaian talent.

Cybersecurity

A pillar for safeguarding critical infrastructure

By Abubakari Saddiq ADAMS

As Ghana continues its rapid digital transformation, the protection of critical infrastructure has become a pressing national priority. From power grids and water supply systems to transportation networks and financial institutions; these essential services form the backbone of Ghana's economy and public safety.

However, the increasing reliance on digital systems has also made them vulnerable to sophisticated cyberattacks. Safeguarding these critical systems is not just a technological challenge but a national security imperative.

This article digs into the significance of protecting critical infrastructure, the unique threats facing Ghana, and the measures needed to strengthen national cybersecurity defenses.

What is Critical Infrastructure?

Critical infrastructure refers to the foundational systems and assets, both physical and digital, that are indispensable for a nation's daily functioning, economic stability, and public safety. These components are vital to the point where their compromise, disruption, or destruction could result in severe consequences, such as economic collapse, loss of life, or national security threats.

Examples of Critical Infrastructure

Critical infrastructure spans across numerous sectors, including but not limited to:

1. Energy Systems:

o Power plants, electricity grids, oil refineries, and natural gas pipelines. Disruption can lead to widespread blackouts, fuel shortages, and hindered industrial operations.

2. **Water Supply Systems:**

o Dams, reservoirs, treatment plants, and distribution networks. A compromised water supply can result in public health crises and limit essential services.

3. **Transportation Networks:**

o Highways, railways, airports, seaports, and mass transit systems. Transportation disruptions can impede the movement of goods and people, affecting supply chains and emergency response.

4. **Communication Infrastructure:**

o Telecommunications networks, internet services, and broadcast systems. Cyberattacks or physical damage to these systems can disrupt information flow and emergency coordination.

5. **Banking and Financial Systems:**

o Banks, financial institutions, stock exchanges, and payment systems. Attacks on these systems can destabilize economies and erode public trust in financial systems.

6. Healthcare Systems:

o Hospitals, clinics, pharmaceutical supply chains, and emergency medical services. A cyberattack or physical disruption could delay critical care and put lives at risk.

7. Government Facilities:

o Administrative offices, military installations, and public service buildings. Compromises here can undermine governance and public safety operations.

8. Emergency Services:

o Fire, police, and rescue services. Interference in these services can hinder disaster response and jeopardize public safety.

The Digital Dimension

In modern times, critical infrastructure is increasingly interconnected through digital networks, making it vulnerable to cyberattacks. Hackers, whether state-sponsored or criminal groups, often target these systems to cause disruptions, demand ransoms, or conduct espionage.

The Importance of Protecting Critical Infrastructure

Safeguarding critical infrastructure is a top priority for nations because:

· It supports the economic engine of a country.

· It ensures public health and safety.

· It maintains national security and sovereignty.

Given its significance, protecting critical infrastructure requires a multifaceted approach involving cybersecurity measures, physical protection, public-private partnerships, and international cooperation.

Cybersecurity Threats Facing Ghana's Critical Infrastructure

Ghana's digital transformation has brought immense opportunities but also heightened exposure to cyber risks. Key threats include:

1. Ransomware Attacks

Ransomware has become a global menace, with hackers targeting critical systems and demanding payment to restore access. For example, hospitals and energy grids could be rendered inoperable, jeopardizing public health and economic activity.

2. State-Sponsored Espionage

Regional and global geopolitical tensions could lead to state-sponsored cyberattacks aimed at espionage or sabotage. Energy and financial systems are prime targets.

3. Insider Threats

Disgruntled or malicious employees or contractors with access to sensitive systems can pose significant risks, especially if proper access controls and monitoring are not enforced.

4. Supply Chain Vulnerabilities

Compromises in third-party software or hardware can introduce vulnerabilities into critical systems, providing attackers with indirect entry points.

5. Cybercrime and Hacktivism

Ghana's expanding mobile money ecosystem and government services are attractive targets for cybercriminals seeking financial gain or hacktivists promoting ideological agendas.

Current Gaps in Ghana's Cybersecurity Posture

While Ghana has made strides in cybersecurity, challenges persist:

- **Limited Expertise:** A shortage of skilled cybersecurity professionals to manage and defend critical systems.
- **Fragmented Efforts:** Lack of cohesion between public and private sector cybersecurity initiatives.
- **Resource Constraints:** Budgetary limitations hinder the adoption of adequate security measures and tools.
- **Insufficient Public Awareness:** Many citizens and employees lack basic cybersecurity knowledge, increasing vulnerabilities.

Building a Resilient Cybersecurity Framework

To address these challenges, Ghana must implement a multi-pronged approach that combines technology, policy, and public-private collaboration.

1. Strengthening Policy and Regulation

The Cybersecurity Act, 2020 (Act 1038) provides a solid foundation for regulating and protecting critical information infrastructure. However, enforcement must be robust, with regular updates to address evolving threats.

· Develop sector-specific guidelines for energy, finance, and healthcare.

· Align national policies with international standards like the NIST Cybersecurity, Framework and ISO 27001.

2. Capacity Building

· Building local expertise is essential. Invest in training programs for cybersecurity professionals through institutions like the Cyber Security Authority (CSA).

· Incorporate cybersecurity into tertiary education curricula.

3. Technological Innovations

· Adopting advanced technologies can enhance threat detection and resilience.

· Deploy AI and machine learning for real-time threat analysis.

· Use blockchain for secure transactions and tamper-proof data storage in sectors like finance and energy.

· Implement robust backup systems for quick recovery in the event of an attack.

4. Public-Private Partnerships

Collaboration between government agencies, private organizations, and international entities is critical.

· Establish information-sharing mechanisms to share threat intelligence and best practices.

· Engage in joint cybersecurity exercises to test and improve response capabilities.

5. Public Awareness Campaigns

Educating citizens on cybersecurity best practices is vital for reducing human error, a major factor in cyber incidents.

· Launch nationwide campaigns targeting mobile money users and small businesses.

· Incorporate basic cybersecurity training into school curricula.

The Role of International Cooperation

Cyber threats are not confined by borders, making international collaboration essential. Ghana can:

· Participate in global initiatives like the Global Forum on Cyber Expertise (GFCE) and the ECOWAS Cybersecurity Agenda.

· Partner with organizations like IIPGH, ISOC and ICANN to enhance technical capacity.

· Share threat intelligence with neighboring countries to strengthen regional defenses.

Conclusion

The protection of Ghana's critical infrastructure is not just a technical issue but a matter of national security, economic stability, and public trust. A resilient cybersecurity strategy must integrate robust policies, advanced technologies, skilled professionals, and strong partnerships.

As Ghana continues its digital transformation journey, proactive investment in cybersecurity will ensure the nation can not only defend against emerging threats but also thrive in an increasingly interconnected world. Safeguarding our critical infrastructure is a shared responsibility—one that demands vigilance, collaboration, and innovation at every level of society.

The author is a | Business IT & IT Legal Consultant with a focus on IT governance and cybersecurity | Member of IIPGH.

For comments: +233246173369 | abubakrsiddiq10@gmail.com

The true meaning of cybersecurity

By Martin Ignacio Díaz Velásquez

As more activities move online, our understanding of cybersecurity must evolve to stay ahead of emerging threats to public health and security. The digital market for illegal recreational substances shows why longstanding law-enforcement strategies will need to be reconsidered.

When we talk about cybersecurity, we usually think of commercial antivirus software, ransomware attacks on large corporations, or leaks of politically scandalous emails. But little is said about public security in the digital realm, and that is a big problem when we increasingly depend on information and communication technologies (ICTs) and the Internet of Things to carry out our ordinary daily activities.

Consider illegal recreational substances. Many people now seek to acquire these over the internet, because buying online is generally seen as safer than meeting a stranger in a dark alley. But online channels tend to put people into direct contact with the organized crime groups that control most of the distribution of illicit substances.

When people hand over money to these groups, they are unwittingly helping to fund the global networks that also finance terrorism and traffic in arms, people, and human organs and tissues. It is well known that the COVID-19 pandemic accelerated many forms of digital innovation and adaptability, and online drug purchases are no exception. Amphetamine-type stimulants and new psychoactive substances are increasingly available on the darknet, the open web, crypto markets, and even social media.

There are both risks and potential benefits associated with these new distribution channels. On a positive note, analyzing digital data flows could allow for faster detection of novel psychoactive substances that pose a threat to public health.

And, of course, transacting on crypto markets or through similar digital channels can protect individual users from physical violence, theft, sexual exploitation, and abduction. Moreover, recent studies show that people who use drugs and acquire substances through ICTs are more likely to adopt harm-reduction practices and promote responsible use, generally because they are operating from the privacy of their homes or other safe settings.

With the sustainable-development agenda under severe strain, leading thinkers examine the initiatives and innovations that are delivering results.

Governments and law-enforcement authorities should keep these findings in mind as they seek to create safe public spaces online. While the state alone is responsible for defining what counts as a crime, policing criminal activity is not its sole purpose; it also must ensure public health and uphold fundamental rights such as privacy. And in the case of drugs, specifically, it will need to be more thoughtful about who is really a criminal, and who is a victim.

Accordingly, many law-enforcement strategies should be reconsidered, and resources should be redirected toward strengthening the competencies of nascent cybercrime units. Rather than pursuing recreational substance users and markets, investigative efforts should focus primarily on ICT-mediated criminal activities and operations that pose a significant threat to the general public.

Here, a promising new model is "pre-arrest police diversion" or "deflection." This collaborative intervention strategy connects law enforcement, biopsychosocial agents, and public-health systems to create community-based treatment and support pathways, so that drug users do not have to enter the justice system. As Jac Charlier of Treatment Alternatives for Safe

Communities explains, deflection positions "law enforcement to be the referral source to community-based drug treatment and mental-health services prior to potential crises. In this way, law enforcement opens up new treatment access points not previously available to those in need." But another problem is that it is difficult to find accurate online information about support pathways that is devoid of stigma or prohibitionist sophisms.

