Kingsgate Advisors Institute

kingsgate Brief

Topic:

Cybersecurity in an Evolving Digital Economy:

Why it Matters Now More Than Ever

Kingsgate Advisors Institute Podcast

Kingsgate Brief

EPISODE 3

JUNE, 2025

Topic: Cybersecurity in an Evolving Digital Economy: Why it Matters Now More Than Ever

Guest:

Funmilayo Akinti
Founder, Saberlight Tech secure Systems

Host:

Kechiro Ambro-Moye
Young Scholar, Kingsgate Advisors Institute

EPISODE SUMMARY:

This segment discusses the current state of cybersecurity, how it can affect economic outcomes, and what a strong cyber policy should look like for individuals, businesses, institutions and government.

Kechiro Ambro-Moye: Hello everyone, welcome to the Kingsgate Brief, where knowledge meets impact. I am Kechiro Ambro-Moye, I am a Young Scholar here at the Kingsgate Institute, and I'll be your host for today's episode. If you're tuning in for the first time or you've been with us from the very start, we're glad to have you.

And if you haven't already, I highly recommend checking out our previous episodes, they are filled with powerful insights and they are absolutely worth your time. In today's episode, we are going to be doing a dive into the world of cybersecurity, not just as a tech issue, but as a major economic, developmental, and even national security concern. To discuss this, I have with me a seasoned cybersecurity specialist, and I'll be revealing her profile very shortly.

So basically, in this episode, we'll be talking about our hyper-connected world as of today. From mobile money to online government services, our lives have been increasingly lived and exposed online. And while digital transformation brings great opportunities, it also has its own downside.

And that's why cybersecurity matters more now than ever in our ever-evolving digital economy. So cybersecurity isn't just about firewalls or passwords, it's about national security, it's about economic stability, investors' confidence, public trust, and long-term development, especially in regions undergoing rapid digital transformation like the global south. But as we connect more, we'll also become more vulnerable to these cyberattacks, and they aren't just disrupting hospitals or bankrupting small businesses; they are shaking investors' confidence as well. And they are even compromising entire governments. So what happens when a hospital is hacked? What happens when a small business loses its customers' data? What's the cost of a breach of a country's rep - utation or investors' confidence? And most importantly, how can we prevent these things from happening in the first place? So to unpack all of this, I have with me our very special guest, Ms. Funmi Akinti.

Ms. Funmi is a seasoned IT and business operations leader with over a decade of experience driv - ing strategic growth across the finance, telecom, and energy sectors. As the founder of Saberlight Tech Secure System, she's passionate about cybersecurity, risk analysis, and aligning technology with business outcomes. Known for her sharp strategic insights and deep technical expertise, she has led major enterprise deployments for organisations like the CBN, NNPC, and the First Bank. She's also an advocate for women in STEM and a strong voice in Africa's evolving tech ecosystem. Ladies and gentlemen, please join me in welcoming Ms. Funmi. Good evening, Ma, and thank you for joining us today.

Mrs Funmi Akinti: Good evening. It's my pleasure to be here today. Thank you for having me.

Kechiro Ambro-Moye: Thank you so much, Ma. It's truly a pleasure to have you here today. So now in our world today, we hear a lot of buzzwords about things like digital transformation, innovation, and even disruptions. But beneath all this excitement is something very quiet that is not spoken much about, and that is the urgent conversation about cybersecurity. And I think for a lot of peo - ple, cybersecurity only becomes a topic of interest when something goes wrong, like when there is a system crash, a data breach or a headline about a major hack. So I would like us to start this conversation from a broad angle, from your own point of view.

How would you describe the current state of cybersecurity globally today, especially in the con - text of rapid digital growth across economies?

Funmi Akinti: Thank you. So, digital innovations and advancements are outpacing cybersecurity investments. What I mean by that is that every other day, new applications and innovations are coming out. And these innovations are hoisting the life of everyday users. We are trying to make things as simple as possible. But the downside to that is that the more we make those things simple, the higher the risk they cause. And most times, people think of this infrastructure and think of security. They think of security as an aftermath instead of embedding it into the whole structure. So, because of these cybersecurity investments, it's taking a close or a fast second to digital investments.

