Making privacy core business

Supply chain privacy risk management

21 December 2021

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000, Australia

Supply chain risks crystalizing – mitigating and managing the privacy risks

In the media we hear more and more news about ransomware attacks particularly targeting suppliers to which other businesses outsource some of their operations. Whether it is human resources, payroll, courier, accounting, legal and management services or even cyber security functions. These suppliers are increasingly vulnerable. Hence, selecting your suppliers carefully and doing the privacy due diligence is critical to mitigate risks and manage recovery faster should your supplier be the unfortunate target of a ransomware attack.

Indeed, in the most recent Notifiable Data Breaches Report, the OAIC reported that it received 446 data breach notifications for the period January to June 2021, with data breaches arising from ransomware incidents increasing by 24%, from 37 notifications in the last reporting period to 46. This is despite it being difficult to assess whether ransomware attacks have caused unauthorised access to, disclosure of or loss of personal information.

This year, Privcore worked with a number of suppliers to check on their privacy posture. From our practical experience, key focus should be given to the following:

1) Review contracts with suppliers and check against what actually happens in practice

Whilst supplier contracts are a great starting point, these are often drafted by lawyers well removed from the operational action, or have been drafted so long ago that with the rapid technology change occurring every year they eventually become no longer fit for purpose. Making sure contracts reflect operations and implementation of services is necessary so they are fit for purpose.

With regulatory assessment and notification obligations around the world required when a reportable privacy incident occurs, it is critical to be clear before incidents arise, which party (you or your outsourced supplier) is responsible for assessments and notifying regulators and/or affected individuals. Some regulators have very short lead times for reporting and notifying, so trying to figure out responsibilities in the heat of the moment should be avoided.

2) Work out what your suppliers can potentially do with your customers' data

Businesses and governments collect personal information about people and generally must advise the purposes of that collection and can only use it for those purposes, unless certain exceptions apply. However, whether those restrictions flow downstream to your suppliers is not always clear, particularly where suppliers are collecting your customers' personal information on your behalf. Make sure that your suppliers limit their data collection practices to suit your needs and purposes only in relation to your customers. Some low-cost outsourced service providers' business models have been known to rely upon revenues generated by monetising the datasets they collect.

3) Find out how long your suppliers are retaining your customers' data

Sometimes supplier contracts address this and stipulate that the data should be deleted or destroyed on termination of contract. However, what happens when your contract is well over 5, 10, 20 years old? Do your suppliers still have all that data? Be very clear from a policy perspective how long your suppliers should actually retain your customers' data and when old data needs to be deleted or destroyed. If you don't, in the event of a reportable privacy incident, your customer notification list will just keep on growing as more data accrues. If you don't need the data, get your suppliers to delete it and obtain assurances of destruction.

About Privcore

Privcore's team with 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a Superstar of STEM in 2021-2022 and a privacy professional practising since 2001 founded Privcore. She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.