Businesses turn to encryption apps to keep out cyber attacks and ransomware

Video
Image

Experts say North Korea may be linked to global cyber attack

AUSTRALIAN businesses are turning to encryption apps to fight the flood of cyberattacks like the crippling WannaCry ransomware that brought down 200,000 computers across the world this week.

The Telstra Cyber Security Report shows the rate of cybercrime had doubled in the past year, with Australia identified as the top target for malware in the Asia Pacific.

Nearly two-thirds of Australian businesses have been hit by ransomware in the past year, and one in 10 incidents take the businesses at least a day to recover.

Tim Gallagher, who has created the SafeSwiss app that runs on servers in Switzerland and provides better than military grade encryption, said he had experienced a 78 per cent spike in downloads this week in the wake of the WannaCry ransomware attack.

Simon Ryan, Chief Technology Officer at First Wave said people were increasingly turning to apps such as WickR and Confide that encrypted messages, or other apps that offered "ephemeral communication" with messengers that destruct once they have been written and read once.

One of the lessons of the crippling ransomware WannaCry that infected thousands of computers across the world is that in times of technology crisis the best backup is a pencil and paper.

REVEALED: New massive cyberattack underway

RELATED: North Korean hackers' secret Cyberwar

Cyber attack aftershocks disrupt devices across Asia
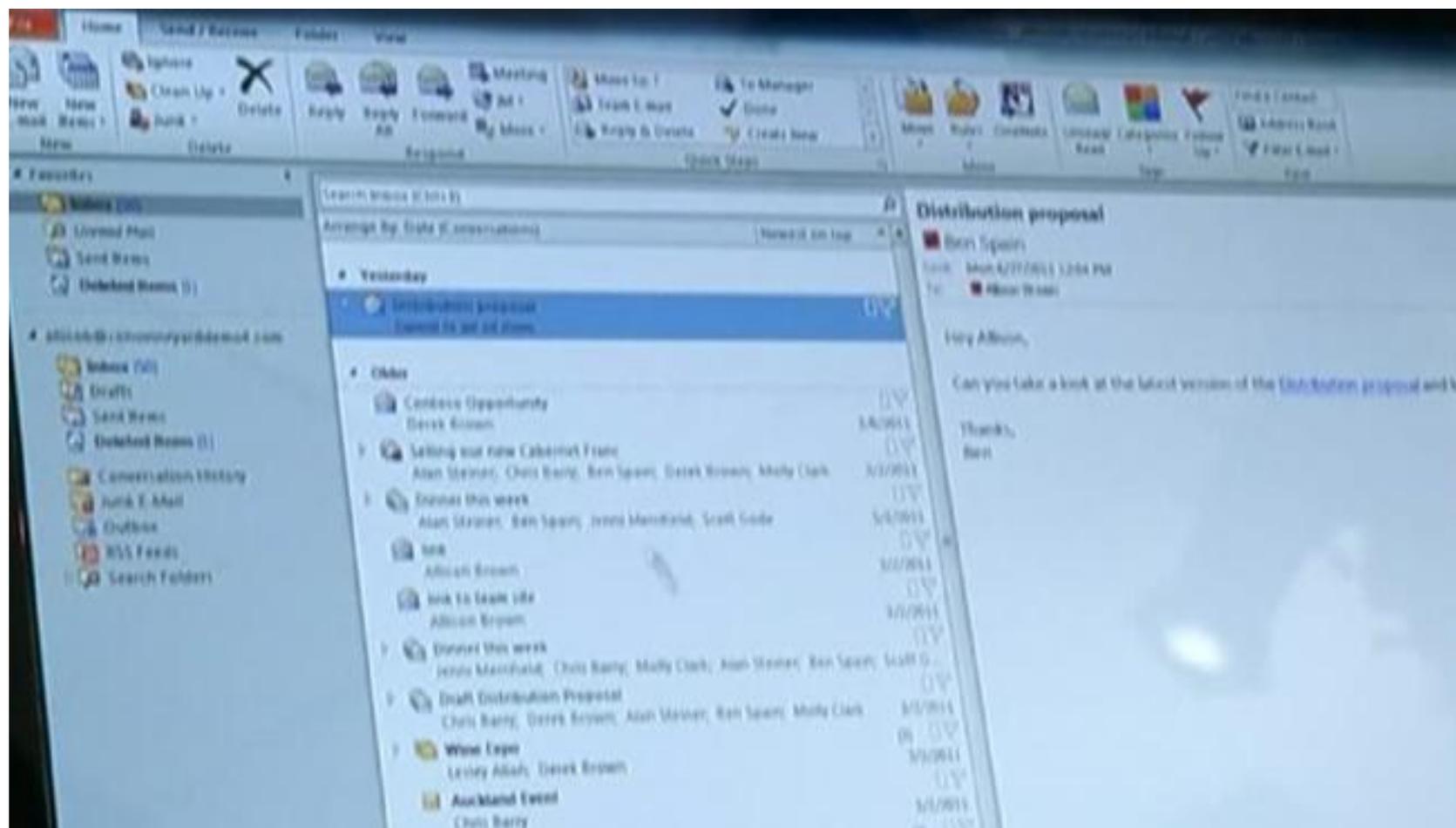
While Australian businesses escaped the worst of the first wave of WannaCry attacks, there were reports in the UK of doctors reverting to handwritten notes and whiteboards when hijacked computer systems

forced them to shut their doors to anything but emergencies.
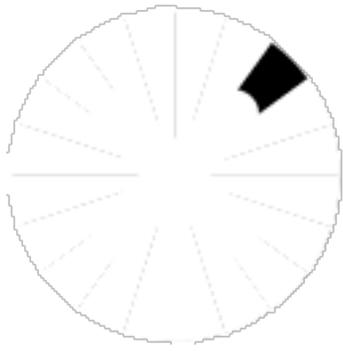
The lesson echoed the experiences at Sony, which was targeted by North Korean hackers in 2014 in protest against the Seth Rogen comedy *The Interview*, with Hollywood executives reportedly bringing out typewriters to write internal messages after leaked emails caused headlines and red faces.

