

Cybersecurity Nigeria: A Digital Transformation Imperative



Contents

Executive Summary 04

Situation Overview 07

Cloud Security Solutions Adoption in Nigeria 07

Cloud Adoption in Nigeria 08

Nigeria’s Cybersecurity Landscape 09

Drivers and Benefits of Security Strategies 17

The Impact of COVID-19 on Security Strategies 18

Current IT Security Strategy Maturity 19

Key Challenges and Opportunities 20

Current Approaches to Data Privacy and IT Security in the Supply Chain 22

Essential Guidance 24

Accelerating your Digital Transformation Journey 26

Microsoft Approach to Zero Trust 26

Uncovering the Security Layers of Zero Trust 27

List of Figures

Figure 1: Cloud Services Usage Now and in Two Years’ Time 08

Figure 2: Current Security Solutions Adoption 10

Figure 3: IT Security Priorities 11

Figure 4: Top Security Priorities for the Next 6–18 months 12

Figure 5: Main Steps to Address Priorities 14

Figure 6: Main Steps to Increasing Security 17

Figure 7: Current Commitment to IT Security 18

Figure 8: Security Strategy Maturity 19

Figure 9: Security Challenges in the Past Year 20

Figure 10: Top Security Concerns 21

Figure 11: Current Approaches to Privacy and IT Security in the Supply Chain 22

Figure 12: Current Level of Compliance with Nigeria’s Data Protection Regulation 23

Executive Summary

Nigeria trails first-world nations in its level of digital transformation (DX). However, local efforts to increase the pace of digitalization and ensure regulatory compliance are being ramped up across all industry verticals. Moreover, Nigeria's gross domestic product (GDP) growth outlook for 2022 appears positive. According to a report from the MEA Business Group, Nigerian GDP will expand 4.3% in 2022, a rate higher than the observed GDP growth of 3.4% in 2021. A positive GDP outlook implies greater economic growth and a faster pace of digitalization. But the potential for cyberwarfare and security breaches often increases as digitalization initiatives get underway.

Only 14% of organizations in Nigeria had embarked on DX journeys before the COVID-19 pandemic occurred. Most organizations began and accelerated digital-first approaches in the wake of the virus outbreak. Following the pandemic, nearly one-half of organizations in Nigeria plan to further expand their resiliency initiatives to prepare for future disruptions. CIO priorities — such as maintaining business continuity and optimizing costs — are accelerating DX initiatives in Nigeria, driving investments in software-based innovations, cloud platforms, cybersecurity solutions, and connectivity excellence. The main challenge most Nigerian organizations face include implementing innovation at speed and scale, selecting capable digital innovation partners, balancing digital innovation with daily operations, and addressing innovation-related risks in a complex regulatory compliance environment.¹

Cloud remains one of the main drivers of most DX initiatives, with 85% of organizations in Nigeria already using cloud for IT operations. According to IDC research, most organizations across Nigeria plan to significantly increase their investments in public and private/hybrid clouds by more than 10% over the next 12–18 months.¹ The public cloud services market in Nigeria is expected to reach \$111.90 million in 2022 and to expand at a compound annual growth rate (CAGR) of 24.03% through 2025.² Indeed, numerous organizations indicated that they will spend more on public cloud in 2022 than they did in 2021. The importance of cloud has significantly increased as remote working became the new normal during the pandemic period. An increase in remote workforces spurred cloud adoption as on-premises domain controllers (DCs) became bottlenecks (due to the requirement to support large volumes of remote workers). DCs also increased the latencies of software as a service (SaaS) applications and internet connectivity.

Alongside its flexibility, agility, and resiliency benefits, cloud guarantees business continuity. Cloud also provides a strong foundation for the adoption of next-gen technologies such as artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), big data analytics, the Internet of Things (IoT), and robotics. Some 64% of organizations surveyed in Nigeria referred to these technologies as key factors influencing their cloud adoption considerations.³ These technologies are also being leveraged in security solutions — to strengthen organizations' defensive postures and enhance threat intelligence capabilities.

Around 21% of the organizations surveyed in Nigeria are taking a balanced approach to cloud and on-premises solutions (i.e., they are making equal use of both types of solution). This percentage is expected to reach 41% within the next two years. At the same time, 2% of organizations in Nigeria will use cloud exclusively within the next two years, according to an IDC security trends survey conducted in 2022.

¹IDC META CIO DX Survey, 2022

²IDC Spending Guide, Q2 2021

³IDC META Cloud Survey, 2022

Unfortunately, the rapid pace of cloud adoption and DX has caught the attention of threat actors. Cybercriminals are trying to exploit vulnerabilities in systems and take advantage of security gaps.

In 2020, Nigeria ranked 16th among the countries most affected by cybercrimes, with the U.S. Federal Bureau of Investigation (FBI) receiving 443 complaints relating to Nigerian cybercrimes during the year.⁴ Most of these incidents were phishing or ransomware attacks. In 2021, the Special Fraud Unit of the Nigerian Police Force arrested an individual for allegedly hacking into a Nigerian bank server and stealing NGN 1.87 billion.⁵ According to a recent IDC survey into security trends, almost 61% of organizations in Nigeria have implemented endpoint protection solutions, including anti-malware and anti-ransomware security solutions.

To address cyberthreats, organizations must adopt formal security strategies. According to a recent IDC security survey, only 16% of organizations in Nigeria have implemented a full end-to-end security strategy with shared responsibilities, risk tolerances, classified events, and recovery plans in case of an attack. Another 15% of surveyed organizations have implemented — but not formally tested or reviewed — a security strategy. Organizations in Nigeria still lag in terms of security solution implementations, but that is not their only challenge. In Nigeria, as is the case everywhere, qualified security professionals are in very short supply.

Cybersecurity professionals were already scarce before the pandemic. Due to remote working practices, increased use of IoT, and the evolving threat landscape, demand for security skills further increased during the pandemic. With cybersecurity skills being in very limited supply, their cost is constantly rising.

To avoid security breaches and limit vulnerabilities, ensuring work visibility in increasingly complex IT environments has become essential. Too often, security is either not taken seriously or is ignored when organizations are planning their cloud migration journeys (as the organizations are more focused on migrating critical workloads). Generally, the basic “lift and shift” of on-premises security processes is the key problem. Because organizations usually focus on protecting their data only after their cloud environments are up and running, they become more vulnerable to threats during the migration period. It is thus important for organizations to understand that security must be implemented consistently during cloud migration. Organizations must develop a formal security and governance strategy, applicable from the initial phase of moving to the cloud to the final implementation phase.

The security of hybrid environments cannot be overlooked. As organizations move into hybrid environments — private and public clouds or cloud and on-premises infrastructure — security becomes critical. Failing to consider security during design may prove very costly in the long run. If organizations do not create a holistic security strategy, IT teams may end up doing redundant work, creating duplicate control solutions, incurring higher costs, and — most egregiously — developing reactive approaches to security.

The COVID-19 crisis has made organizations realize the importance of developing a proactive approach to security. According to IDC's Enterprise Security Trends Survey, 2022, 72% of organizations in Nigeria have increased security budgets by 10% or more in the last few years.

This IDC White Paper presents some key findings from the latest IDC research on security trends and examines current approaches to cloud security in Nigeria.

