May 2022

UK Legal Services Cybersecurity Survey Research Report

Table of Contents

Foreword

At Menlo, we help companies everywhere work safely – boosting productivity by helping individuals and teams to operate confidently, from anywhere, without interruption. To do this, we are always curious as to how individual industry sectors think about and manage their specific cybersecurity issues.

In our experience, legal practitioners both within law firms and in house have become a serious – and often easy – target for cyber criminals due to the extremely sensitive nature of their work and the fact that legal documents are now digital, stored, collaborated on and shared online. The results of this research show the very real impact of cyber breaches in terms of loss of productivity as well as the risk to confidentiality.

While legal industry bodies are taking serious strides to provide guidance on avoiding attacks, it is surprising to see here that a number of firms are yet to action this advice. And, with an increasing shift to home/hybrid working we are also working with law firms to address the consequent gaps in their security stack.

For legal security specialists seeking to make the internet a worry-free, work-freely place, we hope this research gives food for thought as you talk to your users and plan your risk management and security strategy.

Mike East
VP EMEA, Menlo Security

Executive Summary

Introduction

In March 2022, IRN Research was commissioned by Menlo Security to undertake independent research amongst 150 legal professionals in the UK. Using an online survey, these professionals were asked questions relating to the issue of cybersecurity in their own law firm and in the legal services sector in general. The questions asked are included in specific sections of the report.

Context

Given the personal and financial data that law firms hold, they have become a target for cyber attacks and these have increased in recent years. There have also been a few high-profile cases of data breaches and phishing scams hitting some large law firms.

In response to this, both the Solicitors Regulation Authority (SRA) and the Law Society have published guidance and advice for law firms on how to develop cybersecurity policies and procedures and how to deal with an attack.[1, 2] The SRA opened a consultation with its law firms to ask for feedback on the SRA's plans to clarify the scope of cover in professional indemnity policies when a firm is subject to a cyber event. The consultation results were published in October 2021[3]. The Council for Licensed Conveyancers (CLC) has also explored requiring law firms to purchase standalone cyber insurance in a consultation paper in 2021 as "evolving forms of cyber-risk" become more complex.

In the latest Annual Top 100 Law Firm Survey[4] from PWC in October 2021, the top 100 UK law firms stated that cyber attacks were the biggest threat to their ambitions. 90% of the top 100 law firms were "extremely or somewhat concerned" about the impact of cyber threats on their business over the next 12 months, even though only 4% had experienced an attack (none of which were in the top 50)

Against this background of a growing threat from cyber attacks, exacerbated by the increase in digital services for clients and the switch to more home working, this survey canvasses feedback from 150 legal professionals on their concerns over cyber attacks, law firm cybersecurity procedures and training, plus their awareness and use of the published industry guidance on cybersecurity.

Results overview

Cybersecurity and the threat of cyber attacks is a clear concern for a majority of legal professionals, but there is still a minority that do not appear to see these as an issue. Phishing emails to clients are seen as the major threat, probably because these are now a regular occurrence in the legal services sector: 26% of the phishing attacks the SRA examined in

Cyber Security - a thematic review, were targeted at the client's email account, rather than the firm's account. The damage, notably financial loss to the client, which can be caused by these apparently genuine emails that are out of control of the law firm, can have a lasting effect on the client-law firm relationship.

Just over half are satisfied that they are receiving good cybersecurity training. This leaves a sizeable minority that do not. Also, cybersecurity training in some law firms has not kept up with changes in service delivery and working practices, for example - more digital legal services such as documents transferred, stored and signed in the cloud, and hybrid working between home and office.

Key results

- Three of the five cyber attack types listed in the survey have a relatively high threat level according to respondents. Top of the list are phishing emails to clients and malware/phishing emails on mobiles, both seen as offering "threats" or significant threats" to their law firm by 60% of respondents. Just over half – 53% – identify phishing emails to the law firm as a "threat" or a "significant threat". Less than half feel that malware on websites or ransomware offer the same threats.

- An overwhelming majority of respondents are clearly concerned about the reputational damage that could be caused by a major cyber attack: 92% identify this as "damaging" or "very damaging". Not far behind at 90% is the inability to operate and data loss (87%).

