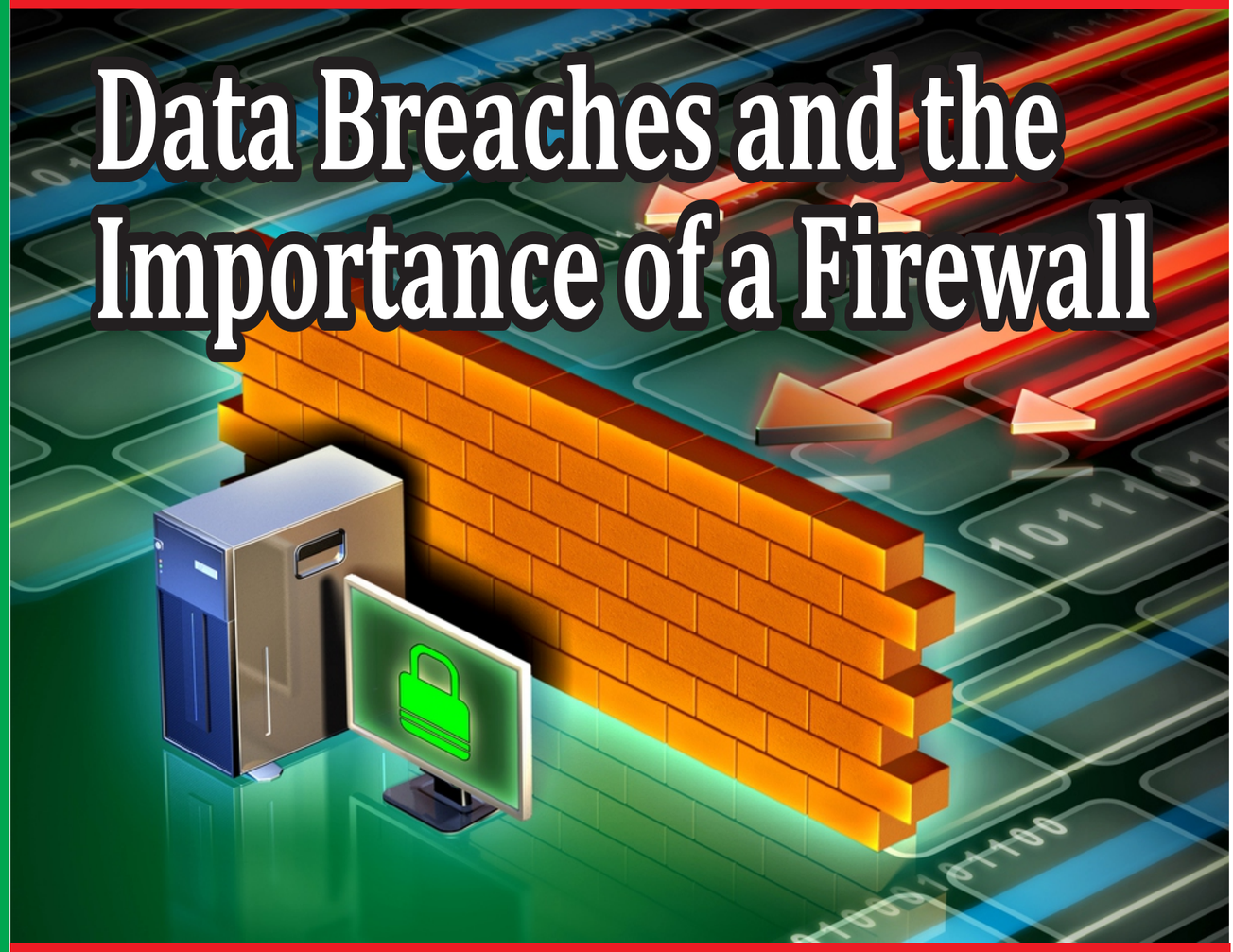
Association of Chief Audit Executives of Banks in Nigeria

Design+printbyProwess08039221516

ACAEBIN
Plot 1398B, Tiamiyu Savage Street, Victoria Island, Lagos.
Office Line: +234-1-3424805
E-mail: info@acaebin.org
website: www.acaebin.org

Eagle Eye

A Quarterly Publication of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) Q3, 2021



Data Breaches and the Importance of a Firewall

Personality Interview:

Auditors must place premium on Fidelity in resolving conflict of Interest.

Page 14

Wellness

Things To Do and Not To Do After Taking Covid Vaccine

Page 26

Open Banking and the Gatekeepers

Page 24

ACAEBIN EXCO MEMBERS

Yinka Tiamiyu
(Chairman)

Uduak Nelson Udoh
(1st Vice Chairman)

Felix Igbinosa
(2nd Vice Chairman)

Gboyega Sadiq
(Treasurer)

Aina Amah
(Auditor)

Prince Akamadu
(Chairman Research & Publication)

Adekunle Onitiri
(Chairman Payment & Systems)

Dele Dopemu
(Ex-officio I)

Cyril Osheku
(Ex-officio II)

CONTENT

Editorial

Welcome to the third edition of your favourite professional publication in year 2021.

As usual, it is a loaded package. We have an interesting article on data breaches and the importance of firewalls. The author does a good job of outlining some of the known methods of data breaches while citing some incidents in recent times as learning points. He however counsels that though the implementation of a firewall alone will not protect the organization from a data breach, it's importance cannot be overemphasized as it is the least minimum requirement expected from an organization trying to protect its asset and data from any type of attack or breach.

We are all aware how the emerging digital transformation in the banking industry continues to change/shape customers' experiences with increasing adoption of digital life and smartphones. The global Covid-19 pandemic has also further enhanced the integration of the physical and digital economic domains. Our article on digital identity and future of banking offers insights into some factors driving the direction of digital identity while making recommendations on best practices in digital identity management.

Often, we pay lip service to the need for collaboration amongst the assurance functions and as a result, the institution suffers as we work in silos and/or build individual turfs. We have culled an article from the Institute of Internal Auditors that depicts a conversation between a Chief Information Security Officer (CISO) and a Senior Auditor on how collaboration between both functions can improve organisational cybersecurity by establishing a good rapport.

It is commonplace that during audit periods, 'there are usually various mindsets and attitudes held by both auditors and their auditees that hamper the successful execution of the audit exercises, resulting in outcomes that are not beneficial to the auditors, the process owners and the entire organization''. In an article titled Redefining Audit Experience, the author argues that 'in an ideal 21st century work environment, panics should not be associated with audit periods. Audit exercises should be a moment of openness and trust among auditors and their auditees. It should be a huge window for transformational improvements within organizations. These are timeless truths and I recommend this article as the author also made recommendations on how to strike the right balance and achieve the desired objective.

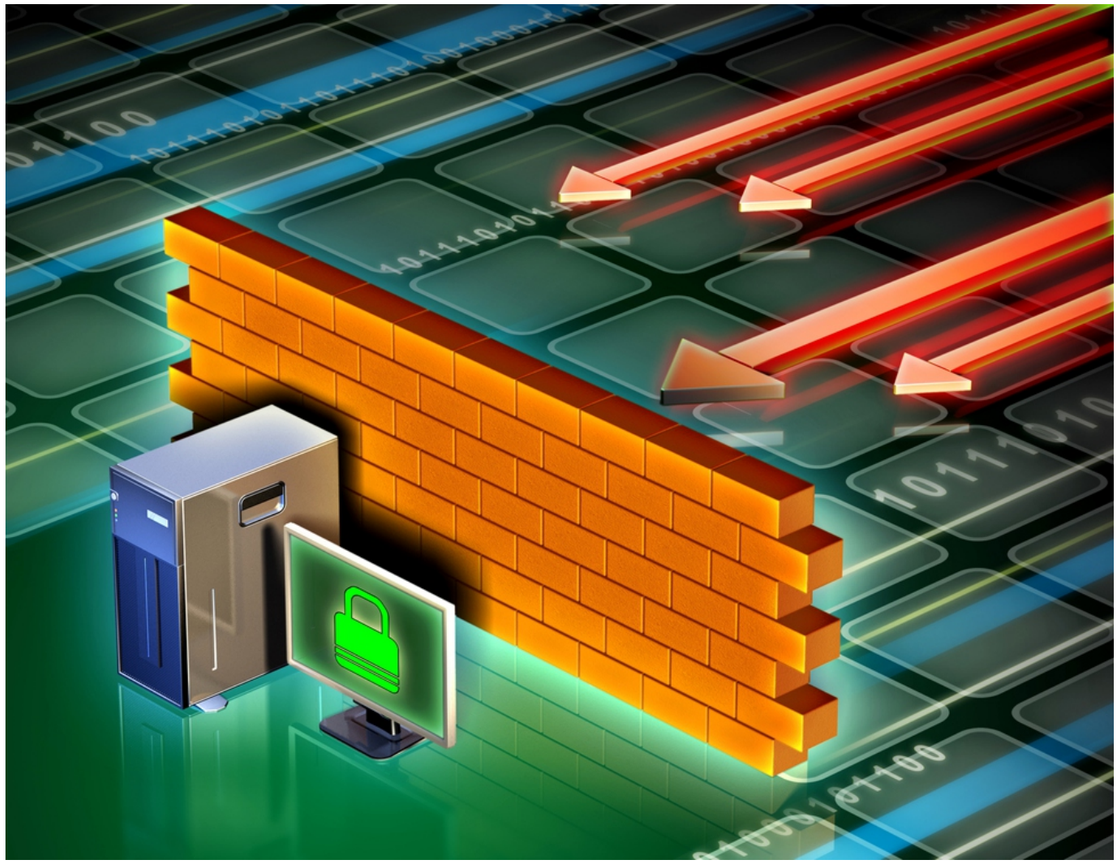
Is the COVID-19 pandemic ebbing away? Hopefully, we can answer that in the affirmative especially as the vaccine roll-outs raise hope that COVID-19 will subside soon. However, auditors may begin to question how the pandemic has impacted financial statements as the risk environment definitely has changed. Since the crisis have exposed the susceptibility of internal controls to work disruptions, internal auditors must learn how to provide assurance over financial reporting and other internal controls in a post-pandemic era. We have therefore included an article which recommends that Internal auditors should consider how to incorporate the impact of changes driven by the pandemic on accounting processes into their risk assessment and planning for audit programs and work.

Also in this bumper package, we have a mouth-watering interview with Mrs Vivian Agu, past Director, Internal Audit of Central Bank of Nigeria and present Chairman, Governing Council of the Institute of Internal Auditors, Nigeria Chapter. It is a readers' delight as she shares her wealth of experience during the interview

There are other interesting articles in this bumper edition that I dare say is a collector's delight. Enjoy reading while I wish the Association fruitful deliberations at the 50th Quarterly General Meeting.

Keep safe!

Prince Akamadu
Editor-in-Chief



Data Breaches and the Importance of a Firewall

DATA BREACH

Data breach is defined as the unlawful and unauthorized access to a computer system, network, sensitive or private data and information such that it compromises the confidentiality, integrity and availability of such information and data on that system or network.

The aim of a data breach could be to steal, manipulate or exfiltrate data for personal, monetary, or political gain. Personal information, such as individual's name and government-issued identification data, financial records, financial account numbers and personal identification numbers (PINs), credit card details, medical records could be subject of a breach depending on the motivation of the attacker(s). A breach can come because of a cyber-attack, insider attack, system misconfiguration, etc.

COST OF DATA BREACHES

Loss of business: The impact of this area tends to be immediate and more relevant from a financial perspective since it eliminates the operation of the business or part of a business, resulting in total loss of revenue. Depending on the industry, the type of loss-of-business areas within the organization can add up quickly and can eat into profits and depending on their business continuity plan some businesses do not survive.

Legal costs: This can be a heavy financial burden for most organizations victimized by a data breach. Absence of a cybersecurity insurance policy covering legal fees, data loss, damages to equipment or tools in the event of a breach, the cost of hiring a firm and/or firms to manage the litigation side of the breach can add up and weigh down the organization financially.

