# AMI Factsheet: Cyber security

## Introduction

This factsheet has been prepared by the Association of Mortgage Intermediaries as an introductory briefing to cyber security.

The frequency and magnitude of recent cyber attacks highlight the need for firms to review their cyber security infrastructure, as all sectors and types of businesses are at risk. This is particularly relevant considering the implementation of the General Data Protection Regulation (GDPR) from 25 May 2018, which requires firms to understand how they hold and process their data, with significant fines for any breaches. Failure to notify a minor breach when required to do so will result in a fine up to €10 million or 2% of total global annual turnover (whichever is higher), and failure to notify a major breach will result in a fine up to €20 million or 4% of total global annual turnover (whichever is higher). The FCA already requires firms to report material cyber incidents under Principle 11.

The FCA also announced in its 2017/18 business plan that it will focus on technological change across all sectors this year, with particular concerns around operational resilience and cyber risk. The FCA will work with the Bank of England and Treasury to engage with firms when outages or cyber attacks occur, particularly where there is a significant consumer or market impact. The FCA has created a dedicated cyber specialists team to oversee the way that firms manage cyber risk, and it plans to undertake a significant amount of work over the course of the year including coordinating with firms so they can learn lessons from both successful and unsuccessful cyber attacks.

## Cyber risks

With a sixth of the UK economy online, risk management needs to be understood in a digital context. For some firms this may mean needing a new model of who carries out these functions and how. Threats to cyber security include:

- Email threats, malware and bots. This includes phishing, where an individual receives an email purporting to be from a known account asking them to log in using a link provided in the email. All users are susceptible to phishing but a common type of attack targets executive users within businesses (known as whaling).
- Mobile vulnerabilities – default credentials on devices and unprotected wifi networks are exposed to 'man in the middle' attacks, where network traffic is secretly intercepted by a third party.
- Web attacks – this includes DDoS attacks (where websites are bombarded with requests with the intent to overload and disable the web server) and where sensitive data, including login credentials and personal information, is obtained when transmitted insecurely over the internet.

- Ransomware – some attacks rely on phishing but also from exploiting vulnerabilities in computers which are not up to date. These can hold all data stored on a computer to ransom with no guarantee of retrieval (firms without separate back up systems will be highly impacted).

- Breaches – personal data can be obtained by using the methods above, published illegally and used for fraud. This is easier for fraudsters where data is not stored securely, systems are configured incorrectly or data is transmitted unencrypted.

As attacks are designed to exploit human behaviour, all individuals are targets. Therefore mitigating cyber risks needs to be done **at all levels in a firm with sufficient staff education**. All of these risks apply to any third party providers, for which firms will be responsible.

Cyber security is not just an issue within businesses as it affects consumers as well. Despite the publicised attacks experienced by banks, intermediaries are also a target. For example one adviser had their email account compromised with fraudsters requesting a customer to transfer additional funds to their "lender", which was a fraudulent account. This has also happened with solicitors and greater awareness needs to be raised with customers.

## Solutions

The following controls are effective and affordable ways to reduce exposure to the more common types of cyber attack on systems that are exposed to the internet:

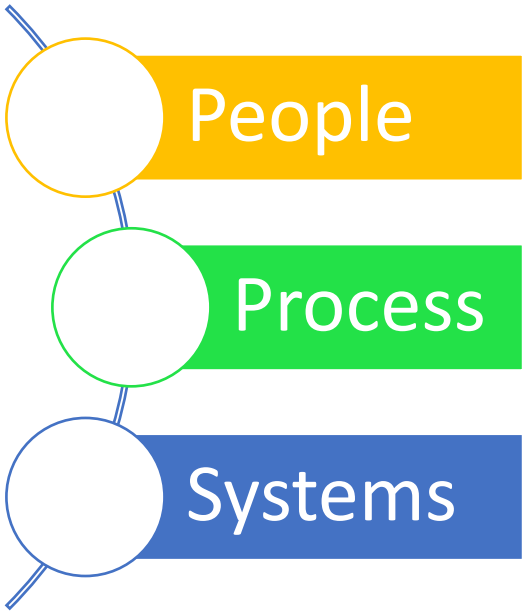
- Boundary firewalls and internet gateways (e.g. web filtering and blocking access to certain websites and services which can increase the risk of exposure)
- Malware protection (i.e. up to date and effective anti virus software and inbound email scanning)
- Patch management (i.e. regular software updates)
- Whitelisting and execution control (i.e. prevent unknown software from being able to run or install itself, including the AutoRun option when USB drives are connected)
- Secure configuration (i.e. restricting the functionality of every device, operating system and application to the minimum needed for businesses to function)
- An effective password policy (see 'Useful support material' on page 3)
- User access control (including limiting user accounts to only have privileges essential to perform their functions)

Getting these basics right is important for firms of all sizes, and firms will need to take a risk management approach to understand the specific operational and strategic risks to their business. This includes reviewing whether and how legacy systems could be improved to help the business function better and more securely, or whether to move any processes to a cloud-based solution, as these are designed with security at their core.

Individuals can check whether their details have been included in any of the data leaks using the website haveibeenpwned. One significant data leak has been from LinkedIn, so if an individual's email address (and therefore password) was included in this leak, they should be warned to change their password not just for LinkedIn but for other websites, which could include a work email account. Users can sign up to ensure they are notified if their details are included in any future leaks (which occur on a regular basis).

## Summary

The best approach to cyber security can therefore be described by addressing three areas: people, process and systems. Examples of measures which firms can adopt include:




- Ensuring an understanding at Board level of cyber risk and regular reviews.

- Regular training of staff which sets out the signs of criminal activity and encouraging them to report it (and is more effective if there is an easy way to do so).

- Engaging with staff on security processes, such as setting strong passwords and changing these regularly, to minimise the risk of individuals seeing these as burdens.

- Similar engagement with customers such as warnings.

- Regularly reviewing processes and systems of third party providers and requiring them to demonstrate compliance under GDPR.

When implementing a cyber security strategy, firms should map the steps that need to be taken and responsibilities if an attack or breach occurs, which includes how this is communicated to staff, data subjects and the press. This should fit within a firm's **overall disaster recovery plan**.

## Useful support material

The National Cyber Security Centre publishes regular guidance for businesses, including:

- 10 steps to cyber security: executive summary
- 10 steps: a Board level responsibility
- Common cyber attacks: reducing the impact
- Password security

There is a joint industry and government initiative, the Cyber Security Information Shared Partnership, which exchanges cyber threat information securely and confidentially. The aim is to increase awareness and reduce the impact on businesses. **Firms may wish to consider joining this initiative.**

Symantec, a provider of security products and solutions, has produced its 2017 Internet Security Threat Report which analyses the cyber landscape. It gives an insight to common attacks over the last year and recommendations on best practice.

The FCA webpage on cyber resilience features an infographic on good cyber security.