Zyber Global

OCTOBER 2021 | ISSUE 15

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 15th Edition, October 2021 of Zyber Global Centre's monthly newsletter.

I feel like 2021 is speeding past, it's October already! Just in case you had not guessed my favorite season is summer, so October with its rainy cold days is just a reminder that winter is just around the corner.
On the positive side, October is not only Cybersecurity Awareness Month but also Black History Month

If you are in London during October and not sure what events are on during Black History Month, go to the website of "Visit London" where they have a full programme of events you can attend.

*There are a number of cybersecurity events happening this month a few are listed on our events page and we will be hosting our '**Stay Safe**' online webinar as well. Since Covid 19 and the move to home working we have seen a massive increase in cybercrime and individuals and organisations have to step up and take responsibility for ensuring that they are protected online. A very basic thing is to "**just think before you click**". Or as Cybersecurity Awareness Month puts it "**Stop, Think, Connect**."*

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, keep safe!!

Esther George, CEO Zyber Global Centre

BEST REGARDS
ESTHER GEORGE

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Ian Walden, Professor of Information and Communications Law and Director of the Centre for Commercial Law Studies, Queen Mary, University of London, and Of Counsel to Baker McKenzie.

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Focus

The focus this month is an article on 'The Post Office Horizon Scandal' by Stephen Mason.

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is due to take place on Friday, October 29, 2021 register now to attend.

"On a domestic level, more investment in the criminal justice system at every level. Successive governments have run down our criminal justice system to the detriment of the public and the benefit of those wanting to do us harm. Greater public education is also key. Internationally, on-going initiatives to deepen and broaden co-operation between regulators, law enforcement and industry are key.".

PROFESSOR IAN WALDEN
QUEEN MARY, UNIVERSITY OF LONDON

Zyber Global – Tel: 07426719579 Privacy Policy Register
To unsubscribe contact us at office@zyberglobal.com

Zyber Spotlight

IAN WALDEN
Professor of Information and Communications Law and Director of the Centre for Commercial Law Studies, Queen Mary, University of London, and Of Counsel to Baker McKenzie

Can you tell us about yourself and your journey to where you are today?
I became an academic in 1987, becoming a research assistant at Nottingham Trent University, researching data protection law. I moved to the Centre for Commercial Law Studies at QMUL in 1992 and have been here ever since! I have also been associated with the law firm Baker McKenzie since 2001, having previously worked with Bird & Bird and Tarlo Lyons. I have shown a distinct lack of imagination with regard to my place of employment!

What are some of the highlights of your career to date?
Difficult to say, but getting my PhD, becoming a solicitor, and being appointed a Professor were certainly proud moments. Similarly, publishing my first article and book was a great feeling. Traveling to new, weird and wonderful places for work has been a constant highlight.

As the Professor of Information and Communications law and the Director of the Centre for Commercial Law Studies, Queen Mary, University of London, can you share with us some of the challenges that you have faced since taking up the role?

The main challenge of being an academic in the field of cybercrime, technology, media, and telecommunications law is keeping up with the evolving technologies and market developments and then trying to figures out the legal implications. I have rarely been able to teach the same content twice, as things are always changing.
I have been Director of the Centre since 2018, so I have had to manage a department of over 80 people and over a thousand students during the pandemic, which has been the most challenging time of my career to date.

What training on cybercrime and or cyber security if any is being offered by Queen Mary?
We teach postgraduate courses on cybercrime, examining the substantive offences and the digital forensic aspects, and information security. We also offer these as executive education courses, on both a bespoke and public basis.

What sparked your interest in cybercrime and cyber security?
As noted above, my first job was researching data protection, so cybercrime and cybersecurity were always related aspects. Criminal law always felt exciting, with great stories to tell. Until recently, cybersecurity has been the poor relation but is now coming into its own and getting the attention it deserves.

What advice do you give to your students and colleagues who want to have a similar career to yours?
Difficult to say, as my career feels like it owes a lot to happenstance. However, I have also been incredibly fortunate to be passionately interested in the field in which I work; as well as having the freedom and flexibility to get involved in lots of different activities. Be open to opportunities!