⁴<https://guardian.ng/news/nigeria-ranks-16th-in-fbis-global-worst-affected-by-internet-crimes/>

⁵Nigeria Cyber Security Outlook, 2022, Deloitte

Situation Overview

Only a limited number of organizations (14%) in Nigeria already had a digital-first strategy in place when COVID-19 broke out. However, the pandemic compelled most organizations to ensure business continuity by adopting digital business models and enabling employees to work remotely. In addition, cost optimization and process reengineering became necessary to sustain operational efficiency. Innovation became important to driving business growth, and automation became a key component in strengthening the workforce. These conditions pushed DX initiatives in the country. IT functions came under pressure as organizations rushed to digital processes.

Many organizations redirected and increased their spending to support digital channels for doing business, with their digital enablement encompassing technologies such as enterprise resource planning (ERP), IoT, AI, automation, application transformation, software/platform as a service (SaaS/PaaS), and analytics. Investments in solutions to secure the organization, its resources, and its business processes, as well as to keep up with governance, risk, and compliance (GRC) requirements, were ramped up during the pandemic period.

Organizations in Nigeria have implemented hybrid working models and solutions to enable and optimize remote work and ensure business continuity. Moreover, cloud has become the standard platform for deploying new solutions, with existing solutions also being moved to the cloud. These developments, however, expand the threat landscape and expose organizations to even greater vulnerabilities. Security has thus become an important consideration for CIOs seeking to address the challenges of the COVID-19 crisis, keep abreast of the latest cyberthreats, and develop DX road maps. According to the IDC CIO DX Survey 2022, the main IT investment priorities of organizations in Nigeria over the next two years are improving business process transformation, enhancing security services, and managing costs. IT spending in Nigeria is forecast to reach \$282.18 million in 2022 and expand at a CAGR of 10.3% through 2025.⁶

The Adoption of Cloud Security Solutions in Nigeria

Organizations in Nigeria have become more vulnerable to cyberattacks due to the growing uptake of technology, the rising adoption of cloud solutions, and the expanding base of digital consumers. When implementing cloud services to ensure business continuity, organizations in the country must consequently adopt cloud security solutions as well. According to IDC's Enterprise Security Trends Survey, 2022, which collated the opinions of CEOs, CIOs, and CISOs in Sub-Saharan Africa, many organizations in Nigeria increased their IT security commitments in 2021 due to accelerated DX initiatives, greater cloud adoption levels, increased awareness of security in senior management, new threats, security incidents, and remote working practices.

⁶ IDC Blackbook, 2022, Nigeria



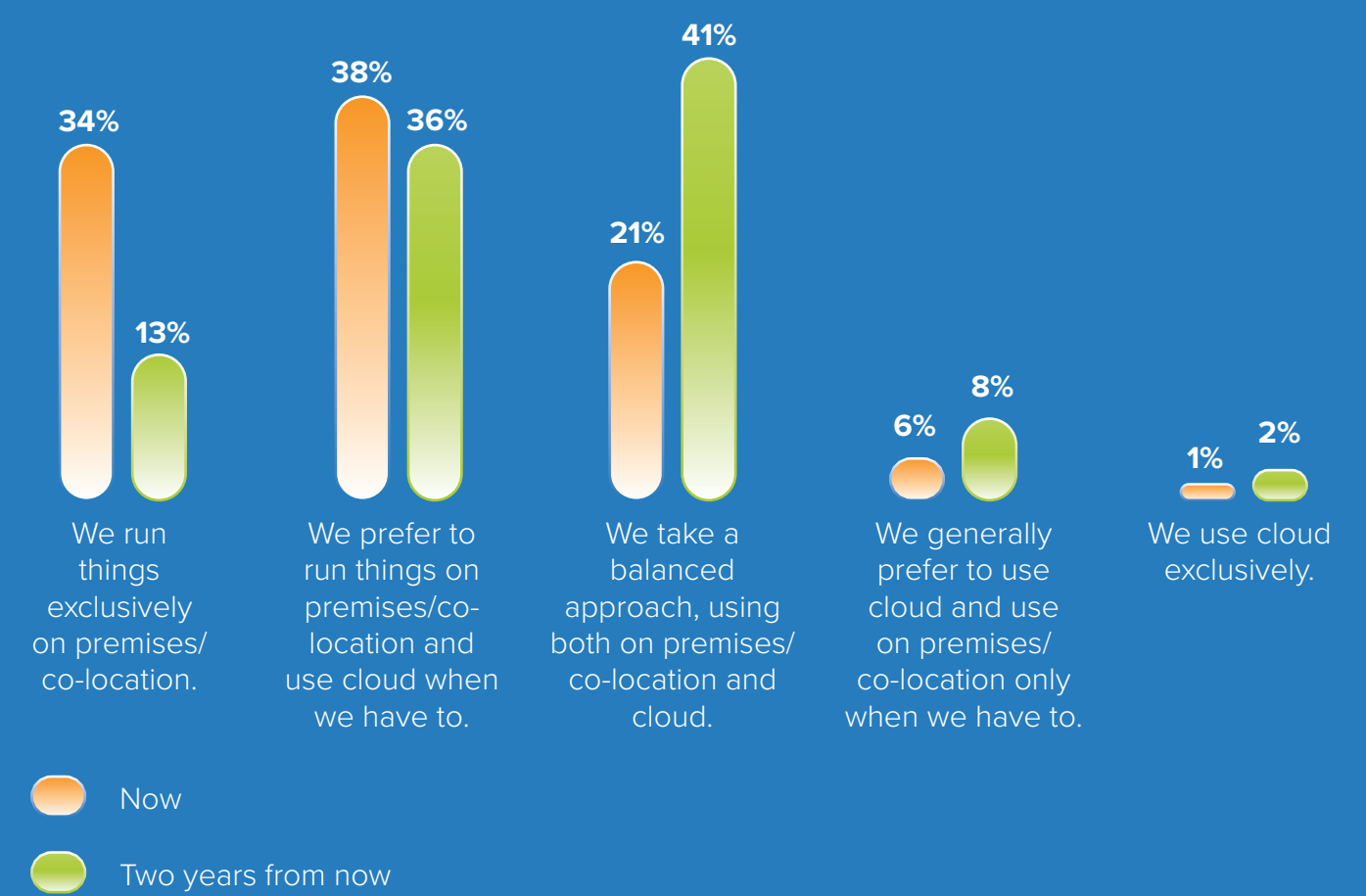
Cloud Adoption in Nigeria

Cloud adoption is still at an early stage in Nigeria, with more than half of organizations currently running operational processes exclusively in on-premises/co-location environments or using cloud platforms only when necessary. Nonetheless, demand for and the uptake of cloud-based solutions in Nigeria will start to increase significantly, particularly as more than half of surveyed organizations in the country currently have or are developing a cloud vision. According to a 2022 IDC cloud survey of CIOs in Nigeria, almost 71% of organizations in the country either fully use cloud to test and develop business applications or are in the initial stages of implementing such cloud capabilities.

Cost optimization will remain among organizations’ top business priorities. According to the IDC META Cloud Survey, 2022, around 63% of enterprises in Nigeria are either slightly or significantly positive about the revenue benefits of cloud, while 77% are slightly or significantly positive about the profitability benefits of cloud. Cloud services such as infrastructure as a service, SaaS, and PaaS enable organizations to ensure business continuity via OPEX models and free up capital for other business-critical investments. Cloud also offers a robust platform through which organizations can leverage emerging technologies, such as AI, ML, IoT, and big data analytics.

