WHITE COLLAR CRIME - JAPAN

Cybersecurity in Japan: being aware of your business partners' risks

24 February 2020 | Contributed by Nagashima Ohno & Tsunematsu

Introduction
Background
Security measures covering related companies
Expected damage
Countermeasures

AUTHORS

John Lane

Munetaka Takahashi

Introduction

A recent high-profile theft of hard drives containing sensitive personal data has highlighted the need for companies based in Japan to ensure that their cybersecurity measures include processes for:

- disposing of personal data that has been entrusted to them; and
- reviewing their security controls regarding business partners who may come into contact with personal data.

Background

Over a nearly four-year period beginning in March 2016, an employee at an IT recycling company in Tokyo stole nearly 4,000 data storage devices (including hard drives, solid state drives, USB drives and SD cards) that were destined for disposal and sold them through the Yahoo! and Mercari online auction sites in Japan. The thefts went undetected until a buyer realised that a number of hard drives which he had bought contained sensitive personal information that had been entrusted to the Kanagawa Prefectural Government.(1)

The Kanagawa government had leased its computers from an IT leasing company, which periodically replaced the hard drives. There was a clause in the contract between the Kanagawa government and the leasing company which stated that old hard drives would be disposed of in a manner which would make data recovery impossible. The leasing company outsourced the disposal of old hard drives to Broadlink Co, an IT recycling company.

Broadlink disposes of nearly 1 million items a year for approximately 10,000 companies and government departments, including banks, courts and the Ministry of Defence. Approximately 70% of storage devices have their data erased, while roughly 30% are physically destroyed. Broadlink seems to have tracked the former, but not the latter.

The leasing company sent 18 hard drives that had been used by the Kanagawa government and contained the personal data of Kanagawa residents – including names, addresses and tax records – to Broadlink. The hard drives had been formatted before they were provided to Broadlink; however, this did not completely remove the data. A Broadlink employee who was responsible for erasing and destroying the hard drives misappropriated the 18 hard drives formerly belonging to the Kanagawa government and subsequently advertised them for sale online.

Subsequently, an individual who owned an IT company bought nine of the 18 hard drives. When he went to use them, he discovered that they contained data that had not been encrypted and, through the use of specialist software, he was able to identify the data as having come from the Kanagawa government.

The Broadlink employee who had stolen the hard drives was arrested in early December 2019, after being recorded by security cameras stealing a number of further items. When questioned by the police, the employee said that he had stolen the hard drives and other items "nearly every day as it was easy to do so".

By late December 2019 the Kanagawa government reported that all 18 hard drives had been recovered and that none of the personal data contained on the devices appeared to have been leaked

further. The Ministry of Defence and the Supreme Court, which also use Broadlink's services, stated that their data had either been permanently erased before the hard drives were provided to Broadlink (in the case of the Ministry of Defence) or that they had received confirmation that their hard drives had been destroyed (in the case of the Supreme Court).

Security measures covering related companies

Even though this case involved traditional physical theft, it is a timely reminder of the need for companies and organisations to have robust cybersecurity measures in place that extend to the third parties with which they do business.

In November 2019 the Ministry of Economy, Trade and Industry and the Information Technology Promotion Agency published the Cybersecurity Management Guidelines Ver2.0.(2) The guidelines list a number of key principles of cybersecurity management, one of which is that comprehensive security measures are necessary not only for companies themselves, but also for companies' business partners, including suppliers and outsourced service providers. The first step is to identify contractors with cybersecurity risks that are not controlled adequately and then assess these risks. (3)

The importance of considering risks created by business partners and suppliers is highlighted by the fact that the Information Technology Promotion Agency ranked the emergence of attacks exploiting supply chain weaknesses for the first time in the 10 major security threats for organisations in 2019.

Expected damage

Many companies in Japan have been slow to recognise the need for comprehensive cybersecurity measures. Typically, some of the justifications given include the difficulty in calculating the returns on digital security expenditure. However, this is slowly changing as companies realise the risks of not properly investing in this area. The major risks for corporates if personal information is improperly disclosed include:(4)

- compensation for damages;
- the cost of the investigation and response;
- loss of profit;
- penalties from regulators; and
- impact on share price.

