Zyber Global

OCTOBER 2022 | ISSUE 27

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 27th Edition, October 2022 of Zyber Global Centre's monthly newsletter.

September went by in a blur for me. Early September I was pleased to be working with the Council of Europe and the Turkish Ministry of Justice on the Sixth Coordination Meeting on Cybercrime – Samsun. I then heard the sad news that Queen Elizabeth II had died and like a lot of other people I watched it all unfold on TV.

It was good last week to be a speaker at the 2nd African Cyber Experts (ACE) Sustainment meeting organised by the African Union and the GFCE. It was an interesting meeting which focused on capacity building, cybercrime and the protection of vulnerable communities, Cyber awareness and skills development, cyber diplomacy and norms, and gender equality and inclusion.

It's October and Autumn has truly arrived in London with its cold, rainy days, a stark reminder that winter is just around the corner. October is not only Black History month but also Cybersecurity Awareness month, so it is going to be a busy month. There are several cybersecurity events happening this month, and a few are listed on our events page.

If you would like to have an online cyber health check – do register early for our Stay Safe Online webinar on the 28 October 2022, see https://zyberglobal.com/webinars

We continue with our usual features and ask that you continue to engage with us and let us know what topics on cybercrime you would like to hear more of. Stay safe. Stay well!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus
This month's focus is an interview with Graham Butler, Chairman, Bitek Global Ltd.

Zyber News
We have a roundup of the latest international cybercrime news.

Zyber Global Events Information
A focus on forums/conferences around the world.

Image courtesy Sabine @ Pixaby

Lack of data regulation for the social media platforms to remove harmful content has failed.
Voice communication will become just an App within your data packages, therefore the challenge for tomorrow in tackling Cybercrime will become increasingly difficult, as each country interprets data communication without any UN defined regulation.

Graham Butler
Chairman, Bitek Global Limited

Zyber Focus Interview

Graham Butler is the dynamic, eloquent and farsighted Chairman and Founder of Bitek Global Ltd.
He is widely recognised as a pioneer and expert in internet voice services. He was responsible for the implementation and rollout of the world's first international VOIP calling card service.

1. Can you tell us something about yourself and your interests.

Living in the UK with my office in Dubai entails lots of travel. Like so many during Covid, I was unable to travel and quickly got used to using Zoom/Teams/Skype video conferences for meetings.

I first became interested in VOIP when I worked at Deutsche Telekom. I was looking at TV documentaries on 'Police Dawn Raids' and I felt that there must be some easier way to get the information from the computer before it was wiped.

I come from the 'school of hard knocks' and recognised early on that VOIP is the future. I was always interested in research and development and asked a friend who is a Senior Data engineer to build a network that was able to see everything yet remain invisible. I bought a sophisticated server and the rest is history. Bitek was born.

Along the way, I interacted with major finance houses who in my view could stop fraud if they really wanted. These financial institutions are content to have a low security threshold as installing low level servers allows for them to insure the risk instead of building up to high level security. They feel that there is no need for it despite the rapidly changing world and techno-savvies out there.

I am married with 3 children and enjoy sailing and reading when I can find the time.

2. You are considered a pioneer on Voice over Internet Protocol (VoIP) which is a term for delivery of voice communications over IP networks, such as the Internet. What are some of the financial and security challenges this industry has faced since development?

I started presenting VoIP back in 1980 and was instrumental in the building of three international VoIP networks but became concerned regarding the lack of information over tracking paedophile activity.

My original wish was to focus on childrens' online safety by developing our Bitek solution, that latterly became known as a Deep Packet Inspection device. However despite offering advanced security services, we found that security services mostly had no budgets to purchase systems. So we would try to offer solutions that could generate new income streams for governments, increase their income by removing fraud by offsetting a percentage of these new revenues to purchase new security solutions. The financial impact of not addressing fraud activity in a small country can be as much as 2-5 million USD losses per month.

3. How were these challenges addressed?

The changes in this industry have been substantial. Originally carriers were faced with card based (bypass-fraud). Now OTT services like WhatsApp and Skype have taken over 65% of the world's voice market. These services are delivered through encrypted links and tunnels, creating extensive issues for police and security services. Tomorrow will be about 5G delivery, but without advanced tracking solutions and new billing structures, major challenges await each government such as taxation, security and fraud, as these concerns will only grow.

4. Have you considered or are you incorporating blockchain technology as a solution to these challenges?

In part, as we have secured involvement with a major blockchain project in the finance sector, by providing additional high level advanced security to protect a financial blockchain service following well publicised Cyber-attacks in this area.

