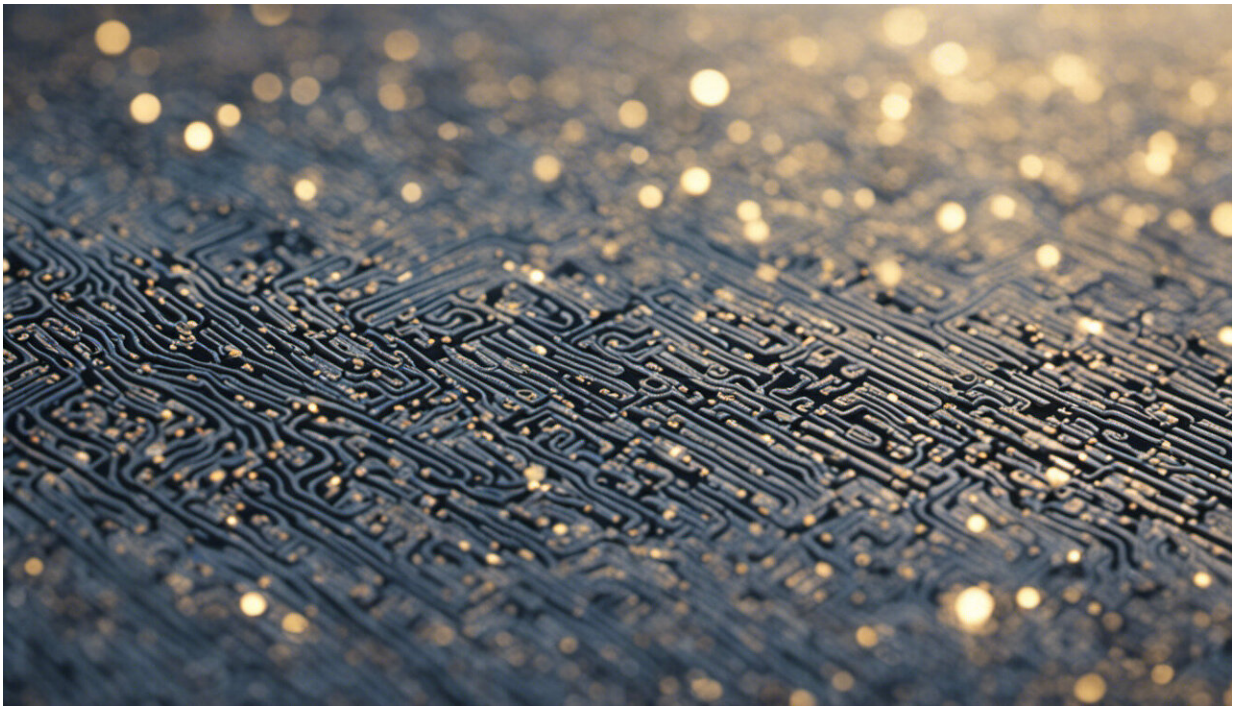
Hackers cause most data breaches, but accidents by normal people aren't far behind

August 10 2018, by Nicholas Patterson



Credit: AI-generated image (disclaimer)

Have you ever had your personal information leaked on the internet? Maybe it was something you purchased online from a website, only to find out that the company was hacked months later? If the answer is "yes", you probably want to know whether the breach was reported and dealt with.

Australian organisations reported 242 data breaches between April 1 and June 30, 2018. There was a dramatic increase in notifications from February 2018, when eight notifications were made, to June 2018, when 90 notifications were made.

There are obvious reasons for this increase. Since the government's Notifiable Data Breaches (NDB) scheme was introduced on February 22, organisations are becoming more aware of cyber security, and the rules and regulations around handling data.

What does a data breach look like?

To give you an example of a data breach, we can look back to 2017, when almost 50,000 Australians had their sensitive information leaked online.

In this case, a private contractor incorrectly configured an Amazon cloud storage service, inadvertently causing the data to become publicly accessible. A Polish security researcher discovered the data, which included names, passwords, identification details, phone numbers, and credit card numbers.

The NDB scheme aims to prevent breaches like this from being kept under wraps, and to allow all affected parties to learn the extent of the damage.

How many people were affected?

The recent quarterly NDB report suggests that most data breach notifications are coming from small or medium-sized organisations, with relatively few customers affected. There were 55 notifications (23%) of breaches in which 11 to 100 people were affected. In 52 instances

(21%), 101-1,000 people were affected. And there was just one notification that affected more than a million people.

This suggests that larger organisations are generally more adept at preventing data breaches.

What kind of data was breached?

The types of information being leaked is broken down into Tax File Number, health information, identity information, financial details, and contact information.

Results show that contact information was the most common type of data leaked, with 216 notifications reported (89%). This was followed by financial information, with 102 notifications (42%); identity information (94 notifications, 39%); and Tax File Numbers (47 notifications, 19%).

It is worrying that financial information was leaked in 42% of cases. Any data breach is problematic, but the leak of financial data can have a dramatic impact on a victim's life if it results in fraudulent purchases.

What is causing these data breaches?

Three main reasons were cited for data breaches in the last quarter: malicious or criminal attacks (59%), human error (36%), and system fault (5%).

Most notifications were the direct result of cyber incidents, including phishing, malware, ransomware, brute-force attacks, compromised or stolen credentials, and hacking. This was followed by theft of paperwork or data storage devices, and breaches caused by rogue employees and insider threats.

Human error is often regarded as the main cause of cyber security incidents. But it was only the second most common cause of data breaches during the last quarter.

In 22 cases, data was sent to the wrong recipient. When organisations unintentionally released or published information this accounted for 12 notifications. The report includes clicking on a phishing email as human error, although this action should really be categorised as the result of a malicious attack.

Which industries were most affected?

The report lists five industry sectors: health service providers; finance and legal services; accounting and management services; education and business services; and professional services.

The health care industry was most affected, with 49 notifications (20%), followed closely by the finance sector with 36 notifications (15%).

Why these sectors? Financial information, such as credit cards or bank details, is a key target for hackers because it can translate into real money quickly.

The health services industry is also a lucrative target for hackers who have in the past put confidential patient data up for ransom. For example, in 2016 the Hollywood Presbyterian Medical Center paid a US$17,000 ransom in bitcoin to hackers who had taken control of its computer system.

The education sector reported 19 notifications (8%). This number is likely to grow as hackers become aware of the value of unpublished research and intellectual property.

A recent example of this was the hacking attempts of Australian National University, where it was reported that ANU spent many months fending off attacks on its systems that were traced back to China.

Combating data breaches

The NDB scheme and reporting is an important way to shed light on the cyber security issues facing Australia, now and in the future. Knowing how breaches are occurring, how often and to which sectors will allow cyber security professionals and researchers to tackle these issues head on.

Some breaches can be defended using technology, such as ransomware prevention tools. But breaches that result from human error are more difficult. Education and training for employees can assist them in preventing simple mishaps from occurring.

Bringing these numbers down will require a mix of technological solutions and education. Until we get this right, we're likely to see more breaches in the near future, rather than less.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Hackers cause most data breaches, but accidents by normal people aren't far behind (2018, August 10) retrieved 26 April 2024 from https://techxplore.com/news/2018-08-hackers-breaches-accidents-people.html