

Cost of Cyber Attacks in Australia

According to the Department of Home Affairs and Stay Smart Online Australia, a new cyber crime is reported every 10 minutes and the cost of Cyber Crime is on the increase each year.



©2023 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation. 1041081720CYBER

The cost of Cybercrime to Australia **\$29 BILLION PER YEAR**

DIRECT COST TO BUSINESS

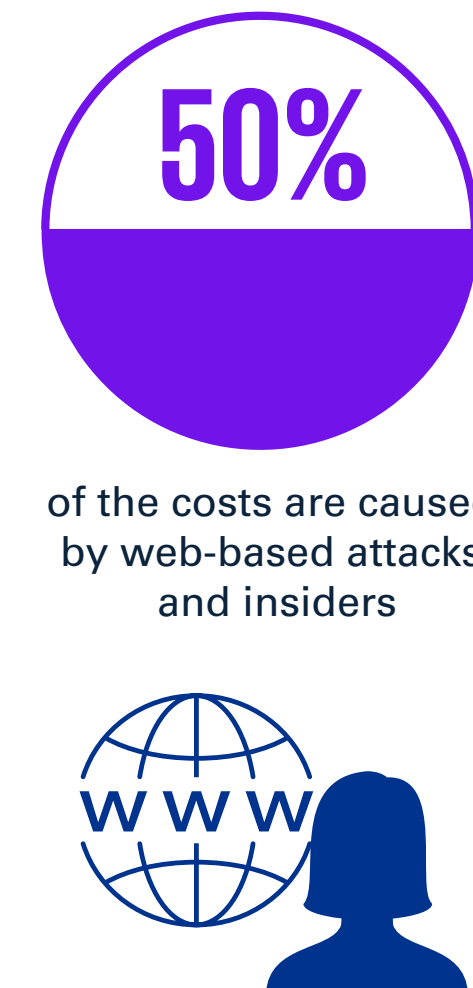


60% OF ALL TARGETED ATTACKS STRUCK SMALL AND MEDIUM BUSINESSES



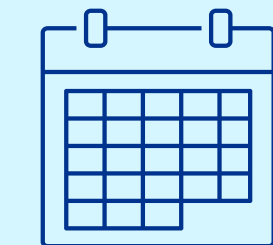
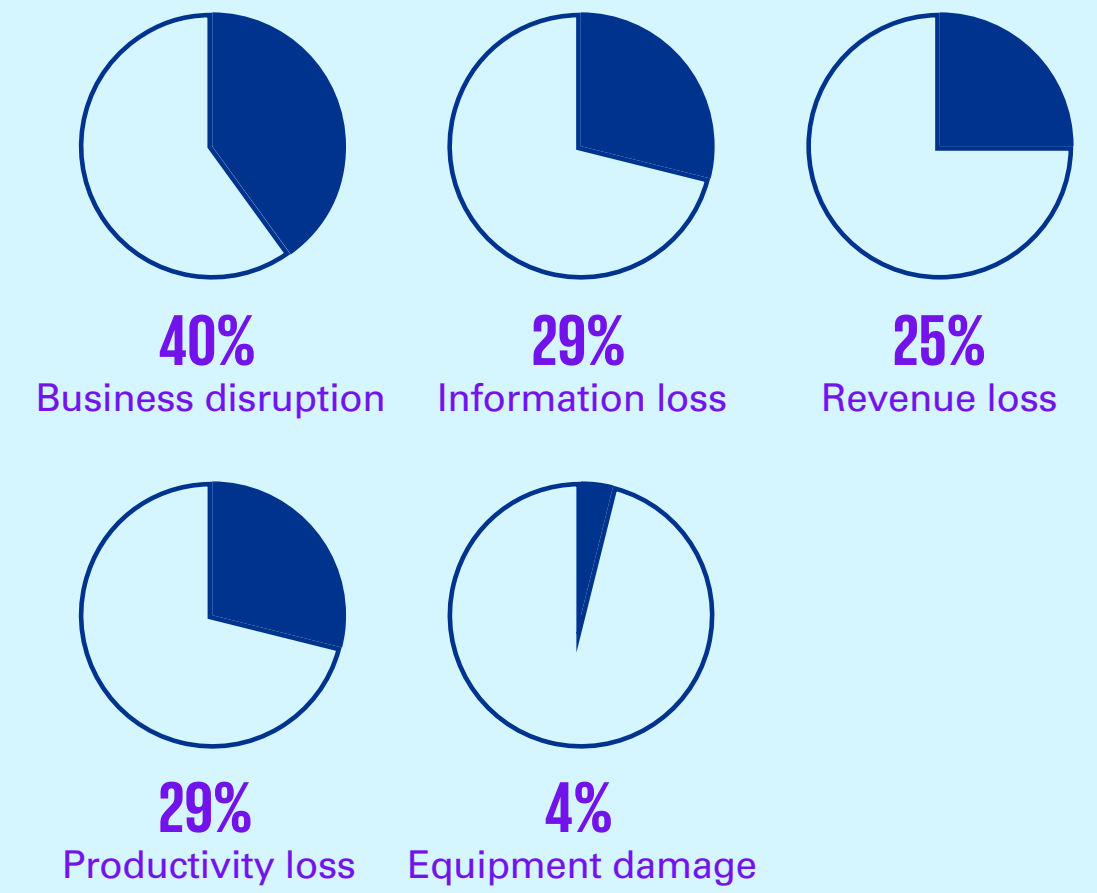
Average cost per attack

Denial of service	\$180,458
Web-based attacks	\$79,380
Malicious insider	\$177,834
Malicious code	\$105,223
Phishing and social engineering	\$23,209
Malware	\$458
Stolen devices	\$13,044
Virus, worm or trojan	\$421
Botnet	\$867



INDIRECT COST TO BUSINESS

Effect of a cyber attack cyber business



Average time to resolve an attack is

23 days



Increase to 51 days

if the attack was a malicious insider, employee or contractor.



Data sources: PWC – Global Economic Crime Survey 2014; ABS – Count of Australian Businesses 2014; ABS – Business use of Information Technology – 2014; Ponemon Institute – Cyber Security Report 2014; Symantec – Internet Security Threat Report 2015.