Thursday Thoughts – 10th June 2021

What a great week. I went for my first social meeting inside with a group that was not family and I've also had so many interesting positive conversations about building back, moving forwards and what the new normal could look like. It has been great to see the business community emerging from their enforced hibernation. Today's Chamber Breakfast Matters with Manchester Airport's Adam Jupp gave us some insights to life at the airport and how their experience was similar to that of many of our own - just on a larger scale!

So what is in this week's Thursday thoughts. Guidance comes in the form of an explanation of the new SCCs, advice for schools facing FOI and SAR requests this summer as well as an explanation of "Pen Testing" and what's in the EDPB annual report. More news of ransomware in schools and given the enormous confusion regarding the scope and nature of the GPDPR, among both healthcare practitioners and the general public the welcome news that this has been paused for now.

I have been looking for something that families could use to get the cyber security message across to all generations and have shared a set of awareness videos will help you explain the risks of public wifi, strong passwords, and how to avoid being scammed. Before you dismiss the "fake mom" idea it is very real. I heard last week of a mum who was nearly scammed by a "fake daughter" – don't let it happen to you.

Blogs of the Week

Fanni Breczku - Twitter Launches New Subscription-Based Service, Twitter Blue.
Alex McCann – How To Engage With Purpose On Social Media
Wizer - Family Data Security Advice – Some great videos

Post Schrems II – SCCs Explained

The new European Union standard contractual clauses for international data transfers came into force last week. We all know these are important. But why now and what do they say? The why is really a result of the Schrems II ruling and the fact that GDPR identified an urgent requirement to write new SCCs because many of the old ones came from the pre-GDPR era. As for the what. Phil Lee from Fieldfisher has written a very comprehensive answer for the IAPP. Headlines are:

- The new SCCs have a "modular" structure with clauses for:
    - Controller-to-controller transfers (Module 1)
    - Controller-to-processor transfers (Module 2)
    - Processor-to-processor transfers (Module 3)
    - Processor-to-controller transfers (Module 4).
- There is a recognition that a non-EU entity can be a data exporter.
- There is provision for multiple data exporting parties to contract, and for new parties to be added to them over time.
- Prior SCCs can still be used for "new" data transfers for a 3-month transition period.

- Prior SCCs can continue to be used for existing data transfers for up to 18 months

You can read the full article here: https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/

Ever wondered what "Pen testing" is?

Pen testing can establish how easy would it be for an attacker to get unauthorised access to your network and many businesses consider it because it allows them to monitor and test their defences. The NCSC have just issued some really helpful guidance on what "good pen testing" looks like. Highlighting that the choice of tester is critical. If you are thinking about a penetration test I recommend you read this before you start.
https://www.ncsc.gov.uk/blog-post/penetration-testing-what-is-it-and-who-is-it-for

FOI Guidance For Schools and Colleges – Proactive Publication

One of the things that was discussed in a session at the ICO conference this year was the idea to proactively publish data that you could be asked for under FOI. Many schools already provide a wealth of such information. This year, as changed marking for exams and pandemic impact the education system it may be helpful for schools and colleges to publish more information than they ordinarily would. Particularly about the processes and frameworks they intend to use for teacher assessments. Schools will already be preparing for information requests about teacher assessments and the ICO recommends that they make sure to have a procedure to quickly identifying with each type of request (SAR/FOI) so they can be dealt with effectively. Proactively publishing as much detail as possible about the process for determining grades and publish as much anonymised performance data as you can afterwards may reduce the number of requests you receive. A word of caution make sure no personal data is published! Oh and be sure to check out their FOI toolkit (launched last year). You can read the guidance here: https://ico.org.uk/about-the-ico/news-and-events/icos-blog-on-its-information-rights-work?utm_source=linkedin&utm_medium=information+commissioner%27s+office&utm_term=48fd8d2e-73e9-42c9-93a2-88ba2d5d299e&utm_content=&utm_campaign=#9june21

EDPB Annual Report Published

The EDPB Annual report has been published. This gives a detailed overview of the work of the EDPB and what it plans to do in the next 12-24 months. This includes advancing harmonisation and facilitating compliance, supporting effective enforcement and efficient cooperation between national SAs and promoting a fundamental rights approach to new technologies. The EDPB also intend to engage with the international community with a focus on cooperation in enforcement and will promote and increase awareness of the use and implementation of transfer tools. Link to the report: https://edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2020_en

NHS Digital Delays GPDPR

Given the concern among healthcare practitioners and the general public it is good to hear that NHS Digital has delayed GPDPR. The whole thing doesn't seem to have been well considered. Neither Medical Professionals nor patients have had enough time to consider the options, seek guidance, and make a rational decision based on the facts. Safeguards like Pseudonymisation are complex and the questions such as where is the "key" going to be held so that patients cannot be reidentified have yet to be answered satisfactorily. There is concern about what is in scanned PDF documents, will these be redacted. Some still have questions over selling data (which some of the gurus say won't happen and others say will). These coupled with the fact that contrary to all the GDPR guidance we are being asked to "Opt Out" rather than "Opt In" makes it troubling to say the least. Let's hope NHS digital really do take more time to engage with its stakeholders, and consider the feedback it is receiving about the plans. At present the jury is very much out!