5. Can you tell us about Bitek Global Ltd and the services it offers?

We have been supplying billing solutions for well over 45 years with staff based in the USA, UK and Dubai and customers across five continents.

We have developed the most advanced government-based Data Billing Solution designed for taxation of data. This self-funded solution has generated significant interest, especially in developing countries around the world that are losing taxes.

Other services include our fraud management solution, assisting security services and advanced topology mapping solutions that measure all communication ingress and egress routes into and out of their counties together with other tracking and interception solutions. Bitek Global Limited consists of various sub-entities across different countries.

6. What are your views on data retention as an approach to avoid difficulties of getting access to traffic data before they are deleted?

Fortunately, our system accesses all data at its source for an entire country, therefore we are not reliant on carriers or any other parties to provide the information. We securely store this for our customers who could be the telecom regulator or the security services or both for as long as they wish. The customer defines how long we store information.

The advantage of seeing an entire country's telecommunications allows for sensible decisions and policies to work for all.

7 .In your view, what are some of the cybersecurity risks currently facing the world globally?

If asked, would you buy a computer without an anti-virus solution, the answer would of course be **no**.

But I have been fortunate to see how many networks and carriers are operated and how open they are to being used for criminal purposes. Data has no legal regulation. Most countries do not enforce data or regulate data in anyway. Many Internet Service Providers don't even have the most basic anti-virus software as so many are unlicensed, but it is tomorrow's communication platform.

The largest global concern will be attacks directly from bad countries or bad countries using another countries' infrastructure to mount an attack on another country (we saw evidence of this in the last US election). Finally we see massive DDOS attacks taking place, hunting for valuable networks to ransom.

Read the full interview: https://zyberglobal.com/blog

Zyber News Roundup

22 Kenyans rescued from human traffickers in Laos

Kenyan authorities on Friday warned against applying for online jobs in South East Asian countries after it emerged that hundreds of East Africans are falling victim to trafficking.

The caution came as the Ministry of Foreign Affairs said it had rescued 22 Kenyans, a Burundian and Ugandan, who had managed to raise distress calls from Laos.

The rescued victims told authorities that hundreds more were still inside the Asian country, having been duped to go for hospitality and teaching jobs only to end up trapped.
"The government in liaison with the Government of Laos and IOM (International Organization for Migration) has rescued 24 nationals, among them a Ugandan and a Burundian, from trafficking cartels in Laos as more, still trapped in Myanmar and Laos, call for help," the Ministry said on Friday.

The 24 who were rescued have since been repatriated with the help of HAART Kenya, the IOM, and Laos government.

Earlier, 13 other Kenyans were rescued from traffickers in Myanmar . *"It is now emerging that there could be hundreds of mostly young Kenyans working in 'Fraud Factories' in South East Asia. More worrying is intelligence information that some of the factories may be facilities for extracting and storing human organs."*

Read more:
https://www.theeastafrican.co.ke/tea/news/east-africa/human-trafficking-victims-rescued-laos-395888

Russian hackers' lack of success against Ukraine shows that strong cyber defences work, says Cybersecurity Chief

Russia has engaged in a sustained, malicious cyber campaign against Ukraine and its allies since the February 24 invasion – but its lack of success shows that it's possible to defend against cyberattacks, even against some of the most sophisticated and persistent attackers, says the UK's cybersecurity chief.

"*Try as they might, Russian cyberattacks simply have not had the intended impact*," said Lindy Cameron, CEO of the National Cyber Security Centre (NCSC) – the cyber arm of GCHQ – speaking at Chatham House in London.

"But if the Ukrainian cyber defence teaches us a wider lesson – for military theory and beyond – it is that, in cybersecurity, the defender has significant agency. In many ways you can choose how vulnerable you can be to attacks."

Since the invasion, Cameron said, "*what we have seen is a very significant conflict in cyberspace – probably the most sustained and intensive cyber campaign on record.*" But she also pointed to the lack of success of these campaigns, thanks to the efforts of Ukrainian cyber defenders and their allies. *"This activity has provided us with the clearest demonstration that a strong and effective cyber defence can be mounted, even against an adversary as well prepared and resourced as the Russian Federation.*"

Cameron argued that not only does this provide lessons for what countries and their governments can do to protect against cyberattacks, but there are also lessons for organisations on how to protect against incidents, be they nation-state backed campaigns, ransomware attacks or other malicious cyber operations.

The NCSC has previously suggested that organisations should be operating at a heightened threat level, and has made recommendations that should be followed to help protect against cyberattacks, or collateral damage as a result of wide-scale cyber events.

