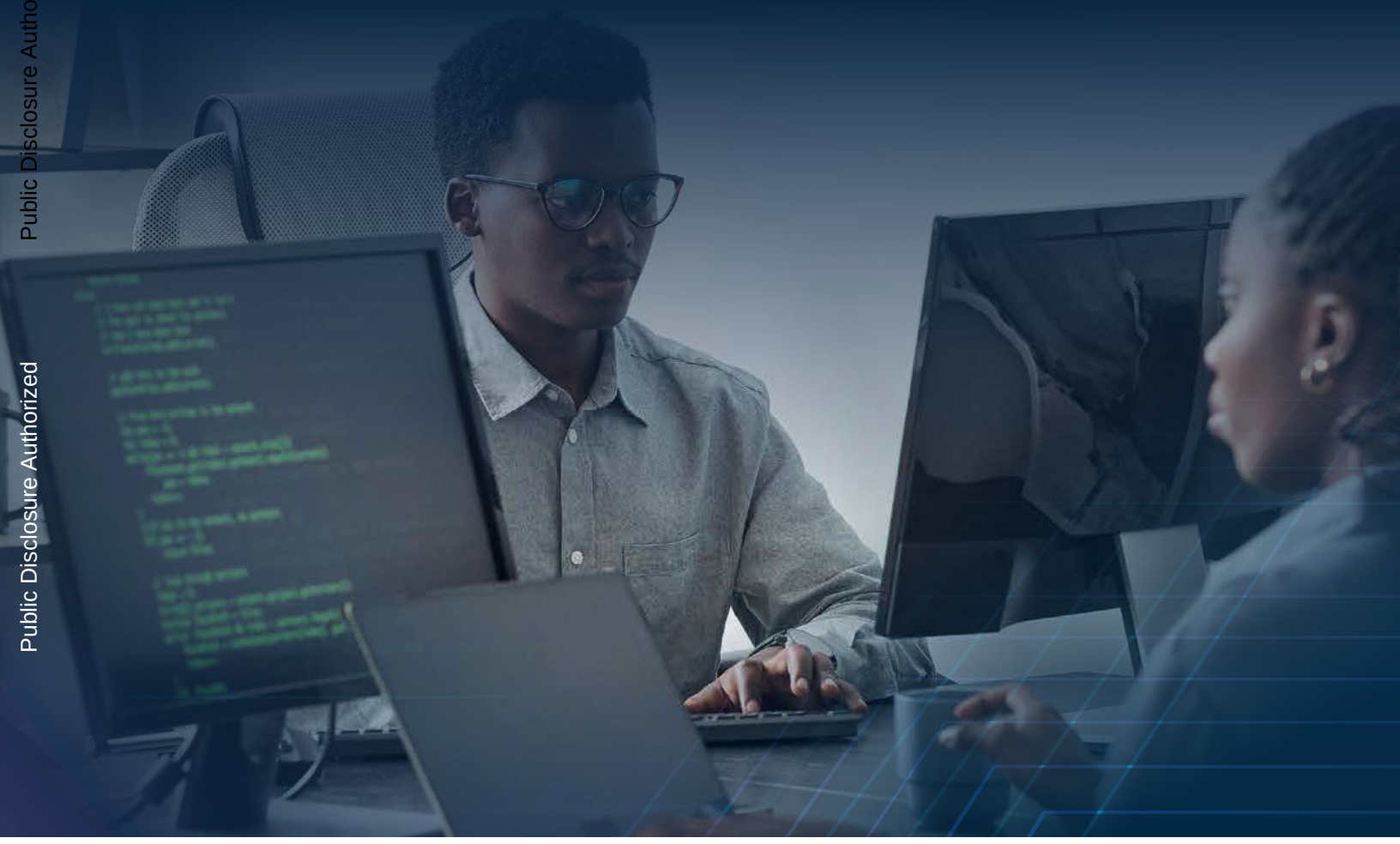
THE WORLD BANK

RESULTS NOTE

GHANA: A CASE STUDY IN STRENGTHENING CYBER RESILIENCE



November 2023

Cybersecurity MULTI-DONOR TRUST FUND

Acknowledgements

This note was written by Robert Collett and Ghislain de Salins and benefited from the inputs and reviews of Anat Lewin, Kamal Siblini, Kaoru Kimura, Lucine MunKyung Park and Casey Torgusson from the World Bank's Digital Development Global Practice. It was developed in close cooperation with staff from Ghana's Cyber Security Authority, in particular Dr. Albert Antwi-Boasiako, Emmanuella Darkwah, Duke Banson, Isaac Socrates Mensah and Eno Brago Attrams.

