LeadingLines
NOVEMBER 2019
JOYCE A TAN & PARTNERS

FIVE THINGS ABOUT HANDLING DATA BREACHES

Introduction

A popular modern nightmare scenario goes something like this: you are the Data Protection Officer of company X, and cyber-attackers have infiltrated your customer database. Financial and sensitive data have been extracted.

The storm is coming. Regulators will want to get into your records and your systems. Customers might want to get out. The media will want answers. Lawsuits may be looming over the horizon.

This article covers 5 points, distilled from experience, to help you think through what is needed in the thick of the storm.

One: Dealing with what you don't know yet

The discovery of data breaches is a forensic fact-finding process. Information will come in instalments. Early intelligence may be wrong.

Establishing what actually happened takes time and professional care. The priorities will be to figure out what the scale of the breach is, whether there are false positives, what is the data compromised, and what is the likelihood or severity of harm.

Two: Speed of command, not chain of command

Establishing a crisis team, a reporting chain, and getting the right people involved – these are all crucial steps.

However, even with a chain of command established, it may be necessary to leapfrog a chain of command to get a quick resolution. Information may need to go up and across to all team members earlier rather than in sequence. When every minute counts, team members may need to be alerted, and be on standby.

Three: Own the remedy, if not the breach

In one particular breach, a team member in one organisation was reluctant to escalate information concerning a breach for fear of the amount of the work that would ensue. He correctly anticipated the volume of work that followed, but the time lag in reporting that result certainly did not help.

He did not, in short, own the remedial steps entrusted to him.

Ownership also begins with management. One clear sign of ownership is whether you have made the effort to prepare your organisation in advance.

Four: What to say, when to say and how to say it

Prematurely making disclosures only to have to double back and correct yourself can cause unintended complications down the road. Have you obtained sufficient certainty to give the statement you plan to make?

Giving some thought to when information can be released, and to whom, is important. Ask yourself:

- Is the disclosure timely and on the right forum?
- Have you considered your disclosure obligations to regulators?

- Have you briefed to your management?
- What other statements to stakeholders are needed?

Notices or harm-preventing disclosures to customers or affected individuals may be key. For example, telling someone to change their passwords in the wake of a freshly discovered breach in a timely manner may help prevent loss.

Also a big one: is your legal counsel involved, and does everyone understand what legal privilege means?

Legal privilege might have important variations in different countries but generally the idea is that certain disclosures to your legal counsel does not need to be disclosed. If anything, this should encourage early engagement of your legal advisers.

Five: Clean up begins even before you own up

Remediation is not something that has to wait for all the dust to settle. Taking risk mitigation steps or rectification early, even as a breach unfolds, may be an important mitigating factor to some regulators.

Steps that do not have to wait include:
- Preserving evidence,
- Shutting down / eliminating security vulnerabilities,
- Recovering lost data,
- Instituting an internal investigation,
- Planning for the next breach.

When the time comes to take responsibility in the proper forum, approaching it as a responsible organisation that did everything it could to make things right is often one saving grace you want to be able to point to.

Conclusion

Perhaps one of the most important principles to consider is one we have not discussed:

Do not wait for a breach to happen to be prepared.

Ask yourself:
- Do you have a crisis team ready go into action?
- Is every role in the team rostered?
- Have you built a process flow in advance?
- Do you have tools on hand?
- Have you kicked the proverbial tyres and road-tested scenarios?

Addressing these questions now, not when a breach is happening, will help you get through the storm.

This article was first published on *www.dataguidance.com* on 24 October 2019.

CONTACT

For more information, please contact us at **all@joylaw.com** or at +65 6333 6383
Joyce A. Tan & Partners LLC
8 Temasek Boulevard
#15-04 Suntec Tower 3
Singapore 038988
www.joylaw.com