ignite

RECRUITMENT & TECHNOLOGY SOLUTIONS

DATA SECURITY:

YOUR DEFENCE AGAINST LEAKS AND BREACHES

DATA SECURITY: YOUR DEFENCE AGAINST LEAKS AND BREACHES

In the first half of 2022 alone, the Office of the Australian Information Commissioner reported 396 data breaches in businesses under the scope of the Privacy Act; that is, those with annual revenues over $3 million. At the same time, the first six months of the year saw a 33% increase in large-scale data breaches affecting at least 5,000 Australians—nearly two-thirds of which resulted from malicious cyber-attacks. The good news is that small businesses can prevent such attacks with a few simple data security measures.

No 21st-century trend has transformed the way we do business more than data has. Unfortunately, cybercriminals are starting to recognise the value of data as well. As data breaches grow in number and scale, organisations in Australia have an obligation to better protect the data they collect and store by understanding and implementing effective data security.

[1]https://www.afr.com/technology/millions-caught-in-data-breaches-before-optus-or-medibank-20221109-p5bwsc

WHAT IS DATA SECURITY?

Data security refers to anything a company does to protect the confidentiality, integrity and availability of the data it holds—preventing data breaches, leaks, and corruption of all kinds. It includes measures taken against both malicious attacks and human error. Data security must be comprehensive in order to be effective, so businesses must consider protections and controls in every location where data might reside, from end-user devices to servers and third-party cloud-based solutions.

Comprehensive data security requires an understanding of data across the entire business. This includes where data is stored, the type of data stored, how it is used within the organisation, who is using it, and how it is collected. Each of these factors will inform best practices for securing data.

In addition to data visibility, data security considers the risks different data types, locations, and uses may pose and seeks to recommend, implement, and maintain security measures relevant to those risks.

By understanding data types, and current security practises, data security helps organisations mitigate the risk of both cyberattacks and human error and prevent data leaks.

WHY DO BUSINESSES NEED TO STORE DATA?

Data security refers to anything a company does to protect the confidentiality, integrity and availability of the data it holds—preventing data breaches, leaks, and corruption of all kinds. It includes measures taken against both malicious attacks and human error. Data security must be comprehensive in order to be effective, so businesses must consider protections and controls in every location where data might reside, from end-user devices to servers and third-party cloud-based solutions.

Comprehensive data security requires an understanding of data across the entire business. This includes where data is stored, the type of data stored, how it is used within the organisation, who is using it, and how it is collected. Each of these factors will inform best practices for securing data.

In addition to data visibility, data security considers the risks different data types, locations, and uses may pose and seeks to recommend, implement, and maintain security measures relevant to those risks.

By understanding data types, and current security practises, data security helps organisations mitigate the risk of both cyberattacks and human error and prevent data leaks.

[2]https://www.optus.com.au/content/dam/optus/documents/about-us/media-centre/financial-reports/2022/halfyear_optus.pdf

THE RISKS OF STORING DATA

With the recent high-profile data breaches at Optus and Medibank Private bringing data security to the forefront in Australia, more than 65% of victims say they would reconsider doing any repeat business with an organisation that leaked their data.

As well as the reputational and repeat business impacts, serious data breaches can lead to class action lawsuits, which lead to legal fees as well as potential damages. The Australian Privacy Act is currently being rewritten to include fines of up to $50 million, three times the value gained from mishandling data, or 30% of a company's adjusted turnover.

In the case of Optus and Medibank, the impact has been significant. Optus has had to set aside $140 million "as an exceptional expense for the expected costs of actions to prevent harm to customers" and Medibank's share price had dropped by 20% just one week after the announcement of their data leak.

[2]https://www.optus.com.au/content/dam/optus/documents/about-us/media-centre/financial-reports/2022/halfyear_optus.pdf

BEST PRACTICES FOR CREATING A DATA SECURITY STRATEGY

In order to create a data security strategy that best fits the needs of the business, organisations can follow these four best practices:

1. Understanding Data

Before determining which data security methods and tools a business needs, it must first have a high-level understanding of the data it currently manages. Only by knowing the purpose and value of each data set can a business know the risks it will be exposed to.

Organisations can use a ranked scale to assess the sensitivity and risks of their data sets. In assessing these factors, they should consider, at a minimum, how and how often the data is accessed, the value gained from using or storing it, and the potential consequences of the data being leaked.

