databreachresponseplan.com.au

A Division of Accountable List Brokers A.B.N. 37067481485

Prelude

I welcome you to utilize this document as a framework to document your own Plan to handle the unpalatable yet highly unavoidable instance, when "mad panic" hits the Office when you and your people release something has gone seriously wrong and you don't know how big that issue is....

.....And it's not something that will go away, with the "big stick" approach now being taken by the Government to ensure you are doing your best to avoid this in the first place.

For a couple of years we have been following the new Law probability.....Internationally it's the "norm" and we have all heard about the major cover–ups for years from Big Companies (until a whistle blower spills the beans.)

Well folks, it's coming here now and don't even think about covering anything up...the personal fines on Companies and their Directors can make it a very bad day, in addition to the drama of a data breach.

However, whenever we looked into getting some information to create a responsible Plan, as we also need to comply with the new laws, all we could find was Corporate waffle.....
with plenty of clip-art pictures pushing their particular Agenda, but nothing Holistic to the big picture...let alone something offered at no-charge that takes as much as we have noted here.....
.
.....Like the immediate impact of sales that won't happen if you have lost your customers confidence,
.....or the demoralising effect on middle level staff, who see chaos around them, the blame game starting and they think "I'm net getting paid enough to put up with this crap!"...and then leave.
So what happens with the Role they had.....try hiring replacement staff during this great drama....it's another issue you don't need, especially if they are followed by others!

So let's leave the Negative and see what you can do...

THIS document will be immensely helpful in you getting your Plan together "90%" quickly, with ongoing tweaks....so you will be ready...and *Seen as ready to your Staff, Suppliers and Customers!*

Our aim in compiling this Guide, is to allow you to "pre-empt" an almost inevitable occurrence, enabling rapid notification to those on your databases, which would involve a logistical and financial impost on your Company and personnel, before the issue arises.

According to the Breach Level Index more than 3 million records were stolen every day across the globe in 2016 alone. That's a total of 1.4 billion data records either lost or stolen in one year – an increase in 86% from 2015. In the last couple of years, this has grown immensely. In Australia, the Ponemon Institute estimates that a single data breach costs a company, on average, $2.64 million. Each lost or stolen record costs $142. So here's the bottom line: data breaches are expensive and they're becoming increasingly common. It's no longer a question of "if" your company will be breached, but "when".

The Official Government position…

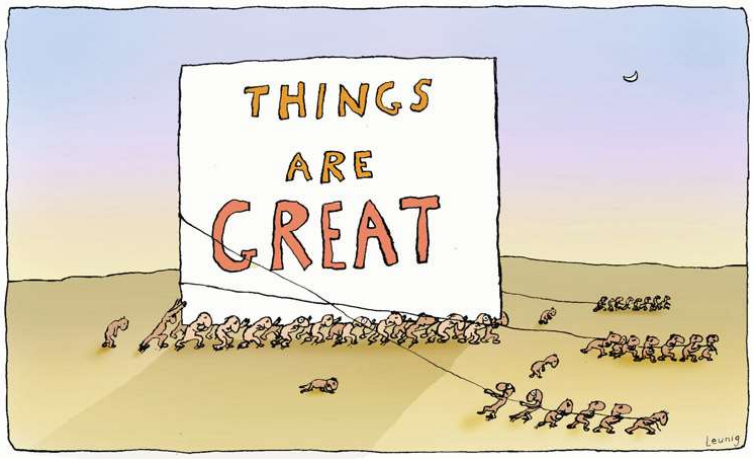
A Data Breach Response Plan: What It Is and why you need one……..
A data breach response plan is framework for managing and mitigating the impact of a data breach….organising your response efforts; it sets out the roles and responsibilities for people within your organisation tasked with managing a breach.

