Zyber Global

SEPTEMBER 2021 | ISSUE 14

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 14th Edition, September 2021 of Zyber Global Centre's Monthly Newsletter

I hope that you are all well and making the best of the last few weeks of summer we have left. For those suffering from withdrawal symptoms as the Olympic Games Tokyo have ended. Take heart the Summer Paralympic games has started and it's also being held in Tokyo and doesn't end till the 5 September. Good news! Great Britain (GB) is doing very well in the medals table! This

Kew Gardens, London, UK

summer, the news has been full of various disasters all over the world our thoughts and prayers are with all who are suffering at this time. So stay safe, until next time.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

This month, the 'Interview Spotlight' is on Chris Painter, a former Federal Prosecutor and now the President of the Global Forum on Cyber Expertise (GFCE).

Zyber News

This is a roundup of the latest international cybercrime news.

Zyber Focus

Making The Digital Money Revolution Work For All
By Tobias Adrian and Tommaso Mancini-Griffoli, International Monetary Fund (IMF)

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is on Thursday 30th September 2021.

" We really need to up our game in cybercrime because it is not going away! We have to make sure as a community that is fighting cybercrime, that there are consequences for these acts. We are also working with the victims, we are not solely talking about putting handcuffs on criminals".

Chris Painter
President, GFCE

Zyber Spotlight

CHRIS PAINTER

President, Global Forum Expertise on Cybercrime

Chris Painter is an intrepid former Federal Prosecutor and Cyber Diplomat who has trail-blazed his way from Los Angeles to Washington, D.C raising the bar in cybercrime cases and domestic and international policies.

What led you to become a Federal Prosecutor and how did you come to specialise in cybercrime?

When I was at the law firm, I wanted to be in court. I liked the challenge and said to myself that 'I was gonna try this' and ended up loving it. I am passionate about justice and protecting victims and doing it in a fair way. I was touched when one of the legal papers in Los Angeles wrote a profile about me when I left to go to Washington where they interviewed a bunch of people, including defense attorneys I worked with, and they said that I was fair and looked out for both sides. I was really touched about that. I really do feel that, as a prosecutor, I believe that you can have an impact on people's lives. It is not about winning the case but making sure that justice is done. You have to exercise your discretion in a fair and equal way. It is a very different pool to be thrown in, from being at a law firm working on long-term research issues and going into court occasionally with pro bono cases. Here you were going to court daily, preparing cases with often complex issues. Trials were often longer and putting together a complex technical or financial case was like a puzzle that you had to put together.

I was a somewhat shy kid (though I grew out of that) and I really wanted to know what it was like to be in court and test my abilities so that was a driving factor. Like every prosecutor would say, as great as that job is, there are challenges and frustrations. It has not always been a smooth ride dealing with witnesses, sometimes seemingly unreasonable judges, and unanticipated problems with evidence. It certainly was never like on television where critical evidence shows up at the last minute and the defendant confesses. In real life, it takes a lot of work and investigation to put a case together. However, I was doing something that mattered, something that made a difference and that was great. When you enter the US Attorney's Office, there is an initial commitment for three years, I ended up staying for eight years. Every day, every case was a new challenge.

I am happy that I did it and I look back fondly on my time there. I recommend people do it. It is good to see and be a part of the process and to try to do justice.

I always had an interest in and a passion for combatting cybercrime. The way the US Attorney's Office works is that you do rookie work to start with. Los Angeles is the bank robbery capital of the world, lots of fraud cases and counterfeiting cases, immigration and that is just to cut your teeth. Then you go into a major area and mine was major frauds and, as a part of that, computer crime. This was a new area and really attracted me. It was fun.

When I started as Federal Prosecutor in cybercrime cases, I noted that many of my colleagues tended to stay away from them. They found it too technical. However, I really liked the cyber cases. I worked with some very techno-savvy FBI Agents and learning on the job was really good. It gave me a grounding and invaluable experience in prosecuting these type of cases.