Read more: https://www.zdnet.com/article/russian-hackers-lack-of-success-against-ukraine-shows-strong-cyber-defences-work-says-cybersecurity-chief/

Optus breach – Aussie telco told it will have to pay to replace IDs

The cyber intrusion at Australian telco Optus, which has about 10 million customers, has drawn the ire of the country's government over how the breached company should deal with stolen ID details. Darkweb screenshots surfaced quickly after the attack, with an underground BreachForums user going by the plain-speaking name of optusdata offering two tranches of data, alleging that they had two databases.

The seller wrote, "*Optus if you are reading! Price for us to not sale [sic] data is 1,000,000$US! We give you 1 week to decide.*"
Regular buyers, the seller said, could have the databases for $300,000 as a job lot, if Optus didn't take up its $1m "exclusive access" offer within the week. The seller said they expected payment in the form of Monero, a popular cryptocurrency that's harder to trace than Bitcoin.

The data breach itself was apparently down to an API endpoint with access to sensitive data was opened up to the internet at large, where it was discovered by a cybercriminal and abused to extract information that should have been behind some sort of cybersecurity portcullis.

Read more:
https://www.infosecuritymagazine.com/news/block-faces-class-action-suit/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

The Centre for Cybersecurity Belgium (CCB) **Online** **6 -7 October 2022**	**14th e-Crime & Cybersecurity Mid-Year Summit** **Park Plaza Victoria, London** **19 October 2022**	**International Conference on Cyberterrorism and Cybercrime** **Los Angeles, United States** **October 27-28, 2022**
The Centre for Cybersecurity Belgium (CCB) is hosting the tenth EU MITRE ATT&CK® Community Workshop on 6th and 7th of October, in a hybrid format. In this event, you will learn best practices on the use of MITRE ATT&CK in prevention, detection and response from your peers and from the MITRE ATT&CK and ENGENUITY teams. The workshop uses a highly-effective format of short (15') lightning talks. If you want to share your experience, you can indicate your interest to present in the in-person meeting. Participation is at no cost, but registration is required. The in-person attendance to the event will be limited to domain experts and with a preference given to user organisations and presenters. Virtual participation is open, but we require attendees to register using their real name and their corporate email address. Although CYCON 2020 was a virtual event, CYCON-2022 will be conducted in-person.	Data privacy has dominated regulators' thinking in the past few years but that is changing. New regulation around resilience and cybersecurity itself will transform the role of the CISO and the cybersecurity function – or at least it should. The regulators are on the case. Operational resilience in critical sectors of the economy is now a key focus. Data privacy legislation is well established. And fines for cyber-related misconduct are beginning to be imposed. Just recently, the U.S. Securities and Exchange Commission (SEC) signalled a significant change in how it thinks about what constitutes a threat to companies: It now considers cyber vulnerabilities to be an existential business risk.	The International Conference on Cyberterrorism and Cybercrime aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyberterrorism and Cybercrime. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Cyberterrorism and Cybercrime.
For further information **https://app.livestorm.co/ccb/centre-for-cybersecurity-belgium-ccb-share-and-connect-event?type=detailed**	**For further information** **https://akjassociates.com/event/midyear**	**For further information** **https://waset.org/cyberterrorism-and-cybercrime-conference-in-october-2022-in-los-angeles**

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/

Courses per sectors

Legal Entities
Customized courses for legal entities: judges, lawyers and public prosecutors.
Explore deeper aspects of digital forensics and the forensic value of evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings.

Law Enforcement
Customized courses for law enforcement officials: First responders, forensic investigators and analysts.
Delve into procedures, techniques, and tools used in digital forensic analysis and how to apply them in forensic investigations.

Private Sector Corporations and Small Businesses.
Customized courses for industry professionals working in the private sector; to help them understand the value and the need for digital forensic, and its implications in a corporate environment.

Course Structure

***FULL-TEXT REVISION**

***QUIZ AFTER EACH CHAPTER**

***CASE-STUDY AFTER FINAL EXAM**

c

At the end of each course, you will be issued a completion e-certificate which is immediately printable for your records. The number of **CPD** (Continuing Professional Development), **CPE** (Continuing Professional Education), and/or **CLE** (Continuing Legal Education) points will depend on the course.

DISCOUNTS

Special discount for groups of 10+ participants on all courses. The bigger the group, the bigger the discount.

BUNDLES

Stay on your forensic digital learning path and get the most from your e-learning experience by using course bundles.
https://bit.ly/31NRYsj

FREE COURSE ON PASSWORD MANAGEMENT

This covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them.
https://bit.ly/3eMu7ED