"It's clear that LastPass has been developed by people who understand the problem they're trying to solve."

Steve Jackson
Head of Information Systems, Tessella

Passwords: Eliminating the weakest link

Data breaches can be catastrophic for both an organisation and its customers. For a business, it means a loss of trust from its customers, as well as damage to revenue, and if the organisation is subject to regulation, there could be financial and regulatory penalties as well.

For customers, there is a fear about what will happen to their lost data, as well as a distrust of the business practices and level of compliance for the company that lost the data. According to the Australian Community Attitude to Privacy Survey (ACAPS),[1] conducted by the Office of the Australian Information Commissioner (OAIC), 58 per cent of consumers said they would not deal with a business due to privacy or security concerns associated with data loss, while a further 79 per cent said they did not want their data shared with third-party organisations.

The ACAPS survey is timely because Australia will shortly introduce its first data breach notification laws, bringing it into line with jurisdictions that already have such laws or are implementing them, including the United States and the European Union.

Like the ACAPS survey, the Notifiable Data Breaches scheme is overseen by the Office of the Australian Information Commissioner. The new laws, which come into effect on February 22, 2018, apply to any organisation that is already subject to the Australian Privacy Act (1988). In practice, this means any company or business that has a turnover in excess of $3 million must comply with the incoming legislation, which is officially known as the Privacy Amendment (Notifiable Data Breaches) Act 2017.

[1] https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017

What is the Notifiable Data Breaches Act?

Under the new law, any organisation suffering a data breach must notify the Office of the Australian Information Commissioner, as well as the general public, as soon as the breach is discovered.

The notice made to the OAIC, as well as the public, must include steps that individuals can take in response to the data breach.

According to the Act, a Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. The Act defines a data breach as occurring when any personal information held by an organisation is lost or subject to unauthorised access or disclosure.

Examples of data breaches provided by the OAIC include situations when:

- A device containing customers' personal information is lost or stolen
- A database containing personal information is hacked
- Personal information is mistakenly provided to the wrong person

An organisation must notify the OAIC and the public with information including: the identity and contact details of the affected organisation; a description of the data breach; the kinds of information concerned in the data breach; and recommendations about the steps individuals should take in response to the data breach.

There are some exceptions to the law. The Notifiable Data Breaches scheme only requires organisations to notify when there is a data breach that is likely to result in serious harm to any individual to whom the data breach relates. The exceptions primarily relate to situations when two or more entities hold the same information, in which case only one organisation needs to notify of the breach, and some cases where law enforcement is involved. There are also provisions relating to secrecy in regard to national security.

The recent breach of a contractor to the Australian Department of Defence is a prime example of what can happen when good security policies and procedures are not put in place. According to news reports[2], a third-party contractor lost around 30 gigabytes of sensitive, but not classified, material relating to Australia's current and forthcoming defence assets.

[2] http://www.skynews.com.au/news/top-stories/2017/10/12/defence-contractor-s-cyber-security-breached.html

At a Glance – The Notifiable Data Breaches Scheme

What is the Notifiable Data Breaches (NDB) scheme?

The NDB scheme requires any organisation covered by the Australian Privacy Act (1988) to notify any individuals likely to be at risk of serious harm by a data breach.

When does it come into force?

The NDB scheme will be applicable from February 22, 2018.

What are some examples of a data breach?

A data breach occurs when a device containing customers' personal information is lost or stolen; a database containing personal information is hacked; or personal information is mistakenly given to the wrong person. These are only examples, and there could be other forms of data breaches covered by the scheme.

What happens after a data breach?

An organisation that has suffered a data breach must notify the Office of the Australian Information Commissioner (OAIC) as well as affected members of the public. A notification must contain the identity and contact details of the organisation; a description of the data breach; the kinds of information concerned; and recommendations about what affected individuals should do.

The Australian Signals Directorate (ASD), which spoke about the breach at a security conference, said that the event came down to poor IT administration, including bad password management. It's not clear who was responsible for the hack, whether it was cyber criminals or state actors, but the upshot remains the same: good policy, good procedures and good password management are vital for maintaining business security.