News

Another Schools Ransomware attack

Two schools in Kent were closed this week after hackers broke into their servers, stole data and encrypted pupil information. The schools were not able to confirm exactly what information hackers have access to and urged parents to warn their banks just in case these details had been taken. The hackers told the schools what information they have access to and although "they did not appear to have access to the School Information Management System" that data had been encrypted so it could not be accessed.

JBS confirms it $11 million following a ransomware attack

The world's largest meat processing company JBS has confirmed that it paid a ransom of $11 million in bitcoins after it suffered a ransomware attack late last month. The attack on JBS affected operations in Australia, Canada, and the U.S and is linked to REvil (aka Sodinokibi) a Russia-linked cybercrime group.

27 Million Messages between Criminal Gang Members Intercepted

This week more than 800 arrests in 18 countries took place in what is being called the "biggest ever law enforcement operation against encrypted communication." Across the world seizures included 55 luxury vehicles, 8 tons of cocaine, 22 tons of cannabis/cannabis resin, 250 firearms, and in excess of $48 million in various currencies and cryptocurrencies. The FBI and Australian AFP ran an encrypted chat service of their own for almost 3 years in a bid to probe transnational and serious organized crime and bring about these arrests.

MS Office Vulnerabilities

News this week of "parsing mistakes made in legacy code found in Excel 95 file formats (MSGraph.Chart.8)" - in essence a legacy equation editor. Although this is a defunct feature in Word it is possible for the code to be used to attack a user's computer. Windows users are being recommended to apply the recent patches as soon as possible.

Fines

Luxemburg Data Protection Authority proposes a $425 million fine for Amazon.com Inc
The CNPD in Luxemburg is Amazon's lead privacy regulator in the EU because Amazon has its EU HQ there. In a draft decision which calls out Amazon's privacy practices and GDPR breaches the CNPD has proposed a $425 million fine and asked other EU national authorities for comment. The fine relates to the collection and use of personal data (insiders say it isn't related to Amazon Web Services). Let's see what the final fine is!

3 companies fined more than £100,000 each for Unsolicited Marketing Texts/Calls
This should come as a warning for those thinking they won't get caught out sending those spam marketing text messages or making unsolicited marketing calls. This week the ICO issued 3 fines in excess of £100K to companies who were doing just that. In all cases, the companies did not have the valid consent required to send direct marketing and this is against the law. This comes after last week's Amex unsolicited marketing email fine. Where Andy Curry, ICO Head of Investigations advised ***"I would encourage all companies to revisit their procedures and familiarise themselves with the differences between a service email and a marketing email"***.

Blogs and Video of the Week

Fanni Breczku - Twitter Launches New Subscription-Based Service, Twitter Blue.
This discussion is a must for Twitter users who want to know about Twitter's newest subscription service Twitter Blue. Fanni thinks Twitter has "completely missed the mark". The problem is not that Twitter has introduced a subscription-based service but that it put what most platforms offer as essential features, like editing a tweet, behind the paywall. The link is here: https://rewardagency.co.uk/marketing/new-twitter-service-twitter-blue/

Alex McCann – How To Engage With Purpose On Social Media
If you have not thought about engaging with purpose, rather than just engaging on SM you will find this blog from Alex McCann helpful. I really like the idea of dedicating time "Specifically For Engagement" and will be trying Alex's his suggestion to find a quiet space, set a timer and engage. Which of the other ideas chimes with you? Is it the list of non-negotiables who you regularly engage with, or having a dream list of ideal clients or have you simply forgotten the golden rule for engagement? You will find the Blog here: https://altrinchamhq.co.uk/how-to-engage-with-purpose-on-social-media/

Wizer - Family Data Security Advice – Some great videos
I have been looking for something that families could use to get the cyber security message across to all generations. This set of awareness videos will help you explain the risks of public wifi, strong passwords, and how to avoid being scammed and this time not in an office but in a home environment. Before you dismiss the "fake mom" I heard last week of a mum who was nearly scammed by a "fake daughter" – don't let it happen to you or your loved ones. https://www.wizer-training.com/personal-safety-security-awareness-videos?utm_content=family_edition_page