The development of this note was funded by the World Bank Cybersecurity Multi-Donor Trust Fund.

Table of Contents

GHANA: A CASE STUDY IN STRENGTHENING CYBER RESILIENCE

Executive summary

In the past few years, **Ghana has emerged as a regional leader for cybersecurity**, ranking 1st in Western and Central Africa and 3rd on the African continent overall, according to the International Telecommunications Union (ITU) Global Cybersecurity Index (2021).

This is the result of the significant reforms and investments in cybersecurity undertaken by the Government of Ghana, with support from the World Bank and other development partners.

Ghana reached a milestone in 2017, when the government established the National Cyber Security Secretariat (NCSC), initially comprising three staff. Six years later, in 2023, the NCSC has turned into **a fully-fledged Cyber Security Authority (CSA)** that counts more than 100 staff. The CSA has helped train over 51,000 civil servants, supported the establishment of three sectoral Cybersecurity Incident Response Teams (CIRTs), provides cybersecurity certification paths to individuals and firms, and created a point of contact for reporting cybercrime, which has been used by Ghanaians more than 50,000 times.

As a result, **Ghana has significantly enhanced its cyber resilience**, with an increased capacity to detect, respond to and recover from cybersecurity incidents. The country also enabled its cybersecurity ecosystem to become more autonomous by alleviating its dependency on foreign actors, and even became an international champion for cybersecurity, hosting the **first Global Cyber Capacity Building Conference (GC3B)** in November 2023.

Ghana's results provide important lessons for other developing countries. In hindsight, three key success factors stand out:

- **Strong governmental commitment** to enhancing cybersecurity, notably by senior leadership such as the Head of State and the Ministers. It helped secure funding and align the government's approach to cybersecurity.
- **A whole-of-government model** for cybersecurity governance. While responsibility for cybersecurity was clearly attributed to a single office with deep technical expertise, a broad range of ministries and public agencies were involved in an inclusive manner.
- **Multi-stakeholder engagement and community building.** The government consulted and worked with many external organizations, while emphasizing a whole-of-society approach. Awareness raising activities directly engaged 275,000 adults and 136,000 students in activities and events, with outreach centered around a widely publicized cybersecurity month each October.

Long-term support from trusted international partners also proved instrumental in Ghana's journey towards cyber resilience. Since 2006, three World Bank projects have helped accelerate digital transformation in Ghana, for an aggregate value of $498 million – of which around $20 million were earmarked for cybersecurity.

The case study of Ghana demonstrates that forward-looking investments and policy initiatives based on international best-practices can go a long way in boosting cybersecurity capacity in developing countries.

Introduction

Cybersecurity risks are increasingly considered a key challenge for the development of low- and middle-income countries, with the **annual costs of cybersecurity incidents representing between 6 and 8 percent of GDP**.[i] In this context, Ghana set a course to improve its cyber resilience and, in doing so, became a regional leader for cybersecurity. Ghana's success is demonstrated by its improved ranking in the International Telecommunication Union (ITU)[1] Global Cybersecurity Index (GCI),[ii] as the country rose from 86th place in 2017 to 43rd in 2021 – ranking 1st in Western and Central Africa and 3rd on the African continent.

Ghana's leadership in cybersecurity did not happen overnight. Instead, the country's achievement is the result of strategic decisions and long-term investments made over the past decade. A significant turning point was reached in 2017, as stronger commitment from senior leadership in Ghana's government enabled further investments in and policy initiatives for cyber resilience.

This note discusses the initial development challenges faced by Ghana (section 1), key decisions and milestones in Ghana's journey towards improving its cyber resilience (section 2), the results of such decisions (section 3), and the lessons learned that could be applied by other countries (section 4). The World Bank's contribution to Ghana's cybersecurity journey is discussed in section 5.

