5 Cybersecurity traps – Webinar FAQ's

On the 2nd of June we hosted a webinar discussing 5 of the biggest cybersecurity traps arising as a result of lockdown easing. Led by Sunil Bothra, Global Cybersecurity Expert at Experis Consulting, there were questions from the audience. The below document captures these with sage advice for individuals and organisations on how to keep data, IP and I.T infrastructures safe from cyber-attacks.

FAQ

1. **What plans do you think we need to make for the next major crisis (i.e. black swan) given the probability is it will be digital?**
    a. Build a clear/documented fundamental risk framework and business policy, including an awareness of the human WFH risk. The fundamental policy and behaviours will encompass the majority of unseen risks. Upskill and educate staff as to expected behaviours and risks
2. **Should IT functions be involving HR to create new policies? If we want to audit home users, some will refuse without a new suite of policies to guide behaviour.**
    a. This is a new territory, where businesses continue to break down the silos – an employee's health can have a material impact on the security of a firm. If you are saying the employee's impact is across soft controls and hardware, there will need to be a group conversation to work across impacted business units, including HR. The new environment will also focus on a relaxed, productive employee that will lean on HR to mould in a rapidly evolving market.
3. **What are the specific risks to the pharma industry?**
    a. Pharma is very much in an arms race at the moment, they are taking risks to win the race to an effective medication and the bounty that comes with that. That means that they are also a target of the hackers, with huge value to the dark market. Due to the risk of pressure driving people to work around controls and risk frameworks they are a critical risk and all parties related to pharma should reassess their relations including supplier interaction and vice versa.
4. **Are COVID-19 contact tracers safe to install? What should I do if I only have a work phone?**
    a. There are vulnerabilities with the apps and communication settings, you can turn them off; Bluetooth and app settings. Install apps only from certified sources, the organisation should have a policy on what can and cannot be loaded.
5. **Could you tell us a little bit more about the risks related to remote employees with Cloud interaction?**
    a. We would need to assess to offer detail; the level of interaction will outline how much risk there is. The level of exposure is what is on the cloud and the value of this to the firm and as a result to criminals. Is there a one solution to protecting the cloud database? Alternatively, do you have multiple levels of access, dependent on the particular data and value to the organisation? Segregate your cloud depositories and the corresponding access. Fundamentally segregate and cleanse current users regularly.
6. **Employees now use work laptops at home, but some use their own personal computers as well - to increase the number of screens, etc. the question to ask is - is it significantly riskier using personal computer as oppose to work computer - both connected via home wifi**
    a. A problem that we addressed in the previous webinar. However, firstly most routers are made by a small number of manufacturers – these have well known vulnerabilities to be able to hack and access your network.

       The Wi-Fi itself needs a password – always change the Wi-Fi password and protect your router. We can assess to offer more valuable analysis, however the basics are the same for everyone. All personal hardware must meet the same corporate standards attributed to organisational assets.

Experis™ ManpowerGroup

7. **How would you further protect from ransomware?**
    a. Training and awareness, make them risk averse to anything coming in, encourage not to click on any links from non-certified sources. Have an escalation strategy in the event of a breach and segregation of access duties, including a cleanse from old users.
8. **I am a small business owner, the webinar was very comprehensive, what do I do next?**
    a. We have created products that can offer risk assessments and creating frameworks based on acceptable proven models that reinforce the behaviour within the organisation. These products are built on institutionally accepted standards, while also built to be affordable and able to be implemented in-house. Visit our website for details and pricing, alternatively you can email Michael.hampton@experis.co.uk