



B&P
ASSOCIATES

Lawyers & Consultants

IN THIS ISSUE

- Enhancing Cybersecurity and Eradicating Cyber Attacks - An All-Inclusive Approach
- Spotlight On Accreditation and Licensing Under The Cybersecurity Act 2020
- Business Updates
- Legislative Corner
- WHO's WHO?
- Firm News

Issue No. 30
November, 2022



ENHANCING CYBERSECURITY AND ERADICATING CYBER ATTACKS - AN ALL-INCLUSIVE APPROACH

October is National Cybersecurity Awareness Creation month in Ghana. While technology has made significant global impact, particularly through the use of the internet, it has also exposed organizations and individuals to several risks including attacks through digital interfaces.¹ Cybersecurity has become increasingly pertinent, especially because of the adverse effects that cyber threats pose. In a world where there is an overload of detail to be found on the internet, including sensitive

information and personal data, ensuring that data remains safe is the ultimate aim of cybersecurity. Cybersecurity protects information and data stored electronically, and communication networks from unlawful use, access or interference.²

Danger Posed by Cyber Threats to Individuals

When thinking about cyberattacks, we usually avert our minds to businesses and

corporations and how gravely they are impacted by these attacks. It must however be emphasised that individuals are targets of cyberattacks too, often because they store personal information on their mobile phones and use insecure public networks. Cyber attackers may use an individual's sensitive data to steal information or gain access to their financial accounts, among other potentially damaging actions, which is why cybersecurity is essential to protect private data.³

Let us not forget that organisations are made up of individuals, and so while cyber-attacks have a distinct impact on organisations, they may also affect people affiliated with those organisations. Data breaches can lead individuals to incur undeserving liability when criminals get hold of enough information to steal their identity and carry out fraudulent activities. On a social level, there is a risk of disruption to daily life or a negative perception of technology. Mentally, being a victim of cyber-attacks can be stressful, it can lead to apprehension, fear and or embarrassment if personal, highly sensitive data is leaked.⁴

Danger Posed by Cyber Threats to Companies or Business Entities

The internet and digital communication have helped deliver huge benefits to corporations, ensuring efficiency and effectiveness. However, malicious actors continue to actively look for new ways to exploit its vulnerabilities. Because systems and devices used by corporate organisations or businesses are interconnected, the risk of intentional or accidental cyber-attacks is very high, especially for Small and Medium

Enterprises (SMEs) that often lack the resources (and awareness) to invest in cybersecurity. However, this does not mean larger companies are immune to cyber-attacks. Ergo, there is a general need for cybersecurity for all types of business entities as a potential attack can cause companies to incur financial and non-financial liabilities for data breaches.

Common Forms of Cyberattacks Faced by Individuals and Companies

Three common cybersecurity incidents individuals and companies face include phishing, ransomware and malware.

Phishing: Phishing attacks occur when an attacker pretends to be a trusted contact, and entices a user to click on a malicious link, download a malicious file, or enable access to sensitive information, account details or credentials. This information could be personal data, passwords, pin codes, email addresses, residential addresses, bank details, medical information or insurance information. Phishing is the most common and most damaging threat faced by businesses. According to research⁵ conducted in 2021,

phishing constitutes about 90% of all data breaches that organisations face and accounts for over \$12 billion in business losses.

Ransomware: This involves hacking into a person or a company's data system, encrypting it and preventing the owner from accessing it. The attackers then extort a ransom amount to be paid by the company or individual before restoring access. However, in most ransomware attacks, the attackers do not restore access to the data even after the ransom is paid and will rather seek to extort more money. In recent times, social media has become fraught with these kinds of attacks. Ransomware can be considered another predominant form of cyber-attack suffered by many businesses every year. For example, patients' medical records could be locked by cyber attackers leaving hospitals with no choice but to pay a ransom since such records are essential to life and health. Hackers may also target small businesses since they are less likely to back up their data with cloud services because they may lack the resources to do so.

Malware: Cyber attackers create malware to gain access to software to steal or destroy data on computers. Malware usually accesses computers through malicious website downloads, spam emails or by connecting to infected machines or devices. Computers become infected with malware from seemingly harmless website downloads, spam emails or through connection to infected devices. Malware can cripple devices, render them slow and lagging and cause them to overheat, and these problems usually require expensive repairs or replacements to fix.

Measures Put in Place by Ghana's Cybersecurity Act and The Role of Relevant Government Agencies.