> *In just four years, we passed a Cybersecurity Law, set up a Cybersecurity Authority and established a Joint Cybersecurity Committee.*
>
> *This reflects our commitment to achieve cyber resilience.*
>
> *Now that every sector is digitally connected,* ***building the cybersecurity autonomy of the Global South*** *has become absolutely critical.*

Mrs. Ursula Owusu-Ekuful,
Minister for Communications and Digitalisation,
Republic of Ghana

1 ITU's GCI is a composite index measuring countries' commitment to cybersecurity in five areas: technical capacity, legal frameworks, co-operation, capacity development, and organizational measures. The latest GCI was published in 2021. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

1. Development challenge and context

Between 2005 and 2017, Ghana made notable economic and social progress, including on its journey towards digital transformation. During this timeframe, the country's GDP grew by 6.8 percent on average, and the proportion of Ghanaians living below the poverty line declined from 42 percent to 25 percent.[iii] By 2017, 98 percent of urban households and 89 percent of rural households had a mobile phone, and 8 million people[iv] – around 25 percent of its population – were using the Internet.[v] Four additional submarine fibre optic cables were deployed between 2010 and 2013, increasing the available bandwidth in Ghana from 320 gigabytes to 12 terabytes, and cutting the cost of internet connectivity for consumers to a tenth of its earlier price.[vi]

However, Ghana's cybersecurity readiness had not kept pace and could potentially jeopardize its rapid digitalization. The rise in cybercrime scams, locally called *"sakawa"*, reduced trust in digital services and e-commerce. Ghanaians were particularly vulnerable to these scams, as many were new to the Internet and accessed it through mobile devices with limited cybersecurity features. Those conducting *sakawa* in Ghana are typically young men lured into working for criminal gangs by the lavish displays of wealth in the *sakawa* culture. The skills they learnt through online scams could be applied to phishing,[2] the second most prolific form of cybercrime in Ghana. This activity posed a greater risk to Ghana's economy because phishing techniques could be used to gain the information needed to access sensitive systems. Such risks materialized in 2016 when malicious actors hacked the Electoral Commission of Ghana's website, with the aim of spreading disinformation and displaying "fake results."[vii]

In 2017, Ghana ranked only 86th in the ITU's Global Cybersecurity Index. Although Ghana adopted its first national cybersecurity strategy in 2016, achieving cyber resilience had not yet been recognized as a top priority by the government. Consequently, the country had no centralized governance of cybersecurity across government agencies. Various bodies had fragmented and siloed responsibilities, without a unified approach or high-level authority driving the national cybersecurity agenda. The national Cybersecurity Incident Response Team (CIRT), established in 2014, had few staff members and limited capacity to support the many critical infrastructure operators, government bodies, and businesses active in Ghana. Due to such sparse resources, there was no official point of contact for cybersecurity incidents. As a result, few incidents were reported to the national CIRT. Thus, Ghana's government had limited visibility into the scale and nature of the attacks the country was experiencing.

Starting from this relatively low base of cybersecurity readiness, Ghana began to implement substantial reforms in 2017, when the President established a new national vision[viii] for digital development and cybersecurity, supporting the Ghana Beyond Aid agenda.[3] This ambition and direction from the highest level of government started a chain of events that transformed Ghana's cybersecurity capacity.

---

2 Phishing is the fraudulent practice of sending emails or text messages in which malicious actors masquerade as trusted entities (e.g., the government, a bank, or a mobile network operator) in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

3 *Ghana Beyond Aid* was the vision of H.E. President Nana Addo Dankwa Akufo-Addo. It sought to build a Ghana that had achieved key development goals and ultimately transformed itself into an aid-free country. The details of the agenda were set out in the Ghana Beyond Aid Charter and Strategy Document of April 2019. https://osm.gov.gh/assets/downloads/ghana_beyond_aid_charter.pdf

2. Ghana's reforms and investments in cyber resilience

In 2017, the President of Ghana launched a set of reforms and investments for cyber resilience that would significantly enhance the overall cybersecurity capacity of the country. The reform process was overseen by a National Cyber Security Inter-Ministerial Advisory Council (NCSIAC), which was established in 2017 and chaired by the Minister of Communications. It was the first time that the eight ministries most closely involved with cybersecurity had been brought together within a single decision-making body.