- Over three-quarters (77%) have switched to home working during the pandemic and 58% of those are in law firms that have changed their cybersecurity measures to deal with home working. However, only a minority (45%) have updated their cybersecurity training to address home working.

- Almost half (47%) have introduced digital services with the majority (77%) changing cybersecurity measures to deal with these new services. However, less than half (47%) have done the same with staff training.

- Despite the gaps in training, 56% feel that they have had good training relating to identifying and dealing with a cyber attack. However, this leaves 44% that have gaps in their training.

- Just over half (52%) feel that their firm is well prepared to deal with a cyber attack but this leaves almost half (48%) believing their firms are less well-prepared.

- A majority are aware of the advice and guidance published by the Law Society and the SRA, but only around a third have read it and just over 4 out of 10 have checked the consultation content from the SRA. More than 6 in 10 individuals (61%) accept that they have a responsibility to identify and report any cyber threats to their firm.

- A majority (57%) are working in firms that have procedures in place to deal with a cyber attack, leaving 43% (or a sizeable minority) with no clear guidance on how to deal with an attack. On an individual level, 69% of respondents are satisfied that they know how to deal with a phishing email.

- Just over half (52%) work in a law firm where there is a dedicated person to deal with cybersecurity, but in 38% of firms, there is no dedicated resource.

Survey sample

The survey sample consisted of legal professionals primarily in UK law firms with an annual turnover of between £10m and over £100m including 22 firms from the UK Top 100. A small sub-sample included 15 in-house legal professionals.

The breakdown of respondents by job title is shown in Figure 1, with the majority of those taking part being solicitors, associate solicitors, partners, or managing partners.

Figure 1 : Job title of interviewees in sample (%)

Position	Number	%
Managing Partner/Partner	26	17%
Solicitor/Senior Solicitor	48	32%
Associate Solicitor	17	11%
Legal Executive/Paralegal	18	12%
Practice Manager/Finance Manager/HR Manager	18	12%
Other	7	5%
In-house legal professional	16	11%
Total	**150**	**100%**

Survey results

Phishing emails to clients identified as biggest threat

Three of the five listed cybersecurity threats are seen as major threats by a majority of respondents. These are phishing emails to clients, phishing emails to law firms, and malware/phishing emails on mobile devices.

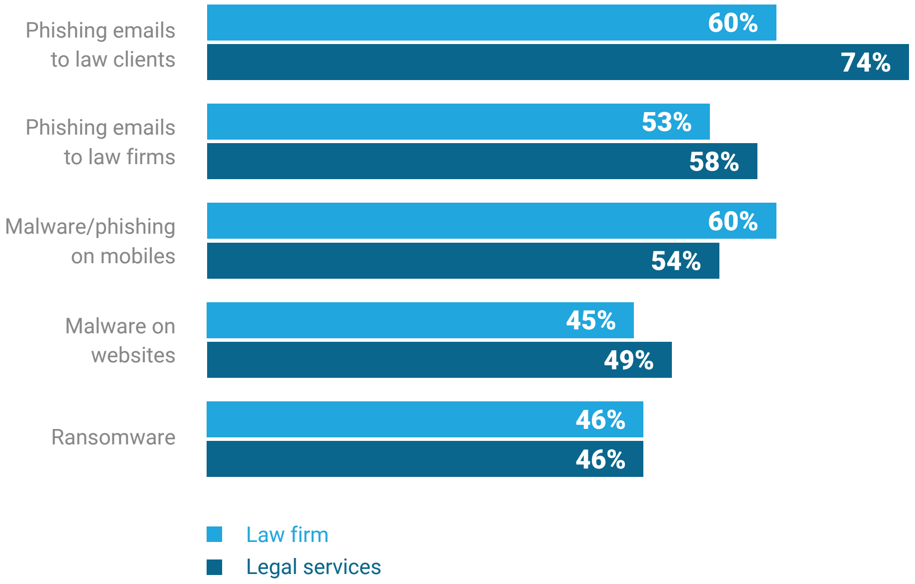
Almost three-quarters (74%) of respondents see phishing emails to clients as either "threats" or "significant threats" to the legal services sector overall, while 60% give a similar threat level for these phishing emails when it comes to their own law firm.

In general, cybersecurity issues are seen as more of a threat to the legal services sector overall compared to their own law firm. The exception is mobile phone-related security threats, with 60% seeing these as "threats" or "significant threats" in their own law firm compared to 54% for the legal services sector overall.

