Zyber Global

JANUARY 2022 | ISSUE 18

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 18th Edition, January 2022 of Zyber Global Centre's monthly newsletter.

The Zyber Global team wishes you a prosperous and happy New Year! May 2022 be full of new achievements and success for you!

A New Year means a new start! I like to not just set goals for the new year but to also look back on the past year 2021 and evaluate it. 2021 has not turned out as I hoped it would. We ended 2020 talking about one of the worst hacks ever called "SolarWinds Breach". Since then, we have experienced so many other hacks, the two that stand out for me are Colonial Pipelines cyber-attack which led to the closure of one of the US' largest pipelines. The other is the Poly Network hack which is alleged to be the biggest crypto heist of all time. Hackers stole $600 million from Poly Network although they gave most of it back.

What do we think will happen in 2022? I would say more of the same. I am sure that we will during 2022 be comparing ever more outrageous hacks which will be called the worst or biggest ever. 2021 has not just been all about the hackers, law enforcement has shown that when they work together, they can make a dent in organized-crime activities. This resulted in law enforcement shutting down an encrypted phone network. I hope to see more of this in 2022.

Unfortunately, Covid is still with us. Like most people I wanted us to have been able to have put Covid behind us by now. Instead, we have a new Covid strain called Omicron running around the world. I am so glad that it's not as lethal as people initially thought it would be.

The new normal is not knowing what is going to happen next. So, I plan to spend some time evaluating the past year and set some goals for 2022. I have already decided that one of my goals will be to think of something every day that I am grateful for. So, let me start now.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

Today I am thankful for you and your continued support and encouragement for the work we do on the newsletter. This is what makes the team and I so excited to send you this our first newsletter of 2022.

We can also tell you that due to popular demand our next newsletter will be about capacity building. As always, do write in and let us know what topics you would like to see discussed in the November newsletter. We always appreciate your feedback! In the meantime, have a great 2022 and keep safe!!

This Month's Features

Zyber Spotlight

The interview spotlight this month is on **Mr. David Satola,** Leading Counsel, Technology & Innovation, World Bank.

Zyber News

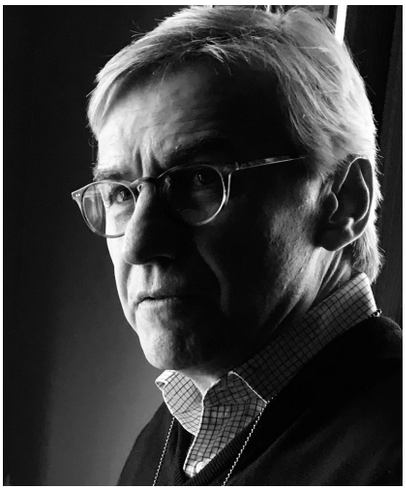
We have a roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

"If the pandemic demonstrated anything it was the almost total reliance of almost every aspect of our daily lives on on-line activity; and with that increased reliance, increased exposure and risk. ".

Mr. DAVID SATOLA,
LEADING COUNSEL, WORLD BANK



Zyber Spotlight

Mr. DAVID SATOLA
Lead Counsel, Technology & Innovation,
WORLD BANK

Can you tell us about yourself and your journey to working with the World Bank and specialising in cybersecurity?

My journey was definitely not in a straight line! It was rather the intersection of two strands of work from early in my legal career, one on human rights and the other on communications infrastructure. My first job after law school was with a human rights NGO in Geneva, the International Commission of Jurists. From there, I joined a big US law firm where I was in the tax department working on international M&A transactions, where one of our clients was a big US telco. I got assigned to that work and it stuck. So I approach cybersecurity from an information/infrastructure security standpoint with a heavy dose of human rights.

Can you set the scene for us and provide a brief overview of the World Bank and its cybercrime work.

For some, it is not obvious why the World Bank would be interested in combatting cybercrime. We are most often thought of as an international financing organization. That is true. It is also the case that we finance a lot of digital development work in our member states (the Bank is a treaty-based, UN specialized agency) and we are at the forefront of helping our members participate in the global digital economy.

We know there are huge advantages for countries to develop vibrant, durable and purpose-ready digitally-oriented economies that are ready to take advantage of globally connected markets in this digital age. But we also recognize the challenges faced by both developed and developing countries in ensuring the safety and security of their citizens – including preserving their basic human rights - in this globally connected world. As part of that, we know that supporting global cybersecurity, including building capacity to combat cybercrime, are key enablers of these efforts. We were very fortunate that the Korea World Bank Partnership Facility saw the merits of this work and has generously provided funding to support this work.

What is the World Bank's vision for increasing the global response to cybercrime? What is your role in that?

Our main focus areas is on awareness raising and capacity building. Within that, we really value collaboration and partnerships, and have learned that it is really through these collaborative and cooperative efforts that the global community will combat cybercrime. This is reflected in our capacity building toolkit (www.combattingcybercrime.org). We had seven other partners working with us on that. It was truly a collaborative effort, and it was in the process of producing the 1st edition of the Toolkit that we first encountered IAP and GPEN (thanks to a Korean prosecutor, Yonghwa Hong, who was seconded to the World Bank at the time) and other partners, like the Global Forum on Cyber Expertise (GFCE) (https://thegfce.org/). We're now working on publishing an updated 2nd edition of the Toolkit – again, a collaborative effort.

What have been some of your successes?

Well, in respect of combatting cybercrime, I think it was when one a couple of the original partners of the 1st edition of the Toolkit informed the Bank team that they had adopted the Assessment Tool that was developed as part of the Toolkit as their primary diagnostic framework. I realized then that we were really on to something, that there was real demand for this kind of collaborative approach, and that it wasn't just an abstract exercise.

