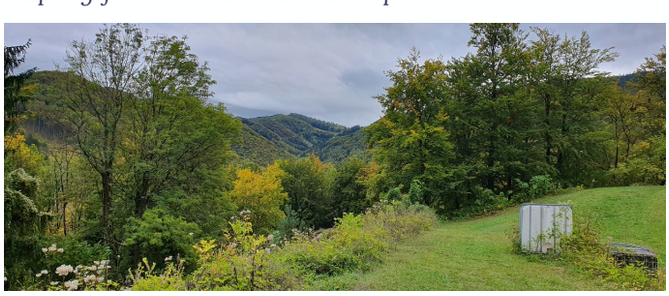
Zyber Global

MAY 2021 | ISSUE 10

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 10th Edition, May 2021 of Zyber Global Centre's Monthly Newsletter

In the UK, we have a couple of bank holidays this month; one at the beginning and the other at the end of May. It's been wet and windy here, so we are hoping for the weather to improve.



This month I will be delivering my last training on cybercrime to my former colleagues who are members of the National Black Crown Prosecution Association (NBCPA). The next webinar on electronic evidence and international cooperation will be held on 19th May 2021. The full details for this last webinar are on the event page. I have really enjoyed delivering the series and I have had a lot of fun meeting up with and reminiscing with former colleagues. So stay safe and have an enjoyable month!

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

This month, there are two articles, namely

- Our Commentary on the Post Office Horizon Case; and
- An Introduction to Cyber-Enabled Crimes

Zyber News

This is a roundup of the latest international cybercrime news.

Zyber Focus

This is an 'excerpt' of Esther George's training on Digital Evidence to the Zagreb Polytechnic, Croatia by Arsha Gosine, Head of Research, Zyber Global Centre

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is on Thursday 27th May 2021.

"Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm "

Anna Maria Chávez, Attorney, and former CEO of the Girl Scouts, USA

Zyber Spotlight

Commentary on the Post Office Case of Horizon – UK's most widespread miscarriage of justice by Esther George