Loss of customers: This will inevitably occur, and it is impossible to place a monetary value on loss of customers since part of the loss is losing consumer faith and, thus, depletion of the brand value happens slowly all sometimes rapidly.

Studies have shown that if an organization were to suffer a data breach, 70 percent of its consumers or customers would stop patronising the business.

Usually when consumer perception is adversely impacted, it may be difficult to retain loyalty and trust. After a data breach, organizations can earn back consumers trust by being as responsive and transparent as possible.

METHODS OF ATTACK

Malware: Attackers use spam and phishing email tactics to try to trick the user into downloading malware attachments or directing users to vulnerable websites where malware is a click away. Email is a common way for malware to end up on a victim's computer. Malwares are malicious software or code that has been around since the advent of computing technology, and it has grown to become among the primary way's breaches occur. viruses are probably the most commonly used type of malware so because they spread by making copies of themselves.

Worms have a similar property. Other types of malware such as spyware are named for what they do; for example, spyware transmits personal information, such as credit card numbers. links or attachments in an email should be carefully scrutinised.

Stolen credentials: Attackers also use spam and phishing email tactics to try to trick the user into revealing credentials. Studies have shown credentials have been stolen using key loggers, via phishing or even exposed by third-party breaches.

Social engineering: The internet is a global village and as such people are interacting more than they did in previous decades and one of the methods of this interaction is social media, almost everyone have a form of presence online including employees in many organizations on major sites such as Facebook, LinkedIn and Twitter however each platform has the potential to provide an attacker several important information about employees, their jobs, roles, preferences and hobbies. This information can make it easier for an attacker to then launch an attack on the employee or his account at the enterprise layer by

spoofing and using social engineering attack technique. Attackers can gather this information to further attack other employees within same organisation.

Brute force: is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered. The longer the password, the more combinations that will need to be tested. It is also attacking the source of the data with as much persistence as possible and try every permutation to get through the password control. This attack method is made easier by the use weak or easily guessable password.

SQL injection is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

BREACHES THAT HAVE OCCURRED

LinkedIn | 117 million

Cybercriminals absconded with email addresses and encrypted passwords for 117 million LinkedIn users in this 2012 data breach. The passwords were encrypted using SHA1 encryption. They were also reports that the hacked LinkedIn accounts were being used in an InMail phishing campaign. These InMail messages contained malicious URLs that linked to a website spoofed to look like a Google Docs login page by which cybercriminals harvested Google usernames and passwords.

eBay | 145 million

In early 2014, cybercriminals were able to break into the network of the popular online auction site and harvested the passwords, email addresses, birth dates, and physical addresses for 145 million users however the damage was limited as the financial information sister site PayPal credential was stored separately from user information in a practice known as network segmentation. This had the effect of limiting the attack and prevented criminals from getting to the sensitive payment info.

Equifax | 145.5 million

The credit reporting company Equifax announced they had experienced a data breach back in 2017. This could have been avoided if Equifax kept their software up to date. Instead, hackers were able to take advantage of a well-known software bug and hack into the underlying software supporting the Equifax website. What makes the Equifax data breach so awful is not the size, though considerable; rather, it's the value of the information stolen. The perpetrators made off with the names, birthdates, Social Security numbers, addresses, and driver's license numbers for 145.5 million Americans. Plus, approximately 200,000 credit card numbers.

Under Armour | 150 million

Sports apparel company Under Armour 'exercise app MyFitnessPal was hacked in February of 2018. In the attack, cybercriminals managed to steal the usernames, emails, and encrypted passwords for 150 million users. Under Armour did well to announce the data breach within a week of its discovery. On the flip side, the company used weak SHA1 encryption on some of the stolen passwords, meaning criminals could crack the passwords and reuse them on other popular websites.

Myspace | 360 million

Cybercriminals stole data on 360 million pre-2013 Myspace users. This may not seem like a big deal, but the stolen passwords used weak SHA1 encryption which vulnerabilities has been discussed extensively by industry experts. As mentioned previously, criminals can try and reuse your old passwords on other popular sites in a credential stuffing attack.

IMPORTANCE OF FIREWALL

Network Protection from viruses and Malware

Installing a firewall is one of the security measures business can take, as firewalls can help control the traffic that comes and goes on the network. They are essentially a barrier between trusted network such as their own and untrusted or less trusted networks, such as the internet, other companies' networks. As firewall only permits traffic from sources that are defined within the firewall through rules. Any other traffic is denied and as such become less prone to virus and malware attack which could reduce data and information loss.

Protection Against DDosAttack

Installing a firewall could be the difference for small business from been compromised and used as part of a botnet to lunch a DDos attack against bigger businesses as the firewall assist in monitoring and alerting of a suspicious activity on the network. The business can also be the victim in this attack thereby causing slow processing of the victim's network leading to inefficiency and low productivity for the business.

Access Control

The firewall is a system of hardware and software components that define which connections can pass back and forth between communication partners.

By using a firewall system, small businesses can for example, set traffic permissions between the intranet and the Internet, they can allow a defined set of services to pass through the different network zones while keeping other services out. For example, they can allow users in their company's intranet to use

Internet services such as mail or http, but not other services such as telnet. Thereby minimizing the risk of attack that could lead to loss of data, information resources and finance

Protect Against Sniffer Attack

A sniffer attack is an application or device that can read, monitor, and capture network data exchanges and read network packets.

If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunnelled) packets can be broken open and read unless they are encrypted.

Man-In-the-Middle-Attack

As the name indicates, a man in the middle attack occurs when someone is between you and the person with whom you are communicating and is actively monitoring, capturing, and controlling your communication transparently. To prevent such attacks businesses should implement a firewall to the company's specifications, so that the firewall will protect the network from eavesdropping tools that might want to capture and analyse network traffic.

CONCLUSION

Although the implementation of a firewall alone will not protect the organization from a data breach it's importance cannot be overemphasized as stated above, it is the least minimum requirement one will expect from an organization trying to protect its asset and data from any type of attack or breach.

The configuration of the rules is also important as having the device implemented is not enough, so is the continuous monitoring of the rules and or policies to confirm their relevance and effectiveness.

Mofoluwaso Olaoye
Coronation Merchant Bank Ltd

What Boards Have Learned from the Pandemic

The past year's crisis provides numerous corporate governance lessons.

Eighteen months have passed since COVID-19 slammed into the world. It's been quite a journey from those first days of panic to, well, whatever this is today.

We can't really say the pandemic has faded from view — because while it has faded in North America, Europe, and several other countries, it hasn't receded in much of the developing world. We can say, however, that the challenge of COVID-19 has changed.

It has evolved from an acute condition, threatening the survival of the organization, to a chronic one that must be managed. COVID-19 exerted enormous influence over the duties and details of corporate governance, and it's likely to keep doing that for a long while yet.

So, what lessons can board directors infer from this ordeal? With the benefit of hindsight, what did they get right and get wrong? And in what unexpected ways did this crisis actually improve corporate governance?

"Companies that embraced change, found different ways to do things, and were agile enough to be flexible have evolved into a better version of themselves," says Alpa Parikh, who serves on the audit committee of a Seattle-area family services nonprofit and who joined tech company Smartsheet as head of internal audit while the pandemic was raging last year. ***"I believe that this resilience will allow such companies to be better prepared to face future challenges."***

Parikh's point is lofty, and very valid. Let's consider it more fully.

Start With Resilience and IT Risk

A recent McKinsey & Co. report, How Boards Have Risen to the COVID-19 Challenge, and What's Next, suggests that boards had a steep learning curve in 2020. Among 673 corporate directors surveyed, only 20% rated their boards as "very effective" at responding to last year's crisis. The most commonly cited obstacles were lack of in-person communications among directors, struggles with remote work and its related technologies, and lack of crisis management processes.

It should be no surprise, then, that boards also made lots of changes last year to address those problems:

investment in digital collaboration tools (cited by 45% of respondents), more frequent communications with management (cited by 37%), and more flexibility in the board's agenda (cited by 37%).

The other big change, according to McKinsey, was much more talk about operational resilience. Only 44% of board directors cited resilience in the prior year's survey; that figure popped to an impressive 60% this year.

The deeper point for board directors is how all these issues tie together. Of course every organization wants to foster resilience in the face of wrenching disruption. But attention to IT risk management is what makes such resilience possible — because without robust IT systems and management of IT risks, the organization isn't going to be resilient. It's going to be paralyzed.

In practice, that means boards should pay more attention to IT risk management and give serious thought to establishing a board risk committee to

oversee security and IT risk. Then the board can drive better operational performance and more resilience to changing conditions because it has the right technology to enable it.

A good example of this comes from the World Discipleship Association (WDA), a nonprofit headquartered in Atlanta that does missionary work around the globe. In a stroke of luck, the WDA had done a review of its IT risks just before the pandemic struck, as part of a larger strategic planning effort. That review led the WDA to take steps such as providing all employees, board members, and volunteers with corporate email addresses, which helped fight the threat of phishing attacks targeting people working remotely.

"It was fortuitous that a lot of our strategic planning to improve operations also allowed us to be more resilient when the pandemic started, because we had no idea how long it was going to last," says Keyaan Williams, chair of the WDA's risk committee.

A Risk Assessment

How can internal audit help boards embrace all of these lessons? Here are a few ideas:

- **Communication channels.** Assess the security and durability of boardroom communication channels. For example, rather than emailing board materials to directors, send secure, individualized login pages to view documents in a virtual data room.
- **Talent risk.** Does the board have the right directors for the new challenges of working remotely or expanding into new, more lucrative lines of business? Is the board asking about employee engagement, and assuring that people working in isolation still feel valued and part of the organizational whole?
- **Policy management.** Not all policies adopted during the pandemic's dark days need to continue. Policies should be revisited at regular intervals to see which ones should be decommissioned. Conclusions should be documented thoroughly; if the policies are

relevant to a regulatory investigation, regulators will want to see the homework.

The Challenges of Engagement

The other big governance lesson from the pandemic was the importance of communication and trust among the board. Yes, to a certain extent that point has always been true but the pandemic made the point more true, so to speak.

The pandemic has been both good and bad on that front. Yes, it drove the need for more board discussions, either as formal meetings or telephone conversations. On the other hand, scheduling Zoom calls adds a certain formality to the process. It also squelches the interpersonal dynamics that exist in physical meetings: the body language that indicates a person's true engagement with a topic, the spontaneous conversations that can lead to surprise insights.

For example, Raoul Ménès, who stepped down in May as audit committee chair for the Salt River Pima-

about the pandemic was that the frequency of communication went up dramatically," he says. ***"People had to get together all the time."***

Those more frequent, more virtual communications can be taxing. For example, boards need to consider confidentiality concerns, and they must work hard at delineating what is or isn't overstepping management's job of running the company.

But ***"there should definitely be options so that board members who cannot make it are able to join in remotely,"*** Parikh says. ***"That, in turn, will open up the options to increase diversity on company boards."***

What Have We Gained Here?

Nobody should say it was good for boards to go through this pandemic; the disruption was severe, and often painful. More accurate is to say that the pandemic taught us valuable lessons. Foremost, boards can step up in difficult times.

Maricopa Indian Community in Arizona, appreciated being able to drop by the internal audit team before a board meeting just to chat. Those days are on hold for a long time. ***"How do we keep people engaged while they're virtual?"*** he asks.

That's a legitimate concern. Williams, however, offers a valid counterpoint: ***"The thing I did appreciate***

"It was a lesson learned," Ménès says. ***"People can throw out words like 'internal audit agility' and 'resilience,' but if you're not living those values and making them part of your DNA, it's just a buzzword with no spine to it."***

Culled from: iia.org

Building a Better Auditor: When the Leader is Challenged

Xi joined a government agency a few years ago and has a good working relationship with the head of the agency, Xyrl. Xi has been able to provide assurance on the agency's objectives in a way that the agency has never seen before.

Previously, Xyrl thought internal auditors only looked out for mistakes or what went wrong, but ever since Xi arrived, providing consulting expertise in addition to assurance engagements has really turned things around.