Figure 1: Cloud Services Usage Now and in Two Years’ Time

Q: Which of the following statements best represents your company’s current position on using cloud services?
Q: Which of the following statements do you think will best represent your company’s position two years from now?



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

According to IDC survey data, the percentage of organizations in Nigeria that will make simultaneous use of on-premises/co-location environments and cloud platforms will almost double, rising from 21% in 2022 to 41% in 2024. General trends that can be seen across most surveyed organizations in Nigeria include the increased adoption of cloud and the shift away from on-premises solutions. The number of organizations that run applications exclusively in on-premises environments will fall from 34% last year to 13% in 2024. The number of organizations that plan to use cloud exclusively will also double over the same period. These survey results indicate that organizations in Nigeria are clearly aware of the benefits of cloud. The opportunities for providers within the next two years will mostly stem from a range of industries, including finance, transportation/logistics, constructing, healthcare, government, construction, and education.

Nigeria’s Cybersecurity Landscape

Per IDC’s Enterprise Security Trends Survey, 2022, around 85% of organizations in Nigeria understand that securing the cloud is just as important as keeping business operations running. However, security technologies, like all others, require a formal strategy and implementation plan.

In Nigeria, organizations are now deploying security technologies when implementing cloud-based solutions and moving workloads to the cloud. Indeed, the local threat landscape has expanded as organizations have enlarged the geographic distribution of workers and implemented remote working practices, having pursued digitalization since the start of the pandemic. It has thus become critical for organizations to constantly monitor employee connections to the network when they work from home, cafes, hotels, coworking spaces, and other remote locations. Organizations in the country have been reevaluating their risk postures and reimagining their business workflows to adapt to the new normal.

Work-from-home practices, driven by COVID-19-related movement restrictions, have increased the number of remote users that need to access mission-critical data and applications. At the same time, the number of cyberthreats in Nigeria has risen, boosting the importance of securing data and preventing unauthorized access. Endpoints have also moved outside the enterprise core as Nigeria has become more digitalized. Edge deployments and the numbers of end-user devices have also dramatically increased.

In this context, organizations have implemented additional endpoint security solutions, including anti-malware solutions. Some 61% of organizations in Nigeria are implementing endpoint security solutions, while 41% are deploying VPNs and virtual desktop infrastructure to secure remote workers. In addition, 50% of organizations in the country have implemented identity and access management (IAM) solutions. The impact of digitalization has created a need for data protection mechanisms, which 46% of organizations currently have in place.

Figure 2: Current Security Solutions Adoption

Q: What security solution types does your organization currently use?



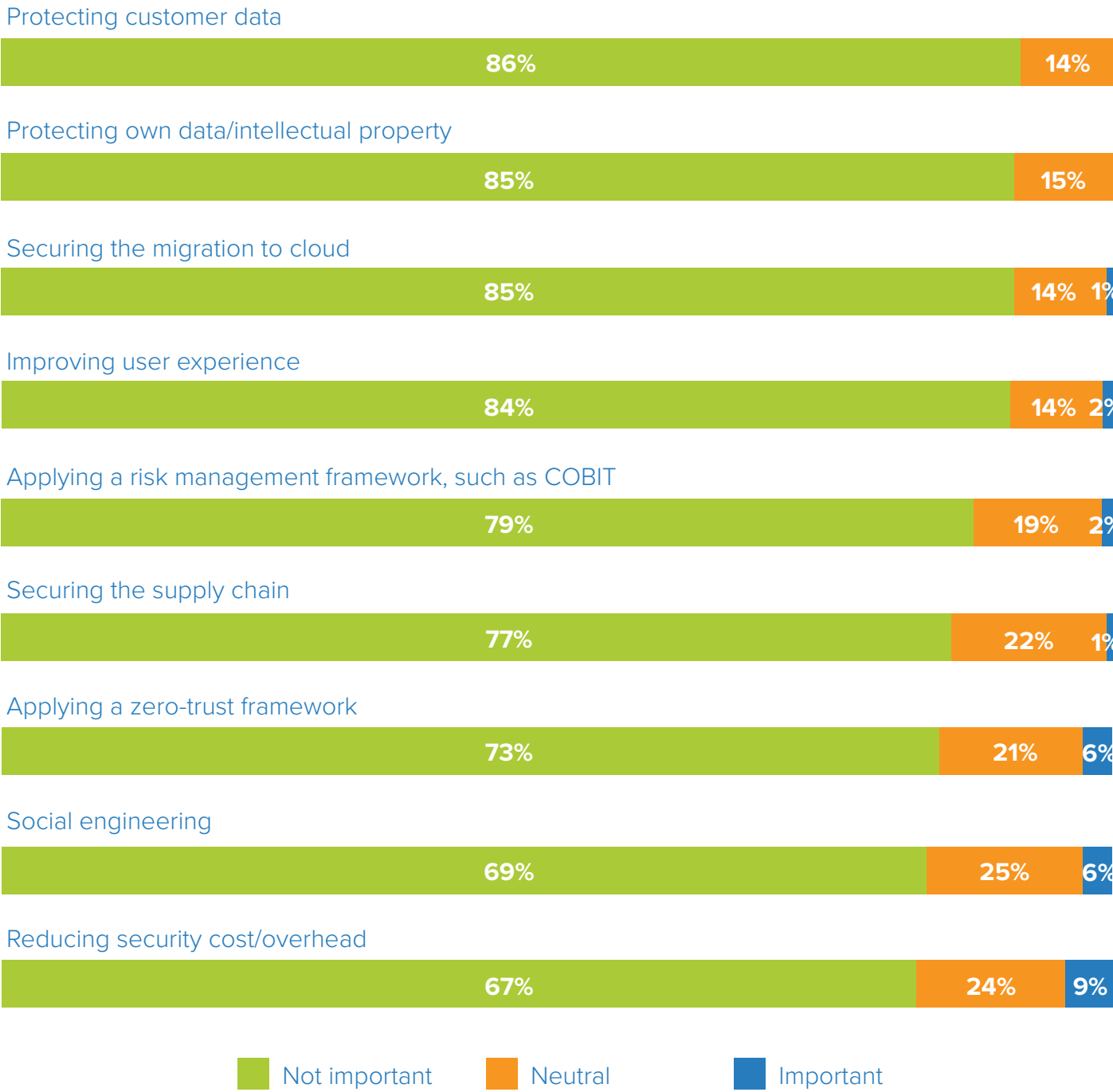
Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

From the perspective of industry verticals in Nigeria, finance organizations are very much in line with the above security solutions usage trends. In government, endpoint protection is the most used solution (highest among all industry verticals), followed by authentication and secure remote access.

The data shows that organizations in Nigeria are becoming proactive in their approaches to security. Around 11% of organizations are adopting security information and event management (SIEM) tools, while 39% are adopting insider risk management applications.

Figure 3: IT Security Priorities

Q: To what extent are each of the following security areas priorities for your business? Please rate each on a 5-point scale on which 1 = not a priority at all and 5 = an important priority.