There are several reasons why you need a data breach response plan:

1. It will help meet your obligations under the Privacy Act. As a company, you're obligated to take reasonable steps to protect any personal information from misuse, interference and loss as well as un-authorised access. Those "reasonable steps" likely include having a data breach response plan. See Addendum 1 …last page…to see if you have to comply.
2. The Notifiable Data Breaches (NDB) scheme requires organisations to notify individuals if they've been affected by a serious data breach. Having a data breach response plan will make it easier to adhere to the NBD scheme and avoid fines for non-compliance.
3. It helps protect your assets. A data breach results in the loss or exposure of your company's more important asset – its data. But it can also result in substantial reputation damage, fines, legal bills and loss of future profitability; ***research has shown that 1 in 5 consumers will avoid doing business with companies that have suffered a data breach***. Apart from stopping additional loss you can maintain a high standard of customer service and transparency (which, incidentally, has the biggest impact on your company's reputation in a crisis).

Framework

Stage One of Three…the BEFORE



1) Know where you process Personal Information

This all sounds pretty logical until you look into it. Primarily, Businesses have "historical " data such as past and current clients which may be under an Accounts Dept. umbrella but I daresay Sales or Marketing have some information on current clients plus prospects. And some of that

information goes back many years, some with phone, some with email, some overlap between files...so it's already looking a bit fragmented. And how up to date is that historical data?...with one in 5 moving every year it highly out of date...and can you imagine the logistics to try and contact them and the huge wastage?...that's something we can solve for you..
At ALB, we can provide you a Delivery Audit within a couple of hours, showing where your database contacts have moved or died...and what you would spend wastefully contacting them when a Breach occurred.

Let's also see who else has Data...the IT Department, Despatch Department (how secure is that?) your salespeople who may have purposely downloaded it to their laptop or phone to use a reference point....if they have "personal" information too, then you are the one responsible for their actions. How safe do you think that data is?...it isn't!!

2) Understand the full lifecycle of Personal Information

The issue is most data is held in a number of sites within a Business, some overlapping and it's doubtful that you know who has got what...and the ages of that data and the actual details held in the form of Bank Accounts, passwords, Date of Birth, Credit Card numbers...so an audit is required to work that out, perhaps remove historical data with personal identification from on-line access (backed up elsewhere for access) so the amount of information that may be well out of data cannot be hacked or "borrowed" by other personnel.

A policy to document staff access is essential so at any one time, you know who has this information in case it has to be rapidly actioned. Don't forget any external companies like processing houses who may also have this ...get them to reply in writing they have deleted it.

3) Determine your ability to 'Anticipate' an incident

From the information collected above the next step is to conduct a risk assessment against how you process personal information. From the minute that information enters your control by the client filling it out on-line or it being key entered by your staff, you need to know where it's going and how much of the personal information is required by each Department.

Of course we always recommend "seeded" or dummy names are also included to monitor if the information is misused

If your in-house Company database is rarely contacted or perhaps it's held within an Accounting Package as "Historical data" then who knows how many of these past clients have moved, passed away, changed phone number...and your only option may be the substantial cost and time to organise a letter to be sent to ALL of them.

This is where our Services, over 30 years, can enable that database to be brought up to speed.

We have direct mainframe access to the most substantial Residential (and for that matter, Business) database in Australia. It's possible to match up your records to a current address, see who has moved, changed numbers, deceased and in many cases, add Privacy Compliant Email information.

The result...you now have your information at the most recent deliverable standard....and you have the option to also contact many of them by SMS and Email (the only Commercial database where you can do this) so the message can get out much cheaper and quicker than Postal Mail and obviously much sooner.

A XLS Report can be provided to you at a minimal cost to summarize your database and also a cost comparison of updating it as opposed to utilizing the existing information as it stands.

This can be done within a few hours and we guarantee it will be far cheaper and hugely less wasteful of resources than sending a letter to many people who will never get it.

4) Determine your ability to 'Prevent' an incident

Access the effectiveness of your information security controls...simply put, this is your front end anti-spam, anti-virus etc firewall provisions. All pretty obvious to try and stop unauthorised access but a key issue is 40% plus of all data breaches are caused by In-house staff who DO have access...whether they download something they shouldn't or in a vindictive mood, all you can do is have policies that all staff individually sign and then your plan is put in place to minimize and control the situation should the breach happen.

