THURSDAY THOUGHTS

Happy human rights day! According to Article 12 of the UDHR - privacy is a human right and should be protected as such. This week's Thursday thoughts comes amid news of big fines and lawsuits against Facebook, Twitter, Google and Amazon which have the potential to affect us all.

There is news of cyber-attacks targeting Vaccine Documents and Vaccine Distribution Chains as well as cyber security company FireEye. So I take a look at what Cyber Threats we may face when we Return to the Office. Patches and Vulnerabilities are covered as usual and a plethora of other "cyber" related news including a Trade Deal with Singapore which is part of the Government's plan to make the UK a global hub for tech and services trade post Brexit

This week I was lucky to attend 3 great and very different virtual events, Alex and his Sisters, Altrincham and Sale Chamber Breakfast Matters and the Mindset Team Christmas Party. I also found out about Ali Davenport's Connection fest which you can read about in one of my Blogs of the Week.

My "Blogs of the Week"
HR Dept (Trafford and Warrington) - Six reasons why a virtual company Christmas is a good idea
Altrincham HQ Social Media - A Great Connector and Connection Fest
Kate Fox - Brand, or Fail

What Cyber Threats Await When we Return to the Office

During the pandemic much of everyone's efforts have been concentrated on protecting staff from the risk of illness. It is entirely possible that organizations have overlooked the "invisible threat" of compromised security.

The sudden move (very often unplanned) to a completely remote workforce lead to changes in long established security solutions and processes. The resulting confusion has provided attackers with the opportunity to bypass many layers of security. For example users may have plugged corporate devices directly into their home Wi-Fi modem in search of more reliable connectivity – potentially without a firewall. Or they may have used their corporate devices for non-work reasons.

Organisations planning to return to the office should recognise these risks and implement appropriate safeguards as workers begin to return. You can read more about these potential threats here: https://www.infosecurity-magazine.com/opinions/cyber-sleeper-cells/

Even Cyber Security Companies Get Breached

FireEye are usually the first company that a cyberattack victim contacts when they suffer at the hands of hackers. This week it was announced that the company has admitted it has been the victim of a state-sponsored attack by a "highly sophisticated threat actor". The hackers stole "Red Team tools" which are often used to mimic a real-world attack.

This emphasises that none of us can afford to be complacent and we should all consider ourselves to be targets and likely to suffer a breach at some stage. It is however up to each organisation to make sure they are adequately prepared. If It Sounds too Good To Be True – There Will be a Catch

Chris Roberts shared a "Too Good to be True" story on Linked In – it featured a "Horse trailer for sale" (on Facebook) which "moved" to eBay. This could be any item so watch out. There was a sob story attached that the owner was TOO busy to deal with it, so they handed it to their finance person to deal. So if you see an all-time good deal and are presented with an "eBay issued invoice" which asks you to pay in pre-pay eBay cards. DON'T DO IT! Especially not if you are asked to take pictures and send them. Instead ask someone you trust for advice and in Chris' words "Please don't get scammed!"

Facebook Marketplace seems to be full of these ads at the moment. So keep safe. The tell-tale signs are when you see a number of accounts offering the same item. If this is combined with a goofy Facebook account name and the account has only been alive for a short time steer well clear.

Hackers and Phishers target Vaccine Documents and Distribution Chains

This week documents relating to the Pfizer/BioNTech vaccine were accessed in a cyber-attack on the European Medicines Agency (EMA). You can read more here: https://www.infosecurity-magazine.com/news/hackers-raid-european-agency/

This announcement comes days after revealed a "sophisticated nation state phishing campaign" had been carried out against organisations who will be called upon to provide the cold chain storage that will enable the vaccine to be distributed on a global basis. Organizations and companies involved in vaccine storage and transport have been urged to review their processes and strengthen their defences. https://thehackernews.com/2020/12/hackers-targeting-companies-involved-in.html

Ransomware Disrupts Maryland Student Classes

115,000 US students in Maryland had online classes disrupted after a ransomware attack just before Thanksgiving. The attack was described by the Baltimore school district as a "catastrophic attack on our technology system".

