G GRAPHIC ONLINE

Securing IT systems, processes: Microfinance institutions undergo training in cyber security

Date: May - 10 - 2022 , 16:52
BY: Graphic Business
Category: Business News

The growth and usage of technology products and services have increased in recent years and have thus, impacted the Small & Medium Scale Enterprises (SMEs) sectors of the economy.

This has led to the adoption of smarter digital applications and processes to satisfy consumer needs and preferences. A key industry in these developments is the microfinance industry which continues to support the growing SME base of Ghana’s economy and is, therefore, a high-risk sector in terms of financial fraud and cybercrimes.

That, therefore, needs a careful and sustainable support to secure investments of stakeholders, protect consumer transactions, meet regulatory compliance, and promote digital safety of the clients and stakeholders the industry serves.

The Ghana Microfinance Institutions Network (GHAMFIN) and its project partner CapPlus, in collaboration with e-Crime Bureau took a bold step to organise a practical and industry specific Cyber Security Training for members of microfinance institutions in Accra and Takoradi.

Participating were Information Technology (IT) officers from various microfinance institutions in Accra. The training was coordinated by GHAMFIN with technical delivery by a team of cybersecurity consultants from the e-Crime Bureau, Ghana’s foremost cyber security and digital forensics firm.

Objectives

The key objectives of the training were; to support IT staff of microfinance institutions to create awareness of existing and emerging information security threats and current cybercrime trends/landscape; create awareness of the impact of user behaviour on the IT infrastructure. Others include equipping IT staff with technical skills that border on third-party technology applications and tools; data protection, information security best practices to secure informational assets, among other things.

Sophistication

Despite financial institutions investing heavily in strengthening their cybersecurity defences, the cyber criminals are becoming more sophisticated in their attack methods.

They have a thorough understanding of the inner workings of the banking system and are quick to exploit any possible vulnerabilities to launch an attack.

Some financial institutions in Ghana have been exposed to cyber attacks resulting in fraudulent transfer of funds because of existing vulnerabilities within technologies being deployed as well as negative user behaviour.

Industry research has shown that 95 per cent of cyber attacks occur due to a lack of knowledge and regular awareness of employees, including management and even customers of banking products and services.

The increase in usage of electronic platforms has led to a surge in fraud related to digital/electronic products and services and consequently, an increase in losses originating from products such as E-Money and ATM/Card fraud.

According to the Bank of Ghana Banks and SDI Fraud Report 2020, Cyber/E-mail fraud recorded a loss value of approximately GH¢1.05 million in 2020.

Intelligence and investigations conducted on electronic facilitated crimes by e-Crime Bureau had revealed that the human resource capacity of technicians and IT staff to detect and respond to the threats of cyber attackers were inadequate to deal with the issues.

Outcomes

The IT officers who underwent the training indicated that the sessions were enlightening, especially in relation to emerging trends of attacks and counter measures to employ to defuse such attacks.

Participants commended GHAMFIN and its project partner CapPlus for putting together the training to build the capacity of IT officers which would go a long way to build the cyber resilience of microfinance institutions in the country.

The participants also recommended for the training to be extended to their colleagues and counterparts in other financial institutions and industry.

It is the belief of e-Crime Bureau that the participants would apply the skills they have acquired in assisting their respective organisations to reduce to the barest minimum, the financial, operational and reputational risks/losses often associated with cyber attacks.