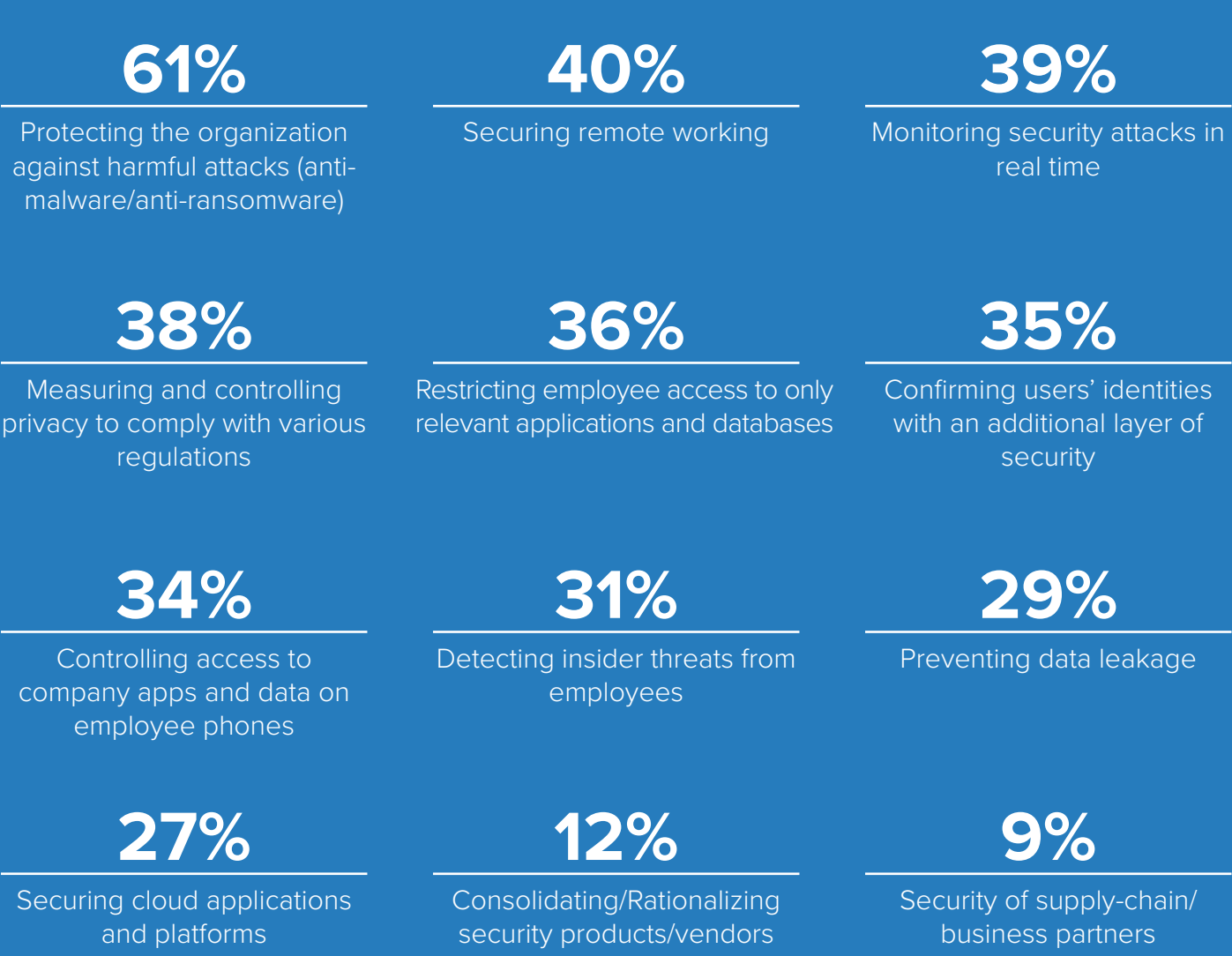


Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

Approximately 86% of organizations in Nigeria surveyed by IDC stated that protecting customer data is an important priority, while 85% indicated that protecting their own data and intellectual property is a key goal. This is primarily due rising cybercrime incidents in Nigeria and the need to prevent reputational and personal damage to organizations and their customers. Some 85% of the surveyed organizations also stated that securing cloud migration is among their top priorities. Ongoing DX initiatives and disruptions to business models arising from the COVID-19 situation are driving interest in zero-trust frameworks in Nigeria, with 73% of respondent organizations rating such frameworks as an important priority.

Figure 4: Top Security Priorities for the Next 6–18 Months

Q: What are your top security priorities for the next 6–18 months?



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria



Organizations’ alignment with IDC’s concept of the “Future Enterprise” can be achieved through transformation to a platform-based, ecosystem-centric, and innovation-driven entity whereby technology underpins all business processes.

Ransomware and malware attacks are the most common threats facing enterprises, and protection against such vectors remains the most common top security priority (as highlighted by 61% of organizations surveyed in IDC’s Enterprise Security Trends Survey, 2022). Cybercriminals are improving their extortion tactics as technology and security solutions evolve and are using advanced technologies such as AI and ML to launch more powerful attacks. Accordingly, organizations must think ahead and adopt advanced security solutions.

Just over 39% of organizations in Nigeria are prioritizing the real-time monitoring of security attacks, while 35% are prioritizing additional layers of security, such as two-factor authentication, to confirm user identities. This prioritization is expected to further increase demand for IAM solutions. A similar percentage of organizations (38%) are prioritizing compliance with the Nigerian Data Protection Regulation (NDPR) in a bid to measure and control data privacy.

Figure 5: Main Steps to Address Priorities

Q: What are the main steps your organization is planning to take to help address your security priorities?



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

Nearly one-half of all surveyed organizations indicated that launching security awareness campaigns will be the first step in addressing their security priorities. Indeed, the security awareness of employees is very important with respect to improving security culture and minimizing the possibility of potential cyberattacks. This awareness also reduces the chances of unauthorized access and data leakage as employees become more cautious about the repercussions of clicking on questionable links. With phishing being a top breach vector, security awareness campaigns (involving phishing simulations) and dark web monitoring should be key focus areas of investors in the Nigerian market.

Around 43% of organizations feel that deploying new technologies will also be an important step in addressing their security priorities. This implies that many Nigerian organizations want to keep up to date with the latest technologies to enhance their existing security environments and address the complexity and quantity of new emerging threats. New investments will mostly be made in endpoint protection platforms, endpoint detection and response, access management, VPNs, secure web gateways, and zero-trust network access. The expansion of security teams was cited as an important step by a fairly small percentage of organizations in Nigeria (19%), while the use of external security consultants and engagements with third-party service providers were identified as key priorities among a greater number of organizations (32% and 31% of organizations in the country, respectively). These results indicate that most organizations in Nigeria have a greater preference for outsourcing security to third-party consultants than expanding their security teams. Regional managed services providers thus have a good opportunity to tap into areas such as gap assessments, vulnerability management, and penetration testing.



Drivers and Benefits of Security Strategies

The COVID-19 pandemic has shown organizations how important it is to be prepared for unprecedented events. The management and mitigation of cybersecurity risks are critical parts of business strategies that can help organizations continue their operations during unprecedented disruptions and even achieve new levels of success. However, such outcomes are only possible with a formal security strategy in place. Traditionally, organizations have independently managed cybersecurity issues for various business functions and departments. But such independent security measures can be unsafe for organizations and can increase the risk of cyberattacks. Developing a wholistic security strategy for the entire organization and its resources — in other words, placing cybersecurity under a single umbrella — is therefore very important.

