CYBER SECURITY KNOW YOUR BLINDSPOTS

by Reena Abraham

In an age where we manage most of our lives digitally, every user should be wary of the simple things that may compromise their personal and organization s security. At work, users live in a complex environment brought on by multiple devices, greater connectivity and a constant stream of information and because of this, the lives of IT and Information Security teams have also become very challenging. In such a setting, CTM360 - a cybersecurity start-up based in Bahrain - offers a managed 24x7 service from the cloud that integrates the needs of IT and Information Security teams to counter threats preemptively.

To identify threats at an early stage, CTM360 looks to detect and respond to incidents that lie in an organization s Cyber Blindspots on the cloud. With such a focus, the start-up is changing the paradigm of security and enabling organizations to prevent paralysis in the face of on-going or expected attacks. Currently, CTM360 works with B2B enterprises and small-to-medium sized businesses (SMBs) globally and is providing the on-going service at-scale. CTM360 s famous Offensive-Defense approach allows security teams to hunt and neutralize threats as they appear.

Operationally, CTM360 has been greatly aided by the core technology built by EDX Labs, a nucleus offering technology R&D and shared services. EDX Labs mission is to nurture and scale technology companies and remains the brainchild of Mirza Asrar Baig, Founder & CEO of CTM360, EDXLabs, and other security companies.

Mirza Asrar Baig is a recognized figure in the GCC s cybersecurity community, and in an interview with Reena Abraham, spoke about the importance of awareness, common sense and how to institute simple measures to keep one s data and personal information safe. His insights focus on the simple things in security and why the broader security industry is lagging behind the evolving threat landscape.

It is generally agreed that Bahrain s ICT sector is amongst the most progressive in the region. What is your outlook on the sector and what have been the main areas of concern for cybersecurity agencies in the last year?

There are many ways in which Bahrain has demonstrated its progressive attitude and efforts. Bahrain is one of the first in the region to initiate e-government migration to the cloud, and this cue was taken up by other sectors at a national level when they began moving toward the cloud. This has been something that many other countries were considering, but the Bahraini government was already encouraging all industries and sectors to move towards the cloud.

On a side note, CBB (Central Bank of Bahrain) has also set up an initiative that has proved to be a great push for the financial sector. I am mainly talking about the focus placed on Fintech. CBB as a regulator has built a sandbox, where anyone can come with their ideas and technologies, experiment, and if it works with regulator s approval, take it live. This demonstrates so much about what has gone into putting Bahrain s ICT sector in the forefront regarding technology used and developed. Historically, Bahrain has had many firsts, and it continues to do that - to lead from the front.

There is a second part to this as well
Development of the support system, which is the growth of cybersecurity in the region. Every year

Mirza Asrar Baig
Founder & CEO, CTM360

at a global scale, the losses from cyber-attacks are increasing exponentially, even doubling I would say. Something is definitely wrong, and I say this only because on one side we have 99% of the world spending so much money on protection at many levels, but at the same time a small 1% of hackers and scammers are winning the game, they are always ahead.

In my humble view, this is one of our biggest concerns today, and this was the reason why I started my company. We need to ask ourselves, why is it that even after all the efforts, the attacks are growing, the losses are increasing and the time it takes to detect an attack is also increasing?

At CTM360 we call it the cyber blindspot, just like when we are driving there are blindspots that can be dangerous. We have built CTM360 on that perspective, and we actually have a product named Cyber Blindspots .

In a global ecosystem where hacking and cybercrime are becoming buzzwords, what do you think organizations can do to protect the rights and obligations of consumers so that they are able to make the best out of the telecommunications services they subscribed for?

There are so many organizations holding too much of our data. If they get breached, the impact will be tremendous. Just weeks ago British Airways data was breached, and people were impacted. Similarly, Facebook was breached, and so was Google+, and you can only imagine the impact for each of these. We re talking about millions of users whose data and personal information was compromised. When all this data goes into the public space, the impact and consequences are frightening. The repercussions may be as simple as one of your passwords being compromised because nowadays, hackers have algorithms that can actually predict passwords, and use it to access all your other accounts. We as humans tend to follow specific patterns to create passwords, or use the same again and again across all their platforms which makes it easier for hackers to gain access. The problem is huge.

Regulators say this is the kind of data that needs to be protected, or else there will be a hefty fine if it’s not, but then again at the same time, consumers still want and need the services. So the service providers start to come up with a long list of conditions in fine print on the license agreement, where consumers are obliged to agree to the terms if they want to use the service. Within that fine print, somewhere it will also mention the effect that while they try to do their best, should something go wrong, they cannot be held liable.