Compensation for damages

Japanese law requires companies to compensate individuals whose personal information has been disclosed improperly. A data breach at Benesse Corporation in July 2014 provides some guidance in relation to the amount of damages a company may face after a customer information leak. An internal investigation by Benesse found that roughly 28.95 million customers were affected by the incident. In response, the company voluntarily offered cash coupons of Y500 to each victim. In addition, on 27 June 2019 the Tokyo High Court ordered Benesse – which had been entrusted with the management of customers' personal information – and one of its suppliers responsible for information management, to pay Y2,000 per person in damages to a small group of claimants. On 6 September 2019 the Tokyo District Court ruled in a related case that Benesse must pay Y3,000 compensation per person to another small group of claimants.

The courts will consider the sensitivity of the information that has been leaked when calculating damages. As information leaks typically affect a large number of individuals, the total amount of compensation awarded as damages tends to be significant even if the per person amount is relatively low.

Cost of investigation and response

The cost of outside experts, such as lawyers and forensic accounts, who assist a company in responding to the improper disclosure of personal information can quickly become significant. Depending on the gravity of the breach, the company may need to set up a call centre in order to deal with enquiries from, and provide information to, victims.

Loss of profit

Part of a company's operations may need to be immediately suspended following the inappropriate disclosure of personal information, and the suspension may need to continue until robust countermeasures can be put in place to mitigate the risk of any further leaks. This will often adversely affect sales and profits.

Regulatory penalties

If a company is found to have leaked personal information, the Personal Information Protection Commission may order the company to take necessary actions to rectify the violation. Parties

(including representatives of a corporate body) who violate an order risk a custodial sentence of six months or a fine of up to Y300,000.

Companies in Japan that also have a nexus to jurisdictions with stringent data protection laws – such as the European Union and California – may also be exposed to penalties under relevant legislation outside Japan.(5)

Impact on share price

According to a report from the Japan Cybersecurity Innovation Committee,(6) companies in Japan that have leaked personal data have typically had 10% knocked off their share price, and their net income has, on average, declined by 21% year-on-year.

Once companies understand the abovementioned potential consequences of data leaks, it becomes difficult to justify ignoring the threat or insufficiently investing in appropriate measures to mitigate risk.

Countermeasures

While it may be impossible to completely protect against the risk of data theft, the following are important measures that will help to mitigate risk:

- increasing employee awareness, including through appropriate training;
- implementing robust security measures and ensuring that business partners also have appropriate measures in place; and
- considering best practices from the market.

Employee training

Training for employees on the appropriate way to handle personal information is necessary. While perhaps it is unlikely that this would have prevented the thefts in the Kanagawa government case, the Broadlink employee who stole the hard drives did claim that he had no idea what kind of information the hard drives contained.

Management must actively implement employee training programmes concerning cybersecurity measures and cannot simply assume that employees are aware of the myriad risks or that they will do the right thing if an incident occurs.

Robust security measures

Companies must check their own cybersecurity measures, but also be aware of those of their business partners. Part of the reason why Benesse paid significant compensation was because it had lacked the appropriate controls to check whether its business partners' security software was effective.

As it becomes increasingly important for companies to do business only with suppliers, service providers and partners that have appropriate cybersecurity measures in place, being able to demonstrate these kinds of robust control will be a comparative advantage when pitching for business.

Best practice

Companies should monitor developments in the market as the risks in this area continue to evolve. It can be particularly helpful for companies to review instances of security lapses at other companies in order to 'stress test' their own controls.

For further information on this topic please contact John Lane or Munetaka Takahashi at Nagashima Ohno & Tsunematsu by telephone (+81 3 6889 7000) or email (john_lane@noandt.com or munetaka_takahashi@noandt.com). The Nagashima Ohno & Tsunematsu website can be accessed at www.noandt.com.

Endnotes

(1) Kanagawa is a prefecture neighbouring Tokyo.

(2) Available in Japanese here.

(3) Item 9 of the guidelines outlines specific measures (available in Japanese here).

(4) Available in Japanese here.

(5) See, for example, the General Data Protection Regulation or the California Consumer Privacy Act 2018.

(6) Available in Japanese here.