The reality of cyber security is that the main weakness in any system is generally the human factor. The core issue of the human factor is that people are unable to remember lots of passwords, and will therefore resort to password re-use for convenience. There are three human actions involved in bad actors accessing systems: the stealing of identities; the appropriation of credentials, such as passwords; and vulnerabilities in the system, which may be introduced through human error. The stealing of identities can result in password theft, and vice versa. And while the appropriation of credentials creates potential new entry points into an organisation, identity theft is potentially devastating for the individual involved. System vulnerabilities could include unpatched operating systems or application software, configuration errors or weak administrative processes.

According to the 2017 Verizon Data Breach Investigation Report (DBIR), 81 per cent of breaches reported in the survey occurred as a result of passwords being stolen or guessed because they were weak.

The DBIR also found that social networks were one of the key sources of stolen or weak passwords. What this means is that people are using passwords on their social media accounts, which can be guessed or hacked, and then reusing those passwords for critical business applications. Another recent report found that 23 per cent of employees are using their personal social media credentials to sign into business applications.[3]

According to research conducted by LastPass[4], of the top 36 domains used by employees in the workplace, at least half are popular consumer solutions, such as Google, Facebook and others. Although web applications can be a source of innovation in the workplace, if they are poorly managed, these hidden password behaviours become a security threat.

[3] Ovum's 2017 report "Close the password security gap: convenience for employees and control for IT" published in collaboration with LastPass.
[4] https://www.lastpass.com/business/articles/importance-of-password-security-for-businesses

According to the DBIR, stolen and weak passwords are the number-one access point for introducing malware into a critical business system. When malware is introduced into a system, it can allow hackers access to sensitive business information (a data breach) or permit them control over the system, leading to further information breaches. This is known as privilege abuse, where hackers use ill-gotten passwords or credentials to then blend into the regular traffic that passes through a network.

Such password abuse is almost impossible to detect, at least for a period, because the person whose credentials have been stolen doesn't realise it has happened. This allows cyber criminals to have what is called 'dwell time,' where they have access to an account or system for a long period of time, using their access to start moving laterally or escalate their privileges, seizing sensitive data and remaining undetected.

There are many high-profile data breaches in the news headlines that underscore the need to use unique and secure passwords for each login we create. For example, the popular cloud application Dropbox lost 60 million account credentials through the reuse of a single password by one employee.[5]

The 2012 incident highlights the importance of educating employees about password hygiene, as well as the necessity of using a password manager. Other examples include the LinkedIn breach in 2012 and the Yahoo breach in 2013, both of which yielded a treasure trove of re-usable credentials. The list goes on, and if you want to check whether any of your passwords have been compromised, you can visit https://haveibeenpwned.com/.

The reality is that every single password is a potential entry point into an organisation that must be secured.

What can be done?

As passwords and human factors are often the weakest links in the cyber security chain, it pays to focus on those elements when strengthening an organisation's security posture. Research has found that employees are constantly logging in, with the average staff member having almost 200 sets of credentials that they need to use and remember. In addition, if passwords are only used a handful of times per month, it's harder for an employee to remember them, making it more likely they will reuse a password.

[5] https://techcrunch.com/2016/08/30dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/

That's why it makes sense to use a password manager, such as LastPass. LastPass allows you to set a master password as the key to all your other passwords, for any site or sign-on that you can think of. The solution uses strong encryption (AES-256 bit and PBKDF2 with SHA-256) to ensure a very high degree of security in the cloud.

LastPass uses local-only encryption, so that your data is encrypted and decrypted at the device level (your computer, smartphone or tablet). Data stored in the password vault is completely secure — even LastPass can't see it. The master password and the keys used to encrypt and decrypt data are never sent to LastPass' servers.

Opting-in for two-factor authentication (2FA) is recommended to add an extra layer of security and defence to your password vault. It involves providing another form of verification along with your master password, such as entering a one-off SMS combination number or scanning your fingerprint on your smartphone. 2FA can also be used by businesses to secure systems access, effectively blocking the use of external authentication systems.