A holistic security strategy can provide several benefits to the organization. For example, such a strategy helps the organization build a robust security posture for all units and resources, prepare for auditing and compliance requirements, improve operational efficiency, and increase accountability for users and other stakeholders. It also provides a solid framework for effective communication and policy enforcement.

To create a security strategy, organizations must first understand their present capabilities and identify the steps they need to take to boost protection levels. Gaining an understanding of how a strengthened security posture can create business value is an important step. Understanding the connection between business outcomes and a highly secure IT infrastructure can yield various benefits, including greater business continuity, higher customer satisfaction, and enhanced business agility. In fact, 65% of respondent organizations in IDC’s Enterprise Security Trends Survey, 2022, indicated that creating or expanding security strategies was their most important step in boosting security.

Figure 6: Main Steps to Increasing Security

Q: What steps should your organization take to increase its security level?



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

Another 64% of organizations indicated that increasing understanding of security’s value to the business is an important step. Business executives and senior stakeholders would be more likely to approve security budgets and take security more seriously if they better understood the importance of protection. The IT security skills gap is a major challenge — not only in Nigeria but almost everywhere. To address this issue, organizations are encouraging IT employees to increase their technical knowledge in security and even paying for them to obtain certificates. Some 47% of organizations stated that increasing the technical knowledge of their IT teams was an important step toward increasing security. Just over one organization in three also considers it important to increase leadership’s role and to dedicate security responsibility to a particular person or team. In this respect, organizations in Nigeria should seek to hire CISOs, particularly as only one respondent in four to IDC’s Enterprise Security Trends Survey, 2022, has a CISO responsible for IT security in place. Alternatively, organizations can seek out vendors that offer virtual CISO programs. The creation of a security operations center team, which would be a huge opportunity for managed security service providers, is another option.

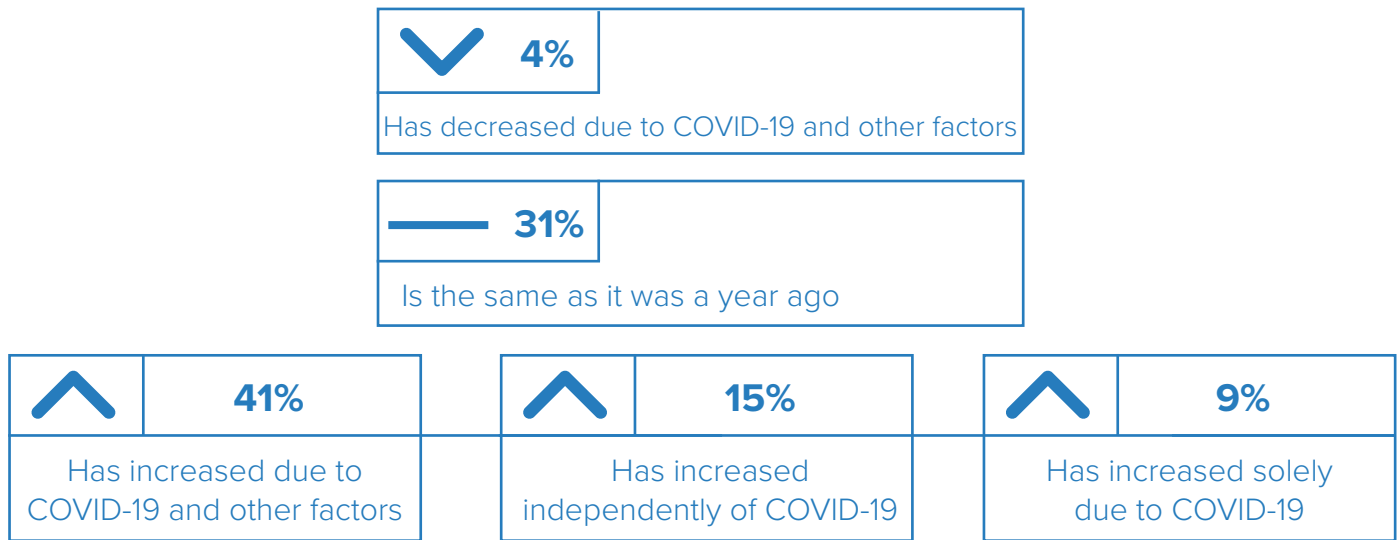
Security should be the shared responsibility of all stakeholders across the organization. Even the best security solutions can fail if employees have no awareness of security. Approximately 20% of organizations in Nigeria indicated that training non-IT employees in security awareness is one of the most important steps for increasing security. Although this percentage is fairly low, it is expected to increase, with many more organizations expected to launch security awareness campaigns.

The Impact of COVID-19 on Security Strategies

Organizations have always recognized the importance of security. Unfortunately, other technologies used to take budget precedence over IT security solutions. Many organizations simply had other important priorities — such as curtailing costs — even though their existing approaches increased security risks. This situation has changed in the past few years. The pandemic has accelerated security investments and forced numerous organizations to increase focus on cybersecurity, although some had prioritized security before the virus outbreak.

Figure 7: Current Commitment to IT Security

Q: How has your company’s commitment to IT security changed over the past year?



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

According to IDC’s Enterprise Security Trends Survey, 2022, almost 65% of organizations in Nigeria increased their spending on IT security in 2021. Of these respondent organizations, 50% did so partly or solely due to the consequences of the COVID-19 pandemic. Conversely, 15% of organizations increased their security spending over the past year independently of COVID-19. This data reflects IT executives’ proactive approaches to IT security over the past few years.

Current Maturity of IT Security Strategies

Organizations must understand their position in terms of their security strategies to take further steps and draft security risk awareness programs for employees and other stakeholders. According to a recent IDC survey, only 16% of organizations in Nigeria have implemented a full end-to-end security strategy outlining shared responsibilities, risk tolerances, classified events, and recovery plans in case of an attack.

Around 15% of organizations have implemented a security strategy without testing or conducting vulnerability assessments (i.e., verifying whether security solutions have been patched or not). Another 28% of organizations have implemented a partial strategy — one that may be limited to certain applications and business processes. These two approaches, however, make organizations vulnerable to security breaches, since they can leave unnoticed loopholes or gaps in the environment. Testing the security environment helps identify these loopholes, manage risk, and realize the benefits of security investments already made.

Figure 8: Security Strategy Maturity



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

Nearly one organization in five in Nigeria has no security strategy in place, and approximately one in ten in the country claims it does not need a dedicated IT security strategy. This number should decrease over the next few years, with many more organizations expected to launch security awareness campaigns. In terms of industry verticals, government organizations have focused more on implementing full security strategies. Some 30% of the government organizations surveyed have implemented a full security strategy. In the finance sector, around 55% of organizations have implemented — but not formally tested or reviewed — a security strategy. This presents a clear opportunity for providers offering full security strategies in Nigeria.