Xyrl has found the contributions very useful and has grown to trust Xi. Putting structures in place has eased her role as the head of the agency. At times, Xi highlights issues for the various departments to consider before, during, and after certain projects. Such contributions have changed their mindsets so that they see the internal auditor as a business partner. But Xi never forgets to remind them that there is a difference between assurance and consulting engagements.

Recently, Xi has noticed that Xyrl has changed her habits. Where Xyrl used to respond to emails and recommendations and look forward to suggestions, she has become somewhat distant. At an internal meeting with other stakeholders, Xyrl suggested that Xi may "take a break," as the recommendation made was not feasible. This was something Xyrl had never done before.

At another encounter, when Xi tried to discuss something urgent she had observed, Xyrl responded, "I'm sure you know how to handle it." Another time, Xyrl decided to override the risk mitigation procedures the internal audit team had recommended in a show of power of who heads the agency.

There were rumors that Xyrl's tenure at the agency may not be extended in a few months, which may have led to the recent "I don't care attitude."

Unfortunately, Xi also has noticed that motivation at work has been slightly affected and mistakes she never used to make when reporting are now occurring. The truth is there may be best governance practices, systems, and policies in place, but in real life, the human element could threaten all of these.

This scenario is typical during the last days of a leader's tenure some handle their last days well,

others burn the structures they had built over time, and some are in the middle. Xi's team noticed the behavior at the last meeting, and one of the junior team members said, "I don't like the way Xyrl talked to you at the meeting. How do you handle the situation?" Here are tips to address the problem Xi encountered.

Be Professional: Work Must Go on

Xi told her team member not to worry about the situation. "My job is to provide assurance on management's activities to relevant stakeholders and not to make enemies. Our work should be able to speak for us and end users must have confidence in our output," she said.

Xi wanted to make sure the junior staff did not see that event as an "us versus them" scenario where they take

situations personally. She further assured her team that internal auditors are to conduct their work in a professional and competent manner. Do your job!

Assume Leadership

Every leader also is a follower of another leader. Thus, while Xi's team members were observing what is going on, Xi also has observed Xyrl's leadership style over time and noticed that her behavior has changed.

Xi is providing mentorship to her team by her actions during these changing times while trying to manage the challenges. Applying the philosophy of Theory U can help refocus the mind on performing core functions.

Theory U is a method of addressing change that advises individuals to observe the environment, sense changes going on and let go of unnecessary/temporary distractions, reassess self-principles, and realign one's self with vision and intention. In assessing changes in behavior, internal auditors should remember that their responsibility is not to an individual but to the institution and stakeholders who rely on their work.

Be Self-aware

It is easy to read theories, scenarios, and case studies until these happen to you in real life and you have to make quick decisions. Rules are written in theory; principles are applied in contexts. Self-awareness is closely linked to principles and this can intersect with an ethical framework when situations arise. The IIA's Code of Ethics expects internal auditors to apply the

principles of integrity, objectivity, confidentiality, and competency.

Keep Documentation

A compensating feature for internal auditors is documentation. While Xi may not have the power to make certain decisions that the agency's head can make, appropriate documentation of observations and issues provides evidence when the need arises. Documentation is not intended to present internal audit as an "I told you so" activity.

Moreover, documentation helps when another individual assumes your role or during a handover period.

Maintain Independence

Xi is fortunate that as the resident auditor at the

agency, she has a dual reporting role. Her primary responsibility is to the government, the government's audit branch, and the agency. Thus, she was not afraid of threats.

Certain situations arise where this scenario occurs in a private organization and Xyrl is the chief audit executive (CAE) who interacts with the board. In that case, auditors cannot override their bosses or call them out if they are doing the wrong things. Nonetheless, self-awareness is important in defining your principles and guiding the actions you take.

Independence is a core feature of internal audit. While internal audit provides assurance to management that controls are in compliance with relevant regulations and laws, auditors do not perform management responsibilities or act as if they are part of management.

Handling Changing Situations

At a private organization, this scenario could be dicier. If Xi reported directly to the CAE, she should assume leadership should be handled with care. That is, while displaying leadership qualities and not letting the situation affect them personally, auditors must take care that their actions do not send a signal to the CAE who frustrates them.

Also, some exiting leaders do not mind destroying structures upon leaving; they can burn bridges that may cause problems for auditors long after they have left. Thus, auditors should not come across as usurping the actual role but instead provide support to the departing leader as much as possible.

Organizational politics are unpredictable. In certain situations, depending on your relationship with the person in question, you can engage by talking, connecting, and sharing experiences. After all, "what is not discussed is not understood."

Culled from: iia.org

Personality Interview:

Mrs Vivian Agu, Chairperson, Governing Council, IIA Nigeria.

Auditors must place premium on Fidelity in resolving conflict of Interest.

When the idea for this interview was broached during one of the Editorial Team meetings, you could feel the excitement of every member – it was like 'yes, she is eminently qualified to grace the covers of our flagship publication'. Her achievements during her time at the Central Bank of Nigeria (CBN) towers shoulder-to-shoulder with her impressive physique but behind that big frame is a very quiet, meticulous and exciting woman with great wisdom and intellect.

Coming from a humble background, this accounting graduate from one of Nigeria's premier institutions, University of Nigeria, Nsukka spent 30 years of her professional career in various departments at the Nigeria's Apex bank namely; Banking Supervision, Bank Examination and the Internal Audit.

Following her retirement from the CBN, one would think that Mrs Agu would take time off corporate world but no, she is currently the Chairperson, Governing Council IIA Nigeria, providing strategic guidance and direction to the Nigeria affiliate of the Global body towards achieving her vision and mission.

In this exclusive interview with the Eagle Eye Magazine, Mrs Agu shares her experiences on internal audit function, IIA Nigeria and banking industry in general. Excerpts:

Madam, congratulation on your successful retirement and appointment as the Chairperson, Governing Council, IIA Nigeria.

How is life after retirement even though you are still actively engaged with IIA Nigeria and seem not tired?

Retirement has been restful and eventful. I am in good health and of good cheer. I enjoy contributing to the development and growth of internal audit profession through IIA Nigeria. I thank God for everything.

Tell us more about yourself – upbringing and journey into the banking industry?

My upbring was normal for my time: nothing unusual or dramatic. As is surely common to most people, I had very loving parents, wonderful siblings, good friends and schoolmates; and others with whom I shared happy memories and some occasional moments of difficulty or challenge. I read accountancy at the University of Nigeria and graduated in 1985. After doing my National Youth Service in Imo State, I joined the firm of Orji Chukwu and Co. Chartered Accountants and worked there till 1990 when I joined the Central Bank of Nigeria as an Assistant Manager. The rest, as they would say, is history.

How would you describe your experience during your time at the Apex Bank, CBN? Did you serve in other departments apart from the Internal Audit?

I treasure my time and experience at the Central Bank. I greatly value and respect virtually all of the people that I served with at various times and positions of work; and on numerous assignments. My most cherished images are of the people, the training, corporate culture and work environment of the Apex Bank that made it possible for me to contribute in a meaningful and impactful way to the organization. I also learnt very useful lessons and skills that will serve me well in subsequent years. I spent about 30 years in the Central Bank; twenty-two of those years were spent variously in Banking Supervision and Bank Examination Departments. My last eights were at the Internal Audit Department where I was the Director.

What would you describe as your most challenging experience and why?

There are broad similarities in the challenges and experiences that I had in Bank Examination/Banking Supervision or Internal Audit Departments. They all involve, to a large extent, the challenge of monitoring and promoting systemic integrity. This is indispensable whether for deposit money banks and other financial institutions, on one hand; or, for the Central Bank of Nigeria itself, as an organization. While the former is largely approached through the perspective of supervision for regulatory compliance, the latter is focussed on auditing for internal control. The first is crucial for the integrity of the banking system in the country. The latter is critical for the functioning of the Central Bank. What made the Internal Auditing role the most challenging for me, is the range of functions and sheer size of the Central Bank; and the scope and gravity of my individual responsibility as the Director of Internal Audit, who must also be a trusted adviser to top management as well as to heads of other coordinate Departments and/or Units of Bank. For the Auditor to successfully triangulate these roles, one must be fair, firm and also friendly. Many times, it is easier said or imagined than done.

What is the core objective/mission of IIA Nigeria and how is it driving her activities and programmes towards achieving its aims and objectives?

IIA Nigeria as a representative of IIA Global in Nigeria, works in conjunction with IIA Inc to carry out various activities in Nigeria, among these include:

- Advocating and promoting the value internal audit professionals add to their organizations.
- Providing comprehensive professional educational and development opportunities, standards and other professional practice guidance, and certification programs.
- Researching, disseminating, and promoting knowledge concerning internal auditing and its appropriate role in control, risk management, and governance to practitioners and stakeholders.
- Educating practitioners and other relevant audiences on best practices in internal auditing.
- Bringing together internal auditors from all parts of the country as well as experts from outside Nigeria to share information and experiences through conferences, seminars and workshops.

Some of the ways IIA Nigeria drives her activities and programmes towards achieving her aims and objectives include:

- Organizing paid and free programmes such as seminars, workshops and conferences to enable networking and knowledge sharing.
- Carrying out career development programs such as preparing members for international professional qualifications such as CIA, CRMA among others.
- Ensuring availability of local and international publications with a wide variety of pertinent information which keeps members current on an ongoing basis.
- Making available highly discounted learning resources to members at significantly reduced prices.
- Providing technical advice and support regarding internal auditing and the application of the Standards to all members.
- Creating awareness on global networking opportunities through the IIA Inc free web-based interactive community, regional (AFIIA) and International Conferences held annually.
- Performing advocacy visits and communicating to organisations and individuals regarding the mutual benefits that exists between individual internal auditors and their organisations.
- Reaching out to government institutions to canvass for internal auditing functions independence and rightful placement within the government hierarchy.

What is the level of collaboration of IIA Nigeria with other sister bodies in achieving her aims and objectives?

At the global level, IIA Global collaborates with notable professional organisations such as IFAC, ISACA, ACCA, COSO among others.

IIA Nigeria by reason of being an affiliate of IIA Global automatically inherited collaborative relationships with the various organisations that have relationship with her parent organisation, including the above listed.

In addition, IIA Nigeria collaborates with other locally domiciled organisations at various levels; and these relationships operate under different arrangements. For instance, ISACA Lagos and IIA Nigeria held a joint Nigeria National GRC conference in 2019, ACAEBIN collaborated with IIA Nigeria to provide training program to internal auditors across banks in Nigeria in 2017, ACCA, ISC2 among others have partnered with IIA Nigeria and enjoyed special payment discounts during IIA Nigeria conferences.

In the years ahead IIA Nigeria would explore more collaborative opportunities as part of her strategic goals.

Auditors are expected to be independent. As an experienced Auditor, do you think Auditors in Nigeria are truly independent? And what is IIA Nigeria doing to ensure the entrenchment/respectability of the independent of Auditors in Nigeria?

The auditor is in a unique position of trust. He has multiple stakeholders - the organization that he or she is auditing, regulatory bodies, national authorities and the public. They all rely on the veracity of his or her professional judgement. In Nigeria, we are drifting more and more into an environment of moral relativism, where there are no longer any absolutes, in virtually all spheres of life and in every profession. It is becoming extremely difficult to assure that every practitioner will be diligent and will respects the high ethical standards of his profession in the face of demands to cut corners, to service some vested interests in order to prosper or remain in business. The pressures on Audit professionalism and independence are no exceptions. IIA Global and IIA Nigeria are aware of these challenges. That is why we are acutely focused on interactive value creation between our members, so that iron will sharpen iron. Next, we are committed, as individuals and as organizations, to strengthen the structures for professional institutions and associations – for continuous development and inculcation of discipline; and, for regulatory bodies to enforce standards and sanctions where situations warrant such.

During your time as the Director of Internal Audit, Central Bank of Nigeria, you were a member of ACAEBIN. Do you think the Association is doing enough in regulating and ensuring professionalism of her members?

