Zyber Global

JUNE 2021 | ISSUE 11

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 11th Edition, June 2021 of Zyber Global Centre's Monthly Newsletter.....

We have had great sunny weather in the UK this week, so I am really rejoicing as summer is here!
I have now delivered the last of the trilogy of webinars (on cybercrime, electronic evidence, and international cooperation) to my former colleagues at the National Black Crown Prosecution Association (NBCPA). The webinars have been very well received and I have enjoyed delivering the series. However, all good things come to an end, and I was pleased to hear that the NBCPA are planning further training to build on what we have started. With vision and forethought, the NBCPA is ensuring that its members have the skills to effectively prosecute cases involving electronic evidence.
I was honoured to be invited to be a guest blogger on Philip Virgo's blog in Computer Weekly, '*When IT Meets Politics*' It's a blog that I usually read, and the week of the 25 May 2021, Philip discussed the lessons from the Post Office Horizon Case.
Read the blog and let me know what you think.

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Terry Wilson, Global Partnership Director & Interim Executive Director Europe & Africa, Global Cyber Alliance

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Focus

The focus this month is on the training that our CEO, Esther George, provided to the NBCPA.

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is due to take place on June 30, 2021 register now to attend.

Coming Soon:

We have an exciting new webinar series in development for later this year

"Cybercrime is arguably the crime of our time. My frustrations are the scale of the problem, under reporting of cybercrime, and the largely invisible impact on victims "

TERRY WILSON

GLOBAL PARTNERSHIP DIRECTOR & INTERIM EXECUTIVE DIRECTOR EUROPE & AFRICA, GLOBAL CYBER ALLIANCE

Zyber Spotlight

Terry Wilson, Executive Director, Europe, and Africa and Global Partnership Officer at Global Cyber Alliance

Insightful and dynamic, Mr. Wilson brings a wealth of knowledge, experience, and understanding in building viable solutions to combat cybercrime.

Can you tell us about yourself and your journey to where you are today?

I have more than 12 years of experience in cybercrime investigation and prevention and 32 years of operational and strategic policing. I began my career with the Metropolitan Police Service (MPS) in 1986, spending most of my career as a detective. My specialist postings with the MPS included the Southeast Regional Crime Squad targeting the illegal trafficking and distribution of drugs, MPS Anti-Corruption Command focusing on police corruption, and Serious and Organised Crime Group - Flying Squad - where I specialised in Armed Robbery investigation at ascending ranks from Detective Sergeant to Detective Superintendent, as well as performing more conventional community-based roles in those ranks. Prior to joining GCA, I held the position of the UK's National Police Chiefs' Council (NPCC) cybercrime programme lead for four years. During this time, I designed, created, and implemented the UK's policing response to cybercrime.

What interests you about cybercrime?

Cybercrime is arguably the crime of our time. As a career detective, the fundamental aspects of cybercrime remain the same. There is a victim or multiple victims, there is a suspect or suspects, there is a crime scene or multiple crime scenes, and the investigative principles of gathering evidence to prove or disprove criminal culpability still apply. The interesting aspect of cybercrime is understanding the methodology of attacks within a developing technology environment, and the challenge of investigating crime with victims, suspects, and crime scenes all in different jurisdictions. My frustrations are the scale of the problem, under reporting of cybercrime, and the largely invisible impact on victims. Satisfaction comes from working with law enforcement and industry partners globally to tackle a specific problem and achieving the judicial outcomes and financial harm avoidance I previously outlined.

What is the Global Cyber Alliance (GCA)?

The Global Cyber Alliance was founded in 2015 as a non-profit by a partnership of the City of London Police, Manhattan District Attorney, and the Center for Internet Security. GCA is an international, cross sector effort dedicated to making the internet a safer place by reducing cyber risk and improving our connected world. We build programs, tools, and partnerships to sustain a trustworthy internet to enable social and economic progress for all. We build concrete solutions that reduce cyber risk, and we make those solutions freely available for any organization or individual to use.

In your view are we ahead in the game or are the cyber criminals one step ahead?

In my opinion, the cybersecurity sector and law enforcement have not been successful in combatting cybercrime, but both are making progress. We have not kept pace for a variety of reasons, but it is important we stay within sight and continue to strive to build protective solutions and interventions that work at scale. It is also vital we work collectively to raise the entry level and expense for criminals committing cybercrime, as well as raise the risk of arrest and prosecution.

