THURSDAY THOUGHTS

As European Cyber Security Month enters it's second phase the focus has changed to developing digital skills (their tag for the month is #ThinkB4UClick). I have therefore included this week some useful tips:

- Things you can put in place to protect customer data
- Strategies You Can Use To Avoid a Data Breach
- How to Answer "that" Type of Call (thanks to @Nick Brown for his timely post)
- Where you can find out if you have been compromised (thanks to Colony Networking)

Also the latest on Hacking and cyber attacks you may not have heard about. A new traffic light system which may help us travel in Europe and even a job on offer in NASA.

My "Blogs of the Week"

Tim Clements - How to you hold your delivery partners to account?
Deloitte – Top barriers to overcome cybersecurity challenges
Altrincham HQ - A Perfect LinkedIn Post – does it really exist?

October is European Cybersecurity Month - #ThinkB4UClick

Every October the EU organises a month-long campaign to promote cybersecurity. Providing up-to-date online security information, awareness raising and an opportunity to share good practice. This year's theme is 'Think Before U Click'. For the next 2 weeks the focus will be on developing digital skills. There are a range of activities and insights on current and potential cyber threats and you can find out more here https://cybersecuritymonth.eu/about-ecsm/

What Losing Customer Data Can Cost You

As well as the potential financial loss (fines and reparations) the cost of losing your customer's data can also mean you lose customers. There is inevitably reputational damage and this can have a long-term impact on your business because customers just don't trust your brand anymore.

There are some things you can put in place to protect customer data:

- Have offsite and offline back ups
- Provide cyber security training for everyone
- Have a virtual chief information security officer
- Conduct quarterly security audits

Strategies You Can Use To Avoid a Data Breach

It is a simple fact that "1 in 4 Organisations will Experience a Data Breach". Breaches can be either accidental or deliberate and occur when:

- personal data is lost, destroyed, corrupted or disclosed
- someone accesses personal data or passes it on without proper authorisation
- personal data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed

There are things you can do and it is really important to have a plan in place in case this happens to your business.

1. Identify and understand the risk – what sort of data do you hold, how does it move, who is it shared with and how is it accessed (especially if people are using their own devices).
2. Make employees your first line of defence (changing the terminology from greatest weakness) – give people appropriate permissions and access and train them appropriately.
3. Concentrate protection where it is most needed - payment data, Social Security numbers, names, addresses, birth dates, etc. should be given the highest level of protection.
4. Invest in cyber insurance with coverage that matches your business risk profile.

How to Find Out if Your email Has Been Compromised

If we think our details have been compromised where can we find out? I attended a really interesting Colony Networking Event last week where DC Tracy Earley shared a load of information on keeping Cyber Safe. One of the things she shared was the https://haveibeenpwned.com/ website. Put your email address(es) in and it will tell you where and when you have been compromised. You can then change passwords and emails etc accordingly. Well worth a check every 6 months or so.

Hackney Council "Serious cyberattack"

Hackney Council was the target of a serious cyberattack this week which affected many of their services and IT systems. According to their statement "Council officers have been working closely with the National Cyber Security Centre, external experts and the Ministry of Housing, Communities and Local Government to investigate and understand the impact of the incident. Our focus is on continuing to deliver essential frontline services, especially to our most vulnerable residents, and protecting data, while restoring affected services as soon as possible." Because the investigation is at an early stage there is very limited information available. Some Council services are unavailable or slower than usual and their call centre is extremely busy.

Carnival Cruises Hack

Back in august Carnival Corp (Carnival Cruises, Holland America and Seabourn and casino operations announced that they had been hacked. The information they accessed included personal information on guests, employees and crew. In a statement this week the company announced that they had been working to recover the files and that they believe there is a "low likelihood of the data being misused". They have made this assessment even though the hackers had accessed and encrypted a portion of their IT system and downloaded data files from the company. I'm intrigued how they can have assessed that there is a "low likelihood" so if you are a Carnival Corp customer or employee I'd make sure that .

Barnes & Noble Cyber Security Attack

On October 10 the Barnes & Noble corporate systems were the subject of a cyber-attack. While payment were not exposed (well done to Barnes & Noble for encrypting all credit cards and payment) the information that was breached included email addresses, billing and shipping addresses, and telephone numbers as well as past transactions. There is potential here for customers to be the victim of further cyber-fraud (depending on their book choices or identity).

New EU Traffic Lights System for Travel

The EU has just approved a traffic lights system which should allow easier travel within the block. The new traffic light system will include a weekly map of the regional situation in EU countries. The colour code will be based on the risk level: Green, orange, and red (and grey where insufficient data is available). You will find the information on the Re-Open EU website. Travellers will be able to check if borders are open in specific countries and understand what restrictions may be in place.

Fancy A Job Working for NASA?

NASA are recruiting an IT cybersecurity specialist to support the NASA Security Operations Center (SOC) at NASA Ames. The SOC is the nerve centre for cybersecurity monitoring, detection, prevention and cyber threat analysis. It would be a great job for the right person!

Blogs of The Week

Tim Clements - How to you hold your delivery partners to account?

This week's Linked In post from Tim Clements is about making sure that your delivery partners are engaged and accountable. It's important to do this as a matter of course and it keeps everyone on their toes. Last week's ICO DfE audit report confirmed that oversight, governance and scrutiny are key ways to prove "accountability" under GDPR. This involves asking the right questions, at the right time. Tim says "if plans don't exist, or meetings not minuted, you're already in trouble". (You will find a link to Tim in the covering Linked In blog post)

Deloitte – Top barriers to overcome cybersecurity challenges

2020 has brought many challenges. Not least for those who work closely with government/state IT departments. The need to balance cybersecurity risks and business continuity and with most employees working from home has been challenging to say the least. This year's Deloitte-NACISCO Cybersecurity Study (by Meredith Ward and Srini Subramanian identifies 5 barriers to overcoming these challenges. Whether at national, state, county or organisation level they are relevant to us all:

1. Lack of sufficient budget for cybersecurity
2. Inadequate cybersecurity staffing
3. Legacy infrastructure and solutions to support emerging threats
4. Lack of dedicated budget for cybersecurity
5. Inadequate availability of cybersecurity professionals

You can read the complete report here: https://www2.deloitte.com/uk/en/insights/industry/public-sector/nascio-survey-government-cybersecurity-strategies.html

Altrincham HQ - A Perfect LinkedIn Post – does it really exist?

This week I had a fabulous Linked In training session with Alex. If you need training on social media then Alex is your man (see my testimonial on Linked In). One thing Alex discusses is whether it is possible to achieve perfection in Social Media posts. Does striving for perfection both encourage some people to be better while at the same time hold others back from posting. In this blog Alex describes the anatomy of the perfect social media post. It is truly though provoking. You can read the blog here: https://altrinchamhq.co.uk/the-anatomy-of-a-perfect-linkedin-post/