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

Zyber News Roundup

Large-Scale Phishing-as-a-Service Operation Exposed

Microsoft uncovered a large-scale, well-organization, and sophisticated phishing-as-a-service (PhaaS) operation.
The turnkey platform allows users to customize campaigns and develop their own phishing ploys so they can then use the PhaaS platform to help with phishing kits, email templates and hosting services needed to launch attacks.
Microsoft researchers discovered the operation, marketed by criminals as BulletProofLink, when they found a high volume of newly created and unique subdomains—more than 300,000 in a single run, according to a post published by the Microsoft 365 Defender Threat Intelligence Team.

With more than 100 available phishing templates that mimic known brands and services—including Microsoft itself–the BulletProofLink operation is responsible for many of the phishing campaigns that impact enterprises today, they said.

Phishing is a common way for cybercriminals to dupe people through socially engineered emails into giving up their credentials to online accounts that can store sensitive data. Phishers use these emails—which sometimes fool people by impersonating a trusted company, application or institution–to direct people to specially crafted phishing sites so they can enter credentials, thinking they are doing so for a legitimate reason.

Phishing is often a gateway into other criminal activity; phishers sell credentials obtained through campaigns on the dark web, and they can be used by ransomware gangs as an entry point into networks to deliver ransomware attacks, among other nefarious activity.
While previously, criminals who wanted to launch these attacks had to build phishing emails and brand-impersonating websites on their own, "the phishing landscape has evolved its own service-based economy," researchers said. Now attackers can just purchase all the resources and other infrastructure they need to launch phishing attacks without investing a lot of time or effort, researchers said.
Read more: https://threatpost.com/phishing-as-a-service-exposed/174932/

EU chief announces cybersecurity law for connected devices

European Commission President Ursula von der Leyen announced on the 15 September a Cyber Resilience Act aimed at setting common cybersecurity standards for connected devices.
"We cannot talk about defence, without talking about cyber," von der Leyen said in her annual State of the Union speech in Parliament. "If everything is connected, everything can be hacked," she added noting that the growing number of connected devices also increases vulnerability to cyber-attacks.

According to von der Leyen, the rapid spread of digital technologies "has been a great equaliser in the way power can be used today by rogue states or non-state groups" to disrupt critical infrastructures such as public administration and hospitals.
The Commission initiative adds to an existing proposal for a Directive on Security of Network and Information Systems, commonly known as the NIS2 Directive. NIS2 expands the scope of the previous directive, by raising the cyber security requirements for digital services employed in critical sectors of the economy and society.

Read more:
https://www.euractiv.com/section/cybersecurity/news/eu-chief-announces-cybersecurity-law-for-connected-devices/

AUKUS Defence Pact Between US, Britain & Australia

AUKUS (a trilateral security pact between Australia, the United Kingdom, and the United States) was announced by US President Joe Biden, UK Prime Minister Boris Johnson, and Australia's Scott Morrison on Wednesday 15th September. The new security partnership is one of the most significant international agreements since the end of the Cold War.

While they did not mention China, AUKUS is being widely viewed as an effort to counter Chinese influence in the South China Sea. The pact, which will also see the allies share cyber capabilities, artificial intelligence and quantum technologies, is a major strategic shift and is clearly an effort to counter China that will see the US and UK give Australia the technology to build nuclear-powered submarines.
Read more:
https://www.cybersecurityintelligence.com/blog/aukus-defence-pact-between-us-britain-and-australia-5877.html

Zyber Focus

The Post Office Horizon Scandal
Stephen Mason

The Post Office Horizon scandal has probably come to the attention of most lawyers over the last 12 months. There are a number of significant issues other than legal questions that surround the scandal, and Paul Marshall of Cornerstone Barristers, Gray's Inn, succinctly summarises them in a lecture he gave at the University of Law on 3 June 2021 ('Scandal at the Post Office: The intersection of law, ethics and politics', to be published in the 2022 issue of the Digital Evidence and Electronic Signature Law Review).

This discussion considers what is, arguably, the underlying legal cause of the scandal – that computers are presumed to be reliable, and the reliance on this presumption by a private prosecutor: the Post Office.

Summary of circumstance leading to group action

A group of ex-sub-postmasters and sub-postmistresses formed The Justice For Subpostmasters Alliance (JFSA) in 2009 because of experiencing significant problems with how the Post Office dealt with apparent shortfalls in their accounts after the introduction of the Horizon IT system in 2000. Following years of campaigning with the support of many MPs, in 2012 the Post Office appointed Second Sight Support Services Limited, a firm of independent forensic accountants, to investigate the claims being made about the Horizon system. In 2013 an Initial Complaint Review and Mediation Scheme was established to investigate individual cases.