Ghana's Cybersecurity Act 2020 (Act 1038) provides for the establishment of the Cyber Security Authority (CSA) and a cyber incident reporting and information-sharing platform.⁶ The CSA is also mandated to establish a cybersecurity incident point of contact to facilitate the reporting of cyber incidents by the general public. Alternatively, reports may be made to the National Computer Emergency Response Team through the cybersecurity incident point of contact established by the Act.⁷

Furthermore, the CSA is charged to carry out programmes to promote public awareness and education on matters relating to cybersecurity.⁸

Although individuals and business owners must protect themselves against cyberattacks, there are various government agencies which also have a role to play in the promotion of cybersecurity in Ghana. Their obligations arise from several legislations including Act 1038, which authorised the creation of the CSA and the Joint Cybersecurity Committee (JCC).

The CSA is the main agency responsible for promoting cybersecurity and curbing all threats to Ghana's cybersecurity space. It is empowered by Act 1038 to regulate cybersecurity activities in the country, promote the development of cybersecurity and prevent, manage and respond to cybersecurity threats and cybersecurity incidents among other functions. As part of its duties, the CSA is mandated to establish and maintain an electronic Cybersecurity Risk Register for the country. This Register contains the personal data of the owners of Critical Information Infrastructure (CIIs), details of identified and potential risks, and the potential level of impact of these

identified risks.⁹ The CSA also has a duty to develop or implement technology solutions to mitigate existing and emerging cyber security threats and vulnerabilities to ensure the cybersecurity of the country and to monitor cybersecurity threats within and outside the country.

Besides the CSA, the National Communications Authority (NCA) has also agreed to collaborate with the CSA to build the capacity of staff of both institutions to ensure that the personnel have fundamental knowledge and appreciation of cyber security. The National Information Technology Agency (NITA) also intends to collaborate with the CSA to develop a sectoral directive for the protection of CIIs in the government sector. They will also collaborate in the area of capacity building and knowledge transfer through personnel exchanges.

Again, the Ghana Association of Banks (GAB) plans to liaise with the Bank of Ghana (BoG) to review the existing financial sector Cybersecurity Directive based on the current cyber risk profile of the financial sector and to align with Act 1038. There is also the JCC which is a high-level committee made up of heads of various stakeholder

security institutions, that is, the Judiciary, the NCA, the Financial Intelligence Centre, BoG, NITA, the Ghana Domain Name Registry and the Attorney General's Department. It collaborates with the CSA, the sectors and institutions it represents to implement relevant cybersecurity measures.

The Need for a Collaborative Approach to Fight Cyberattacks and Challenges

Cybersecurity threats and cyberattacks are only growing in scope and intensity with the increased adoption and use of the internet and technology. Cyber criminals are becoming more sophisticated, changing what they target, how they affect organizations and their methods of attack for different security systems.

Individuals, companies and institutions have a role to play in supporting the government to fight cyberattacks in Ghana. The private sector, churches, schools, Civil Society Organizations (CSOs), and various governmental agencies must come on board to help create awareness by providing education on cybersecurity in order to increase our cyber hygiene levels.

Virtual workspaces, online marketplaces, e-transactions and e-governance have become the norm and an integral part of our day-to-day activities. While this presents opportunities to revamp economies and streamline public service delivery, it may also heighten exposure to cybercrime.

Considering the rate at which the country is experiencing cyberattacks in recent times, the government must adopt different innovative measures in ensuring that these threats and attacks are well managed and, most importantly, prevented from reoccurring.

Again, cybersecurity challenges and threats are borderless and as such, countries need to cooperate and embrace collaborative efforts on cybersecurity. Governments, national and international institutions have critical roles to play in the implementation of innovative projects and policies that are geared towards solving the cybersecurity challenges in the African continent and the world at large. Amidst all the cybersecurity threats and attacks that have occurred on the continent, very few countries in Africa have developed national policies or strategies on cybersecurity and its

associated challenges. To curb the cybersecurity threats and challenges that are being faced on the continent, there must be a great commitment by nations with respect to cybersecurity-related issues. These collaborative efforts may be in the form of setting up bilateral and multilateral organisations that are mandated to ensure that measures are put in place to solve cybersecurity challenges.

Just as these cyber attackers are constantly working together, sharing tools and techniques for penetrating security systems, we must also adopt a collaborative approach to work together to counter their efforts. There is so much we can achieve for our cybersecurity ecosystem if we collaborate.

State of Cybersecurity in the United States 2022, https://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf (last accessed 14/10/2022).

Overview of Cybersecurity in the United States 2022, <https://uk.practicallaw.thomsonreuters.com/9-617-7682> (last accessed 14/10/2022).

