News

Cyber security Q&A

Updated 9 April 2020 (first published 31 March 2020)

The coronavirus situation is causing difficult business conditions and uncertainty for many law firms and solicitors.

The Law Society has advised that unless you are part of the justice system and therefore classed as a key worker, you should be doing all you can to close your office and work from home. [https://www.lawsociety.org.uk/topics/coronavirus/] That means an unprecedented number of solicitors and staff will be working from home and providing their services digitally, some having never done so before.

This will present many with new cyber security challenges. Below we set out our view how the cybercrime risk is affected by the requirements of social distancing, and of what you can do to protect yourself and your firm.

Open all [#]

How has the cybercrime situation changed?

The change to mass homeworking is that more people might be exposed. And criminals have taken advantage of concern over the Covid-19 outbreak.

- The National Cyber Security Centre (NCSC) has reported a 400 percent increase [https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march] in coronavirus related fraud reports in March.
- They believe this is linked to the increase in homeworking.

However, the basic nature of the threat to solicitors and law firms from cybercrime has not changed.

The money and sensitive information that solicitors and law firms handle is still attractive to criminals.

- Those criminals are still operating.
- The cybercrimes we now hear about are using the same basic tactics as criminals were using before the current crisis.

Ransomware is still a threat to firms.

- With more people working remotely or from their own devices, your risk of encountering ransomware may increase.

- Most ransomware spreads through phishing campaigns, so training against these will help against ransomware.
- You should not assume that ransomware that has encrypted client confidential information has not also stolen that information.

What are the technology risks from homeworking?

Routine homeworking will present staff with new challenges and an unfamiliar situation. At the same time, they will be feeling anxiety and stress from the ongoing pandemic. This may make them less likely to recognise cyber threats. To protect you, your staff and your clients, consider the following:

- You will need to introduce and communicate sensible and pragmatic security arrangements that support you and your staff while using remote IT systems
- You might consider giving staff simple how-to guides to help them adapt.
- This is particularly important for those staff who have not previously worked remotely.

Working outside a secured office presents some additional challenges. Staff might be more likely to have their devices stolen when they are away from the office.

- Encrypt laptops and install a system to track and delete data from tablets and phones remotely if they are lost or stolen.
    - Someone who is not authorised to access a device or system should not be able to access in formation on it or use it to access working systems.
    - A suitable PIN or complex password will protect your device, and many devices include fingerprint recognition.
    - The NCSC give more detailed advice on how to protect mobile devices [https://www.ncsc.gov.uk/guidance/keeping-your-smartphones-and-tablets-safe] .
- Use two-factor authentication for log-ins where possible:
    - Two factor authentication means systems that need two different methods to prove identity before they allow access, for instance a password combined with a code sent to a smartphone.
- Make sure that you and all staff avoid predictable passwords, using longer strings of characters that cannot be easily guessed.
    - Make sure your staff have access to good guidance on choosing passwords that are easy to remember but hard to guess.
    - The NCSC give advice on how to choose a non-predictable password [https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0] .

- Be careful about who can see or overhear what you are doing when working with sensitive information.
    - We appreciate that it may be hard to avoid family members overhearing conversations while working at home. You should use your best efforts to avoid this.
    - Screen protectors are available which can help stop people from reading over your shoulder.
    - Remember to always lock the screen when away from your computer.

Particularly given the rapid move to mass homeworking, we know many staff may be using their own devices rather than work-issued machines. These can be less secure.

- Always make sure to log out of a shared device when you have finished using it to ensure nobody else can see confidential material
- You will need to make sure that your security controls can be applied to any device your staff are using. This will increase the demands on your IT support.
- The NCSC give advice on controlling the risks from staff using their own devices [https://www.ncsc.gov.uk/guidance/byod-executive-summary] .
- The Information Commissioner's Office (ICO) give advice on the law relating to bring your own device policies [https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf]

Remote users may need to use software and applications differently.

- It may be helpful to produce a series of basic written guides to help them work effectively.
- This will be particularly helpful when introducing software that your staff do not ordinarily use in the office, such as online collaboration tools or video chat rooms.

You will need to make sure that your staff can securely access your IT resources. The best way to do this is with a virtual private network (VPN) from a reputable provider.

