Zyber Global

DECEMBER 2023 | ISSUE 41

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - December 2023, the 41st edition! This is where we bring you exciting updates from the dynamic world of cybersecurity!

November was an eventful month, marked by extensive travels and impactful engagements. At the beginning of November, I had the privilege of representing OCWAR-C (the West African Response on Cybersecurity and Fight against Cybercrime) in Takoradi, Ghana. There, I conducted a training session for prosecutors and law enforcement officials on cybercrime and electronic evidence. It was an enriching experience to collaborate once again with Lady Justice Afia Asare-Botwe and reunite with my fellow trainer, Yolanda Van Setten, after nearly a decade.

The journey then took me to Ankara, Türkiye, for the final Coordination Meeting of "Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of the European Convention on Human Rights Violations in Türkiye" project. Having been involved in this initiative for over four years, it is a moment of immense pride when we can reflect on our achievements. The project, aimed at bolstering the Turkish criminal justice system, has reached a pivotal juncture, and I am confident that our recommendations will all be implemented.

Working alongside the dedicated Council of Europe Ankara team, representatives of the Ministry of Justice, and the Justice Academy was truly rewarding. This collaboration highlights the power of international partnerships in enhancing legal frameworks and cybersecurity measures. As we wrap up another productive month and look forward to new adventures and challenges in 2024,let's continue to foster a world where cybersecurity and justice go hand in hand, protecting our digital landscapes and upholding human rights.

Stay tuned for more insights and stories in our upcoming editions. Here's to a December filled with learning and growth in the ever-evolving realm of cybersecurity!

Let us know what topics you would like to see discussed in future newsletters and remember to stay vigilant in the digital realm!

Keep safe! See you in 2024.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

A snow covered UK

This Month's Features

Zyber Focus Article

Interview with the dynamic duo, Kristine Hamann Executive Director and founder of Prosecutors' Center for Excellence (PCE) and Antonia Merzon ,Senior Attorney, Consultant, Author, Editor PCE.

Zyber News

A roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

Zyber Focus Interview

Kristine Hamann

Executive Director and founder of Prosecutors Centre for Excellence (PCE) and

Antonia Merzon

Senior Attorney, Consultant, Author, Editor, PCE.

This interview is with the dynamic duo, Kristine and Antonia who together through PCE (a non-profit organisation), provide policy expertise for modern prosecutors on cybercrime and cybercrime related issues. They promote best practices, spur innovations and implement solutions through their consulting and research services. They also support statewide prosecutor-led Best Practices Committees that have formed in 20 states. They host regular national meetings for prosecutors to share ideas on best practices and emerging issues. They provide a wealth of experience in tackling cybercrime.

1. Can you tell us about yourselves (separately) and your journey to working as a Prosecutor.

Antonia: To become a lawyer in the U.S., you must first obtain a Bachelor's degree from a university, then obtain a Juris Doctorate degree from a law school, and then pass the Bar Examination in the state(s) where you wish to practice. Law school is a three-year graduate program. During law school, many students work various law-related jobs through internships and externships. I knew that I was interested in criminal law, and had several jobs with prosecutor offices in New York while in law school. I joined the New York County (Manhattan) District Attorney's Office immediately after graduating and worked there for 11-12 years.

Kristine: I followed the same educational path as Antonia. I started in a large Wall Street firm doing corporate litigation. However, I realized that my interest was in criminal law and so I joined the New York County (Manhattan) District Attorney's office. I worked there for over thirty years, first doing violent crimes, and ending up on the Executive Staff of the office.

2. Can you share with the readers some success stories of when you were both prosecuting to date (anonymized of course)?

Antonia: I worked on many cases involving organized criminal groups committing complex forms of crime. These cases included burglary rings, pickpocket rings, identity theft rings stealing in numerous ways, and cybercrime rings conducting massive theft and money laundering operations. Figuring out how these groups commit their crimes, and building the evidence against them, can be challenging. Identity theft and cybercrime victims often feel there is no hope that the people who have victimized them will be prosecuted, so it is very gratifying to show them that justice can be sought on their behalf.