The Ministers were supported by technical and policy experts, most notably the newly appointed National Cybersecurity Advisor and a National Cyber Security Technical Working Group (NCSTWG), later renamed the Joint Cybersecurity Committee (JCC). The JCC brought together representatives from across government and external stakeholders, while the National Cybersecurity Advisor provided a single focal point for technical leadership.

A national cybersecurity maturity assessment, finalized in 2018, informed the reforms and subsequent investments. The assessment, based on the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the University of Oxford, was commissioned by the government of Ghana and supported by international partners, such as the World Bank.

At the operational level, Ghana established the National Cyber Security Secretariat (NCSS) to implement the reform process. The NCSS started in 2017 with three staff, and quickly grew to 16 staff by 2018, when it became the **National Cyber Security Centre (NCSC)**. Despite significant improvements in the first two years, some challenges remained. Chief among them was the need for more financial autonomy. Without a stable and dedicated budget for the NCSC, it was difficult to formulate a long-term strategy and hire enough cybersecurity talent. To address this, Ghana passed new legislation in 2020. **The Cybersecurity Act (Act 1038) enabled the NCSC to transition to a Cyber Security Authority (CSA),** with a secured budget and a stronger mandate to regulate cybersecurity activities nationwide.

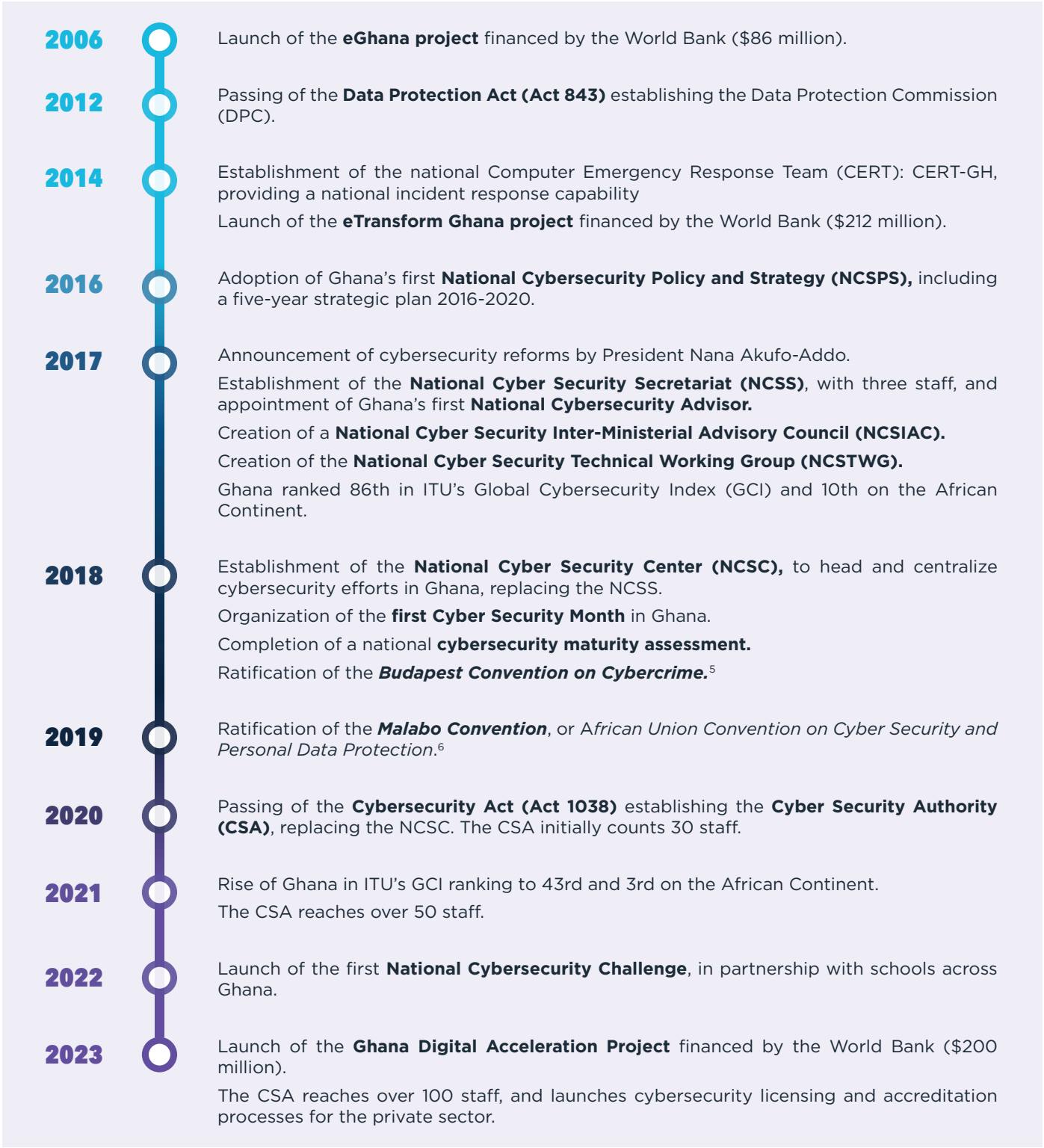
Now a fully-fledged cybersecurity agency, CSA could begin working on tasks that had received little or no resource before the reforms, such as awareness raising, international cooperation, and building close relationships with key industry stakeholders. CSA's vision was to look outwards at ways to help citizens, business, and critical infrastructure operators be better prepared and more resilient. This approach is best illustrated by Ghana's national cybersecurity month, which runs annually in October. By 2021, it had **engaged over 275,000 Ghanaians through workshops and events,** including civil servants, businesses, youth, and children. As part of these outreach activities, the CSA provides trainings to students in high schools, professional associations, regional security councils, staff of government institutions, and officials of the criminal justice system.