It is a big challenge globally. People need to think about how much needs to be revealed and exercise caution. Sometimes they give out so much data which isn t required, and when that system is breached, all that information is out there and could be misused.

More awareness and understanding would help consumers protect themselves. The attitude often is to say, What to do I have to lose? But the thing is, we all have a responsibility to protect ourselves.

Things will go wrong, but let's balance the impact by being prepared. It shouldn t be a knee-jerk reaction. I see this so much. Awareness and preparedness are vital. This is the challenge in our line of services, to show them what can go wrong or what is going wrong. We don t want to scare them because technology is something that improves performance and business, so the response has to be appropriate.

We can show you what has been breached and is available to the rest of the world, and we can guide you as to how to move forward. We can help you make better passwords, adopt better practices and at the same time, you don t need to plug yourself off the Internet. There are many advantages in being part of the digital platform, so all you need to do is to work with secure practices in mind.

How susceptible is the Fintech industry to cybercrime?

Simply speaking, very. But that shouldn t scare us. I ll give you an example I used when I was a speaker at the central bank conference in Malaysia about the resilience of cybersecurity. I was listening to the speakers and the subsequent Q&As.

When it was my turn, I explained it to them in a story. This is a story which everyone knows. The story of the tortoise and the rabbit. As we know it, the tortoise won the race and the lesson learned was Slow and steady wins the race.

But those times have gone. Now is the time of the rabbit. The rabbit will win the race every time. There are no more marathons, there are only sprints. Things change fast. You have to be agile. You have to adapt to new technologies. All this applies to Fintech, but this haste invariably also opens doors to cyber-attacks.

On the other side, regarding using the technology, it is extremely expensive to build and maintain your own data centres. Everything is going into the cloud. Yes, you are susceptible to security breaches, but you still have to take the risk. You learn about it and figure out the best way possible, keeping security in mind as one of the checkboxes from the very beginning, and then you move.

Is there any way for countries in the region to strategize and harmonize telecom regulatory practices so that everyone can benefit?

There are many ways this can be done, and I have been participating in at least one of these ways. In KSA, they have something called the BCIS - Banking Committee for Information Security - since 2001, where the security managers of banks meet up every month and collaborate on many initiatives. We also need the outlook with other industries, so that everyone can get together, discuss the issues and work out common practices and solutions. At every level, industry-wise, sector-wise, regions have to work together to overcome challenges.

The World Economic Forum has a platform where they get different minds from across the world together and come up with directives. One of their goals is to remove the disparity between nations, and they are trying to do that in the cybersecurity world as well. It gives you a platform where people can get together and work on common goals. In the cybersecurity industry, they have created many such platforms where they are getting together and trying to achieve this.

One of the areas the IT Industry focused on was with Domain-based digital signature, (Domain-based Message Authentication, Reporting, and Conformance - DMARC) or having your email digitally signed when it leaves your network. The framework was a collaborated effort and is now being adopted globally, and it is only a matter of time where even those who aren t involved will get involved in the initiatives. The pace should be faster especially with what s happening now in the world of digital transformation with cryptocurrency, blockchain and FinTech. There are pressures on governments at the national level as well, and you will undoubtedly see more collaboration in time.

In the wake of all that s been happening with Facebook and the increased public scrutiny of social media platforms, can you tell us about what measures are being taken to protect consumer data?

In the past, this is not a question that service providers would have liked because security breaches somehow always took a back seat. Now, the big organisations are very concerned about security and data of the consumers. The General Data Protection Regulation (GDPR) is the most critical change in data privacy where the EU came up with regulations in which all organisations who have consumer data will be held accountable if that data is breached. They will have to pay significantly large fines.

They may have gone a bit overboard in my opinion, because some data, which would have been public is now not. This gives us a bit of a problem in the field of security because researchers can t know who is registering the domain, and we don t know enough details to see if it is fraudulent. On the upside, this is even forcing people who would think of security only in the last stage, to think ahead.

What must we, as responsible users do to protect ourselves?

Don t use the internet!

No, no. I am only joking! It is a great channel, but we should be responsible about what we reveal online. Not just us as individuals, but also our families and organisations. As I said, too much is being exposed, and this is being abused by certain service providers, who use the available information in a manner that they shouldn't.

What is the need to tell everybody where you are at a particular time? Why do you need to announce to the world that you are not at your house right now? So if a person wanted to intrude your home, and rob the place, they would know when to break-in because you have already shared your whereabouts with them online.

I will give you a real-life story. An experiment was conducted in a town, where they had set up a psychic who said he could read people s minds. He would hold their hands and says things that were on their mind or what happened to them in the past. People were amazed, but actually, it was easier than you think. The truth is that the psychic was relayed information dug from their social media accounts, information that people put publicly themselves!

