AMI Factsheet: Cyber risks and security

Introduction

This factsheet has been prepared by the Association of Mortgage Intermediaries to give an overview of cyber risks and provide suggestions on how to improve cyber security. With a shift to mass home working due to Covid-19, there has been an increase in the number of Covid-19 related cyber-attacks as firms and employees are outside of normal working environments and may be more susceptible and vulnerable to attacks. Firms have also been forced to shift their focus to survival and may be thinking less about cyber risks and security. However, it is important that data information security is kept as a business priority as cyber criminals are opportunistic and will use this time to exploit any weaknesses or lapses in judgment.

So, what is cyber-risk? Cyber risk commonly refers to any risk of financial loss, disruption or damage to the reputation of an organisation from the failure of its information technology systems. Often a more common area is cyber security risk where the exposure or loss is from a cyber-attack or data breach in an organisation.

The lure of data

Businesses need to consider data as a valuable business asset, especially as findings from the 2020 Department for Digital, Culture, Media and Sport Cyber Security Breaches Survey show that almost half (46%) of businesses report having cyber security breaches or attacks within the last 12 months, increasing to 68% among medium businesses and 75% among large businesses.

But what is important is the frequency, as, among this 46%, more are experiencing these issues at least once a week in 2020 (32% vs. 22% in 2017).

Mortgage intermediaries are a target for cyber criminals, due to the amount of personal data which they obtain and store, their use of cloud storage systems and the interconnectivity between their systems and those of third parties. This means that firms of all sizes cannot afford to become complacent and should never think “it won’t happen to me”.

Firms are reminded that under Principle 11 of the FCA’s Principles for Businesses they must report material cyber incidents to the FCA. For clarification on what may constitute a material cyber incident, please click here.

Back to basics

The introduction of General Data Protection Regulation (GDPR) in 2018 has been attributed to firms taking positive steps in managing their data. However, there is more that firms can do to minimise the threat of a cyber-attack. Whilst some may invest in technology to detect and monitor cyber threats, there are some more straightforward tips and techniques which should be considered.

Review and challenge existing password policies

Default passwords are often left unchanged making systems easy to hack. Password policies are also either too relaxed or too strict and some firms are not enforcing and monitoring their own procedures. Firms are encouraged to review their existing password policies to ensure they remain fit for purpose.

Accounts with elevated privileges require special attention from a security perspective, with minimum extra precautions such as Multi-Factor Authentication (where multiple means of identification are used) a sensible approach as this helps mitigate the risk of password guessing and theft.

Firms should adopt a zero-trust strategy that requires systems to prove their trustworthiness before they can communicate inside/outside of a network - this can take the form of whitelisting (the practice of explicitly allowing some identified entities access to a particular privilege, service, mobility, access or recognition).

Third parties and supply chain risk

The FCA's consultation paper on operational resilience discusses the importance of firms having a comprehensive understanding and mapping of the resources that support their business, which includes those outsourced and third-party services over which the firm may not have direct control.

Covid-19 has also highlighted the dependencies on other firms in our highly connected world so firms should consider reviewing the security capability and risk exposure of those in the supply chain. Some questions to consider asking third party suppliers include asking what international industry standards and certifications the supplier has, the scope of the certifications they hold, and whether they can share their latest audit reports[1].

Email compromise

The use of tools to block, quarantine and dispose of malicious emails and attachments both in the mailbox and at the perimeter is recommended. The application and testing of email kill switches that can remove an email from multiple recipients' mailboxes is also suggested.

If there is any doubt over the legitimacy of an email (especially due to the 'new norm' of working arrangements), then is the firm satisfied that its staff will know what to do i.e. should the sender of the email be telephoned to verify the source.

[1] https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups#lf-chapter-id-ccg-insights-third-parties-and-supply-chain-

Use of technology

Covid-19 has forced many firms to embrace new ways of working and many teams are using video chat software, such as Zoom. There has been some concern over the security of these applications and Zoom has updated their settings so that meetings now require passwords and waiting rooms have been turned on by default. They have also added an option in the meeting controls called 'Security' which gives access to security features. Firms should also set the screen sharing to 'host only' and disable file sharing. Firms should ensure that they have taken reasonable steps to review the suitability of the technology before introducing it into their daily routines, noting actions and evidence should it need to explain the steps undertaken.