Awareness raising helped limit the impact of cybersecurity incidents and also made it more likely that people and businesses would report cybercrime. To facilitate report submission, the government set up **a suite of reporting channels – including an online portal, phone hotline, SMS number, and mobile application**[ix] **– which have been used over 50,000 times**. In parallel, investments in a digital forensics lab and the ratification of both the Budapest and Malabo conventions[4] increased law enforcement's capacity to respond to cybercrime reports.

By 2023, CSA comprised more than 100 staff, **helped train over 51,000 civil servants,** and **launched a cybersecurity certification scheme for individuals and firms.**[x] It is now prioritizing the protection of critical infrastructures, licensing and accrediting cybersecurity service providers, and planning **to roll-out a dozen sectoral CIRTs.** The first three of these – for government systems, finance, and telecoms – are already in place. **Figure 1** details the steps Ghana took to enhance its cyber resilience from 2006 to 2023.

4 As discussed above, the *Budapest Convention on Cybercrime (*ratified by Ghana in 2018) and the *Malabo Convention on Cybersecurity and Personal Data Protection* (ratified by Ghana in 2019) are legal frameworks that facilitate international cooperation when investigating and prosecuting cybercrime through, for example, aligning legislation and definitions of relevant crimes.

Figure 1– Milestones in Ghana's journey towards cyber resilience and of its partnership with the World Bank



5 Since its entry into force in 2004, the Budapest Convention on Cybercrime has been considered the gold standard for legal frameworks aiming at combating cybercrime. Accession to the Convention is therefore a good indicator of a country's cybersecurity capacity when it comes to legal frameworks.

6 The *Malabo Convention on Cybersecurity and Personal Data Protection*, adopted by the African Union in 2014, just recently gathered enough ratifications to enter into force.

3. Results and outcomes

Ghana's cybersecurity reforms and investments resulted in a measurable improvement in its cybersecurity readiness. From 2017 to 2021, the country's ranking in the ITU's Global Cybersecurity Index rose 43 places, from 86th to 43rd. Ghana's significant enhancement in cyber resilience has resulted in an increased capacity to detect, respond to, and recover from cybersecurity incidents. It has also enabled Ghana's cybersecurity ecosystem to become more autonomous by alleviating its dependency on foreign actors, and has even made the country an international champion for cybersecurity – in November 2023, Ghana hosted the first Global Cyber Capacity Building Conference (GC3B).

