Zyber Global

OCTOBER 2023 | ISSUE 39

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - October 2023, the 39th edition!

Hello Everyone! I am excited to bring you the October edition of the monthly newsletter!

The Zyber Global Webinar held on 21st September 2023, was a real game-changer! It was themed "Cybercrime Uncovered: From Prosecution to Prevention," and it provided a ground-breaking platform for discussions revolving around the intricate web of cybercrime and the pivotal role of preventive measures.

We had some amazing talks from four speakers: Matteo Lucchetti, Director of Cyber 4.0; Ana Jakimovska, Chief Prosecutor of North Macedonia; Musa Jalloh, Deputy Director, National Communications Authority Sierra Leone; and Terry Wilson, Global Partnership Director at the Global Cyber Alliance (GCA) bestowed their invaluable insights, shedding light on the multifaceted aspects of cybercrime prosecution and prevention.

Each speaker, with their unique experiences and perspectives, unraveled the complexities of the cyber landscape, delving into topics ranging from managing cyber threats to African critical infrastructure to the legal considerations in cybercrime prosecution. The discussions emphasized the importance of interdisciplinary collaboration between tech and legal experts and the need for proactive solutions to build cyber resilience. The participant's interaction and engagement throughout the webinar were testament to the relevance and urgency of the topics discussed, with the audience gaining enriched understandings of the criticalities surrounding cybercrime and its countermeasures. This dialogue initiated in this webinar serves as a stepping stone for future collaborations and discussions aimed at forging a secure and inclusive digital realm.

At the webinar, we inaugurated the "Zyber Global Community" on LinkedIn, a collaborative space for professionals at the nexus of technology and governance, aiming to foster shared learning and mutual aid in addressing cyber challenges. This global forum aspires to foster international responses, ensuring global trust in law enforcement and government agencies' ability to counter cyber threats. We encourage open dialogue, questions, and knowledge sharing, looking forward to the innovative collaborations that will emerge. Join us in making the online world safer!

See you there! 🔗🌍 Click here to join: https://www.linkedin.com/groups/12896201/

This Month's Features

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

Zyber Focus Article

Cybercrime and Cybersecurity in Latin America and the Caribbean Part II

by Arsha Gosine, Head of Research, ZGC

"***Raising the political prioritisation of cybersecurity must start within the region itself and be sustained with strategic patience***"

[Louise Marie Hurel (a Research Fellow at the Royal United Services Institute for Security and Defense (RUSI) and Dr. Joe Devanny (a Lecturer in the Department of War Studies at King's College London)].

In my previous article, I focused on the background of Latin America and the Caribbean: 'Cybercrime and Cybersecurity in Latin America and the Caribbean' and where they are today in terms of cybercrime/cybersecurity. (see https://zyberglobal.com/blog/f/cybercrime-and-cybersecurity-in-latin-america-and-the-caribbean)

We saw that the area as a whole were working to improve their own response to cybercrime through a cybercrime strategy and a cybersecurity strategy. However, the political commitment was sometimes lacking which led to slow progress.

So, let us look at the difference between cybercrime strategy and a cybersecurity strategy? A cybercrime strategy and cybersecurity strategy main aims are a strategy to fight attacks against computer systems. However, there is a difference: a cybersecurity strategy will look at what can be done from a preventive perspective, often through technical means; while a cybercrime strategy will look at how to address transgressions in cybersecurity from a legal perspective including the need to enact legislation to criminalize acts that compromise cybersecurity and to ensure that adequate capabilities are in place to enforce such cybercrime legislation. Countries require both, if they are to tackle cybercrime per se.

Let us go a little further and breakdown that relationship. Cybersecurity strategy can be compared to fighting burglary by installing locks on a front door and surveillance cameras, whereas a cybercrime strategy can be compared to ensuring that law enforcement has the capacity to catch the thieves if they commit a crime. It would be impossible for law enforcement to deal with theft if there was not adequate technical security such as strong front doors to protect valuables. However, security features alone will not prevent crime either, there is a need to have a legal sanction and not just technical protection to act as a deterrent to commit crimes.