Figure 2 : Cybersecurity issues seen as a threat or a significant threat (%)

Question: *Please rank each of the following types of cybersecurity attack on a scale of 1 to 5 based on their threat a) to the legal profession overall and b) to your law firm in particular?*

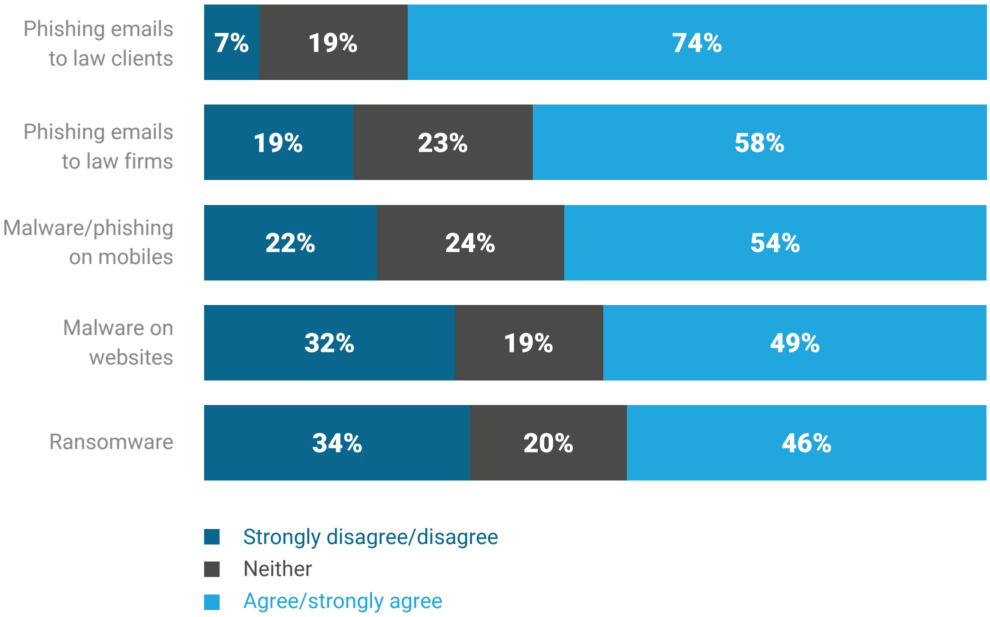
The ranking is: 1 is not a threat at all, 2 is not a threat, 3 is neither, 4 is a threat, 5 is a significant threat



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Ransomware and malware on websites are seen as less of a threat for the legal services sector by around a third of respondents, 34% and 32% respectively. Malware on websites and ransomware are considered even less of a threat to specific law firms – 37% and 35% respectively do not see malware on websites and ransomware as threats.

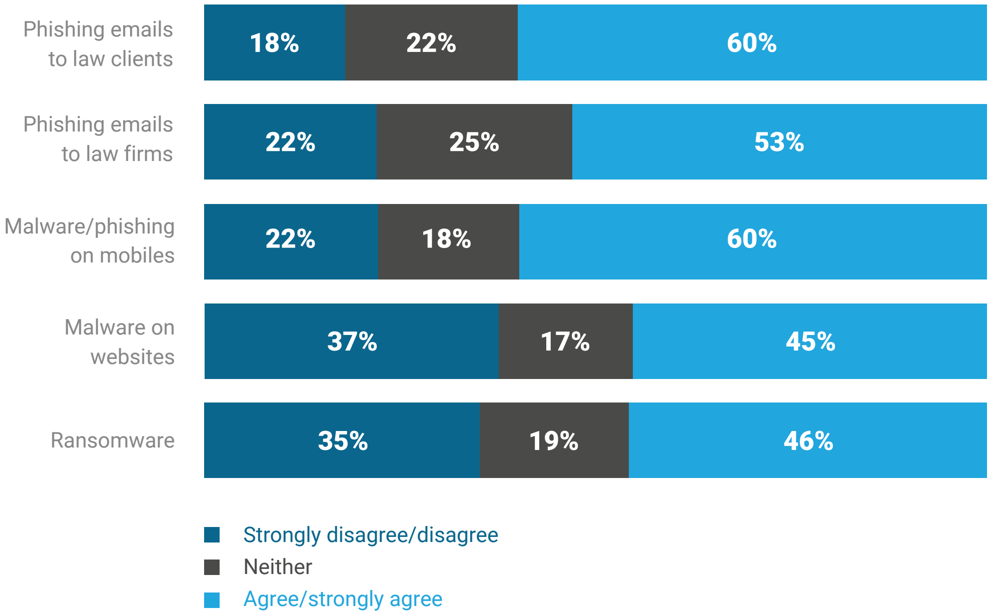
Figure 3: Ranking of cybersecurity threats across legal services sector (%)