I think that in the context of our environment, ACAEBIN members are doing their best; but like in all things in life, there is a lot of room for improvement.

Auditors are sometimes faced with the challenge of conflict of interest in the discharge of their duties. Were you ever in that shoe, how were you able to find a balance without compromising your independence?

Quite frankly, I do not recall any moment of significant conflict of interest in the course of my work in an audit

firm or the Central Bank of Nigeria. In my considered view, if a conflict of interests should arise in the course of an audit exercise, I would expect the auditor to respect our professional hierarchy of values which places the highest premium on fidelity. In such a case, the auditor should either declare his or her interests or recuse him/herself from the audit exercise. But there were many instances where, as a Bank Examiner or as the Director of Internal Audit I would not totally agree with the presentations of a bank or a Department/Unit of the Bank on some aspects of policy compliance and/or internal control. For such situations, one would use a range of mechanisms like audit queries, meetings and reviews of audit reports to get more information or harmonize issues before I take a final position. In the process, one's position can change - especially if availed with pertinent explanations or superior logic. This is part of the audit process. It is quite distinct from compromise of one's independence.

The internal audit function is a highly skilled area, do you think auditors are adequately equipped/given the desired exposure in terms training and retraining to enable them deliver

We live in an era of rapid changes especially in the forms, content and expectations of organizations; and in the nature, range, speed and instruments of financial transactions. While most change are in response to the demands for greater efficiency driven by new technologies and the requirements for transparency, there are down-sides, in that the volume and speed of fraud and the potential for consequences for misuse of technology can run far ahead of the internal auditor and in some cases, wreck irreparable damage. As such the internal audit function must change with the changing times even as it holds fast to its unchanging principles. In that wise, I cannot over emphasis the importance of training for all internal audit practitioners and even more importantly, retraining for the older ones.

In your experience, do you think that Nigerian banks are doing enough in supporting the real sector of the Nigerian economy which has been identified as the engine of growth and development of our economy. What other areas would you want banks to focus efforts at?

As you said the real sector is the engine of growth and development of our economy. From the outset, the Central Bank of Nigeria has been relentless in developing policies to support the real sector. If you recall, one of the objectives of banking consolidation of about two decades ago was to have banks with enough financial muscle to drive the sector. In the last couple of years, the Central, Bank has developed a plethora of intervention schemes; including preferential exchange rate mechanisms that are all aimed strengthening the real sector. I am following our banks and their role in the Nigerian economy with very keen interest. I think they must now come out of their comfort zone, and try to match the Central Bank of Nigeria in initiative and innovation. They should try even harder to spur agricultural production, food processing, storage and distribution; as well core manufacturing and of course start-ups across board and SMEs.

What is your advice to your ex-colleagues in ACAEBIN and the younger auditors in general?

As I said earlier, the world is changing all very rapidly. This applies equally to professions, to organizations and institutions; and the workplace. The internal auditor – regardless of whether he or she is a member of ACAEBIN, a young man or woman;

Regardless of whether one is old or young in the audit profession, there is no substitute to strong professional ethics and sound personal moral principles. These aspects of and requirement of the auditor are as old as time. They can never be annulled by change. These, together with sound training and retraining, are the pillars upon which we will build an ever inspiring, vibrant and well-respected internal audit profession in Nigeria, and around the world. Finally, to my former colleagues in ACAEBIN, I am delighted to extend my warm regards; most especially - my immense appreciations for the wonderful work we all did together.

Cyberrisk Quantification for Improved Cybersecurity

Cyberthreats and cyberattacks are inevitable. Cyberrisk, which formerly was considered relevant only to cybersecurity professionals, is now recognized as having the potential to threaten an entire organization. Dependence on technology-driven, efficient and secure systems increased throughout the COVID-19 pandemic, which allowed many enterprises to operate from the homes of their employees. In this new working environment, the threat of a cyberattack can undermine the trust that stakeholders have in the organization.

Protection from cyberattacks should undoubtedly be a top priority for organizations. Many cyberattacks are predictable, but the severity of their impact on an enterprise can only be estimated. The ability to mitigate cyberrisk is based on the effectiveness of an organization's risk management. Complex, diverse technology ecosystems and the interwoven business processes create a variety of sources of cyberrisk. These may vary in terms of frequency or implications for the organization.

Organizations have finite resources, therefore, cyberrisk must be understood, evaluated and quantified. These activities are prioritized based on the implications for the organization. According to the ISACA white paper, *Cyberrisk Quantification*, "cyberrisk quantification (CRQ) sometimes called cyberrisk economics is a technique adopted by many enterprises to understand cyberrisk exposure and rationalize their options to manage it." These techniques also aid in understanding different sources of cyberrisk and their impact. Best practices for cybersecurity governance dictate that management should be presented with information about the sources of cyberrisk facing the organization to enable a uniform level of understanding. CRQ that began as an approach to cyberrisk became integral to most enterprise risk management (ERM) programs.

Risk is traditionally quantified as the product of probability and impact. Typically, labels such as "high," "medium" or "low" are assigned to these variables to perform quantification. However, this assignment of labels is not based on accurate measurements, but influenced by individual perception. Although labelling does allow for some quantification, it does not necessarily reflect accurate CRQ.

> **"Organizations have finite resources, therefore, cyberrisk must be understood, evaluated and quantified."**

Many industry-accepted cybersecurity standards emphasize the importance of quantifying risk accurately through a systematic risk management process. Risk identification, quantification and mitigation are essential phases of risk management. Mitigation of cyberrisk through adequate controls is an inherent aspect of implementing robust

cybersecurity measures. The evaluation of controls is often equated to risk evaluation. The presence of appropriate controls is associated with low risk, while the absence of controls is associated with high risk. The significance of controls in the overall risk management process cannot be ignored.

However, there is more to CRQ than the evaluation of control quality. Antimalware, for example, is an important control for most systems. In the case of hermetically sealed or air-gap systems with no external interfaces, this control may be less significant than other connected systems. Therefore, evaluation of the effectiveness of controls without a thorough evaluation of the context may not yield adequate CRQ.

Measurement also lies at the heart of CRQ. The elements used to calculate CRQ must be measured and quantified correctly. Relying on approximation has its pitfalls. Participants in a CRQ exercise may be asked to describe the frequency of events using descriptive terms such as “likely,” “often” and “frequently.” These words are then translated to numerical values. This technique, however, suffers from inaccuracies, bias and individual cognition. A respondent, for example, may consider a label “frequently” to be 60% of the time, while others may consider it to be 85% or even higher. Further responses may be skewed by participants' biases and cognition. It is therefore, desirable, to adopt techniques that minimize the possibility of any bias.

The increasing importance of cybersecurity has made organizations more willing to invest in cybersecurity controls and tools to protect against cyberattacks. Many of these tools continuously scan for indicators of cyberthreats. An application layer firewall, for instance, is always scanning the traffic flowing to and from applications. It, like other tools, analyzes a large quantum of data. Traditionally, these firewalls have been considered a cybersecurity measure rather than a measurement tool. The data processed by the various tools can serve as rich repositories and inputs to CRQ. Processing the data yields parameters, indicators and measures can be presented systematically through reports or dashboards. This concept is analogous to security information and event management (SIEM) tools that collect data, albeit for entirely different reasons.

It is also beneficial to include external data sources for relevancy in CRQ computations. External data including security breach reports such as global threat intelligence reports may be useful when benchmarking with the external world or when analyzing events that have not yet been experienced by the organization. Thus, a combination of internal and external data may be useful. Various service organizations provide information and security metrics based on publicly visible technology elements or services belonging to various organizations. For example, invalid Transport Layer Security (TLS) certificates are a parameter that is publicly visible without intrusive activity. Such perimeters help identify security issues related to the system. This information is helpful when identifying and quantifying cyberrisk.

A significant cyberrisk that has been of concern since 2020 is the supply chain attack. Such cyberattacks initially compromise the security of software solutions organizations offer their customers. Attackers then exploit the compromised solutions to launch cyberattacks against the customer organizations that have purchased the software. Thus, visibility of cyberrisk pertaining to one's own organization and across organizations in the supply chain is important. The availability and analysis of relevant external data helps assess and measure cyberrisk and CRQ pertaining to one's own organization and organizations in the supply chain.

When analyzing cyberrisk, whether within the supply chain or one's own organization, one may come across

many unique data elements or parameters that measure cyberrisk. While some of these represent a past event (i.e., lag indicator), others present a forward-looking scenario (i.e., lead indicator). A lag indicator measures an activity or event after it has occurred, while lead indicators attempt to predict or state the possibility of a future outcome. There is an interesting association between some lead and lag indicators as they relate to cyberrisk. For example, many organizations have effective vulnerability management programs (VMPs) that aim to identify and remediate vulnerabilities in the IT infrastructure and systems. The vulnerabilities identified represent a lag indicator, since the report is based on existing vulnerabilities. The information related to these lag indicators can be combined with additional data. The vulnerability data, when combined and corelated with data pertaining to external scanning attempts or unauthorized network connection, provide a very different kind of value. This information can be used to predict the possibility of future attacks perpetrated by exploiting vulnerabilities. The lead indicator provides quantifiable information and is of immense value for CRQ.

Conclusion

CRQ is important to organizations, since identifying and addressing sources of cyberrisk are fundamental to maintaining adequate cybersecurity. CRQ helps enterprises conduct a cybersecurity self-assessment and enables the prioritization of corrective actions. Measuring data elements using a mathematical measurement scale provides more objectivity than using a qualitative assessment that is subject to individual cognition. The various security tools implemented provide a rich source of data for the CRQ exercise. Along with internal data, external data sources can be effectively used to identify cyberrisk of one's own and of other organizations in the supply chain.

Considering the multitude of data sources, data elements, parameters and cyberrisk measures relevant to CRQ, organizing these elements into a CRQ dashboard can provide an effective monitoring and data visualization tool. Implementing CRQ requires persistent efforts, experience, expertise and a great deal of patience. Implementing CRQ is the best way forward for any organization that intends to build a sustainable, rational and demonstrable approach to cyberrisk management.

Culled from: isaca.org

Training on Cybersecurity - Cloud Security, Areas of Vulnerability, Challenges & Assurances held between August 30-05, 2021 in Conjunction with FITC.

Stakeholders Engagement with the management team of the Economic and Financial Crimes Commission (EFCC) in Abuja.

Open Banking and the Gatekeepers

Nigeria's financial inclusion target was 80% by 2020, but statistics at the end of December, 2020 revealed that only 64% of Nigerian adults were financially included. With current figures that 10% of the unbanked population have access to mobile phones and the internet, an increase in Fintech solutions is expected to reduce the number of persons without access to financial services. One of the critical drivers of financial inclusion is Open Banking.

Open Banking is a financial service term used to describe the use of open technologies by third-party providers to build applications for the financial space. It provides guide and standard format for a transparent and secured means of sharing data. Open Banking is to the financial industry what OSI (Open System Interconnectivity) model was to computer networking. Before the era of the OSI model, there was no standard handshake for data interchange between devices from different vendors. In Nigeria, It takes time and effort for a stand-alone Fintech to integrate with the core banking system of the whole commercial Banks in Nigeria. Developing an interface for each of the Bank with specific standards can delay the time to market. Open Banking is a paradigm shift to an open model of sharing data between data controllers and third parties within the financial ecosystem.

February 17, 2021, the Central Bank of Nigeria (CBN) issued a regulatory framework for open banking in Nigeria. This was long-awaited after several organizations like PWC and Open Banking Nigeria has written papers on a case for the adoption of Open Banking in Nigeria. Within 12 months, the CBN is expected to regulate the development of a common Banking Industry standard with technical design standards, data standards, information security standards and operational rules. The CBN framework fosters sharing and leveraging customer-permission data by banks with third-party firms to build solutions and services that provide efficiency, greater financial transparency, options for account holders, and enhance access to financial services in Nigeria.

