HP PPS Australia Pty Ltd
Level 5, Building F, Rhodes Corporate Park
1 Homebush Bay Drive
Rhodes NSW 2138
Australia

www.hp.com.au

Fact Sheet

HP Australia IT Security Study

Executive Summary

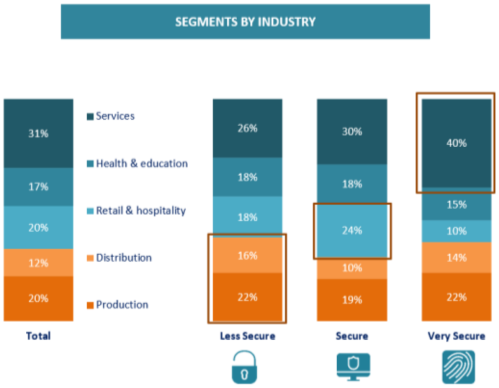
Overview

Key findings:

- Almost half of all Australian SMBs with an annual turnover of $3M+ do not consider themselves to be prepared for the mandatory data breach disclosure laws that will come into operation from February 2018
  - only 18% currently have a compliance policy in place; while 33% are currently developing a policy
- 57% of SMBs have not done any sort of IT security risk assessment in the last 12 months, putting their devices, data and documents at risk
- Of the 43% of SMBs that have undertaken a risk assessment, just 29% included printers in their analysis, a device that is increasingly an entry point for data breaches
- 63% of respondents state their employees work remotely on a regular basis, and as a result are becoming increasingly concerned about associated security risks – e.g. visual hacking
- 63% of respondents allow employees to access company data from personal devices;
  - less than half (44%) of respondents have a security policy in place for employees that bring a personal device to work
  - only 37% restrict the data that can be accessed from the device

How do SMBs differ on IT security?

Australian SMBs have a level of confidence in their IT security performance, with network security (75%), detecting and recovering against malware (66%) and end-user management (64%) the areas in which they are most confident. Conversely, almost half (44%) rate themselves lower on protecting company data from visual hacking.



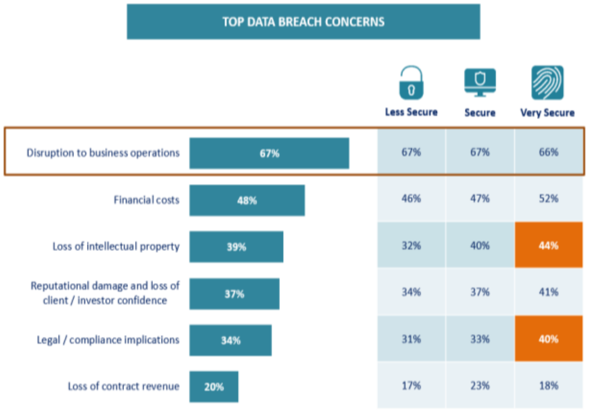
Based on these self-ratings of security performance, the research identified three segments within the Australian SMB community (22% Very Secure, 55% Secure, 24% Less Secure), with clear differences in terms of their level of preparedness, IT security preparations and policies. While the segments are evenly distributed by employee size and location, some industry skews do emerge, with two in five (40%) Very Secure businesses operating within the Services sector, and more than a third (38%) of Less Secure businesses in either Production or Distribution.

What is the overall level of preparedness for IT threats?

Australian SMBs recognise that there are gaps across all aspects of their IT security. As employees increasingly work remotely, and use their own devices in the workplace, SMBs also recognise the potential for breaches as a result of device loss (75% not at all / somewhat secure) and data theft (78% not at all / somewhat secure).

