INSURANCE COUNCIL OF AUSTRALIA

Media Release

July 29, 2015

Business can no longer afford to turn a blind eye to cybercrime

In the wake of reports today that incidence of cybercrime attacks in Australia have increased 20 per cent to 1131 last year, the Insurance Council of Australia (ICA) said business could no longer ignore the threat, estimated to cost the nation $1 billion a year.

Media reports today quote data from the Australian Cyber Security Centre (ACSC) showing dramatic increases in the incidence of cyber security attacks in Australia, growing from just 313 attacks in 2011 to 1131 last year.

The ACSC says the primary targets of such attacks are banking systems, energy providers and the communications sector.

Media reports today cited ACSC coordinator and Australian Signals Directorate Deputy Director, Clive Lines, saying the current level of cyber threat in Australia is “undeniable, unrelenting and continues to grow”.

ICA CEO Rob Whelan said though the insurance industry had been working with law enforcement agencies for many years to address the issue, the broader Australian business community had been slow to recognise the scale of the potential threat – a threat that was evolving daily.

“Australian business can no longer afford to turn a blind eye to cybercrime. The ACSC has estimated it costs the country $1 billion a year. Business owners are urged to undertake a detailed risk assessment of potential vulnerabilities and liabilities and to take action to ensure appropriate protection is in place,” Mr Whelan said.

“One example of significant threat is the ACSC’s recent warning that a new wave of ransomware emails are targeting Australian government and private-sector enterprises in the guise of emails purporting to be from Australia Post parcel collection and also Australian Federal Police infringement notices.

“The ACSC warned the sheer scale of the attack and the continual use of new domains by the hackers has reduced the effectiveness of domain-blocking as a long-term solution. Once executed, this ransomware encrypts the users’ files, including those on networked or shared drives used in the corporate environment, making them inaccessible to the user.”

Mr Whelan said a range of products were available from insurers or through insurance brokers that enabled businesses to mitigate financial losses caused by cybercrime.

The Insurance Council of Australia continually liaises with all Australian police forces to keep abreast of the latest trends in crime and criminal activity.

- ENDS -

Media contact: Media adviser 02 9253 5161 0432 121 116 Twitter: @ICAUS