According to the CBN regulatory framework, categories for open exchange of data and services are stated below:

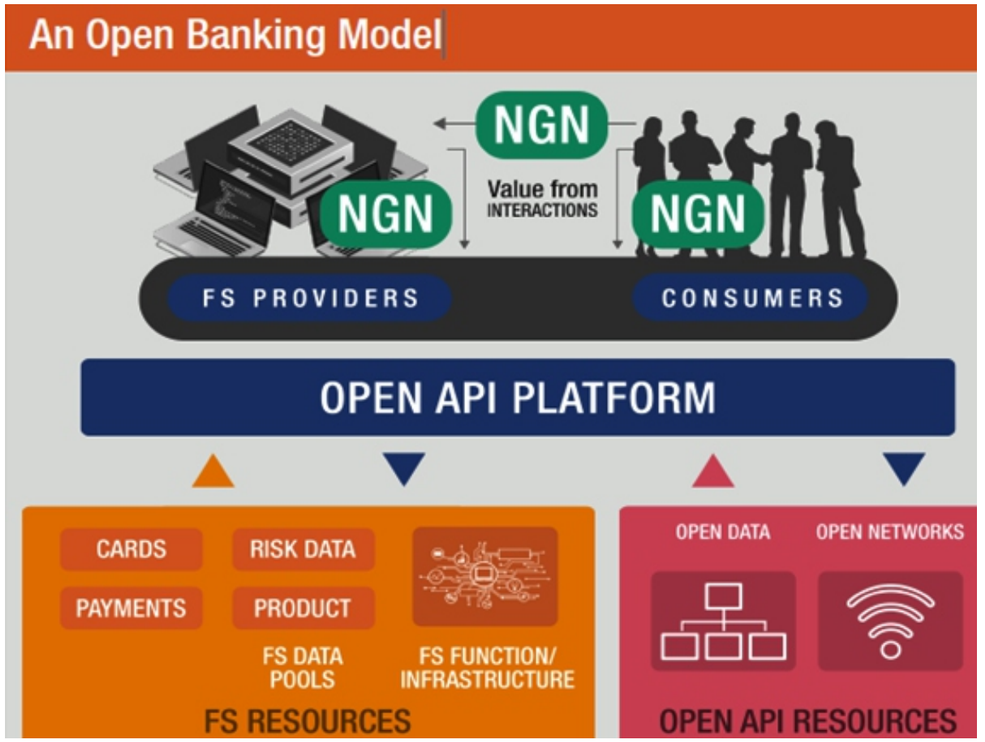
I. **Product Information and Service Touchpoints (PIST)**: This shall include information on products provided by participants to their customers, e.g. ATM/POS/Agents locations, channels (website/app) addresses, institution identifiers, service codes, fees, charges and quotes, rates, tenors, etc.

ii. **Market Insight Transactions (MIT)**: This shall include statistical data aggregated basis of products, services, segments, etc. It shall not be associated to any individual customer or account.

iii. **Personal Information and Financial Transaction (PIFT)**: This shall include data at individual customer level either on general information on the customer (e.g. KYC data, total number or types of account held, etc) or data on the customer's transaction (e.g. balances, bills payments, loans, repayments, recurring transactions on customer's accounts, etc)

iv. **Profile, Analytics and Scoring Transaction (PAST)**: This shall include information on a customer which analyses, scores, or gives an opinion on a customer e.g. credit score, income ratings etc.

The framework also defined risks ratings for categories of data to be exchanged and states requirements for classified participants in the ecosystem.



Open Banking is enabled by Application Programming Interface (API). An open exchange of data via API comes with risks, and it is the role of the "gatekeepers" to ensure the protection of information assets. Internal Audit as one of the gatekeepers is expected to provide the CIA's role of confidentiality, integrity, and availability as the Bank exposes her data to third parties. Below are best practices to mitigate API risk.

Inventory of API calls: The Bank is either receiving or giving out information for all API calls. Data Controllers like Banks should have an inventory of all APIs and what data is being received and shared with third parties. Reasons for the requested data must be stated and how the data would be processed. Gatekeepers must ensure availability and proper maintenance of API inventory. There should also be an API risk register that states all possible risks and mitigating controls.

Audit trail of API logs: There must be a log for all API calls. An audit trail must be available and compliant with the Bank's retention policy. Data analytics and fraud monitoring tools should analyze logs to detect suspicious trend. Setting alerts that trigger downtime and irregularity would allow the Bank to fix issues before they cause larger problems proactively. Errors in API calls need to be analyzed to trace the root cause.

Proper Encryption: Ensure adequate data encryption to avoid exposure of sensitive data to man in the middle attack. There should be data masking policies, and gatekeepers should ensure compliance.

Authentication and Authorization: Ensure compliance with the Auth 2.0 authorization framework, an open standard for authorization that enables third-party application access to protected resources. There must be an authorization server and ensure all API calls are authenticated and authorized at the authorization server before admission to the resource server.

Data Privacy and Protection Compliance: Nigeria Data Protection Regulation (NDPR) has a framework for data protection and privacy. Gatekeepers are to ensure that data exchange via API calls is compliant with NDPR. Availability of a privacy contract with a third-party data processor is not negotiable. All Banks should be ISO 27701 compliant, an extension to ISO 27001 for privacy information management.

Open Banking can be one of the biggest innovations to be introduced into the financial ecosystem in Nigeria. Still, if the gatekeepers do not play their role to protect information assets, open banking can be a gateway to disaster.

Nosa Omoruyi,
Internal Audit Group, Sterling Bank Plc

Things To Do and Not To Do After Taking Covid Vaccine

The pandemic has changed the way of life for most; outings, clubbing, partying can never be the same again. However, with the vaccine, life got easier.

The vaccine works as a preventive way to slow the surging pandemic, however, there are certain things that vaccinated people may be free to do which they previously could not because of the prevailing pandemic.

This does not mean that people who have taken the vaccine should be careless. Below are some things to do and not to do after taking the vaccine.

Not Using Mask

You are not considered fully vaccinated against COVID-19 until 14 days after your last dose of the vaccine, you still need to follow basic COVID-19 prevention guidelines. Even after that time, continue to wear a mask until there is a final solution to the Coronavirus issue, a mask is a must. Do not think that you are completely immune to COVID-19 after vaccination: No vaccine has a 100 percent success rate. You may contract COVID-19 even after being vaccinated but chances are the infection would be much milder. The vaccine only protects you from hospitalization, death, and serious disease.

Lose or throw away your vaccine card

If you need a second shot, you will have to show your provider the timestamp on your vaccine card, so you need to keep the card handy. Apart from the point mentioned earlier, public places and transportation, including airlines, may start to require some form COVID-19 vaccine documentation for safety.

Not Taking Water

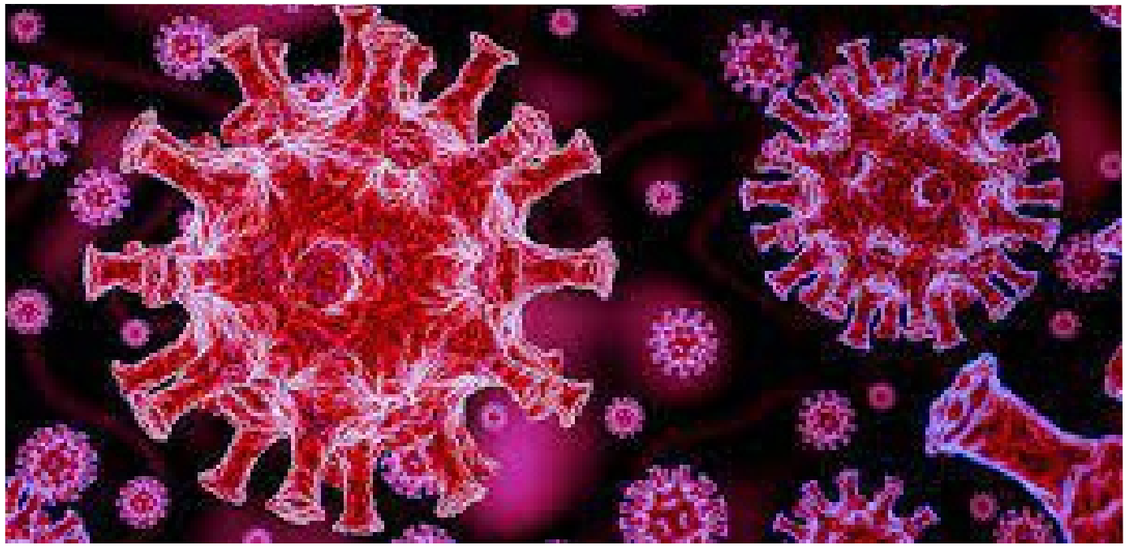
You need to stay hydrated after taking your vaccine; it helps keep you strong. Water helps your body process your body's immune response to the vaccine. Plus, if you do spike a fever because of the vaccine, staying hydrated will help your body fight it off.

Not Isolating

If you visit a high-risk area before taking the vaccine, you still need to self-isolate for 14-days after taking the vaccine. Taking the vaccine does not automatically clear Covid from your body system. And if you start having symptoms of Covid after taking the vaccine, you need to self-isolate and talk to your doctor.

Taking Alcohol or Smoking

According to UNICEF, although there are no approved



scie
ntific studies that quantify the effect of alcohol or smoking on vaccination, it is advisable to avoid tobacco or alcohol consumption as it may aggravate and worsen vaccine side effects making the experience more stressful and unpleasant. Alcohol also affects the body's immune system negatively and the immune response to the vaccine may not be as effective if there is excessive alcohol in the system. The same goes for tobacco consumption as well.

Eat a Well-balanced Diet

To avoid serious side effects, you need to eat a well-balanced diet. Superfoods like green vegetables, turmeric, and garlic, which are high in nutrients and boost immunity, should be included in your diet. Seasonal fruits rich in Vitamin C can also aid in fighting the vaccine side effects, this is essential both before and after taking the vaccine. Eating a well-balanced diet will help boost your immune system generally.

Get Enough Rest

When you get vaccinated, the body relies on immune responses to develop protection. It is advised that recently vaccinated people sleep for at least 7-8 hours as sleep deprivation can cause suppressed immunity since the body rebuilds its defence mechanisms during sleep. Not getting enough sleep can also trigger stress, which further suppresses the immune system. So get enough sleep and rest.

Apply a Clean, Cool, and Wet cloth (or some ice) Over the Arm

After the vaccination, to help reduce being uncomfort
able and pain, you can apply ice or a clean wet cloth. You can also do mild exercise or use the arm for light activities to further lessen the pain and discomfort.

Mothers Can Continue Breastfeeding

The antibodies produced through COVID-19 vaccination could pass to the babies though milk and it may also offer immunity to the baby like other vaccines given in pregnancy do. Pregnant women can also take the vaccine, as approved by the Ministry of Health and Family Welfare India and WHO.

Remember, keep safe and keep healthy.

Culled from: guardian.ng

Digital Identity and Future of Banking

INTRODUCTION

The emerging digital transformation in the banking industry is continuously changing customers' experiences. A great customer experience means convenience, real-time, and mobile-first.

There is consistent fast increase in adoption of digital life and smartphones. The global Covid-19 pandemic has enhanced the integration of the physical and digital economic domains. Digital identity therefore:

- ✓ Becomes a vital enabler for accessing online and on-demand financial services
- ✓ Offers consistent authentication and facilitates delivery of financial services, which require verification of identity
- ✓ Enables secure access to online financial services and ecosystem interactions customers, banks, telcos, FINTECH, merchants, regulators, and others

Hence, systematic customer profiling and associated privacy concerns have become major business concerns for the regulators, banks, and customers.

Digital Identity is defined as:

"An online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device. These users may also project more than one digital identity through multiple communities. In terms of digital identity management, key areas of concern are security and privacy." (**Techopedia)**.

