PHYS.ORG

Why and how businesses should protect against data breaches from within

April 24 2017, by Craig Horne

Credit: Unsplash/CC0 Public Domain

As we become more connected and companies hold more data, breaches are increasing, with more than 4,000 reported in 2016 alone. A statistical analysis of breaches in the United States found that 85% were conducted by someone known to the business, usually an employee or partner.

To protect both themselves and their customers, companies need to secure their data. This starts with critically evaluating what data they hold, and then securing, dumping and outsourcing it as necessary.

We can never be entirely protected from data breaches, but understanding data is the first step to minimising the risk.

Data breaches can take a number of forms

Recently, Australian startup ShowPo alleged a former employee had exported a customer database before going to work for a competitor.

A DuPont employee was charged just this month with stealing 20,000 files – including trade secrets – with the aim of selling them to rival companies in Taiwan.

Employees at Wells Fargo Bank leaked customer information, allowing criminals to impersonate customers and steal more than half a million dollars. Around US$16 billion was stolen, affecting more than 12 million consumers in the US in 2014 alone due to identity theft.

What makes these breaches worse is that once information has been stolen it cannot be easily recovered. If a thief steals a wallet, it can be returned. But this is not true for information theft because the owner still has it. Data can be replicated almost infinitely. The genie can't be put back in the bottle.

This only gets worse as technology improves, allowing for greater storage, concealment and transmission of data.

What data needs to be secured?

The first step in securing data is to do an audit. What data does the organisation hold and where is it stored? Which suppliers, customers, regulators or staff have access to it? This is important as data comes in many forms, and ownership can be quite murky.

For example, does a business own the emails downloaded onto a workers' smartphone?

Next, the type of data needs to be profiled and classified as public, confidential or secret. Not all data is created equal and some may not require confidentiality, such as sales brochures.

Customer data, on the other hand, would be classified as confidential. Especially due to tough penalties in recently passed legislation. These include fines of A$360,000 for individuals and A$1.8 million for organisations, for those that don't divulge breaches of customer data.

So companies need to identify what is high-value or strategically important information.

The next step is to decide whether any outsourcing constraints exist and are relevant to the organisation. For example, do privacy obligations prevent organisations from storing personal information in data centres outside of Australia?

Three strategies

Once the data has been sorted, there are three strategic approaches to reduce the danger of data breaches.

The first strategy involves securing sensitive information with protective fortifications. This could take the form of encrypting it.

But there are some weaknesses to this approach. Encrypted information may make workflows cumbersome, and it may not stop an insider who has been trusted with passwords. It could also lead to a false sense of security.

The second strategy involves devaluing the data held by actively deciding not to hold sensitive information. This is analogous to a retail shop hanging a "no cash kept on premises" sign in the window.

Does a company really need to hold credit card details, for instance, or could that be outsourced to a company like Paypal? Businesses may always need to protect their "secret sauce", but by methodically devaluing data they are less of a target and can concentrate on what to protect.

The third strategy involves seeking outside assistance. This may not be an option for some sectors due to regulation, but storing data in the cloud or hiring a security service provider may be wise if possible. These services often offer security infrastructure unavailable to small organisations, as well as specialists to counter a lack of security expertise inside an organisation.

But, again, there is a trade-off. Outsourcing comes with a lack of control, which may increase other risks. The Australian Red Cross found this out when an external administrator accidentally leaked the personal information of blood donors.

In the end, we can never be entirely safe. But if businesses critically analyse what data they hold, and adopt strategies in response to this, the risk of an insider attack can be minimised.

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

Provided by The Conversation

Citation: Why and how businesses should protect against data breaches from within (2017, April 24) retrieved 26 April 2024 from https://phys.org/news/2017-04-businesses-breaches.html