# News release

## *Cybercrime issues continue*

28 March 2017

Cybercrime is a priority risk for us and for law firms, and the problem is increasing.

New scams are emerging all the time, and we recently warned of firms being contacted by email by criminals pretending to be potential clients, but who then send attachments containing malware.

Go to the warning [/sra/news/press/2017/scammers-target-firms-march-2017/]

We outlined the issues of malware in our latest paper on cybercrime, which was presented to the Board in December.

Go to our December report [/risk/risk-resources/information-security-report/]

Malware can be used to infect your IT systems with a virus which locks you out and only the criminals can let you back in, if you pay them a 'ransom'. Alternatively, the virus gives the criminals control over your IT systems, allowing them access to sensitive information.

You have an obligation to report an incident to us if there is a shortage on the client account. It is important that firms that are involved in cyber crimes meet their obligations to replace any monies that have been wrongly paid out of the client account.

Our warning notice from June 2015 pointed out the duty firms have to replace any client account shortages as quickly as possible.

We have, in the last two months, disciplined two firms for not making good on client shortages in a timely manner. Reporting any cybercrime incidents to us, regardless of whether or not the attempts were successful, is also key.

### *What information you should share*

We need you to report all your experiences of cybercrime so we can keep on building a clear and up-to-date picture of the risks, and warn the whole sector of the dangers. Currently, you have an obligation to report an incident to us if there is a shortage on the client account.

Sometimes, because firms are doing the right thing for their client and making good the loss immediately, some attacks are going unreported. Even when the client has been taken care of, we still need to be informed.

There are other instances where there is no obligation to tell us, but we still want you to get in touch. For example, an unsuccessful attempt to hack your systems.

And of course, cybercrime is not just about hacking. There might be email or phone attempts to obtain sensitive information from your firm (known as phishing and vishing). These attempts might come to nothing, but they are still cybercrime incidents ,and the information helps us to make sure everyone know what the latest threats are.

### *Making clients aware*

We also want to see firms taking steps to make their clients aware of the risks. So, for example, in conveyancing we would recommend that people avoid sharing bank details over email, or transferring money before confirming the source of any request.

## *Protecting yourself*

When it comes to cybercrime, it's up to you to make sure your firm and clients' money and information is safe. That means training staff and staying vigilant, as well as maintaining up-to-date technology protections

You should have robust procedures in place to deal with cybercrime attempts or if you or your client is affected - for example do you know who to contact at your bank to try and stop payments going through

Further information is available in the December report [/risk/risk-resources/information-security-report/] .