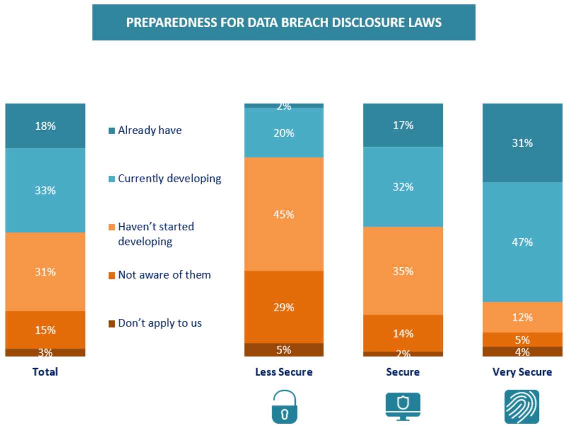
Within the segments, Less Secure SMBs mainly worry about staff behaviour when it (46% employee carelessness, 38% malicious behaviour by an employee), with Very Secure businesses considering the risks of connected & personal devices in the workplace (49% internet-connected devices, 32% personal devices in the workplace).

Disruption to business operations (67%) is the top consequence SMBs are concerned about facing in the case of a data breach (ahead of financial costs – 48%), although Very Secure SMBs are also looking beyond the immediate disruption of a breach, recognising the potential loss of IP (44%) and legal or compliance issues (40%) that they may face.



How are SMBs preparing for potential IT threats?

Almost two thirds of Australian SMBs cited the security of their customer (63% business critical) and business information (61% critical) as the most important considerations when it comes to IT security.



Despite this, less than half (47%) have conducted a risk assessment in the last 12 months. Among those who have undertaken one, they still primarily focus on 'traditional' hardware (server – 78%, desktop computers – 76%, network infrastructure – 71%, and laptops – 66%), ahead of smartphones (55%), and printers (29%).

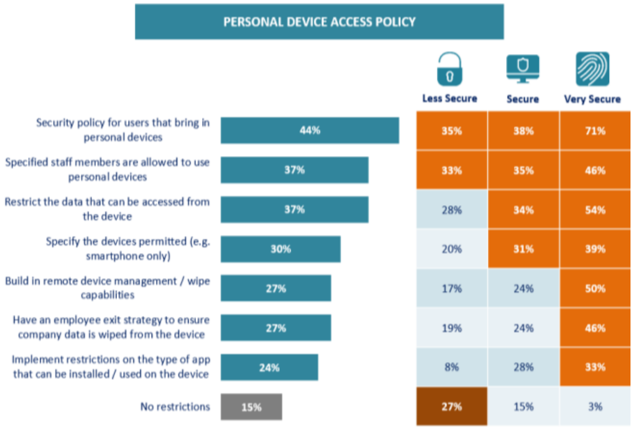
Reflecting on the mandatory data breach disclosure laws that will come into operation from February 2018, almost half of SMBs turning over $3m+ (49%) admitted that they were not yet prepared for the laws, with just 18% having compliance policies in place.

How do SMBs manage remote working & personal devices?

The challenge of managing corporate IT security is becoming increasingly complex, with two thirds of Australian SMBs (63%) reporting staff working remotely on a regular basis, and just one in ten (13%) not allowing any remote access.

Building on this, staff typically have significant freedom in how and where they access company data (work from home – 73%, work in public places – 53%), although Very Secure businesses are more likely to restrict working in public places (43% allowed), due to the risks of visual hacking and device loss or theft.

To mitigate risk, the majority of SMBs have personal device access policies in place (85%), with security policies for users that bring in personal devices (44%), specified staff members being allowed to use personal devices, and restrictions to the data that can be accessed from personal devices (both 37%) the most common.



Methodology:

This research was conducted by ACA Research on behalf of HP. The survey engaged 528 decision makers of Australian businesses with 10 – 99 employees. The research was conducted in November 2017, with quotas set on employee size and location to ensure a good mix of Australian SMBs. Participants were distributed across the services, production, retail and hospitality, health and education, and distribution sectors.

About HP

HP Inc. creates technology that makes life better for everyone, everywhere. Through our portfolio of printers, PCs, mobile devices, solutions, and services, we engineer experiences that amaze. More information about HP Inc. is available at http://www.hp.com.

Stephanie Aye, HP South Pacific
stephanie.aye@hp.com
+61 408 387 333
www.hp.com/go/newsroom

Gloria Lee
Edelman for HP
gloria.lee@edelman.com
+61 2 9291 3352