But business and security experts said scratching down frantic notes while computers were down for repair was a temporary measure.

The modern reliance on the internet and email means business cannot fight back at cyber attacks simply by going back to an analog era.

'The Interview' trailer
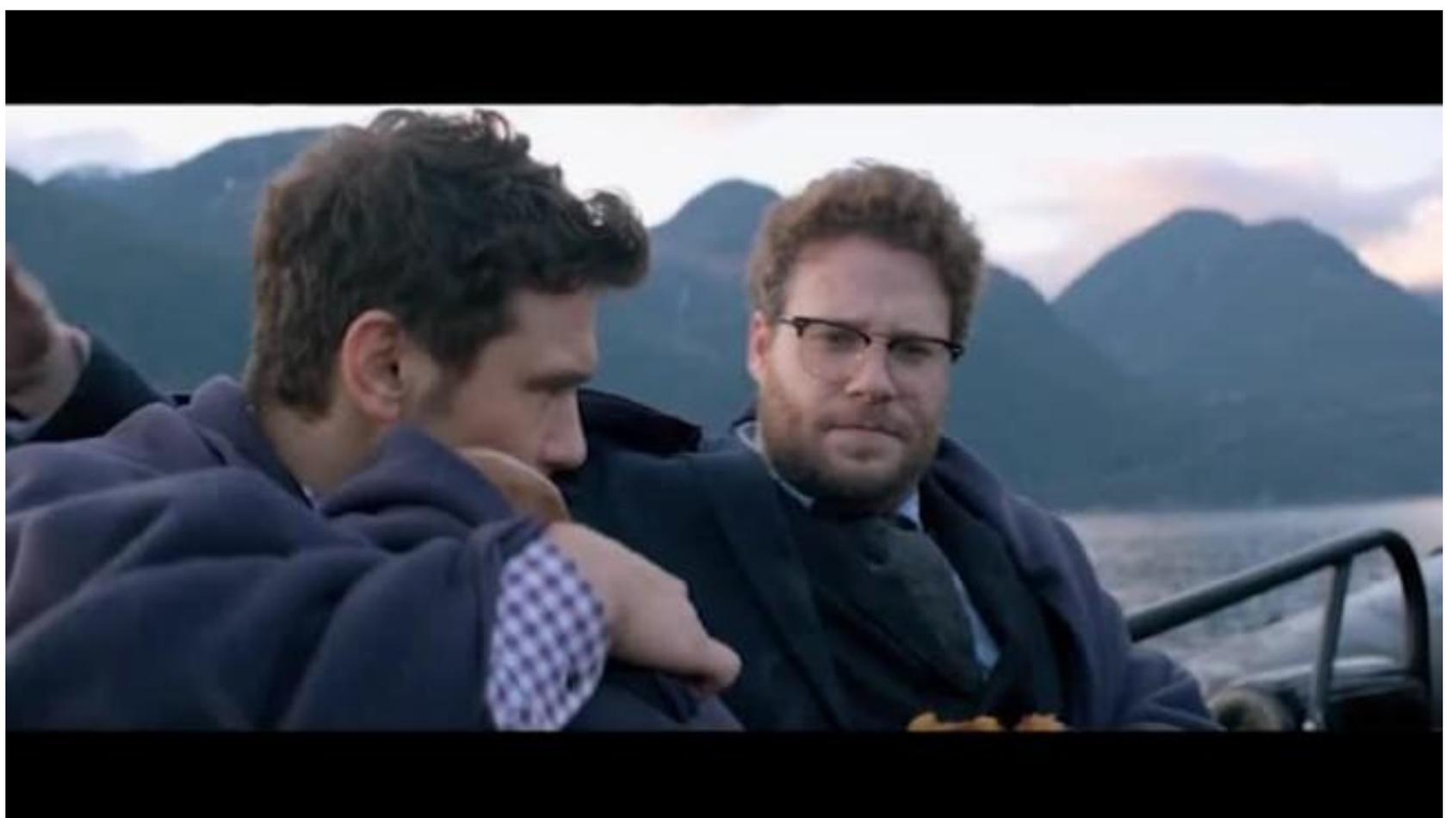
Bogdan Botezatu, senior e-threat analyst at Bitdefender said some businesses shut down their computers last week to install the software update to protect against Wannacry.

"However, with everything interconnected, it is currently impossible to revert to pen and paper," he said.

Australian Small Business Council CEO Peter Strong said with the rise of cybercrime and ransomware causing headaches for small business, there was often talk about turning to old-school tools.

"Some people are talking about it but nobody is going to do it because in small business the change process is worrying," Mr Strong said.

"I haven't heard of anyone that is actually doing it."

He said some small business owners might be tempted to store vital information in paper form to keep it safe from hackers but it would be difficult for business to communicate with their clients without technology tools.

"You're not going to go back to post it anymore," he said.

"Post only delivers every second day anyway."

Originally published as [Encryption apps in cyber fight](#)