7 Types of Cybersecurity Threats, <https://online.degrees.und.edu/> (last accessed 14/10/2022).

Researcher identifies negative impacts of cyberattacks, <https://www.ox.ac.uk/news/2018-10-29-researcher-identify-negative-impacts-cyber-attacks> (last accessed 14/10/2022).

5 Middle Eastern Phishing Statistics Updated 2022, <https://www.tessian.com/blog/phishing-statistics-2020/> (last accessed 18/10/2022).

6. Cybersecurity Act, 2020 (Act 1038), Section 47.

7. Ibid, Section 48.

8. Ibid, Section 60.

9. Ibid, Section 85.



SPOTLIGHT ON ACCREDITATION AND LICENSING UNDER THE CYBERSECURITY ACT 2020

Under the laws of Ghana, a private business, firm or individual shall not offer cybersecurity services unless the entity or the individual is licensed or accredited by the Cyber Security Authority (CSA).¹⁰ Application for a cybersecurity licence is done by submitting an application accompanied by supporting documentation and paying the prescribed fee determined by the CSA.¹¹ Where the CSA is satisfied that the applicant meets the requirements for the grant of a licence, and the grant of this licence is not against the public interest, the CSA may grant the licence to the applicant.¹²

A licensed cybersecurity service provider who uses a licence for a purpose besides

that for which the licence was granted is liable to pay an administrative penalty to the CSA.¹³

A cybersecurity licence shall not be transferred to another person, and anyone who transfers a licence commits an offence and is liable on summary conviction, to a fine of not less than sixty thousand Ghana Cedis (GHS60,000) and not more than one hundred thousand Ghana Cedis (GHS100,000) or a term of imprisonment of not less than six months and not more than two years, or to both.¹⁴

A licence granted under Cyber Security Act, 2020 (Act 1038) is valid for two years from the date the licence is granted.

Renewal of a cybersecurity licence must be done at least one month before the licence expires.¹⁵

10. Ibid, Section 49.

11. Ibid, Section 50.

12. Ibid, Section 51.

13. Ibid.

14. Cyber Security Act, 2020 (Act 1038), Section 52.

15. Ibid, Section 53.

formalise the partnership aimed at deepening collaboration with the Diaspora Investment Desk of GIPC and engaging the diaspora to invest in equities to help grow the country's economy.

Tier IV Data Centre Opened In Ghana

Ghana's first Tier IV Data Centre known as the Onix Data Centre has been opened in Accra. It is a US\$48 million investment which adds to Ghana's existing data centre, which will serve the country and sub-region. The establishment of the data centre will offer businesses more alternatives for sensitive data storage. As a Tier IV enterprise-class facility, which is the highest level for a data centre, Onix is set to offer reliable and uninterrupted service with an annual expected uptime of 99.995%. To enhance the security of data, the Data Centre has 2.5 times the amount of required backup, when maintenance or planned or unplanned disruptions occur.

Bank Of Ghana (BoG) Regulatory Sandbox

The Bank of Ghana has established a regulatory and innovation sandbox to regulate the financial industry, to ensure a



BUSINESS UPDATES

Boost In Legal Aid Funding

The Government of Ghana has supported the Legal Aid Fund and the Law Reform Fund with a contribution of GHS 2.2 million aimed at promoting the rule of law in the country. The Legal Aid Fund will strengthen the financial capacity of the Legal Aid Commission (LAC) to discharge its duties effectively, and the Law Reform Fund, which will help the Law Reform Commission (LRC) undertake development projects and regular law reforms, will each have GHS 1 million seed money. 822).

Ghana Stock Exchange Partners (GSE) with Ghana Investment Promotion Centre (GIPC) to Increase Access to Offshore Capital

The World Investment Report has indicated that FDI inflows into Ghana grew by 39% in 2021; the second highest in the West African sub-region. In furtherance of its objective to transition the local stock market from a frontier to a more robust emerging market, GSE has partnered with the GIPC to improve access to offshore capital. Both parties have executed a Memorandum of Understanding to



LEGISLATIVE UPDATE

As of 19 October 2022, the Legislative numbers are as follows:

2 Legislative Instruments; **1** Constitutional Instrument; **341** Executive Instruments; and **6** Substantive Legislation, which include:

1. The Electronic Transfer Levy Act, 2022 (Act 1075)
2. Students Loans Trust Fund (Amendment) Act, 2022 (Act 1076)
3. Supplementary Appropriation Act, 2022 (Act 1077)
4. Ghana Standards Authority Act, 2022 (Act 1078)
5. Criminal and Other Offences (Procedure) (Amendment) Act, 2022 (Act 1079)
6. Fees and Charges (Miscellaneous Provisions) Act, 2022 (Act 1080)

a more conducive environment for innovation and mitigation of risks. This framework enables small-scale, live testing of innovative financial products, services and business models by eligible financial service providers and start-ups (operating under a special exemption, allowance, or other limited, time-bound exception) in a controlled environment under the supervision of BoG. By this arrangement, innovators are permitted to temporarily test new ideas without being subjected to the full set of regulatory requirements applicable outside the sandbox while addressing users' and the regulator's respective concerns.