Read more:
https://zyberglobal.com/my-blog

Zyber News Roundup

Telephone fraud: More than 300 targeted in bogus police officer scam

Telephone fraudsters posed as police officers to target older people on more than 300 occasions this year, the Police Service of Northern Ireland (PSNI) has said.
Victims handed over money or valuables 36 times, with a total of £135,000 in cash and jewellery worth £15,000 stolen. Ten people have been arrested and seven charged over the scams.
Police are warning older people and their families to be vigilant.
According to Action Fraud, which records scam figures for the whole of the UK, people in Northern Ireland lost almost £22m to a number of scams last year alone.
Police say there have been 308 reports of the bogus police officer scam since January.
PSNI Det Ch Insp Ian Wilson said if people were called in this way they should immediately hang up. He said the scammers engaged householders in conversation which develops into asking whether they keep cash or other valuables in their house.
"The scammers will then tell them that they have information that in the very near future they are going to be the victim of a crime, such as a burglary or a fraud," he said. Mr Wilson said the scammers would offer to take possession of cash and valuables in order to keep them safe. "If that is agreed to, they will ask the householder to put those valuables and cash into an envelope and set it somewhere - very often under the front doorstep," he said. The envelope would be collected and its contents stolen.
"The police will not phone you up and ask anything about your personal finances, whether you have cash or other valuables in your house and they certainly will not ask to take that into their possession for safekeeping," he said.
Read more: https://www.bbc.co.uk/news/uk-northern-ireland-57244355

Skin cell DNA gives authorities a new way to prosecute sexual assault

Skin cell DNA is being used to identify suspects who may touch a victim's clothing during a sexual assault.
This is possible because research has found that skin cells are left behind. And they can be used to identify a suspect based on their DNA.
Dr. Julie Valentine, a nursing professor at Brigham Young University, USA has been working to develop techniques for Skin DNA identification, and she said they can be used in groping cases or other situations where no bodily fluids are left behind.
The DNA from the skin cells can often meet the STR DNA standard used by the national FBI database, allowing a search and potential identification of a suspect.
"I had a case where a woman was abducted by two men. One man held her down while the other raped her," Professor Valentine told KSL Newsradio. "I was able to collect DNA from both."
Professor Valentine says the skin cell DNA can back up a victim's account of what happened.
"If the survivor reports non-consensual groping of their genitals, well, if we develop skin cells from the genital area, that corroborates there was non-consensual touch," she said.
Professor Valentine says there have been successful prosecutions using the technique, and police agencies from around the world have expressed interest in the technique. Read more: https://kslnewsradio.com/1949234/skin-cell-dna-gives-authorities-a-new-way-to-prosecute-sexual-assault/?

French authorities have seized their third dark web marketplace

French authorities have dismantled their third dark web marketplace over the last four years after they seized control of "Le Monde Parallèle" (The Parallel World) last week. Active since early 2020, the site was taken down in an operation coordinated by the French National Directorate of Intelligence and Customs Investigations.
"The two site administrators were arrested and LMP's activities were disrupted," officials said in a press release. LMP, as it was most commonly known, operated as both a discussion forum and marketplace for French-speaking criminal groups.
According to French investigators, threat actors used the site to sell carding data, narcotics, forged documents, and weapons.
Read more: https://therecord.media/french-authorities-seize-their-third-dark-web-marketplace/

Zyber Focus

Excerpt from Ms. Esther George's Training to the NBCPA on Electronic Evidence and International Co-operation

On May 19, 2021, our CEO and Cybercrime Specialist, Ms. Esther George, provided training on Electronic Evidence and International Co-operation to prosecutors and interested persons from the Crown Prosecution Service (CPS) through the auspices of the National Black Crown Prosecutors Association (NBCPA).

Mark Gray, Chief Digital Information Officer introduced the training. He had this to say: 'the world is becoming more and more digitised and so is criminal activity. We are passionate about innovations and while we continue to be a global leader in this sphere, just think about the digital evidence that we are using today. The CPS has made considerable strides despite facing innumerable challenges where digital evidence is concerned. We have to continue building on our knowledge and rising to the challenges that cybercrime continues to pose on a daily basis.

Ms. George spoke about the Post Office Horizon case and made four interesting points.
1.That it was not an ideal situation to have an institution i.e The Post Office be the victim, investigator, and prosecutor in a case.
2. In commissioning large technological projects such as Horizon, the customer should have the knowledge to work with the contractor to ensure that the contractor provides a system that is fit for purpose and takes into account the needs of the user.
3. Disclosure of evidence to the defence - How the law of evidence applies to automated computer-based decisions. This has wide-ranging implications across the public and private sector because of the growth of artificial intelligence in its capacity as a general purpose technology across every aspect of the economy means that the number of decisions involving software-based systems will increase both in the private sector and in the delivery of public services. Computer evidence must follow the Common Law rule that a "presumption will exist that the computer producing the evidential record was working properly at the material time and that the record is therefore admissible as real evidence".

