Solicitors Regulation Authority

Cybercrime – Covid-19, homeworking and changing risks

Robert Loughlin, Executive Director, Operations and Performance,

What we will be covering

Solicitors Regulation Authority

- The developing situation
- Cybercrime thematic review
- National Cyber Security Centre (NCSC) update
- Q&A
- What might be coming
- Top tips

The developing situation

- What we are seeing
- The impact on law firms

Cybercrime – the trends

Cybercriminals are developing & boosting their attacks at an alarming rate

Jurgen Stock,
INTERPOL

300% increase in phishing emails during first two months of lockdown

NCSC

Ransomware is a growing threat - globally cases doubled in 2020

Cybersecurity
researchers

The consequences

Solicitors Regulation Authority

£2.5m stolen in the first six months of this year

Losses are not just financial for victims

High costs for affected firms too

How we are responding

Solicitors Regulation Authority

- Enforcement Strategy – taking a proportionate approach
- Risk Outlook has the latest NCSC guidance
- Help and guidance on our website –our latest thematic review

Cybercrime thematic review

Rachel Clements

How risks looked in our review

- £4m stolen from 23 firms
- £400k paid by firms
- Data security & governance
- Email modification fraud
- Phishing and vishing
- Ransomware

Key risks: training and support

Solicitors Regulation Authority

60% of firms viewed their staff as the greatest risk

20% of firms had not provided any cyber training

88% of fee earners could not explain the term ‘ransomware’

Test your knowledge

Solicitors Regulation Authority

You have received a ransomware demand. What is the first thing you should do?

A. Determine if it is legitimate. If so, inform the SRA and follow the instructions carefully to get your data back

B. Ignore the demand and back up your data, you do not need to inform the SRA

C. Do not pay the ransom. You may need to inform the SRA, ICO and the police

Policies, controls and technology

- 32% no disaster recovery plan
- 57% had not tested processes
- 20% no policy on USBs
- 20% no incident records
- 37% using Windows 7
- 55% using external USBs

- **Evidence of IT support over-reliance**

Remote working risks

Managing client risks

- Warn you would not email bank a/c changes
- Monitor firm email accounts
- Scrutinise 'out of place’ emails
- Confirmation strategies for transfers
- Look at alternatives to holding client money

Test your knowledge

You have received a ransomware demand. What is the first thing you should do?

Correct answer

C. **Do not pay the ransom. You may need to inform the SRA, ICO and the police**

Help and support

Solicitors Regulation Authority

Cybercrime thematic review

sra.org.uk/cyber-security-review

Cybersecurity tips and advice

https://www.sra.org.uk/solicitors/resources/cybercrime/

National Cyber Security Centre
a part of GCHQ

Solicitors Regulation Authority

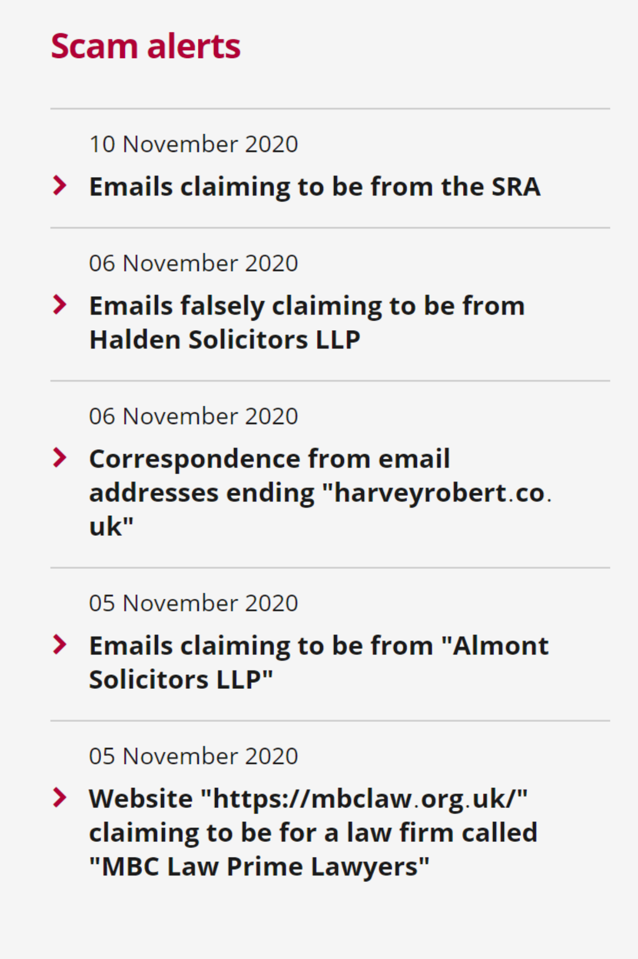
26th November 2020

Karen J, NCSC

National Cyber Security Centre
a part of GCHQ

46% of all UK businesses identified at least one breach or attack in the last year