Criminal And Other Offences (Procedure) (Amendment) Act, 2022

Parliament has amended the Criminal and Other Offences (Procedure) Act, 1960 (Act 30) to provide for plea bargaining in the administration of criminal justice in Ghana. The amendment makes provisions for plea negotiations in criminal actions in Ghana.

Ghana Housing Authority Bill, 2022

The Ghana Housing Authority Bill, 2022 is soon to be passed by Parliament. The purpose of the Bill is to establish the Ghana Housing Authority which is an institution which would be responsible for the operationalization of public housing policies. The institution will also be responsible for organising public housing developments and shall have regulatory oversight over the activities of real estate developers.

WHO's WHO? ¹⁶



Abena Amoah has been appointed as the new Managing Director of the Council of the Ghana Stock Exchange, effective from November 24, 2022. She joined the Exchange as Deputy Managing Director in 2020. She has been in the capital market industry for more than 24 years. Her experience covers stock market listings and trading, mergers and acquisitions advisory, investment research, asset management, private placement of equity, debt and hybrid instruments, large infrastructure project development, business start-ups and incubation, public education on investment and financial matters, and capital markets development.

Ms Amoah has undertaken academic and leadership studies at the Stanford Graduate School of Business, Harvard Business School and the University of Denver's Daniels College of Business.

Patrick Kwaku Ofori has been appointed as the Chief Executive Officer of the Chamber of Bulk Oil Distributors, effective August 1, 2022. He has over 16 years of executive professional experience spanning Higher Education, Sports and the Oil and Gas industry. He holds a PhD in Sports Psychology from the University of Stirling, Scotland and an MSc in Accounting and Finance from the University of Ghana. He is a Commonwealth Scholar and an International Convention on Science, Education and Medicine in Sports (ICSEMIS) Scholar.

FIRM NEWS

16

Driving The Digitalization Agenda



The Firm was represented by two of its Legal Associates in the Ghana Fintech Breakfast Meeting, which was held on the 25th of October, 2022. This meeting organised by CCI France Ghana and MEST Africa was themed “Corporate start-up partnerships for fintech innovation in Africa.” The Breakfast Meeting was aimed at connecting fintech start-ups and entrepreneurs to corporates within the industry to catalyse corporate start-up partnerships within the industry.

The event consisted of two 40-minute roundtable discussions and a pitch showcase from select fintech companies, which focused on how corporate start-up partnerships contribute to corporate innovation in the fintech sector, and leveraging fintech innovation in traditional financial institutions, respectively.

Strengthening Our FIDIC Affiliations

Abisola Odunayo-Ogunbadejo, a Senior Legal Associate of the Firm acquired FIDIC Certifications in Contracting in Construction and Engineering Projects, Preparing Contracts for Infrastructure Projects, Reviewing Construction Contracts for Commercial and Contractual Risks, New Frontiers of Risk in Delivering Successful Projects for Clients and Profits for Constructors.

Gaining more expertise in this field adds to the already rich human resource of the Firm. The Firm is more equipped to provide solutions to address the pressing needs of clients in the area of Construction.

CONTRIBUTORS

- [1. Bessy Agyeiwaa Crentsil](#)
2. David William Akuoko-Nyantakyi
3. Priscilla Wepia Ametame
4. Nana Adoma Amoah



About B & P ASSOCIATES

B & P ASSOCIATES is ranked as a Legal 500 Europe, Middle East & Africa (EMEA) Leading Law firm. We are a Corporate and Commercial legal practice and consultancy, with an excellent reputation, based in heart of Accra. The Team is highly regarded for its cross-border legal expertise, responsiveness and commitment. We provide business-oriented legal advice across a range of sectors, to both local and international clients. For more information, visit us at www.bpaghana.com to learn more about what we do.

This publication may provide a summary of legal issues but is not intended to give specific legal advice. If you require legal advice, please speak to a qualified lawyer, which may include a qualified member of our legal team at B&P ASSOCIATES.