This must change. To create safe digital spaces, we need to shift public actions vis-à-vis drug users from a repressive perspective to an educational one. That means leveraging specialized law-enforcement units and optimizing the reach of biopsychosocial agents.

With these modifications, we also can start to rebuild the lost trust between this population group and law-enforcement agencies. These methods are known to reduce the impact of controlled-substance use on communities and households, while freeing up law-enforcement resources to focus on what really matters, such as terrorist financing, the rise of new opioid markets, counterfeit pharmaceuticals, arms trafficking, and child sexual-abuse material distributed online. But, owing to the hybrid nature of these forms of cybercrime, effective implementation of new law-enforcement strategies will require international coordination.

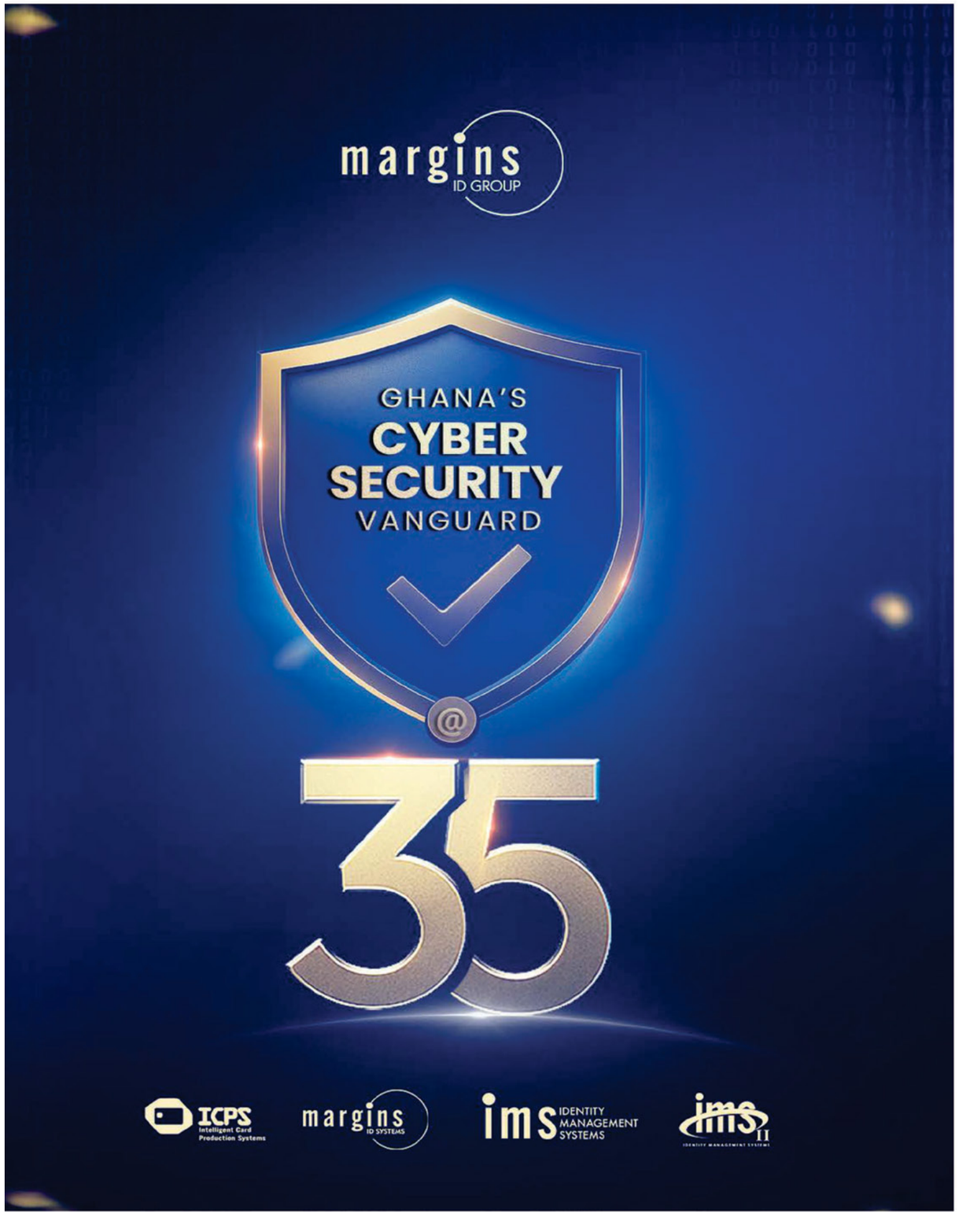
The United Nations has formed an ad hoc committee to draft a "Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes." But to ensure public security in cyberspace, the convention will need to couple improved law-enforcement procedures with the kind of humanitarian vision that underpins deflection.

As long as states insist on criminalizing recreational substances, people will continue to seek them on the black market, and law-enforcement agencies will continue to fight an uphill battle. But with the right strategies in place, ICTs have enormous capacity both to reduce harm to drug users and to empower law enforcement to focus on truly pernicious criminal behavior.

As the world increasingly moves online, we must recognize that cybersecurity is about more than preventing hacks and fraud. It is also about improving the safety, health, and well-being of the people behind the screens.

Martin Ignacio Díaz Velásquez, an ambassador for One Young World, is Co-Founder and CEO of the Knowmad Institut.

Credit ; Project Syndicate



SPECIAL PUBLICATION Cyber Security & IT Survey 2025 TOOLS, FIRMS AND FOUNDERS SHAPING DIGITAL SECURITY IN GHANA

MARGINS ID GROUP: GHANA'S CYBERSECURITY VANGUARD AT 35

The New Reality of Cybersecurity

The rapid adoption of emerging technologies is rewriting the rules of cyberspace. Artificial intelligence, cloud computing, and Internet of Things (IoT) are transforming economies, while expanding the attack surface at unprecedented speed. Cybercriminals are moving just as fast, leveraging these same technologies to launch more complex, large-scale, and borderless attacks.

Against this backdrop, cybersecurity is no longer a technical add-on. It is an indispensable foundation for resilience, a national imperative, and the cornerstone of digital trust.

AI: Risk and Opportunity

Artificial intelligence represents both the most formidable risk and the most powerful tool in today's cyber landscape. While adversaries weaponize algorithms to probe vulnerabilities and automate attacks, defenders are harnessing machine learning for predictive threat intelligence, anomaly detection, and real-time response.

According to the Global Cybersecurity Outlook 2025, 66% of organizations expect AI to significantly impact cybersecurity within the year. Yet, only 37% have processes to evaluate the security of AI systems before deployment. The gap between ambition and preparedness is widening; proactive frameworks will separate the resilient from the vulnerable.

Margins ID Group, with decades of expertise in secure systems, has long anticipated these shifts. By embedding vigilance into the design of every solution, the company has ensured that emerging technologies become opportunities for resilience rather than gateways for risk.

Africa's Digital Test Case

Too often, Africa is dismissed as a passive participant in the global cyber arena. That is a dangerous illusion. Rapid digitization, mobile-first economies, and accelerating fintech adoption have made the continent become a prime target for cybercriminals. Weak regulation and low awareness make emerging markets fertile ground for exploitation.

Ghana, however, is charting a different course. Through the Ghana Card, one of the most secure and integrated national ID system on the continent, millions of citizens transact daily under a cyber-hardened framework. Every secure payment, border crossing, and healthcare access point strengthens the nation's digital trust architecture. This is not theory; it is lived resilience.

Margins ID Group: Building the Backbone of Trust

For thirty-five years, Margins Group has been anticipating the very challenges that now dominate the global agenda. From its origins as a print and document finishing enterprise in 1990, Margins has evolved into a fully integrated provider of identity and cybersecurity solutions. Today, it sits at the intersection of technology, governance, and trust.

The Ghana Card, access control solutions and e-Immigration systems are not just technological projects; they are testaments to how identity and cybersecurity can be fused from design to deployment.

Each of these platforms carries the same philosophy: that secure identity is inseparable from secure systems. Identity assures who you are; cybersecurity ensures you remain protected. Together they form the DNA of digital trust.

Margins ID Group's leadership is reinforced by its global certifications including:

- CSA Cybersecurity Establishment & Cybersecurity Service Provider certification
- ISO 27001:2022 (Information Security Management)
- ISO 22301:2019 (Business Continuity Management)
- ISO/IEC 20000-1:2018 (Service Management System)
- CREST Pathway+ accreditation

These certifications form the operational backbone that allows the company to secure billions of transactions across banking, healthcare, immigration, and governance.

Equally important, Margins contributes directly to Ghana's wider cybersecurity ecosystem. Its role extends beyond technology deployment into thought leadership, policy engagement, and capacity building. By training new cybersecurity professionals, participating in collaborative forums, and advocating for stronger frameworks, Margins ID Group has helped ensure that Ghana's digital transformation remains ambitious yet defensible.

In this way, Margins has become more than a service provider. It is an institution of trust. The systems it has delivered prevents breaches and inspire confidence at every level. Citizens trust that their personal data remains secure when they use the Ghana Card to open a bank account. Businesses trust that digital payments will not be hijacked. Government trusts that online services are credible and safe. In each case, the product is not only protection, but belief; the confidence that digital systems can be relied upon.

The Vanguard of Trust

The complexity of cyberspace will only deepen in the years ahead. The next decade will bring sharper threats, smarter adversaries, and deeper dependencies on digital infrastructure. In this borderless environment, resilience will require more than firewalls; it will demand public–private collaboration, AI-driven defences, continuous compliance, and a culture of awareness.

Margins ID Group stands ready to lead this effort as Ghana's proof of concept and Africa's partner in resilience. The company's 35-year journey demonstrates that Africa need not be a follower in global cybersecurity. With fresh infrastructure, local expertise, and a steadfast commitment to trust, Ghana has proven it can set the standard.

Cybersecurity is not optional; it is sovereignty.
The time to act is now.