What does the Global Forum on Cyber Expertise (GFCE) do? Where do you see its role in the future?

The goal of the GFCE is to coordinate capacity building across several different pillars including cybercrime and making sure these countries have the help they need.

I think it is a great organisation, there are about 60 countries, a lot of Civil Society, academia and industry. What is unique about the GFCE is that it is a true multi-stakeholder enterprise.

When I was at State, we did capacity building seminars in Africa and other regions. Justice was part of the team working with countries on cybercrime and investigatory cooperation.

Capacity building is foundational for countries around the world both to realize the benefits of a connected world and to deal with the threats. Yet the resources devoted to and organization of cyber capacity building is severely limited. Given the need, we can't afford to have the same three people in a country get trained by six different countries – we need to be smart.

Part of the GFCE goal is to coordinate capacity building. If a country seeks help we can match them with the funders and the implementers who can deliver what they need. Another goal of the GFCE is to highlight capacity building and make participants aware of the tools and resources that exist.

The GFCE has created the Cybil Portal with hundreds of best practice, research papers, and self-assessment tools, etc. that are available to all. In addition, the GFCE focuses its efforts through working groups including ones on national strategies and policy (also comprising diplomacy and norms), critical infrastructure and incident response, cybercrime, standards, and awareness and training.

The GFCE has also launched a Global Research agenda to help fill gaps. All these things are aimed to promote capacity building and make it accessible where it's needed. The GFCE was launched by the Dutch Government 6.5 years ago but it became an independent foundation just 1.5 years ago.

I think the GFCE has a huge part to play in this important area. We need to work as a community. We need more countries to have the relevant laws, the resources, and the capabilities and that is not easy, but we have lots of great partners.

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

Photo by Bermix Studio on UnSplash.

Zyber News Roundup

Parents of teens who stole $1 million in Bitcoin sued by the alleged victim

The parents of two teenagers allegedly responsible for stealing $1 million in Bitcoin are being sued.
According to court documents obtained by Brian Krebs, Andrew Schober lost 16.4552 in Bitcoin (BTC) in 2018 after his computer was infected with malware, allegedly the creation of two teenagers in the United Kingdom.
The complaint filed in Colorado accuses Benedict Thompson and Oliver Read, who were minors at the time, of creating clipboard malware.
The malicious software, designed to monitor cryptocurrency wallet addresses, was downloaded and unwittingly executed by Schober after he clicked on a link, posted to Reddit, to install the Electrum Atom cryptocurrency application.
During a transfer of Bitcoin from one account to another, the malware triggered a Man-in-The-Middle (MiTM) attack, apparently replacing the address with one controlled by the teenagers and thereby diverting the coins into their wallets.
According to court documents, this amount represented 95% of the victim's net wealth at the time of the theft. At today's price, the stolen Bitcoin is worth approximately $777,000.
"Mr. Schober was planning to use the proceeds from his eventual sale of the cryptocurrency to help finance a home and support his family," the complaint reads.
The pair tracked down during an investigation paid for by Schober, are now adults and are studying computer science at UK universities.
The mothers and fathers of Thompson and Read are named in the complaint. Emails were sent to the parents prior to the complaint requesting that the teenagers return the stolen cryptocurrency to prevent legal action from being taken.
However, the requests, sent in 2018 and 2019, were met with silence.
Schober's complaint claims that the parents "knew or reasonably should have known" what their children were up to and that they also failed to take "reasonable steps" in preventing further harm. In response, the defendants do not argue the charge, but rather have requested a motion to dismiss based on two- and three-year statutes of limitation.