"A collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions. A digital identity system refers to the systems and processes that manage the lifecycle of individual digital identities." (**World Bank**)

"A digital identity is a collection of features and characteristics associated with a uniquely identifiable individual stored and authenticated in the digital sphere and used for transactions, interactions, and representations online" (**https://learn.g2.com/).**

THE FINANCIAL SERVICES IN THE PHASE OF THE DIGITAL ECONOMY

- Rapid evolution in digitization, technologies and user behaviors are transforming the ways banks interact with their customers
- The online identity and behaviour have become pivot of the digital economy
- The identity management obligations are continuously changing.
- Banks are re-evaluating their role in the identity supply chain
- Effectiveness of customers' digital identity becomes a major concern for banks:
  - ✓ No standardized formats for digital identity
  - ✓ No standardized methods for verifying the source and integrity of digital credentials
  - ✓ The technological advancements have not addressed the concerns
  - ✓ Lack of official and foundational form of identification
  - ✓ Limited financial inclusions access digital financial services

SOME KEY FACTORS DRIVING THE DIRECTION OF DIGITAL IDENTITY

- Digital transformation
- Customer experiences
- Rapid adoption and migration to cloud services
- Privacy, security, and compliance
- Digital identity providers
- Geopolitical trends.
- Emerging technologies IoT, Blockchain, biometrics, AI, machine learning

SOME CONCERNS FOR DIGITAL IDENTITY IN FINANCIAL SERVICE DELIVERY

- Customers access financial services from multiple platforms, identities are becoming progressively more complex and expensive to manage
- Balancing Know Your Customer (KYC), Anti-Money Laundering (AML) regulations, and ensuring the safety of consumer
- Cyber-attacks are continuously threat to banks and their customers
- Consistent fast increase in adoption of digital life and smartphones has heightened the rise on the following:
  - ✓ The internet of things (IoT)
  - ✓ complexity in digitization
  - ✓ Proliferation of mobility
  - ✓ Hyper-connectivity alongside the thriving new risks and threats
  - ✓ Spread of untrusted digital identity
- The regulation protects the customers first amidst the fraudulent activities
- The banks are required to address the digital identity concerns

TECHNOLOGY DEVELOPMENTS IN DIGITAL IDENTITY MANAGEMENT

- Creation of smart digital first platforms that can deliver omni-channel, smart, modular, open banking services, and cross-channel connections
- Offer identity as a service flexible, scalable, and easy to integrate identity capable platforms
- The advent of distributed ledger technology (e.g., blockchain) and biometrics undertake innovative approaches to digital identity management
- Provision of user centric solutions with streamlined onboarding processes

- "Unique customer identity" system that enhances security, eliminates duplicate data, boosts efficiency, increases user satisfaction, and improves service levels
- Reduce average onboarding process time
- Eliminate business bottlenecks
- Measure onboarding satisfaction

- Measure customers' experience and service satisfaction
- Improve resistance to fraud and abuse
- Drive customer inclusions to conveniently assert their own identities through biometric recognition
- Channels for Unique Digital Identities are: ATM, Call Centre, Mobile Banking, Online Banking, Online Customer On-Boarding, Merchant Payments, Social media, etc.

RECOMMENDED PRACTICES IN DIGITAL IDENTITY MANAGEMENT

- Deployment of state-of-the-art secured technologies to ensure confidentiality, integrity, and availability of the digital identity
- Establish and verify unique identity for each customer to uphold trust and transaction security based on combination of:
  - ✓ What the customer knows (password, PIN, security code)
  - ✓ What the customer has (identity card, bank card, token)
  - ✓ Who the customer is (biometrics spanning physical/behavioural features)?
  - ✓ Where the customer is (mobile number, geo-location, IP address, social network site)
- Enable customers' identification, authentication, authorization, and accountability capabilities, leveraging on latest technologies such as biometrics, blockchain and AI
- Ensure compliance with data privacy, security, regulations, and seamless authentication experience
- Leverage on the intense emerging and disruptive innovation around financial services
- Collaboration among major stakeholders across segments for a broader digital service delivery adoption and trust
- Embed agile digital experiences into financial services to attract new customers and drive inclusion
- Exploit new identity sources, biometrics, and advanced analytics technologies to increase customer insight and service relevance, while reducing fraud, waste, and abuse
- Most importantly, drive customer awareness

THE FUTURE OF BANKING SERVICES

- The future growth of financial services requires the existence of dependable and resilient digital identity systems
- Development of new identity systems driven by emerging technologies such as blockchain, biometrics, and machine learning
- Innovative business models and ecosystem connections, seamless online experiences, all combined with enhanced security, privacy, and user control
- Dynamic online interactions among banks, customers, devices, data, locations, business processes, and regulators
- New digital trends in banking services – technologies, customers, regulations, etc.
- Emergence of password-less and biometric authentication systems
- Delivery of efficient, secure, digital-based Fintech services
- Leveraging on availability of mobile phones to enhance financial inclusions, financial services to non-financial sectors, and individuals
- Provision of affordable, secure, and convenient access to diverse range of authenticated financial products and services for individuals and SMEs
- Greater customers' control of personal finance, quick financial decision making, and the ability to make and receive payments within seconds

CONCLUSION

Digital Identity:

- Is a vital enabler for accessing online and on-demand financial services.
- Offers consistent authentication and facilitates delivery of financial services that require verification of identity.
- Enables innovation with enhanced data access, safeguard and share privacy to only trusted parties.
- The frontier of privacy and security in the digital world
- With digital identity, banks will become a bigger player in financial inclusion.

Dr. Frances Nkechi Undelikwo
Group Head, Information Systems Audit
Fidelity Bank Plc

How Internal Auditors Can Redefine Audit Experience for Improved Organizational Performance

Introduction

More than ever, periods of audit exercises are now characterized as 'panic moments' in many organizations. The relationship between internal auditors and their fellow employees has been seared with fear and suspicion. This apparently impacts on the quality of audit outcomes where employees do not trust the rationale behind the efforts of their auditors. This articles expounds on the underlying causes of such distrust and discoordination in the relationship between the internal auditors and their auditees, and how internal auditors can redefine such experiences and build cohesion for improved organizational performance.

The Need to Redefine Audit Experiences

During audit periods, there are usually various mindsets and attitudes held by both auditors and their auditees that hamper the successful execution of the audit exercises, resulting in outcomes that are not beneficial to the auditors, the process owners and the entire organization. These issues are presented below, alongside recommendations to avert further occurrences of those instances within organizations.

1. Conflicting Mental Dispositions of Auditors and their Auditees

In many cases, there are two major conflicting mental dispositions held by internal auditors and employees which sabotage the openness and trust that could have been built between both parties. On one part, many internal auditors assume there are cover-ups in the work done by employees to exonerate themselves from audit troubles. On the other hand, employees believe auditors are mainly on the lookout for issues in their work or processes to advance the recognition or validation of their competence.

Because of this disconnect in the relationship or cooperation between internal auditors and their auditees, organizations are robbed on many opportunity areas and experiences that could foster organizational excellence and ultimately, industry competitiveness. Yet, cooperation between both parties would mean there is a free environment where corresponding flow (giving and receiving) of feedback or recommendations thrive to facilitate creation of more efficient processes. Through open and participatory audit dialogues of this kind predicated on trust and cooperation, opportunities around latest trends in innovation can be uncovered, freeing up pathways for organizations to adapt quickly and be ahead of the industry.

Hence, if organizations will lead the pack by building an unparalleled measure of efficiency in their internal systems or become early arrivers to the future of their industry, this shift in audit relationships from a stance of mutual suspicion to mutual trust or cooperation is vital.

2. Flawed Audit Rationale of the Auditors

Some organizations primarily gauge the performance of internal auditors by the number of gaps uncovered, which drives many auditors to the radical extremes of faultfinding. In this case, internal auditors perform audits solely to churn out gaps even in pristine processes since there is an inherent need for their competence to be recognized and validated.

Yet, this approach is pernicious and could be frustrating to auditees as it seems no amount of due diligence or alignment to standard practices will ever be adequate to tighten their grip on processes within their control. This ultimately could lead to future indifference or resistance in some cases from process owners against the efforts of the internal auditors.

Thus, internal auditors must make audit purposes and benefits clear to the process owners at the beginning of audit exercises to dissolve any ambiguity from the minds of the owners. As much as possible, meaningful and value-adding recommendations must also be provided by internal auditors for all issues uncovered during audit exercises. This gives process owners a first-level confidence that internal auditors sufficiently understand the processes and furthermore, an assurance that the audit carried out is in line with expected standards; hence, exercises were executed objectively and professionally. There is also an engendered trust in the minds of the process owners that the audit exercises were conducted to add value to their work, foster a culture of continuous improvement and perhaps, open more windows of opportunity for new innovation - but not solely for faultfinding.

3. Superiority Complex of Internal Auditors

Many internal auditors have a rather skewed outlook about themselves. As their roles within organizations many-a-time give them the power to vet work done across many functions against the standard procedures, they can develop a sense of superior power over their counterparts. Usually, if this audit power is not properly managed, it can unsettle or threaten fellow employees.

In reality, the audit function is just a role - a function almost like any other. For instance, the absence of a strategy in an organization would imply the absence of organizational direction or at the minimum, there will be no tactical approach to navigate the waters in the short or medium term. An incompetent finance department may result in massive financial loss to an organization. Inadequate operational competence will result in lagging operations, thus curbing the revenue power of an organization; incompetent legal/compliance team may subject an organization to the jeopardy of regulatory infractions, and so on. And since the corporate environment works as a system, any lagging part affects the whole. Thus, no function is indispensable or overly superior. As every employee must competently and adequately carry out their duties, so the internal auditor must ensure that every process is implemented at an optimal level. This must also be with a view to ensuring functions are operating in line with best practices.

Ultimately, the feeling of superior power which comes with carrying out audit responsibilities is only an imaginary impression. Hence, internal auditors must cure themselves of the mental disposition of audit powers while sticking to the core ethics of objectivity and professionalism.

4. Performance Fears of Employees

For fear of negatively impacting on key performance indicators (KPIs), and to assume a sense of satisfaction that duties are excellently performed, employees would rather pray for process gaps within their control areas to go undetected. Where detected, their backs are turned against the auditors, sometimes in vicious defense of their work, resulting in a blind eye on what they could have done better or how.

Chief Internal Auditors within organizations should develop a system to encourage heads of all departments or functions to educate their teams (all employees) on the critical importance of familiarizing themselves with the standard operating procedures or practices required of their functions, alongside every policy that guides their work. Negligence of employees can be rampant in this area due to inattention to those practices and policies. As a result, most defects are identified here and are flagged during audit exercises.

In addition, employees should be encouraged to develop a personal culture of ownership on the job, which inspires proactiveness. This attitude helps employees preempt process or operational gaps ahead and tackle them headlong before audits are carried out. Employees who take ownership understand that self-auditing should be an essential part of their work. Hence, they perform their duties with the understanding of applicable standards and policies in mind which helps them perform constant audit health-checks on their work to ensure execution is in line with defined procedures. When executed tasks seem incongruent with defined standards, they realign and cure the issues where necessary and save themselves the humbling pain of a yellow card (medium risk) or red card (high risk) from the umpire the internal auditor during audits.

Conclusion

In an ideal 21st century work environment, panics should not be associated with audit periods. Audit exercises should be a moment of openness and trust among auditors and their auditees. It should be a huge window for transformational improvements within organizations and this could happen if internal auditors can take further steps to adopt the recommendations contained in this article as they find relevant to their various organizational contexts.

Ayobami Onakomaiya
(Internal Audit Management Trainee)
Development Bank of Nigeria

The Need for Continuous Digital Awareness and Security

The digital world! A space where millions of people get connected globally, billion-dollar transactions being consummated in seconds and countless interactions between individuals from all walks of life.

Flashback five decades ago, before the advent of the internet, the world moved at the pace of a snail, however it is without doubt that the level of cybercrimes was low. We cannot disagree that improvements in online technologies have brought cybersecurity challenges that barely existed before.

