THE AUSTRALIAN

SE Feature

HD Cyber crime part and parcel of digital age

BY Laura Cencigh-Albulario
WC 1,019 words
PD 20 May 2014
SN The Australian
SC AUSTLN
ED Australian
PG 26
LA English

LP

No modern business is immune to the threat of a digital attack, but boosting protection and planning for the aftermath can help to lessen its access and impact, writes Laura Cencigh-Albulario

FOR many businesses, being impacted by cyber crime is not a case of if, but when.

TD

One in four businesses have experienced a cyber crime, says PWC's 2014 Global Economic Crime Survey. In Australia alone, this is an annual cost of about $4.5 **billion**.

Small players are not immune from the threat, and are often used as soft targets, or as entry points for tapping into bigger businesses, according to PWC Cyber Asia-Pacific leader Steve Ingram.

"Everyone's security is only as strong as the weakest link," he says. "Service providers, vendors and customers are all part of an organisation's system today. If you're a big business but have a small business servicing you, they've probably got a direct connection into the system." Last year's Black Friday data breech, for example, when credit card details were stolen from **millions** of Target shoppers in the US, reportedly saw hackers use use an airconditioning subcontractor's credentials to gain access to the system.

The average period of detection of an online security breech is 240 days, and two thirds aren't picked up by the organisation itself, but by law enforcers, suppliers, customers or others.

Along with opportunistic smash-and-grab attacks are long-term, strategic hacking **operations**. "They're sitting there quietly, wanting to gather information on who you deal with, passwords and user information for competitor intelligence or commercial espionage,'' Ingram says.

"You might be a law or accounting **firm** looking after a merger and **acquisition** deal. There might be lots of security around the acquirer and target, but if it's not as strong at the law **firm** that's advising them, this will be the entry point." The vast quantities of personal information made easily accessible through social media can also weaken defences.

In one example, a manager received a phone call from someone purporting to be his CEO, asking for a sum of money to be transferred urgently.

He was so knowledgeable about the manager's interests and family, even enquiring after his children, that the manager transferred the funds without hesitation. Facebook seemingly gave the scammer all the information he needed to set the manager's mind at ease.

The complexity of cyber security threats makes prevention about far more than a firewall. "This is not an IT issue, it's a whole of business issue," Ingram says.

He explains firewall protection is no better than the Great Wall of **China**. Just as enemies can pass through corrupt guards, or catapult diseased carcasses over the wall, so too may malicious or naive staff open the gateway, use a USB with a virus or fall victim to a phishing scam.

Deloitte cyber security **lead** partner Tommy Viljoen says the first step in protecting against cyber crime is ensuring anyone with access to a **company**'s systems knows how to operate securely at work and at home, given the large crossover. "The digital age doesn't determine what part is work and what part is home," he says. "If you're using the same passwords at home across all your personal websites, and at work, if one of these is compromised, whoever is using it can try to gain information from a work perspective." Next come the IT solutions, including firewalls, basic penetration testing and access controls. "You cannot operate in the digital economy without this basic security," Viljoen says. "If this is outsourced, you need to make sure whoever you've outsourced it to is a reputable cloud service that can assure you your security is handled appropriately." Thirdly, businesses need to prioritise their cyber security concerns – what's of most value to the business, what might be of greatest value to hackers and what's most at risk. For a start-up, for example, it might be the intellectual property for their products and designs.

For a small listed **company**, hackers accessing business results prior to their release could affect the share price.

"Outsiders might value what you do in different ways," Viljoen says. "You cannot spend enough on security to protect everything and nor should you. It's about what's most at risk." Finally, a cyber security plan should include processes for what to do when a breech occurs. "You will be hacked at some stage; they will break through so be prepared," Viljoen says.

Monitoring systems and an appropriate response procedure that won't prompt malicious damage from the hackers and destroy evidence should be part of this plan.

Insurance against cyber attacks is another aspect.

Deloitte financial crime **lead** partner Ivan Zasarsky says businesses should not assume they're covered for cyber security breeches.

"Policies are designed to protect tangible assets – there aren't enough test cases to ascertain whether this extends to intangible assets," he says. "Your laptop might be covered, but the theft of the data that's on it is far more valuable. You don't want any surprises when you're already struggling financially to cope with a breech." Liability is another big aspect.

Regulatory changes being rolled out across the globe are adding to the responsibility placed on **company** heads to protect against cyber security breeches.

"What seems to be standard practice today may be tomorrow's circumstances of negligence," Zasarsky says.

"The personal risk of officers of corporations that face these cyber breeches is not only looking at damages, reputation, share price and brand. The spectre is changing where prosecution in terms of negligence is reaching the executives themselves." Keeping up with the risks of cyber crime should simply be accepted as the cost of operating in a digital age, Zasarsky adds."What won't change is the threat, but what will change is the response to the threat, the regulation and heightened awareness of the absolute need to pay attention to that risk."

IN isecpri : Security/Privacy Software | i3302 : Computers/Electronics | i330202 : Software | i3302021 : Applications Software | icomp : Computing | itech : Technology

NS ghack : Computer Crime | reqrcm : Suggested Reading Computers | gcat : Political/General News | gcrim : Crime/Courts | ncat : Content Types | nfact : Factiva Filters | nfcpex : FC&E Executive News Filter | redit : Selection of Top Stories/Trends/Analysis | reqr : Suggested Reading Industry News

RE austr : Australia | apacz : Asia Pacific | ausnz : Australia/Oceania

PUB News Ltd.

AN Document AUSTLN0020140519ea5k00001