Read more:
https://www.zdnet.com/article/parents-of-teens-who-stole-1-million-in-bitcoin-sued-by-alleged-victim/

Singapore:
"Sophisticated" Cyber-Attack Compromises Patient Data at Private Health Clinic

Personal and clinical data of more than 73,000 patients have been affected by a “sophisticated ransomware cyber-attack” on a private medical clinic in Singapore.
In a press release, Eye & Retina Surgeons revealed the attack took place on 6 August, compromising sensitive data including patients’ names, addresses, ID card numbers, contact details, and clinical information. However, no credit card or bank account details were accessed or compromised in the incident.
“Patients are now being progressively informed of this cyber-incident,” the release stated.
The clinic confirmed that the attack impacted servers and several computer terminals at its branch in Camden medical, although none of its other branches were unaffected. Thankfully, none of the eye specialist’s clinical operations were affected, and its IT systems are now securely restored.
The company noted it “maintains segregated networks and active medical records are maintained separately on a cloud-based system and thus were not accessed or compromised.”
The incident was reported to the Personal Data Protection Commission and the Singapore Computer Emergency Response Team (SingCERT), while the Eye & Retina Surgeons’ IT team is working with the Cybersecurity Agency of Singapore (CSA) and the Ministry of Health (MOH) to investigate the causes and perpetrators of the attack.
The clinic said there is no evidence that any compromised data has been published, but it will continue to monitor the situation. It added: “(Eye & Retina Surgeons) regrets this breach and wishes to assure its patients that it takes patient confidentiality very seriously.”
In a separate statement, Singapore’s MOH reassured citizens that the compromised systems are not connected to its own IT network, including the National Electronic Health Record, and “there have been no similar cyberattacks on MOH’s IT systems.”

Read more:
https://www.infosecurity-magazine.com/news/cyber-attack-compromises-patient/

Photo by Dimitry Demidko on Unsplash

Zyber News Roundup

US charges HeadSpin ex-CEO over fake $1bn valuation scheme

The US Securities and Exchange Commission (SEC) has charged the former CEO of HeadSpin for allegedly defrauding investors.

Founded in 2015 and based in Silicon Valley, HeadSpin markets itself as an AI testing, dev-ops, and mobile testing platform. The co-founder and former chief executive, Manish Lachwani, led the company until May 2020.

According to the SEC and the US Department of Justice (DoJ), the 45-year-old allegedly defrauded investors out of $80 million "by falsely claiming that the company had achieved strong and consistent growth in acquiring customers and generating revenue."

For approximately two years, the executive allegedly pushed for a valuation beyond $1 billion by inflating key financial metrics, doctoring internal sales records, and falsely increasing deal values currently under discussion with potential clients, making out that they were secure and guaranteed revenue streams.

The SEC says that through these methods, as well as the creation of fake, inflated customer invoices, Lachwani also "enriched himself" by selling $2.5 million of his own HeadSpin shares during a funding round.

However, his alleged actions did not go unnoticed, and an internal investigation by the firm's board found issues with HeadSpin's financial reporting.

According to the US agencies, the probe resulted in the startup's valuation being slashed from $1 billion to $300 million. The former CEO was then required to resign.

The SEC's complaint charges Lachwani with violating US antitrust laws. The regulator is pursuing penalties, an injunction, and a court order to prevent the former CEO from acting as an officer or director in the future.

Separately, the DoJ has filed one count of wire fraud and one count of securities fraud against the former executive. If convicted, Lachwani faces a maximum sentence of 20 years in prison for each charge, as well as fines of up to $250,000 and $5 million, respectively.

Read more:

https://www.zdnet.com/article/us-agency-charges-headspin-ceo-over-fake-1bn-valuation-scheme/

-

WhatsApp, Facebook, and Twitter fined for not storing user data inside Russia

A Moscow court has fined WhatsApp, Facebook, and Twitter for not storing the data of Russian users inside Russia's borders, Roskomnadzor, the country's telecoms regulator, announced.

The fines were imposed based on Russia's data-localization law. Passed in 2014 and entered into effect in 2015, the law requires that any company that caters to Russian users to store the data of those users on servers inside Russia.

Russia began enforcing the law in 2016, when, in a show of force, it banned LinkedIn.

