Solicitors Regulation Authority

Cybercrime Thematic Review 2020

What did we do?

- Analysis of the experiences of 40 firms we interviewed
- Randomly selected from 458 reports between 2016 and 2019

Cyber Quiz

Solicitors Regulation Authority

How much client money did firms report had been stolen in the first half of 2020?

a. £591,644

b. £982,781

c. £1.8m

d. £2.5m

Cyber Quiz

Solicitors Regulation Authority

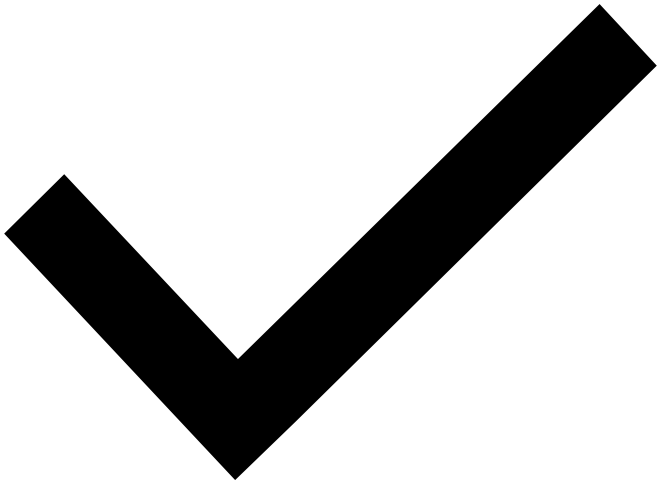
How much client money did firms report had been stolen in the first half of 2020?

a. £591,644

b. £982,781

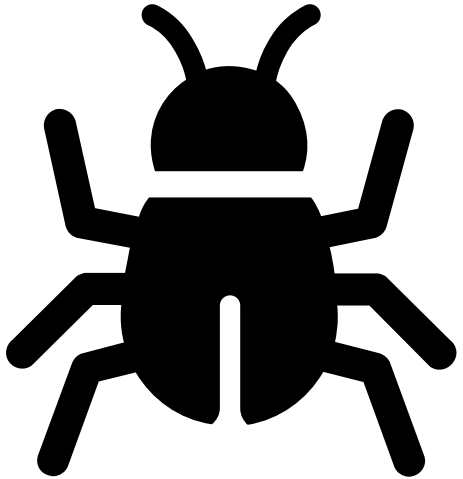
c. £1.8m

d. £2.5m



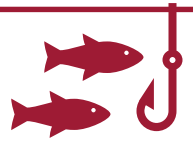
Types of attack

- Email modification most common attack
- 26% of attacks targeted clients
- Large firms targeted hundreds of times
- Opportunist and targeted
- Conveyancing transactions most targeted but not the only area
- 60% of firms felt their biggest risk linked to staff behaviors



Case study

- **Type of attack:** Vishing



- **Tactic:** Psychological Manipulation

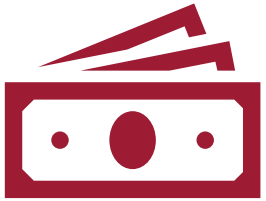
- **Funds transferred:** £1.2m

Impact

- £1.2m shortage and client matters halted
- SRA Investigation
- Policy excess charge – £2.5k

The immediate impact of attacks

Solicitors Regulation Authority



Loss of 4m client money at 23 firms

394K paid directly by firms to replace client money

Disruption, excess costs, time and effort

Reputational damage and emotional impact

Mitigation: Policies and Processes

Solicitors Regulation Authority

Good Practice

- 30% had specific cyber insurance
- 5 with Cyber Essentials Plus accreditation had good policies
- 15 escalated concerns to senior managers
- 5 had a specific cyber budget
- Most had good banking details procedures

Mitigation: Policies and Processes

Solicitors Regulation Authority

Poor Practice

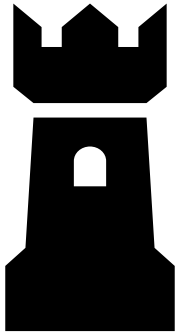
- 60% did not keep an incident log
- 25% had inadequate policies
- 20% had never provided cyber training
- 20% without a policy on removeable media
- One firm's PII did not cover client losses from cybercrime

Mitigation: Controls

Solicitors Regulation Authority

Good Practice

- Two factor authentication used by most
- Most firms used accounts and permissions
- 50% protect & delete equipment remotely
- All systems password controlled and most used software to change regularly
- Clear reporting lines and IT support

