THURSDAY THOUGHTS

At some stage normal activities have to start again so this week I was able to start auditing again. Not the same as the old way of doing things but everyone's familiarity with Video Conferencing made it much easier. At least it was possible to have everyone together for the initial talk and then people could come and go as required; even those who are shielding can take part which is really helpful. Things take a little longer but you still get the job done!

There has been lots going on in the world of cyber news this week. I have pulled together information on Video conferencing including what software there is and how you and your children can use it safely. Smart devices, phishing and malware also feature as always. There is a lesson on subject access requests and the dangers of sending imperfectly redacted information to the data subject.

My "Blogs of the week"

Amanda Coleman - "Think Through Brew"
Becky Field - Is it over yet?
Martin Hambleton - A day in the Life | PR photoshoots and social distancing
Altrincham HQ - Instagram captions: how to write better Instagram

What is the best video conferencing software around?

We have all got used to video conferencing software which allows audio/video meetings and seminars with different offerings of features such as chat, screen sharing, and recording. Some video conferencing systems even offer integrations with marketing automation and CRM software to sync critical business data into relevant conferences and allow for streamlined follow-up communications and updates. A comparison of the various Video Conferencing Software currently on the market can be found here: https://www.g2.com/categories/video-conferencing#grid

Using video conferencing securely

Even if you're familiar with video conferencing it's good to take a moment to check how you're using it. The NCSC have some guidance on how to use video conferencing securely. There is also advice for parents on keeping children safe. Here are some useful links:

- Setting up Video Conferencing https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely
- Guide for primary school children https://parentinfo.org/article/video-chatting-a-guide-for-parents-and-carers-of-primary-school-age-children
- Guide for secondary school children https://parentinfo.org/article/video-chatting-a-guide-for-parents-and-carers-of-secondary-school-age-children

Zoom suspends some paid user accounts

Zoom suspended some paid accounts early in June, allegedly based on the content of the meeting. Zoom is not currently blocked by China's "Great Firewall" of censorship, meaning it is accessible in the mainland without a VPN however the company has strong ties to China which is home to nearly a third of its staff. Zoom suspended the U.S.-based accounts of activists marking the anniversary of China's Tiananmen Square crackdown on its platform, drawing criticism that the firm whose product has quickly become ubiquitous in quarantine life is not committed to protecting free speech. You

can read more here: https://variety.com/2020/politics/news/zoom-censorship-tiananmen-square-humanitarian-china-zhou-fengsuo-1234631652/

Using smart devices safely

While we are all stuck in our homes we may have forgotten about our smart devices or we may have installed them in a bit of a rush as we started lockdown. Unlike conventional household items, you can't just switch on a smart device and forget about it; you need to check a few simple things to protect yourself. If you want some helpful tips, the NCSC has a guide which explains how to set up and manage your smart devices to keep your home - and your information – safe. Using these tips will prevent your smart devices (smart speakers, fitness trackers and security cameras AND fridges, lightbulbs and doorbells) from sharing your personal information with their makers ... or others. You can read the guide here: https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

Phishing explained

Sadly, although phishing is a threat that most people know about we still seem to get caught out by Emails that trick us into clicking a malicious link or divulging passwords and other credentials. Phishing is still the number one initial attack route. Unfortunately, there is no silver bullet and Phishing can only be dealt with by using multiple complementary measures. If you don't really understand what Phishing is and want some ideas on protecting your organisation from phishing here is a really helpful guide from the NCSC which links to a 30 minute webinar on the topic: https://www.ncsc.gov.uk/blog-post/phishing-still-a-problem-despite-the-work

Malware and ransomware

Public sector organisations in particular will always be a target of Malware but we can all take 4 steps to stop ourselves from being a victim:

1. Regular backups – so you can recover your data without having to pay a ransom.
2. Preventing malware from being delivered to devices by filtering and blocking.
3. Preventing malware from running on devices by using device-level security features
4. Limiting the impact of an infection and having a rapid response should one occur.

Files encrypted by most ransomware have no way of being decrypted by anyone other than the attacker. Do not waste your time or money on services that promise to do it. If you think your organisation is already infected then the following steps may help limit the impact of the infection.

1. Immediately disconnect the infected computers, laptops or tablets from all network connections (wired, wireless and mobile phone).
2. Consider turning off the Wi-Fi and disabling any core network connections (e.g. switches).
3. Reset credentials including passwords (especially for administrators).
4. Safely wipe the infected devices and reinstall the operating system.
5. Check the backup is free from malware and ransomware before you restore from it.
6. Connect devices to a clean network to download/install/update operating systems and software.
7. Install, update, and run antivirus software.
8. Reconnect to your network.
9. Monitor network traffic and run antivirus scans to identify if any infection remains.

