News

Reporting cybercrime incidents

11 January 2024

There have been a number of high-profile cybercrime incidents in recent weeks, including on IT provider CTS, who supply services to a number of firms.

We wanted to remind you of our expectations if you are subject to an attack.

If your firm or its clients are directly affected by a cyberattack, we would expect this to be reported promptly. If there has been serious breach of our Standards and Regulations [https://upgrade.sra.org.uk/solicitors/standards-regulations/] , your firm has an obligation to report this under Rule 3.9 of the Code of Conduct [https://upgrade.sra.org.uk/solicitors/standards-regulations/code-conduct-firms/#rule-3] .

However, in all cases where an attack has had or has the potential to have an impact on clients, we would still expect a prompt report to be made. For example, an attack that means you can't complete transactions, or service to clients is significantly delayed, or there is a risk that client data or assets have been lost. This allows us to understand and monitor the risks and root causes of attacks impacting the sector. Read our guidance on how to make a report to us [https://upgrade.sra.org.uk/solicitors/guidance/reporting-notification-obligations/] .

We also encourage firms to report significant cyberattacks to us, even if these attacks have not been successful or haven't negatively impacted clients. We recognise that your firm, like most organisations, will experience a lot of malicious activity, such as phishing and other forms of cyberattacks, which are managed as part of business as usual.

It would be disproportionate to ask you to report every routine attack, but sharing information about near misses and significant or novel attacks can help us form a picture of the risks in the sector. This helps inform our advice and warnings for the profession.

You can make a report via the form on our website [https://upgrade.sra.org.uk/consumers/problems/report-solicitor/] . Please include 'Cybercrime incident' in the subject box of your email.

Protecting your clients and business, support and advice

Although you can reduce the risk of successful cyberattacks, we recognise that no business can eliminate that risk completely. It is therefore vital that you have business continuity plans in place that work through how you would keep your business running in different scenarios and continue to deliver a good service for clients.

You can find helpful advice in our Risk Outlook on information security and cybercrime. [https://upgrade.sra.org.uk/sra/research-publications/risk-outlook-report-information-security-cybercrime/]

You might also want to consider getting accredited under the Government-backed Cyber Essentials scheme, which you can get more information about from the National Cyber Security Council [https://www.ncsc.gov.uk/cyberessentials/overview] (NCSC).

The NCSC also has a range of guidance on how to secure systems against common attacks, including:

- Phishing attacks: defending your organisation - NCSC.GOV.UK [https://www.ncsc.gov.uk/guidance/phishing]
- Small Business Guide: Cyber Security - NCSC.GOV.UK [https://www.ncsc.gov.uk/collection/small-business-guide]
- Russian FSB cyber actor Star Blizzard continues worldwide - NCSC.GOV.UK [https://www.ncsc.gov.uk/news/star-blizzard-continues-spear-phishing-campaigns]
- Guidance for high-risk individuals on protecting your accounts and devices [https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals]

You can also report related suspicious activity [https://report.ncsc.gov.uk/] to the NCSC.

Any firm with questions about the effects of an attack, such as client confidentiality or indemnity insurance issues, can contact our Professional Ethics helpline [https://upgrade.sra.org.uk/contactus] for advice.

Finally, the Legal Ombudsman has advice on how to help your clients in this matter to keep complaints to a minimum. You can find this in their technical advice desk [https://www.legalombudsman.org.uk/information-centre/learning-resources/technical-advice-desk/] section.