TOP 10 TIPS FOR
securing your business against cyber attack

Cyber attack - It's something that you hope will never happen in your business, yet is increasingly happening to businesses around the world, with the financial sector being a primary target of malicious intent.

Research by Intelliflo shows that 44% of people in advice businesses have direct experience of cyber attack. 82% of consumers said that they would seek to change or avoid in the first place, an advice business that had been hacked*.

The spreading of WannaCry 2, a form of ransomware that struck in 99 countries globally and affected companies as wide ranging as Telefonica and the NHS, is a prime example of how cyber attacks can strike from nowhere.

What can financial advice businesses do to prevent, identify and deal with attacks?

44% of advisers have direct experience of cyber attack. 82% of consumers would look to change their adviser if they were hacked. This is a major challenge for advice firms.

1. Identify your weaknesses

The primary gateway to your business is the people you work with. It only takes one person to open a malicious email and malware could be uploaded to your system – this means staff training on cyber security is vital. How can you tell the difference between genuine and malicious emails? Training is widely available and should be conducted at least every other year to keep your staff up to date with current trends.

2. Keep your system up to date

The other weakness is your system itself. How up to date is it? The WannaCry 2 malware spread like wildfire through unsupported Windows XP operating systems. Hackers identify security weaknesses in systems and exploit them. It is imperative to deploy the latest patches and updates on your system. 10% of Intelliflo clients are functioning using unsupported operating systems and browsers. It may seem onerous to constantly update your system, but an attack would be much worse. Prevention is better than the cure.

3. Use strong password protection on everything

User authentication is the simplest form of security and one that almost everybody uses every day in the form of passwords. Surprisingly, however, many people do not password protect all of their devices, which leaves them open to being accessed by unwanted third parties at the click of a button. Pass phrases with uppercase, number and special characters are the most secure. For example, using the first line of a song like the Elvis classic, Suspicious Minds, could appear as Imc@ught1n@tr@p.

4. Two-factor authentication

On top of basic encryption, you should seek to add two-factor authentication to your login processes. This has been deployed by banks for years now, where you enter your login credentials, then have to generate a code using an external dongle or text message to further verify your identity. It is an added layer of easily implemented security to your system.

5. Back up your data

Having a reliable backup of your operating data is crucial to business continuity in case of attack. If your primary data becomes infected and unusable, what are you going to do? Switching to backup data at least gives you a platform to rebuild on. So back your data up regularly – if you last backed up three hours before an attack, the loss to your business will be those three hours, which is much better than losing everything.

6. Moving to the cloud

Safe storage and backups can be easily achieved by deploying the services of the best cloud provider for your business needs. Providers such as Amazon Web Services, trusted by the CIA in the US and Microsoft, which spends $1bn annually on its security operations, are increasingly being trusted by banks and large financial corporations. The agility afforded by cloud storage is one reason, but the sheer scale of the security operation is another.

Most cloud providers also run multi-encryption of your data, so it is not all stored under the same credentials. This means that, in the event of a breach, not all of your data will be affected at once.

Cloud storage also leverages the spending of your chosen provider and the investment of other firms utilising the service. With multiple users of a service, breaches in cloud services make it much less likely that your data can be singled out for attack.

7. Net spend

Microsoft is able to invest $1bn annually in security – it is unlikely you can match that sort of spending, so why not leverage it to protect your business? As a provider of cloud-based software to its clients, Intelliflo spends over 10% of its annual turnover on cyber security measures.

8. Due diligence

Conduct thorough due diligence on partners and providers. As the FCA makes absolutely crystal clear in its guidance on cyber security and data breaches, the ultimate responsibility is always yours and cannot be delegated.

Find out how your data will be stored and whether it's compatible with your business model. What security does the provider offer? What is the pricing model? Does the provider comply with rules and regulations that you need to comply with? Can it scale up to meet your business needs? What are the disaster recovery protocols? Should misfortune befall the provider, what exactly does that mean to you?

9. Plan for when, not if

Always plan for the worst. What will you do if you are hacked? Who will take responsibility for what? How will you liaise with clients and the regulator? How will you get back up and running? Having a plan, designated personnel, proper insurance and backed up data in place will make the whole process a lot smoother. Making it up when you've already been hacked will potentially result in greater losses to your business.

10. Testing

Finally, the only way to stay on top of your planning and procedures is by testing them rigorously. It is important to stay on top of the threats to your system.

Regular testing will help to identify weaknesses in your security and can be conducted in-house or by external agencies such as NCC Group, who are experts in the field of cyber security. This will provide invaluable information which will help you to prevent breaches and also ensure that you are in the best position to handle any 'worst case' scenarios.

If you would like more information on the threats posed to your data security and how to identify and deal with them, Intelliflo has partnered with NCC Group to produce a joint white paper entitled 'Mitigating cyber risk in the financial services sector'

Download our white paper here.

*220 Intelliflo clients and 500 consumers, surveys conducted in Spring 2017

If you have any questions, please feel free to call us on **0330 102 8402** or email **info@intelliflo.com**

Intelliflo