To whom it may concern,

Over the past year there has been a nationwide increase in the number of legal firms subjected to cyber-attacks; in particular ransomware attacks. In response to this increase we are reaching out to provide advice and guidance to law firms within Avon and Somerset Police force area. If it would be of assistance to your members you may wish to raise this concern and to distribute the below Cyber Protect advice.

What is ransomware?

Ransomware is a form of malware that is designed to deny a user or organisation access to files on their computer or device. This means the user cannot access the locked files on the computer making them unusable. Often the files are copied, with threats made to publish the contents on the dark and/or surface web. Once the files have been locked and/or copied, the cybercriminal will contact the victim and offer to unlock and/or delete the copied files for a 'ransom'. The payment is usually requested in cryptocurrency or another hard to trace route.

Technical controls to consider

Whilst you should always seek your own specialist cyber security advice the following are recommendations:

File permissions and access

- User accounts with special access privileges should only be assigned to authorised individuals and managed effectively.
- Remove or disable user accounts when no longer required.
- Admin accounts should be used as little as possible with no email or internet access if possible.

Locking accounts

- Automatic lock on accounts after a small number of unsuccessful login attempts.

Two-factor Authentication (2FA)

- Always implement 2FA where available, especially on admin accounts.
- This prevents an attacker, who knows your password, accessing or modifying your account because they cannot pass the second factor without access to the mobile number

Updates

- Regularly update devices and software as soon as reasonably possible.
- Replace unsupported devices and software as soon as possible.
- Keep anti-virus and anti-malware up to date.

People and Processes

Attitudes and culture

- Always aim to maintain a positive cyber security culture throughout the organisation.
- Provide regular training and raise awareness of the latest threats and scams.
- Provide a 'no blame culture' to allow for an easy reporting environment.

Phishing

- Ensure all staff are aware of how to spot phishing emails and how to report them.
- Look out for urgency, authority, and curiosity as indications of phishing emails
- Don't click on links or unknown attachments within emails.
- Always consider Take Five and take a moment to stop and think what is being asked of you.

Strong and unique passwords

- Have a strong password policy which may include using three random words (e.g. WindowZebraRainbow).
- Provide staff with a safe way of managing and storing their passwords
- Avoid sharing passwords or account credentials.

Be prepared

- Keep your response plan up to date and review it regularly.
- Carry out regular tests.

Further resources and support

Avon and Somerset Police Cyber Protect Officers can deliver protect and prepare training sessions to help reduce the organisation's attack surface and lower the chances of a cyber-attack. The advice that we provide focusses on prevention and how we can stop people from becoming repeat victims. Advice can range from simple online safety advice like complex passwords and two-factor authentication to physical hardware, implementations of software, and security mechanisms behind applications. Our aim is to ensure people are following the right guidance available to them, which is vital for online survival against threat actors.

If you would like more information, please contact:
CyberProtect@avonandsomerset.police.uk

For further information and resources:

- The National Cyber Security Centre (NCSC) provides advice and guidance covering a broad range of topics - https://www.ncsc.gov.uk/
- Cyber Essentials helps you to guard your organisation against cyber-attacks - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Security Information Sharing Partnership (CISP) allows UK organisations to share cyber threat information - https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
- South West Cyber Resilience Centre (SWCRC) is led by serving police officers and aims to help businesses and charities in the region protect themselves from cybercrime. They provide free core membership which delivers simple and comprehensible guidance on reducing cyber risks - https://www.swcrc.co.uk/

Reporting

If you are a victim of cybercrime, please report it to Action Fraud either via phone on 0300 123 2040 or their website.

If you require additional assistance, please contact me on the details provided below.

Sincerely,
Megan Haldane 6068
Cyber Protect Officer

Mobile 07514 622819
Email megan.haldane@avonandsomerset.police.uk