The rising menace of illegal loan apps in Ghana

By Dickson ASSAN

Across Ghana, the demand for quick and accessible credit continues to grow. Small business owners, traders, and individuals struggling with daily financial pressures often look to digital platforms for relief. Unfortunately, this need has become fertile ground for the proliferation of illegal loan applications, which operate without approval or oversight from the Bank of Ghana.

As of today, the only licensed and approved digital lending app in Ghana is Fido, according to the data from the Bank of Ghana website. Every other loan app you encounter is operating illegally. Yet, despite this clear regulatory position, unlicensed loan apps have mushroomed across the country, luring thousands of unsuspecting Ghanaians into debt traps.

Since I first wrote about this issue last year, more than 20 people have reached out to share their harrowing experiences with these platforms. Their stories expose the true cost of engaging with unregulated lenders and the urgent need for stronger enforcement.

Exploitation Through Data and Privacy Breaches

Because these apps are illegal, they do not fall under the protections of the Data Protection Act, 2012 (Act 843). Borrowers are often forced to surrender access to their personal information, including phone contacts, photos, and messages. This sensitive data is then misused for harassment, threats, and public shaming when borrowers miss payments. The psychological toll on victims and the reputational damage inflicted cannot be overstated.

Exorbitant and Hidden Charges

One of the most alarming practices is the way these apps impose interest rates. In direct violation of Section 55(2) of the Borrowers and Lenders Act, 2020 (Act 1052), which requires all banks and Specialized Deposit-taking Institutions (SDIs) to calculate interest rates on an annual basis only, these unlicensed lenders quote rates by the day, week, or month.

Some charge as much as 15% per month, without ever disclosing the annual equivalent. For market women and small traders, the deception is even worse. Many are told, "We give you GHS 10,000 and you pay GHS 200 each day for six months." A simple calculation reveals that the borrower ends up paying GHS 36,000 for a GHS 10,000 loan — more than triple the original amount.

These predatory terms, coupled with hidden fees, trap borrowers in cycles of debt that are almost impossible to escape.

Harassment and Defamation

Beyond financial exploitation, victims face severe social consequences. Illegal lenders are notorious for sending defamatory messages to borrowers' employers, colleagues, and family members. Even individuals who are up to date with their repayments have been harassed in this manner. The goal is simple: to shame borrowers into compliance, regardless of fairness or legality.

A Gateway for Money Laundering

Perhaps the most dangerous element is the risk of financial crime. Because these loan apps operate outside the regulatory environment, they are not bound by the Anti-Money Laundering Act, 2020 (Act 1044) or by Bank of Ghana and Financial Intelligence Centre (FIC) guidelines on Know Your Customer (KYC) procedures.

This makes them convenient channels for criminals to move illicit funds under the guise of legitimate lending and repayment. Fake borrowers, shell accounts, and rapid micro-transactions can easily be used to whitewash dirty money. Left unchecked, these activities threaten not only individual borrowers but also the integrity of Ghana's financial system.

Risks to the Wider Economy of Ghana

First, these platforms distort the credit market. By offering loans outside the regulatory framework, they set their own exploitative terms, often with interest rates far beyond legal limits. This undermines fair competition and makes it difficult for responsible, licensed institutions to serve the same customers without appearing less attractive in the short term.

Second, they undermine licensed financial institutions. Banks and Specialized Deposit-taking Institutions (SDIs) are required to follow strict regulations under the Bank of Ghana, including transparent disclosure of interest rates, proper customer due diligence, and fair debt recovery processes. Illegal loan apps sidestep all of these rules, gaining an unfair advantage while weakening confidence in the institutions that play by the rules.

Another danger lies in tax evasion and capital flight. Many of these apps are backed by foreign operators who repatriate profits without paying local taxes. Funds that could have been reinvested into Ghana's economy instead disappear across borders, reducing government revenue and undermining economic development.

Finally, illegal loan apps degrade the quality of financial data available to policymakers, credit bureaus, and regulators. Because these transactions are outside official reporting systems, they create gaps and distortions in the data used to measure borrowing patterns, assess creditworthiness, and design effective monetary policies. In the long run, this weakens the ability of regulators to make informed decisions that protect both consumers and the economy at large.

The Role of Key Institutions

Tackling the menace of illegal loan apps demands a coordinated response from key state institutions. The Bank of Ghana must not only license, monitor, and sanction lenders but also intensify public education on safe borrowing practices.

The Financial Intelligence Centre (FIC) has a critical role in tracking suspicious transactions and enforcing compliance with anti-money laundering laws. At the same time, National Security must recognize these platforms as a genuine security threat, given their potential use in organized crime and illicit financial flows.

Finally, the Cyber Security Authority must step up efforts to investigate and dismantle predatory digital platforms, working in partnership with app stores, telecommunication companies, and law enforcement agencies.

A Call for Vigilance

Small business owners, traders, and individuals must be especially cautious. The promise of "quick money" comes at too high a cost. Always verify lenders through the Bank of Ghana's official list of approved institutions before borrowing. If you encounter a suspicious app, report it to the Bank of Ghana, FIC, Cyber Security Authority, or National Security.

Dickson ASSAN

Dickson is a Chartered Accountant and SME Business Coach. He is the Lead Consultant at CareerCompass Gh Limited, where he works with entrepreneurs and small business owners to strengthen governance, improve financial management, and build sustainable enterprises.
Mobile: +233242771314/Email: dicksonassan@gmail.com

Cybersecurity: Africa's unseen business risk—and its greatest opportunity by McDon Consolidated

Africa's Digital Boom: A Double-Edged Sword

From the vibrant markets of Accra to the tech corridors of Nairobi, Africa is experiencing a digital renaissance. Mobile money is mainstream, e-commerce is thriving, and cloud-based platforms are transforming how businesses operate. But as African enterprises embrace digital tools to scale and innovate, a silent threat is growing louder: cybercrime.

Cybersecurity breaches are no longer distant headlines—they're local realities. And while the continent celebrates digital progress, many businesses remain dangerously exposed.

The Real Cost of Cybercrime

Cyberattacks don't discriminate. They hit startups, SMEs, corporations, and even public institutions. A single breach can freeze operations, compromise customer data, and drain financial resources.

- **Financial Losses:** Ransomware, fraud, and recovery costs can cripple cash flow
- **Data Theft:** Sensitive customer and business data can be leaked or sold
- **Operational Disruption:** Attacks can shut down systems and halt transactions
- **Loss of Trust:** Customers lose confidence when their data is compromised
- **Legal Consequences:** Non-compliance with data protection laws can lead to fines and sanctions

In 2024 alone, African businesses lost an estimated $4 billion to cybercrime, according to data from INTERPOL's African Cyberthreat Assessment Report and coverage by Graphic Online during the AfPI meetings in Accra.

The figure reflects a growing threat that spans sectors and borders, underscoring the urgency for robust cybersecurity strategies.

Cybersecurity Is Not Just Tech—It's Strategy

Let's be clear: cybersecurity isn't just an IT issue. It's a business imperative.

When your systems are secure, your customers feel safe. Your team works confidently. Your data becomes an asset—not a liability. And your business becomes resilient, ready to scale without fear.

Investing in cybersecurity means:

- Protecting your revenue
- Complying with emerging data laws
- Empowering remote teams
- Building digital trust
- Future-proofing your operations

It's not a cost—it's a competitive advantage.

Why Many Businesses Still Hesitate

Despite the risks, cybersecurity adoption across Africa remains slow. Why?

- **Limited Awareness:** Many business owners don't realize how vulnerable they are
- **Cost Concerns:** Security sounds expensive—but breaches cost more
- **Resistance to Change:** Teams cling to outdated systems
- **Infrastructure Gaps:** Internet access and digital literacy vary widely

But these barriers are solvable. And the solutions are already here.

McDon Consolidated: Your Cybersecurity Partner

At McDon Consolidated, we're more than a software company—we're your go-to partner for cybersecurity solutions. We understand the African business landscape, and we've built tools that are:

Affordable: Scalable solutions for startups, SMEs, and enterprises

User-Friendly: No jargon, no complexity—just protection that works

Mobile-Ready: Designed for teams on the move

Locally Supported: Training, onboarding, and real-time assistance

Whether you're a retailer in Kumasi, a fintech in Lagos, or a logistics firm in Nairobi, we help you secure your digital future—without slowing you down.

How to Get Started

Cybersecurity doesn't have to be complicated. Here's how to begin:

Assess Your Risks: Identify your digital vulnerabilities

Train Your Team: Human error is the #1 cause of breaches

Secure Your Systems: Use firewalls, encryption, and secure platforms

Backup Regularly: Ensure you can recover quickly from any attack

Partner with Experts: Let McDon Consolidated tailor a solution for your business

Conclusion: Secure Growth Is Smart Growth

Africa's digital future is bright—but only if it's secure. Cybersecurity is not a luxury for large corporations. It's a necessity for every business, from the corner shop to the multinational.

At McDon Consolidated, we don't just offer software—we offer peace of mind. We help African businesses protect what matters most: their data, their customers, and their reputation.

The question isn't if you'll face a cyber threat. It's when. And when that moment comes, will your business be ready?

Secure your business. Empower your future. The time is now.

Unlocking Business Growth

Why Africa Must Embrace CRM Technology

Continued from previous page

- customers to manage policies, payment history, policy statements, submit claims, file complaints, and track updates independently—anywhere, anytime
- Integrated payment solutions for seamless premium collection, refunds, and customer transactions across all supported Insurance products

DigitInsure doesn't replace core Insurance systems—it enhances them, making operations smarter, faster, and more customer-centric.

Both platforms are built to international standards but speak the language of African business—flexible, intuitive, and scalable.

Homegrown Solutions Matter

In a December 2021 article for Harvard Business Review, tech entrepreneur Elo Umeh made a compelling case for why Africa's digital transformation must be powered by homegrown solutions. Imported platforms, he argued, often fail to accommodate the continent's mobile-first behavior, fragmented data ecosystems, and regulatory diversity.