Keep in mind that for credentials, we should always enable two-factor authentication. For instance, Facebook gives you the option to use your email

ID or your mobile number to send a One-Time-Password(OTP). Enable that, and use it. So even if someone knows your password, they can t get into your account because there is a second factor enabled. The service providers have created the functionality for the user s benefit, but people don't have time to use it. I have advised my friends regarding this time and again. Only when their account gets hacked, or their wife s account gets hacked, they wake up. They could have avoided this whole mess if they were preventive and used 2FA the invalid excuse of not having the time to look into it is of no avail.

Consider another example, in your house, you obviously have an internet router. Have you ever checked the password? I could bet it would still be the default password for the majority of people. Your router could be used as a direct entry to your home through the Internet available to any and everybody. This means anyone could access your router, hack your TV, and watch you if it has a built-in camera. They can hack your net cameras, get into your computer, listen in to your conversations going on back and forth. People need to realise, for all the devices that they use and connect to, require secure practices. We need to educate ourselves on this, nobody will do it for us. Take the time to do it. It is not hard, just take the time to wrap your head around it.

What about mobile app security? What are the most significant trends in this area now?

This is a nightmare. I, myself carry two phones - Personal and Business. On the Business phone, we don t allow anything except for the applications we trust and nothing else. The mobile security landscape is a nightmare because it gives away so much information about yourself, the worst part is that we are the ones giving such apps permissions in the first place. Manufacturers try to come up with schemes and update your software. But when you download and install the app, how do you really know what that app is doing? The simplest apps, like a torch, can actually listen in to your calls and messages. They create all these apps to get this information from you. They push them onto you. Sometimes, they claim to reward you if you install the app. But once you do so, do you know what permissions you are giving the app? Can it read all your texts can it switch on your microphone can it turn on your camera? If yes, this app is really a spy tool, which someone could be using to listen in on your communications. Please spend some time, learn about it, be a responsible user.

> That demonstrated so much about what has gone into putting Bahrain s ICT sector in the forefront in terms of technology used and being developed. Historically Bahrain has had many firsts and it continues to do that - to lead from the front.

What trends lie ahead for cybersecurity and for CTM360 in 2019?

Something that is very exciting on one hand, and also challenging on the other, is that we are the only company in this part of the world that is doing this. It is scarce to see companies attempting to build on security, intelligence technology and so on. The area we are addressing at CTM360 is called the Cyber Blindspot . We believe that we are unique because of our unorthodox approach to cybersecurity. We look after organizations from outside their network. For example, inside your house, you have locks for your main door, room, cupboards, security cameras inside and outside-everything you think you need. But we do not operate from the inside. We operate outside, like out in your neighbourhood or in your city. Our job is to scan and see if someone is planning to get into your house to rob you, and once identified we take them down. For example, your company's Facebook account is not within your organization, its outside, residing on the internet. So we look at how many places an organisation s data or account is outside their network and create a catalogue for them. We call it their cyber footprint. this catalogue helps us to identify the attackers and their infrastructure, which could be anywhere on the Internet, in cyberspace.

With that in mind, we are working towards an AI - Artificial Intelligence engine. Today, work is divided into 70-80% of the work being done by technology and 25% by my team however, when I started building the system 4 years back, it was 20% technology and 80% manpower so you can see how we are automating processes with time. But now the curve is more challenging to tackle unless we have an AI engine. To do so, we will leverage our Big Data to apply machine learning and mature detection with manageable false-positives. So we took this project upon ourselves. We have 90+ entities that we protect till date, and we are looking after their attack data on the Internet. But now we are working on a project where we are focused on profiling global financial institutions of the world to formulate industry benchmarks. Coupled with an AI engine with a high accuracy threshold, attacks will be predicted and attackers identified much earlier. This is the biggest challenge for CTM360 for now.

Along with that, leveraging our Technology and R&D arm, EDX Labs, we have launched one more company, DMARC360. Earlier I mentioned the digital signature on an email where the recipient can verify the mail came from you and not an imposter. This service will be the first of its kind in this part of the world. It is a platform where there are no installations, but it is just a configuration that you need. We will start receiving a lot of intelligence data, which will translate it into what s going on, so if someone is trying to use your email ID or contents or are trying to impersonate you, we will be able to find it. PENTEST360 is another one of the technologies that in time we will reveal.

So a lot is happening here. I ve noticed your team has grown exponentially since we met last.

Yes. Thank you. We used to work with 3-4 people, now we are more than 35 people and recently moved into a bigger office as we expect to hire 60-70 people within the next year. ⊜