Continuous sensitization about cybersecurity risks seems like an over flogged topic, but it's significance cannot be overemphasized. According to a February 2018 report by the Center for Strategic and International Studies, Cybercrime costs almost $600bn worldwide, that's about 0.8% of world GDP. Some of us may think we have gotten to a level where it is impossible to fall victim, but our Personally identifiable information (PII) may be compromised without even knowing.

Also, the advent of Open-Source Intelligence (OSINT) has made information publicly available to both good and bad users. For example, a company trying to recruit over social media can contact you via your email or phone number because it is publicly available while a black hat hacker may maliciously contact you for the purpose of extracting more PII for fraudulent purposes. While it is beneficial to connect with other users over the internet and through social media, it is more important to take necessary steps and precaution in our online activities. Below are some techniques used by cyber criminals to extort personal information for suspicious purposes:

Data Scraping

Have you ever gotten spoofed mails or calls from unknown persons trying to phish your data? Chances are your data was scraped from your social media; however, this does not necessarily mean that you were careless with your personal data. Data scraping is the process of extracting data from websites without the explicit permission of the individual whose data is being scraped.

These may include email, phone number, birth date, current city, organization, spouse, or partner details. In early 2020, a vulnerability that enabled seeing the phone number linked to every Facebook account was exploited, creating a database containing the information of 533 million users across all countries. Another data scrape was discovered in July 2021 when threat actors posted the personal data contained in 700 million LinkedIn user profiles in the RaidForums underground market.

Information gotten from this data scrape can then be used to perform different attacks like phishing, brute force, ransomware etc. While we might not be primarily responsible for our data being scraped, we cannot deny the impact if the attackers perform a successful attack from the personal information gotten.

Unsecured Website

Data protection regulations i.e GDPR and NDPR outline the need for protection of user data. Some websites collect personal information such as computer or phone's technical configurations, previous sites visited, IP address, location etc. Cookies are also used to collect information about the user visiting the website, these are unique to your computer and can be traced back to you.

For instance, a website without a proper Secure Sockets Layer (SSL) Certificate can create an unsafe connection for the user which can lead to a man in the middle attack. Also, there are open-source tools which hackers use to collect data from websites that are unsecured.

The easiest and simplest way of determining an unsecure website is to check the website URL as it will start with HTTP instead of HTTPS. You can also get a prompt from certain browsers like chrome about the insecure connection. Before giving out sensitive information such as emails, credit card, username, and password, it is best to do a quick check.

Malwares

While surfing the web, you may have come across an ad for a software available for free download or received a crafty email from the supposed Chief Financial Officer of your organization with an attachment. Both these scenarios are samples of ways by which viruses are transmitted into our computers.

Files that look legitimate can be purposefully infected with malwares, this can come in different forms including spyware, trojan, worm, rootkit, bots etc. There have been many successful attacks which have utilized malware to compromise systems and assets - some examples are the AET Attack (Amsterdam 2012) and the USB Attack (London 2011).

It is reported that malware accounts for two third of the world data breaches as attackers develop malicious code or tactics to get unauthorized access to people's data stored on their computer or mobile devices. It is therefore imperative for users to protect sensitive information on their systems by staying clear of viruses.

Are there remedies?

Having considered some causes of data leakage and breaches, below are a few tips for protecting your

Personal Identifiable Information, including the organization you work for:

1) To prevent a successful data scrape, leave out personal information not explicitly required on your social media. i.e. phone numbers, organization, official email address, date of birth etc. This will reduce the chances of being spoofed.

2) Change your social media passwords regularly or when you notice any suspicious activity.

3) Utilise open-source tools to check if there has been a breach on your email or phone number. You can do a quick check on Haveibeenpwned.com, Social recon, Goolag scanner.

4) As an administrator, ensure that your website is secured. If not, purchase an up to date SSL certificate.

5) There are free open-source intelligence (OSINT) applications that can be used to verify the security of a website if you are unsure about the safety of your information. Spiderfoot, screaming frog, Shodan, Paliscope etc.

6) Constant training and awareness for employees about cybersecurity and the need for data protection.

7) Tighten your network security by making use of a firewall to prevent unauthorized access by users outside your network.

8) Ensure appropriate security measures have been implemented to protect data including encryption and storage.

9) Purchase a robust anti-virus software and make regular updates and patches.

10) Also configure your antivirus software to automatically scan downloads before files are stored on your computer.

In conclusion, it is important to note that continuous awareness and security consciousness is important in our every day cyber-life. In the words of Mark Bouchard (CISSP), a hacker with persistence only has to be successful once, whereas your defence has to be successful every time.

Adedeji Adeboye ACA, ACIB, CISA, CCSP
(IS Auditor, Development Bank of Nig. PLC)

Collaboration as a Control

A CISO and a Senior Audit Leader discuss how a good rapport between information security and internal audit can improve organizational cybersecurity.

One of the features of The IIA's Three Lines Model is its clear description of accountability among key players within an organization. The governing body is responsible for organizational oversight, management is tasked with achieving organizational objectives, and internal audit's role is to provide assurance and advice. The model also points out that this *delineation* does not imply *isolation*. Among all roles, "the basis for successful coherence is regular and effective coordination, collaboration, and communication," the model states.

This idea of teamwork boosting organizational objectives is backed by empirical evidence. A 2018 study by Arizona State University, the University of Nevada, the University of Massachusetts Amherst, and Iowa State University shows that a positive relationship between internal audit and information security can improve an organization's cybersecurity efforts. For instance, the findings indicate that stronger relationships between the two functions results in better detection of security incidents, internal control weaknesses, and incidents of noncompliance.

At Cboe Global Markets Inc., Umesh Yerram, chief information security officer (CISO), and Heidi Zenger, senior director of internal audit, demonstrate how a successful relationship between information security and internal audit works in practice. As a global exchange operator with 21 markets offering options, futures, equities, and foreign exchange products that trade billions in contracts daily, Cboe is naturally focused on cybersecurity as a critical risk. Yerram, based in Philadelphia, and Zenger, who works in the Kansas City, Kan., metro area and heads up IT audit, discussed how a strong collaboration between information security and internal audit helps them amplify their findings and better mitigate cyber risk.

How did the working relationship between your functions evolve?

Zenger One pivot point was hiring an auditor with

specialized security skills. As auditors, we say that a process is a process; we can understand all of the risks if you have the time to dedicate and teach us. But there really is a place for specialized skills; so I think that helped [enhance] our relationship quite a bit. After Umesh joined the company as CISO, I think the next real pivot point was the security team stepping into more of a second-line monitoring role. There's still some first-line activities, but by increasing that second-line monitoring role, it just brought us a little bit closer to speaking the same language from a risk management perspective.

Yerram I joined Cboe in January, and the relationship between Heidi's team and my team has definitely expanded over the course of seven months. We have clear role responsibilities; I am part of the second line, and internal audit is the third line. But at the end of the day, we are both trying to make sure that cyber risk or any other risk is properly identified, addressed, or brought to leadership's attention. That's been our goal and what we've been doing from day one. We want the board to hear the same message, whether it's coming from me or it's coming from internal audit. Heidi and team present to the audit committee, and I present to the risk committee and, of course, to the full board so we want to make sure that we convey the strong collaboration between our two functions.

Another thing that helps us build that strong relationship is to Heidi's point: Heidi has a resource who is a cyber specialist, so we can actually speak the same language. [The specialist] does work behind the scenes to make sure Heidi and team are aware of some of the technical nuances that need to happen in remediating. Now it's a lot more streamlined to have those conversations without any barriers. So that definitely helps.

To what extent is that relationship formalized?

Zenger Umesh has a security governance team within his group. The security governance team and our IT audit team meet on a monthly basis to talk through risks, monitor any issues or vulnerabilities, and discuss any upcoming audits. Umesh and I meet one-on-one on a monthly basis, as well, to talk about the same things on a slightly higher level, and Umesh also meets with our chief audit executive once a month to make sure that we're communicating with each level of the organization.

In addition, the company has a formal weekly project management meeting where we discuss the status of larger projects within the organization, as well as approve any new ones coming on board. This gives audit and security an opportunity to say, "Hey, we need to be involved in this, and we want to review the risks before this is approved and moves forward." Or if we've identified anything with the ongoing projects, we have an opportunity to voice those concerns upfront.

Yerram I also have a security council meeting that Heidi participates in, so that's another touch point where she and I have conversations about cyber risk. We use some of the open findings from internal audit that Heidi's team presents, so that our chief operating

officer and chief risk officer understand the audit items that are coming to them, along with any delays or risks that we need to highlight at that point. We want to make sure that leadership is aware of the progress on a monthly basis before we present to the board on a quarterly schedule.

How do your teams collaborate?

Yerram If two teams have two different messages, that creates confusion, and then, how do you prioritize the risk? But with the relationship we have, the expertise internal audit has, and the communication we have established, it helps us to really get on the same page. So we have those conversations regularly and say, "OK, we've identified 10 risks, but what are the top three, four, or five that we can actually bring to senior leadership's attention? Then when we are aligned and we go and make that case together, it definitely gets heard and reacted upon. I think one of the biggest benefits of our collaboration is that now we actually prioritize the highest risks for the company from a cyber perspective.

Zenger The security team conducts its own security risk assessment based on all of the input and data they're receiving from their tools and an awareness of external threats. The security risk assessment serves as one of the inputs we can use in the internal audit risk assessment, which is our own independent perspective of risks throughout the company. And then, similarly, as we have audit issues and findings that we're aware of and that we include in our reports, that's one of the things the security team can pick up and use to inform its security risk assessment. So it's a two-way street from that capacity. I also see a lot more of the information sharing occurring across the teams now where we say, "OK, we identified these vulnerabilities or risks and we're seeing this on our side. What are you seeing through all the monitoring activity that you're doing and how does that inform each one of our programs?'

What has been the impact of the relationship on your organization's cybersecurity efforts?

Yerram A good measure for us is patch management. I talk to my peers constantly and it's not a very exciting piece of work to do. Nowadays, given the onslaught of zero day [attacks] and the vulnerabilities that threat actors are exploiting, it's not on the top of everybody's priorities to go patch the system. By working together on this risk, we significantly improved our ability to patch, to align with our changing risk profile. We now have more resources and awareness from the senior leadership that this work has to be done, based on the risk that we articulated.

Zenger Cboe recently invested in a leadership training program, and I believe that has helped us foster and maintain a healthy relationship. We don't always see eye to eye. I see things through an audit perspective; I view the world based on the evidence of the body of work and conclusions we're reaching. And Umesh sees the risk to the organization from the outside and from a cyber perspective. We do have a lot of challenging conversations, and I think that's to our benefit. In our training, we call these kinds of conversations "crucial conversations." We have these crucial conversations on a regular basis and that's good, because if we weren't having them, that means we're afraid to bring up those differences in opinions, and the organization suffers as a result of the lack of conversation and challenge. Umesh called me one day after having a conversation the previous day, and just as he started it out, I paused and said, "Umesh, are we having a crucial conversation right now?" and he said, "Yes, exactly!" And so, by knowing that we were going into an important conversation, we could both relax. We could both appreciate the idea that, "We've got to do some hard work today and we can tackle it together."

Culled from: iia.org

Financial Reporting During the Pandemic

A new study spotlights how the crisis is impacting financial misstatement risks and internal control audits.

As the vaccine roll-outs raise hope that COVID-19 will subside, auditors may question how the pandemic has impacted financial statements. There are many views regarding how the crisis has changed the world and whether these changes are permanent.

The risk environment definitely has changed. Specifically, there may be greater risk of material misstatements in financial statements, according to our study, "COVID-19 and the Accounting Profession," published in May in the *Journal of Accounting, Ethics, and Public Policy*. Internal auditors should consider how to incorporate the impact of changes driven by the pandemic on accounting processes into their risk assessment and planning for audit programs and work.

Survey Findings

The study surveyed 139 accountants in the U.S. to gain broader insights into their work during the pandemic. Respondents who perform external audits disagree with the notion that the crisis will lead to an increase in earnings management or attempted fraud. Although this finding may reflect respondents' beliefs that stakeholders will be more forgiving of reduced earnings, management may have greater incentive to manipulate earnings during the pandemic.