"Success requires enterprise solutions that reflect the context and nuances of the continent's market needs." — Elo Umeh

McDon Consolidated's products embody this philosophy. They're not just software—they're strategic tools built for Africa's unique business terrain.

Proof That These Products Work

Real-world results speak louder than features. Here's how DigitCRM and DigitInsure CRM have transformed businesses:

- A Ghanaian retail chain boosted repeat purchases by 35% using DigitCRM's segmentation tools.
- An insurance firm in Kenya slashed claims processing time by 50% with DigitInsure CRM.
- A pan-African logistics startup expanded into three new markets and increased operational efficiency by 40%—managing everything from their phone.
- A Canadian travel and tour company increased invoice processing speed by 30%, reduced payment delays by 40%, and streamlined client document requests and staff shift coordination by 45% using DigitCRM
- A Ghana-based life coaching and counselling business increased client retention by 60% and reduced missed appointments by 50% with DigitCRM's automated follow-ups.
- A UK-based homecare provider enhanced caregiver scheduling accuracy by 55% and improved client communication response time by 35% through DigitCRM's mobile dashboard.

These aren't just numbers. They're stories of transformation. Stories of possibility.

The Future Is Digital and Collaborative

Africa's business potential is immense. But to unlock it, companies must embrace tools that drive efficiency, transparency, and growth. CRM is not a luxury—it's a necessity.

With platforms like DigitCRM and DigitInsure CRM, McDon Consolidated is not just offering software; it's offering a vision for a smarter, more connected African business landscape.

It's time to move from spreadsheets to strategy. From manual to mobile and automation From reactive to proactive.

Africa doesn't need to catch up—it needs to leap forward.

Reference: Elo Umeh, "Digital Transformation in Africa Requires Homegrown Solutions," Harvard Business Review, December 15, 2021.
https://hbr.org/2021/12/digital-transformation-in-africa-requires-homegrown-solutions or Scan

Sidebar: CRM as a Cybersecurity Ally

In today's digital economy, customer data is currency—and protecting it is essential.

While CRM platforms are often seen as sales tools, they also play a vital role in cybersecurity readiness:

- **Centralized Data:** Controlled Access CRM systems consolidate customer records, making it easier to apply access controls and monitor usage.
- **Audit Trails and Accountability:** Every interaction and transaction is logged, supporting compliance and forensic analysis.
- **Secure Communication Channels:** Built-in messaging and document sharing reduce reliance on unsecured third-party apps.
- **Role-Based Permissions:** Platforms like DigitCRM and DigitInsure CRM allow businesses to assign roles and restrict access, minimizing internal threats.
- **Mobile Security:** With mobile-first design, these platforms support secure remote access—critical for hybrid teams and field agents.

As African businesses digitize, CRM adoption isn't just about growth—it's about resilience. A well-implemented CRM is a frontline defense against data breaches, fraud, and operational chaos.

Fraud, scams top cyber threats to businesses – Zenith Bank's CISO

By Christabel DANSO ABEAM

Currently, the biggest cyber threats facing Ghanaian businesses are fraud and scams, especially through emails, card transactions and mobile money, says Chief Information Security Officer (CISO) and Data Protection Supervisor (DPS) at Zenith Bank Ghana Limited, Emem Umoh,

Unlike traditional hacks that primarily targeted systems, Mr. Umoh noted that cybercriminals are increasingly focusing on exploiting people.

Earlier this year, the Cyber Security Authority (CSA) raised concerns over a sharp rise in cybercrime incidents across Ghana, warning that escalating digital threats present significant risks to individual safety, business operations, and national security.

According to the CSA, reported cybercrime cases rose from 1,317 in the first half of 2024 to 2,008 during the same period in 2025—an alarming 52 percent increase that underscores the urgency of the challenge.

However, the expert also underscored talent shortages as an emerging challenge in the cybersecurity sector, pointing to critical gaps in specialised areas such as cloud computing, artificial intelligence (AI), and digital forensics.

The authority indicated that the most common types of incidents were online fraud scoring 36 percent , cyberbullying 25 percent, and online blackmail 14 percent.

Financial losses associated with these crimes rose by 17 percent year-on-year, reaching GH14.94 million.

Notably, online fraud and impersonation accounted for over 90 percent of the total losses.

Speaking to the B&FT, he underscored the importance of encouraging digital transformation in companies while maintaining security and awareness creation.

"With every new digital project — whether it's a mobile app or moving to the cloud — safety must be built from the start. So, it is important to involve security early, check risk and train staff to think "safety first." That way, we innovate without exposing customers and the organisation to danger".

Reflecting on lessons learnt from managing cyber incidents, Mr. Umoh noted that communication is the most important solution, while stressing that timely updates to boards, regulators and customers can protect trust while breaches are solved behind the scenes.

According to him, the role of a chief information security officer extends beyond technical expertise, serving as both a guardian who protects the organisation and a translator who simplifies risks for leaders and staff to act upon. He added that the position also demands strong collaboration with regulators and industry peers, as no single entity can combat cybercrime in isolation.

Among other concerns, he highlighted talent shortages as a growing challenge in the cybersecurity environment, pointing to significant gaps in specialised areas such as cloud security, artificial intelligence, and digital forensics.

He noted that addressing this deficit would require investment in training, mentorship, university programmes, and retainership schemes to build a home-grown cybersecurity workforce.

He further urged boards of directors to engage their chief information security officer with critical questions, including how exposed the company would be in the event of a major attack, whether the organisation is meeting all regulatory requirements, and how quickly it could recover while safeguarding customer trust.

Looking ahead, he predicted that artificial intelligence (AI) would significantly reshape cybersecurity, noting that it would have both positive and negative impacts.

While AI could enable faster detection of fraud, he cautioned that criminals would equally exploit it to make scams harder to detect. He further observed that cloud services would continue to transform the way data is stored and protected.

On where the next cedi should be invested in cybersecurity, he was emphatic that the priority must be people. "No matter how advanced our systems are, if staff and customers are not alert to scams, it can translate into losses. Awareness and training deliver the best return on every cedi spent," he explained.

Cybersecurity risk exposure for Ghanaian Businesses The way forward

Continued from page 9

is equally critical. Businesses rely heavily on suppliers, contractors, and outsourced developers, yet these partners can become the weakest link.

For SMEs, even simple steps such as secure backups, antivirus software, and basic staff training can close significant gaps.

Cybersecurity firms in Ghana are uniquely positioned to bridge the gap between regulatory expectations and business realities. They are more than service providers; they are partners in resilience.

Among them, Cyberteq stands out as a trusted partner, providing end-to-end services that help organizations safeguard their infrastructure, comply with regulatory directives, and prepare for the evolving threat landscape.

On the offensive security front, Cyberteq conducts Vulnerability management throught its property MUNIT solution to uncover hidden weaknesses before attackers can exploit them. Secure code reviews are performed to ensure that software applications meet the highest security standards and are free from exploitable flaws. These proactive measures give businesses the confidence that their systems are tested, hardened, and ready to withstand threats.

Cyberteq provides round-the-clock protection through its 24/7/365 Security Operations Center (SOC). The SOC continuously monitors networks, detects suspicious behavior, and responds to potential threats in real time. When incidents do occur, Cyberteq's Incident Response and Digital Forensics (DFIR) team step in to investigate, contain, and remediate breaches. This integrated approach minimizes downtime and ensures that organizations can recover quickly and with confidence.

Cyberteq also delivers Governance, Risk, and Compliance (GRC) services. This includes implementing and auditing Business Continuity Management Systems (BCMS), guiding organizations through international standards such as ISO 27001 and ISO 27701, and ensuring compliance with local requirements such as the Bank of Ghana Cyber & Information Security Directive and the Critical Information Infrastructure (CII) Directive.

Beyond compliance, Cyberteq works with clients to design cybersecurity strategies tailored to their business objectives, helping them embed resilience into their culture and operations.

Awareness is a critical component of this strategy. Cyberteq runs targeted awareness training programs for boards, executives, employees, and even external stakeholders like agents and customers. These sessions demystify cybersecurity and build a culture where everyone plays a role in defending the organization.

For SMEs, Cyberteq offers affordable, scalable packages that combine essentials such as cloud security, data backups, and staff training, ensuring that protection is not the exclusive privilege of large corporations.

Finally, Cyberteq leverages artificial intelligence and behavioral analytics to provide advanced monitoring solutions. By analyzing patterns of user and system behavior, these tools detect insider threats and fraud attempts early, often before they escalate into damaging breaches.

In short, firms like Cyberteq bring together the full spectrum of cybersecurity from offense to defense, compliance to strategy, awareness to advanced analytics offering Ghanaian businesses the confidence to innovate and grow securely in a digital-first economy.

Ghana's progress in cybersecurity is undeniable. From fragmented beginnings, the country now has a dedicated regulatory authority, a functioning national CERT, global recognition, and an expanding ecosystem of professionals and service providers. But the challenges ahead are equally undeniable. Fraudsters are innovating as quickly as defenses are being built. Insider threats persist. SMEs are increasingly vulnerable. Recovery rates remain low.

The stakes are high. Without robust cybersecurity, the hard-won gains of digital transformation could quickly unravel. But with the right mix of governance, investment, awareness, and partnership, Ghana can build a resilient digital economy that thrives securely.

For businesses, the imperative is clear: cybersecurity is not optional. It is a strategic necessity that protects not just data but also reputation, trust, and survival.

For cybersecurity professionals and service providers the responsibility is equally clear: to provide the expertise, tools, and resilience Ghana needs to move confidently into the future.

The digital future will not wait. Neither should we defend.