Enhanced cyber resilience

In 2022, a ransomware attack on the electricity sector in Ghana caused customers to lose power for up to a week. Had this attack occurred before the reforms that began in 2017, the repercussions would have been significantly worse. Instead, the **CSA successfully coordinated an immediate response, mobilizing the government and the private sector in a joint effort.**

This example provides an important lesson about measuring a developing country's progress towards cyber resilience. Although it may sound counter-intuitive, enhanced cybersecurity capacity does not guarantee fewer cyberattacks, but rather provides greater resilience – in other words, an enhanced ability to prepare for and detect incidents, as well as to respond to and recover from them.

The activities carried out by the CSA enhanced the cyber resilience of stakeholders in other critical sectors, including e-government services. For instance, the Ghana.gov portal was launched in 2021 as a way for citizens and businesses to pay their taxes online and access other services, such as passport renewal. Since its launch, Ghana.gov has not suffered a serious interruption or data breach.

Greater autonomy

While Ghana received support from international partners when planning and implementing its cybersecurity reforms, the country's original aim was to **transition away from intensive consultancy support towards self-sufficiency.** This ambition aligned with the Ghana Beyond Aid agenda. Today, Ghana has largely achieved this goal. The CSA is now a fully-fledged autonomous agency with more than 100 local staff. While the CSA can continue to make use of international experts for advice and training, as do most countries, the agency does not depend on these experts to fulfill its mandate.

Spillover international benefits

The results Ghana has achieved at a national level have delivered spillover benefits to other countries, in particular in Africa. In October 2019, Ghana hosted the Economic Community of West African States (ECOWAS) inter-ministerial roundtable, at which ECOWAS Member states asked Ghana to champion cybersecurity in the region.[xi] The World Bank contributed to this regional agenda by sponsoring officials from ECOWAS countries to come to Ghana and witness its cybersecurity approach first-hand.

The decision of key global stakeholders[7] to choose Ghana as the host country for the first-of-its-kind **GC3B** in November 2023 was also a testament to Ghana's leadership in cybersecurity.

---

7 The Global Forum on Cyber Expertise, the World Economic Forum, the World Bank, and the Cyber Peace Institute, amongst others.

4. Lessons learned

In hindsight, three key elements stand out from Ghana's reforms and investments in cyber resilience: strong governmental commitment to cybersecurity; a whole-of-government governance model; and multi-stakeholder engagement and community building. Each element provides lessons learned, which may be used to help other developing countries enhance their cyber resilience.

> *The Cyber Security Authority's **partnerships with stakeholders are vital** for raising awareness and facilitating implementation of our laws and policies.*
>
> *From operators of critical infrastructures to NGOs and academia, stakeholders are included in our governance structure and decision-making process.*
>
> *Multi-stakeholder cooperation has been a key feature of our journey towards achieving a secure and resilient digital Ghana.*
>
> **Dr. Albert Antwi-Boasiako,**
> Director General of the Cyber Security Authority,
> Republic of Ghana

Strong governmental commitment to enhance cybersecurity

High-level governmental commitment to set ambitious targets and deliver tangible results catalyzed Ghana's cybersecurity achievements. This commitment began with senior leadership, namely the Head of State,[8] providing clear direction to the government (through the Ministry of Communications) to prioritize cybersecurity. Critically, this commitment cascaded down from political vision to technical implementation. Senior governmental commitment enabled fast resolution of key issues within the reform agenda. For example, officials had the support they needed to ratify both the Budapest and Malabo Conventions in back-to-back years and finalize the Cybersecurity Act (Act 1038). Commitment from the Head of State is also helpful in encouraging a collaborative approach among ministries and agencies. In any reform process, there will be issues of disagreement within government, but high-level leadership helps reduce their impact and promote problem-solving.