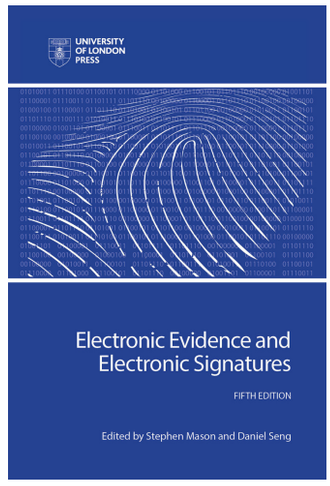
A Working Group, comprising of representatives from Second Sight, the Post Office, and the JFSA was established with an independent chair. The Scheme closed to applicants after twelve weeks. On 9 April 2015, the Post Office ended the Scheme Working Group and terminated the contract with Second Sight, together with that of the independent Chairman. The draft of Part Two of the Report by Second Sight was due to be released to the Working Group on 10 April 2015, but the action of the Post Office prevented this from taking place. The second part of the Second Sight Report eventually appeared on a journalists' website.

In 2015, Freeths LLP agreed to represent those ex sub-postmasters and sub-postmistresses that wanted to take part in any legal action. Therium Group Holdings Limited funded the litigation. A Group Litigation Order was subsequently made on 22 March 2017 by Senior Master Fontaine and approved by the President of the Queen's Bench Division.
The first trial concerned the contractual position between the Post Office the sub-postmasters and sub-postmistresses. The judgment is in Bates v Post Office Ltd (No 3) [2019] EWHC 606 (QB). (http://www.bailii.org/ew/cases/EWHC/QB/2019/606.html)

The second trial, dealing with the Horizon software, took place between 11 March 2019 and 22 July 2019. Between the end of the second trial and the judgment, the parties sought mediation. An agreement was reached on 11 December 2019. The Confidential Settlement Deed was eventually made public.
(https://www.onepostoffice.co.uk/media/47518/20191210-glo-confidential-settlement-deed-executed-version-redacted_-003.pdf.)

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

For concise and specific information on Electronic Evidence and Electronic Signatures, see book by Stephen Mason and Daniel Seng.



Zyber Global Events

The next **Stay Safe Online Webinar** by Zyber Global is due to take place on Friday, October 29, 2021. Register now to attend.

OTHER CYBERSECURITY EVENTS

International Conference on Criminology and Digital Forensics ICCDF **October 21-22, 2021** **London, United Kingdom**	**The 15th International Security Conference (ISEC) 2021** **October 21-22, 2021, Seoul, Korea**	**Techno Security & Digital Forensics Conference** **25 - 27 Oct 2021,** **Hilton La Jolla Torrey Pines,** **San Diego, USA**
An International Conference on Criminology and Digital Forensics which aims to bring together leading academic scientists, researchers, and research scholars to exchange and share their experiences and research results on all aspects of Criminology and Digital Forensics. It also provides a premier interdisciplinary platform for researchers, practitioners, and educators to present and discuss the most recent innovations, trends, and concerns, as well as practical challenges encountered and solutions adopted in the fields of Criminology and Digital Forensics	ISEC 2021, Korea's largest security conference, discusses cybersecurity. With the theme of "DIGITAL: SECURITY", ISEC 2021 is expected to be a place to share the latest trends and information. ISEC 2021 will be held as a hybrid event, offline and online at the same time. Anyone in the world can experience the Republic of Korea's security solutions and trends. The lecture of ISEC is approved for CISSP credits. If you pre-register online, you can listen to ISEC's online lecture for free.	Techno Security & Digital Forensics Conference provides a unique education experience that blends together the digital forensics and cybersecurity industries for collaboration between government and private sectors. The purpose is to raise international awareness of developments, teaching, training, responsibilities, and ethics in the field of IT security and digital forensics. Educational sessions cover topics within the following primary tracks from which CPE credits can be earned: Audit/Risk Management, Forensics, Investigations, Information Security. Learn from industry experts, connect with leading suppliers, and discover the latest innovations in cybersecurity and digital forensics.
For further information: https://waset.org/criminology-and-digital-forensics-conference-in-october-2021-in-london	For further information: https://www.isecconference.org/eng/index.html	For further information: https://10times.com/techno-security-digital-forensics-conference

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