B&FT Business & Financial Times SPECIAL PUBLICATION
MONDAY OCTOBER 6, 2025

SPECIAL PUBLICATION
Cyber Security & IT Survey 2025
TOOLS, FIRMS AND FOUNDERS SHAPING DIGITAL SECURITY IN GHANA

Securing a digital future

Cybersecurity as a national and an economic imperative

By Simon ANANI

By Simon ANANI

Contact me at askify77@gmail.com

Hey there, and welcome to the very first edition of my cyber blog. In this Op-ed, I invite you to spend a few moments with me exploring a critical topic — cybersecurity.

Beyond serving as a shield against threats, cybersecurity is a powerful business enabler that fosters trust and drives innovation. More importantly, it is also a silent force behind nation-building, safeguarding the digital foundations of our economy and society.

From my background in military operations, I can say this with certainty: the next great war between nations will not be fought with boots on the ground, but with keystrokes in cyberspace. And in this battlefield, victory will belong to the most prepared.

Cybersecurity and Economic Resilience

Let us be clear: no economy can thrive without trust. Investors will only bring capital if they know their assets and intellectual property are secure.

Entrepreneurs will only innovate if they are confident their business systems cannot be easily compromised. Citizens will only embrace digital services if they believe their personal data will not end up in the wrong hands.

A single major cyber incident can wipe out years of economic progress. Imagine if a widespread attack disrupted Ghana's mobile money ecosystem — the very lifeline for millions of Ghanaians who use it for daily transactions. Such an event would not only paralyze financial services but could also shake investor confidence and undermine our position as a digital leader in the region.

This is why cybersecurity should be seen as a strategic investment in nation-building. Countries that prioritize it create an environment of trust, which attracts investors, empowers businesses, and enables innovation. Singapore and Estonia are excellent examples. Both countries transformed themselves into global digital hubs by making cybersecurity the backbone of their digital development. Ghana can learn from these models as we position ourselves in West Africa.

Cybersecurity and Nation Building

When we think of nation building, we often picture roads, bridges, schools, and hospitals — visible symbols of progress that every citizen can touch and feel. Yet in today's digital age, there is another foundation equally important but less visible: cybersecurity. Without it, all the gains we are making as a nation can be undone in seconds.

Ghana stands at the crossroads of opportunity and vulnerability. The government's ambitious Digital Ghana Agenda is transforming how we access public services, do business, and connect with one another.

Mobile money transactions worth billions of cedis flow through our economy every year. E-commerce platforms empower small businesses to reach customers far beyond their neighborhoods. Digital health solutions are streamlining patient care. Education is increasingly moving online. These changes are exciting, but they also expose Ghana to risks that we cannot afford to ignore.

Cyberattacks are no longer abstract threats from distant lands. They are here, and they are growing. Mobile money fraud, phishing scams, ransomware attacks, and data breaches are increasingly common. Each incident erodes trust, destabilizes businesses, and threatens the progress of our digital economy. If cybersecurity is not taken seriously, all the digital infrastructure we are building risks becoming a castle built on sand.

Cybersecurity as a Pillar of National Security

We often think of national security in terms of protecting borders, securing our military, and ensuring law and order. But in the 21st century, borders extend into cyberspace.

A cyberattack on our energy grid could plunge cities into darkness. A coordinated assault on our healthcare systems could delay treatment for patients in critical condition.

A breach of government databases could expose sensitive citizen information. These scenarios may sound extreme, but they are real possibilities in today's interconnected world.

Globally, cyberattacks are now used as tools of geopolitical influence. State-sponsored hackers have disrupted elections, manipulated information, and infiltrated defense systems in several countries. Ghana is not immune. As our digital footprint grows, we become more visible targets for cybercriminals and hostile actors.

That is why Ghana's Cybersecurity Authority is such a critical institution. Its role in coordinating national cyber defense, awareness campaigns, directing and leading policy discussions, and incident response is indispensable. But the government alone cannot shoulder this responsibility. Businesses, civil society, and citizens must collaborate to foster a culture of cyber resilience.

Unlocking Opportunities for the Youth

Cybersecurity is not only about defense — it is also about opportunity. Ghana is blessed with a vibrant, tech-savvy youth population. With the right training and policies, our young people can become the cybersecurity professionals the world desperately needs.

Currently, there is a global shortage of more than 3 million cybersecurity professionals. This gap is an opportunity for Ghana. By investing in cybersecurity education and skills development, we can position our youth to fill this gap, not only safeguarding our nation but also exporting talent to the world.

Imagine a Ghana where cybersecurity is not just a defensive measure but also a thriving industry. Where young entrepreneurs develop cybersecurity solutions for local businesses. Where universities produce world-class experts who are sought after across Africa and beyond. Where cybersecurity careers provide stable and rewarding jobs that keep our brightest minds at home while connecting them to global opportunities.

This vision is possible — but it requires deliberate investment in training, research, and innovation.

A Shared Responsibility

Cybersecurity is a collective effort. It cannot be left solely to government agencies or corporate IT teams. Every stakeholder has a role to play:

- The Government must create and enforce strong regulations, ensure coordination among agencies, and invest in capacity building.
- Businesses must adopt secure systems, train employees in best practices, and take responsibility for protecting customer data.
- Citizens must learn to use digital services responsibly — from avoiding suspicious links to using strong passwords and verifying sources of information.

In short, cybersecurity begins at home, in schools, in offices, and in boardrooms. Each one of us has a responsibility to protect not only ourselves but also the nation's digital future.

The Call to Action

Ghana is building a digital future. However, we cannot build strong roads and then leave them unguarded; nor can we expand digital services without securing the infrastructure that supports them. Cybersecurity is the invisible shield that protects everything else.

So, I ask: if we are serious about nation-building, can we afford to treat cybersecurity as an afterthought? The answer is NO!. We must treat it as a national priority.

Cybersecurity is not a cost — it is an investment. Every cedi spent on strengthening our cyber resilience safeguards our economy, protects our democracy, and secures the future of our children.

The time to act is now. Ghana cannot wait for a major cyber catastrophe before treating cybersecurity with the urgency it deserves. We must act decisively, collaboratively, and strategically to ensure that the digital foundations we are building today will stand firm tomorrow.

Cybersecurity is not just about computers — it is about the future of Ghana itself. I hope you have got something out of this write-up. Let me know your thoughts and suggestions in shaping the subsequent write-up.

Cracking the code

Addressing weak passwords and Cybersecurity Risks In Ghana

By Bismark Junior APPIAH

Bismark Junior APPIAH

Cybersecurity and Forensics, University of Gujarat, Ahmedabad, India

Executive Summary

Passwords remain one of the most vulnerable entry points in Ghana's digital infrastructure. Weak or reused credentials are a leading cause of cyber breaches, yet password security is often neglected. This article explores the threat landscape, how hackers exploit password patterns, real risks faced in Ghana, and what firms can do to build stronger defences against threat actors.

> Despite evolving password policies, weak password habits persist, many users still rely on the familiar: "123456," "password," birthdates, and a host of other personal information. An analysis of over 27 billion leaked credentials found that a surprisingly high proportion contain predictable patterns, and many surfaces later in real-world attacks (Xie et al., 2025).

The Weak Password Culture

Despite evolving password policies, weak password habits persist, many users still rely on the familiar: "123456," "password," birthdates, and a host of other personal information.

An analysis of over 27 billion leaked credentials found that a surprisingly high proportion contain predictable patterns, and many surfaces later in real-world attacks (Xie et al., 2025).

Academic research also supports this, for instance, a study of 61.5 million passwords across 107 online services found that 38% of users reuse exactly the same passwords across multiple sites, and another 20% adopt minor modifications to a base password.

For example, a person might use the exact password Summer2025# for their email, banking, and shopping accounts; or they might slightly modify a base password, Summer2024# for email, Summer2025#Bank for banking, and Summer2025#Shop for shopping, making it easy for an attacker to guess once the base password is exposed.

The authors showed that many of these "modified" passwords can be cracked within just 10 guesses. (Wang et al., 2018).

Meanwhile, another study found that while people are starting to make their passwords longer and a bit more complex, they still tend to fall into predictable habits, like using dictionary words, sticking to just letters or numbers, or adding something personal such as a name or a date. (Furnell et al., 2018). These patterns are very much predictable, and that's precisely what attackers rely on.

How Hackers Typically Predict and Crack Passwords

Password cracking techniques have advanced significantly with time, expanding from simple guesses to sophisticated, resource-intensive methods; attackers choose techniques based on the tools and compute they have, how much time they can spend, and the target's defences. Core methods include dictionary and brute force attacks, credential stuffing, social engineering, and exploitation of leaked credentials (Bonneau & Preibusch, 2010).

In Dictionary attacks, attackers start with commonly used words, names, and patterns. They also use tools that iterate through combinations, especially when passwords are weak. Credential stuffing is possible because many users reuse passwords, when one system is breached, attackers test those same credentials across multiple platforms. If an account matches, they gain access instantly.

However, the most used and common type of cyber-attack relies not only on computer tools but also on human psychology, in social engineering attacks, threat actors gather social media data, birthdays, loved ones' names, favourite sports teams, or cultural references mostly through Open-source Intelligence (OSINT).

Then they combine that with observed weaknesses to guess business credentials more effectively. Social engineering is a targeted attack that seeks to trick the user to release sensitive information which includes passwords and login information willingly and/or unknowingly.

It's worth noting that, hackers don't always need to brute force everything. They just need to exploit human predictability and reuse.

Ghana in Focus: The Local Context & Risks of Weak Passwords

Ghana's digital adoption has surged, but so has cybercrime. A 2025 report from IMANI Ghana noted that reported cybercrime incidents rose from 1,317 in early 2024 to over 2,008 in 2025 (IMANI, 2025). According to the Cyber Security Authority (CSA), Ghana suffered losses of GH¢14.94 million in the first half of 2025 alone, marking a 17% increase compared to the same period in 2024.

A campaign run by CISAB: Vigilance First found that 60% of participants reused passwords and clicked malicious attachments or links, while only 42% adopted multi-factor authentication after training (Global Cyber Alliance, 2024). In 2019, passwords and usernames of 18 institutions were stolen and sold (GhanaWeb, 2019).