Since 2019, the Russian government has been using a system of fines to warn and nudge foreign companies to comply before enacting a full ban again.

The Roskomnadzor said that almost 600 companies are now storing data of Russian users inside the country's borders, including some big names such as Apple, Microsoft, LG, Samsung, PayPal, and Booking.

Read more:

https://therecord.media/whatsapp-facebook-and-twitter-fined-for-not-storing-user-data-inside-russia/

Photo by Souvik Bannerjee on Unsplash

Photo by Brett Jordan on Unsplash

Photo by Bermix Studio on UnSplash

Zyber Focus

Making The Digital Money Revolution Work For All

By Tobias Adrian and Tommaso Mancini-Griffoli

First published on July 29, 2021, on the website of the International Monetary Fund's (IMF) and reprinted here, courtesy, Mr. Glenn Gottselig, Editor, IMF Blog

The link to the blog on the IMF website can be accessed here:
https://blogs.imf.org/2021/07/29/making-the-digital-money-revolution-work-for-all/

History moves in uneven steps. Just as the telegraph erased time and distance in the 19thcentury, today's innovations in digital money may bring significant changes in the way we lead our lives. The shift to electronic payments and social interactions brought on by the pandemic may cause similarly rapid and widespread transformations.

But we must look beyond the dazzle of technology and the alluring image of futuristic payment services.

At the IMF, we must identify and help countries solve the deeper policy trade-offs and challenges that are arising.

The rapid pace of change is a call to action—for countries to guide, and not be guided by, today's transformations. It is also important for the IMF to engage early with countries, and usher in reforms that will contribute to the stability of the international monetary system, and foster solutions that work for all countries. There is a window of opportunity to maintain control over monetary and financial conditions and to enhance market integration, financial inclusion, economic efficiency, productivity, and financial integrity. But there are also risks of stepping back on each of these fronts. We must enact the right policies today to reap the gains tomorrow.

We emphasize this in two papers published today, one on the new policy challenges, and one on an operational strategy for the Fund to engage with countries on the digital money revolution.

Digital money developing rapidly

Digital forms of money are diverse and evolving swiftly. They include publicly issued central bank digital currencies (CBDC)—think of these as digital cash, though not necessarily offering the same anonymity to avoid illicit transfers.

Private initiatives are also proliferating, such as eMoney (like Kenya's mobile money transfer service MPesa) and stable coins (digital tokens backed by external assets, like USD-coin and the proposed Diem). These are digital representations of value that can be transferred at the click of a button, in some cases across national borders, as simple as sending an email. The stability of these means of payment, when measured in national currencies, varies significantly. The least stable of the lot, which hardly qualifies as money, are crypto-assets (such as Bitcoin) that are unbacked and subject to the whims of market forces.

These innovations are already a reality, and growing rapidly. According to IMF data, CBDCs are being closely analyzed, piloted, or likely to be issued in at least 110 countries. Examples range from the Bahamas' Sand Dollar already in use, to the People's Bank of China's eCNY pilot project, to countries like the United States where the benefits and drawbacks of a digital dollar are still being studied. Stablecoins, still esoteric two years ago, tripled in value in the last six months (from $25 billion to $75 billion), while cryptoassets doubled (from $740 billion to $1.4 trillion). And adoption is global. eMoney accounts are not only growing much more rapidly in low- and middle-income countries than in the rich ones but are now also more numerous. Africa, in particular, is leading the way.

Opportunities are immense. A local artisan can receive payments more cheaply, potentially from foreign customers, in an instant. A large financial conglomerate can settle asset purchases much more efficiently. Friends can split bills without carrying cash. People without bank accounts can save securely and build transaction histories to obtain micro-loans. Money can be programmed to serve only certain purposes, and be accessed seamlessly from financial and social media applications. Governments can tax and redistribute revenues more efficiently and transparently.

