Security

ISO 27001 - what's all the fuss about?

Justin Kerr
Nov 9, 2022 • 4 min read

So you think your system is secure, huh?

2022 - Optus Australia (Telco) - hacked - 10 million records
2022 - Medibank Australia (Health) - hacked - 3.9 million records
2021 - Facebook - hacked - 533 million accounts
2021 - LinkedIn - hacked - 500 million accounts

Although all of these incidents were costly, it’s worth noting that incidents with a high

number of breached records aren't necessarily the most damaging overall.

The LinkedIn breach, for example, comprised information scraped from people's public profiles. No financial records were affected, and although attackers will almost certainly have used the information in scams designed to turn data into currency, it's unclear how successful that was.

By contrast, the much-publicised ransomware attack on Colonial Pipeline affected a limited amount of personal data (the attackers reportedly gained access to the organisation's systems after stealing an employee's login credentials in a phishing attack), but the attackers were able to leverage that information to cause far greater damage.

The fuel supplier's systems were crippled by ransomware, and it was forced to shut down its operational technology network and billing system.

As a result, petrol stations were left without fuel, and people hoarded supplies – often in buckets, plastic bags and other unsafe materials – as the crisis deepened.

It was arguably the most damaging cyber security incident of the year, with Colonial Pipeline eventually paying the attackers $4.4 million (about £3.3 million at the time) to regain access to its systems.

Which sectors are most targetted?

For the third consecutive year, the healthcare and health sciences sector suffered the greatest number of data breaches. Almost 300 million breached records.

This is concerning not just because of the sheer number of records affected but also the types of data involved. For example, depending on the nature of the incident, healthcare breaches can reveal medical issues that can affect victims' reputations.

Likewise, healthcare data can be used to conduct fraud, launch phishing attacks and, in some cases, reveal financial data.

