THERE ARE
NO SHORTCUTS
TO SECURING
YOUR BUSINESS

FOLLOWING FIRTH
AUGUST 2023

For years, we have been hearing about the increasing need for cyber security, but the number of attacks seems to be growing exponentially alongside increased investment into security solutions. In the first half of last year alone, 2.8 billion malware attacks happened. There were also 255 million phishing attacks over six months in 2022. Reports indicate that around 71% of businesses became victims of ransomware last year, with $1.4 billion lost to breaches on cross-chain bridges.

As part of their security measures, many companies are employing increasingly stringent login procedures, leading to growing numbers of long, complicated passwords. As a result, they are faced with a whole set of new problems: Either staff find their passwords so hard to remember that they leave them written down somewhere – making them easy for hackers to find – or they use third-party solutions to help manage their passwords, adding yet another layer that needs to be secured.

Unfortunately, everything on the internet can be hacked, and that includes password managers. Late last year, hackers stole encrypted copies of LastPass customer passwords and other sensitive data such as billing addresses, phone numbers and IP addresses. This is by no means the only time a password manager has been compromised, with Passwordstate, Dashlane, Keeper, 1Password, and RoboForm all having been found to have security vulnerabilities over the past few years. The latest incident was announced in January, with Norton LifeLock users being warned that their accounts had been compromised.

Inherent vulnerabilities

The LastPass hack provides a perfect example of the danger inherent in using a password manager. According to the company, source code and technical information were stolen as part of the hack, which were then used to target another employee. As a result, the hackers were able to obtain credentials and keys to access and decrypt data stored on a third-party cloud storage space.

The hackers not only gained access to basic customer account information, including e-mail addresses and the IP addresses from which customers accessed LastPass, and "fully encrypted sensitive fields such as website usernames and passwords, secure notes and form-filled data", they got what they needed for future targeted attacks through social engineering and phishing attempts. Considering that 45.5% of companies experienced between one and five successful cyber attacks last year, and that 77% of companies are woefully ill-prepared when it comes to thwarting an attack or a data breach according to Ponemon Institute statistics, incidents like the LastPass hack should be even more concerning.

In fact, password managers have one inherent vulnerability: companies are effectively putting all their eggs in one basket. From credit card details, to login credentials, to secure notes, password management tools contain a plethora of valuable information, so one breach could result in a knock-on effect that would be felt for months after.

Strategic security

With most companies now employing remote and hybrid work strategies, cyber security and user authentication have become even more vital. However, there are no shortcuts to securing an organisation, so password managers should be included in a much wider and broader security strategy.

First and foremost, businesses need to know what they're up against. Passwords are a vital primary security control, but social engineering attacks, for example, can negate any confidence passwords can provide. Conversely, simply knowing about the threats out there won't protect the organisation, nor will taking a shotgun approach to cyber security.

Companies must identify their most valuable digital assets and determine where their current cybersecurity measures need to be improved. Strong passwords should be matched with robust security policies that allow for a variety of security tools, including multi-factor authentication (MFA). Most importantly, a business should be aware of where its data sits at all times so it can ensure the security of its entire supply chain through stringent management of authentication protocols.

RICHARD FIRTH
CHAIRMAN & CEO, MIP HOLDINGS