How identity data is turning toxic for big companies

December 4 2017, by Bhargav Mitra And Robert Mccausland

Credit: AI-generated image (disclaimer)

Google might be in trouble for collecting the personal data of its users, but many companies have a growing incentive to rid their hands of the data that users entrust them with. This is because of growing costs of holding onto it.

A major cause is the rising number of cyber attacks where hackers steal the identity information held by companies, often to sell them on to various black markets. Take the recent example of US giant Equifax, one of the top three companies in the consumer credit reporting industry. It chalked up another 2.5m identity-theft casualties to its existing toll of 143m in October 2017. The firm has suffered a steady stream of identity information loss following a cyber-attack that took place in May this year, where hackers capitalised on weaknesses in its software.

The security breach – as a primary cause – resulted in around US$4.8 billion being wiped off Equifax's market value from May to September 2017. It also tarnished its image and cost the firm's longstanding CEO his job.

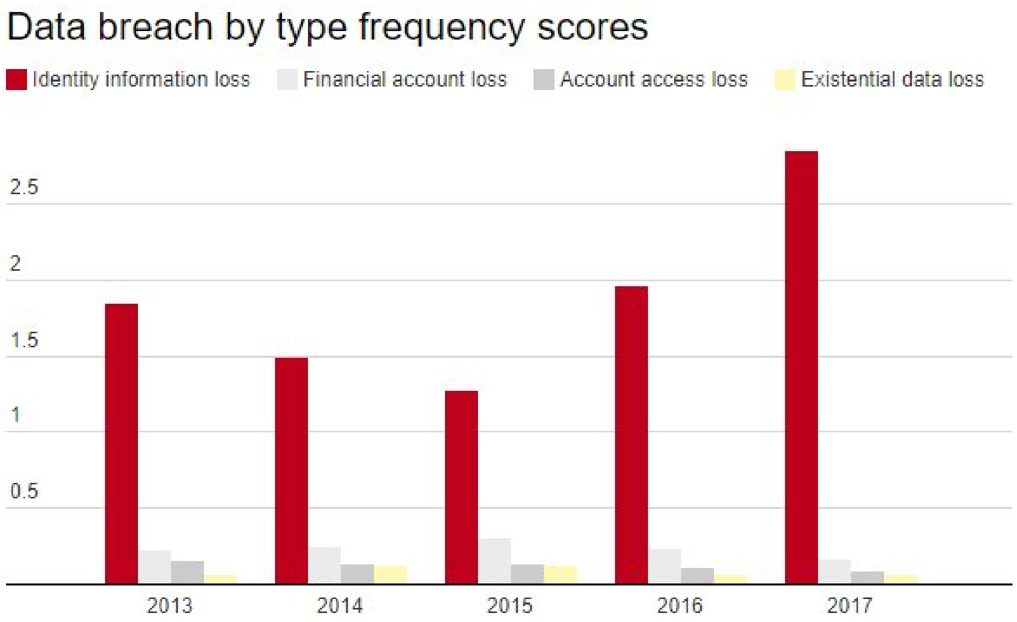
The Equifax data breach is just the tip of the iceberg. The latest Breach Level Index (BLI) published by digital security company Gemalto shows a mounting figure of around 9.2 billion data-record losses since 2013. The BLI also reports that only a meagre 368m out of the 9.2 billion stolen records were concealed from potential hackers through the use of data-encoding technology.

The rate at which valuable identity information is flying out of the control of firms is alarming – more than 3,500 records per minute. Around 23% of the top data-breaches over the past five years contained consumers' identity information – like names, dates-of-birth, addresses and account passwords. Corporate victims include big names such as Yahoo, eBay and JP Morgan Chase.

The volume and sophistication of these cyber-assaults will make top-level executives of firms that hold sensitive identity data anxious about its safe-keeping.

Growing cost of regulation

As well as cyber attacks, companies are having to contend with growing levels of regulation. As well as the regulations of the jurisdiction they are based in, when firms are spread across nations, they must also abide by international standards.


Data breach by type frequency scores

Frequency scores are calculated as the ratio of frequency of a type of loss and the sum of frequencies for other types of data loss.

Source: The Conversation | Data: Breach Live Index

The costs of this compliance in the banking sector is increasing at an alarming rate. One report has found that banks spent nearly US$100 billion on compliance in 2016 and the global spending on meeting the regulatory requirements increased from 15% to 25% over the previous four years. This skyrocketing spend on compliance leaves little room for product development.

It has now become imperative for companies holding information on EU citizens to implement control mechanisms to protect personal data in accordance with the EU's strict General Data Protection Regulation (GDPR) guidelines. GDPR, in essence, is about enhancing existing privacy protection. It will be enforced from May 25, 2018.

Non-compliance with GDPR may lead to fines to the tune of €20m or 4% of a firm's global annual sales figure – whichever is greater. Already, implementing the necessary steps to adhere to the new regulation is proving to be expensive for organisations – especially firms with diverse and intertwined business portfolios.

Some estimates predict that purchasing the technology to adhere to the GDPR standards and avoid paying the exorbitant fines will cost Fortune 500 companies on average US$1m each. Add to this the costs of permanent staffing and legal advice for this compliance, you get the picture of overall spending required for one set of regulatory standards. Clearly, the price of such compliance will compel large organisations to explore the burgeoning market of cost-effective and innovative regulatory technology.

A logical solution?

At the point where the cost of protecting identity assets outweighs the benefit of storing it, it becomes toxic for the organisation. As with any risk, companies must act to mitigate or remove it – in this case breach of identity data. When similar risks emerged around the processes for securing payment card processing, solutions focused on tokenisation of card information within an organisation to minimise handling of clear text credit card numbers. It is hard to see how a similar approach could be applied to a multifaceted entity such as identity.

However there is a potential in the application of decentralised technologies that have emerged from the development of cryptocurrencies such as Bitcoin. In these models people could choose whether a centralised entity – such as a bank, for example – would manage their identity or whether they could manage it themselves. Models for a decentralised identity are emerging with parallel developments in the creation of a decentralised web.

There are a number of challenges for both private individuals and the traditional identity provider to overcome for this move to become a reality – including wider adoption of peer-to-peer trust models. But it seems increasingly possible that the cost of cyber attacks, together with regulatory compliance, could be the nudge that drives organisations to surrender their control over vast pools of identity information.

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

Provided by The Conversation

Citation: How identity data is turning toxic for big companies (2017, December 4) retrieved 26 April 2024 from https://phys.org/news/2017-12-identity-toxic-big-companies.html