Zyber Global

SEPTEMBER 2020 | ISSUE 2

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the second edition of Zyber Global Centre's Newsletter.....

I hope that in spite of COVID -19, you have been able to enjoy a relaxing summer break.

Each month this newsletter will bring you up to date information on cybercrime and cybersecurity.

Please share this newsletter with your friends and colleagues. The newsletter will also be posted on our website.

Do contact us with any comments or suggestions you may have. We always welcome feedback and would love to hear from you!

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Judge Rainelda Estacio-Montesa, Manila, Philippines who is a leading figure in the fight against cybercrime.

Zyber News

We also have a roundup of the latest international cybercrime news.

Zyber Focus

The focus this month looks at Fraud; this feature is by Arsha Gosine, Head of Research.

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is due to take place on the 29 September 2020 register now to attend.

Coming Soon:

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

> "Awareness,education and information dissemination is key in effectively combatting cybercrime"
>
> *JUDGE RAINELDA ESTACIO-MONTESA*

Zyber Spotlight

Judge Rainelda Estacio - Montesa

Trailblazing and setting standards in the adjudication of cybercrime cases in the Phillipines, Judge Nelda sets the policy agenda and trains judges ensuring that they have a clear understanding of cybercrime law and its application!

What interested you about Cybercrime?

In 2014 I was chosen to be a part of the '*Introductory Training of Trainer's Course on Cybercrime Electronic Evidence for Judges, Magistrates and Prosecutors of the ASEAN Region*'. This was organized by the Philippine's Department of Justice, Office of Cybercrime and the Council of Europe in coordination with the Philippine's Supreme Court.

Cybercrime caught my interest in a big way as it challenged my ability to think and discern especially where Information and Comunication Technology (ICT) is involved.

I found it very relevant in life and society today and I just had that feeling that this is for me.

The desire to learn more about the subject was so great that I made sure to actively pursue and participate in future training and projects.

I also met Esther George, Cybercrime Expert in 2014. She was very inspiring and took time to explain the concepts and issues pertaining to cybercrime. I was very impressed with Esther and over the years she has mentored me and cemented the passion that I have for cybercrime today.

How do you think we can effectively combat cybercrime in its many forms?

Awareness, education and information dissemination is key in effectively combatting cybercrime.

Stakeholders of the justice system such as law enforcement, prosecution, magistrates and judges must be equipped with the knowledge on how to investigate, build a case, prosecute and adjudicate on cybercrime cases respectively.

Law Enforcement Agencies (LEA's) must possess the skill and knowledge on how to effectively investigate and catch cybercriminals.

Members of the community should be informed of the threats and trends that are evolving in this Information Communication Technology (ICT) age.

It is only when the public becomes more aware of the problems that cybercrime can cause and take appropriate action when anything does happen, will we effectively begin to combat cybercrime

What is the Philippines doing to combat cybrcrime?

The Philippines, in my opinion, is one of the ASEAN (Association of Southeast Asian Nations) countries that has gained a head start in combatting cybercrime.

Our Cybercrime Law was passed in 2012 and we became a member of the Budapest Convention in 2018. Most of our law enforcement authorities, prosecutors, judges and justices have been trained on cybercrime.

The Supreme Court has also passed the Rules on Cybercrime Warrants seeking to provide procedural measures and remedies for data preservation, disclosure and collection.

There are designated cybercrime courts and the Court over which I preside is one such court.

(For the full interview see: https://zyberglobal.com/my-blog)

Zyber News Roundup

Ransomware

If you are infected by ransomware: .

- Disconnect your device from any others, and from any external drives.
- If there is a ransom note on your screen take a photograph of it.
- Determine what type of ransomware you have been infected with as there are some free decryption tools available - see news article below.

RANSOMWARE

Why one city chose to pay the ransom after falling victim.........

A US city has explained why it gave into the demands of cyber criminals and paid a ransom demand of $45,000 following a ransomware attack.

Lafayette, Colorado fell victim to ransomware on July 27, which encrypted the city's computer networks and caused disruptions to phone services, email and online-payment and reservation systems.

After examining the incident the city of Lafayette opted to pay the cyber criminals the ransom they demanded, perceiving it to be the quickest and most cost effective way restore municipal services to residents, rather than attempting to restore services from scratch

Read the full story here:
Why one city paid the ransom

R***ussian cybercrime suspect arrested in $1m ransomware conspiracy ....***

In a fascinating mix of old-school face-to-face techniques and new-wave cyber criminality, Kriuchkov, who is 27 years old, is alleged to have set up a meeting via What's App.

.

He then travelled to San Francisco and drove on to Reno in Nevada, to talk to an unnamed employee of his planned victim company to propose a “special project”.

Acting on behalf of unnamed co-conspirators, presumably safely back in Russia where (if they are Russian citizens) they have constitutional protection against extradition, Kruichkov is supposed to have dangled a million-dollar carrot in front of the insider in return for them helping to perpetrate the crime.

The court filing claims that the insider would have been expected to provide information relevant in tailoring the attack to the victim’s network, and then to connect up and run the malware to infect the network. In return, Kriuchkov promised the insider a cool $1,000,000. The insider contacted the authorities, and Kruichkov was arrested.