- You will need to make sure that your systems are protected against ransomware and other malware
- Backup your important data to protect it from loss due to an accident or a ransomware attack.
- Make sure that access to your backup is restricted
- Make sure that your backup system is not permanently connected to the device holding the original copy
- Make sure that you know how to restore your system from a backup
- For more information, the NCSC give information on mitigating malware and ransomware attacks. [https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks]

Given the circumstances, this might be a good time to encourage staff to take the e-learning courses provided by the NCSC. This will help to update their knowledge and give them the latest information.

You should make sure that staff know how to report any problems or breaches to you.

- Make sure that staff know the importance of keeping software and devices up to date, and that they know how to do this
- Use training to help build a positive and blame-free culture of reporting, where staff feel comfortable coming forward with issues that they have encountered.

How have phishing scams changed?

We know that criminals are using fears about Covid-19 in their phishing attempts.

- Some scams claim to have information about treatments for the disease.
- Others are disguised as charity communications seeking donations.
- Some impersonate official bodies, such as the UK government or the US Centre for Disease Control.

The phishing scams that were circulating before the current crisis have not stopped. These include emails and telephone calls claiming that HMRC are investigating the recipient.

As with all phishing scams, fake Covid-19 emails will contain falsified documents or links to websites. Clicking on the attachment or link will either download malware onto your computer or try to get you to give the criminals personal information and passwords.

For more information about phishing, you can look at the National Cybersecurity Centre (NCSC) guidance on spotting and dealing with phishing emails [https://www.ncsc.gov.uk/guidance/suspicious-email-actions] .

What should I do if I have been affected by cybercrime?

If you or a member of your staff have accidentally clicked on a phishing link, then there are steps that can be taken to help control any damage.

- Open your antivirus software and run a full scan, following any instructions given
- If you may have been tricked into giving away a password, then change the password on all your accounts
- Contact your IT department and let them know

If you or your firm have experienced an incident that has affected client money or information, or that may have affected them, then you will need to report it to us, and where relevant to Action Fraud [http://www.actionfraud.police.uk/] and/or the ICO [https://ico.org.uk/for-organisations/report-a-breach/] .

We recognise that these are exceptional circumstances and that the coming months could present firms with particularly challenging issues.

As our enforcement strategy [https://higher-rights.sra.org.uk/sra/corporate-strategy/sra-enforcement-strategy/] sets out, we will take a proportionate approach. When you report breaches to us, we will take into account all mitigating circumstances. We will focus on serious misconduct, and will distinguish clearly between people who are trying to do the right thing and those who are not.

If you do face compliance difficulties linked to the virus, you should clearly document the approach that you have taken. If you are unsure about a specific scenario, then please contact our Professional Ethics team [https://www.sra.org.uk/contactus] .

Where can I go for further advice?

Our report on Technology and legal services [https://higher-rights.sra.org.uk/archive/risk/risk-resources/technology-legal-services/] gives more advice on cyber security, including while working away from the office.

For advice from the NCSC on cyber security while homeworking, you can see their latest guidance [https://www.ncsc.gov.uk/guidance/home-working]

The Law Society has also produced guidance on cybersecurity while working from home. [https://communities.lawsociety.org.uk/practical-support-features/cybersecurity-when-working-from-home/6000880.article?utm_source=professional_update&utm_medium=email&utm_campaign=PU-03%2f27%2f2020]

The ICO [https://ico.org.uk] has produced guidance on data protection and the coronavirus.

For official information about Covid-19, please refer to trusted resources such as Public Health England [https://www.gov.uk/government/organisations/public-health-england] or the NHS [https://www.nhs.uk/conditions/coronavirus-covid-19/] .

What are the technology risks from remote meeting systems?

Many firms are using remote meeting systems for team communications and meetings. These can be valuable tools to help firms operate while most staff are working from home.

However, there have been cases of unauthorised people hijacking meetings where the platform has not been used securely. As well as causing disruption, this may let a criminal overhear confidential communications.

To protect yourself and your staff, consider the following:

- Do not leave meetings set to "public".
- As the host of a remote meeting, set a password for access or use your platform’s features to control who is allowed to attend.
- Post meeting links directly to the people you want to attend, rather than sharing links on media that could be publicly available.
- Set screen sharing to "host only".
- Make sure that you and your staff keep remote working applications fully updated.
- Consider producing a simple guide for your staff on how to use these systems effectively and appropriately.
- Make sure that your information security policies cover appropriate use of remote working systems.