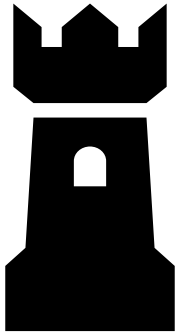


Mitigation: Controls

Solicitors Regulation Authority

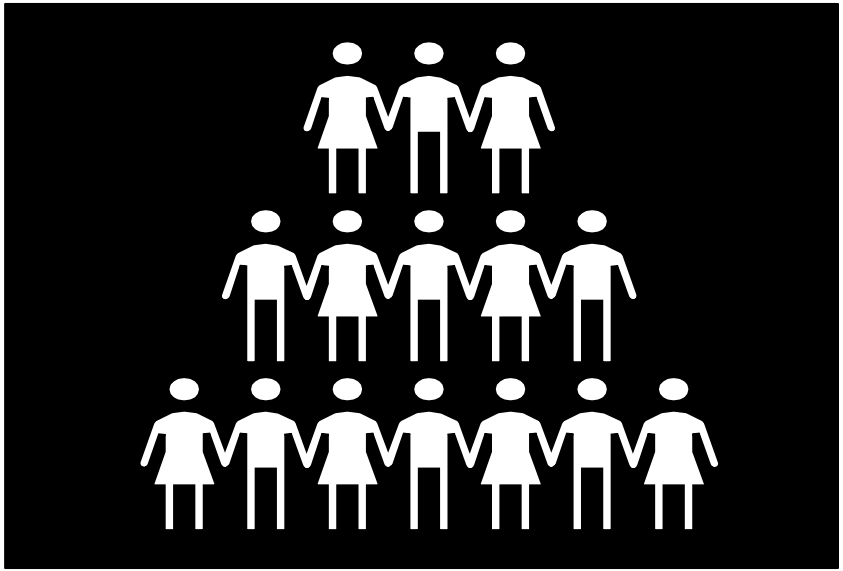
Poor Practice

- 25% did not encrypt laptops/mobile devices
- Two firms exposed to attacks by IT providers
- 60% accepted data sticks from 1/3 parties
- 47% did not have a systems inventory
- 37% operating systems almost outdated



Mitigation: A Human Firewall

- A supportive ‘no blame’ business culture
- Reward and motivate staff
- Regular training (free!)
- Encourage staff to regularly scrutinise emails
- Oversight and clear reporting lines



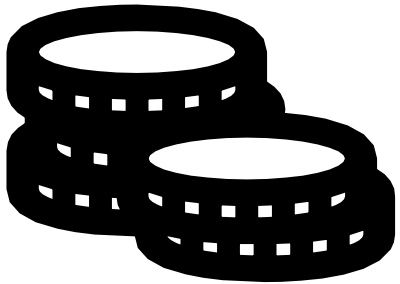
Your Obligations:

Solicitors Regulation Authority

Rule 6.1 Solicitors Accounts Rules:

Repay client money

immediately

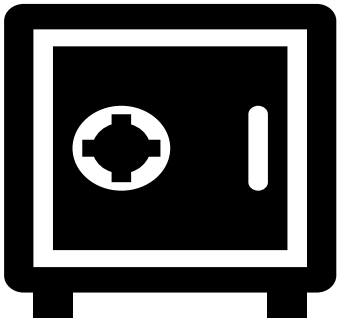


Your Obligations

5.2 & 2.9

Standards and Regulations

Monitor risks, safeguard funds and assets



Reporting Obligations

Solicitors Regulation Authority

Know your

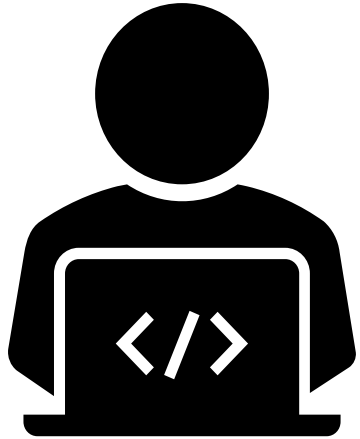
reporting requirements:

The SRA and ICO

Five steps to manage cyber risks

Solicitors Regulation Authority

- Update your knowledge
- Patch software and monitor malware defences
- Support and motivate staff
- Plan for future threats
- Have effective cyber management oversight



Further reading:

Solicitors Regulation Authority

SRA Cybercrime Thematic Review:
www.sra.org.uk/sra/how-we-work/reports/cyber-security/

Cyber Essentials Scheme
www.itgovernance.co.uk/cyber-essentials-scheme

SRA guidance and materials
www.sra.org.uk/solicitors/guidance/cybercrime