Online Shoppers Beware Phishing Attacks

With more Christmas shopping taking place on line there have been an increasing number phishing scams disguised as delivery emails. A 440% rise in shipping-related phishing emails has been seen in the last month. Beware emails that look real but encourage you to make a further payments or log on so your email address and password are compromised.

UK Trade Deals with Singapore and Vietnam

The UK International Trade Secretary signed a trade deal in Singapore today and will travel to Vietnam to conclude another deal. These deals bring the UK closer to a deal with the 11 nation "Trans-Pacific Partnership". The UK/Singapore deal was described as paving "the way for a cutting-edge relationship in digital as part of the government's plan to make the UK a global hub for tech

and services trade post-Brexit". This will certainly be an area to watch over the next few months. You can read more here: https://www.gov.uk/government/news/uk-strikes-singapore-and-vietnam-trade-deals-start-of-new-era-of-trade-with-asia?utm_source=linkedin&utm_medium=organicsocial&utm_term=&utm_content=645e8b47-598a-4eaa-a32c-983a9d8c90e8&utm_campaign=

Fines and Sanctions

Facebook Accused Of Abusing Its Power To Neutralize Competitors

In a ground breaking antitrust lawsuit, the US government has insisted that Facebook be broken up. It is alleged that the company deprived users of better, privacy friendly, alternatives when it acquired Instagram and WhatsApp. They were also accused of putting anti-competitive conditions on software developers to eliminate threats to their monopoly. The lawsuits aim to set aside the acquisitions of Instagram and WhatsApp and turn them into independent companies. The intention is also to prohibit Facebook from imposing anti-competitive conditions on software developers, and require the company to seek prior notice and approval for future mergers and acquisitions. You can read more here: https://edition.cnn.com/2020/12/09/tech/facebook-antitrust-lawsuit-ftc-attorney-generals/index.html

Facebook Ireland Face A €302.3M Data Protection Fine

Facebook Ireland are due to meet the Irish supervisory authorities in the High Court next week. This is a result of the judicial review that Facebook requested in august. Facebook hope to quash both an inquiry and a preliminary decision from the authority. If the judgement goes against them Facebook will have to stop transferring EU users' data to the US immediately. They will also face a significant fine for breaches of data protection regulations which , according to their company accounts, Facebook Ireland estimate will be between €154m and €541m (they therefore set aside €302.3M).

Google and Amazon fined €100M and €35M respectively

Google and Amazon have received fines in France for failure to comply with EU Cookie rules. Amazon Europe Core were fined €35M for placing advertising cookies on users' computers without obtaining prior consent and without providing adequate information. CNIL "noted that the cookie banner did not explain to the user that it could refuse these cookies and how to do it."
This sort of thing is quite common and organisations should make it a priority to check that their site doesn't flout these rules or they are likely to stand the risk of a significant fine.

Twitter Fined For Making Private Tweets Public

The Irish data protection commissioner are expected to fine Twitter for making some users' private tweets public. It falls to the Irish Commissioner to make this fine as they are Twitter's lead supervisory authority in the EU.

Patches and Vulnerabilities

Microsoft Patch Tuesday

The last Microsoft Patch Tuesday of 2020 has 58 patches (9 rated as Critical, 46 rated as Important, and 3 as Moderate). The patches are for security flaws in 11 products including Microsoft Windows,

Edge browser, ChakraCore, Microsoft Office, Exchange Server, Azure DevOps, Microsoft Dynamics, Visual Studio, Azure SDK, and Azure Sphere.

Your D-Link VPN Routers May Be Vulnerable

Some popular D-Link VPN router models (D-Link DSR-150, DSR-250, DSR-500, and DSR-1000AC and other VPN router models in the DSR Family running firmware version 3.14 and 3.17) have been found to be at risk. The routers are remotely exploitable in a way that could allow threat actors to "execute arbitrary commands on vulnerable networking devices" or launch a denial-of-service attack.

