Custodia Continuity

Cyber Security Webinar

This webinar is built in three clear sections.

Firstly What are the threats, external and internal, awareness allows mitigation and security.

Secondly what can you do, as a business and as an individual.
We suggest solutions that are cheap or free and will stop participants becoming the low hanging fruit.

Finally the surgery where participants can ask their specific questions and get real world useful answers from our technical and training teams.

We aim for participants to leave with a clear idea of the threats to their businesses and a good idea of all the steps they can take to stay safe.

1. **Intro**

   Introducing Custodia and what we do,
   The expectations for the session

2. **What does Cyber security mean to you?**
   Let's go over what cyber security is. Quick q and A with participants on their understanding of Cyber Security.

3. **How serious are the external threats**
   a. Webhost (look at live screen share of fail2ban, showing current attacks) This will show the live scale of the attacks we face on the internet.
   b. 65000 attacks a day a look at a survey of external attacks
   c. Ransomware, how big is this business? How can we stay safe?

4. **How serious are the internal threats?**
   a. Look at email hacking, how easy it is to find out if you have been hacked. Live demo
   b. How dangerous is phishing? Look at the threat of Phishing even to well prepared organisations
   c. How quickly phishing has responded to the current crisis. Some pointers to remember when dealing with email.

      Are you all aware of phishing? Do you think you would recognise a phishing attack?

d. Social media:
   How great is the threat?
   What do the attackers do?
   Do we share too much? Is this making us a target?
   Who can we trust?

e. Data leaving the building, we are all working at home so our data is in theory all outside the building.
   How can we lower the likelihood of loss?
   The old leave the laptop on the train trick, can we mitigate against this?

5. **So, what can you do? As a Business**.
   a. NO TRUST
   b. Personal devices a and guest wifi
   c. No trust and cloud services,
   d. Firewalls
   e. Encryption of devices
   f. Keep software up to date
   g. Looking at popular cloud services
   h. Backups and how they can save your bacon

6. **Individual**
   a. Training (how many did training in last year?)
   b. Does training help? If not why not?
   c. Can we make more secure choices?
   d. How many of you changed your passwords in the last three months?
   e. How many of you use the same password over and over? Why?
   f. Have you changed your home router logins?
   g. Do you use separate wifi networks for work and home?
   h. How have you configured your zoom meetings?
   i. Do you use mobile devices for work? Do you use your personal device?
   j. How many people asked for help? Was help forthcoming?

7. **GDPR and Cyber security**
   a. What are your responsibilities (transparency, availability, security (Confidentiality), Integrity, permission/consent) CIA!

b. Generating or losing trust how to keep customers and show how awesome you are.
c. Privacy educated clients, they all know too much.
d. Possible repercussions. Avoiding regulators fines.

8. **Cyber surgery** with Jae and Chris (rest of session roughly 30mins) Questions and answers, problems solved