

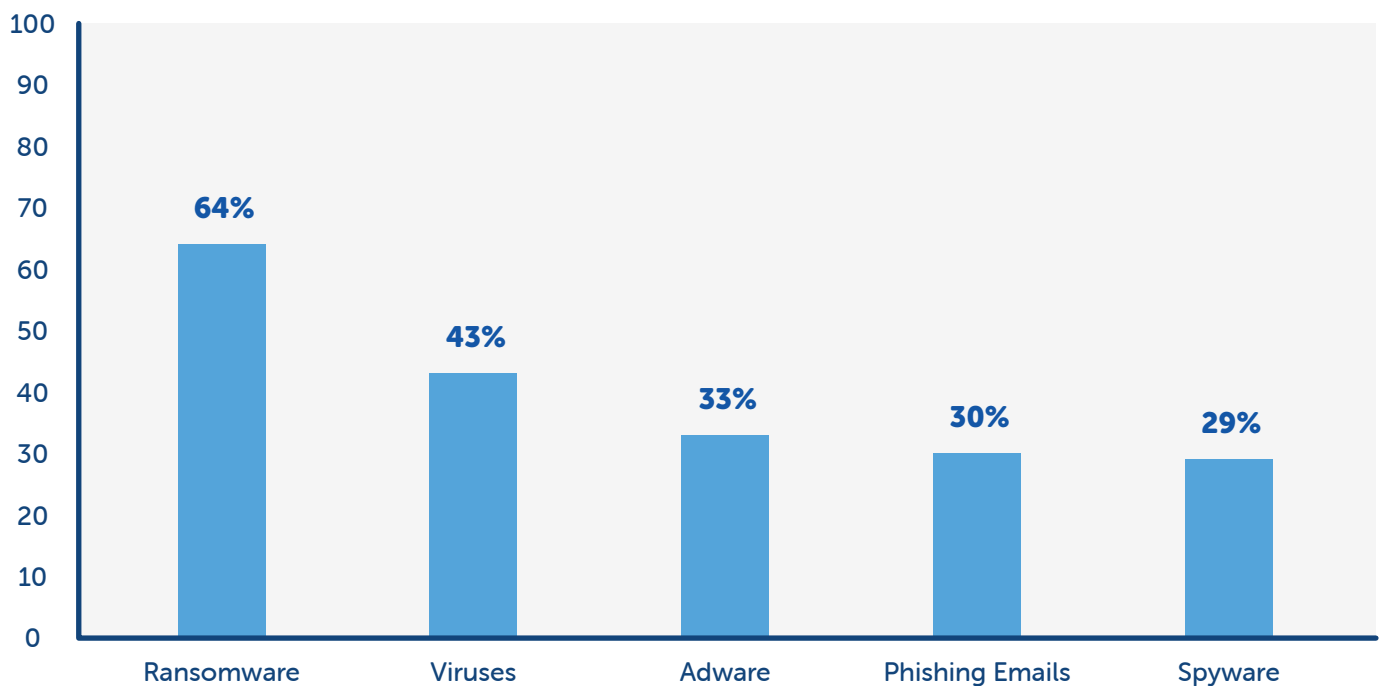
# Cybercrime Statistics in Australia 2020

Australia is fighting a battle against cybercriminals who want to exploit and make money from individuals and businesses. Here's what you need to know about the state of cybersecurity in the country.

Cybercrimes by the Numbers	
<b>\$29 Billion</b>	Estimated cost of cybercrimes to Australian businesses
<b>\$15.8 Million</b>	Losses due to cyberthreats that steal personal information
<b>\$9.2 Million</b>	Malware detections recorded by Australian businesses
<b>\$276,323</b>	Average cost of cybercrime to a business
<b>53%</b>	Cost of being paid for detection and recovery
<b>23 to 51</b>	Days to resolve an attack
<b>1 of 3</b>	Aussie adults affected by cybercrime

Sources: Department of Home Affairs, Stay Smart Online Australia, ACCC Scamwatch 2019, and CIO Magazine 2019