Key Challenges and Opportunities

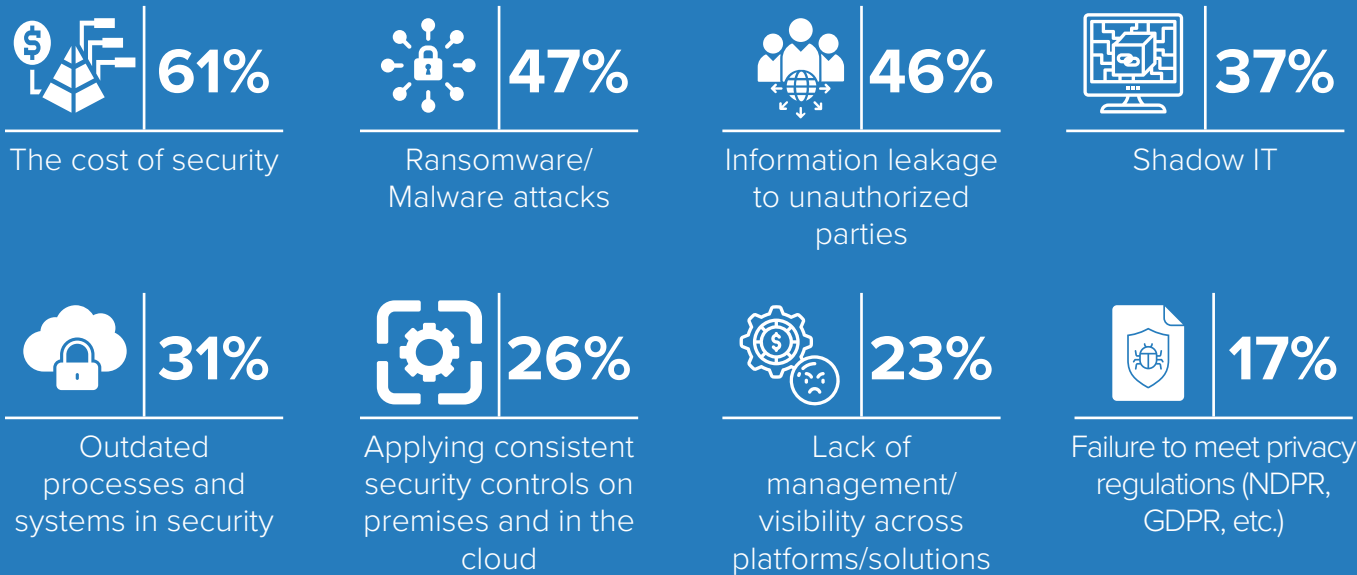
According to IDC’s Future Enterprise Resiliency and Spending Survey, 2021, nearly one enterprise in two experienced a ransomware attack in 2021. Nigeria is no exception to rising cybercrime rates, having been ranked 16th in cybercrime by the FBI in its Global Cybercrime Victims Report of 2020. Unfortunately, ransomware has evolved into ransomware “as a service” (RaaS). Criminals can now purchase ransomware on the dark web and use it to exploit organizations without knowing the technicalities of ransomware coding.

Malware attacks are another highly widespread form of cybercrime. The majority of successful ransomware and malware attacks stem from phishing emails and a lack of sufficient security-oriented culture in organizations. According to an IDC survey data conducted this year, 47% of organizations in Nigeria encountered ransomware and malware in 2021, while 46% experienced information leakages to unauthorized parties. Information leakages are also cited by many security service providers in their threat intelligence reports. The Cyber Security Experts Association of Nigeria (CSEAN) has released statements about it. Organizations must not give in to ransomware demands, even though they may feel it is necessary to do so, as any payment would only lead to increased numbers of attacks and higher amounts of extortion.

Modern security solutions must be capable of tackling the complexity and load of various cyberthreats and attacks. Naturally, this means that cybersecurity solutions are now costlier than ever before. In fact, some 61% of organizations in Nigeria cited the cost of security as the top security challenge they face. However, vendors may be able to lower prices by incorporating AI and automation into their existing solutions. Shadow IT and outdated processes and systems remain additional challenges as organizations move to new digital business models.

Figure 9: Security Challenges in the Past Year

Q: Which of the following security challenges have you encountered in the past year?

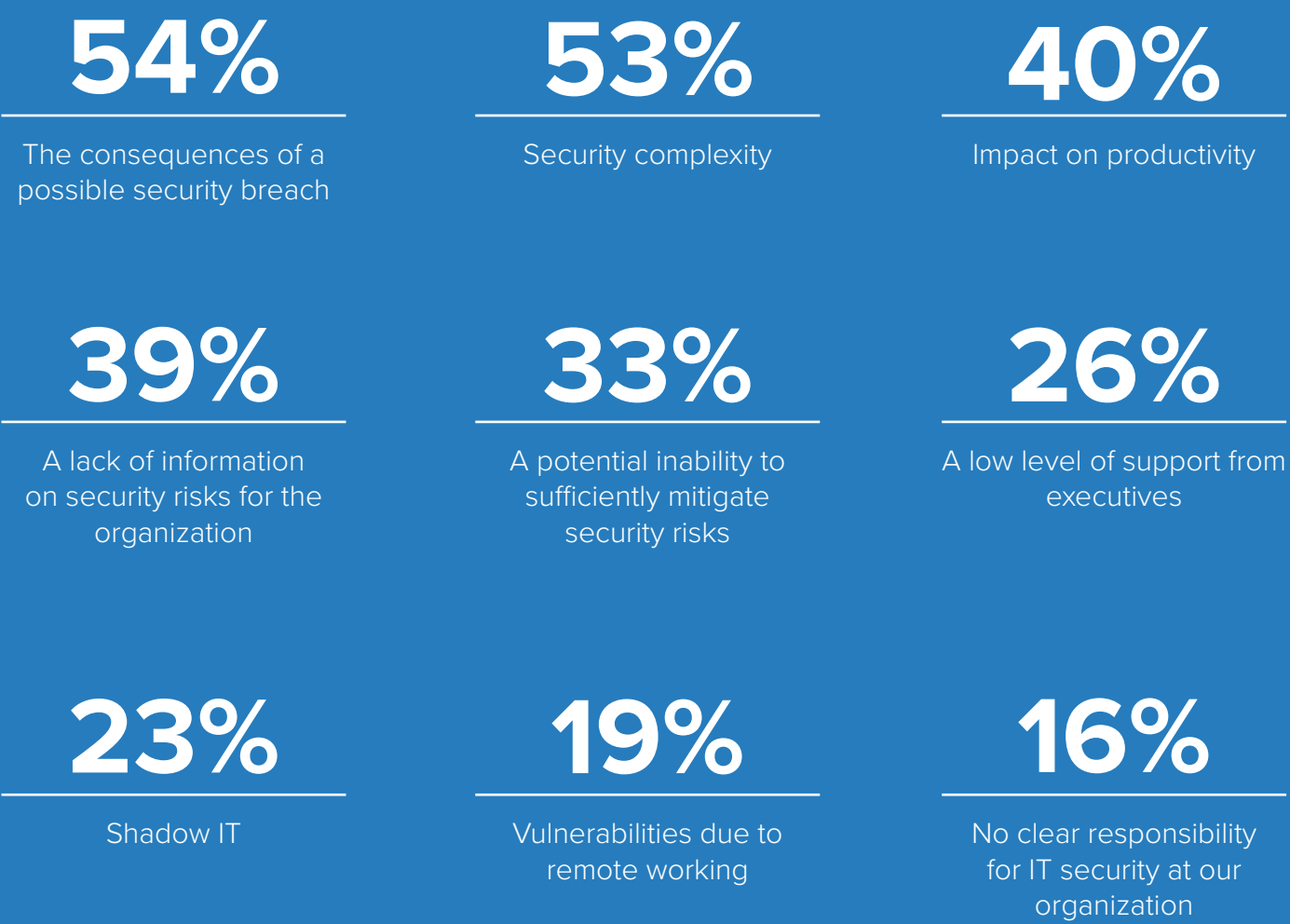


Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

Although security solutions are typically expensive to procure and security professionals are difficult to attract and retain, security budgets are not the only concern organizations face when addressing IT security.

