THURSDAY THOUGHTS

Well this week whizzed past again and here we are on a Friday finishing off Thursday Thoughts. It remains my aspiration to get this blog out on a Thursday, just for now writing it on Thursday and finishing it on Friday will just have to do.

This week there is news on the latest NHS Test and Trace, which has apparently much improved and has at least involved a security specialist from the UK national Cyber Security Centre in its development. Let's see if it works, and more important how many people sign up to use it! If it's a way of returning to some semblance of normality I think many will be keen to take part. After all we are all so willing to have smart speakers, the internet of things and use platforms like Tik Tok which all collect much more of our personal information than this app.

So, what else is on this week? An explanation about the Schrems II Privacy Shield ruling, updates on where TikTok will be based, latest patches, warnings about Chrome browsers, using Amazon Alexa on smart speakers, the Samsung 'Find My Mobile' app and details of the latest Microsoft patches. Some great advice on phishing from the NCSC and from advice from yours truly on data breaches.

My "Blogs of the week"

Sheridan Voysey - Here's Why You're So Tired Right Now – and What to Do About It
Kevin Keen - Is Data Protection on your Board Radar?

The NHS Test and Trace App – Released "AGAIN"

A new version of the NHS Test and Trace app is being released for trials this week. This time a senior security architect from the NCSC was involved. From what I have seen what is being proposed is more than the simple digital contact tracing app first envisaged. It will also have:

- Location check-in – where users can track places on their own device by scanning QR codes at the venue. The app will alert you if one of these locations was judged to be high risk when you were there.
- Regional risk score alerts – letting users know the level of risk in their declared postcode district.
- Digital contact tracing - letting users know if they may have been in contact with someone who tested positive for COVID-19.
- Symptom recorder – letting the user record symptoms and giving out information.
- Testing services - letting users order a test and get the results back through the app in a privacy-preserving way.
- Self-isolation countdown and advice

Once it has been tested in Newham and on the Isle of Wight it will then be rolled out nationally. You can read more here: https://www.ncsc.gov.uk/blog-post/nhs-test-and-trace-app-security-redux

EU-U.S. Privacy Shield Schrems II Ruling

The Schrems II ruling which declared that the Privacy Shield framework is no longer a valid mechanism to transfer personal data from the European Union to the United States. The European Commission and US Department of Commerce have started to discuss a new EU-U.S. framework which will comply with the 16 July ruling. I will be keeping an eye on this and will publish information as it comes to light. If you want to understand what the fuss is all about you can read about it here: https://jerseyoic.org/blogs/eu-us-privacy-shield-invalidation/

Tik Tok

The Chinese firm behind TikTok (ByteDance) is considering whether it should move its headquarters to London. Microsoft are also considering making an offer to ByteDance for their operations in US, Canada, Australia and New Zealand.

Microsoft issues its latest patches -including one for Windows 10

The latest MS update affects 13 products and includes patches for 17 'critical' bugs and 97 'Important' bugs in the Windows 10's security features, Microsoft Edge browser, Office, SQL Server Management Studio, .Net Framework. The same patch fixes 26 vulnerabilities in Adobe Acrobat and Reade. You can see the full list of what the update includes here: https://rawcdn.githack.com/campuscodi/Microsoft-Patch-Tuesday-Security-Reports/5635e8c428e93bf3d4a9b661edc198a03f084a6b/Reports/MSRC_CVEs2020-Aug.html

A Warning If You Use Amazon's Alexa In You Smart Speakers

We know that hackers see smart speakers and the 'Internet of Things' as entry points into our lives. There is increasing evidence of them being used to access data, eavesdrop on conversations or do certain things without the owner being aware. The latest warning is for those who use Amazon's voice assistant Alexa in their smart speakers. If a user clicks a links that takes them to an Amazon subdomain ("track.amazon.com") the site will allow attackers to install hacking skills on their device and use it to spy on their activities. You can read more here: https://thehackernews.com/2020/08/amazon-alexa-hacking-skills.html

Did You Know Hackers Can Bypass Chrome

According to Hacker News, cybersecurity researchers are warning of a flaw in Chrome based web browsers on Windows, Mac and Android systems. The flaw could allow attackers to entirely bypass Content Security Policy (CSP) rules. So if updating your Chrome, Opera, or Edge web browser to the latest available version is on your to-do-list I recommend that you do it as soon as you can.

