The AFR View

All must probe and plug digital data defences

All levels of governments and companies need to move quickly to find and fix the weaknesses that are clearly afflicting digital data handling.

Nov 2, 2022 – 6.40pm

All levels of Australian government and companies now need to move quickly to find the weaknesses clearly afflicting digital data handling and fix them. No one is far off from the purgatory that Optus and Medibank have endured in the past weeks after criminals pillaged their databases of everything from passport numbers to sensitive medical records [https://www.afr.com/technology/medibank-shares-stabilise-as-privacy-regulator-drags-heels-20221027-p5bten]. Woolworths MyDeal, and wine seller Vinomofo have also had large numbers of customer data pilfered this month too.

Harvesting customer data is not just a business model for everyone from tech giants to supermarkets, but a dynamic new source of economic growth. The risks of failing to keep that information secure – and the potential damage done to millions of customers' lives from identity theft or extortion – is also a massive operational vulnerability and an unprecedented political, legal, and reputational liability. Think of angry politicians, a fuming public, class actions and legal perdition. All companies now have to assume that they are going to be hit, even if it's just a ransomware attack on their own operations. So, what do they do next?

Medibank has been hit by a significant cyber attack. **Louise Kennerley**

It remains unclear how the data of 10 million Optus customers was removed, while 3.8 million records were stolen from Medibank with a likely pinched administrator log-in. The criminal world has considerable resources available: global 'black hat' hackers for hire, easy to use software off the shelf, or subscriptions to sophisticated hacking-as-a-service. And while the criminals have to be lucky only once; the targets have to be lucky all the time. Yet 'white hat' cyber defenders are in very short supply. Boards which are assured that their operations are fully staffed in this area should question how.

Cyber minister Clare O'Neil also needs to fix an unforced error where an earlier attempt to streamline skilled visa queues has inadvertently sent cybersecurity experts to the back of the line in the midst of an emergency, alarming the tech industry.

Terrible dilemma

Companies which do face ransom demands from hackers or data thieves have a terrible dilemma. They are crime victims too. The federal government wants to take a Team Australia approach, advising strongly that nobody pays up because it just encourages attacks on everyone. Government bodies do not pay ransoms, and subsequently most attackers aim at private companies, 80 percent of which do. But at that point they are simply anxious that the brunt does not fall on their customers.

It gets easier to insist on a no-pay principle, or even to ban ransoms for private companies too, if everything has been done beforehand to create a baseline level of cybersecurity that makes everyone more resilient.

The Australian Cyber Security Centre's Essential Eight list of precautions – tailored for different businesses and risks – is the major starting point, covering the control of apps, patches, privileges and so on. For smaller businesses, at least the first four are essential. Yet even government departments routinely fail their cyber audits. And making the Essential Eight mandatory for all companies would simply reveal how really deficient we are. Many of the problems are in legacy components which depend on easily compromised connecting software to talk to each other. A great many companies would claim they cannot afford to replace hardware in one go without a long phase-in period.

The other option is simply to narrow the gush of information into leaky companies. Hotels, telcos and others that need to verify customers are left holding far too much information such as passports or driver's licences. The federal government has a single Digital ID which replaces those documents as legal proof.

The government should use the debacles at Optus and Medibank [https://www.afr.com/technology/optus-hack-prompts-5-5m-for-privacy-commissioner-20221020-p5brgv] to iron out its problems and relaunch it. The government also proposes new fines for companies that egregiously sit on unnecessary data. But many claim that other laws oblige them to hold years of data. This has to be resolved too.

In the meantime, companies have to do more to protect themselves at the most basic levels. Multi-layered authentication and protection of passwords is critical. For bigger companies, war gaming and simulating attacks to work out how they would manage when a breach is found would treat cybercrime like the existential threats that they are.

Data has been called the new oil. But it took catastrophic spills, harsh regulation, and big investments for oil companies to learn how to move petroleum safely. But even the oil business does not have to face hardened pirates as well as human error. The need to act is urgent here.

RELATED

Police warn Medibank not to pay cyber ransom

https://www.afr.com/technology/police-warn-medibank-not-to-pay-cyber-ransom-20221031-p5bucd

RELATED

Medibank customers in limbo as hacker ransom dilemma plays out

https://www.afr.com/technology/medibank-customers-in-limbo-as-hacker-ransom-dilemma-plays-out-20221028-p5btwd

The Australian Financial Review's succinct take on the principles at stake in major domestic and global stories - and what policy makers should do about them.