This year, we've seen ransomware happen to the popular Marks & Spencer. This just happened around March this year. And then United Nations food. And these things are easier because of AI and deepfakes. Before now, it was usually much harder to come up with cyberattacks. But now, because of AI, it has made it very easy to deploy attacks, to attack organisations, leading to millions in losses. So globally, security investment is taking a very slow or second place to digital connectivity, digital investments, and innovations. Innovations are going on and are coming out. Both cybersecurity and security investments are taking a very close look.

In fact, there's something we call a platform as a service. Platform as a service means that you don't need to have your own server, just subscribe to cloud services and then have access, like your email. You don't have any infrastructure, but you are using email and stuff like that. So, do you know that there are things called ransomware as a service, where you can go and subscribe, and then they help you attack people with ransomware? That is how fast these things are now because of AI. It's really the distance between the investments in security investments and then digital investments, they are quite water fast, and most times, we react to security incidents as much, instead of embedding them into our day-to-day processes.

Kechiro Ambro-Moye: Okay, thank you so much, Ma. So, from what you just said, it's really sad that big companies and large economies fall victim to all this cyber malware, cybercrimes, and all of that. But it's a good thing that we have an antibody to attack this, and that leads us to our second question.

As more economies move online from mobile money to e-government platforms, what kinds of new vulnerabilities are emerging, especially in the global south that's coming up?

Ms Funmi Akinti: Okay, so there's something called SIM-SWAP, everybody has SIM now, and that SIM-SWAP is that people, attackers, they will pretend to be the user, and then they will use tele - phones stating that their number is missing, and then from doing that, so they will get other peo - ple's number. Because of that SIM-SWAP, they are not the owner, but they just cook up soft tales and then take people's SIMs. And use SIM cards to commit all kinds of atrocities. The reason we are able to do that is because we have what is called mobile money.

You could do almost everything on your phone, you could use USSD to do all sorts of things, and you could pay bills. Because of this ease, whereby you don't need to go to banks to do this trans - action, it has also led to a breakdown. We are seeing people sending just links, even to mobile phones, or SMS, oh, can you click this, and then you click that, and then they install something on your phone, which captures your details, and they can take away your money. That is one reason, because people are moving online, it is easy to commit mobile money fraud.

Now, another one is APIs. There are transactions that, or there are platforms or gateways, let me use, there are gateways that you can only access through the government, because some are like names. You can only do those things if you only go through these government agencies, we call those things API. API is one or two things from the government, and brings them to me.

Just to put it in layman's terms, this API, there are lots of organisations that want to do the same services, let's take POS, for instance, we have a lot of organisations that are now into POS, and all of them connect to perhaps one API. Just imagine that one is able to hack into that API, and everybody's data is in trouble. Because of the way our infrastructure is being used, this API, most people, and third-party APIs are connected to just one, so if you break into that, then you break into what's called a lot of people's databases, and then even for governments.

You'll find out that we have just one point of failure. If one main database, like the CAC database, is just one, it means that if anything goes wrong, or if those things are penetrated, millions of pieces of data will be harvested. Or do we want to talk about data ID platforms, because now your bank has a copy of your fingerprints and other stuff that has a copy of your fingerprints?

So as we move online, we are at risk of these things, data, names, even PII, and that's personally identifiable information, as a risk, because of this online movement. The, should I say the "Oga pata pata of them all", (ultimate) is social engineering and phishing. The reason it would work is that you don't know the number of places that you are connected to. I mean, you have a vendor on Instagram, you have another vendor on Facebook, you have another vendor somewhere, so one way or the other, because of this very interconnected market, you really don't know whether you

are being socially engineered, or you are being phished.

Because you don't know the number of places that you have put your username, and you have created passwords. The vulnerabilities that we have now are mobile money and telco fraud. Our IDs are everywhere, and we have one point of failure for all these databases, and then we have social engineering and phishing. Which has become more rampant now, because they can find your name anywhere, they can call you, and say what and when you did, and it would likely be true because you must have done something when in a place, or a portal, so those are the vulnerabil - ities. Thank you.

Kechiro Ambro-Moye: Okay, so from what I just got, is that even we as individuals who fall victim, not just because we are careless, but because most of these organisations that we tend to trust might have issues and fall victim to all these cyber-criminals. So, from there, in places like Nigeria, where digital financial services and tech adoption are growing fast, what are the biggest cyberse - curity risks that businesses and institutions should be aware of?

