BIRGER.

Securing the continent

Jacques Harel, CEO, BIRGER., discusses cybersecurity risks facing financial institutions and the company's cybersecurity services

The last time we spoke you discussed plans for BIRGER. to expand operations on the African continent, how is this progressing?

BIRGER. started expanding its activities in the African continent in 2014 when we were awarded a technology project by an insurance company with newly acquired operations in Kenya, Rwanda, Tanzania and Uganda. Moving to Africa was a logical extension to our Indian Ocean regionalisation strategy, which we had started in 2010 and by 2014 we had four offices outside our Mauritian head office in Comoros, Madagascar, Rodrigues and Seychelles.

Our expansion on the African continent was accelerated when we partnered with Symantec to develop a Cyber Defence Centre in Mauritius. Its objective is to provide managed cybersecurity services from Mauritius to the Indian Ocean Islands but more specifically to the African continent.

BIRGER.'s cybersecurity offering is made up of our Cyber Defence Centre, advisory services, training services and value added services. Over the past year, we have been busy offering these services to both financial institutions and government bodies in the Indian Ocean Islands and East Africa.

What challenges have you faced with this expansion?

Our expansion on the African continent has been progressive, starting with a technology project in 2014 delivered by our team located in Mauritius, and there after we have incorporated companies in Kenya, Tanzania and Uganda as well as in Rwanda, which is now our East African regional hub.

Incorporating these companies in East Africa has been done with the usual administrative challenges, but these have been addressed with good professional advice available in East Africa. The challenging issue that we face for our expansion is to identify and recruit competent and reliable professionals.

It is known that globally there is a shortfall of security professionals and in East Africa it is also the case. Our requirement to recruit competent and reliable cybersecurity professionals is very challenging. Hence to address this issue, we have decided to approach local universities to detect competent and reliable professionals for our operations.

Can you explain a little bit about the cybersecurity centre and what your aims are with it?

Symantec, world leader in delivering cybersecurity solutions, powers our Cyber Defence Centre (CDC) located in Mauritius. Our CDC offers managed cybersecurity services with a 24/7/365 operation model.

To offer our managed security services, we collect metadata at our customers' premises from various sources namely endpoints, servers and firewalls. The metadata is standardised, compressed and encrypted on a Log Collection Platform (LCP). The LCP sends the encrypted data over a secured internet connection

Jacques Harel

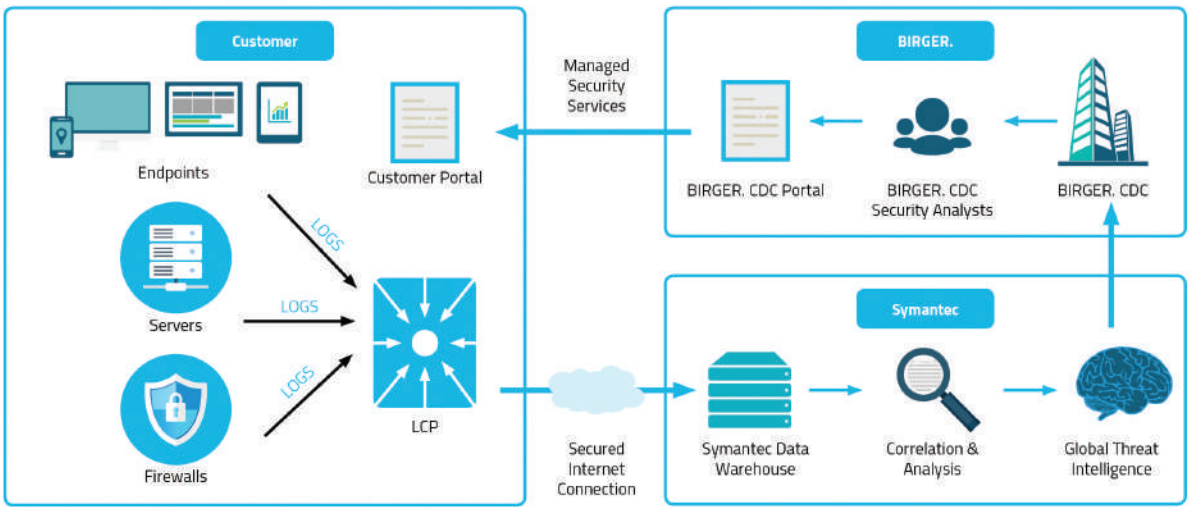
to Symantec's Data Warehouse. The metadata is correlated and analysed against 250,000 variables using Symantec's Global Intelligent Network (GIN). The results are then sent from Symantec to our CDC Analysts in Mauritius where they review the results before taking the required actions to provide the managed security services.

What are the biggest cybersecurity risks facing financial institutions?

The digital transformation that our world is currently witnessing is being driven by the exponential increase of connected devices. These connected devices are mobile phones, computers, tablets but also physical security devices, domestic appliances and cars. These connected devices are becoming more complex and have flexible software capabilities. The combination of these elements provides a larger surface of attack to cybercriminals.

Today financial institutions have a wider-connected ecosystem covering

A SUMMARY OF THE OPERATIONS AND PROCESS OF THE CDC



Source: BIRGER.

various devices, which make them more vulnerable and are potential cybertargets. This larger surface of attack is exacerbated with other factors such as:

- Lack of employees awareness towards security.
- Evolving working models on a 24/7 availability and working remotely.
- Complex IT systems.
- Lack of competent security professionals.

The first risk facing financial institutions is the loss of its data such as customers' details, account numbers and passwords. Cybercriminals may use a technique known as phishing to get hold of such data.

The second risk faced by financial institutions is financial risk. Cybercriminals may use a technique known as ransomware. This would imply that they would seek to take control of a computer and its content, which would be released once a ransom is paid. We have witnessed two Ransomware attacks this year namely WannaCry in May and Petya in June.

The third type of risk for financial institutions is reputational risk that could be caused by a DDOS (Distributed Denial of Service). In the event of a DDOS attack the financial institutions would be overwhelmed by requests for transactions, driving the whole IT system down hence not being able to provide the required services such as internet banking and website.

What can banks and financial institutions do to mitigate these risks?

To mitigate these risks banks and financial institutions must secure their human resources, their processes and their technologies to ensure that the whole ecosystem is secured. Cybercriminals will attempt to exploit any vulnerability, which will enable them to penetrate into the targeted ecosystem.

Hence, our initial recommendation is for regular security audits to be carried out to identify potential vulnerabilities and to attend promptly to these vulnerabilities by applying the required patches to avoid cybercriminals to exploit these manually or by using automated tools.

Securing a wide ecosystem is a multi-disciplinary approach where technical know-how is required but human factor is also very important to minimise these risks. We would recommend that all banks and financial institutions improve their security posture by deploying the following three-pronged approach.

The first step is to PREVENT any potential cyberattack of happening is by securing both its physical premises and its IT systems. The second step is to DETECT promptly when there is a threat or a cyber-attack. The third step is to RESPOND in case of an event, which implies that banks and financial institutions should be resilient if they are attacked.

Do you have any new product innovations on the horizon that you can discuss?

The launch of our CDC powered by Symantec in September 2016, is a pioneer project and a major innovation for the African continent. Our CDC has put Africa on the cyberdefence map.

In July 2017 BIRGER. concluded a Cyber Security Survey, in various countries of the Indian Ocean Islands and East Africa. The results will be published during the third quarter of this year. Based on the survey's findings we shall refine our security offerings for the African continent and we will also be opening more offices in countries of Africa where proximity cybersecurity services are required.