Regardless, the finding suggests that external auditors may be less likely to change their audit procedures to identify and assess changes to risks of material misstatements brought on by the pandemic. Internal auditors should consider the impact of a higher risk of material misstatement in their audit work.

Ironically, survey respondents also agree the crisis will reduce the effectiveness of internal controls and make it more difficult to audit them. Taken together, these findings suggest that financial statements prepared and audited during the pandemic are

susceptible to higher risks of material misstatements. Additionally, while some impacts of the crisis on the internal control environment may be permanent such as remote work organizations may need to modify existing internal controls and internal audit techniques to accommodate the post-pandemic paradigm.

The Impact on Control

When internal controls designed to prevent and detect financial statement errors and fraud fall short, detection mechanisms such as reconciliations of accounts and internal audits serve to catch those errors and fraud. External audits add a layer of protection to prevent material misstatements.

However, both the prevention and detection features of internal controls are susceptible to weakening due to systemic organizational changes in response to the pandemic. Organizations and their auditors were not prepared for the dramatic and immediate implications and ramifications of living and working through a global health crisis.

Unforeseen economic hardships and physical limitations forced organizations to reallocate resources. People and other resources that had been directed toward internal controls were reallocated to other business functions deemed more critical for survival. As an anonymous auditor commented, "Clients were 'distracted' by the pandemic and therefore providing us with information became low priority." In short, internal control environments were impaired.

Employees' execution of internal control activities also was affected by work-at-home limitations and distractions, coupled with the stress caused by the pandemic. The study finds that the pandemic has impaired the quality of external auditors' work. One auditor explains the downsides of working from home: "It is taking longer to produce work, especially administratively. The office equipment at home, such as printers and scanners, is not as fast as the office equipment at the job office. … People have families and kids who can be a distraction and do not necessarily allow for everyone to be available at the moment you need them."

Audit Difficulties

Specific preventive activities embedded in internal

controls also have been impacted. Because of limited workplace access, the ability to separate certain duties has been reduced. Physical access to workplace areas and resources may be restricted to fewer individuals to decrease COVID-19 spread. Physical restrictions to inventory and other assets may be lifted out of necessity, as only a few, select individuals report to work in person. Without the watchful eyes of fellow employees, the ability of internal controls to prevent error and fraud may fall short on other fronts, as well.

Regarding internal controls aimed at error and fraud detection, employees without sufficient home office equipment may be unable to reconcile accounts remotely. Without co-workers in the same room during internal audits to brainstorm or answer questions, a full evaluation and assessment of the effectiveness of internal controls may be limited.

Unable to conduct physical walk-throughs of accounting departments and manufacturing plants,

noncompliance issues that would have been detected in person may go undetected. Another survey participant says the pandemic caused "difficulty being efficient as an audit team when not working on the client premises and face-to-face. Internal control walk-throughs (inquiry, observation, inspection) are more difficult when done remotely, as are fraud discussions (harder to coordinate and to physically inspect and observe)."

Other Audit Risks

While respondents agree that the pandemic has made it harder to determine the effectiveness of clients' internal controls, the study also finds that assessments of going concern questions could be more difficult. However, the study did not find that the pandemic increases risk in all areas of financial audits. For example, respondents neither agree nor disagree that the pandemic:

- Will make it more difficult for auditors to determine whether clients' accounting numbers reflect the economic reality of underlying events and transactions.
- Will lead clients to engage in greater earnings management in their financial reporting.
- Will increase the risk that auditors will not be able to detect material misstatements due to fraud in the financial statements and footnote disclosures.
- Will make it more difficult for auditors to determine whether management has disclosed every important item to investors and creditors in the financial statements so users can make informed, strategic decisions.

Because the study did not find that the pandemic increases risk in these areas, internal auditors need not change their risk assessments with regard to valuations, earnings management, fraud, or full disclosure.

Immediate and Future Implications

Financial statements prepared and audited during the pandemic will undoubtedly reflect business results differently than preceding financial statements. It will be difficult to disentangle the financial implications caused by crisis-related economic hardships from errors or fraud attributable to weakened internal controls. Economic indicators determined using financial statements prepared and audited during the pandemic should be addressed with caution.

Although it is uncertain when organizations will revert to previous activities, there could be permanent shifts in work habits on the other side of the pandemic. With the crisis shining a spotlight on the susceptibility of internal controls to work disruptions, internal auditors must learn how to provide assurance over financial reporting and other internal controls in a post-pandemic world. As organizations re-examine their long-term strategic plans, they must revisit internal controls and devote time, money, and reorganization to these critical safeguards.

Culled from: iia.org

Access Bank Plc
Yinka Tiamiyu
Plot 999C Damole Street,
Victoria Island, Lagos
tiamiyuy@accessbankplc.com
08023220367, 2364062

Bank of Agriculture Limited
Daniel Olatomide
1 Yakubu Gowon Way
Kaduna.
d.olatomidei@boanig.com
08067007183

Bank of Industry Limited
Yemi Ogunfeyimi
23, Marina
Lagos.
yogunfeyimi@boi.ng
08033059361

Central Bank of Nigeria (CBN)
Lydia I. Alfa
Plot 33, Abubakar Tafawa Balewa
Way Central Business District,
Cadastral Zone, Abuja,
Federal Capital Territory, Nigeria
lialfa@cbn.gov.ng
08033177216

Citibank Nigeria Ltd
Bolaji Ajao
27 Kofo Abayomi St
Victoria Island, Lagos
bolaji.ajao@citi.com
Tel: (234)1 2798400, 4638400 Ext. 8446
DL: (234)1 2798446, 4638446.
Mobile - 07057878877

Coronation Merchant Bank Ltd
Dele Dopemu
10, Amodu Ojikutu Street
Victoria Island,
Lagos.
ddopemu@coronnationmb.com
01-4614892, 07034109732.

Development Bank of Nigeria
Joshua Ohioma
The clans place
Plot 1386A Tigris Crescent,
Maitama, Abuja.
johioma@devbankng.com
08129145586

Ecobank Nigeria Ltd
Felix Igbinosa
21 Diya Street, Gbagada
Lagos
FIGBINOSA@ecobank.com
07068754692 ; 08023633203
D/L: 01 2260449

FBNQuest Merchant Bank Limited
Dr. Romeo Savage
18, Keffi Street, Ikoyi
Lagos
Remeo.Savage@fbnquestmb.com
01-270-2290 Ext-1245
08023551492

Federal Mortgage Bank of Nigeria
Wakeel Imam Galadanci
Plot 266, Cadastral AO, Central
Business District
P.M.B 2273, Abuja
wakeelimam@yahoo.com
08023040123, 01-4602102

Fidelity Bank Plc
Ugochi Osinigwe
Fidelity Bank Plc.
2, Adeyemo Alakija Street, V/I, Lagos.
ugochi.osinigwe@fidelitybank.ng
08023030298, 08092147012.

First Bank of Nigeria Ltd
Uduak Nelson Udoh
9/11, McCarthy Street, Lagos
Uduak.udoh@firstbannigeria.com
01-9054583, 08022902268

First City Monument Bank Ltd
Adebowale Oduola
10/12 McCarthy St,
Lagos.
Adebowale.Oduola@fcmb.com
01-2912276(D/L) 08034468071

FSDH Merchant Bank Limited
Dare Akinnoye
Niger House (6/7 foors)
1/5 Odunlami St, Lagos
dakinnuoye@fsdhgroup.com
08022017090

Greenwich Merchant Bank Ltd
Rasaq Alawode
Plot 1698A Oyin Jolayemi Street,
Victoria Island, Lagos
rasaq.alawode@greenwichbank
group.com
08083248797

Guaranty Trust Bank Plc
Lanre Kasim
178, Awolowo Road, Ikoyi, Lagos
lanre.kasim@gtbank.com
08023020839

Heritage Bank Ltd
Soridei Seba Akene
130, Ahmadu Bello Way,
Victoria Island, Lago
Soridei.akene@hbng.com
08037025486

The Infrastructure Bank Plc
Sadiku Ogbhe Kanabe
Plot 977, Central Business District
(Adjacent National Mosque)
P.M.B 272, Gark
F.C.T, Abuja
Nigeria.
skanabe@tibplc.com
08033039481, 08056900079

JAIZ BANK PLC
Abdullahi Usman
No. 73 Ralph Shodeinde Street,
Central Business District,
P.M.B. 31 Garki Abuja,
Nigeria.
ABDULLAHI.USMAN@jaizbankplc.com
09-4605138, 08032089010,
08086103555

Keystone Bank Limited
Abiodun Okusami
707 Adeola Hopewell Street,
Victoria Island, Lagos
biodunokusanmi@yahoo.com
08033534920

NEXIM BANK
Mr Ichide Friday
NEXIM House
Plot 975 Cadastral Zone AO,
Central Business District,
P.M.B. 276, Garki,
Abuja, Nigeria.
akpofureif@neximbank.com.ng
07085122928.

Nigeria Mortgage Refinance Company
Olusemore Adegbola
No 18 Mississippi Street,
Off Alvan Ikoku Way
Maitama,
Abuja, Nigeria
oadegbola@nmrc.com.ng
08033769975

Nova Merchant Bank
Ifeatu Onwuasoanya
23, Kofo Abayomi Street
Victoria Island, Lagos.
Ifeatu.onwuasoanya@novambl.com
08024114481

Polaris Bank
Olurotimi Omotayo
3 Akin Adesola St
Victoria Island, Lagos
romotayo@polarisbanklimited.com
08023096373

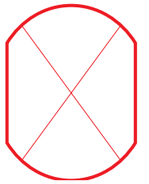
Providus Bank Ltd
Aina Amah
Plot 724, Adetokunbo Ademola Street
Victoria Island,
Lagos.
aamah@providusbank.com
08029087442

Rand Merchant Bank
Femi Fatobi
3RD Floor, Wings East Tower,
17A, Ozumba Mbadiwe Street
Victoria Island, Lagos
Femi.fatobi@rmb.com.ng
01-4637960, 08028514983

Stanbic IBTC Plc
Abiodun Gbadamosi
Plot 1712, Idejo Street
Victoria Island, Lagos
Abiodun.Gbadamosi@stanbicibtc.com
07057215563.

Standard Chartered Bank Nig. Ltd.
Emeka Owoh
142, Ahmadu Bello Way
Victoria Island, Lagos
emeka.owoh@sc.com
08037027452

Sterling Bank Plc
Cyril Osheku
1st Floor,
Sterling Bank Plc Head Office
(Annex), Ilupeju
239/241, Ikorodu Road, Lagos.
Cyril.osheku@Sterlingbankng.com
08023046639, 08056656866



SunTrust Bank Nig. Ltd.

1, Oladele Olashore Street,
Off Sanusi Fafunwa Street,
Victoria Island, Lagos

TajBank Nigeria Limited
Aminu Habu Alkassim
Plot 72, Ahmadu Bello Way,
Central Business District,
Abuja.
aminu.alkassim@tajbank.com
08032868266

Union Bank of Nigeria Plc
Prince Akamadu
36 Marina,
Lagos.
Poakamadu@unionbankng.com
08037649757

United Bank for Africa Plc
Gboyega Sadiq
UBA House
57 Marina, Lagos
gboyega.sadiq@ubagroup.com
08025011046

Unity Bank Plc
Olusegun M. Famoriyo
Plot 290A, Akin Olugbad Street,
Off Adeola Odeku Road,
Victoria Islan d, Lagos
ofamoriyo@unitybankng.com
08023145535

Wema Bank Plc.
Adekunle Onitiri
Wema Towers
54 Marina, Lagos
adekunle.onitiri@wemabank.com
+234 1 4622364, 08022245818

Zenith Bank Plc.
Mogbitse Atsagbede
Plot 84 Ajose Adeogun St
Victoria Island, Lagos
mogbitse.atsagbede@zenithbank.com
08023270998