BCYBER

Advisers Association

Protecting your clients' trust

Karen Stephens | BCyber

The topic of trust is a complex one, especially when you are talking about a financial advice business. Your clients entrust you with their financial health and expect you to protect their data and use it responsibly - it's all about trust, because without it our businesses cannot survive.

However, as we have seen in recent years, this trust can be easily broken. A cyber incident or data breach can expose your clients personal financial details to the public, leading to fraud or a loss of trust in your business. And these breaches are not necessarily the result of "proactive" external intervention. Data errors can also lead to loss of trust (e.g., accidently sending an email to the wrong person), and a loss of client confidence in your ability to handle their finances safely.

According to a KPMG Small Business Reputation & The Cyber Risk Report, financial services businesses are most likely to lose clients due to a cyber breach, with nearly two in five businesses surveyed seeing clients leave after a breach.

Can your business afford to to be one of the unlucky ones?

Protecting your client trust needs to be made a priority - but where to start can seem beyond the reach of the ordinary financial advice business. Let's take the first steps of your your cyber resilience journey together - I promise they won't break the bank:

1. **Identify where the cybercriminal can get in (aka "vulnerabilities"):** Reviewing business cyber risk is a must. Once you have identified your vulnerabilities and gaps you can make incremental and affordable changes suited to your workload and budget.

Hint: *If you're stuck, check out BCyber's complementary health check, it provides a quick quick snapshot referencing two respected frameworks - NIST and the Essential 8 framework.*

BCYBER

Advisers Association

2. Have an asset register: We are talking about a cyber asset register, not an investment one - by understanding what devices and software you are using (and even not using but still have "sitting around") you get a snapshot of everything in your business that interacts with the internet and has the potential to be a doorway into your business.

Hint: Include everything than interacts with the internet - go beyond the PC, Laptop and tablet etc- include printers/photocopiers, phones, automatic fish feeders… the lot and the better ones include virtual assets e.g., software licenses (I wasn't joking about the fish feeding app - Criminals Hacked A Fish Tank To Steal Data From A Casino). One final thought on this matter. Please do not save (and backup) your asset register in the same location as everything else - imagine how much fun a cybercriminal could have if they found your list!

3. **Your best first line of defence are your people:** And by people I mean your staff and your clients.

Cyber threats are evolving and changing, and many believe that it's an issue only technology can solve. Stopping the cybercriminal before they start work in your business is the cheapest and most effective form of defence and it comes down to cyber risk awareness. Education of your staff and clients is key as you are only as strong as your weakest link so bringing everyone on the cyber safety journey makes real business sense.

Hint: Go beyond the "tick-the-box cyber training" - embed cyber risk into your business DNA - by taking a multifaceted approach e.g. All staff (mailroom to boardroom) need to take part in the training and regular team cybersecurity discussions. Add it as a standing item to your regular team meetings and discuss what's working, what needs to be improved, new ideas people may have and what is happening in and/or to your competitors (i.e. learn from their mistakes - don't repeat them). Once cybersecurity becomes top of mind, you are well on your way to having a strong cyberculture. Consider adding

BCYBER

Advisers Association

cybersecurity to your client onboarding process, annual reviews or even your newsletters and email communications - it may just help you stand out from your competitors.

It's no longer a matter of "if" your business will be breached, but "when" and according to the The Advisers Association CEO, Neil Macdonald "the advent of Covid has seen our clients become more cyber aware so it makes sense to make your business cyber secure. It's a journey that we all need to be on". Each improvement is one step on the journey, so let's get started — you have no time to lose.

Need more cyber risk mitigation assistance from people who understand the advice business, then visit the BCyber website or drop us a line at support@bcyber.com.au.

BCyber. BCyber Safe.

BCYBER

Advisers Association