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Every few days the home page of the SRA has details of scam alerts where fake emails have been sent to clients pretending to be from law firms. So it is no surprise that phishing emails to clients come top of the threat list.

Figure 4: Ranking of cybersecurity threats in law firms (%)



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Over 90% identify reputational damage as major consequence from an attack

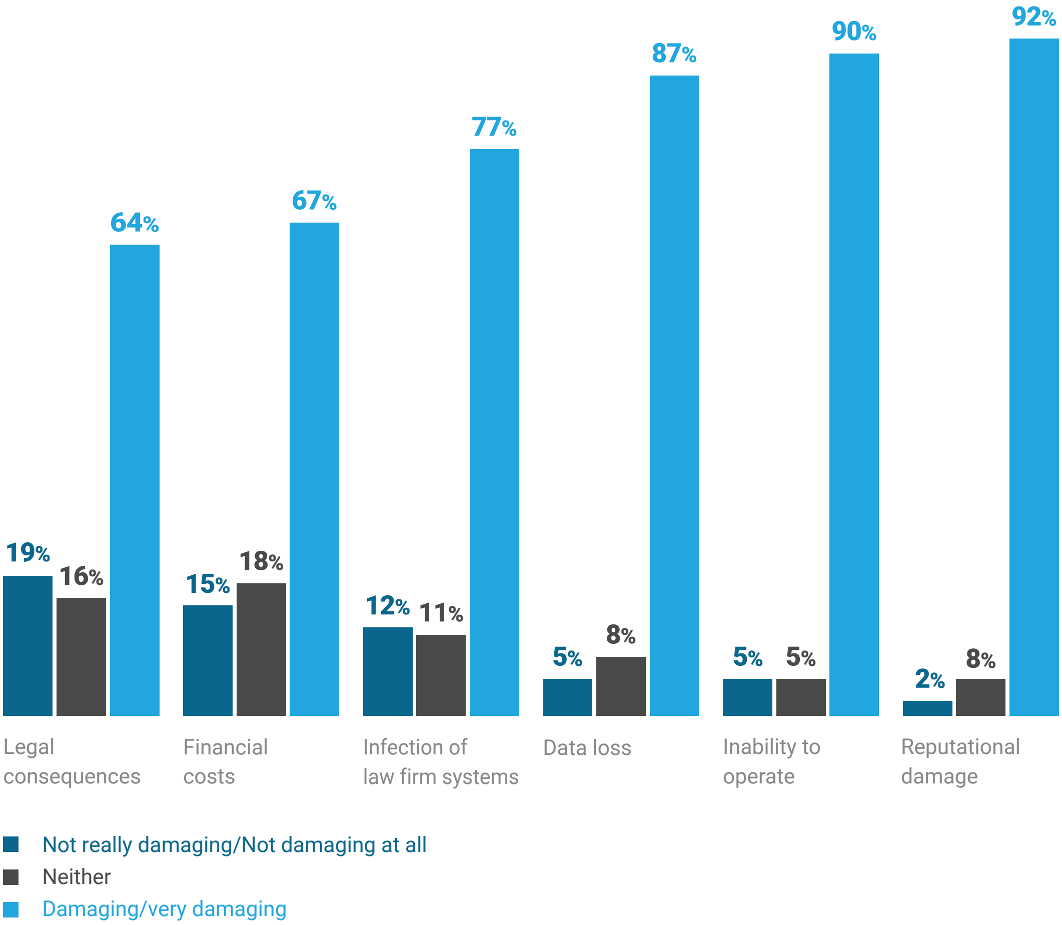
The impacts of a cybersecurity attack range from legal consequences i.e., claims for data breaches against the law firm, through to reputational damage with the majority of respondents regarding them as “damaging” or “very damaging”. Reputational damage to the law firm tops the list with more than 90% seeing it as “damaging” or “very damaging”. This is followed by the inability to operate (90%) and data loss (87%).

