THURSDAY THOUGHTS

The biggest struggle this week when compiling #thursdaythoughts after a 2-week break was deciding what to include and what to leave out. It certainly has provided me the proof if any was needed that a weekly blog is the only way to keep on top of the cyber news! Not only have we a Brexit Trade Deal, there is another national lockdown and a return to home schooling for many to cope with.

Then comes some news that I never thought I'd see - Twitter and Facebook lock Donald Trump's accounts after his video address with many seeing him as the author of an attack on American democracy. Facebook and Instagram have blocked him 'indefinitely and at least for the next two weeks'. His comments and the ensuing violence are already being seen as something that will negatively impact the US economy and have led to calls to invoke the 25th Amendment as well as penalties for those who took part in the "demonstrations". It shows us all the power of social media and clearly underlines the importance of understanding the impact your comments can have.

This week you will find slightly less detail in the blog with all the usual links to source documents but I cover more areas than usual. You'll still find the usual details of fines, breaches, hacking, information and advice. For those who are home schooling I also include a link to an article that tells you how to use a keyboard with your Xbox or PlayStation and that way get your children on line. Also a little section on cyber things to watch out for in 2021.

Blogs of the week:
Aaron Fletcher - 7 Reasons Why Podcasts Should Be Part of Your 2021 Marketing Strategy
HR Dept - Employment law changes and priorities for 2021
Jamieson Law - Level up your business in 2021 – don't DIY your contracts

Can You Access Online learning with your Xbox or PlayStation

With the return to lockdown, remote teaching once again started and there has been much in the media highlighting concerns that not all families have the hardware they need to be able to access education. One solution that may provide a solution in the short term, for pupils who do not have access to a laptop but do have a gaming console is to plug a keyboard into the Xbox USB slot, find Microsoft Edge in "my games and apps" and navigate to the online learning platform. With a PlayStation you select the internet browser from the library and navigate to your online learning platform and log in as usual. You will find more here: https://www.tes.com/news/how-use-xbox-or-playstation-online-learning

Networking

Today was also the first Breakfast Matters of 2021 for our Local Chamber of Commerce. We were lucky to have Elizabeth Vega, Amanda Coleman and Richard Wilkinson as our panel discussing "Brexit and New Beginnings". It was great to get to discuss something positive with fellow business owners after all the doom and gloom in the media. Still not face to face but great to connect for a chat afterwards.

1

Fines

Over the Christmas period you may have missed the news of the following fines:

Romania - Banca Transilvania

The Romania DPA fined Banca Transilvania €100k EUR because their employees forwarded the content of an email from a customer internally and then printed and shared it on social media because it was "funny". This breached the company privacy and confidentiality policies.   A reminder for us all that a rogue employee's actions can affect the business financially as well as reputationally.

Ticketmaster

Ticketmaster have been fined $10 Million because, having employed an individual from a rival business, they encouraged them to retain their log in credentials at the rival firm and use them to hack into systems, monitor activities and find out which artists planned to use the rival company - a blatant attempt to 'choke off' the rival's business.

Leaks

Spotify

Spotify was forced to resets passwords after it was noticed that user information including account registration information, email address, preferred display name, password, gender, and date of birth had been made visible to business partners for a period of seven months.

Phlebotomy Lab Suffers a Data

A cyber-attack on US Laboratory was discovered last month when patient personal and health information was posted online in the attacker's blog.   Many in the medical field believe that they don't have anything of value to cyber criminals. However, the opposite is true. Medical records have become "the holy grail for social engineers and bad actors". I recently read a report that said that the price of a medical record is about $250 on the dark web which is significantly higher than the usual fee of $5 for a stolen credit card.

British Airways Data Breach

British Airways plans to start settlement discussions with the customers who were victims of their 20018 data breach. It has been revealed that the compensation pot is approx. £3bn.

Cyber Attacks

Travel Companies

In December the Norwegian shipping and cruise line Hurtigruten was crippled by a ransomware attack. Many of its systems went down including the company's website. Many other travel companies have had a similar fate in 2020. About 9 Million easyJet customers had their data stolen by hackers in May. Carnival cruises, the shipping giant CMA CGM, and the United Nations International Maritime Organisation (IMO) all suffered cyber-attacks.

Healthcare Organizations

The most prevalent cyber-attacks at the moment are on healthcare organizations which has seen a 45% increase in attacks (more than double the rate of other sectors). This equates to 626 weekly

attacks on average per organization.   The most common type of attack is ransomware, however botnets, remote code execution and DDoS are also being deployed.

SolarWinds

I located a great article by Allen Woods which explains much of the detail of the SolarWinds "hack". Most of which is well above my head so be warned there is lots of "technical speak" in it. Discussions as to who was behind it (widely speculated to be the Russians), what was at fault and was Microsoft's open source code a contributing factor have been widely discussed. The number of organisations and email accounts compromised is staggering. If you are a SolarWinds' customer I'd think seriously about whether to stay that way. https://lnkd.in/gjVBMAC . You may also want to check out Stephen King's posts on the same topic.

FireEye Hack

FireEye the cyber security firm who deploy their "red team tools" to the defences of its clients was hacked at the end of last year in what they suspect was a state-sponsored attack. The breach was disclosed in a blog post which stated while their "red team tools" had been stolen there was no evidence that the attacker removed customer data from their systems. FireEye have also published hundreds of countermeasures to enable the broader security community to protect their organisations and their customers.