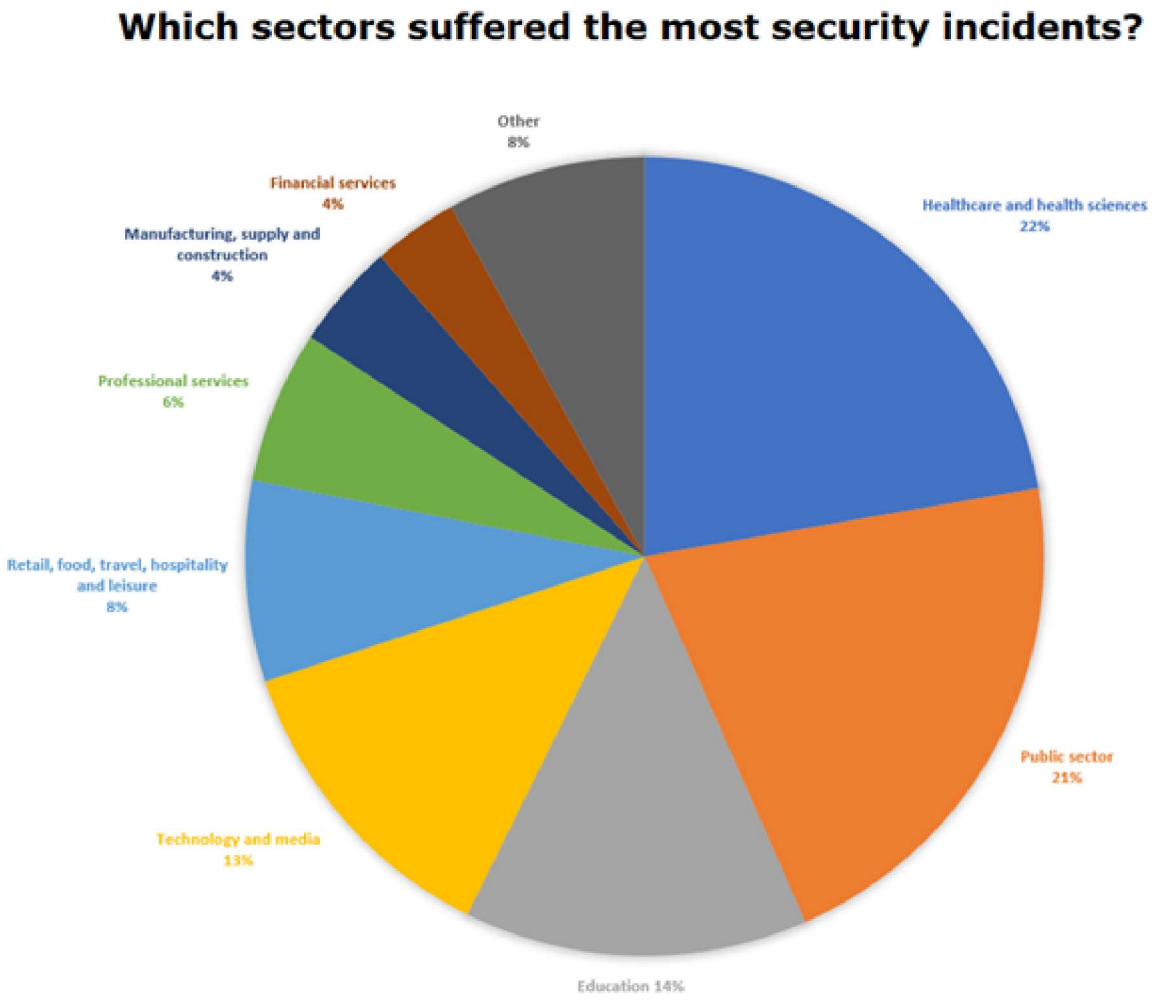

image courtesy of Luke Irwin (itgovernance.co.uk)

HealthMetrics has built the most secure data vault that you can build. Coupled with procedures and policies which exceed the requirements for our ISO 27001 certification, we believe our customers' data is as safe as it can be.

A word or two from Previn our Senior IT Administrator

"ISO 27001 is a set of standards that help organisations protect their data by introducing various controls. We use it to help reach certain IT security goals. Thanks to ISO 27001, we have identified these security gaps and have worked to enforce users to adhere to certain methods.

For instance, one of the steps we have taken to enhance our security is Microsoft Multi-Factor Authentication (MFA) or Microsoft Authenticator. This method uses a secondary piece of information, often a code generated by an application or sent via SMS. This secondary piece of information helps to prove it really is you trying to log in, as the codes are often accessed on the phone in your pocket. Even if you do have a password that's easy to guess, an attacker is unlikely to get access to an account with MFA turned on. These are the steps taken in enhancing our security.

There are various ways an attack can take place and at different levels. The most vulnerable would be end-user devices. Cybercriminals prefer to target endpoints because they are doorways to corporate data and, by nature, are vulnerable to attack. They are outside network security and dependent on users putting security measures into place leaving room for human error. To overcome this, we have Information Security Management System (ISMS) training for new joiners. This

training better explains the important aspects that should be practiced to safeguard the device and the data in it.

Additionally, we have introduced Microsoft Endpoint Manager (MEM) in HealthMetrics. Endpoints are physical devices that connect to and exchange information with a computer network. Some examples of endpoints are mobile devices, desktop computers, virtual machines, embedded devices, and servers. Endpoint security, or endpoint protection, helps protect endpoints from malicious threats and exploits.

I would say that ISO 27001 is here to provide us with a guide and a clearer view of any missing gaps within our control which we can fix or secure to avoid being prey to hackers.
Alongside ISO 27001, every individual in HealthMetrics will have to play their role in contributing to this."

Thanks Previn!

How does a healthtech start-up start-up?

Alvin Yuan is currently the Chief Executive Officer of HealthMetrics. He graduated as a pharmacist and spent the next years of his career in healthcare, financing, business…

Dec 1, 2022 4 min read