Internet of Things Risks

A set of 33 vulnerabilities which impact four open-source TCP/IP protocol stacks (uIP, FNET, picoTCP, and Nut/Net) and are most commonly used in Internet-of-Things (IoT) devices have been identified. Attackers are potentially able to "compromise devices, insert malicious code, perform a denial-of-service (DoS) attack, steal sensitive information, or poison the DNS cache".

Microsoft Teams Chat Message Risk

A "zero-click remote code execution bug" has been identified in the Microsoft Teams desktop app. It is possible for a threat actor to compromise a target's system just by sending a chat message with specific code in it. The result is a "complete loss of confidentiality and integrity for end users. This potentially affects Microsoft Teams for Windows (v1.3.00.21759), Linux (v1.3.00.16851), macOS (v1.3.00.23764), and the web (teams.microsoft.com). It is possible that it could be made "wormable". Another reason to keep your software patched and up to date!

ICO Survey closes on 31 December 2020

The ICO consultation on the role of data ethics in complying with the GDPR closes at the end of December. Data ethics "seeks to help data controllers to determine what is a right (or wrong) purpose or means of processing personal data." If you wish to make comment on the consultation you should go to: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-role-of-data-ethics-in-complying-with-the-gdpr/

Make Sure You Confirm The Identity Of The Caller

Whether someone who calls you in your own home or at work even if they are making a subject access request. You absolutely need to make sure you confirm the identity of the person before you give them personal information (or indeed make a new payment).

The National Cyber Security Centre have a great online 'Contact Validation Form' where you can confirm the identity of the person calling you and get the reassurance that you are speaking to a government cyber security expert. I'd like to see more organisations do this to protect the vulnerable.

Emerging Technologies Guidance

The Spanish Supervisory Authority have issued useful guidance (in English) which analyses some of the emerging technologies being used by Public Administrations. The document highlight the most

relevant features from a data protection perspective of Cookies and tracking technologies, Social networks, Cloud Computing, Big Data and Smart Cities amongst others and shows some of the inherent risks of their use. You can read the guidance here: https://www.aepd.es/sites/default/files/2020-12/guia-tecnologias-admin-digital-en.pdf

Microsoft "Productivity Score" To Be Changed

Microsoft has accepted that it's "productivity score" service could be used for workplace surveillance and will make changes to the service by removing individual user names from the productivity score entirely. You can read more here: https://www.theguardian.com/technology/2020/dec/02/microsoft-apologises-productivity-score-critics-derided-workplace-surveillance

Blogs of The Week

HR Department (Trafford and Warrington) - Six reasons why a virtual company Christmas is a good idea

With employees working away from the office or at a distance while in the office the HR Department blog is a timely reminder of the importance of even virtual events to lift spirits and bring staff together. There are some great benefits to celebrating Christmas virtually with employees this year not least combatting loneliness at work. You can read the other benefits here: https://www.hrdept.co.uk/trafford-and-warrington/blog/six-reasons-why-a-virtual-company-christmas-is-a-good-idea

Altrincham HQ Social Media - A Great Connector and Connection Fest

Alex McCann's blog this week comments how social media has kept him sane this last 12 months. His theme is all the connections he has enjoyed this year. Whether this is connecting with friends, memories, interests or even (when it comes) reconnecting with normal life. You can read his blog here: https://altrinchamhq.co.uk/connection-festival-aside-from-business-social-media-is-a-great-connector/. AS part of the blog Alex highlights the work Ali Davenport is doing with her Connection fest this month which is set up as a way of spreading positivity - and hope - to help us through this difficult chapter in the human story (https://www.soulsurvivalguide.co/connection-fest).

Kate Fox - Brand, or Fail

In this week's blog Kate discusses why she thinks Branding is everything. If you don't know why a pretty logo does not class as a brand strategy then this set of blogs from team Fox will set you right. They clearly describe why branding is the very foundation of business success. For those who want to listen not read there are even YouTube and Facebook live talks. You can access the blog here: https://foxgraphicsdesign.com/2020/11/17/brand-or-fail/ be sure to read all 3 blogs.