Policy implications—opportunities and challenges ahead

We may well reap these benefits, but we must be aware of risks, and—importantly—of the bigger policy implications and tradeoffs. The challenges to policymakers are stark, complex, and widespread.

The most far-reaching implications are to the stability of the international monetary system. Digital money must be designed, regulated, and provided so that governments maintain control over monetary policy to stabilize prices, and over capital flows to stabilize exchange rates. These policies require expert judgment and discretion and must be taken in the interest of the public. Payment systems must grow increasingly integrated among countries, not fragmented in regional blocs. And it is essential to avoid a digital divide between those who gain from digital money services and those left behind.

Read more:

https://zyberglobal.com/my-blog

Zyber Global Events

Zyber Global's ***Stay Safe Online Webinar*** is on Thursday 30 September 2021 at 1600 hours BST. ***Register now to attend.***

OTHER CYBER SECURITY EVENTS

Cyber Security and Cloud Expo September 6-7 Business Design Centre, London September 13 -15 Virtual Event	**The Future of Cyber Security Virtual Conference September 21-22, 2021**	**The Joint PILON Cybercrime Working Group and SGBV Working Group 'Addressing Image-Based Abuse' webinar September 23, 2021**
This EXPO is taking place on 6-7 September at the Business Design Centre, and virtually from the 13-15 September. The Cyber Security & Cloud Expo event is co-located with the IoT Tech Expo, AI & Big Data Expo, and Blockchain Expo, so you can explore the future of these convergent technologies under one roof. Expand your knowledge and gain the security skills needed to steer your organisation to a more secure future.	The Future of Cyber Security's Virtual Conference will be a closed-door, invite-only conference, featuring 150 hand-picked senior executives from major UK firms. The Virtual Conference will be even more targeted than before, with exclusive speakers addressing urgent topics across multiple vertical industries. The conference will feature eight key talks and a live Q&A with speakers at the end of each session. It will also be possible to engage in the networking time delegates usually enjoy at a physical conference through post-event virtual drinks, and live prize draws to be spread across the three days. The event is aimed at board-level executives and senior IT decision-makers from government and industries including critical infrastructure, retail, healthcare, and financial services	We are very pleased to share that Part 2 of the joint PILON Cybercrime Working Group and SGBV Working Group 'Addressing Image-Based Abuse' webinar will be held on Thursday 23 September, 10am Canberra time. Panellists include representatives from Tonga Police, the Australian eSafety Commissioner and New Zealand Crown Law. This webinar follows on from Part 1 which was held on Thursday 26 August. Please note we are currently editing the webinar recording and poster for Part 1 and will share these with you in the coming weeks.
For further information: https://www.cybersecuritycloudexpo.com/global/?gclid=CjwKCAjwmqKJBhAWEiwAMvGt6NKpJjNr8n1S03FVVKQ53tXAPnt7Ejnnt3lwLbjf7W5qWwvUbLHOcRoC_zYQAvD_BwE	For further information: https://www.cybernewsgroup.co.uk/virtual-conference-september-2021overview/	For further information: To register to attend the upcoming Part 2 webinar, please provide your details in the following link: https://us06web.zoom.us/meeting/register/tZElceGppzkrH93JUZEszMjhTcqL81MLi9UO

Zyber Global Online Events

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

Courses per sectors

Legal Entities
Judges, lawyers and public prosecutors
Customized 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. a subheading

Law Enforcement
First responders, forensic investigators and analysts
Customized 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.
Customized 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.

Course Structure

- Full Text Reading
- Quiz after each chapter
- Case study final exam

At the end of each course, you will be issued a completion e-certificate which is immediately printable for your records. Certificates bring you CPD (Continuing Professional Development), CPE (Continuing Professional Education), CLE (Continuing Legal Education) points. The number of points depends 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 digital forensics learning path and get the most from your e-learning experience by using course bundles. https://bit.ly/3lNRYsj

Free Courses

Password Management
The course covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them
https://bit.ly/3eMu7FD