Data Protection - Guidance Note

Managing a Data Security Breach

One of the rules of data protection states that "appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction." In view of this it may be prudent for organizations to have a policy in place to manage a data security breach if or when it happens. Below are some practical guidance notes which you may find useful.

There are several scenarios which can trigger a data security breach:-

- Loss or theft or data or equipment on which data is stored
- Inappropriate access controls allowing unauthorized use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- "Blagging" offences where information is obtained by deceiving the organization who holds it.

However the breach has occurred, there are four important elements to any breach management plan:-

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

1. Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage control. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following:-

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognize when someone tries to use stolen data to access accounts
- Where appropriate, inform the police

2. Assessing the risks

The following points are likely to be helpful in making this assessment:-

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

3. Notification of breaches

Informing people and organizations that you have experienced a data security breach can be an important element in your breach management strategy. However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

Answering the following questions will assist you in deciding whether to notify:

- Are there any legal or contractual requirements? At present, there is no law expressly requiring you to notify a breach.
- Can notification help you meet your security obligations with regard to this key data protection principle?
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example the cancelling of credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences, you should inform the Data Protection Commissioner

- Consider how you need to notify as over notifying could create disproportionate enquires and work
- If you do notify, use the most effective and secure medium
- Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach
- When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them
- Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.

When notifying the Office of the Data Protection Commissioner (ODPC) you should include details of the security measures in place such as encryption and, where appropriate, details of the security procedures you had in place at the time the breach occurred.

You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing “business as usual” is not acceptable. Similarly, if your response was hampered by inadequate policies or lack of a clear allocation of responsibility then it is important to review and update these policies and lines of responsibility in the light of experience.

You may find that existing procedures could lead to another breach and you will need to identify where improvements can be made. The following points will assist you:

- Make sure you know what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if you know which data are involved.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Do you store data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced.
- Identify weak points in your existing security measures and seek to strengthen them
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice
- If your organization already has a Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches
- It is recommended that at the very least you identify a Compliance Officer/Team responsible for reacting to reported breaches of security.

For more information, please refer to our Website article “Are you ready for Data Protection?” You may also e-mail us at dataprotection@bahamas.gov.bs