In the Caribbean, the Caribbean Community known as CARICOM is comprised of 15 member states, including Antigua and Barbuda, Bahamas, Barbados, Dominica, Grenada, Jamaica, Montserrat, Saint Lucia, St Kitts and Nevis, St Vincent and the Grenadines, and Trinidad and Tobago.

Alongside these island groups, Suriname and Guyana on the South American mainland are also members, as is Belize in Central America, and Haiti, located on the island of Hispaniola.

The Caricom's remit is to enable integration and cooperation across the region. It operates via a wide range of autonomous institutions, focused on areas such as trade, criminal justice, the environment, and technical standards.

In 2019, CARICOM was given a boost when it secured funding from the European Union to undertake a 'Capacity Development' project across CARICOM nations. The overarching goal of the initiative is divided into two tracks, cybercrime and asset recovery respectively. The aim is to increase the region's skills base and, ultimately, its security.

Public Technology interviewed Dale Joseph (October 2022), a cybercrime policy specialist for the CARICOM Implementation Agency for Crime and Security (IMPACS), who led the cyber element of the programme.

Mr. Joseph said that the work began with an exercise in "*legislation harmonisation within all CARICOM member states*". "*We hired a legal consultant who looked at all the technology-based legislation and all 15 CARICOM member states and we did a comparative analysis [with each other] and with legislation in other jurisdictions. We also mapped it to what is happening in the Budapest Convention on Cybercrime*," he says "*[We look at] what happens if, for example, in Trinidad and Tobago, if the criminal offences does not match that in Barbados. And we wanted to share information… to enable investigative continuity. So that was the first phase: we did the legislative gap analysis, and then we did an action plan as to how we could move towards harmonising legislation, with a view of bolstering our ability to prosecute, investigate and prosecute cybercrimes in the region.*"

All this work on cybercrime began from the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP), the implementation of which is overseen by IMPACSand was signed off by the CARICOM member states in 2017. The plan is intended to help member states address threats and vulnerabilities by codifying a practical, harmonised standard of practices, systems and expertise for cybersecurity, to which each Caribbean country could aspire.

After working on closing the gaps by implementing relevant legislation (many of the Caribbean countries are still working on this), training was provided to law-enforcement authorities, members of the judiciary, and senior government officials with oversight of national infrastructure and responsibility for responding to related cyber incidents.

Particular areas for example law enforcement live data forensics, which involves collecting data from devices that remained switched on at crime scenes were targeted for further education.

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

Zyber News Roundup

International Criminal Court hit in cyber-attack amid Russia war crimes probe

The International Criminal Court (ICC) announced that its IT systems were breached by cybercriminals last week, and the "cybersecurity incident" is still ongoing.
The ICC detected "anomalous activity" and took immediate action to respond and mitigate the impact of the breach. Additional response and security measures are being implemented with the assistance of Host Country authorities. While the ICC did not provide further details about the intrusion, it mentioned that it's working to strengthen its cybersecurity framework, including accelerating the use of cloud technology. There is currently no information on the identity of the attackers or whether any data was stolen.
The security breach occurred as the ICC investigates suspected war crimes in Ukraine, and with 13 pending arrest warrants, it has become a potential target for cyberattacks. Experts noted that any tampering with or accessing the ICC's information can be a powerful way for threat actors to disrupt international criminal justice proceedings.
This incident highlights that even highly professional organizations, like the ICC, are not immune to cyberattacks, further underscoring the importance of robust cybersecurity measures.

Read more:
https://www.theregister.com/2023/09/20/icc_hack/?td=keepreading

India's biggest tech centers named as cyber crime hotspots

A report from the Future Crime Research Foundation (FCRF) highlights a significant surge in cybercrime in India over the past three and a half years, with cities like Bengaluru and Gurugram being major hubs for such activity.
The analysis revealed common factors contributing to these cities' vulnerability, including their proximity to major urban centers, limited cybersecurity infrastructure, socioeconomic challenges, and low digital literacy. Gurugram, known for its status as a major corporate and IT hub, accounted for 8.1% of reported cybercrime, despite having less than 0.2% of India's population, making it an attractive target for cybercriminals. Similarly, Bengaluru, often referred to as the "Silicon Valley of India" due to its concentration of IT employers, emerged as an emerging cybercrime hotspot. The report also noted that nearly half of all reported cybercrimes in India (47.25%) were related to Unified Payments Interface (UPI) fraud, with financially motivated crimes accounting for 77.41% of all incidents.