On 23 April 2021, a group of thirty-nine (39) sub-postmasters/mistresses saw their names cleared at the UK Court of Appeal after a very long running complex legal battle with the UK Post Office (PO). The PO said it "sincerely apologises" for "historical failures".
The facts are that between 2000 and 2014, many PO sub-postmasters and sub-postmistresses were accused of stealing, misappropriation of funds and false accounting. Some paid back the monies it was alleged that they stole. While others pleaded guilty to offences they did not commit, serving jail time and obtaining a criminal record in the process. Many were financially ruined and have described being shunned by their communities.
It was later recognised that it was the PO's defective Horizon Accounting Software System which failed because of a number of 'bugs' in its system.
Horizon was first introduced into the Post Office network in 1999. The system, developed by the Japanese company Fujitsu, was used for tasks such as monetary transactions, accounting, and stocktaking. By 2000: Post Office literature stated that Horizon terminals were being installed "every five minutes" in 18,000 Post Office branches, with 63,000 Post Office employees trained to operate the system.
Very soon, sub-postmasters were complaining about bugs in the system. They reported shortfalls, some of which amounted to many thousands of pounds. The PO always responded that the system was not at fault.
Many stories have emerged where some sub-postmasters attempted to plug the gap with their own money, even remortgaging their homes, in an (often fruitless) attempt to correct an error.
Between 2000 and 2014, the Post Office prosecuted 736 sub-postmasters and sub-postmistresses - an average of one a week all based on the inaccuracy of information from a recently installed computer system called Horizon.
In September 2009: A campaign group on the issue, Justice for Sub-postmasters Alliance (JFSA) was formed by Alan Bates, a former Sub-postmaster and others.
By 2012: Investigative firm Second Sight conducted an independent inquiry into Horizon. In January 2012: The PO set up the Initial Complaint Review and Mediation Scheme, to which 150 former sub-postmasters sign up. Second Sight uses their testimonies to conduct another investigation.
By 2013: The PO finally admitted that there were defects within the Horizon software, but claimed the system had been fixed and was effective.
In 2014: A report found that the technology "was not fit for purpose" in some branches. The PO says that "there is absolutely no evidence of any systemic issues with the computer system".
In 2014: James Arbuthnot MP accused the PO of rejecting 90 percent of applications for mediation. The PO said that the claims by Arbuthnot were "regrettable and surprising". The MP then branded the company as "duplicitous".
In 2015: the PO scraped the independent committee overseeing the investigation, and terminated the Initial Complaint Review and Mediation Scheme without notice and published a report clearing themselves of any wrong doing. Later that year, Private Eye reported that the PO had ordered Second Sight to end their investigation just one day before the report was due to be published, and to destroy all the paperwork they had not handed over. The UK trade magazine Computer World UK reported that the PO had obstructed the investigation by refusing to hand over key files to Second Sight. The Post Office denied these claims.
In 2017, the JFSA took the Post Office to court through a group litigation action by 550 former employees, who were mainly ex sub-postmasters. By 2018, Second Sight's second investigation found that PO software experienced 12,000 communication failures every year, with software defects at 76 branches, as well as old and unreliable hardware.
Finally in December 2019, at the end of a long-running series of civil cases, the Post Office agreed to settle with 555 claimants. It accepted it had previously "got things wrong in [its] dealings with a number of postmasters", and agreed to pay £58m in damages. The claimants received a share of £12m, after legal fees were paid.
A few days later, a High Court judgement said that the Horizon system was not "remotely robust" for the first 10 years of its use, and still had problems after that. The judge said the system contained "bugs, errors and defects", and that there was a "material risk" that shortfalls in branch accounts were caused by the system.
The judgement also referred to Fujitsu's incompetence and that they were inaccurate about what they had told the PO in what was kept in the 'Known Error Logs'. It pointed out the PO's obstructive attitude to disclosure and their failure to consult and audit data.
The judgement spoke about the PO's institutional obstinacy and their lack of transparency and accuracy. Despite their own failings and that of Fujitsu, the PO confirmed earlier this year that it will retain its controversial Horizon contract with Fujitsu until 2024, following a one-year extension to its retail and accounting system agreement.

Zyber Spotlight cont'd

Commentary on the Post Office Case of Horizon – UK's most widespread miscarriage of justice - Esther George

---

"This approach by the Post Office has amounted, in reality, to bare assertions and denials that ignore what has actually occurred, at least so far as the witnesses called before me in the Horizon Issues trial are concerned. It amounts to the 21st century equivalent of maintaining that the earth is flat." –

Hon. Mr. Justice Fraser

Following the High Court ruling, more cases were brought forward to the Criminal Cases Review Commission (CCRC), an independent body which investigates suspected miscarriages of justice. So far, it has referred 51 cases back to the courts.

The ruling has also determined that these 39 convictions were also "an affront to the public conscience". This means that the postmasters may pursue civil action against the Post Office for malicious prosecution, seeking significant sums in damages.

In looking at this case there are a number of lessons we can learn from it, I have suggested four below:

1. In the first instance it is not an ideal situation to have an institution be the victim, investigator, and prosecutor in a case. The other complex matter was that they were prosecuting people who were either their own employees or those they had a contractual agreement of some sort with. It would be better in such cases that where a Government institution is the victim of an offence that either the investigation or the prosecution is performed by others such as the police and /or the Crown Prosecution Service (CPS) etc...

2. . In commissioning a large technological project such as Horizon, the customer should have the knowledge to work with the contractor to ensure that the contractor provides a system that is fit for purpose and takes into account the needs of the user. This is of ever-growing importance especially as the government is in the process of commissioning and installing other such projects.

3. Disclosure of evidence to the defence - How the law of evidence applies to automated computer-based decisions has wide-ranging implications across the public and private sector because of the growth of artificial intelligence in its capacity as a general purpose technology across every aspect of the economy means that the number of decisions nvolving software-based systems will increase both in the private sector and in the delivery of public services.