2. Align Importance and Risk Factors with Security Controls

Once a business understands the locations, types, values and risks of its data, it can begin to prioritise and implement appropriate security controls.

Security controls may be technical in nature, such as encryption or MFA; physical, such as air gapping and offline storage; organisational, such as limiting access to specific roles that require it; or contractual, such as enforcing minimum cybersecurity standards within vendors who store or process data on behalf of the business.

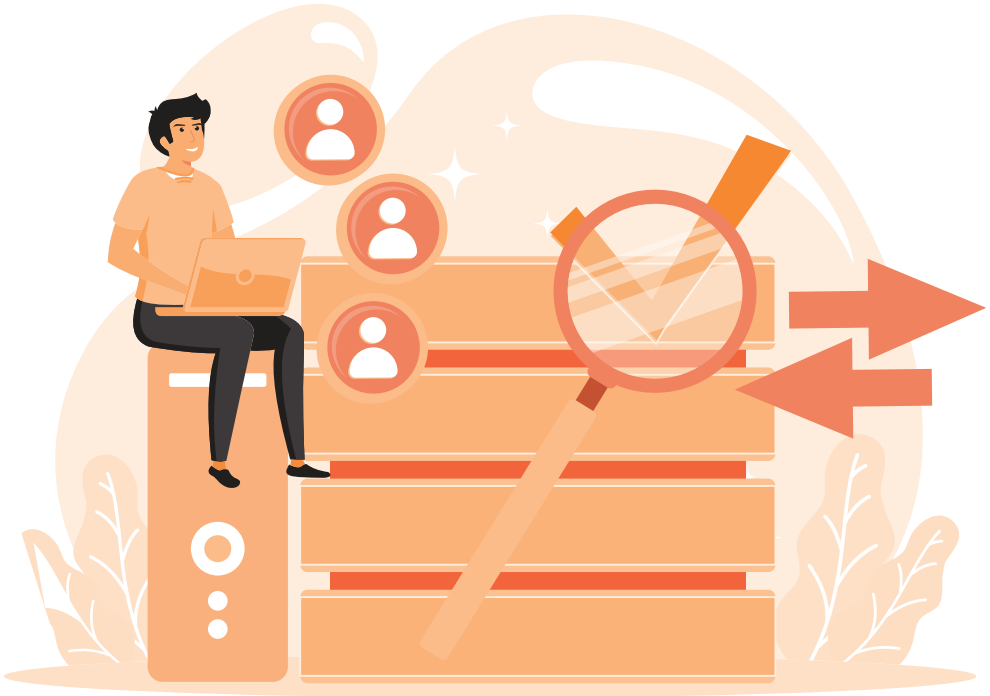
Almost all data represents some level of risk, so when a business has data that they're gaining no value from, the best strategy is often to simply delete it—removing all risk of it being leaked. In today's increasingly cybersecurity-conscious world, many businesses are reassessing the cost/benefit of much of their data and concluding that deletion is the most cost-effective choice.

3. Continuously Assess New Data Gathered

To ensure data security stays relevant as its data needs change, the business must regularly assess and classify new types of data to determine and apply appropriate security controls. This is especially true in growth phases; as a business expands, so does the data it gathers, and so should the measures used to secure this data. Many organisations implement data classification to streamline this process, ensuring that data of a particular value/risk combination is handled and stored in a standardised way.

4. Regularly Examine the Effectiveness of the Data Security Strategy

Finally, for a data security strategy that stands the test of time, its effectiveness must be evaluated on a regular basis. Cyberattacks are constantly changing in nature and technology. To keep data safe, businesses must stay current with data security and cybersecurity best practices. They must regularly test and validate that their understanding of their data is correct and that their security controls are aligned and performing as expected.



CONCLUSION

Given recent headlines, data security has become a talking point for all Australian consumers. Businesses that disregard the hazards of data storage risk significant, negative and long-lasting impacts on their operations.

Data security seeks to identify all the data a business stores and processes, outlining the risks, costs and benefits it comes with so that appropriate security controls and strategies can be chosen and implemented. By first understanding the value and location of specific data types, businesses can ensure their investment in data security is as efficient as possible, reducing their risk to an acceptable level without overspending.

ignite
RECRUITMENT & TECHNOLOGY SOLUTIONS

CONTACT INFO

1300 481 179

www.igniteco.com

www.linkedin.com/company/igniteco