WORKING IN PARTNERSHIP WITH Paradigm CONSULTING

MITIGO CYBERSECURITY

MITIGO CYBER DOCTOR

DANGEROUS CYBERSECURITY MISCONCEPTIONS

IFA firms are under cyberattack and many are suffering serious consequences as a result of dangerous misconceptions about cybersecurity. In the following Q&As, we reveal the real underlying reasons why so many IFA firms are suffering from cybersecurity incidents.

Q. As a small IFA firm, will we really be a target for cybercriminals? Why would they attack us?

A: This is the entry level misconception - thinking that a cyber attack and a cyber breach won't happen to you. Well it can, and if proper defences are not in place, it will. Because every IFA firm is a target.

Cybercrime is most definitely not young lads in hoodies trying to hack you for fun. It's properly organised crime run by organised criminal gangs (many in E Europe), often working in syndicates, using sophisticated automated techniques, including artificial intelligence.

So while your firm might not have been singled out initially, once a gap is found, once they get in, we are increasingly finding they are willing to be patient, watching email exchanges, waiting for the right transaction to divert, or running some ransomware to disrupt your operations.

Q. We have an IT company that look after our computers and systems. Am I right to assume they are covering cybersecurity?

A: This is probably the most dangerous misconception of all - thinking that your IT support, whether in house or external, is properly looking after your cybersecurity.

Because in almost every case, you would be wrong.They are not. Aside from the fact that having them mark their own homework is not good risk management, cybersecurity is different from generalist IT support. It's a different discipline. You would not want your GP to carry out your heart surgery.

So don't expect your IT guys to know the latest attack methods; to specialise in defensive configuration; to do penetration testing and vulnerability assessments; to know your legal and regulatory obligations; to undertake and document your legally required risk assessment; to train and test your staff; to advise on risk governance and then draft your staff cybersecurity handbook; to implement a risk management framework; or to know your record keeping obligations. I could go on.

Q. We are a wealth management firm and we do an annual penetration test. Is this enough to protect us?

A: No, it is nowhere near enough. Putting to one side the fact that we find many firms paying over the odds for it, it usually only looks at one part of the technology within a defined scope, and usually only tells you whether the pen tester has been able to break in.

Crucially, it is not assessing, or addressing, your real business risks. A proper vulnerability assessment needs to be broader than that, and investigate things such as access controls; remote working arrangements; mobile phone security; the transfer of data; the configuration of backups; and so much more.

Plus, usually the pen testing only leaves you with a technical report, but does not prioritise (within the context of your business) the remedial actions or help you with them. And of course pen testing only looks at some part of the technology. It does not help with training or governance.

FOR AN INDEPENDENT, NO STRINGS CONSULTATION CALL:
CALL 0161 8833 626 OR EMAIL: PARADIGM@MITIGOGROUP.COM

Q. Q. We already have Cyber Essentials. Does that mean we have adequate protection in place?

A: I am afraid not. CE is a desktop assessment of the answers you give in respect of 5 very basic technical aspects. It does not even provide minimum legal compliance for personal data which requires you to do training, put in place policies/procedures and more. Relying solely on CE is asking for a breach.

Q. We use cloud systems and we store our data in the cloud. Surely that protects us?

A: No, it does not. Putting to one side the fact we frequently see a complete absence of any kind of due diligence on cloud providers, even if the cloud "safe" you are using is secure, there is a whole host of policy, set up, configuration and enforcement aspects to get right.

This includes access controls, the way data is allowed to be moved in and out of the business, the collaboration arrangements with colleagues and third parties, and lots more. We often find that firms who are using the cloud have merely increased their attack surface, making them less, not more, secure.

Q. We subscribe to a compliance training package, which includes some general cybersecurity in it. Is that enough?

A: No. They are usually ineffective because they do not change behaviour. We often find many do not deal with the type of attacks which are happening in real life; they are not testing whether staff have understood and learnt from them; and they are not simulating the attacks (such as phishing attacks) which are happening in real life.

Why is this so important? Because over half of incidents start with people doing the wrong thing, trusting the authenticity of emails or websites without checking, clicking on something they should not, not understanding the consequences of putting too much information on social media.

Q. We have previously had a cyber "health check" done by a company who said we were in good nick. How long should we rely on that?

A: Cybersecurity is now a crucial part of ongoing risk management. It is not a one off spot check. Methods of attack change (as may your technology and the way you work) and defences need to evolve to keep you protected.

It's an ongoing process that requires periodic reviews, and arrangements for assessing that your defensive configurations, policies and controls you have in place continue to be right to protect your firm and checks to prove they are actually working. That's also now a legal requirement.

Your clients remain as clients because they trust you and they like you. If you have an incident which means they can no longer trust you, then they had better really, really like you. Because otherwise they will be gone. Simple as that.

Paradigm has partnered with Mitigo to provide trusted cybersecurity services to its members, covering technology testing, people training and governance, and ensuring legal and regulatory compliance.