Samsung's 'Find My Mobile' App Vulnerable

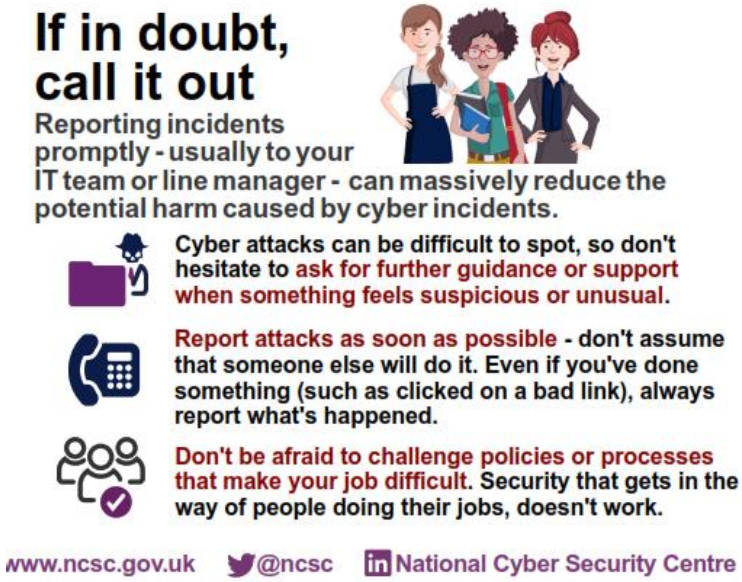
The 'Find My Mobile' app that comes pre-installed on many Samsung smartphones has a flaw which means the phone could be permanently locked remotely or the user could suffer a complete data loss with factory reset (SD card included). This has serious privacy implications via IMEI and location tracking as well as call and SMS log access. So if you have a Samsung Galaxy S7, S8, or S9+ device make sure your software is updated.

A Night Time Economy Webinar

The Altrincham and Sale Chamber of Commerce webinar discussed the role that the night time economy has played in the recent successful regeneration of Altrincham town centre. You will be able to view this soon on the Chamber Youtube Channel where you will also find videos of recent webinars with our local MP and Council Leader. You will find the channel here: https://www.youtube.com/channel/UCJCDH87oAvRA_MfwivT6fiw

Phishing – If in doubt call it out

With the prevalence of Phishing attacks at the moment I thought it was timely to remind you that the NCSC have an e-learning package 'Top Tips For Staff' which you can either build into your own training platform or complete online. This week I'd like to focus on just one section of their infographic which they call "if in doubt call it out"



And a reminder…..

The NCSC launched a Suspicious Email Reporting Service earlier this year. If you have received an email that isn't quite right you can forward it to the report@phishing.gov.uk email address and they will investigate and close down the user account if necessary. As at 31 July 2020 more than 1,708,000 reports had been made and 6,501 scams and 15,805 URLs removed.

Data Breaches – Practical Guidance Based on Recent Experience

The best bit of advice I give about data breaches is to recommend that businesses assume that there will be one! As our IT systems get more complex attackers find new and novel ways to compromise them. By assuming a breach will occur I am not giving you an excuse to run up the white flag and stop trying to protect your IT. I see it as a way to help understand the problem and operate on the basis that something will go wrong at some point. That way you can plan for the eventuality in a structured and organised way.

Discussing what you would do and then putting a process/procedure/system in place at a time when you are not actually dealing with an 'breach incident' is invaluable. Trying to put a system in place during a crisis is difficult (at best). Think about who should deal with any breach, the steps you want them to go through and drawing up a simple flow chart below is a good starting point.

Once you have a process you need to think how you will monitor that the breach has been dealt with appropriately (you only have 72 hours if there is a risk to someone's rights and freedoms).

Whatever happens you need to record the incident, put measures in place to address the breach and prevent it from happening again. Keeping a simple log of what happened and what you have done is all that is required.

If you would like examples of a Breach Log/Data Breach flow chart there are some in my book ("GDPR: A Game of Snakes and Ladders" ISBN: 978-1-003-00479-0 (ebk). Alternatively DM me and I will be happy to email you a copy.

Blogs of the week

Sheridan Voysey - Here's Why You're So Tired Right Now – and What to Do About It

Thanks to a friend, I found Sheridan Voysey's latest blog. I thought it was just for me that almost everything I do was taking longer. Sheridan likens it to "feeling like an old laptop streaming video on weak Wi-Fi—the hourglass symbol just kept spinning". If you are in the same place then he has some hints that might help you too….I'm adopting monotasking as my goal this week, focussing on one project at a time, broken into manageable bits, to reduce cognitive overload. You can read Sheridan's blog here: https://sheridanvoysey.com/lockdown-fatigue/

Kevin Keen - Is Data Protection on your Board Radar?

On the Jersey ICO blog Kevin discusses how he thinks of Data Protection as being similar to Health & Safety legislation. Yes, there are severe legal or financial penalties for breaking the law but it is the other consequences, risk of injury or release of personal data, that are more troubling. Kevin believes that the penalties are there to incentivise us to do what we should be doing anyway - running our businesses responsibly and taking account of the interests of all our stakeholders. Good data protection should really just be part of our culture. You can read the blog here: https://jerseyoic.org/blogs/is-data-protection-on-your-board-radar/