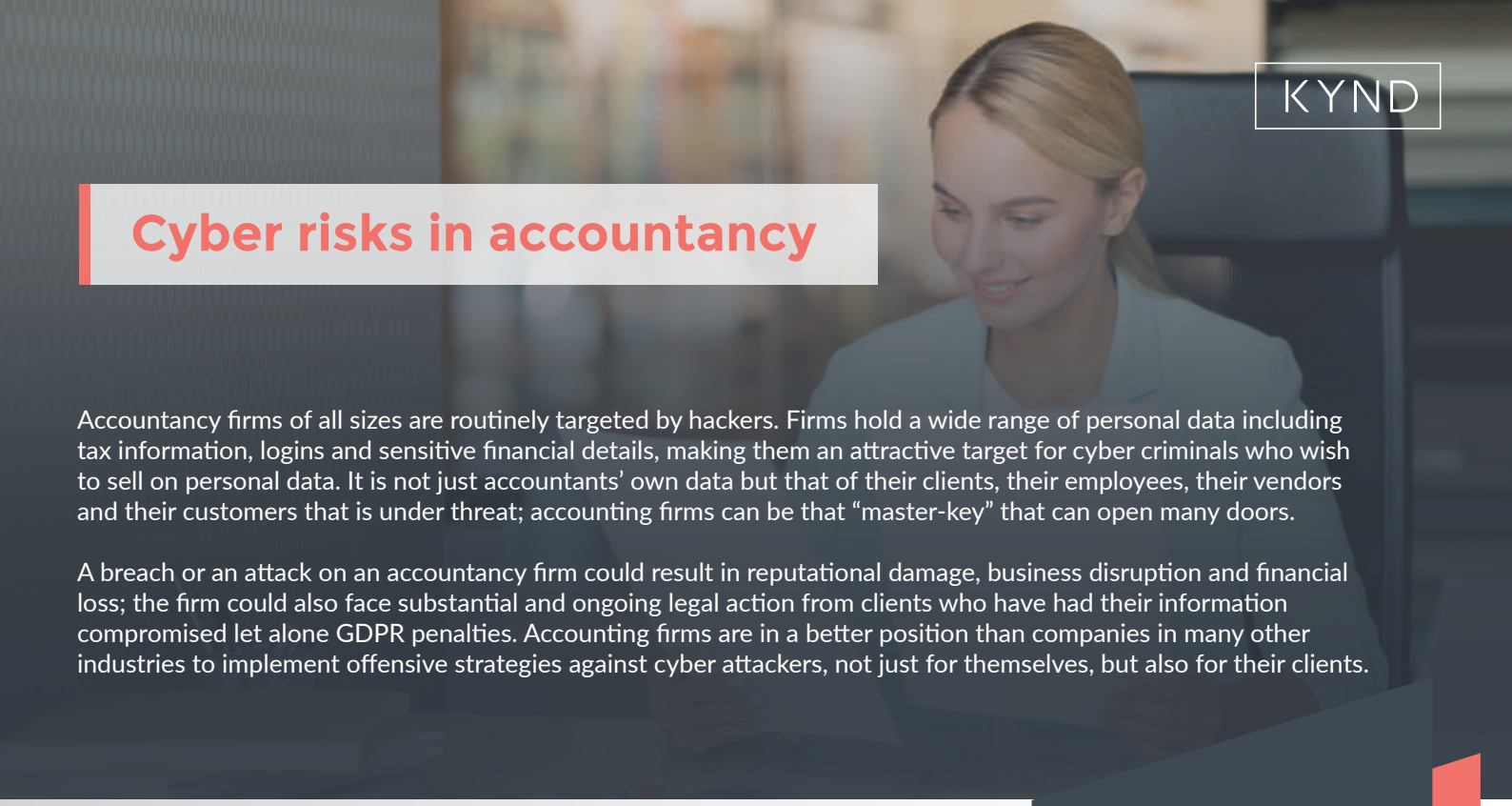

KYND

Cyber risks in accountancy

Accountancy firms of all sizes are routinely targeted by hackers. Firms hold a wide range of personal data including tax information, logins and sensitive financial details, making them an attractive target for cyber criminals who wish to sell on personal data. It is not just accountants' own data but that of their clients, their employees, their vendors and their customers that is under threat; accounting firms can be that "master-key" that can open many doors.