Read the full story here:
Russian Cybercrime Suspect

Ransomware: These free decryption tools have now saved victims over $600m........

Over four million victims of ransomware attacks have now avoided paying over £600 million in extortion demands to cyber criminals in the first four years of Europol's No More Ransom initiative.

Read the full story here:
Ransomware free decryption tools

For up to date zyber news follow me on twitter https://twitter.com/Esther_George
or
LinkedIn
https://www.linkedin.com/in/esther-george/

Zyber Focus

Fraudulent Scams

As Cyber technology continues to evolve at an alarming rate, it is matched by an even more sophisticated criminal activity.

Cyber fraud is defined in the Cambridge Dictionary as the use of the internet to get money, goods, etc from people illegally by deceiving them. It has become the most common type of fraud.

Sean McGrath a cybersecurity expert at BestVPN.com in 2018 said that:

"To call out a single cybersecurity risk and claim it is 'the one to watch' is a false dichotomy..."

He said that by and large the threats remain the same year in, year out for example ransomware, phishing attacks and malware... the usual stuff. He further commented that "What is changing, and will become only more apparent in 2019, is the size of the attack surface and the velocity of the attacks themselves. The Internet of Things felt like a neat buzzword a few years ago, but literally every facet of our lives is now online. From the cars we drive and the planes we fly to the critical infrastructure we rely on for our energy, water and safety – everything has an IP address. If it's online, it is susceptible to attack and the larger the attack surface, the greater the real-world consequences will be when things do go wrong.

While this might sound like a problem for governments and businesses to focus on, the reality is that any major threat to critical infrastructure will be powered by the devices in our homes".

His comments are very relevant today. We continue to see 'ransomware' attacks; phishing; and hacking despite having security software for online protection.

Three years ago, the WannaCry ransomware attack took place globally. In the UK the National Health Service was particularly affected, having been knocked offline. This had severe repercussions as it caused high risk to lives with ambulances being routed incorrectly. The ransomware affected computers operating Microsoft Windows, files were kept 'hostage' until a ransom was paid using Bitcoin. Microsoft moved quickly to 'patch' their system but consumers and companies were slow to do so. In just a few hours the ransomware had caused billions of dollars in damages.

Today, the scale and complexity of cybercrime incidents continue to increase with the growing technical capabilities of malware which means evolving harm as well as facilitating new crimes, such as the crypto mining malware which attacks digital currencies like Bitcoin.

> ***Our ability to manufacture fraud now exceeds our ability to detect it!***
> ***Al Pacino***

Last year, Lancaster University was subject to a sophisticated and malicious cyber attack which resulted in students' personal data being stolen. Fraudulent invoices were then sent to some students in an effort to elicit money. A 25-year old man from Bradford has recently been arrested on suspicion of committing Computer Misuse Act (CMA) and fraud offences, following this incident.

Finally, scams abound where least expected. Remember to be vigilant with your personal data. Check your phone bill as you could be charged for unsolicited 'premium short code text messages'. Also known as 'reverse billed' messages, premium rate text (SMS) messages come from four, five or six-digit numbers and are normally for subscription services such as games or weather updates. The texts generally cost about £1.50 each for which you might not realise you're being charged, and can mean you end up with a shockingly high phone bill. So do pay attention.

Zyber Global Events

The next **Stay Safe Online Webinar** by Zyber Global is due to take place on the 29 September 2020. Register now to attend.

Other events are as follows:

Gartner Cybersecurity Summit September 14 -17, 2020	European Cyber Security for Critical Assets Summit October 6-7, 2020	CyberSec&AI Summit October 8, 2020
In today’s risk reality, you have to anticipate new cybersecurity threats, understand the ongoing implications of COVID-19, deal with disruptive technologies and build resilience in a world where nothing is certain. The theme of the virtual Gartner Security & Risk Management Summit 2020 is to showcase how to create an agile security and IT risk management plans to manage the risk inherent in digital business and be better prepared for the next global shock.	CS4CA Europe is a CPD certified industrial security conference, uniting 100’s of senior critical infrastructure leaders who represent major players from the Energy, Oil & Gas, Utility, Power, Water, Chemical, Healthcare & Maritime industries. Some of the key themes include: • Cyber security in the 5G era • Governance in OT environments ....and much more.	The main theme for this year's conference: AI for privacy and security, CyberSec&AI Connected will explore the themes of AI for privacy and security, revealing the challenges and opportunities facing all those working and researching at the intersection of AI, machine learning and cybersecurity.
For further information: www.gartner.com/	For further information: https://www.cs4ca.com/	For further information: cybersecai.com

.

Zyber Global Events

Our Online Courses with INsig2 –
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
For an extra 15% off use coupon code **ZYBER** during checkout.

Legal Entities

Judges, lawyers and public prosecutors

Customised courses for legal entities on deeper aspects of digital forensics and forensic value of the evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings.

Law Enforcement

First responders, forensic investigators and analysts

Customised courses for law enforcement officials on procedures, techniques, and tools used in digital forensic analysis and how to apply them in their forensic investigations.

Private Sector

Corporations and small businesses

Customised courses for various 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.

Try our free course on Password Management
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/