* *The Department for Digital, Culture, Media and Sport's 'Cyber Security Breaches Survey 2020' reported that almost half (46%) of all businesses have identified at least one cyber security breach or attack in the last 12 months (and 43% have among micro and small firms)



Scam alerts

10 November 2020

› **Emails claiming to be from the SRA**

06 November 2020

› **Emails falsely claiming to be from Halden Solicitors LLP**

06 November 2020

› **Correspondence from email addresses ending "harveyrobert.co.uk"**

05 November 2020

› **Emails claiming to be from "Almont Solicitors LLP"**

05 November 2020

› **Website "https://mbclaw.org.uk/" claiming to be for a law firm called "MBC Law Prime Lawyers"**

2019 Incident trends

1. Cloud Services

2. Ransomware ✓

3. Phishing ✓

4. Vulnerability scanning

5. Supply chain attacks ✓

https://www.ncsc.gov.uk/report/incident-trends-report

Cloud Services

Ransomware

Newcastle University cyber attack 'to take weeks to fix'

6 September

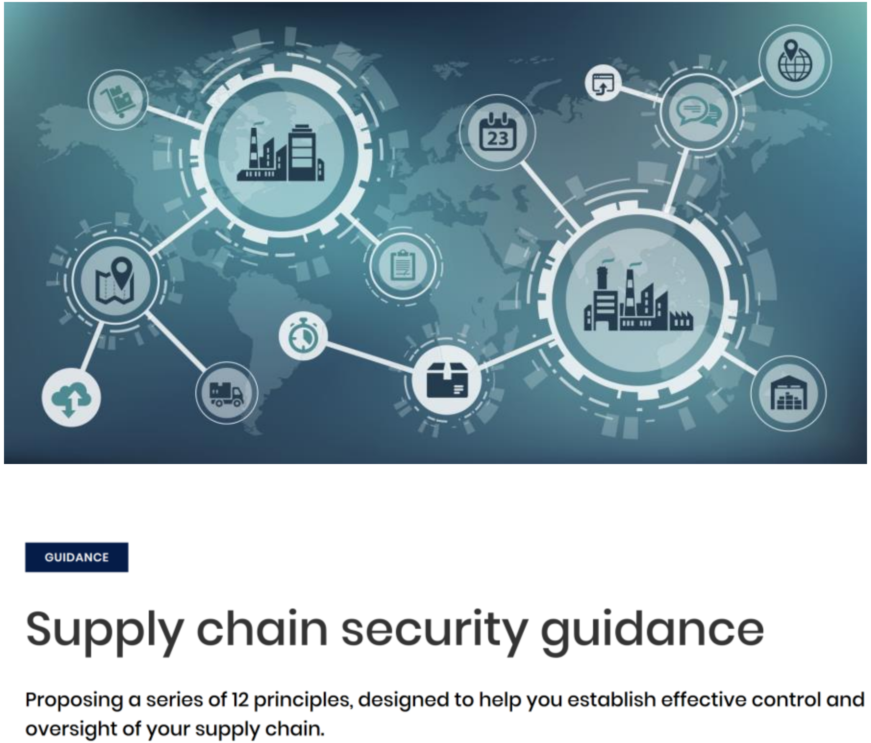
Phishing and Vulnerability scanning

Phishing has been the most prevalent attack delivery method seen over the last few years. Common tactics include:

- *targeting Office 365 credentials*
- *sending emails from real, but compromised, email accounts*
- *fake login pages*

- **Vulnerability scanning** remains a common reconnaissance method to identify unpatched, legacy or vulnerable software.

Supply chain



GUIDANCE

Supply chain security guidance

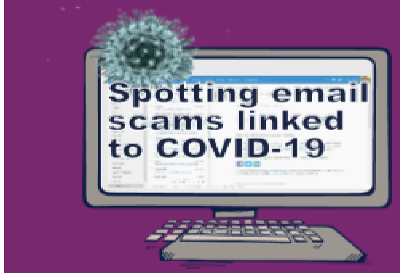
Proposing a series of 12 principles, designed to help you establish effective control and oversight of your supply chain.