Facebook Forces WhatsApp to Accept new Privacy Policy

The thing that attracted many to WhatsApp was that it had privacy coded into its DNA. However Facebook's acquisition is now giving its users an ultimatum "agree to share their personal data with the Facebook" or delete their accounts. This is delivered via an in-app alert directing users to agree to sweeping changes in the WhatsApp terms of service which include allowing Facebook to share information with outside entities. Those who don't accept the revamped privacy policy by February 8 will no longer be able to use the app.   If you aren't happy with this you'll need to find another messaging service.

Threats to Businesses in 2021

Here are a few things to watch out for in 2021

- Attacks on organisations who have just begun digitizing. The speed that government institutions, schools and businesses moved everything online left little time for planning and security.
- An increase in Social engineering attacks.
- More exploitation of discrepancies between multi-server applications, through the likes of request smuggling, parameter pollution and path normalization exploits.
- A move by hackers towards obscure business logic flaws and conditions.
- More attacks on companies that store critical information (medical records) or host critical infrastructure (hospitals) including SCADA systems, Telco's, Healthcare and Education.
- An increase in authentication bypasses and access control issues.

What is the greatest cybersecurity challenge going to be in 2021 …… ensuring security for remote employees. You can read more here: https://www.techrepublic.com/article/how-the-coronavirus-outbreak-will-affect-cybersecurity-in-2021/

Brexit and Data Transfers

AKA the adequacy debate. For those worrying about data transfers to Europe post 31 December there is a 6 month "window". This interim period will allow seamless data transfers to UK and extends the time before the adequacy decision has to be made. You can read more here: https://www.linkedin.com/pulse/brexit-trade-deal-what-does-mean-data-protection-law-katie-hewson/?trackingId=gUwbO1%2BTdDZW%2BYoUvjPuyA%3D%3D

Advice and Guidance

Avoiding Data Breaches

One way to avoid the information being opened by the "wrong" person is to password protect your attachments. I also recommend you have a clear file naming strategy and folder structure and go to that when adding an attachment to an email. This way you can identify the "correct" attachment rather than relying on your computer to provide you with the one it thinks you want.

Deepfakes: Guidance By The Italian DPA

The Italian Garante has issued a handbook that explains the phenomenon of deepfakes and provides suggestions on how to protect against them. https://www.garanteprivacy.it/home

New ICO Guidance on Sharing Data for Law Enforcement

Data protection law allows data to be shared with a law enforcement authority if it is necessary and proportionate. The ICO has just produced information on how to share data lawfully and a toolkit for smaller organisations to use in these circumstances. You will find these here: http://ow.ly/m9Od50CRVlb, http://ow.ly/AOI350CRVlc

NCSC Guidance

Criminals often use email, phone call and text messages. The NCSC has new guidance on spotting and reporting suspicious messages. They also share how to make yourself less of a target and what to do if you've already responded. https://www.ncsc.gov.uk/guidance/suspicious-email-actions

European Commission Digital Services Act

With thanks to Neil Evans. The new EU Digital Services and Digital Markets Acts address challenges that have surfaced with digital developments. With the aim of creating a safer digital space and "overhauling" the digital market. You will find them here https://lnkd.in/gCJpX8W and https://lnkd.in/gYpU9kG

Personal Information Management Systems

The European Data Protection Supervisor has blogged about how PIMS products and services will help by allowing individuals to have full control over their online identity, allowing them to share their personal data however they like and delete information at will. You can read more here: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-32020-personal-information_en

VMWare Patch Action Required

Russian state-sponsored actors have been exploiting a vulnerability in VMware products. Therefore a joint advisory form the US' National Security Agency (NSA) and the UK National Cyber Security Centre as well as VMWare itself urge organisations to patch the vulnerability in VMware identity management products. Failure to do so could allow cyber criminals to access your data on the affected systems.

Blogs of the Week

Links to all the blogs are in the comments.

Jamieson Law Level up your business in 2021 – don't DIY your contracts

In her first blog of 2021 Babs Jamieson reminds us of the need to protect our businesses so we can see them flourish. If you are thinking of doing DIY contracts read her blog first to see what perils face you. https://jamiesonlaw.legal/2021/01/04/level-up-your-business-in-2021-dont-diy-your-contracts/

HR Dept (Trafford and Warrington) - Employment law changes and priorities for 2021

This week's blog from HR Dept is aimed to reduce business owner and manager's stress levels in 2021. One way to do this is to get ahead on any changes in the Law, especially those tricky Employment Law changes. The blog includes a number of changes you will want to know about. https://www.hrdept.co.uk/trafford-and-warrington/blog/employment-law-changes-and-priorities-for-2021

Aaron Fletcher - 7 Reasons Why Podcasts Should Be Part of Your 2021 Marketing Strategy

In the last 12 months we have been connected to each other via the internet, but also disconnected from what's around us. It's hard to have lost a lot of the personal relationship and connection with customers and clients for the time being. Aaron suggests a great way to stay connected to clients/customers is via podcasts. You can read his reasoning here: https://www.buzzinsounds.com/post/7-reasons-why-podcasts-should-be-part-of-your-2021-marketing-strategy-conversations