The consequence? A single weak password has been enough to ruin entire businesses. A recent real case: a 158-year-old UK company collapsed when hackers exploited one weak credential to launch a ransomware attack (BBC report). In Ghana too, weak credentials open doors to fraud, data exfiltration, ransomware, and reputational damage.

Business Consequences: What's at Stake

For businesses in Ghana, weak passwords don't just mean inconvenience, they invite significant losses. Financial loss and recovery costs include incident remediation, regulatory fines, and lost business.

Reputational damage arises when a breach undermines client trust, especially since clients entrust businesses with sensitive data. Regulatory and legal risks are substantial, as Ghana's Data Protection Act, 2012 (Act 843) and laws on electronic transactions impose penalties for negligent security. Small and medium enterprises (SMEs) are especially at risk because they often don't have dedicated cyber security teams, making them easier targets for cybercriminals.

Best Practices: How to Prevent Weak Passwords in Your Organization

A practical first step for Ghanaian businesses is developing a strong password policy, one that requires at least 12 characters with a mix of letters, numbers, symbols and spaces, while avoiding dictionary words, names, or repeated patterns. Passwords should change only when there's a suspected breach, as fixed schedules often lead to weaker replacements.

Implementing multi-factor authentication (MFA) adds another critical layer of protection. Even if passwords are compromised, MFA can block unauthorized access. Campaigns such as CISAB's Vigilance First in Ghana have shown encouraging uptake when training and awareness programs are offered.

The use of password managers should also be encouraged, enabling users to generate and securely store unique, complex passwords without the trouble of having to memorize complex passwords for every account. Very secure suggestions include, 1Password, Keeper and NordPass.

Regular credential audits and leak monitoring are important. Businesses should check whether user credentials have appeared in public breaches using services such as Have I Been Pwned, and conduct internal audits to detect weak or reused passwords before they are exploited.

Building a culture of security awareness and education is equally important. Staff should be trained on phishing and social engineering attacks and how to notice potential threats.

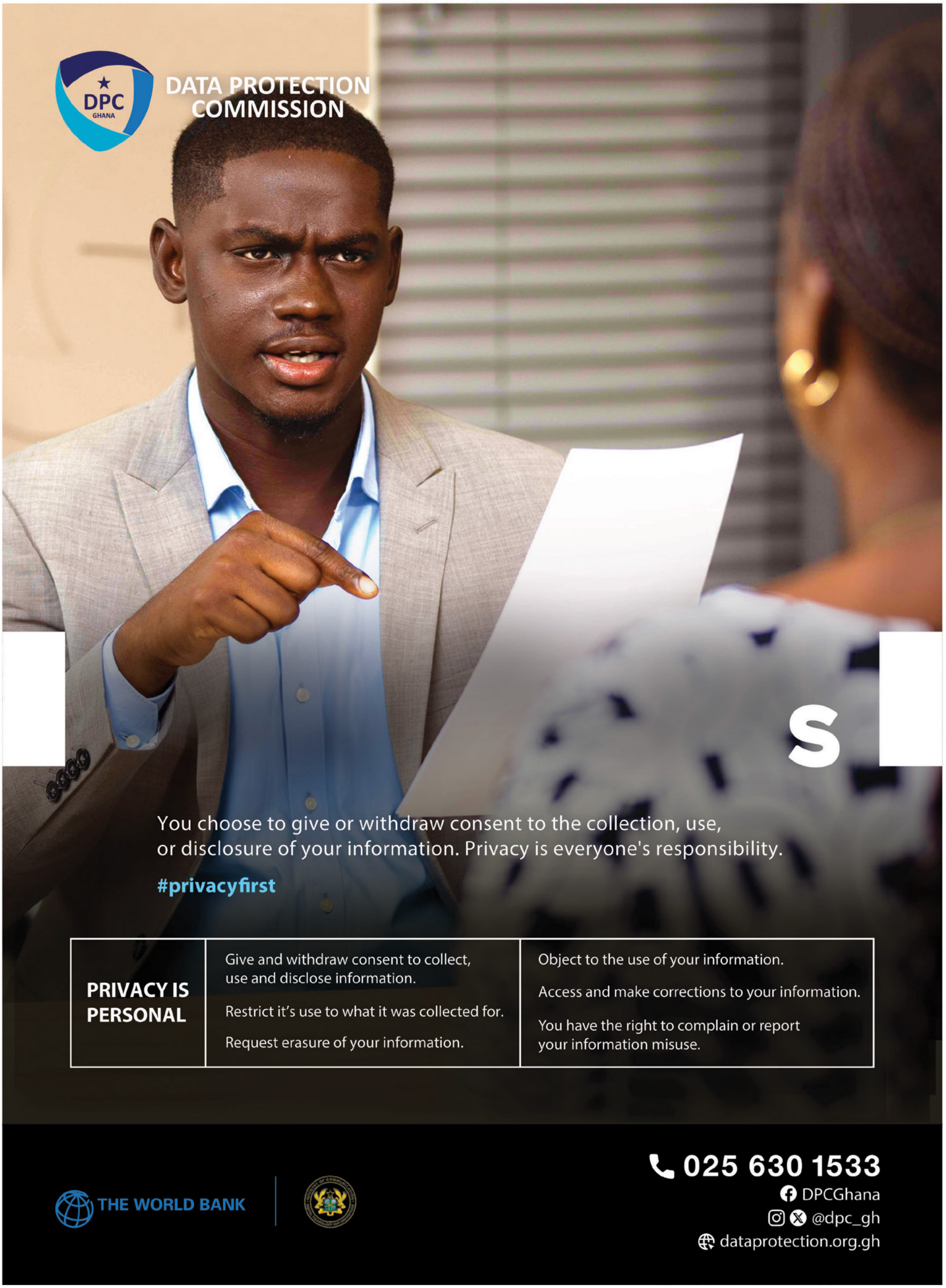
Finally, adopting segmentation and least privilege principles limits how far an attack can spread. The principle of least privilege means giving users, applications, and systems only the access needed to perform their tasks.

Conclusion

The persistence of weak passwords underscores the reality that technology alone cannot secure Ghana's digital future, human habits play an equally critical role. As cybercrime grows more sophisticated and costlier, organizations and individuals must rethink their relationship with passwords and prioritize stronger authentication practices.

By combining robust policies, tools such as MFA and password managers, and continuous security awareness, Ghana can significantly reduce the risks posed by weak credentials.

Ultimately, cybersecurity is not only a technical responsibility but also a cultural shift, where vigilance and accountability become part of everyday digital life.


DPC GHANA
DATA PROTECTION COMMISSION
You choose to give or withdraw consent to the collection, use, or disclosure of your information. Privacy is everyone's responsibility.
#privacyfirst
PRIVACY IS PERSONAL
Give and withdraw consent to collect, use and disclose information.
Restrict it's use to what it was collected for.
Request erasure of your information.
Object to the use of your information.
Access and make corrections to your information.
You have the right to complain or report your information misuse.
THE WORLD BANK
025 630 1533
DPCGhana
@dpc_gh
dataprotection.org.gh

State of ISO certification in Ghana – Innovare Group

ISO Compliance: A silent powerhouse driving Ghana's business competitiveness

In the changing realm of international trade, few instruments are as overlooked yet tremendously impactful as ISO compliance. For businesses in Ghana, whether in fintech, agriculture, energy, logistics, or manufacturing, the subtle influence of ISO standards might be the key difference between average performance and market leadership.

With Ghana establishing itself as the entry point to West Africa and a center for innovation and investment, recognizing and adopting ISO compliance is not only wise; it is increasingly essential.

What Is ISO Compliance and Why Should Businesses in Ghana Be Concerned?

At its essence, ISO compliance involves synchronizing business operations with the norms established by the International Organization for Standardization, a worldwide entity comprising 167 member nations.

ISO develops comprehensive management systems that incorporate global best practices across multiple operational areas such as quality management, IT security, workplace safety, environmental stewardship, and more.

Although not enforceable by law, unless adopted via industry regulations, ISO standards serve as a strong indicator of trust in global commerce. For Ghanaian SMEs aiming to export cocoa products to Europe, fintech companies trying to lure investments from Dubai or London, or oil and gas businesses collaborating with multinationals, ISO compliance can serve as the gateway to new markets and valuable partnerships.

"Achieving ISO compliance goes beyond merely checking off requirements," states C.K Bruce, CEO of Innovare Group, a wholly Ghanaian-owned management consulting and technology services firm in Ghana. "It's about showing the world that your governance structures, processes, and systems align with global standards."

A Fresh Chapter of Compliance for a Renewed Ghana

Ghana's private sector is swiftly diversifying, supported by AfCFTA's potential and government initiatives for domestic manufacturing and digital transformation.

However, with opportunity comes examination. International investors, development finance organizations, and worldwide purchasers are increasingly seeking proof of robust internal frameworks, especially concerning quality control, data security, and ESG outcomes.

Consider ISO 9001, the internationally recognized standard for Quality Management Systems. In a nation where the quality of service can fluctuate significantly across companies, ISO 9001 assists organizations in ensuring uniformity, optimizing processes, and promoting ongoing advancement. From a corn processor in Tamale to a tech company in East Legon, this benchmark enables enterprises to assess their performance thoroughly and establish systems that facilitate growth.

Next is ISO 27001, the standard for information security. For Ghana's expanding digital economy, where fintech applications manage billions of cedis in transactions each month, this standard is now a necessity. ISO 27001 safeguards digital assets while also reassuring regulators and clients that a company prioritizes cybersecurity.

In sectors like construction, mining, and manufacturing, ISO 45001 focused on Occupational Health and Safety becomes invaluable. In industries where on-site risks are high, this standard ensures employee welfare is safeguarded while protecting businesses from litigation and operational downtime

Adherence as a Strategic Edge

Importantly, ISO compliance enhances not just internal processes. It also improves a company's public image. In Ghana, where faith in formal institutions is still developing and informal networks frequently prevail, the capability to showcase ISO certification communicates a distinct message: "We're committed, we're organized, and we're prepared for the international arena."