WHAT CAN WE DO TO PROTECT OURSELVES

National Cyber Security Centre

Home working:
Managing the cyber risks

Working from home is not new to many of us, but the coronavirus (COVID 19) means organisations are using home working on a greater scale, and for longer periods. This page will help organisations introducing (or scaling up) home working. It also provides advice on spotting COVID-19 scam emails.



Spotting email scams linked to COVID-19

Cyber criminals are preying on fears of COVID-19 and sending scam emails. These may claim to have a cure for the virus, offer a financial reward, or might encourage you to donate. If clicked, you're sent to a dodgy website which could download viruses onto your device, or steal your passwords.

Don't click on any such links. For genuine information about the virus, please use trusted resources such as the **Public Health England** or **NHS** websites.

If you' ve already clicked, don't panic:

- open your antivirus software and run a full scan, following any instructions
- if you've been tricked into providing your password, you should change your passwords on all your other accounts
- if you're using a work device, contact your IT department and let them know
- if you have lost money, you need to report it as a crime to Action Fraud (you can do this by visiting **www.actionfraud.police.uk**)

1. Setting up user accounts & accesses

Set strong passwords for user accounts; use NCSC guidance on passwords and review your password policy. Implement two-factor authentication (2FA) where available.

2. Preparing for home working

Think about whether you need **new** services, or to just **extend** existing services so teams can still collaborate. NCSC guidance on implementing Software as a Service (SaaS) can help you choose and roll out a range of popular services. In addition:

- Consider producing 'How do I?' guides for new services so that your help desk staff aren't overwhelmed with requests for help.
- Devices are more likely to be stolen (or lost) when home working. Ensure devices encrypt data whilst at rest. Most modern devices have encryption built in, but may need to be turned on and configured.
- Use mobile device management (MDM) software to set up devices with a standard configuration in case the device needs to be remotely locked, or have data erased from it.
- Make sure staff know how to report any problems, or raise support calls. This is especially important for security issues.
- Staff feeling more exposed to cyber threats when home working should work through the NCSC's Top Tips for Staff e-learning package.

3. Controlling access to corporate systems

Virtual Private Networks (VPNs) allow home workers to securely access your organisation's IT resources (such as email). If you've not used one before, refer to the NCSC's VPN Guidance, which covers everything from choosing a VPN to the advice you give to staff.

If you already use a VPN, make sure it's fully patched. You may need extra licenses, capacity or bandwidth if you're supporting more home workers.

4. Helping staff to look after devices

Whether using their own device or the organisation's, ensure staff understand the risks of using them outside the office. When not in use, staff should keep devices somewhere safe.

Make sure they know what to do (and who to call) if devices are lost or stolen. Encourage users to report any losses as soon as they can.

Ensure staff understand how to keep software and devices up-to-date, and that they apply updates promptly.

5. Using removable media safely

USB drives may contain sensitive data, are easily lost, and can introduce malware into your systems. To reduce the likelihood of infection you can:

- disable removable media using MDM settings
- use antivirus tools where appropriate
- only permit the use of sanctioned products
- protect data at rest (encrypt) on removable media
- encourage alternative means of file transfer (such as online tools).

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

National Cyber Security Centre
a part of GCHQ

Video conferencing services: security guidance for organisations

National Cyber Security Centre

Moving online

Questions to ask your IT providers

COVID-19 has seen many organisations shutter their physical premises and move their business online. Establishing the IT services to support this transition can seem like quite a challenge. This guidance will help you determine how ready your business is, and point the way to any new cyber security measures you should put in place.

Dealing with new ways of working

Moving your business online will present some new risks, placing more reliance on digital technologies such as web hosting, credit card processing, and productivity tools like email, video and chat.

You shouldn't need a degree in computer science to run your small business securely. But, cyber security is complicated. If you don't have all the IT skills yourself, it can be hard to know what to do - and when you've done enough.

Having good relationship with your IT service provider(s) will help massively with this. So we've identified and explained the key cyber security topics we think you should care about, so you can be sure you're covering all the right bases.

1. Assess the cyber security of your business

Consider if the measures you take to deal with the lockdown will become more permanent ways of working. For example, will you look to expand your online business? If so, you'll need systems which are sustainable and can scale as your business adapts and grows.