A breach or an attack on an accountancy firm could result in reputational damage, business disruption and financial loss; the firm could also face substantial and ongoing legal action from clients who have had their information compromised let alone GDPR penalties. Accounting firms are in a better position than companies in many other industries to implement offensive strategies against cyber attackers, not just for themselves, but also for their clients.

Business exposure and implications

Financial loss

A firm may incur first party costs/losses in connection with business interruption, ransom payments, reputational harm, legal fees, IT improvements, client notifications.

Reputational damage

It is often reputational damage which can have the most significant impact, as a loss of trust from clients (whether justified or not) can be disastrous if widespread.

Malpractice claims

Failing to adequately secure client data specifically, could see the company facing a hefty fine under GDPR. Clients may make claims against professional financial firms which are unwittingly caught up in cyber frauds. The most common examples are that of claims by clients against accountancy firms.

Insecure devices

Printers and scanners are internally networked devices that store and process data. Due to the nature of their work, accountancy firms use such devices for printing and scanning important and confidential contracts or personal documents. These are often overlooked which leaves firms, and often their most sensitive client information, open to data theft and malware or virus infections.

Access to confidential and sensitive client information

Compromised intellectual property such as tax identification numbers, logins, sensitive financial details can provide a roadmap for criminals to gain access to further systems.

Key industry statistics

72%

is the percentage of tax-filing adults in the US who have expressed some level of concern over their personal data being compromised when they file taxes[1]

80%

is the increase in data breaches in CPA firms from 2014 - 2020.[2]

300%

is the increase in cyber attacks on accounting firms since the start of the Covid-19 pandemic[3]

329,000

is the number of CPA Canada members affected by a cyberattack in 2020[4]

What types of risks exist?

There is a variety of different threats that the accountancy sector could be impacted by, but the most common include:

Phishing
Malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers or stealing passwords in the process.

Viruses
Code which infects computer systems, corrupting or deleting data.

Hacking
An individual or group attempting to gain access to company systems with the intent to steal or destroy data.

Ransomware
A malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

KYND

KYND's analysis of key cyber risks of the top* 100 UK accountancy companies
*by turnover

Ransomware Risk

33.0% of companies had at least one external internet service exposed which would place them at a higher risk of a ransomware attack.

Email Spoofing

96.0% of companies were vulnerable to having their email addresses spoofed.

Vulnerable Services

57.0% of companies were running at least one service, such as an email server or web server, with a well-known vulnerability to cyber attack.

Out of Date Software

33.0% of companies had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

Certificate Issues

69.0% of companies had at least one security certificate which had expired, been revoked or distrusted.

Case Study

Type
An accountant is a target of email fraud after a client is hacked.

Scenario
An accountancy firm had a mid-sized manufacturing company as a client. The client's system had a data breach and was hacked.

Sting
The fraudsters sent emails to the accountants, purportedly from the client, asking them to transfer funds and make payments on their behalf. The accountant complied with the requests, as this was their usual practice previously agreed with the client.

Investigation
The accountant became suspicious of a request for a larger than usual amount, contacted the client and the fraud was brought to light.

Conclusion
The client held the accountant responsible even though it was the client's system that had been breached. Had the accountant and client had correct procedures in place for transferring money and security measures implemented this could have been avoided.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch
broker@kynd.io
www.kynd.io

References:
https://www.swizznet.com/blog/top-accounting-security-threats, 2021, SWIZZNET
https://www.ncsc.co.uk/post/why-an-accountancy-firms-targets-for-cyber-attacks, 2021, The Cyber Resilience Centre for the South East
https://www.saycyber.com/blog/cyberattacks-on-the-rise-for-accountancy-firms, 2022, Say Cyber
https://blog.axisgroup.insure/impact-of-cybersecurity-breaches-and-data-hacks-on-accountants, 2022, Axis Insurance