Numerous multinational tenders, projects funded by donors, and substantial private contracts now require ISO certification as a condition. This phenomenon is not confined to Accra. In Tema's free zone areas and the developing industrial parks in Kumasi and Takoradi, ISO-certified firms are exceeding rivals in both local and international markets.

"ISO compliance is becoming more integral to due diligence for investors," Ck Bruce states. "It reduces the risks in the business environment." It indicates that the company has well-defined governance, risk management, and control frameworks.

ISO Compliance in Ghana: An Expanding Initiative

Though the adoption of ISO compliance in Ghana has been relatively slow historically, a significant change is now evident. Innovare Group, providing ISO certification consultancy and implementation assistance, has noted a 60 percent rise in client inquiries during the past year.

Major areas fueling this interest consist of:

Fintech and Banking: Pursuing ISO 27001 to enhance cybersecurity in response to increasing cyber threats.

Agro-processing: Implementing ISO 22000 for food safety and ISO 9001 to access EU and Middle Eastern markets.

Oil, Gas, and Mining: Aiming for ISO 14001 for environmental administration and ISO 45001 to comply with ESG reporting criteria.

Event Management and Tourism: Investigating ISO 20121 for sustainable events as Ghana enhances its MICE provisions.

But Isn't It Costly?

A prevalent misconception within the Ghanaian business sector is that ISO compliance is excessively costly or appropriate solely for large companies. Innovare Group debunks this misconception by providing phased implementation models designed for SMEs.

CK states, "ISO compliance represents an investment rather than an expense." "It enhances efficiency, minimizes waste, and decreases operational risks." "When the moment arrives to compete for that major contract, your ISO certification might be your most significant distinguishing factor."

Ghana's Standards Authority, along with private sector development partners such as GIZ and UNIDO, has been investigating co-financing options and training initiatives to enhance the accessibility of ISO certification for SMEs

What is Required to Achieve ISO Compliance?

Achieving ISO compliance does not happen instantaneously. It necessitates dedication, commitment, documentation, record-keeping, internal assessments, and regular evaluations. Companies need to create or adjust systems based on the criteria of the selected standard. When prepared, a third-party auditor performs an official certification audit.

The path to compliance encompasses:

Gap Analysis – Evaluating current systems in relation to ISO standards.

Documentation – Creating process maps, guidelines, and operational handbooks.

Training – Making certain that employees grasp and implement the updated standards.

Internal Audits – Performing practice audits prior to certification.

Certification Audit – Performed by an authorized organization like SGS, Bureau Veritas, or DNV

After obtaining certification, companies must uphold compliance via yearly surveillance audits and ongoing enhancement initiatives.

ISO Compliance and the Future of ESG in Ghana

With global capital progressively adhering to ESG metrics, Ghanaian businesses must not overlook standards such as ISO 14001 for environmental management and ISO 26000 for social responsibility.

As Ghana's 2025 Green Economy Strategy progresses and extractive industries face greater demands to improve their environmental impacts, ISO standards offer a distinct, globally acknowledged guideline.

In this regard, ISO compliance is not merely focused on improved business. It's focused on creating a more sustainable and fair Ghana

Conclusion: The Moment Is Here

For Ghanaian businesses looking to expand, scale, and export, ISO adherence provides a quiet yet significant advantage. It instills discipline, encourages innovation, safeguards customers, and opens up market access.

The communication from Innovare Group is straightforward. Compliance is not a bureaucratic obstacle. It serves as a tactical armament.

In a future influenced by digital evolution, environmental awareness, and international commerce, ISO compliance may represent the most powerful declaration a company can convey regarding its aspirations and authenticity

SPECIAL PUBLICATION

Cyber Security & IT Survey 2025

TOOLS, FIRMS AND FOUNDERS SHAPING DIGITAL SECURITY IN GHANA

Resilience over Defence

Why incident response & cyber drills are non-negotiable in today's threat landscape

By Eric Sowah BADGER

In today's digital economy, one unsettling reality is clear: everybody will be hacked. Yes—everybody will be hacked.

Whether it is a global financial institution, a healthcare provider, or a small business with only a handful of employees, cyber incidents are no longer rare; they are inevitable.

The explosion of ransomware, phishing, and supply chain attacks has shifted the cybersecurity conversation.

The focus is no longer on whether organisations can prevent every attack, but on how well they can respond and recover when—rather than if—an attack occurs. This is why Incident Response (IR) and Cyber Drills (CD) have become cornerstones of modern cybersecurity strategy.

Prevention alone is not enough

For decades, businesses have poured resources into preventive measures such as firewalls, antivirus software, intrusion detection and prevention systems, and monitoring tools. While these defences remain essential, cybercriminals have repeatedly demonstrated that no system is impenetrable.

Even technology giants with world-class security teams have suffered breaches. This underlines the need to shift the conversation towards a strategy where preparedness stands shoulder-to-shoulder with prevention.

Incident response: the digital fire drill

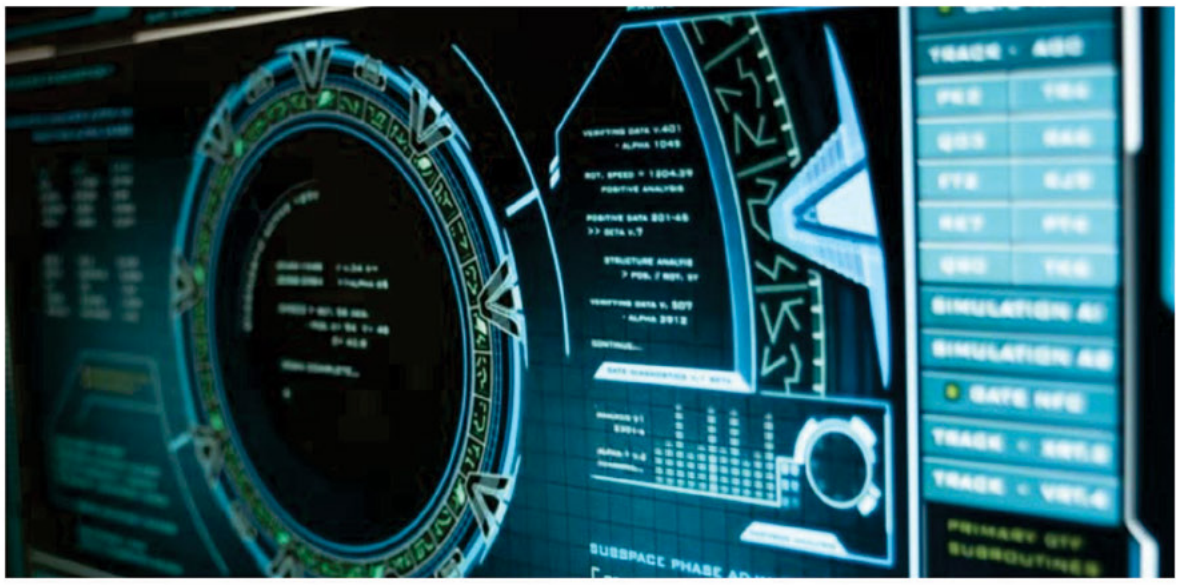
An Incident Response (IR) plan is the digital equivalent of an emergency evacuation strategy. It provides step-by-step actions for containing threats, minimising damage, and ensuring that business operations can continue. Without such a plan, companies often scramble in confusion during an attack, leading to costly mistakes, reputational harm, and sometimes irreversible damage.

Having a plan on paper is only the first step. The next step is to test that plan—and this is where cyber drills come into play.

Much like fire drills, these exercises simulate real-world scenarios such as ransomware outbreaks, phishing campaigns, or denial-of-service attacks. They test not only technology, but also people and processes under real pressure.

Through drills, can:

- expose gaps in defences before criminals exploit them;
- build businesses staff confidence to act decisively in crises;
- strengthen teamwork across IT, executives, and communications teams; and
- demonstrate resilience to regulators, investors, and customers.



Advanced "red team" exercises, in which ethical hackers launch mock attacks to test defences, further strengthen organisational resilience.

Compliance—and beyond

Across industries, regulators are tightening rules on cyber preparedness. Financial institutions, critical infrastructure operators, and healthcare providers are already mandated to conduct incident response planning and testing.

But compliance is only the baseline. Companies must move away from treating drills as box-ticking exercises and instead embrace them as a necessity for resilience.

In today's environment, customers and partners demand assurance. Organisations that can confidently say, "We're ready," not only meet compliance obligations but also build trust and gain a competitive edge.

The reality check

Cyber experts often warn: It's not a matter of if you'll be hacked, but when. This is not fearmongering, but a sober recognition of the current threat landscape. The critical question for leaders is no longer, "Can we prevent every attack?" but rather, "How ready are we to respond when it happens?"

Conclusion: resilience is the new security

In a world where breaches are inevitable, resilience has become the new definition of security. Incident Response and cyber drills are no longer optional—they are survival tools for businesses navigating relentless cyber threats. Preparedness is not just about defence; it is about continuity, trust, and the confidence to thrive even in the face of inevitable attacks.

Cyber capacity building and digital financial inclusion

Continued from page 3

A New Paradigm: Capacity as Collective Intelligence

The concept of "cyber capacity" itself needs an upgrade. It's not just about the number of trained engineers or the existence of a national strategy. It's about collective intelligence — how well a country's entire digital ecosystem can anticipate, prevent, detect, and respond to threats.

That includes frontline fintech agents trained to spot red flags. user experience (UX) designers who know how to nudge users toward safer behavior. Journalists who can decode cyber incidents for the public. Parents who teach their children not to share PINs. True resilience emerges not from a single cybersecurity office but from the informed actions of millions.

