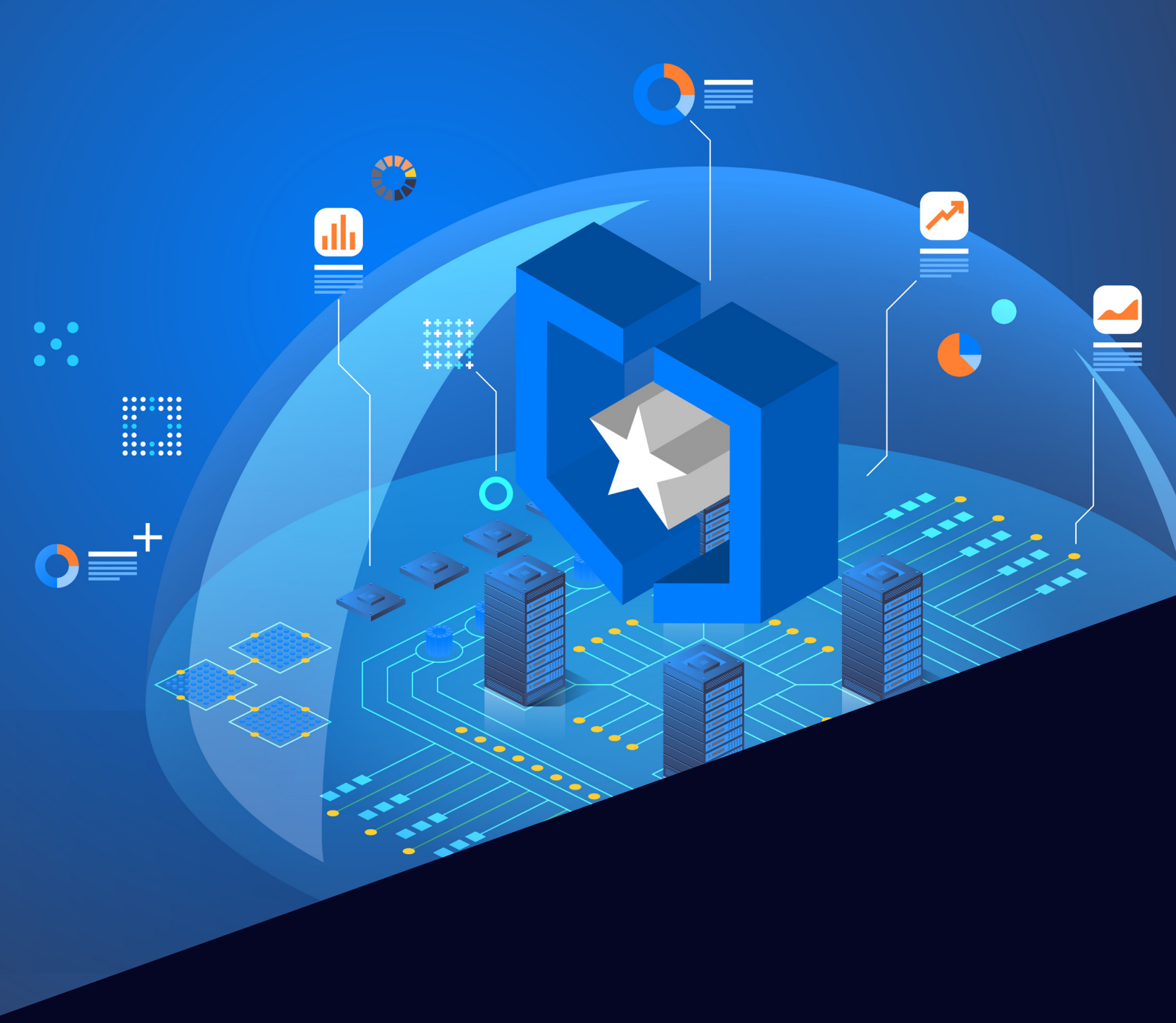

The impact of Covid-19

Home Working

IN PARTNERSHIP WITH

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Scottish Business Resilience Centre

Home Working and the impact of COVID.

Home or remote working can be a godsend for employees. It can mean more time with family, less commuting, and meetings from the comfort of your own living room. However, as millions across the world switch to working from home due to the COVID 19 pandemic they may be putting the security and privacy of themselves, their families and their employers at risk.

Employees working at home can also be expected to use video conferencing facilities such as Microsoft Teams, Zoom, Skype and Houseparty to stay connected to colleagues and friends now that physical contact is restricted.

This kind of internet access leaves the user, and by default the company, susceptible to Data loss. There are different circumstances where this problem could arise, from a system failure resulting in deletion of files that don't have a back-up, to the theft of a password that leads to a loss of sensitive corporate information. Many organizations were not and are still not, ready for this change in working practices.

WHAT ARE THE RISKS OF HOME WORKING?

Cyber Fraud:

Fraud is the most commonly experienced crime in the UK. Fraud costs the UK many billions of pounds every year .The Information Commissioners Office (ICO) estimates that annual fraud in the UK is costed at £190 billion. Deloitte, the multi-national professional services network, observes that widespread 'working from home' as a result of the pandemic is an opportunity for Cyber Criminals to devise new ways of data theft and as a result companies face increased cyber risk. They also note that cyber criminals attempting to access corporate data, customer information and intellectual property are not the only threat to businesses - employees can also be a weak link in corporate IT security systems and therefore an increase in staff working from home presents new risks.