Ms Funmi Akinti: Okay, so before, they would usually tell you that if you get a phishing mail or a scam mail, if you read through it, you'd likely find typos, badly written English, and grammatical errors. But because we have AI, and because we have deep-fakes, you cannot verify, just like that, what is a phishing email, or what a scam email looks like, because of AI. So now, the key risk that we have is AI-driven phishing, like when people would use just ChatGPT to coin fantastically destructive emails for you. Still, this third-party and API risk, as I've said, a lot of people may be connected to API, and you don't know, so organisations are advised, you know, to create security postures, to create their own security profile, but you don't know what the third-party is doing, do you understand?

You don't know what they are doing to keep their own data safe, you don't know what they are doing to secure their databases, and you don't know what they are doing as per policies. So sometimes before fitting to this third-party, there are also third-party and API risk, there is also regulatory exposure, you know, there are huge fines for, even though we don't have, you know, I don't want to say non-governing body, but we don't have very strict chains following up, because there are very strict fines for non-compliance, even though nobody's, for now, nobody's really following up if those things are met or not. But there are strict fines if you are exposed, and the talent gap is one, you know, I think I mentioned something about zero-day attacks and all that. So the talent gap is also one vast space, security professionals, there are cars, and in between, and let me talk about maybe SMEs.

SMEs, sometimes you find one person being in charge of IT, so you want the person to create your IT portfolio, and then you want the person to also have a holistic view, about your, what was it called, your IT, so those are the risks.

Then one more is that sometimes, most times, we leave IT, security knowledge, we leave it to IT departments, they don't have that knowledge, but we leave it to them. We do not understand that when a cybersecurity threat happens, even though it breaks down IT infrastructures, it affects your finances, and if you're a food service company, it affects your food. So those are the risks. We leave that area, we think it really doesn't affect it, it's just for the IT department. So those are the risks that we have, and then maybe the payment fraud too, just as it is globally, loss of money because of all these very porous, easy but porous platforms that we have. Thank you.

Kechiro Ambro-Moye: Okay, so it's quite disturbing because big companies like this, you would, like you just said, you would only see one person in the IT department, and this person is manag - ing everything, IT, cyber security, which is not supposed to be. In fact, they are supposed to have separate departments for these things, you have for IT, and cybersecurity.

So, when we often hear cyber security, it's not just about technology, but also about culture and awareness, so what role does digital literacy play in improving cyber security, and where are we falling short at this point?

Mrs Funmi Akinti: Okay, so you know literacy is really properly used when you're online. So what literacy does is, let me give a scenario, most times when an organisation, let's say a huge organisa - tion, wants to protect their company, we buy devices, we do a firewall, and sometimes, in fact, we won't install ion bars here, we install biometric doors. And the reason we do that is so that, maybe from the outside world, attackers will not gain entrance.

Do you know that MOOCs, for instance, I'm an attacker, and I just followed my friend, my friend that is not well-versed in cybersecurity behaviour, and I just follow, hey, what's up, and then I tailgate. Tailgate means me not having access cards, and then I enter into the premises, and then maybe my friend has access to server room, me not also having access card, but because of my friend, because my friend trusts me, and she knows me, she doesn't know what's in my heart, but she trusts me. So me not also having access, I enter the server room, do you know that all those in - vestments on firewalls, gates, solutions have been wasted.

So, digital literacy is the bedrock of cybersecurity; we are as strong as our weakest link, that's really the basis of it. Proper digital school, they know what to do, they know not to click links, they know not to share links, they know if their devices are, maybe tagged or infected, they know not to plug it somewhere else, and stuff. Little things like this, as much as I figure out, people should know, but people do not know. So, when people are digitally literate, it saves. It can save you 50% of your costs, because people know what to do. You've embedded this into your policies and all that.

Where are we missing it? Number one, people think they know; we assume that people know. If people are not forced, they are not going to know. They like their friends, but they don't know what

their friends are thinking. It's in cyber security, or it's digital literacy that will tell them, trust nobody, it is digital literacy that will tell you, least privilege, it is digital literacy that will tell you, don't click these kinds of links. Another point that we're also failing in is that we do cybersecurity awareness training once a year, you know, it's not something that is part of our system, so people do not know, and then we cannot say it in a language that is understood. For instance, my parents, the only awareness they would have is if I give them, or maybe their bank sends them messages, but there is nothing in their own local language that says that, maybe in Yoruba, this is what it would look like.