Computer evidence must follow the Common Law rule, that a "presumption will exist that the computer producing the evidential record was working properly at the material time and that the record is therefore admissible as real evidence".

The presumption of the machine functioning properly in practice means that the prosecution can rely on the presumption that a computer was operating reliably at all material times. It needs to be remembered that the presumption is rebuttable. The defendant has to raise the possibility that it was not, once that is done the prosecution will then have to prove that the computer was working properly at the material time. Section 129 of the Criminal Justice Act 2003 contains a similar presumption.

In my view this presumption was not really the problem in this case. Rather the problem was the fact that the prosecution did not make full and proper disclosure of the unused material in the case to the defence. On what we now know if such disclosure was made the presumption would have been rebutted. The PO did not comply with the guidelines in force at the time, they were the Attorney General's guidelines on disclosure' issued in 2005 and the supplementary guidelines on digital material issued in 2011, which is an annex to the general guidelines. The Attorney General's Guidelines are not detailed operational guidelines. They are intended to set out a common approach to be adopted in the context of digitally stored material.

4. A major problem that runs throughout the case is the lack of training for all involved. There was said to be a lack of training by the PO for the sub-postmasters and their staff utilizing the Horizon system.

The PO investigative and prosecution team should have been properly trained in respect of electronic evidence and its disclosure.

The Court (Judge) needs to take notice of the fact that the PO in their cases are the victim, investigator, and prosecutor. In such cases, in order to avoid future miscarriages of justice, it is essential that the judge hearing the case has been properly trained in respect of electronic evidence and its disclosure requirement to ensure that the PO has properly fulfilled its disclosure responsibilities.

Disclaimer: The views expressed above are my own.

Thanks: I would like to thank Stephen Mason (https://ials.sas.ac.uk/about/about-us/people/stephen-mason) who is a leading expert on Electronic Evidence. We discussed this case some years ago and Stephen has been involved in working on it and was kind enough to send me some very useful material to read.

A full copy of the Article can be found at:
https://zyberglobal.com/my-blog

Zyber Spotlight

An Introduction to Cyber-Enabled Crimes: Part 1 - by Arsha Gosine

The internet is a vast place where all sorts of information and articles can be sought and bought. It is used to transact business and connect socially. It is also open to abuse in many ways, in that it is used to commit acts of fraud; hacking; and other criminal activity.
In this article, we are going to look at some of the cyber-enabled abuse that takes place. These are crimes that do not depend on computers or networks but have been transformed in scale or form by the use of the internet and communications technology. They fall into the following categories:

Malicious and offensive communications, such as:

- Communications sent via social media
- Cyberbullying/trolling
- Virtual mobbing

Offences that specifically target individuals, including cyber-enabled violence against women and girls ('VAWG'):

- Disclosing private sexual images without consent
- Cyberstalking and harassment
- Coercion and control

Child sexual offences and indecent images of children, such as:

- Child sexual abuse
- Online grooming
- Prohibited and indecent images of children

Extreme pornography, obscene publications, and prohibited images

The NSPCC states that: '*Online abuse is any type of abuse that happens on the internet. It can happen across any device that's connected to the web, like computers, tablets, and mobile phones*'. With the growing reach of the internet, we see that abuse can and is happening online, through social media, text messaging, emails, chatrooms, and live streaming sites.

Let us take a look at some of the malicious and offensive communications which take place online.

Cyberbullying is any type or form of baiting online which involves sending abusive and hurtful comments across all social media platforms via phones or computers. Cyberbullying can take many forms such as harassment, denigration, flaming, impersonation, trolling, outing and trickery, cyberstalking and exclusion.

In the United Kingdom (U.K.), these offences can be prosecuted under the Malicious Communication Act 1988 and the Communications Act 2003. In a recent national bullying survey, by Bullying UK, 56% of young people said they have seen others be bullied online and 42% have felt unsafe online. Cyberbullying can happen 24 hours a day, 7 days a week and it can go viral very fast.