8 This is in line with the OECD Recommendation on Digital Security Risk Management (revised in 2022), which recommends commitment to enhancing cybersecurity "at the highest level of leadership in governments," OECD, 2022, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479

A whole-of-government governance model

Keeping in line with the recommendations from the 2018 CMM national cybersecurity maturity assessment, Ghana established **a whole-of-government governance architecture cascading from the President down to the operational level.** Four features of Ghana's governance model are highlighted below as good practices:

- **Clear attribution of authority and accountability at the core.** Clear responsibility for cybersecurity was attributed to a single office with deep technical expertise, through the Ministry of Communications and Digitalization: the Cyber Security Authority (previously referred to as the NCSS and NCSC).
- **A whole-of-government approach.** Senior governmental leadership recognized that cybersecurity was a transversal topic and that its governance needed to include various parts of the government. At the ministerial and senior technical level, councils and committees brought together ministries and agencies from within and outside government. At the working level, institutions promoted a whole-of-government working culture.
- **A strong connection between strategic leadership and technical implementation.** The National Cybersecurity Inter-Ministerial Council worked together with the National Cybersecurity Technical Working Group. This partnership comprised key government stakeholders involved in technical or practical implementation of policies to combat cybercrime and enhance cybersecurity. This technical group, chaired by the National Cybersecurity Advisor, was tasked with running day-to-day operations. In 2022, this group became the Joint Cyber Security Committee.
- **Inclusive leadership for cybersecurity governance.** Ghana's governance model relies primarily on subject matter expert leadership, while fostering collaboration and trust-based relationships with key stakeholders, such as the private sector and civil society. This inclusive model allows the country to address a wide array of national development goals, transcending narrowly-focused, security-centric priorities.

The inauguration of Ghana's Joint Cybersecurity Committee.

Multi-stakeholder engagement and community building

Perhaps most strikingly, Ghana's approach to **building its cybersecurity capacity relied on multi-stakeholder engagement, as the country recognized that governments cannot achieve cyber resilience on their own.** This collaborative approach has been a defining feature of Ghana's cybersecurity journey. As the President declared in his 23 October 2017 speech, upon launching the reforms, *"[We are adopting] a multi-stakeholder approach as a foundation for the effective implementation of the various cybersecurity activities and programs."*

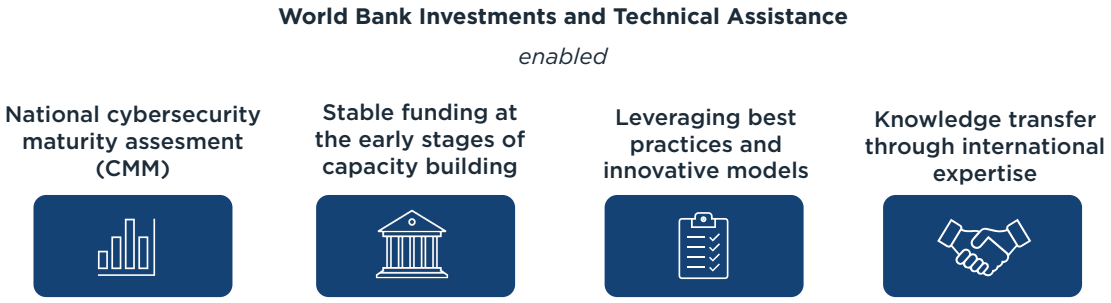
In practice, Ghana's multistakeholder approach is evident through the inclusion of stakeholder representatives in the Joint Cyber Security Committee as well as the CSA board. Stakeholders are given opportunities to contribute to important cybersecurity policy decisions through consultations and an industry forum.

As a result of the multistakeholder approach, **non-government groups play important roles in areas such as policy advocacy, technical training, and awareness raising.** Organizations like the African Center for Cyber Law and Cyber Crime Prevention provide specialized legal expertise and input to policymakers. Groups such as the Africa Cybersecurity and Digital Rights Organisation, the Media Foundation for West Africa, and Child Online Africa have organized events, raised awareness, and directly informed the development of Ghana's cybersecurity strategy.

5. World Bank contribution

To achieve these cybersecurity reforms and investments, Ghana has worked with a range of international partners. In particular, the close partnership between the government of Ghana and the World Bank helped accelerate the country's cybersecurity capacity building and delivered quick results in four key areas (see Figure 2).

Figure 2 – Key areas where World Bank support enabled quick results.