Figure 10: Top Security Concerns

Q: Aside from budgeting issues, what are your top security concerns?



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

The financial, reputational, and business-related repercussions of a possible security breach are the top security concerns for more than one-half of organizations in Nigeria. Managing the complexity of security solutions and infrastructure is the second biggest concern, as cited by 53% of respondent organizations. The expanding threat landscape and the evolution, complexity, and cost of associated security solutions and governance mechanisms make it even more difficult for organizations to keep pace with cybersecurity developments. Around 40% of organizations are concerned about the impacts successful cyberattacks would have on productivity. A lack of information on security risks, an inability to sufficiently mitigate security risks, and a low level of support for security solutions among executives are additional concerns for organizations in Nigeria.

Current Approaches to Data Privacy and IT Security in the Supply Chain

Digital supply chains are expanding as the number of stakeholders involved in managing businesses increases. Organizations are also engaging with multiple players, such as software vendors, service providers, systems integrators, telcos, hardware providers, and cloud hyperscalers. Organizations typically engage with such players over the long term. During such engagements, organizations must ascertain whether their partners are complying with regulations and have the necessary privacy frameworks in place. If such partners do not have privacy frameworks in place and are not compliant with regulations, organizations could be susceptible to different kinds of breach.

Figure 11: Current Approaches to Privacy and IT Security in the Supply Chain

Q: Which of the following describe your organization’s current approaches to assessing the privacy (in relation to GDPR, NDPR, etc.) and IT security of your supply chain?



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

Nearly half of the organizations surveyed in Nigeria scrutinize their suppliers’ capabilities (in terms of certifications) and ensure vendors follow the current data privacy regulations. Around 46% require the completion of a questionnaire or checklist form, while 43% seek privacy assurances in supplier contracts. In some cases, this means including penalties in contracts for failure to meet certain requirements or service-level agreements. A minimal number of organizations regularly audit their suppliers’ and vendors’ security and privacy processes, while nearly one organization in ten does not assess the compliance levels of their suppliers.

NDPR was established by the National Information Development Agency (NITDA) and came into force in October 2019. The NDPR’s aim is to address rising levels of cybercrime and regulate who can access and control personal data. The provisions imposed prior to NDPR were ineffective in ensuring compliance and addressing cybercrime. NDPR is currently Nigeria’s most comprehensive law on data protection and has been pivotal in enforcing compliance. During 2020, NITDA issued 230 compliance and enforcement notices, but this number fell drastically in 2021, to 105. Even though nearly half of the surveyed organizations have a basic level of compliance in place, most still have a long way to go to become fully compliant with NDPR.

Figure 12: Current Level of Compliance with Nigeria’s Data Protection Regulations

Q: How would you rate your organization’s current level of compliance with Nigeria’s data protection regulations?



Source: IDC Enterprise Security Trends Survey, 2022, Nigeria

Some 27% of organizations in Nigeria are still working on achieving a basic level of NDPR compliance. Only 12% of organizations are fully compliant, while 14% are very compliant and are working on embedding compliance in their usual business activities. Organizations in the healthcare and finance verticals are the most compliant with NDPR. Because businesses in Nigeria are under pressure to take data privacy more seriously, security companies that offer compliance and GRC services have a huge opportunity in the country.

Essential Guidance

Organizations embarking on digital transformation should follow the below security guidelines to ensure secure and smooth transformation:

- **Prioritize securing the cloud journey.** Organizations moving to cloud environments should not ignore security during migration. They should avoid lifting and shifting security controls and adopt more scalable and agile cloud-native security solutions upon migration. Securing the cloud is not the responsibility of the vendor alone; it is a joint responsibility with the customer. Organizations must ensure no loopholes are created in new environments during migration.
- **Focus on security GRC requirements.** Countries are taking steps to ensure data sovereignty as the threat landscape evolves. By complying with GRC requirements right at the beginning of a technology implementation, organizations can effectively manage IT and security risks, reduce costs, and meet compliance requirements.
- **Develop an end-to-end security strategy.** Gone are the days when security was considered a standalone solution that sits at the network layer. With evolving technologies and the expanding threat landscape, organizations now need to formulate end-to-end security strategies. They must avoid independent and siloed security implementations and focus on establishing a broad and expansive security umbrella.
- **Understand the value of security on your business.** Organizations have been ignoring the risks of not implementing security solutions and remain largely unaware of the impact breaches might have on their operations. One security incident can completely jeopardize an organization and undermine years of business building. A secure and resilient organization, on the other hand, can generate incremental revenue and positively impact brand value as customers gradually recognize and appreciate its competence in managing and securing their data.
- **Recognize that risk assessments and vulnerability testing are essential.** Organizations must not sit back after implementing a security solution. Conducting regular risk assessments increases security awareness at the board level and enables faster implementation of the necessary security solutions. It also paves the way for new levels of technology adoption. With technologies constantly and rapidly evolving, lines of business may occasionally feel the need to adopt new software or solutions that unintentionally create vulnerabilities in the existing operational environment.
- **Audit suppliers' security and privacy processes regularly.** The digital supply chain is evolving, and the number of entities organizations engage with is rapidly increasing. Organizations typically have long-term contracts with suppliers. Over the duration of these contracts, suppliers' working models and relevant regulations can change significantly. Organizations must seek assurances from suppliers about compliance with new regulations and regularly audit them to ensure that the privacy terms stipulated in supply contracts are fulfilled.

- **Raise security awareness among employees.** Many attacks and viruses are triggered by employees unintentionally opening malicious emails and clicking on unsecure links. Running regular security awareness training sessions for employees must consequently become a critical mandate for organizations.
- **Select the right security vendor.** All the above efforts will bear fruit if organizations select the right security vendors. A security vendor should act as a DX partner and guide the customer throughout the DX journey to ensure a safe and successful transition. Selecting a partner with strong technological knowhow and vast exposure to the global threat landscape will be essential for organizations embarking on digital transformation.



Accelerating your Digital Transformation Journey

The COVID-19 pandemic has accelerated the digital transformation of the workplace, with much of this digitalization being enabled by cloud. Throughout 2020, we watched companies drive innovation, make more informed decisions with data analytics, outpace their competitors, and deliver products, services, and applications faster. Migrating to the cloud is a business imperative — one that can be tailored to an organization's unique needs with Azure and Microsoft 365 and secured by Microsoft's Zero Trust Security and Microsoft Compliance Management solutions.

With more than 60 regions, Microsoft boasts the largest datacenter network in the world. Its datacenters are 98% more carbon efficient than traditional datacenters, with over 4 million servers containing 40 million hard disks and solid-state drives.