Around two-thirds believe that financial costs to the law firm would be “damaging” or “very damaging” while 64% say the same for legal consequences such as claims for data breaches against the law firm.

Figure 5:
Ranking of damages from cyber attacks in law firms (%)

Question:
Please rank the consequences of any cybersecurity attack on a scale of 1 to 5 based on how damaging the specific consequences would be to your law firm.

The ranking is: 1 is not damaging at all, 2 not really damaging, 3 is neither, 4 is damaging, 5 is very damaging



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Figure 6: Remote working in pandemic – those agreeing/ disagreeing (%)

Question: *Please state if you agree or disagree with the following statements.*

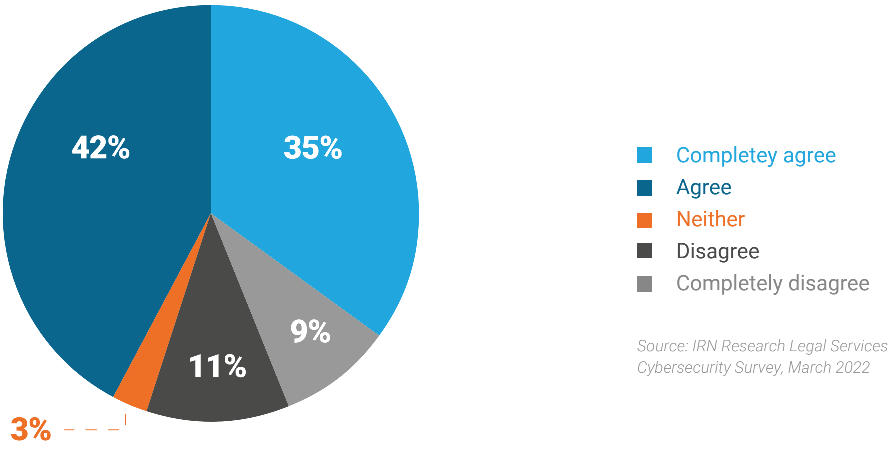
1 is Completely disagree, 2 is Disagree, 3 is Neither, 4 is Agree, 5 is Completely agree:

My firm shifted to remote working (entirely or partly) during the pandemic.

My firm has decided to continue with remote working (entirely or partly) moving forward.

Most updated their cybersecurity measures to deal with remote working but not cybersecurity training

Over three-quarters of respondents – 77% – are working in law firms that switched to remote working (entirely or partly) during the pandemic.

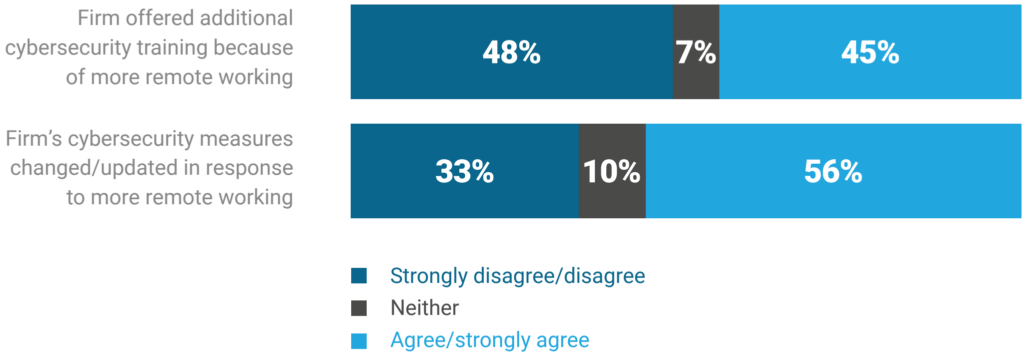


Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Over half of the firms that started working remotely in the pandemic (58%) have decided to continue with some form of remote working moving forward.

While a majority of firms – 56% – changed or updated their cybersecurity measures to address remote working, only a minority (45%) offered their staff additional cybersecurity training.

