TOSHIBA

2016 Australian SMB

Information Technology and Online Security Survey

In 2016, Toshiba Australia surveyed a wide range of businesses from their client base to gain insight into the IT environment of small to medium businesses (SMBs) in Australia.

47% of the businesses surveyed had less than 20 staff, 20% had 20 to 50 staff members and 33% had more than 50 employees.

Given the significant changes in the application of information technology (IT), this survey focused on security, performance, risk mitigation and proactive management.

TOGETHER INFORMATION

7

6% of businesses surveyed said that they did not have a plan to ensure business continuity in case of a disastrous event, and 25% were unsure.

A disaster recovery plan includes a detailed analysis of an organisation's position in event of disaster. This plan also includes guidelines and practices which define how an organisation should act during these critical situations, in order to reduce impact on the organisation.

For example, an organisation might protect all of their data with off-site backups, including regular testing, to ensure that in the event of fire or flood they are able to recover the data to other systems.

90% of businesses that lose data from a disaster are forced to shut within 2 years of disaster
London Chamber of Commerce

8

35% of businesses said that they liked the idea of out-sourcing routine IT support so they can focus on "the business".

Many SMBs turn to managed service providers to address the need for strong IT security and integrity. Outsourcing IT makes sense for SMBBs specifically, as they often lack the time and internal resources to manage it in-house.

There are a number of security benefits of outsourcing IT to managed service providers including:

- State-of-the-art security-based technology
- Proactive continous monitoring of infrastructure and security systems
- Strategic guidance and support, tailored to the needs of your business

THE CONCLUSION

The statistics gleaned from this survey reflect that a large number of Australian SMBs are not managing their IT to the optimal level and are putting their business at risk every day.

Toshiba Australia can provide a comprehensive review of your IT environment and expert advice on state-of-the-art technology that will provide the best protection for your business.

THE RESULTS

1

24% of businesses surveyed said that they felt their IT department was working at over 100% capacity and 41% said they were unsure.

When IT human resources are stretched there is a high chance that essential tasks related to protecting organisational data and infrastructure are missed. When managing IT internally, it is essential to ensure that businesses are sufficiently resourced to protect themselves from infrastructure failure, security threats and data loss.

2

Nearly 20% of businesses surveyed said that they were not confident that their IT backups were restorable.

IT security measures protect your computers and internet-based systems from unintended or unauthorised access, modifications, theft, and obliteration.

Security measures including strong passwords, firewalls, antivirus, network monitoring, encryption, data backup, disaster recovery and education are essential to ensure the highest level of data integrity.

These measures are critical to guarantee you are able to keep your data secure,ensure IT downtime does not affect the day to day running of your business and make certain that your business remains viable in the longterm.

3

A staggering 25% of businesses did not know what IT security measures they have in place.

Data backup is one of the most important areas of IT for any businesses. Having secure access to your data at all times is critical to the everyday operation of your business.

The most common causes of data loss are physical failure of a PC or server, computer viruses, accidental error, theft and disasters such as fire or flood. Without a regular, secure and reliable back up system, businesses face the prospect of a catastrophic loss of data that can cost businesses considerable time and expense. Every company's data is an investment; businesses should protect it and take steps to avoid losing it.

THE RESULTS

4

20% of businesses are unsure if they are compliant with national privacy guidelines.

Protecting your data is not just about ensuring your business remains a viable entity. There are also serious legal implications around protecting the personal information of your staff and clients.

The Privacy Act 1988 (Privacy Act) regulates how personal information is handled in Australia. The Australian Privacy Principles (APPs), which are contained in schedule 1 of the Privacy Act, outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called APP entities) must handle, use and manage personal information.
Office of the Australian Information
Commisioner

5

62% of businesses said that they were unsure if using an operational expenditure model to pay for external support would help them focus on "the business" while 9% of businesses felt sure it would.

The rapid advancement of technology means that IT infrastructure requirements are becoming less predictable. What once required dedicated floor space, skilled employees, an abundance of time and significant capital expenditure, can now be filled remotely by specialist companies that charge a fee for service. Organisations can now afford the most up-to-date technology without a substantial up-front investment, allowing them to focus on their core business. Transitioning capital expenses relating to IT over to operational expenditure, also allows businesses to redirect funds into investments and projects that drive revenue and growth.

6

35% of businesses said that they were currently being reactive to infrastructure and support issues rather than being proactive.

One of the major challenges in maintaining IT infrastructure is trying to predict what will fail and when. Proactive IT management provides continuous monitoring to detect issues before they become real problems. This guarantees that systems remain secure and that data is backed up effectively. It also ensures all devices operate effectively at all times.

Toshiba (Australia) Pty Ltd
Bldg C, 12-24 Talavera Rd
North Ryde, NSW 2113

Telephone
1300 794 202

www.toshiba-business.com.au

TOSHIBA

TOGETHER
INFORMATION

[This Class 1 laser product complies with IEC60825-1]. Technical data is subject to change without prior notice. All company and/or product names are trademarks and/or registered trademarks of their respective manufacturers in their markets and/or countries. All rights reserved. We are constantly making efforts to deliver the latest status of data to our partners. Specifications for some models may change in the time between the production and the release of this documentation. Productivity and paper specifications are related to paper size of A4 and a paper weight of 80 g/m2 if not otherwise mentioned.
Bradnam's Case Study