Consent and “invite a friend”

Nobody should share contacts details without checking with the person concerned that this is ok with them! So be wary of social media platforms that urge you to invite friends to join the platform via an "invite a friend" option. The Belgian Authorities fined one company €50,000 for processing personal data of non-members without an appropriate legal basis (a user gave the provider access to his or her list of contacts). Then an automatic message was sent to all contacts on the user’s behalf urging them to join the social media platform or, if they were already members of the social media platform, to become part of that user's network of friends on the platform. There was no opportunity for the user to consent to this nor for the recipients to give their consent.

Redaction and Subject Access Requests

If the person you send redacted information as part of a subject access response can “un-redact” the information and identify a data subject then YOU as the data controller will have caused a data breach. It is also an offence under GDPR to recklessly re-identify someone or process re-identified personal data without the consent of the data controller so any person who does will also be at fault. This week was reported that the London Borough of Lambeth Children’s Services department had failed to effectively redact information they provided in response to a Subject Access Request. This meant that the data subject was able to electronically manipulate the information provided and remove redactions (they then were able to make contact with someone who had made allegations against them). You can read more here: https://informationrightsandwrongs.com/2020/06/05/high-court-subject-access-breach-of-confidence-and-the-offence-of-reidentification/

Email security and anti-spoofing tool for Colleges and Universities

Mail Check has been around for a while as a service for the public sector but they have now made it available to all UK colleges and universities. Mail Check is the NCSC’s platform for assessing email security compliance. It helps you to setup and maintain good DMARC, SPF, DKIM and TLS configurations. It also collects, processes and analyses DMARC reports. You can find the link to register here: https://www.mailcheck.service.ncsc.gov.uk/

The NCSC research problem Book

The NCSE have published a Problem Book to shed a little light on what they are doing. The most significant of what they see as their long-term challenges are divided into 7 themes. The Problem book then emphasises the problems they want to solve in each area so that they can continue to address the problems and opportunities presented by evolving technology. You can read more here: https://www.ncsc.gov.uk/information/the-ncsc-research-problem-book

AI and Deepfake

AI and Deepfake technology have made it super easy to create convincing counterfeit videos. There is voice technology which allows attackers to impersonate the sound of their chosen target and video technology that learns the real entity’s facial mannerisms and allow them to be replicated. This is a worry because it is estimated that about 75% of the population are "sensing" learners who have to "see it to believe it" - because deepfakes "show" people on video talking about something they may be more quickly be accepted as "real" by sensing learners. If you want to see it in action follow the link to see a convincing deepfake of former president Barack Obama: https://www.infosecinstitute.com/blog/how-artificial-intelligence-is-changing-social-engineering/

Bug in Facebook Messenger for Windows

Make sure your Messenger App is up to date. Cybersecurity researchers disclosed details this week of a vulnerability they had discovered in the Facebook Messenger application for Windows (Messenger version 460.16) which could allow attackers to use the app to execute malicious files already present on a compromised system to help malware gain persistent/extended access. You can read more here: https://thehackernews.com/2020/06/facebook-malware-persistence.html

Europe after coronavirus

There is a really interesting piece from Chatham House about the effect of COVID-19 on the role of the state in relation to the market in Europe. If the crisis leads to a larger role for the state and a move away from market-oriented policies, the EU will face a challenge in accommodating that change. You can read the article here: https://www.chathamhouse.org/publication/europe-after-coronavirus-bergsen-et-al

Blogs of the week

Amanda Coleman - "Think Through Brew"

Amanda has recognised that developing communication strategies at this time can be a huge pressure especially if you are working in isolation from your usual team. She has therefore decided to offer a "Think Through Brew" where she gives around 20 minutes each day to help someone. Why 20 minutes? You'll have to read her blog to find out: https://amandacomms1.wordpress.com/2020/06/10/time-for-a-think-through-brew/

Becky Field - Is it over yet?

I really like that Becky asks the question many of us are thinking. She has a super positive practical approach to try to move her reader from anxiety and panic to a "new normal". I love the analogies she uses in the blog. If you can't do what you were doing what else can you offer, what other skills do you have and can you use them. Are you using the time wisely (note to self!). What else can you do support local businesses, build connections and above all focus on the positives. There is so much more in the blog: https://westfield-coaching.com/is-it-over-yet/

Martin Hambleton - A day in the Life | PR photoshoots and social distancing

Martin has spent much of Lockdown writing his blogs and as ever this blog is accompanied with some fabulous photos. In this one he reflects on whether he could achieve social distancing in PR shots. And his answer … yes I think so, with some tweaks … after all it's always been possible to shoot portraits from more than 2 metres. So with the addition of a face mask, gloves and sanitiser he is ready for action. You can read his blog here: https://www.commercialphotographynorthwestblog.co.uk/pr-and-event-photography/a-day-in-the-life-pr-photoshoots-and-social-distancing.html

Altrincham HQ - Instagram captions: how to write better Instagram

Instagram is a great way to show your personality and engage at a personal level with your followers. If you're new to it or want to be "better" at it then Alex's will help you. Remember to find that strong opening line to get attention. Alex has a wealth of advice in this blog which will really help you if you want to "do" Instagram better: https://altrinchamhq.co.uk/instagram-captions-how-to-write-better-instagram-captions/