Then there are online threats which can take many forms including threats to kill, harm or to commit an offence against a person, group of people or organisation.

Disclosure of private sexual images without consent, for example, so-called "revenge porn" is a broad term covering a range of activities usually involving an ex-partner, uploading intimate sexual images of the victim to the internet, to cause the victim humiliation or embarrassment.
In the U.K, it is a criminal offence to re-tweet or forward without consent, a private sexual photograph or film, if the purpose was to cause distress to the individual depicted.

Continue reading:
https://zyberglobal.com/my-blog

Sources:
https://www.nspcc.org.uk/
https://www.bullying.co.uk/
https://www.cps.gov.uk/

Zyber News Roundup

Emotet Botnet

Emotet botnet harvested 4.3 million email addresses. Now the FBI is using "*Have I Been Pwned*" to alert the victims.
The FBI has handed over 4.3 million email addresses that were harvested by the Emotet botnet to the "*Have I Been Pwned*" (HIBP) service to make it easier to alert those affected.
HIPB, run by Australian security researcher Troy Hunt, is a widely trusted breach alert service that underpins Mozilla's Firefox's own breach alert notifications.
The FBI collected the email addresses from Emotet's servers, following a takedown in January. The Emotet malware botnet was taken down by law enforcement in the US, Canada, and Europe, disrupting what Europol said was the world's most dangerous botnet that had been plaguing the internet since 2014.
Emotet was responsible for distributing ransomware, banking trojans, and other threats through phishing and malware-laden spam.
For individuals or organisations that find their details in the data, Hunt suggests:

- Keep security software such as antivirus up to date with current definitions.
- Change your email account password, and change passwords and security questions for any accounts you may have stored in either your inbox or browser, especially those for services such as banking.
- For administrators with affected users, refer to the YARA rules released by DFN Cert.

Read more:
https://www.zdnet.com/article/emotet-botnet-harvested-4-3-million-email-addresses-now-the-fbi-is-using-have-i-been-pwned-to-alert-the-victims/?ftag=TRE-0310aaa6b&bhid=29633521617577276770654057469299&mid=13349810&cid=2354413351

US Arrests Alleged Crypto Mixer

Law enforcement officers in the United States have arrested a man on suspicion of laundering hundreds of millions of dollars worth of Bitcoin (BTC) through a cryptocurrency mixing service.
A crypto-mixing service—also known as a cryptocurrency tumbler—obscures the original source of potentially identifiable or "tainted" cryptocurrency by jumbling it up with other funds in a single pool.
A dual Russian and Swedish citizen Sterlingov is accused of unlicensed money transmission, money laundering, and transmitting money without a license.
In an affidavit, special agent to the Internal Revenue Service, Devon Beckett describes how Bitcoin Fog's administrator publicly advertised the organization's crypto-currency mixer service "as a way to help users obfuscate the source of their Bitcoin" on a Twitter page and through a clearnet site.
"Historically, the largest senders of BTC though Bitcoin Fog have been darknet markets, such as Agora, Silk Road 2.0, Silk Road, Evolution, and AlphaBay, that primarily trafficked in illegal narcotics and other illegal goods," wrote Beckett.
Beckett wrote that analysis of Bitcoin transactions, financial records, internet service provider records, email records, and additional investigative information identified Sterlingov as the principal operator of Bitcoin Fog.

Read more:
https://www.infosecuritymagazine.com/news/us-arrests-alleged-crypto-mixer/

Zyber Focus

Excerpt from Ms. Esther George's Presentation and Training to the Zagreb Polytechnic, Croatia

On the 26 and 27 April 2021 respectively, students at the Zagreb Polytechnic, Croatia heard from Ms Esther George on the following issues, namely:

- What is cybercrime and why worry about it;
- Illegal activities and cybercrime tools;
- Current trends in the perpetration of criminal acts;
- What is digital evidence;
- Types of digital evidence;
- Principles of good practice re digital evidence;
- Identifying the challenges offered by “digital evidence, including evidence in the “cloud”
- International cooperation and digital evidence looking at the global dimension of the Internet and the need for fast and efficient channels for international cooperation;
- ·Practical problems that may be experienced during any effort to cooperate internationally; and
- ·Cooperation between the public and private sectors in an international context

The course was very well received with positive feedback.