The way people have access to digital literacy, maybe they work in organisations, so people are also not exposed to this knowledge, and so they fall prey anyhow. And then we also think it can - not happen to me. We hear of breaks, we hear of ransomware attacks, we hear of all these kinds of attacks, and then we think it cannot happen to us. We don't retrace from those incidents, and then think, oh, what can I do so that this cannot happen to me? I always say that even though cybersecurity affects cyber infrastructure, the aftermath is processes, people, food, and what is called infrastructure. For Marks and Spencers, orders were delayed, even though it affected IT departments, which resulted in people.

There was one that happened in 2024. It was a lab; even though they shut down the IT lab, it affected transfusion, it affected surgeries, and the way the attack happened was via social en - gineering. I mean, it was just via social engineering, so we don't train enough, we think it can't happen, or we even limit training to IT departments. No, the training is for everybody, from interns to executives, everybody should be part of the policies, at least a little literacy, not the hands-on high tech, but at least what to do, how to behave. If we have that, more than half of, you know, your expenses are gone, thank you.

Kechiro Ambro-Moye: Yes, thank you. I strongly believe that even in schools, let's say in higher in - stitutions, cybersecurity should be taught before you start a job. And when you become an intern, they will now teach you what to do about cybersecurity. All these things can be taught, because it's from, I trust my friends so much, that it could even cost people's lives, especially when it comes to hospitals.

Moving away from individuals, let's go to small businesses and other things. How can small and medium-sized businesses, which often lack big IT budgets, protect themselves from cyber threats without breaking the bank? How can they protect themselves without breaking their budget, and are there simple, effective steps that they can take today?

Mrs Funmi Akinti: Okay, all right, thank you for that. So you see, let me start by saying that IT is for the business, the business is not for IT. IT supports the business, IT supports whatever threat. So you are always going to create your cybersecurity answers for your profile. So if I am, let's say I'm 100 million, I'm not going to create a cybersecurity profile of 1 trillion; it absolutely makes no sense. Well, because IT is to support the business, it does not exist in silence, so yes, there is stuff that

SMEs can do. One is to effect, when we are even employing from our user, from our onboarding, we must have a policy that leads to clean, simple cybersecurity practices. So that when they enter, it can't be an aftermath. Oh, we don't leave our computer open; we must always shut it down when we leave. We change our password every other day; those must be embedded in the policies. It can't be an aftermath, because you are small, so you don't have the infrastructure to create.

Also, you must find ways to embed clean, simple cybersecurity policies into your onboarding sessions. You can also get a password manager. When people create managers, they use what they know, maybe by their third name, their father's name, they change it somehow, but it's re - ally around what they know. So, SMEs can buy small, simple password managers, which will keep generating new passwords. It will remind people of when to change and how often to change their passwords. There's no way someone there is sniffing their password. They are also encouraged to do monthly awareness training. You see what you wrote in your policies, you must find ways to decimate it monthly. You must find processes to remind your staff; it must be part of your core values.

I know we want to be the next best thing after..., but whatever your security policies are, they must also be part of your core values. And then all those free email platforms, as much as you can, try not to use them; get one that comes with email filtering, so that you don't have spam and phishing emails. One very important one is backup. Backup like no man's business, back up and test your backup, before you take another backup, always try to test your backup.

Then again, MFA, two-factor authentication, find a way, like when someone logs in, find a way to either do a mobile, maybe to check something, your fingerprints. Just make sure there's two-fac - tor authentication, post policies, and put cybersecurity practices into your policies. Use password managers, you can buy chip phones, backup immediately, and then, I think that's about it, yeah, your application updates, you can create a small, small table, and just paste it somewhere. Backup every two

days, just write it somewhere within your office, have you updated today, you know, paste these things around. It's cheaper than paying for ransomware, all these things are cheaper than paying for ransomware, thank you.

Kechiro Ambro-Moye: Thank you so much, you spoke very well on the whole two-factor authen- tication, and how very seriously we should take it. Especially updating our applications, where a lot of us are known not to update applications, because we just overlook it, so updating is very important, and that's really nice, thank you so much, ma.

So, how can cybersecurity affect economic outcomes? Whether it is at the national level, for small businesses, or for non-profit organisations?

Mrs Funmi Akinti: It is trust. There are two ways it affects, on the customer side, it breaks their trust. They are weary, afraid, sceptical, and they may even fall into the wrong hands, because they are trying to escape from something. For the other one, for the people affected, first, their rep - utation is damaged. The Marks and Spencer, I think they were the ones that lost about 30 billion pounds just around this. The United Nations ' stock went down five per cent. So, being a prey is something that you really can't recover from.

