DID YOU REALLY SAY "YES" TO THIS?

3rd party access to your data: what you should know

Last week, a marketing and communication company was hacked. Not headline news in itself, but the company was also a third-party providing the Commonwealth Bank Health Fund (CBHS) with marketing services. As a consequence CBHS members had their information stolen. The hack resulted in CBHS customers' names, suburbs, and dates of birth, postcodes and email addresses being stolen. CBHS customers have since reported receiving unsolicited emails from suspicious email addresses, some containing the customer's personal information, and demanding payment.

A colleague of mine belongs to a car club here in QLD, and was recently informed that his personal information had been compromised when the club president's personal computer was hacked and infected by ransomware. The president had downloaded a membership spreadsheet onto his personal computer from the club's (more secure) database, which was subsequently stolen when his personal computer was compromised.

These are examples of third-party vulnerabilities that we seldom consider when assembling our online security strategies. One thinks of data security as primarily the need to secure one's own data via one's own systems and computer. Having heeded the many cautionary tales of online information theft via phishing emails and malware we spend (or should) time and resources to protect our own systems and information. We make significant investments in anti-spam, and virus protection programmes, and are vigilant when it comes to deleting (and not clicking on) unsolicited emails.

But, as we have seen in the above examples, not only is physical and digital security essential in this endeavour but also a detailed audit of the suppliers and associate companies who may at some point have or require access to some or all of the information in the function of providing a service to the original entity. It is evident any entity a company does business with can make them vulnerable, and as a result companies must make security a top criteria when choosing the partners

and suppliers with which they'll do business. When dealing with an institution that requires your personal information you have a right to ask what outside parties have access to that information, and what your recourse is if those third parties are vulnerable to hacking and your information is stolen.

This degree of third party scrutiny applies as much to our own personal online security as it does to larger institutions. Think of the many times in a week, or a month, where you are required to share some of your personal contact information, in some cases a driver's licence, physical address, names and ages of children etc. Think of the myriad of forms and applications we fill in. Everyone from doctors, schools, magazine subscriptions, competitions and health clubs to raffle tickets, retail complaint procedures and loyalty programmes. Then extrapolate how many other organisations and people have access to those databases for seemingly justifiable reasons and one develops a sense of a widening, and increasingly less secure, sphere of your personal information filtering outwards.

There are two key ways to ward against this type of information creep:

1. **Share as little as possible**. Is it really necessary that a doctor have your driver's licence or credit card number on file? Does buying a raffle ticket require anything more than your cell phone number?
2. **Ask questions:** Enquire who else has access to this information? What procedures are in place to screen third parties and what is your recourse if your personal information is stolen from the original institution?

In this age of sophisticated social engineering scams, mass online marketing efforts and identity theft personal information is like gold. Be aware of the information you share, be cautious of who you share it with and never forget all the other entities that could have access without you ever knowing about them.

By Johann Koelmeyer (CEH) - Cyber Security Engineer