Kris:tine: I was a violent crime prosecutor at a time when New York City was awash in crime. I handled many homicide cases. Maybe the most notable was one where in one week a young crack addict shot 11 people in separate incidents, killing six. Those were bad times and luckily these types of crimes do not happen as frequently in New York City.

3. What are some of the pitfalls you faced when prosecuting these types of crimes?

Antonia: Organized criminal activity of any kind usually involves numerous suspects and victims, and it takes time and determination to untangle the threads of what has occurred. These cases often span multiple jurisdictions within the United States, and across the world, which can create challenges for gathering evidence and enlisting cooperation among law enforcement and prosecution agencies.

Kristine: Resources are always an issue. Now violent crime cases are heavily dependent on digital and forensic evidence such as surveillance videos, cell phone downloads, social media searches and complex forensics. Gathering this evidence is time consuming and expensive.

4. What have you achieved since the opening of the PCE?

PCE has created a respected presence in the prosecutor community in the United States. We distribute weekly Articles of Interest on policy issues to 2000 prosecutors nationally, and conduct national meetings on current topics,. We also undertake independent case reviews, and assess prosecutor offices with the goal of improvement and innovation. Some of our assessments are focused solely on the cybersecurity status of a prosecutor office.

5. What would you say to law enforcement in investigating these crimes?

Antonia: Never give up! Cybercrime can seem like a daunting investigative task, but these cases are successfully investigated. Investigators sometimes believe that a cybercrime must be the work of a sophisticated, international, tech mastermind. But with a little digging, many cases turn out to be the work of a local criminal who is not hard to identify or locate. And even if the case is international in scope, there are far more resources and partners available now to pursue those investigations. When you uncover a cybercriminal, you are likely protecting many future victims. It's worth the effort!

6. What advice can you offer those seeking a career in cybercrime?

Antonia: Hopefully, they are seeking a career in fighting cybercrime! There are so many ways to be involved in this effort. Whether as an investigator or a prosecutor. Whether working to improve an organization's or industry's cybersecurity. Whether working to identify and stay ahead of cybercriminals and their activity. There is so much opportunity in this area – find the role that fits and go for it!

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

Zyber News Roundup

Cybersecurity Executive Pleads Guilty to Hacking Hospitals

The chief operating officer (COO) of a US network security firm has pleaded guilty to compromising the IT systems of two hospitals in order to generate business for his company.

Securolytics executive, Vikas Singla, admitted hacking Gwinnett Medical Center (GMC) hospitals in Duluth and Lawrenceville, Georgia, as explained in a 2021 indictment.

The incidents, which took place in September 2018, began when Singla modified the configuration files of GMC Duluth hospital's ASCOM phone system, rendering over 200 handsets inoperable, the plea agreement revealed.

This disrupted the work of nurses and doctors who use the phones to coordinate "Code Blue" emergencies and other work, the document said:
'The same day, Singla managed to steal personal information on over 300 patients from a password-protected Hologic R2 Digitizer, which was connected to a mammogram machine at the Lawrenceville hospital'.

He also transmitted commands resulting in over 200 printers at both hospitals printing out the stolen personal information, interspersed with the message: "We Own You."

His attacks are said to have caused over $800,000 in "financial harm" to the hospitals, which Singla will pay back plus interest in restitution. Although the former COO could have faced a jail term of up to 10 years, prosecutors are recommending 57 months of home detention/probation due to the fact that Singla has been diagnosed with a rare and incurable form of cancer and a "potentially dangerous vascular condition."

Read more:

https://www.infosecuritymagazine.com/news/cybersecurity-executive-guilty

Japan's space agency suffers cyber attack, points finger at Active Directory

Japan's Space Exploration Agency (JAXA) has reported a cyber incident. Chief cabinet secretary Matsuno mentioned the incident in his morning briefing, telling reporters that the agency suspected a breach, possibly to its Active Directory implementation, so they conducted further research and found illegal access. JAXA has since shut down part of its network, including an intranet, as it seeks help to determine the extent of the incident.