This is especially important in an environment where fraud often comes wrapped in familiarity — a message from a known number, a trusted contact, a local-sounding app. Digital literacy, then, becomes the first firewall. Yet it is often the most underfunded, least prioritized aspect of cyber capacity programs.

Strategic Recommendations: Building Trust by Design

To move forward, Ghana and other African nations need to reframe cyber capacity building as an economic imperative, not just a technical one. Financial inclusion is only as strong as the trust that underpins it. That means:

- Integrating cybersecurity education into fintech accelerator programs and university curriculums.
- Offering tax incentives for startups that meet cybersecurity thresholds.
- Embedding user protection features directly into fintech platforms — from transaction alerts to fraud reporting buttons.
- Launching public awareness campaigns in local languages that explain not just what threats exist, but how to act when they occur.

It also means creating feedback loops. Regulators should regularly consult fintech operators on compliance burdens. Users should have clear channels to report suspicious activity. Civil society should have seats at the policy table.

Conclusion: Secure Inclusion or Strategic Regression?

The stakes are clear. Africa's digital economy is too important — and too fragile — to be built on shaky security foundations. As fintech drives financial inclusion, it must do so in a way that builds, but not erode public confidence.

Cyber capacity building is no longer optional; it is foundational. And it must evolve from a donor-driven, government-centric model to one that is user-focused, ecosystem-driven, and deeply embedded in local contexts.

Ghana has the opportunity to lead here — not by mimicking others, but by pioneering a cyber capacity model that matches its digital ambition with grounded, homegrown resilience. If it gets this right, the dividends will be lasting: safer users, stronger startups, and a digital financial system built not just for growth, but for trust.

The Writer is a Partner at AGNOS Legal Company | The founder of Information Security Architects Ltd | Law lecturer at the Ghana Institute of Management and Public Administration (GIMPA) Law School | Member, IIPGH.

For comments, email: desmond.israel@gmail.com

Digital credit licensing

...A turning point for inclusive finance

By Ernestina MENSAH

BoG's new licensing framework seeks to balance innovation, inclusion, and protection in Ghana's fast-growing digital credit space.

Acheampong is a young dealer in Abossey Okai who trades in spare parts. Every week, he takes a small loan through his mobile wallet to restock some of the parts for his stall. The money arrives within minutes—faster than any bank loan—and without collateral. But the interest rate is high, and when sales slow, Acheampong borrows again from another digital lender just to repay the first. Instead of helping him climb out of poverty, easy credit sometimes deepens his struggle.

His experience mirrors both the promise and the peril of digital credit—an industry now too big to ignore. Across the country, thousands rely on mobile loans for survival and opportunity. Students pay fees, farmers buy inputs, and families cover hospital bills—all with quick loans delivered through their phones. This innovation has been revolutionary for financial inclusion. Yet it has also exposed many borrowers to hidden costs, harassment, and cycles of debt.

The Bank of Ghana (BoG) has now stepped in. With its newly released licensing requirements for digital credit service providers, the central bank is charting a new path: one that seeks to harness the benefits of digital credit while safeguarding borrowers and strengthening the financial system.

This is more than regulation. It is a turning point in Ghana's financial evolution.

Dr. Johnson Pandit Asiama, Bank of Ghana Governor

The Megatrends: Why digital credit matters

Mobile money has been Ghana's biggest financial innovation of the past decade. By June 2025, transactions exceeded GH¢1.9 trillion, up from GH¢571 billion in 2019 (BoG data).

Today, there are over 22 million active mobile money accounts, compared to just 18 million traditional bank accounts. For many Ghanaians, mobile wallets have become their first "bank."

Digital credit rides on this backbone. For women, rural farmers, and youth, it lowers barriers that excluded them from formal credit for decades.

MSMEs, which account for about 70% of GDP and over 80% of employment (Ghana Statistical Service), face an annual financing gap that the IFC estimates at $330 billion across Africa. In Ghana, digital loans have plugged critical liquidity gaps, enabling traders to restock, farmers to purchase inputs, and transport operators to keep vehicles running.

The speed of digital credit has also been transformative. Traditional loans can take weeks to process; digital loans are disbursed in minutes. In Kenya, M-Shwari disbursed more than 6 million loans in its first two years. Ghana has followed a similar trajectory, with telco-fintech collaborations ensuring quick access to funds for emergencies such as school fees or hospital bills.

Digital credit is also building new credit histories. Currently, only 16% of Ghanaians are covered by credit bureaus (World Bank, 2023). By using mobile money transactions as a proxy for creditworthiness, digital lenders are creating "reputational collateral" that could eventually unlock larger, cheaper, and longer-term loans.

Competition among banks, telcos, and fintechs has spurred innovation. MTN's QwikLoan disbursed over GH¢1 billion within its first 18 months (BoG/GSMA), while buy-now-pay-later schemes and nano-loans are broadening consumer choices.

In 2024, the digital financial services sector contributed an estimated 4.5% to GDP (World Bank Digital Economy Report), cushioning household consumption and MSME cashflows—critical to Ghana's post-COVID recovery and fiscal reforms.

The Risks: Shadows behind the promise

Yet the very features that make digital credit appealing also make it risky.

One of the most pressing risks is over-indebtedness.

The ease of borrowing without collateral encourages borrowers to take multiple loans, rolling over debt to repay debt. In Kenya, over 2 million people were blacklisted by credit bureaus between 2016 and 2019 for failing to repay small mobile loans, turning a tool of inclusion into an engine of exclusion. Ghana's growing reliance on mobile money loans suggests a similar risk if regulatory guardrails are not enforced.

Opaque pricing and predatory terms are another concern. Some lenders charge effective annual rates above 200%, disguising them as "service fees" or through ultra-short repayment tenors. For low-income households, many of whom lack advanced financial literacy, this lack of transparency creates dependency and financial stress.

Aggressive collections compound the problem. In Nigeria, a 2022 survey revealed 35% of borrowers had experienced intimidation or harassment, including threatening calls and public shaming. Such practices erode trust in financial systems and can cause long-term psychological harm.

There are also data privacy risks. With over 20 million mobile money subscribers, Ghana's digital credit market sits on a goldmine of sensitive information. Lenders often use data on airtime usage, GPS location, and even contact lists. Without safeguards, this data could be exploited, compromising both privacy and consumer confidence.

Poorly designed systems also risk creating financial exclusion through blacklisting. If small defaults automatically lead to long-term bans, millions of Ghanaians could be locked out of the financial system entirely.

At a behavioral level, the instant gratification of mobile loans encourages borrowing for consumption—airtime, entertainment, or non-essentials—rather than investment. This undermines the developmental potential of credit and risks fueling dependency.

Finally, the scale of mobile money means there are macro-financial risks. Ghana's mobile money ecosystem already processes transactions equivalent to over 80% of GDP annually. If defaults surge, fintechs and telcos could face liquidity strains that spill into the banking system. The IMF has repeatedly cautioned against unregulated "shadow banking" in emerging markets, noting how quickly small shocks can cascade across the economy.

The safeguards: BoG's new architecture

BoG's framework directly addresses these risks. Licensed providers must maintain minimum capital adequacy, ensuring they can withstand shocks. Governance rules now require management and boards to meet strict "fit and proper" standards, bringing integrity and professionalism to the sector.

Transparency is also being enforced. Lenders must disclose annualized percentage rates (APRs) and provide clear cost breakdowns, ending the era of hidden charges. Borrower protection is being prioritized with ethical debt collection rules, mandated grievance mechanisms, and compliance with the Data Protection Act (2012, Act 843) and cybersecurity directives.

Quarterly reporting requirements mean BoG will now track defaults, disbursements, and exposures—giving the regulator visibility to spot bubbles early. Crucially, licensing brings digital lenders into Ghana's formal financial architecture, strengthening investor confidence and encouraging partnerships.

Opportunities for banks

Rather than losing ground, banks stand to gain from this framework. Licensed digital lenders provide banks with access to underserved markets—small traders, rural households, and informal workers—segments banks have historically struggled to reach.

By generating standardized repayment data, digital lenders also create pipelines of new clients that banks can graduate into larger facilities. Wholesale partnerships allow banks to provide liquidity lines to fintechs, earning returns without bearing the full cost of retail outreach.

Finally, the framework gives banks confidence to co-develop products with fintechs and telcos. By blending their stability and risk expertise with fintech agility, banks can deliver hybrid savings-loan products, SME working capital solutions, or bundled credit-insurance offerings.

This is not a zero-sum game. It is the foundation of an integrated ecosystem where banks, fintechs, and telcos all contribute to advancing inclusion.

Lessons from Abroad

· Kenya (M-Shwari): 50 million loans disbursed in five years, but defaults and blacklisting forced regulators to step in.

- **Nigeria (FairMoney, Carbon):** More than $300 million disbursed annually, but scrutiny over harassment and data abuse damaged credibility.
- **India (Paytm Lending):** Rapid expansion tied to e-commerce, but central bank intervention highlighted governance gaps.
- **Global:** Nonbank financial institutions now account for nearly 50% of global credit (IMF, 2023), proving the potential of innovation but also its risks when left unchecked.

Ghana is acting early—learning from these lessons to regulate before problems spiral out of control.

Bottom line

The licensing of digital credit providers is a structural milestone in Ghana's financial journey. If implemented well, it will empower families with transparent access to emergency funds, enable businesses to thrive with reliable credit, strengthen the system with safeguards, and create opportunities for banks to innovate and expand.

For borrowers like Acheampong, it could mean moving from cycles of debt to genuine empowerment. For Ghana, it is a chance to prove that financial innovation can align with value-based banking—finance that serves people and purpose, not just profit.

If innovation is the engine of progress, regulation is the steering wheel. Ghana now has both—and must drive toward a future where finance is not only smart, but safe, inclusive, and sustainable.

Ernestina is the Head, Market Risk – Bank of Africa Ghana, Founder, Glimmer of Hope Foundation