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.

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

DIRECT COST TO BUSINESS

33% = **693,053 businesses**

experienced a cybercrime

11,703 reported a cyber incident

→ **153 reports of critical infrastructure**

Energy · Utilities · Finance

60% OF ALL TARGETED ATTACKS STRUCK SMALL AND MEDIUM BUSINESSES

$276,323

Average cost of a cyber crime attack to a business

53% of the cost is on detection and recovery

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

50%

of the costs are caused by web-based attacks and insiders

INDIRECT COST TO BUSINESS

Effect of a cyber attack cyber business

40% Business disruption

29% Information loss

25% Revenue loss

29% Productivity loss

4% Equipment damage

Average time to resolve an attack is **23 days**

Increase to 51 days if the attack was a malicious insider, employee or contractor.

KPMG

Australian Government Initiative
Stay Smart Online

STAY SMART ONLINE

FOR MORE TIPS VISIT STAYSMARTONLINE.GOV.AU

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.