More than just a password vault

LastPass isn't just a password vault. LastPass Enterprise gives organisations valuable insight into employee activity, such as the apps and devices they use. The admin function allows employee access to passwords and specific applications to be turned on and off, or employee accounts to be deactivated, in the event that roles and privileges change, or staff leave the company. LastPass can also generate strong, unique passwords for users.

Implementing change

With humans at the centre of cyber security, any organisation that wants to increase the strength and security of its password use needs to engage in a change management process. This ensures that all staff are on board with the company changes to password management, as well as the processes that go along with it.

Change management is a discipline unto itself, but there are several simple steps that you can follow to ensure that the change you want to see in the behaviour of your staff and your organisation happens quickly and effectively.

At a Glance – LastPass Enterprise

- LastPass Enterprise allows users to set a master password that controls an encrypted vault containing all of their app and website passwords.
- LastPass Enterprise permits organisations to have insight into employee app, website and device use via its password manager.
- LastPass Enterprise enables organisations to disable access to employee passwords (for example, when a staff member changes jobs or leaves the organisation).

Here are eight steps that you can follow to ensure that change happens in your organisation:

1. **Conduct a readiness assessment.** This includes organisational and cultural assessments, employee assessments and change assessments. These should be led by a nominated person, IT tiger team or change management team. You also need to assess the scope of the change, including how big it is (changing password behaviour is tough) and how many people are affected (likely everyone).

2. **Communication and communication planning.** It's easy to assume that communicating a change in behaviour once is enough. It's not. Change needs to be communicated and reiterated several times before it will take hold and become effective.

3. **Sponsorship from the top.** Upper management needs to communicate that it is on board with the change happening, and that they expect it to flow through the organisation.

4. **Manager training.** Managers have great influence over employees' motivation to change the way they do things. Managers need to be equipped to handle the change process, and to coach their staff through the change that is occurring.

5. **Develop and deliver the change.** In essence, staff need to be trained in the new ways of doing things. In this case, it's using a password manager and coming up with a strong master password to control access to their encrypted vault.

6. **Dealing with resistance to change.** Humans like to do things the way they have always done it. A program needs to be initiated to help people form new habits, and deal with those that fall back into their previous methods of password management.

7. **Feedback.** Implement a process loop, so the change management team can understand if there are any roadblocks to the new processes.

8. **Review the project.** Has it been a success? Has the change in the way people handle and use passwords been reflected in the entire organisation?

Conclusion

With the introduction of the Notifiable Data Breaches Act in February 2018, it's vitally important that every organisation does everything it can to ensure that it does not suffer a data breach, or other form of hacking. Businesses that suffer data breaches risk loss of revenue and damage to reputation. The law also lays down penalties for data breaches, although these are not mandatory, and are at the discretion of the Office of the Australian Information Commissioner.

The reality is that most breaches come down to human factors, and of those factors, weak and easily guessed passwords are the number-one reason that bad actors gain access to a system. That's why the use of a password manager, which is encrypted and only accessible to the user, is a foundational protection against data breaches.

Take the first step towards better security practices today. Contact LastPass so we can help you understand how to better protect your organisation's systems through secure password management.

About LastPass

LastPass is an award-winning password manager that helps millions around the world organise their online lives. LastPass provides secure password storage to make going online easier and safer, with convenient access from any internet-enabled device. LastPass Teams and LastPass Enterprise remove password obstacles in the workplace, so businesses of all sizes can manage employee access and mitigate the risk of data breaches. Founded in 2008, LastPass is headquartered in Fairfax, Virginia and is a product of LogMeIn (NASDAQ:LOGM). LastPass is a trademark of LogMeIn in the U.S. and other countries.

About LogMeIn, Inc.

LogMeIn, Inc. (NASDAQ:LOGM) simplifies how people connect with each other and the world around them to drive meaningful interactions, deepen relationships and create better outcomes for individuals and businesses. One of the world's top 10 public SaaS companies, and a market leader in communication & conferencing, identity & access and customer engagement & support solutions, LogMeIn has millions of customers spanning virtually every country across the globe. LogMeIn is headquartered in Boston with additional locations in North America, Europe, Asia and Australia.