Lancashire Cyber Foundry

5 tips to help your business return to work cyber securely

READ TIME: 2 MINS

AUDIENCE: BUSINESS & TECHNOLOGY

At the time of writing this article (Feb 2021), businesses are starting to discuss what returning to work looks like. With cyber-attacks on SME's up by nearly 40% since we started working from home, now is a great time for your business to consider cyber security for when you return.

1. PUT POLICY IN PLACE FOR RE-INTRODUCING DEVICES THAT HAVE BEEN AT HOME

Policy seems such a formal way of putting it, but basically you need a plan. It will be a long time since everyone's worked in an office environment and since working from home, our practices have all slipped a little. Viruses could have been downloaded and lie dormant; unauthorised software could have been downloaded; a child could have split juice over the keyboard. You actually don't know what state your equipment is in, until you look.

We would recommend writing some rules for when people return to work with their devices.

2. COLLECTION OF DATA FROM HOME LOCATIONS

With the combination of work life and home life, there are lots of places sensitive business data could have ended up that isn't a business IT system. Have people used their personal emails at all? Is there data on USBs or external hard drives anywhere? Is there paperwork in someone's spare room?

We would recommend thinking about what process you need to ensure all data returns to the building and IT systems.

3. CYBER SECURITY TRAINING UPON RETURNING

Had we known we were going to work from home for over a year, I'm sure many of us would have undergone some working from home cyber security training. We would have spent time deliberately learning about the risks in this new working environment. Fortunately, we have been

European Union
European Regional Development Fund

NORTHERN POWERHOUSE HM Government

Lancaster University

warned that we will be returning to the office and so it's a great time to relearn those policies and practices we've not had to think about for a while.

We would recommend putting your staff through your usual cyber security training (or new training if you don't already insist on this).

4. BACKUP YOUR DATA

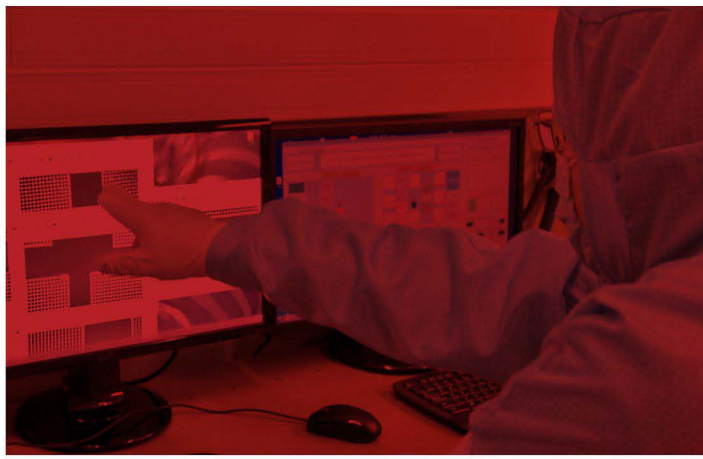
Ransomware has been increasing since 2019. As people return to work and start to centralise their IT systems again this will become an increasingly valuable target to hackers. One quick way you can defend yourself against the disruption that can cause to your business is to regularly backup your IT systems.

We would recommend you backing up your business data and any IT machines which your company uses every 24 hours.

5. REVIEW YOUR NEEDS

Inevitably your working setup will have changed and will continue to change once you've returned. Will you have a more relaxed working from home policy? Will you have a more relaxed Bring Your Own Device policy? Are you looking to hire more staff? Or let some go?

We would recommend planning several check-in points where you and your team evaluate how cyber security is working for you in your current setup and whether you need to change anything.



FIND OUT MORE

We run a series of business strategy and cyber workshops specifically designed for SMEs in Lancashire. We're passionate about seeing Lancashire business become more cyber aware and innovative and so offer funded places for companies to come and learn how to defend, innovate and grow their business.

To find out more about how your business can access support or register on one of upcoming workshops contact us: *cyberfoundry@lancaster.ac.uk*

ABOUT THE AUTHOR

Geraint Harries

Before starting at Lancaster University over 4 years ago, Geraint had worked in software development roles in both IBM and the Civil Service. In addition to being a qualified teacher, Geraint has worked freelance with a varied client base as a software developer and graphic designer.