Read more:
https://www.theregister.com/2023/11/29/jaxa_cyberattack/

US nuclear lab confirms data breach

The Idaho National Laboratory, a major US security lab, had its personnel system breached, with attackers leaking detailed data on thousands of the lab's employees. INL confirmed it suffered cyberattack.

Politically motivated threat actors SiegedSec claim to have breached the Idaho National Laboratory (INL), a US-based research facility instrumental in US nuclear energy research for decades. The attackers claim to have accessed a trove of sensitive data on INL's employees, including names, dates of birth, email addresses, phone numbers, Social Security numbers (SSNs), home addresses, employment details, and other information.

The Cybernews research team has confirmed that the leaked dataset contains sensitive data, and the dataset appears to be legitimate. NL confirmed the breach to Cybernews, saying the attack affected Oracle Cloud Human Capital Management (HCM) system.

Read more: https://cybernews.com/news/idaho-national-lab-data-breach/

KidSecurity's user data compromised after app failed to set password

KidSecurity, a popular parental control app that's used to track children, has exposed its activity logs, leaving users' private data in the hands of threat actors.

With more than a million downloads on Google Play, KidSecurity provides parents with services to track their children's location, listen to the sounds around the child to ensure safety, and set gaming limits.

On September 16th, researchers discovered that the app failed to configure authentication for Elasticsearch and Logstash collections.

Due to KidSecurity's oversight, user activity logs were left publicly available to anyone on the internet for more than a month, according to estimates.
"The exposure of sensitive data, such as user emails, phone numbers, and payment information in a kids' tracking mobile application, is of paramount importance due to the potential risks it poses," Bob Diachenko, who first identified the leak, told Cybernews.

"In the wrong hands, threat actors could misuse this information for identity theft, fraud, and unauthorized financial transactions, putting children and their families at significant risk. While location details were not exposed in this instance, the leak still represents a severe breach of privacy and security for the affected users."
Read more:

https://cybernews.com/security/kidsecurity-parental-control-data-leak/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

Black Hat Europe 2023 **EXCEL London,** **United Kingdom** **4-7 December 2023**	**The Cybersecurity@CEPS SUMMIT** **Brussels, Belgium** **14-15 December 2023**	**Octopus Conference 2023** **Bucharest, Romania** **13- 15 December 2023**
Black Hat provides attendees with the latest in research, development, and trends in Information Security. Here the brightest professionals and researchers in the industry come together for a total of four days—two or four days of deeply technical hands-on Trainings, followed by two days of the latest research and vulnerability disclosures in the Briefings. Black Hat Europe will be a Live, In-Person Event in London, December 4-7, followed one week later by a Virtual Experience including recordings of all Briefings and Sponsored Sessions, available December 13.	With its theme “Cybersecurity in the European Union: going beyond the Brussels Effect”, this year’s CEPS Cybersecurity Summit will be dedicated to exploring the EU’s profound influence on the global cybersecurity landscape, from the monumental GDPR to the groundbreaking Cyber Resilience Act (CRA). Despite this influence, problems have arisen when it comes to effective implementation and enforcement. The event will therefore address the challenges of moving from cyber policy initiatives to action and policy implementation despite challenges posed by the ever-changing cybersecurity landscape in the EU.	The Octopus Conference is part of the Octopus Project which is currently funded by voluntary contributions from Canada, Hungary, Iceland, Italy, Japan, Netherlands, UK and USA. Held every 12 to 18 months by the Council of Europe, the Octopus Conference constitutes one of the biggest and finest platforms of exchange in cybercrime gathering experts from more than 100 countries, international organisations, private sector and academia. The focus for the 2023 edition will be two-fold: • Securing and sharing electronic evidence: the tools are here – let’s use them! • Capacity building on cybercrime and electronic evidence: 10 years of Cybercrime Programme Office (C-PROC) – What impact so far; what’s next?
For further information **https://www.blackhat.com/eu-23/**	**For further information** **https://www.ceps.eu/ceps-events/cybersecurityceps-summit-2023/**	**For further information** **https://www.coe.int/en/web/cybercrime/octopus-conference-2023**

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