Microsoft's Approach to Zero Trust

Microsoft relies on Zero Trust for increased security and compliance agility, speed of threat detection and remediation, and simplicity and availability of security analytics. Based on the principles of “verify explicitly”, “use least privileged access”, and “assume breach”, Microsoft offers a comprehensive Zero Trust architecture with strong foundations in compliance. Fundamental to this multilayered security model is an ability to work behind the scenes so as not to disrupt the end user's day-to-day tasks and duties. Microsoft not only recommends this approach for its customers and partners, but also embraces it for its own global security and software development.

Uncovering the Security Layers of Zero Trust

• Identity

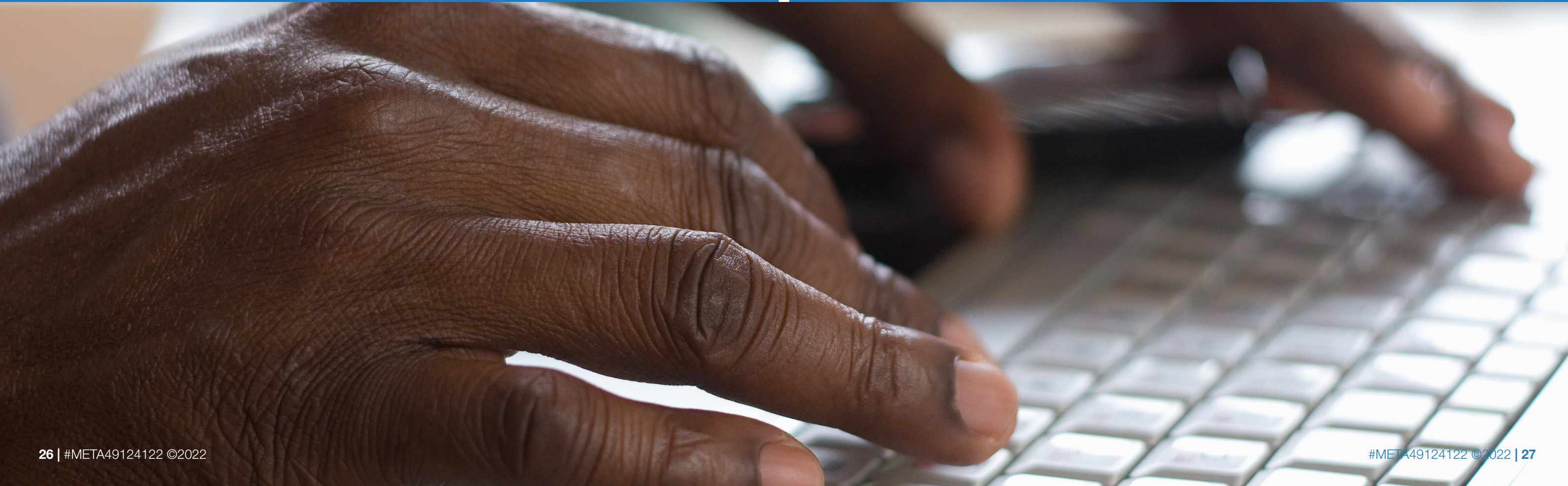
Starting with identity, Zero Trust verifies the people, devices, and processes that have been granted access to an organization's resources. Microsoft's Azure Active Directory (AD) assigns identity and conditional access controls to users, apps, processes, and devices. Azure AD can also provide a single identity control plane with common authentication and authorization for all your apps and services. This prevents the use of multiple credentials and weak passwords across different services and helps to universally apply strong authentication methods, such as passwordless multifactor authentication for users.

Insider Risk Management is integrated with Azure AD and can act on potential risks within your organization. By quickly identifying and remediating code-of-conduct policy violations, Insider Risk Management can support your organization's overall security and meet industry-specific compliance requirements.

• Endpoints

Next in the multilayered framework is the security compliance of endpoints — the hardware accessing your data. This includes IoT systems at the edge. If endpoints are not up to date or appropriately protected, they run the risk of data exfiltration from unknown apps or services. By using Microsoft Endpoint Manager, you can make sure your devices and installed apps meet your security and compliance policy requirements, regardless of who owns the device or where it is connecting from.

Also, Microsoft Defender, with its Extended Detection and Response (XDR) management controls, can identify and contain breaches discovered on an endpoint and force the device back into a trustworthy state before it is allowed to reconnect.



- **Applications**

Whether local or in the cloud, this layer provides oversight of your applications as the software-level entry points to your organization's information. Azure AD can also provide authenticated sign-in and conditional access to your cloud and local apps that connect to cloud-based services. Additionally, Microsoft Endpoint Manager can be used to configure and enforce policy management for both desktop and mobile apps, including browsers. For example, you can prevent work-related data from being copied and used in personal apps.

Knowing which apps are used within your organization is critical to mitigating new vulnerabilities. With its catalog of more than 17,000 apps, Microsoft Defender for Cloud Apps - MDCA can discover and manage shadow IT services. You can then set policies against your security requirements to scope how information may be accessed or shared by these services. For example, you can use policies to block actions within a cloud app, such as downloading confidential files or discussing sensitive topics while using unmanaged devices.

- **Network**

The network is the fourth layer in the Zero Trust security model and protects access to resources, especially those in the corporate perimeter. With modern architectures and hybrid services spanning on-premises and multiple cloud services, virtual networks — or VNETs — and VPNs, Microsoft gives you several controls, including:

1. **Network segmentation** to limit the blast radius and lateral movements of attacks on your network
2. **Threat protection** to harden the network perimeter from things like distributed denial-of-service (DDoS) or brute force attacks, with the ability to quickly detect and respond to incidents
3. **Encryption** for all network traffic, whether internal, inbound, or outbound

Microsoft offers several solutions to help secure your network, including Azure Firewall and Azure DDoS Protection to protect your Azure VNET resources. Importantly, Microsoft's XDR and SIEM solution, comprising Microsoft Defender and Azure Sentinel, can help you to quickly identify and contain security incidents.

- **Infrastructure**

The infrastructure layer includes the physical or virtual hosting of data. This is where configuration management and software updates are important so that all deployed infrastructure meets your security and policy requirements. Azure Security Center, along with Log Analytics, helps with configuration and software update management for your on-premises, cross-cloud, and cross-platform infrastructure. Microsoft Defender with Azure Sentinel monitors for the detection of vulnerabilities, attacks, and anomalies, with depth and breadth threat protection for multicloud workloads.

- **Data**

At the final layer, there is data. By applying the right controls to protect your data, you have the ability to limit access only to the people and processes that need it. Microsoft Information Protection enables policy enforcement at the document level based on Azure AD identity. Microsoft's data loss prevention solution prevents the movement of sensitive information at the boundary of the cloud, between Microsoft and third-party clouds, and at the device endpoint. For data outside of Microsoft 365, Azure Purview automatically discovers and maps the data sitting across your Azure, on-premises, and SaaS data sources; it works with Microsoft Information Protection to help you classify your sensitive information.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,200 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in more than 110 countries worldwide. For more than 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Middle East, Africa, and Turkey
Thuraya Tower, Level 15,
Dubai Media City,
P.O. Box 500615,
Dubai, UAE
www.idc.com/mea

Corporate Headquarters
140 Kendrick Street, Building B, Needham,
MA 02494
+1 508 872 8200
www.idc.com



Copyright Notice: External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC vice president or country manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason. Copyright 2022 IDC. Reproduction without written permission is completely forbidden.