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

Zyber News Roundup

NY Man Pleads Guilty in $20 Million SIM Swap Theft

A 24-year-old New York man who bragged about helping to steal more than $20 million worth of cryptocurrency from a technology executive has pleaded guilty to conspiracy to commit wire fraud. Nicholas Truglia was part of a group alleged to have stolen more than $100 million from cryptocurrency investors using fraudulent "SIM swaps," scams in which identity thieves hijack a target's mobile phone number and use that to wrest control over the victim's online identities.

Truglia admitted to a New York federal court that he let a friend use his account at crypto-trading platform Binance in 2018 to launder more than $20 million worth of virtual currency stolen from Michael Terpin, a cryptocurrency investor who co-founded the first angel investor group for bitcoin enthusiasts.

Following the theft, Terpin filed a civil lawsuit against Truglia with the Los Angeles Superior court. In May 2019, the jury awarded Terpin a $75.8 million judgment against Truglia. In January 2020, a New York grand jury criminally indicted Truglia (PDF) for his part in the crypto theft from Terpin.

A SIM card is the tiny, removable chip in a mobile device that allows it to connect to the provider's network. Customers can legitimately request a SIM swap when their mobile device has been damaged or lost, or when they are switching to a different phone that requires a SIM card of another size.

But fraudulent SIM swaps are frequently abused by scam artists who trick mobile providers into tying a target's service to a new SIM card and mobile phone controlled by the scammers. Unauthorized SIM swaps often are perpetrated by fraudsters who have already stolen or phished a target's password, as many financial institutions and online services rely on text messages to send users a one-time code for multi-factor authentication.

Compounding the threat, many websites let customers reset their passwords merely by clicking a link sent via SMS to the mobile phone number tied to the account, meaning anyone who controls that phone number can reset the passwords for those accounts.

Read more:
https://krebsonsecurity.com/2021/12/ny-man-pleads-guilty-in-20-million-sim-swap-theft/

Russia Fines Google $100m Over "Illegal" Content

Russia has slapped American tech company Google with a record-breaking fine for failing to remove "banned content."

A Russian court issued the $100m financial penalty on Friday in response to Google's alleged "*systematic failure to remove banned content*."

Although the financial penalty is the largest fine of its kind ever to be issued by a Russian court, it reportedly represents a mere 6.7% of the money Google made in Russia last year.

The court set the fine at $100m after being informed by Russia's internet regulator, Roskomnadzor, that Google's annual revenue in Russia in 2020 exceeded 85 billion rubles (approximately $1.5bn). This is the first time Russian authorities have calculated such a fine based on a tech company's turnover.

The fine follows legislation signed into law in July that requires large social media companies that operate in Russia to open an office in the country by January 1 2022 and maintain a physical presence there. Failure to comply with the law could result in restrictions or total bans.

Read more: https://www.infosecurity-magazine.com/news/russia-fines-google-100m-over/

Cybercrime incidents in 2021 should be a warning for the future

As Africa has moved toward digitalisation with vigour during the COVID-19 pandemic, cybercriminals have targeted the continent with just as much vigour.

The African continent provides a massive attack surface and low levels of technological literacy make for easier targets when compared to a continent such as North America.

South Africa has experienced its own fair share of cybersecurity incidents throughout 2021 and we hope that moving into the new year we all take the threat a bit more seriously.

Let's start our look back at cybercrime in South Africa in 2021 with arguably the biggest story – Transnet. In July, Transnet's IT systems were targeted by an attack. All signs pointed to a ransomware attack because of how Transnet's systems were suddenly struck offline and how methodically they had to be returned to service. September was a big month with debt recovery firm Debt-IN Consultants being breached.

Read more: https://htxt.co.za/2021/12/cybercrime-incidents-in-2021-should-be-a-warning-for-the-future/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

PrivSec South Africa Livestream Event 18 January 2022	**FinCrime Global 25-26 January 2022**	**PrivSec LATAM Livestream Event 26 January 2022**
The event will focus on the South African Protection of Personal Information Act (POPIA) plus regional insights on data protection, privacy, security and compliance. Attendees will hear from over 30 subject matter experts across10 sessions, debating and learning best practice from peers who operate in a range of industries. The aim is to facilitate thought provoking presentations, panel discussions and debates with both practical and theoretical approaches, to encourage collaboration and for each attendee to gain knowledge to drive change, innovation and progression in their organisations. Secure a free place today and gain access to the full programme of sessions live or with on-demand recordings.	Financial Crime is a complex, multi-faceted and ever evolving global issue which has become increasingly sophisticated in nature. FinCrime Global (formerly FinCrime World Forum) will return on 25-26 January 2022 for 2 days of expert insight, guidance and debate to help inform financial and banking professionals and senior practitioners working within the financial crime sector. Bringing together over 70 thought-leaders that are committed to fighting financial crime and lead the way on how we can do this better, more efficiently and effectively.	The event will focus on Brazil's LGPD plus regional insights on data protection, privacy, security and compliance. The event will seek to answer questions such as: • How to fight back against Latin America's cybercrime outbreak • Biometric identification: is Latin America sleepwalking towards widespread biometric surveillance? • Habeas data: how is the Latin America privacy, data protection, and security landscape developing? • How to manage cross-border data transfers in Latin America • Plus much more, view the agenda here
For further information: https://www.grcworldforums.com/privsec/privsec-south-africa	For further information: https://www.grcworldforums.com/fincrime/fincrime-global	For further information: https://www.grcworldforums.com/privsec/privsec-latam

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