Figure 7: Cybersecurity changes and training linked to remote working (%)



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Figure 8: Digital legal services introduced – those agreeing/ disagreeing (%)

Question: *My firm introduced more digital legal services during the pandemic, i.e., online services available for clients as opposed to physical face-to-face consultations, document signings*

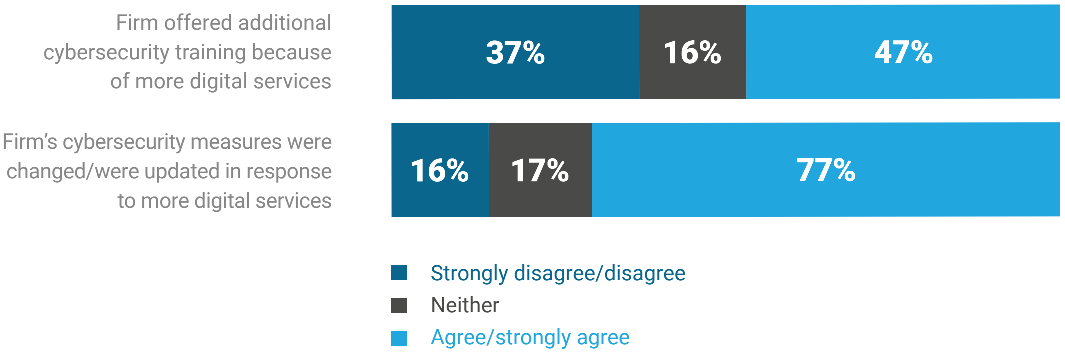
Overwhelming majority introducing digital services updated cybersecurity measures

Just under half of those responding (47%) introduced more digital services for clients during the pandemic.

	Number of respondents	%
1 - Completely disagree	26	17%
2 – Disagree	28	19%
3 – Neither	26	17%
4 – Agree	39	26%
5 - Completely agree	31	21%
Total of respondents	**150**	**100%**

Of those launching additional digital services a large majority (77%) updated their cybersecurity measures as a result. However, only 47% were able to offer additional cybersecurity training corresponding to the new digital services.

Figure 9: Cybersecurity changes and training linked to digital services (%)



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Just over half of firms are well prepared for an attack and offer good training

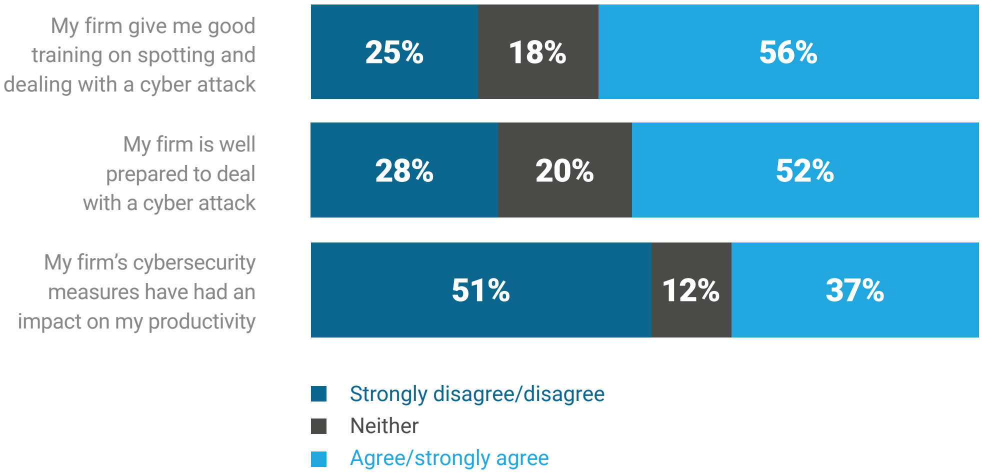
Despite previous responses suggesting that there have been some gaps in cybersecurity training when remote working or digital services were introduced, just over half of respondents (56%) feel that their firm has given them good training on spotting and dealing with a cyber attack.

However, a quarter (25%) feel that the training has not been good enough.

There are similar results when asked if their firm is well prepared to deal with a cyber attack: 58% “agree” or “strongly agree” leaving 28% who don’t.

Over a third (37%) suggest that the firm’s cybersecurity measures have had an impact on their productivity, but just over half (51%) feel that there has been no impact.