Ms George explained about data interference and gave an example of the 'I love you virus' which was a badly coded computer virus by a twenty-three (23) year old. This virus disrupted businesses globally from Merill Lynch and Ford to the British Parliament and the Pentagon. It caused billions in damages and exposed vulnerabilities that remain twenty (20) years on.

The virus which originated in the Phillippines was an email that said 'I love you' and was opened unwittingly by people across the globe.
The virus was instantaneous and in no time it wiped the hard drive and renamed and deleted files on the system.

Ms George also highlighted the various sources of digital evidence and said that every device has evidence, for example, laptop/iPad/watch/Gameboy/server/network storage devices/thumb drives, etc

Each device has its own specific characteristics which require experts in that particular device for the evidence to be extracted. New technologies emerge very rapidly which has to be kept up with

She said that digital evidence is invisible to the untrained eye and has its challenges. She identified some of these challenges as follows:

- identifying and locating the evidence;
- securing the hardware;
- the capture and analysis of data;
- maintaining the integrity and chain of custody;
- complying with the rules of court and admissibility.

The important steps to take when seizing and handling electronic data are to ensure that data integrity is maintained; that there is an audit trail; and that there is the right expert support.

Ms George also pointed out the need for international cooperation

In the final analysis, new technologies develop very quickly and there is a need for constant update not only of the new technologies themselves but also of the procedures and techniques that have to be applied in order to seize their content and analyse it. There is a need for highly-trained specialists in these emerging areas of cyber technology. Due to the borderless nature of cybercrime, it is incumbent on the international community to continue to work together in developing practices and procedures to ensure efficient cooperation in this field.

To learn more about cybercrime, see courses offered by Zyber Global Centre
www.zyberglobal.com

Zyber Global Events

Zyber Global's ***Stay Safe Online Webinar*** is Thursday 27 May 2021 at 1600 hours BST. ***Register now to attend.***

OTHER CYBER SECURITY EVENTS

IAP & Council of Europe "Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence" May 13, 2021	**NBCPA (CPS) presents: A Series of Webinars to inform on Cybercrime and Cybersecurity** May 19, 2021	**Gulf Information Security Expo and Conference (GISEC) Global 2021** May 31st, 2021 - June 2nd, 2021 United Arab Emirates, Dubai
This Webinar is presented by the IAP, the GLACY+ project of the Council of Europe and the European Commission, and the Octopus project of the Council of Europe. The webinar will focus on procedures for Direct Cooperation with Service Providers in Foreign Jurisdictions, as foreseen in the 2nd Additional Protocol to the Budapest Convention.	This is the last in the series of one-hour Webinars, open to NBCPA members and CPS staff only. **Webinar 3: 19 May 2021.** Electronic Evidence and International Cooperation The training will be delivered by Esther George LLB (Hons), LLM, MA, Cybercrime and Cybersecurity Consultant and CEO, Zyber Global Global Centre https://zyberglobal.com/	The pandemic accelerated the rise of the digital economy, forcing governments globally to rethink several industries' functioning. It was the power of digital processes that helped keep the economy functional. GISEC's hard-hitting conference agenda brings together handpicked global CISO's, CIO's, CTO's, Big Thinkers & Futurists, Regulators & Policymakers at the brand new Government, Finance, Healthcare, Telecom, Energy & Utilities conference tracks, hear them unpack innovative strategies for creating a robust cyber-resilient ecosystem that inspires trust in the digital economy.
For further information: https://www.coe.int/en/web/cybercrime/enhanced-cooperation-and-disclosure-of-electronic-evidence-towards-a-new-protocol-to-the-budapest-convention	For further information https://www.nbcpa.org.uk	For further information: https://www.gisec.ae/?ref=infosec-conferences.com

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