Your customers become sceptical, and they go somewhere else. Sometimes, they even fall prey, and then you lose money, and then you lose reputation. People may not want to engage with you or, I mean, something that, you know, is going to start buying back, I mean, that, and that reputa - tion. So, those are the costs: money, reputation, and trust. Those are what we lose.

Kechiro Ambro-Moye: Okay, thank you so much, ma, for coming this far with us. So, the last ques- tion would be, from a public sector angle.

Are governments and regulators in emerging economies keeping pace with cybersecurity needs, and what would a strong, forward-looking cybersecurity policy actually look like?

Mrs Funmi Akinti: Okay, so what we have generally is reactive, we are quite reactive. So, we have policies after the fact, and even when we have those policies, we don't have ways of measuring, of tracking, of seeing if that policy is doing what it is, you know, supposed to do. So, one of the, you know, maybe what a good policy can look like. So, usually, when you want to get paid by the government, you are asked to present some documents, one of which is your tax clearance, your CSE, things that confirm that you are sort of like compliant, you're Nigerian, and you've registered your business.

So, one policy that can also help is just make some sort of training, some sort of regulatory, some sort of compliance, just make it compulsory, such that before you can get some jobs, before you can access some stuff, you must show proof that you can understand that these policies, or these statutes, or what are the regulations, are done in your organisation. So, just like they will ask for your CSE, there should also be some sort of requirements, like you can't have this, except you've abided by this framework, you can't access this loan, this grant, if you have not done this.

And another one is baseline, what that baseline is, or an example is WIAC. You know, before any child would enter university, they must have WAEC, even if universities would then bring up their own exams, and all of that, they must have WAEC. So, there should also be a baseline. And we don't have that baseline, there must be a baseline for infrastructure, and as a baseline, I'm saying a baseline security posture, that you must become like, so you must have this before selling your services, or before bringing yourself out, so there must be some sort of that baseline. If there isn't that kind of baseline, everybody will just do what they want, and then security will be an add-on.

Do you know that, if you go to, well, maybe not the Play Store, but if you go online, you will find some applications, and those applications, people can download them, not knowing that they are malicious apps, you know.

So, if we had regulations, bodies, checking, all of these things, checks in place, there should be like a baseline security for some cloud providers, or infrastructure providers. And then maybe just tie policies to grants, loans, and all that stuff, but you don't have the certification, and it should be followed, not just get the certification without, how people would do bodies, and all the things would come inside providers, because most times, we have policies, or policies have been made, but they are not being added to us, which just makes them ineffective.

They maybe create a national, maybe CIRIC's body, 24-7 and one other one would be something around general, what's it called, social cyber security, you know, something that could be dispersed in languages, that would go to all those regions, all those, then those to most places. So, I think that's what it should look like, so let me just mention it again, tie policies to funding, just the same way you request a CAC, you should also find something that certifies that you have at least some sort of things, something that will audit you. And then let's have a baseline requirements for every really cloud provider, or infrastructure provider, or even any app, like, so before anybody deploys the application, let's fix that, or someone, an external body said that it feels, what's it called, basic security requirements, and there may be a body, a national body whose sole job is around that, what's it called, around risk response, and all that, so that's about it.

Kechiro Ambro-Moye: Okay, I strongly agree with everything you've mentioned, especially the baseline that you just mentioned, and passing information in local languages for elderly people, and also for rural people to understand what cybersecurity is all about. So this brings us to the end of today's episode of Kingsgate Brief. Thank you for staying with us.

If something stood out to you or challenged your thinking, simply drop your thoughts in the comments below, and let's keep the conversation going. As you do so, please do us a small favour with a big impact by liking, sharing and subscribing to our channel. Also, do well to follow us on our other social media platforms like LinkedIn, Instagram and Twitter. If you have any topic that you would like to hear us discuss in the coming episodes, you can also drop it in the comment section, as we've got more powerful conversations coming your way, so stay tuned. Thank you.

Bye.

CONNECT WITH US:

 kingsgate_advisors_institute

 Kingsgate Advisors Institute

 Kingsgate Advisors Institute

www.kingsgateinstitute.org

Kingsgate
Advisors
Institute