Read more:
https://www.theregister.com/2023/09/21/india_cybercrime_trends_report/

Nigerian Pleads Guilty in US to Million-Dollar BEC Scheme Role

A Nigerian national living in South Africa, Kosi Goodness Simon-Ebo, pleaded guilty in a US court to his role in a million-dollar business email compromise (BEC) fraud scheme.
Simon-Ebo was involved in a conspiracy to commit BEC fraud and money laundering, with intended losses of nearly $7 million, though the actual loss was just over $1 million. He admitted to unauthorized access to email accounts, sending spoofed emails to trick victims into making wire transfers, and conspiring to commit money laundering by distributing funds sent by victims to other controlled accounts, among other activities.
Simon-Ebo is scheduled for sentencing on November 29 and faces up to 20 years in prison for wire fraud and money laundering conspiracies.

Read more:
https://www.securityweek.com/nigerian-pleads-guilty-in-us-to-million-dollar-bec-scheme-role/

Chinese students terrified as scammers reap millions

Chinese international students in Australia are falling victim to elaborate scams where con artists pose as Chinese police and officials, resulting in nearly $8 million being handed over.
Scammers use technology to create fake documentation, including arrest warrants, and make phone calls with fake police numbers to threaten students with extradition or deportation unless they pay. The scammers sometimes even send people dressed as Chinese police to the victims' residences to deliver fake documents, and are using messaging platforms and video technology to monitor victims 24 hours a day.

Read more:
https://www.afr.com/work-and-careers/education/chinese-students-petrified-as-scammers-reap-millions-20230924-p5e74c

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

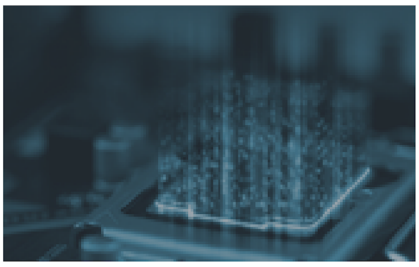
Critical Infrastructure Protection & Resilience Europe **Prague, Czech Republic** **3 - 5 October 2023**	**Cyber Security World Asia 2023** **Marina Bay Sands, Singapore** **11 - 12 October 2023**	**Australia Cyber Conference** **Melbourne, Australia** **17 - 19 October 2023**
The Critical Infrastructure Protection and Resilience Europe brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe. The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk [...] Attacks on critical infrastructure sites are now a fact of life not simply a potential threat. Power stations, chemical plants, nuclear facilities are routinely targeted by cyber-attacks, the most successful so far being the Ukraine power outage that caused 225,000 customers to lose electricity. This is just the start of what we can expect to be the repeated targeting of our critical infrastructure.	The Cyber Security World Asia 2023 is a standout event that brings cybersecurity pros and business leaders together, offering a platform to fast-track digital transformation initiatives. Happening on October 11-12 at Marina Bay Sands in Singapore, this marks the 9th instalment of what has become one of Asia's most buzzed-about cybersecurity events. Expect to rub shoulders with a who's-who of the industry from leading solution providers and cutting-edge innovators to the brightest minds in the field. The event will be jam-packed with insightful sessions that cover a range of vital topics, including data protection, privacy laws, threat intelligence, and beyond.	The Australian Cyber Conference 2023 - Attending this conference will enable you to hear from industry experts to help you better understand and manage current threats, as well as identify and prepare for emerging challenges. An interactive format of workshops, plenary sessions and the opportunity to network with industry practitioners in the field of cyber security is a must for all organisations. Delegates range from company directors and managers to public servants, lawyers, risk professionals, software architects, and technical security specialists. They come from a broad range of industries from education to finance, government, healthcare, manufacturing, mining, transportation, and utilities. The diverse nature of the audience enables a variety of perspectives and subjects for discussion and help to independently promote awareness and understanding of cyber security issues in the community.
For further information **https://www.cipre-expo.com**	**For further information** **https://www.cybersecurityworldasia.com**	**For further information** **https://cyberconference.com.au**

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
Special discount: 15% Use Code: zyber

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