Then run through a scenario of a Data Breach...are the systems working?...are the people working? Do they understand a preventable Breach is in their control?

If not, now is the time to implement changes via your Prevention Plan.

5) Determine your ability to 'Respond' to an incident

Now you can document an Incident Response Plan that help you to manage a Cyber Risk Event such as a Breach, Denial of Service or Ransomware attack.

Assemble your data response team

All Department Heads responsible for coordinating your company's efforts in the event of a breach. They will play a critical role in mitigating the damage caused by a breach and execute your data breach response plan with their personnel…and be responsible for that

When should the response team be activated?

Not all data breaches require a formal response, and it is the CPO or Director's job to determine whether a breach needs to be escalated to the response tea. But how do they decide whether a breach should be escalated? Consider these questions:

How many individuals, if any, have been affected by the breach?
Is there a risk of significant harm to these individuals?
Was the breach caused by a breakdown in company process, procedure or security protocol?
Could there be legal, financial or reputational ramifications?

If the answer to any of these questions is "yes", then the response team should be notified in writing as soon as possible. This activates the response team and your data breach response plan.

6) Document your Communications Strategy...Internal & External

Essentially the Buck now stops at the Top...since Directors are personally liable for being able to implement a Response Plan.

Of course all Senior Management have a role to play...excepting those who “bail out” and leave the Company when it becomes a problem to them...and don’t believe they wont.

The minute an issue happens, all in the chain of command should be notified and that includes the middle management and lower level staff, since all have to know about the ramifications and disruption that might now happen....this should come from the CEO since there's no time to stuff around. They should all be aware prior, in writing, of what their responsibilities are.

Most importantly, all must know there's an issue and the responsible Data Breach Team are reviewing what’s happened to work out the extent of the breach and whether it's Reportable.

7) Get help from the External experts

It takes each staff member to work together to mitigate the impact of a data breach and keep the “Business as usual” operating. They can’t do everything, so that’s why it’s important to proactively engage partners **before an issue** who can help you investigate, remedy and prevent security incidents. Initially consider engaging:

A cyber insurance partner. For data breach laws overseas, many companies have Insurance to cover the multitude of direct and indirect costs…review this as a matter of course.

A forensics partner. They conduct technical investigations into data breaches, advise on how to stop data loss, help you manage reporting and evidence gathering during an incident.

Legal Counsel. If you don’t have the resources in house, an external partner is essential. They’ll advise you on what you need to disclose to individuals and authorities and help you avoid litigation risks.

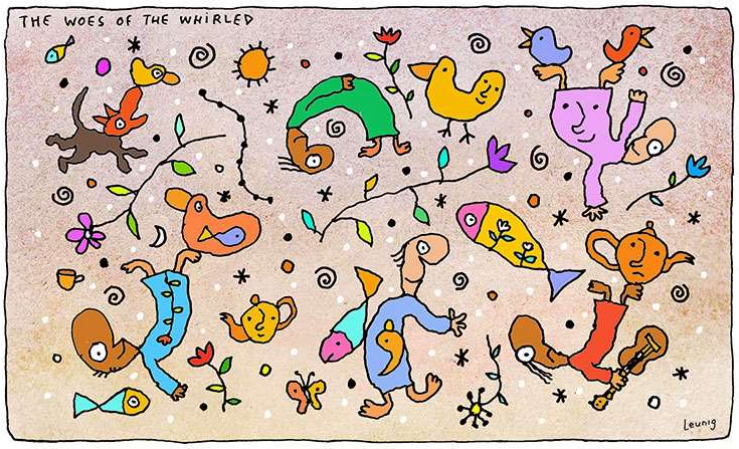
Communications partners.
Again, if you don’t have the resources of capability in-house…..... it’s worth investing in a Communication partner to help you with logistics to communicate with your customers (that’s what we do) and a PR Contact to manage highly-publicised security incidents.

