NSW
MAKING IT HAPPEN

Key Findings
Cyber Scare

A look at small to medium-sized business and the emergence of cybercrime in Australia

May 2017

NSW GOVERNMENT
Small Business Commissioner

The NSW Small Business Commissioner has conducted research to examine small to medium-sized business attitudes and views of cybercrime. This is so that we can better inform government, industry and other stakeholders of cyber security awareness amongst small to medium-sized business owners in NSW.

cybercrime

noun

dishonest or criminal activity online or by phone. Cybercrime can include deceptive conduct like malicious software or viruses, online or phone scams, theft of critical business information, fake overpayments, fake invoicing or hacking a business to obtain a customer's details or access to a supplier's network.[1]

Key findings

Small to medium-sized enterprises (SMEs) have a limited online presence

50% of SMEs limit their digital footprint to a business website with contact details and social media.

Only **20%** of businesses sell their products or services online.

> "What scared me most was when my email was redirected ... I was scared for my family and if their personal information had been compromised from the hack. I was also concerned for my clients' data and the confidential information that I held for them."
>
> Small business owner and cybercrime victim

Cybercrime is rated by SMEs as the 5th biggest risk to their business

SMEs are most concerned about fraudulent emails or phone calls, social media hacking, online banking fraud, crypto-ransomware and malware.

The cost of cybercrime to businesses in Australia is rising exponentially, costing Australians an estimated $1 billion each year.

Cybercrime costs businesses globally more than **$3 trillion** annually and it is anticipated that by 2021 this will exceed $6 trillion.[2]

1 Australian Government 2013, Cybercrime Act 2001, Schaper and Weber 2012. References: Schaper, M.T. and Weber, P. (2012) 'Understanding Small Business Scams', Journal of Enterprising Culture, 20(3) pp. 333-356.

2 Australian Government, 2017, Australia's Cyber Security Strategy – enabling innovation, growth and prosperity – First annual update, Attorney-General's Department, Canberra. Cybersecurity Ventures, 2016, Hackerpocalypse: A Cybercrime Revelation, Cybersecurity Ventures.

SMEs feel informed about cybercrime

When it comes to the perception of cybercrime, almost **2 in 3** SME owners feel well-informed about the risks of cybercrime.

80% of SME owners feel their business can respond to a security breach, making SMEs more confident than some ASX-listed companies.

> "[With the help of an IT expert] I am so much more savvy now! My website is being redone—SSL and a more secure server, and information provided by my clients will be encrypted. All my passwords to my emails now are nonsense words."
>
> Small business owner and cybercrime victim

SMEs believe their limited online presence protects them from cybercrime

The most frequent digital activities of SMEs are receiving and sending emails.

Almost **50%** of SMEs have a social media presence. It is through these activities that SME owner-operators may, unknowingly, expose their businesses to cyber security risks.

Less than 30%

of SMEs report having suffered a cybercrime event

When it comes to seeking help

IT Forensic consultants ranked highest **60%**

then Google **40%**

Police **35%**

and then the Government **34%**

SMEs manage the risks to their business through their own experience

75% indicated they are influenced by their own experience rather than advice they received from a specialist (lawyer, accountant).

SMEs want a tool to help them manage cybercrime

93% said they would like a tool. There is a need for risk-management tools for SME owner-operators to protect their businesses from cybercrime.

NSW GOVERNMENT

Small Business Commissioner

See the full research:
www.smallbusiness.nsw.gov.au