Ms. George spoke at length on the many challenges faced in investigating cases where electronic evidence was concerned. For example, data is not always stored locally. It is usually stored remotely on someone else's computer. Microsoft has a storage system in Ireland and questions arise as to how can that data be accessed. As prosecutors, you will have to see which jurisdiction and legislation apply and you may have to make an application under Mutual Legal Assistance agreements. You would have to ensure that there is cross-border access to the data; identify and locate the evidence; secure the hardware; capture and analyse the data, and finally maintain the integrity and chain of custody of the electronic evidence.

Ms. George spoke about cross-border crimes, for example, if a crime begins in Country A, continues through Country B, and ends in Country C then it is likely that offences have been committed in all three countries. Then issues would arise as to jurisdiction, how the data could be accessed and how quickly.

"Countries must improve their ability to share data quickly. If not done quickly, the electronic trail will disappear"

Albert Rees
Department of Justice, U.S.A

Ms. George pointed out that there were international instruments such as the Budapest Convention which lent itself to more formal cooperation in sharing data. The disadvantage however was the bureaucracy involved, and a slow response time of approximately 6-24 months, by which time the data may have been deleted. The advantage was that standards could be verified, it is more than likely that there would be an unbroken chain of custody, evidence admissible and further assistance can be requested.
This is just a snapshot of the training provided. Suffice it to say that the training was well received and prosecutors left more knowledgeable on how to garner electronic evidence using both formal and informal processes.

Zyber Global Events

The next **Stay Safe Online Webinar** by Zyber Global is due to take place on June 30, 2021. Register now to attend.

OTHER CYBERSECURITY EVENTS

Cybercrime and Children in a covid-19 World Part 2-Addressing Child Sexual Abuse Material (CSAM) 4 June 2021, 2pm Samoan time (WST)	**GovSummit 2021 USA Government Security Conference. Connecting Government, Security and Technology Virtual Event June 9 2021**	**Think Cybersecurity for Government 2021 Virtual Event 22 June 2021**
This webinar is the second of a two-part webinar series on Cybercrime and Children in a Covid-19 World. Covid-19 has changed the world as we know it. While we have been forced to physically distance, we have become more connected through the internet, adapting to remote work, learning and video calls. Cybercriminals have adapted to our increased online engagement, rendering children more vulnerable than ever in this new criminal landscape. As the second of our two-part webinar series on Cybercrime and Children in a Covid-19 world, the CSAM webinar will discuss the challenges of keeping our children safe when engaging with digital technology and will consider opportunities for adapting laws and policies to prevent harmful practices. The webinar will be chaired by Chair of the PILON Cybercrime Working Group, Linda Folaumoetu'i, Attorney General of the Kingdom of Tonga and live scribed by graphic artist Ms Jessamy Gee.	SIA GovSummit Is free for all Government/Military/Defense/Public Safety Employees! Tickets start at just $149 for industry attendees. GovSummit – the government security conference hosted annually by the Security Industry Association – brings together government security leaders with private industry technologists for top-quality information sharing and education on security topics affecting federal, state, and local agencies. You'll find specialized sessions on topics such as security technology procurement strategies, evolving federal acquisition priorities, infrastructure protection technology, identity management, and access control policies, cybersecurity, school security, and more. This annual government security policy and technology conference examines emerging policy trends, technology needs of the government, and changes in the risk environment to meet evolving security challenges.	Cybersecurity and the government have always been intrinsically linked. Cybersecurity threats against local and central government continue to test both resources and stamina. Now, more than ever, there is a need for vendors and government to come together to find the best way to tackle sophisticated and complex cybercrime. Think Cybersecurity for Government conference program is designed to build bridges across this government-vendor ecosystem. Our events are renowned for delivering to the needs of the industry. This virtual event will be the most focused cybersecurity-government conference in the calendar.
For further information: https://zoom.us/meeting/register/tJ0lcOmgrT0pGdRG5KB0Ebf0FExE4omB9TyV	For further information: https://govsummit.securityindustry.org/why-attend/	For further information: https://www.thinkcybersecurityforgovernment.com

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