DPO Connect May 2016

Managing Personal Data Breaches with C.A.R.E

In this highly-connected day and age, personal data breaches can happen to any organisation. This is why organisations should always have a data breach management plan in place.

With more and more personal data being collected and stored in the digital format in an increasingly connected world, savvy organisations know that they should not only take steps to prevent data breaches, but to also be ready for them if and when they occur.

Personal data breaches can happen in various ways. This includes malicious activities such as hacking or theft of electronic storage devices, human errors such as accidental disclosure to an unintended recipient via email or improper disposal of devices containing personal data, and computer system errors where errors or bugs in programming code render the software vulnerable to unauthorised disclosure.

"Personal and sensitive data have always been the target of criminals due to the value they bring," says Mr Alagu Karuppiah, Head of Information Technology Department at Diners Club Singapore. "As the world becomes more intertwined with Internet of things (IoT), we foresee that cyber security incidents and data breaches will increase in the future."

This concern is shared by Mr Tan Boon Chew, Data Privacy Officer and Head of Regulatory Compliance and Assurance at AIA Singapore (AIAS). As a life insurer, AIAS is the custodian of policy records belonging to over one million customers. These records contain a multitude of personal data such as customers' NRIC number and date of birth, and are stored in digital format for ease of administration and processing.

"With increasingly sophisticated methods in data theft, it is important to protect and secure these personal data against intrusion," he says.

Consequences Of A Data Breach

A personal data breach can exact a high toll on an organisation, not just from a financial standpoint but also in terms of reputational damage.

Mr P K Raman, Chief Information Officer at Standard Chartered Bank Singapore, shares findings from the 2015 Cost and Data Breach Study conducted by Ponemon Institute, which pegged the average cost paid for each lost or stolen record containing sensitive and confidential information at US$154.

More serious than that, however, is the potential fallout in terms of customer trust and confidence.

"For the bank, our most valuable assets are trust and reputation and we need to uphold these vigorously," says Mr Raman. "Losing customers' trust will damage corporate reputation and can in turn lead to loss of customers and business. Moreover, banking is a heavily regulated sector and we have to comply with all regulations or risk facing enforcement actions."

Building and protecting trust is also an important business imperative for the insurance sector. "The insurance business is built on trust as we deal with customers' personal and sensitive information, such as their medical history, claim details and financial data," says Mr Tan. "Hence, a major breach on personal data would significantly impact an insurer's reputation, brand and market value."

Besides these business considerations, organisations that fail to safeguard personal data may also be subject to enforcement actions by the Personal Data Protection Commission (PDPC).

Under the Protection Obligation of the Personal Data Protection Act (PDPA), organisations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Penalties for breaching the PDPA depend on numerous factors, such as the seriousness and impact of the breach, the immediacy and effectiveness of corrective actions taken to address the breach, and whether the breach was caused by the organisation deliberately, wilfully or out of negligence.

Minimising The Impact

Prevention is always better than cure. However, an organisation should also have in place a data breach management plan so that it can respond swiftly and effectively to personal data breaches.

While Diners Club Singapore had worked with an audit firm to develop its policies and operating processes for data breach management, Mr Karuppiah shares that there are many reliable sources of information that can help organisations build a data breach management plan, such as the resources found on the PDPC website.

PDPC's Guide on Managing Data Breaches points out that organisations may consider adopting the CARE model when developing a data breach management plan. The acronym CARE stands for containing the breach, assessing risks and impact, reporting the incident and evaluating the response and recovery to prevent future breaches (refer to box).

Putting The Plan To The Test

Having a data breach management plan itself does not suffice; it has to be tested regularly to ensure that it is effective, says Mr Karuppiah. This can be done alongside an organisation's business continuity planning.

Testing may involve putting a case study through the various stages of breach management to see if the plan works. However, this cannot be a one-time effort, he adds. "Incident management is a continuous learning process. The organisation has to adapt and change with the environment and situation."

At Standard Chartered Bank, its data breach management plan is also constantly tested and revised in line with industry best practices, says Mr Raman. "This helps ensure that if a data breach happens, we can act promptly and appropriately to identify the issue, minimise the impact, recover, and restore the confidence of our stakeholders quickly".

Getting Senior Management Involved

Another point that was highlighted by the organisations is the importance of involving senior management in data breach management.

Having support from the top and a culture of ownership are essential in developing a good data breach management plan, says Mr Tan. This will help ensure that critical components of the plan such as an effective reporting system, lapse treatment and remediation processes are well embedded within the organisation.

One suggestion would be to have the incident response committee spearheaded by the senior management. Key stakeholders that oversee the plan should also recognise that the plan is not intended to be static and must be refined along the way for continuous improvement, he adds.

Conclusion

Due diligence, trained staff, regular audits and reviews of systems and processes are essential in ensuring the security of personal data. However, prevention alone is not enough. Organisations also have to be prepared to deal with data breaches when they occur by putting in place an effective data breach management plan.

As Mr Karuppiah says, it should not be a question of "if" but "when" a data breach will occur. "With a tested breach management response plan, an organisation will be better able to minimise the impact of a breach by engaging its legal, insurance, public relations, technology and management among other stakeholders, in a timely manner to save its reputation and business."

Data Breach Management And Response Plan

1. **Contain the breach – act as soon as you are aware of a data breach.**

2. **Assess risks and impact – determine the severity of consequences to affected individuals and the steps necessary to notify the individuals affected.**

3. **Report the incident – notify individuals affected by the breach and inform PDPC at info@pdpc.gov.sg with the email subject "Data Breach Notification" or Tel +65 6377 3131**

4. **Evaluate the response and recovery to prevent future breaches – review the cause of the breach and evaluate if existing protection and prevention measures are sufficient to prevent similar breaches from occurring.**