Cripps

How secure is your data?

Over the last year or so we have seen an increasing number of businesses fined for breaches of data privacy laws. This shows that the Information Commissioner's Office (ICO) is willing and able to focus its attentions on data privacy breaches committed by businesses other than large banks and multi-nationals.

Most recently, on 10 March the ICO imposed a £98,000 penalty on a law firm affected by a ransomware attack. The decision in this case has important implications for all businesses which rely on personal data which we explore in this update.

Could you be next?

Firstly, it's fair to say that it's impossible to completely protect electronic systems from external attack. For this reason, the ICO often declines to impose penalties where good practice has been applied and the data controller has promptly detected and resolved breaches, at least in cases where no large-scale loss of data or harm results. This latest decision provides a useful indication of the limits of the ICO's tolerance and highlights important steps that any business which uses personal data in core business functions should take to protect itself.

The ICO found that attackers had exploited an unpatched vulnerability on a server hosting the firm's archived files to gain access to almost a million archived files. These files were unencrypted, not protected by multi-factor authentication and the server was using an old, unsupported operating system.

In the opinion of the ICO the firm had failed to maintain adequate security measures to protect the server and, in addition, it had failed to properly apply its own file retention and data security policies. As a consequence of

these breaches a fine of £98,000 (calculated based on a starting point of 3.25% of turnover) was imposed on the firm despite the fact that the records accessed were historic archives, no harm other than "distress" was likely to have been caused, and the firm taking prompt and effective remedial action.

Key takeaways

As many businesses owners reading this may be thinking "There but for the grace of God go I" there are three key "takeaways" for businesses which use personal data:

1. Use multi-factor authentication applications and tools (MFA) and review your systems' technical security against best practice and industry standards.

The ICO emphasized the firm's four-month delay in applying a critical patch, failure to apply multi-factor authentication ("MFA") and use of an outdated system. It specifically compared the firm's practices to guidance and technical standards from the ISO, NIST and National Cyber Security Centre and sector-specific guidance for the Solicitors Regulation Authority.

If your business is attacked, you may need to justify your data security not only against what is "market", but against best practice and against codes of conduct, even if these are not binding on you. The ICO may expect you to be aware of "best practice" and to apply it if justified after balancing cost and risk. Key points for any business which uses personal data are:

- Use MFA, where practicable, for any remote login
- Ensure all systems, including archives, are patched up to date
- Ensure personal data is encrypted "at rest" – not only when sending copies externally
- Consider "cyber essentials" certification or higher standards if relevant to your business
- Best practice is the safest course – what are your competitors doing, what do regulators and industry bodies recommend, and what steps could you take without undue cost?

2. Review your internal policies and procedures – are they being followed?

The internal policies of the law firm mentioned above stated that its software and operating systems would be kept up to date and mandated a 7-year retention period for old files. The ICO was able to contrast these statements with the use of an unsupported operating system, four-month delay in applying critical patches and the fact that some files affected were more than 7 years old. In other words, the firm was not complying with its own policies.

We commonly see similar problems, especially in businesses which have relied on external consultants or copying third-party documents from the internet to simplify policy making. Directors and officers are often unaware of what is in their policies and IT teams may not be directed by management or resourced to apply them. Under the Data Protection Act 2018, businesses are required to document their compliance and be able to demonstrate it to the regulator – this case illustrates the problems which can result if policies (including ones the business may have paid to create) are treated as a one-time tick-box exercise and don't reflect actual practice.

3. Is your IT team properly resourced with the right external support?

If your business has a significant personal data component, consider whether you have invested sufficiently in technical staff and support to protect the confidentiality of that data. Here is a list of questions you may want to use as a call to action:

- Is our IT team properly staffed and resourced? Are there enough people on staff with the right knowledge for the work they do? Do they know and have input into our security policies and can they implement them with the resources available?
- Do we have the right external support? Regular penetration testing (if this is proportionate) and being aware of relevant industry standards and best practice are important.
- Do we train our staff regularly? Businesses are under a legal obligation to ensure staff have the necessary training – can we demonstrate that this is being done?
- Are we able to apply best practice and keep on top of it? Are we applying cost-effective security measures like encrypting personal data, strictly applying retention policies to delete old data and ensuring our systems use up-to-date software?

How we can help

If your core business involves working with personal data, our commercial team can help you to review your practices and procedures and minimize the reputational and financial risks from external attack. Contact our commercial team to see how we can help you.

Ian Lindley

Partner