2. Establish a baseline

Answering the questions below will give you a good idea of your security status, and identify what areas need attention. The NCSC's Cyber Essentials scheme provides a way to demonstrate to others that you have good security in place.

What IT products and services do you use? Is it your job to look after these, or a service provider's?

Some insurance policies now include a basic level of cover for cyber risks. This can be useful if you suffer an incident. Review your policies to understand the level and type of cover (if any) that is provided.

Are you using cloud services? The NCSC's cloud guidance can help you choose secure products, and use them safely.

Do you have access to IT support? As you become more reliant on digital services, think about how you'd cope if these were unavailable.

Are there any regulations you need to follow? If your business is now processing Personally Identifiable Information (PII) online, you will need to read up on GDPR. If you are processing card payment information, the Payment Card Industry Data Security Standard will apply.

3. Talking to your IT service providers

If you are talking directly with your supplier, the following questions will help you ensure that security is at the forefront of any new service you decide to take on.

Patching & Updates: Ask your suppliers how often they patch the services you use, and check any contracts or SLAs to ensure that patching is included.

Backups: What sort of backup arrangements are in place and how often are these tested? You should know how often your data is backed up, where it is stored, and who has access to it.

Access: Is your data (and the data of others which you have responsibility for) being properly protected? Are you able to put 2FA in place to limit access to your data and services?

Logs: Are logs being kept for security purposes? Logging can play a vital role in diagnosing any problems. Logs will also prove invaluable when responding to and recovering from security incidents.

Incident Response: What will happen if things go wrong? Service providers should operate on the presumption that they will be attacked. It should be clear how and when they will engage with you during a security incident.

Find out more

For more information about how to improve cyber security within your organisation, please read the NCSC web pages especially for small businesses at www.ncsc.gov.uk/smallbusiness.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

National Cyber Security Centre
a part of GCHQ

TLP AMBER

Products & Services

National Cyber Security Centre

CSP REPORT AN INCIDENT CONTACT US

BETA This is our new site, your feedback can help us to improve it.

About NCSC Information for... Advice & guidance Education & skills Products & services Keep up to date

The National Cyber Security Centre

Helping to make the UK the safest place to live and work online

Learn more

NCSC Website

National Cyber Security Centre

Cyber Security Small Business Guide

Backing up your data

Preventing malware damage

Using passwords to protect your data

Keeping your tablets & smartphones safe

Avoiding phishing attacks

Small Business Guide

National Cyber Security Centre

10 Steps to Cyber Security

Network Security

User education and awareness

Malware prevention

Removable media controls

Secure configuration

Set up your Risk Management Regime

Managing user privileges

Incident management

Monitoring

Home and mobile working

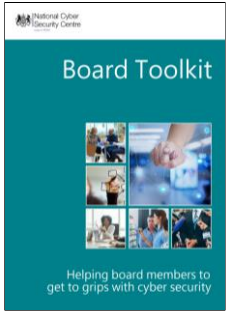
10 Steps

Cyber Essentials (Plus)

CiSP

Trust Groups

Top Tips for Staff


National Cyber Security Centre

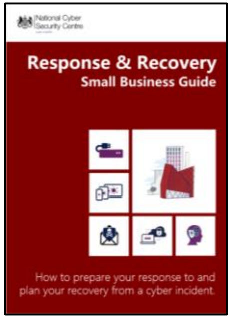
Board Toolkit

Helping board members to get to grips with cyber security

Board Toolkit

BRC CYBER SECURITY TOOLKIT

Sector Specific Toolkit


National Cyber Security Centre

Response & Recovery Small Business Guide

How to prepare your response to and plan your recovery from a cyber incident

Response & Recovery Small Business Guide

National Cyber Security Centre

Sector Specific Assessment

Exercise in a Box

National Cyber Security Centre
a part of GCHQ

Themes & Scenarios

Themes:

- Preventing malware damage
- Backing up your data
- Avoiding phishing attacks
- Using passwords to protect your data
- Keeping your smartphones and tablets safe.

Scenarios:

- Phishing leading to ransomware
- Mobile phone theft and response
- Insider threat Leading to a Data Breach
- Third party software compromise
- BYOD
- Threatened leak of sensitive data
- Unknown Wi-Fi attack
- Supply Chain Risks
- Home & Remote Working
- Technical Scenario

Is Cyber insurance right for you?