Other considerations

Senior Manager's Regime

At the core of the Senior Manager's Regime is accountability and those with Senior Management Function (SMF) responsibilities need to be able to understand the threats and vulnerabilities that may affect a firm. When having discussions with technical departments, senior managers shouldn't be afraid to ask further questions if they have knowledge gaps or want clarification on a complex technical subject matter. If needed, they could look to obtain independent assurance or specialist advice.

Staff training

A 2019 survey by Centrify found that 77 per cent of UK workers admit that they have never received any form of cyber skills training from their employer[2]. Staff are important as a first line of defence and firms may wish to consider dedicated cyber security training to cover topics such as common cyber threats; how to spot suspicious behaviour; data breach notification procedures; the importance of software and antivirus updates; and the perils of using public WiFi when working remotely (during the Covid-19 crisis firms may wish to consider using a business Virtual Private Network).

An analysis of Information Commissioner's Office (ICO) data shows that in 2019 human error caused 90 per cent of cyber data breaches[3]. To try to prevent hackers from gaining access to a system, firms may wish to send regular phishing simulation emails to all members of staff (regardless of seniority) and review click through rates to understand any gaps within staff awareness and to identify further training needs. Employees may drop their guard during the current crisis, as emails sent from an employee's mobile phone may not necessarily seem out of the ordinary in the current working setup and criminals can easily set up a phishing attack online to take advantage of this.

[2] https://www.centrify.com/about-us/news/press-releases/2019/over-three-quarters-uk-workforce-lack-basic-cyber-training/
[3] https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/

Cyber insurance

Many firms may rely on an element of cyber cover which could be included under an existing commercial insurance policy, but this may not be comprehensive enough in the event of a cyber breach or attack and may not include added value services such as incident response and business continuity planning. The ABI[4] has said that businesses are increasingly buying specialised cyber insurance policies to supplement their existing insurance arrangements, particularly if they handle sensitive customer details, rely heavily on IT and online services to conduct their business and process payment card information. As mortgage intermediaries fall into one or more of these categories, it is worthwhile reviewing (with the help of a specialist, such as an insurance broker) whether there is a gap in cover.

Malware and ransomware

Malware (malicious software) and ransomware (a type of malware that prevents you from accessing your computer unless a ransom amount is paid) are threats that are becoming more common, as criminals move away from targeting consumers to carrying out organised attacks on businesses. The National Cyber Security Centre has created useful guidance on how to defend against these types of attacks.

Additional resources

Cyber essentials scheme

The National Cyber Security Centre (NCSC) has guidance and recommendations to improve cyber security as well as a self-assessment checklist, which is mainly aimed at small-medium firms. The scheme also enables organisations to gain one of two Cyber Essentials badges, which are suitable for firms of all sizes. These badges can help to reassure customers and suppliers that a firm takes cyber security seriously and allows a firm to assess whether they have the necessary procedures in place to be protected from a wide variety of cyber-attacks.

NCSC weekly threat reports

The NCSC publish weekly threat reports, with a useful filtering tool to help firms find information that is most relevant to them in terms of topic and the size of the business.

Exercise in a box

Aimed at small-medium firms, Exercise in a Box is a free online tool from the NCSC which helps firms test and practise their response to a cyber-attack by providing a number of scenarios based on common cyber threats.

[4] https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/

Useful websites

Cyber security advice for small-medium firms

SME cyber security toolkit

Cyber security toolkit for larger firms

Cloud security guidance

How to implement cloud security principles

FCA Cyber Insights (published March 2020)

FCA cyber resilience guidance (includes a cyber resilience self-assessment questionnaire)

NCSC Covid-19 homeworking guidance

NCSC Covid-19 cyber threat update