More details on the types of cyber threats, (including solutions) can be obtained from a recently created Cybercrime themed document from the SBRC.

Insider Threat:

There needs to be corporate acknowledgement that homeworking could lead to uncharacteristic behaviours and, in the most extreme cases, enhanced risk-taking or internal fraud through lack of regular checks. This 'insider threat' is illustrated by research by CIFAS in the UK showing that almost 40 % of businesses have dismissed employees since the pandemic begun; due to breaches of cyber related policies. This 'homemade' threat to organizations was further illustrated with 55 % of the 200 companies surveyed, planning to formally ban staff from using personal devices at home for work related purposes. Errors could range from poor security practices to using public accessed Wi-Fi or employee fear of reporting faults due to user error.

Scams:

Fraud is being increasingly committed online and its impact can be devastating, ranging from unaffordable personal losses suffered by vulnerable victims, to losses impacting the ability of organisations to remain in business.

Two of the most common offences to be aware of are Phishing and Vishing.

Phishing – the fraudulent practice of sending emails purporting to be from reputable companies, often companies you are already in business with, in order to induce individuals to reveal personal information such as passwords and credit card numbers

Vishing – the same practice as above but using phone calls or voice messages.

Family distractions/ overheard conversations:

'Being overlooked' is a real threat for home workers. Many may share houses with family or housemates and some users will have to work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials. Additionally, they could be easily distracted by family members, phone calls to landlines at home or callers to the house, including children coming home from school or deliveries to the home address.

Environment:

Working from home also carries risks to employers in terms of health and safety, accident reporting, electrical safety, trip hazards etc. All of this, if it impacts on an employee or the company IT equipment, needs to be a consideration.

SO HOW CAN YOUR ORGANISATION MITIGATE THE RISKS PRESENTED BY HOME WORKING?

It is uncertain how long the current situation will last, but the UK may be in this for the long haul and the impacts may be enduring, **so firms will require long-term adjustments to working practices and culture.**

Whilst there will undoubtedly be further regulatory guidance in many areas, firms will need to be proactive in assessing and addressing the new emerging risks and the changing priorities.

There are therefore a number of things organisations can do to mitigate against these threats and protect employees working remotely, not to mention protecting their own corporate data.

Organisations should consider reviewing and communicating policies to home working staff. There needs to be **clearly defined guidelines for managing information**, particularly where employees have access to or responsibility for personal or corporate information.

KEY CONSIDERATIONS FOR MITIGATING HOME WORKING RISKS COULD INCLUDE:

Additional training for employees. If staff are clear about what they are to do and how to do it whilst working from home this will mitigate the risk of accidental loss or theft of data.

Reminders about company policy and security protocols leaving the home worker in no doubt that they require to follow the same security guidelines at home as they would in the office. A reminder to always keep confidential documents out of sight of prying eyes, securely store materials and only refer to them when it is safe to do so would also be important.

Better access to IT support during office hours with clear lines of communication for this and access to managers for advice and support.

Investing in technology- If employees are to be able to work from home at the same pace and with the same efficiency as in the office, most will require the latest technology. This includes high-spec hardware (laptop, smartphone and printer), up to date software (video-conferencing tools and data management systems), and a reliable internet connection (fast broadband and secure access to the corporate network via VPN). No use of public WIFI networks. This could include the use of software enabling a computer to shut down quickly when idle, protecting sensitive data.

HR/ Line management contact- Staff should be confident in reporting issues they are concerned about, so ensuring there are reporting mechanisms in place is vital for all workers. Line managers should consider a daily contact and keep clear lines of communication open. This is essential in maintaining employee mental well-being and in ensuring that remote workers do not feel detached or isolated from colleagues or managers. Clear management direction on tasks should be a prerequisite and welfare a key consideration with scheduled breaks and 'ground rules' in place and re-enforced.

Guidance on homeworking set up- This may seem obvious but organizations should be prepared to provide guidance for employees to identify a safe and dedicated workspace where they can concentrate. This may make practicalities easier and reduces distractions. If the employee doesn't have a home office, an ad-hoc space could be utilised and boundaries created for family members or other occupants. Regular working hours aligned with those that are working from an office will also benefit homeworker's routine and assist with access to other employees and technical support if needed.

Safety advice- If an employee is working from home and this by definition becomes their working environment then consideration should be given to safety and environment advice. Companies might want to reiterate advice on appliance safety, accident reporting procedures or advice on seating posture and even home security or fire safety as the corporate relationship between employee and employer extends to other areas and locations.

HELP AND FURTHER GUIDANCE

The National Cyber Security Centre (NCSC) has published advice and guidance to help organizations of all sizes with their cyber security during the changes in work practices imposed by COVID-19.

Home working advice for organizations and phishing guidance useful to any organization working remotely.

Bring Your Own Device (BYOD) being the new 'norm' for industry, with wider guidance to help businesses with choosing and purchasing devices, as well as the advice offered to users.

The NCSC's Board Toolkit provides resources to help encourage important conversations between decision makers and their technical experts to ensure cyber security is taken seriously.

NOTES

Scottish Business Resilience Centre

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

01786 447 441
enquiries@sbrcentre.co.uk
www.sbrcentre.co.uk
@SBRC_Scotland

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27

IN PARTNERSHIP WITH

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

SOCT
SERIOUS ORGANISED CRIME TASKFORCE