Figure 10: Cybersecurity measures and training (%)



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Just over a quarter have experienced a cyber attack

Just 26% work in a law firm that has experienced a cyber attack and, for the largest group (33%), the attack closed services and operations for only a few hours. Another 28% suffered a loss of service and operations for less than 24 hours.

Lengthy delays of one day or more were experienced by 18%, while a fifth (21%) didn't know.

Figure 11: Length of delay to services/operations after a cyber attack (%)

	Number of respondents	%
A few hours, i.e., 2-10 hours	26	33%
Less than 24 hours	28	28%
1-2 days	26	13%
More than 2 days	39	5%
Don't know	31	21%
Total of respondents	**39**	**100%**

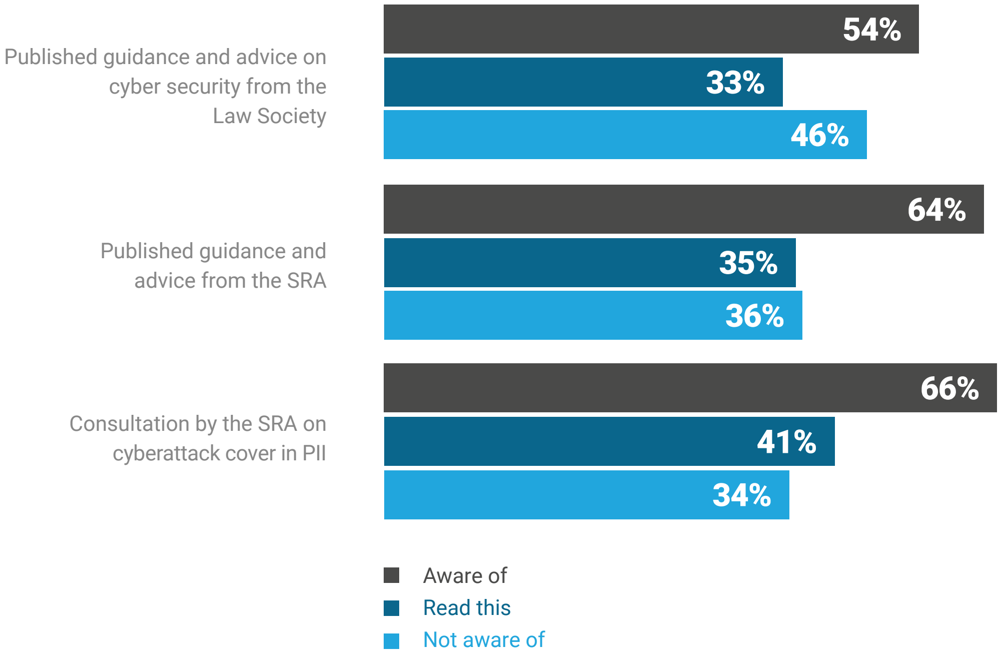
Majority aware of Law Society and SRA guidance but only a minority have read

In the last 18 months, both the Law Society and the SRA have published guidance notes and briefings on cybersecurity while the SRA opened a consultation with its law firms to ask for feedback on the SRA's plans to clarify the scope of cover in professional indemnity policies when a firm is subject to a cyber attack. The consultation results were published in October 2021.

More than 6 in 10 respondents are aware of the SRA guidance documents (64%) and the consultation (66%) but only 35% have read the guidance with 41% having looked at the consultation documents.

Just over half – 54% – are aware of the Law Society guidance, but just a third of respondents (33%) have actually read it.

Figure 12: Awareness and use of published guidance/ consultations on cybersecurity (%)



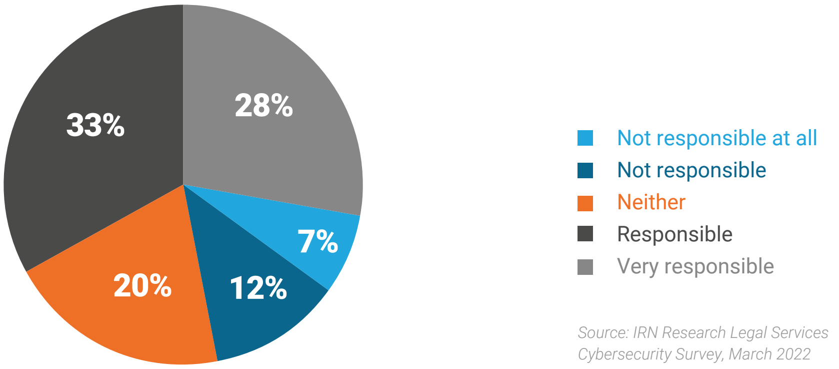
Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Over 6 out of 10 feel responsible for identifying and reporting cyber threats

A third of respondents feel "responsible" for identifying and reporting a cyber threat while 28% feel "very responsible". Almost 1 in 5 (19%) believe that it is not their responsibility to identify and report these threats.

