How could better Data Governance have helped Optus mitigate their massive data hack?

For those of you buried under a rock, or not from Australia, Optus Telecoms (one of the major telecommunications providers in Australia) recently announced that they had suffered a major data breach and customer data on something approaching 10 million customers, including some personal documents such as drivers license and passport information.

To start with, I need to advise the readers of this blog post of two things:

1. I have no insider knowledge of this hack. I'm only working from what has been reported in the media. A lot of the content in this article is speculative and will be expressed so; and,
2. My details are included in the information extracted by the hacker, so I'm personally engaged in this issue.

The key issues I will be addressing in this article are based on the following statements in the mainstream media:

- Government ID numbers such as health IDs, Driving Licenses and Passport numbers have been exposed
- More than 50% of those numbers exposed are out of date
- Some of the data belongs to people and organisation who are no longer customers of Optus and have not been for several years.
- Some news outlets have reported that the data leak came from a non-production system. This is not widely reported and may not be reliable.

With this as background, the question I have asked myself is "how could good data governance have mitigated this impact?". I won't be addressing the topic of how to stop the hack from occurring in the first place, as that's a cyber-security question that I have neither the skills nor the knowledge to comment on. However, Data Governance can mitigate the impact of such a penetration, in at least the following 3 ways.

1) Data lifecycle management

Good data governance practices include data lifecycle management, which is the management of data from its "birth" in data collection through to its "death" in archiving and data deletion. Principle 11 of the National Privacy Principles in Australia requires that organisations to which the privacy principles apply must delete or de-identify data after it is no longer needed for that organisation's business purposes.

Whilst this is a very vaguely worded deadline, it is pretty clear that sensitive personal data on people and organisations who are no longer customers (and have not been customers for some time) should fall under this principle.

A strong Data Lifecycle Management policy and set of supporting practices and tools would have archived or deleted data on ex-customers from active operational systems (production and non-production), which would have reduced the amount of personal data exposed.

2) De-identification

Good data governance practices include de-identification processes (such as data masking or tokenisation) when populating data into non-production systems. This is the practice of using modified real production data to populate development or test systems, but in a manner that does not expose actual correct personal information. There are many different approaches to this problem, including:

- **Tokenisation**, which is the process of replacing key personally identifiable values with an alpha-numeric value that stands in for the actual value. Everywhere the specific value would have been shown, the same alpha-numeric value is used, thus ensuring that table joins can still occur, but that actual values are not stored.
- **Data Masking**, which is the process of replacing parts of key information with random characters (e.g. when credit cards as displayed as XXXX XXXX XXXX 0062, the 'X's are used to mask the original values). This process ensures that the full correct values cannot be used, whilst still showing that data was populated and a portion of the correct value.
- **Data Scrambling**, which is the process of using jumbled versions of real information to create valid-looking data for made-up people and organisations. The randomness of the jumbling of real data to create the made-up records is critical to the success of this approach. The benefit of this approach is that the data still looks valid and reasonable, supporting effective testing processes.

If the Optus data breach did occur on a non-production system (which is not established at this time), then some form of Data Masking should have completely prevented personal information being exposed.

3) Clear data retention policies

The Australian National Privacy Principles have as their core focus that organisations must only use data for the purpose for which those details were initially shared, or any purpose reasonably related, except under certain specific exceptional circumstances. There are other items of legislation that will impact on the storage of telecommunications data for 2 years (the Telecommunications Interception Act of 1979 amongst others) that make this area more complex.

As I understand it (and please check with your legal advisor before acting on any information here), there appears to be no legal requirement to retain any detailed personal data on ex-customers after 2 years. It may be necessary to retain summary information for tax or financial records for a 7 year period, but this should not need to include passport, drivers license or other critical personal data.

A strong, clear statement on data retention periods, and the regular review and enforcement of this policy, could have further reduced the data available to be exposed and reduced the scale of the data breach.

Conclusion

In the absence of more detailed information about the nature of the data, the nature of the method of the hack and the data governance and data management policies of Optus, it is not possible to identify additional benefits from strong data governance, but at least these areas can be reasonably speculated about.

Next time your management asks you about the value of data governance functions, you've got some clear and compelling ways in which your area of expertise can help save your company from the costs and brand damage that Optus is currently facing.

If your business needs help with ensuring their Data Governance is robust, please contact a Fujitsu Data & AI specialist now.

Contact

Fujitsu Data & AI
+61 3 9924 3000