Single-factor authentication: now a CISA 'bad practice'

Ali Vaziri, Legal Director with Lewis Silkin LLP, makes some forecasts about the effects of a US agency's recent categorisation regarding Single Factor Authentication

When it comes to knowing what 'good' information security is from the perspective of the Information Commissioner's Office ('ICO'), the regulator's fines against British Airways and Cathay Pacific were a clear indication that multi-factor authentication ('MFA') for remote access to systems was a desirable practice. In recently maligning single-factor authentication as technology 'bad practice' (especially by organisations supporting critical infrastructure), the US Cybersecurity and Infrastructure Security Agency ('CISA') has sent a clear signal that MFA is now not only desirable, but a baseline security measure which should be prioritised. This will no doubt be picked up by regulators on this side of the Atlantic.

For readers who aren't clear on the distinctions, single-factor authentication ('SFA') only requires one 'factor' to gain access to a system — commonly something you know (e.g. a password). MFA, on the other hand, requires two or more different factors — so not just something you know, but also something you have (e.g. a code sent to your smartphone such as a one time password/SMS, or using a card in your possession) or something you are (e.g. a biometric such as your fingerprint or voice).

Having a second 'factor' of authentication is more secure because passwords can easily be guessed by attackers where they are weak or have previously been compromised and then re-used. Since they are data, passwords can also be stolen by attackers without being physically present. One study by Google and two US universities illustrated how effective use of a second factor can be. It found that using MFA blocked 100% of automated bots, 99% of bulk phishing attacks and 66% of targeted attacks on users' Google accounts.

No surprise then that, following a spate of attacks this summer in key industries such as energy (Colonial Pipeline) and meat (JBS), CISA — the federal agency formed in 2018 and tasked with improving cybersecurity across US government — launched its 'bad practices' project. The project aims at cataloguing 'bad practices that are exceptionally risky, especially in organisations supporting Critical Infrastructure or [National Critical Functions].'

When launched in June, there were two bad practices identified: the use of unsupported (or end-of-life) software; and the use of known/fixed/default passwords and credentials. In late August, the CISA added a third bad practice: the use of SFA for remote or administrative access to systems. More practices, such as use of weak cryptographic functions or key sizes, are in the pipeline.

In adding the use of SFA, the CISA observed that: "This dangerous practice is especially egregious in technologies accessible from the internet." In a world where many of us have been working remotely since the beginning of the pandemic and will likely continue to do so to some extent even as we return to offices, this observation will have particular resonance.

You may be thinking: "who cares? We're not in the US; nor are we critical infrastructure".

As stated above, there is likely to be a trickle-down effect from the CISA's categorisation. Suppliers to the US government will be expected to up their game which, in turn, will lead to a more widespread adoption, or more accurately a drop in the use of SFA. This in turn will influence the consensus of professional opinion in the field of cybersecurity more generally. It is that consensus which informs what 'appropriate' security means under the GDPR. So the CISA's labelling signals the direction of travel, and will likely play a role in influencing the regulators' thinking (and fines) in a similar way that guidance has from other US organisations regularly cited in UK monetary penalty notices, such as the Open Web Application Security Project and the National Institute of Standards and Technology.

Although you might not be critical infrastructure, if your organisation is supporting that infrastructure, there is likely to be an increased risk and, therefore, expectation in relation to the use of MFA. For those whose services are critical, as the 'competent authority' for 'relevant digital service providers' under the Network and

(Continued on page 16)

(Continued from page 15)

Information Systems Regulations 2018, the ICO could well refer to CISA bad practices when flexing its enforcement powers (and the same applies to 'operators of essential services' which, although subject to a different competent authority, are nonetheless also controllers subject the UK GDPR).

The focus in the extensive body of security guidance available is often on promoting best practices rather than avoiding bad practices. Although invaluable, the breadth of recommendations can be daunting.

Whilst this change in perspective by the CISA is not a substitute for implementing best practices, highlighting bad practices does at least help with prioritisation efforts, especially where there are limited resources available to identify and mitigate risk. This something which will surely appeal to all organisations, irrespective of the sector they operate in, or where they are located.

Finally, MFA is not infallible. It can be bypassed, as evidenced (for example) by the recent rise in OTP (one time password) attacks, with unsophisticated fraudsters using readily deployable social engineering bots like 'BloodOTP' to capture the second 'factor' of authentication. Keeping up with the crooks is a constant effort — even where an organisation's practices are not 'bad'!

Ali Vaziri
Lewis Silkin LLP
Ali.Vaziri@lewissilkin.com