Figure 13: Perceived personal responsibility for identifying and reporting cyber threats (%)

Question: *How responsible do you feel personally for identifying and reporting cyber threats when they occur?*



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

Majority of firms have cyber attack procedures in place

A majority of firms (57%) have procedures in place to deal with a cyber attack, but that leaves a sizeable minority – 43% – that are not prepared to deal with an attack.

At an individual level, 69% of respondents are satisfied that they know how to deal with a phishing email.

Just over half (52%) work in a law firm where a dedicated person is tasked with dealing with cybersecurity issues but, in 38% of firms, there is no such individual.

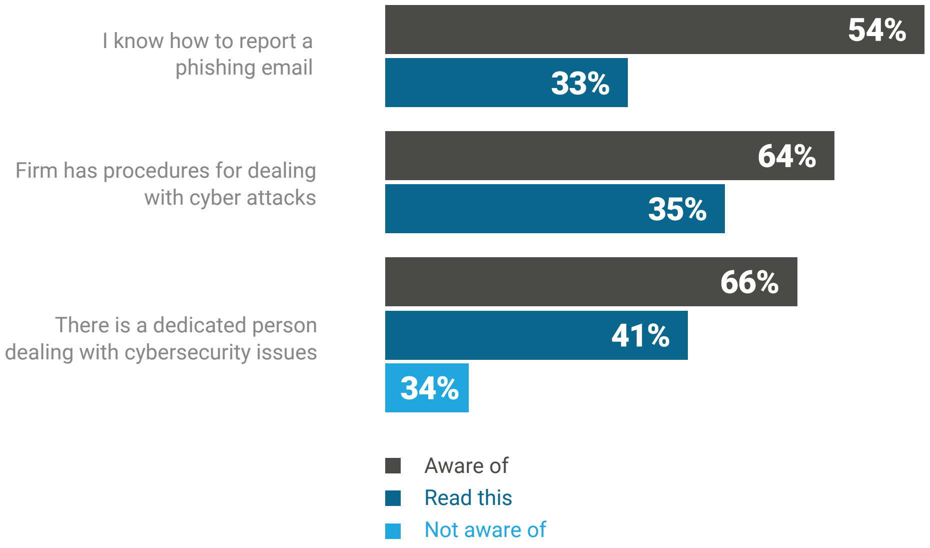
Figure 14: Cybersecurity reporting and procedures (%)

Question: *Please answer YES or NO to the following statements:*

I know how to report a phishing email if I receive one

The firm has procedures in place for me to follow if I discover a possible cyber attack

There is a dedicated person in the firm responsible for dealing with any cybersecurity issues



Source: IRN Research Legal Services Cybersecurity Survey, March 2022

About IRN

IRN Research (trading name of IRN Consultants Ltd) is a full-service market research consultancy with a strong track record in providing market research and analysis services to the legal services sector. Clients include law firms, other legal services providers, regulators, and a range of suppliers to the legal sector. If your needs are for a small-scale UK-based research project or for a large- scale, multi-country research project, we can help. We use a range of market research techniques, including desk research, telephone/ online surveys, face-to-face interviews, focus groups, and can provide a full results analysis. Responding to our client's needs, we go beyond the data and present our clients with actionable insight. We also publish a range of annual market reports on the UK legal sector providing a unique resource for monitoring trends in the sector.

www.irn-research.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

Learn more at www.menlosecurity.com

Sources

[1] *https://www.sra.org.uk/solicitors/resources/cybercrimecybersecurity-advice/*
[2] *https://www.lawsociety.org.uk/topics/cybersecurity/*
[3] *https://www.sra.org.uk/sra/consultations/consultation-listing/pii-cyber/*
[4] *https://www.pwc.co.uk/industries/law-firms/law-firm-survey-report-2021.pdf*