We cannot impress this enough since it can go from Bad to “very worse” if the media get onto the story and a spokesperson fronts the cameras without a clear concise and confident message…..you have seen the Drama when a PR exercise goes belly up!

8) Assess your ability to Recover

Have you documented and tested your IT Disaster Recovery capabilities? Self explanatory really but a couple of Trial runs will point out where you are lacking....and how you handle this is not only relevant in a legal perspective but also to the health of your business when that Breach **does** occur!

Stage Two of Three…the DURING



9) Containment

Record the date and time the breach is discovered. Also note down the date and time your response plan is activated.

Alert and activate the Response Team. Begin with executing the response plan.

Contain the beach. Secure the area where the breach occurred and take affected machines offline. Activate the ICT incident response plan.

Gather documentation. Record who discovered the breach, to whom it was reported, the extent of the breach and any other evidence that may be of use to forensics firms and law enforcement. Interview involved parties about their knowledge and document their responses.

10) Assess your ability to maintain services

i) Evaluation

Launch the initial investigation. Begin collecting the following information. Date, time, location and duration of breach. How the breach was discovered and by whom. Type of information compromised in the breach. What personally identifiable information (PII) or proprietary information was exposed, if any. Names of (possibly) affected individuals and organisations. Carry out a risk assessment. Evaluate the extent of the damage caused by the breach to individuals and your business. Assess priorities and evolving risks based on what you currently know about the breach. Engage a forensics firm. Commence in-depth investigation into the breach.

ii) Notification

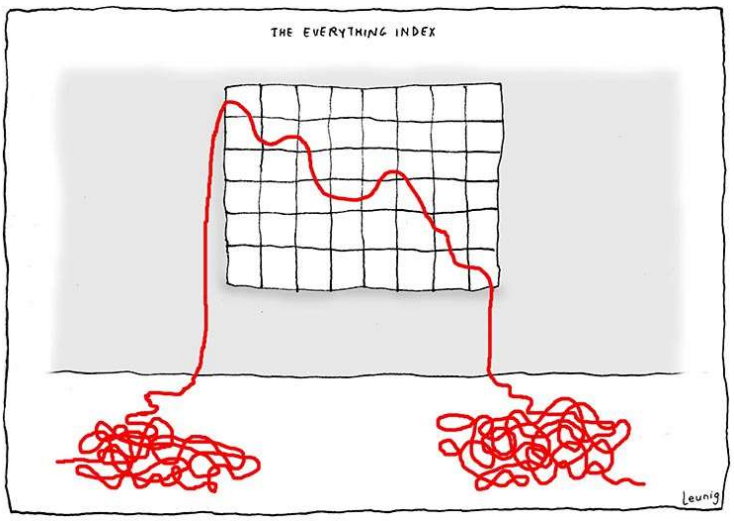
Review notification procedures. Determine who needs to be made aware of the breach, both externally and internally in preliminary stages. Ensure all notifications occur within mandated timeframes.

Notify affected individuals if there is a risk of serious harm. If there is a high risk of serious harm, individuals must be notified immediately. This can be very expensive and laborious.

Notify law enforcement if necessary, after consulting legal counsel and leadership.
Engage communications and PR teams. Activate media plans and notification protocols.

iii) Prevention
Review findings of investigation into the breach. Collate all documentation, evidence and findings for evaluation. Update response plan and other incident response plans as necessary. Make appropriate changes to policies and procedures, including information security and data management policies. Revise staff training practices to ensure staff have up-to-date knowledge of procedures and responsibilities. Evaluate the response and audit if necessary.

Stage Three of Three…the AFTER



The Upshot

Who knows about the Breach, apart from the staff, probably their Partners and relatives, the Privacy Commissioner, and your external contractors?

Maybe it's a good time to advise Clients that an issue happened but its been contained because you had an Actionable Plan, possibly the only one in your Industry to do so…then you have a Positive message…for staff too.