Source: World Bank

Throughout Ghana's reform journey, the World Bank provided support either through trust-fund grants or broader investment projects that primarily focused on accelerating the country's digital transformation (see Box 1). In 2018, funding from various international partners (including the World Bank) supported the national cybersecurity maturity assessment that enabled the government of Ghana to prioritize further policy work. That same year, funding from the eTransform Ghana project enabled the NCSC to build its operational infrastructure (see details below).

Box 1. World Bank support in accelerating digital transformation in Ghana.

The World Bank has supported Ghana in accelerating its digital transformation since 2006 through three large-scale projects worth a total of $498 million.

The **eGhana project** (2006-2014) invested $86 million to generate growth and employment by leveraging ICT and public-private partnerships to develop the local IT industry and by improving the efficiency and transparency of public services through e-government applications. The project also provided financial support for the establishment and operations of the national CIRT.

The **eTransform project** (2014-2023) invested $212 million to improve the efficiency and coverage of government service delivery using ICT. The project included funding for data center security and assistance to the NCSC to build its operational infrastructure, including an incident management platform, a contact center, and a forensics lab. International consultants provided advice on organizational policies and procedures, with the aim of upskilling Ghanian officials to enable them to ultimately deliver services and internal trainings autonomously.

The latest World Bank partnership with Ghana, **the Ghana Digital Acceleration Project** (2023-), will invest another $200 million in accelerating the country's digital transformation through activities such as expanding mobile phone service to 6 million rural Ghanaians and digitizing government services. The project is also supporting the establishment of a sectoral CIRT for the health sector.

Each of these projects secured specific budget allocations for cybersecurity capacity building. Additional activities were supported through various trust-funds managed by the World Bank.

Source: World Bank.

Conclusion

Ghana's journey towards cyber resilience highlights the tremendous progress that can be made when countries prioritize and invest in building their cybersecurity capacity. Through strong governmental leadership, inclusive governance, multi-stakeholder engagement, and leveraging international partnerships, Ghana was able to implement holistic cybersecurity strategies drawing upon international good practices. **With forward-looking investments and policies, developing countries can make rapid strides in increasing technical capability and strengthening cybersecurity readiness.**

As this case study demonstrates, Ghana is now a source of expertise and lessons learned for other developing countries, as well as a respected host of international knowledge sharing events for cybersecurity capacity building. The World Bank will continue to partner with Ghana through the ongoing Ghana Digital Acceleration Project and potentially follow-on programmes.

References

[i] Baldini, G. et al. (2020), https://publications.jrc.ec.europa.eu/repository/handle/JRC121051, and Cybersecurity Ventures (2022), https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[ii] International Telecommunication Union (2021), *Global Cybersecurity Index,* https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

[iii] World Bank (2022), https://pip.worldbank.org/country-profiles/GHA

[iv] Sasu, D.D. (2023), G*hana: total number of internet users 2017 to 2023*, https://www.statista.com/statistics/1171416/number-of-internet-users-ghana/

[v] Ghana Statistical Service (2018), *Poverty trends in Ghana (2005–2017)*,https://www2.statsghana.gov.gh/docfiles/publications/GLSS7/Poverty%20Profile%20Report_2005%20-%202017.pdf, p.37

[vi] Baylon, C. and Antwi-Boasiako, A. (2016) *Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study. Global Commission on Internet Governance*. https://www.cigionline.org/static/documents/documents/GCIG%20no.44_0.pdf, p.2

[vii] BBC News (2016), *'Ghana election commission website hit by cyber attack'*, https://www.bbc.com/news/world-africa-38247987

[viii] Graphic Online News (2017), https://www.graphic.com.gh/news/general-news/ghana-to-have-cyber-security-centre-prez-akufo-addo.html

[ix] Amesimeku (2019), https://3news.com/october-declared-cyber-security-awareness-month-2/

[x] Cyber Security Authority of Ghana (2023), https://www.csa.gov.gh/resources/CSA-ESIT%20Joint%20Press%20Release-27-04-2023.pdf

[xi] Council of Europe (2023), *Octopus Cybercrime Community*, https://www.coe.int/en/web/octopus/-/ghana