The NCSC's Early Warning system provides an organisation notifications of threat events against their networks. This may be alerting that a client on the network has joined a botnet, sharing that there is a vulnerable application on an IP address or that an IP address has been seen conducting abusive activities, such as participating in a DDOS.

Q&A

Solicitors Regulation Authority

- Question during the session
- Questions previously summited:
  - Our IT system was hacked via email and our IT providers are working on protecting the system. They have told us not to tell anyone, is this correct?
  - Our cloud based case management system was attacked. We don’t think the clients are affected, do we need to tell them?
  - I know about phishing and ransomware, what new risks are there?

What might be coming?

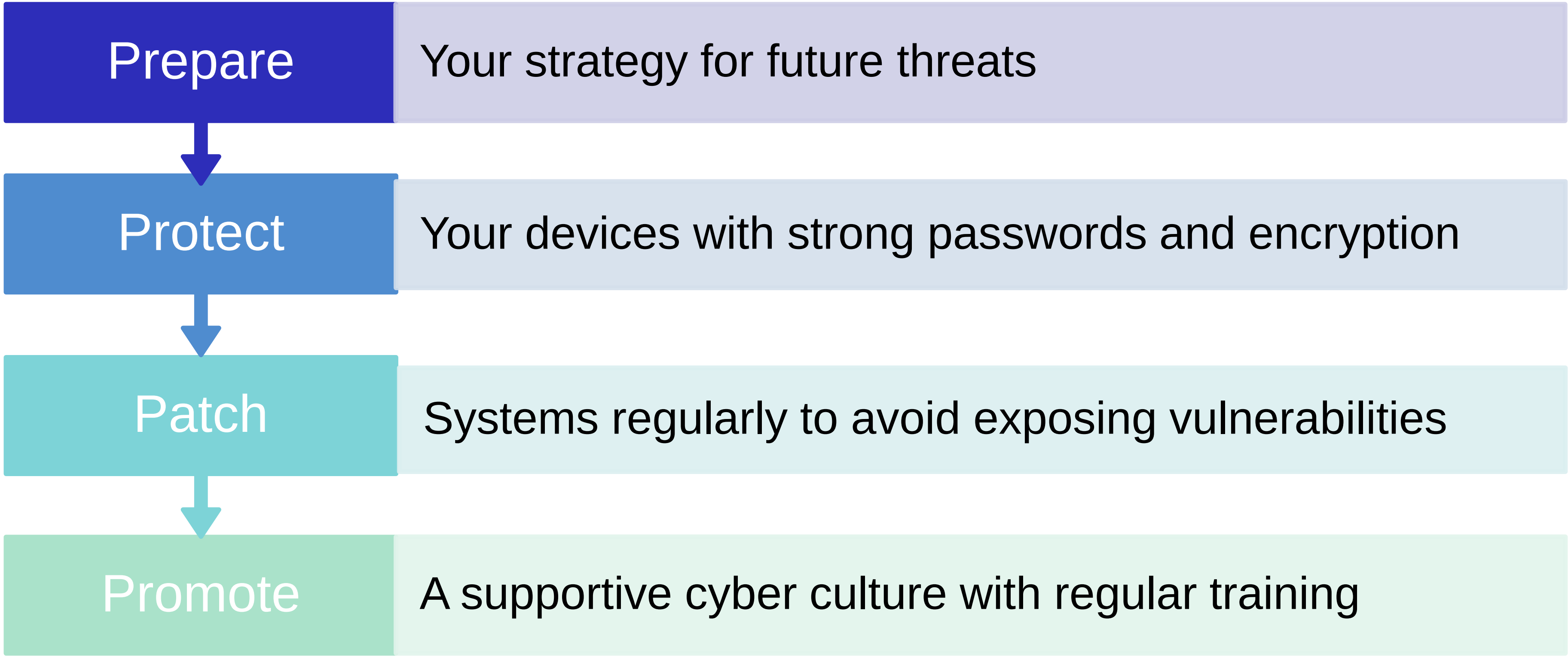
Solicitors Regulation Authority

Criminals will find new ways to attack

Deepfakes may become a significant threat

Principles for a Cyber Secure Environment

Solicitors Regulation Authority



Prepare – Your strategy for future threats

Protect – Your devices with strong passwords and encryption

Patch – Systems regularly to avoid exposing vulnerabilities

Promote – A supportive cyber culture with regular training