It's an Issue you don't want to repeat and hopefully you won't. If you minimized the downtime and expense, good for you. It's just part of doing business...anticipating issues largely out of your control. At least you are forewarned with this.

Now, let's review at the Costs that might be incurred. **How costs are calculated?** To calculate the average cost of a data breach, both the direct and indirect expenses incurred by the organisation are aggregated.

Direct expenses include:
• Engaging forensic experts to assess the nature of the breach.
• Outsourcing extra staff to support inbound enquiries, crisis team costs.
• IT costs to rebuild failed systems and networks
• The burden of notifying customer network and government.
• Legal fees.
• Remediation for customer losses (changes to banking accounts) potential damages payouts. (the law is open to aggrieved customers suing you.....frankly, it becomes a nightmare)

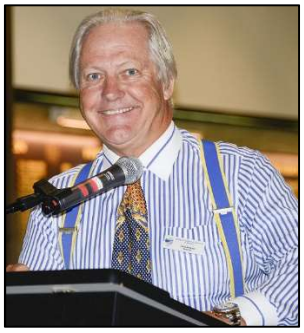
Indirect expenses include:
• In-house investigations and communication.

• The future value of customer loss, and lack of new customer acquisitions.
• Rebranding due to harm of Reputation.
• Public relations campaigns & new marketing strategies.
• Increased level of audits and Government scrutiny

Further to the financial risk of cyber security, an enterprise facing a data breach also stands to lose the trust of their customers. The Unisys Security Index Australia 2011 revealed at the time that 85 percent of Australian customers would stop dealing with an organization if their data was breached. The ramifications of a cyberattack can spread much further than a simple loss of short-term income.

About us

Again, I hope this assists you with a framework to work within....just one little element missed out can make a big difference!...***Laird***



www.databreachresponseplan.com.au is a Division of Accountable List Brokers, who have been a list broking and a marketing management firm specialising in database and production activities for direct marketing for over 30 years. Accountable List Brokers works with a broad cross-section of clients in the consumer and business markets. For details, see http://www.listbroker.com.au

Acknowledgements.....

- Images courtesy of Michael Leunig

- From isdefence.com (enquiries@isdefense.com) who allowed me to extract the “Must Do” key points as part of this Report.

Addendum 1.....

The **Cyber Security Bill** applies to organisations that have responsibilities under the Privacy Act. This includes these, where we have shown most with Contact names as a guide...

- Australian Government agencies...**Departments.....**

  Local 5532 , State 7193, Federal 3257...= 15,982

- Businesses with an annual turnover of **more than $3 million**..... 36,100 (with 10 plus employees)
  (Dealing with Consumers...ie Retail, some Services, Hospitality, Travel etc)
- Not-for-profit organisations with turnover of **more than** $3 million.... Total ??...(50,000 in total are "active")
- **Annual turnover of $3 million or less.....(some of which may be in above)**

- Clinics of General practitioners and medical specialists 16,400
- private hospitals and day procedure centres 1,840
- pharmacists 5,185
- Over 2243 other health and allied health professionals in private practice including psychologists, physiotherapists, dentists (8,500,) podiatrists, occupational and speech therapists and optometrists...
- private aged care facilities 2,500
- pathology and radiology services...300
- complementary medicine practitioners, including herbalists, naturopaths, chiropractors, massage therapists, nutritionists, and traditional Chinese medicine practitioners ....3000 plus
- health services provided in the non-government sector, such as phone counselling services or drug and alcohol services....est.200
- private schools 6,600
- child care centres 5,260
- gyms and weight loss clinics 1,369
- blood and tissue banks...est. 20
- assisted fertility and IVF clinics....est.130
- health services provided via the Internet (eg counselling, advice, medicines), telehealth and health mail order companies...est 15
- Real Estate 6,900
- Businesses that sell or purchase personal information along with credit reporting bodies….estimate 50
- TAFE's/Uni's..... 6,500 Departments RTO's 3,778

Summary.....over 112,000 Businesses plus those others Home Based / "under the radar."