## Top 5 Threats Targeting SMBs in the Last 2 Years



Source: DATTO State of Channel Ransomware Report 2019

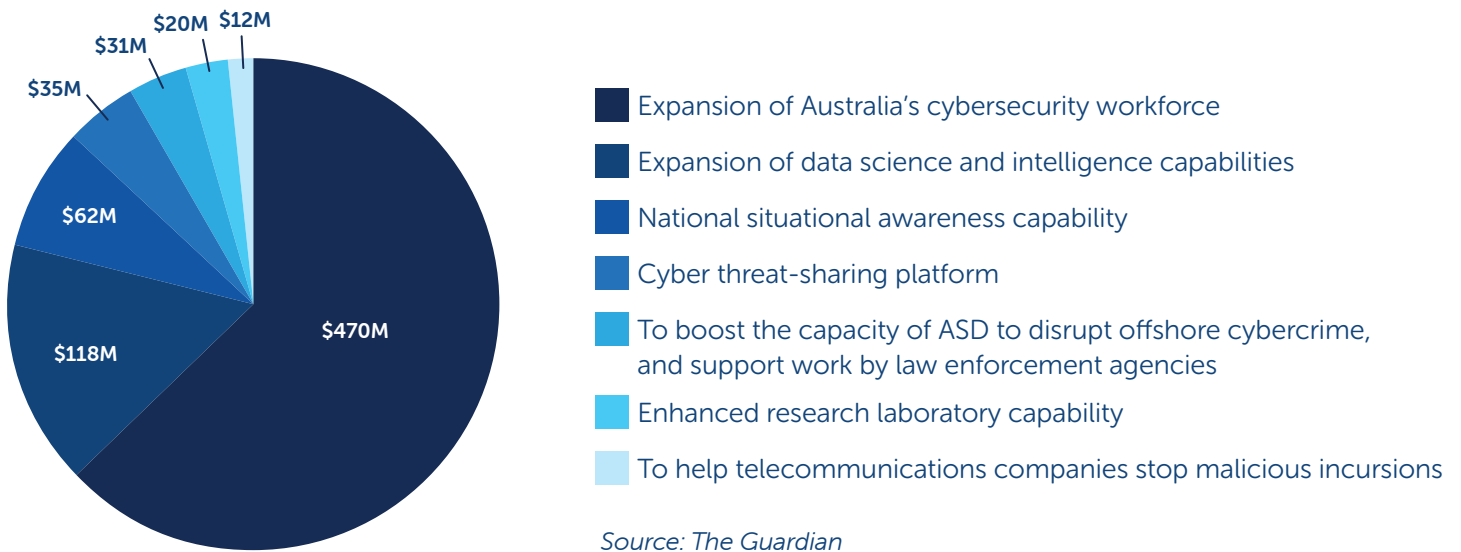
**HUMAN ERROR** is the greatest risk for cybersecurity in businesses. It includes sending an email to a wrong recipient, opening an attachment from someone thought to be critical to the business operations, and unintentionally revealing personal information to a third party because of a lost/misplaced data storage devices.

### Human Error Statistics in Cyber Security

<b>83%</b>	percent of data breaches that affect fewer than 1,000 people
<b>55%</b>	health sector breaches due to human error
<b>41%</b>	finance sector breaches due to human error
<b>39%</b>	data breaches where contact information is released

**773 Million email addresses and usernames** are affected by a significant data breach, which involves credentials for multiple users of businesses websites or services (Source: Australian Cyber Security Centre) It is essential to change passwords regularly, use strong password combinations, and implement multi-factor authentication on accounts if available.

### Allocation Of The \$748 Million Government Budget For New Initiatives And Expanded Security Workforce



### Information and Guidance on Cybercrime

**SCAMwatch** ([scamwatch.gov.au](http://scamwatch.gov.au)) to stay up to date on current scams

**Office of the eSafety Commissioner** ([esafety.gov.au](http://esafety.gov.au)) for online safety education resources and information for young people, parents and teachers

**Australian Cyber Security Centre** ([cyber.gov.au](http://cyber.gov.au)) for private and public sector collaboration and information sharing to combat cybersecurity threats

**Stay Smart Online** ([cyber.gov.au/acsc/view-all-content/programs/stay-smart-online](http://cyber.gov.au/acsc/view-all-content/programs/stay-smart-online)) to find out more about online safety and security and receive regular alerts

**Australian Institute of Criminology** ([aic.gov.au](http://aic.gov.au)) to access cybercrime research and complete the annual consumer fraud survey