Cybersecurity / Resilience Review on Bank's Covid-19 Pandemic Response Plans

Laja Sorunke

May 26, 2020

	Central Bank of Nigeria	
	Advisory Notice	**Date: May 7, 2020**
Attention	Chief Information Security Officers (CISOs)	
Subject	Cybersecurity/ Resilience review on bank's Covid-19 Pandemic Response Plans	
Summary	• The Coronavirus (COVID-19) pandemic has caused widespread concern for the World, the Central Bank of Nigeria (CBN), Deposit Money Banks (banks) and customers. • To ensure the stability of the banking system, the Banking Supervision Department conducted a survey on the COVID-19 pandemic response plan across all banks. • The survey assessed Management's commitment towards ensuring cyber and operational resilience during the pandemic: 1. Availability of essential staff, 2. Critical IT system capable of monitoring, 3. Identifying and responding to cyber-incidents etc.	

	Central Bank of Nigeria	
	Advisory Notice	**Date: May 7, 2020**
Attention	Chief Information Security Officers (CISOs)	
Subject	Cybersecurity/ Resilience review on bank's Covid-19 Pandemic Response Plans	
Result	• The outcome of this exercise revealed that this unprecedented threat has spurred banks to implement some drastic containment measures to deal with its impact. • The pandemic has also increased reliance on digital banking and remote working. • Consequently, there has been a geometric increase in the number of: ✓ Virtual Private Network (VPN) connections, ✓ Phishing attacks, ✓ Insider threats, ✓ Malware, ✓ Malicious internet banking sites.	

	Central Bank of Nigeria	
	Advisory Notice	**Date: May 7, 2020**
Attention	Chief Information Security Officers (CISOs)	
Subject	Cybersecurity/ Resilience review on bank's Covid-19 Pandemic Response Plans	
Required Action	Banks are advised to: 1. Review and minimize the “work-from-home” VPN connections to thwart unforeseen cyber-attacks and other inherent risks. If possible, the split teamwork arrangements should be embraced. 2. Devise a strategy that provides assurance that computers or laptops used to access their infrastructure from home receive latest endpoint protection updates. 3. Document all unusual system changes and exemptions done to ensure operational resilience during the COVID-19 pandemic for reset at post-pandemic period. 4. Devise measures to hunt and shutdown malicious internet banking websites and increase cybersecurity awareness to foil social engineering attacks.	

Thank you for Joining ISSAN Membership

ISSAN
INFORMATION SECURITY
SOCIETY OF AFRICA-NIGERIA