FTR Now

The Science of Data Breach Prevention and the Art of Breach Response

Date: March 22, 2013

Organizations should be paying close attention to data loss prevention and response in light of recent developments. Recent media frenzies over the loss of portable storage devices illustrate that individuals' fears and perceptions can cause great pressure on organizations even when the risk of real harm to individuals is remote. In addition, the risk of malicious intrusions into networks – generally associated with more grave consequences than mishaps – is increasing at such a rate that the Obama administration has ranked cyber security as a top concern.

In this *FTR Now*, we provide you with a guide that includes practical advice on the salient issues. We hope it's useful to you.

THE SCIENCE OF DATA BREACH PREVENTION

DATA SECURITY "LOW HANGING FRUIT"

It is dangerous to be too simplistic about data security, but recent headlines suggest that organizations can address 80% of their risk by effectively managing 20% of their exposure. In this regard, consider the following "low hanging fruit":

- **Mobile media.** This includes USB keys, portable hard drives and laptops. Personal information should not be stored on these devices if not encrypted.
- **Passwords.** Have a workable password rule that promotes the use safe passwords.
- **Shredding.** Do your employees know the difference between the grey bin and blue bin?

You may have a rule, but is it being enforced? What needs do employees have that are causing them to circumvent the rule? Can those needs be met in a manner that reduces the risk or is greater attention to the existing rule required? Communicate, audit and enforce.

SOME ELEMENTS OF A COMPREHENSIVE PRIVACY AND DATA SECURITY PROGRAM

Given a privacy and data security program must always be developed with a view to managing particular risks, there are few, if any, mandatory requirements. The following, however, are program elements that have been endorsed by Canadian privacy commissioners as important to achieving reasonable and duly diligent protection of personal information.

- **Risk assessment structures.** Programs should contemplate periodic, routine risk assessments and assessments that are done in response to specific events. Risk assessments should be methodical and recorded.
- **Intrusion detection and security audit structures.** The duty to monitor and audit for potential misuse is distinct from the duty to assess risk. Organizations should take advantage of available technical means to gain a very strong view of computer system use and vulnerabilities.
- **Internal transparency structures.** Privacy program elements that encourage sharing of information about risks and controls are a best practice for promoting reasonableness and due diligence.
- **Records management structures.** Good records management enables good data security because it minimizes the amount of information retained for no good reason and because it allows for records to be classified and managed according to their sensitivity.
- **Vendor selection and oversight policy.** Programs should address the risks associated with the processing of personal information by third party organizations. Considerations include: diversification mandates, vendors selection

procedures and criteria, contractual minima, consequence management and oversight.
- **Human resources policy.** Given the need to protect against the risk of employee neglect and purposeful malfeasance, privacy programs should identify and address key issues in which the protection of privacy should be considered in managing human resources. Consider hiring, orientation, supervision and termination.
- **Disposal procedures.** Disposal of records containing personal information has been the subject of great attention by Canadian privacy commissioners, who have provided relatively detailed guidance to organizations on what is required to meet the reasonableness and due diligence standard of care.
- **Privacy breach procedures.** Programs should contain a procedure that includes an obligation to immediately report incidents to the appropriate internal office and that structures the incident response process.

THE ART OF DATA BREACH RESPONSE

THE INCIDENT RESPONSE PROCESS

At some point, an “incident” involving the potential for unauthorized access to data (including data amounting to personal information) becomes a “breach” – an incident involving reasonably foreseeable harm.

The incident response process is about taking all steps reasonably necessary to appreciate and prevent foreseeable harms and about learning from the incident to improve how data is kept secure.

- **Contain.** Take immediate steps to reduce the risk of unauthorized access.
- **Investigate.** Gather evidence and determine the key facts that characterize the incident and its risks.
- **Assess.** If there has been a breach, consider whether it has been contained. Consider what is necessary to mitigate. Consider the cause of the incident and its significance to the company’s data security program.
- **Mitigate.** Share information and take other steps reasonable to ameliorate the consequences of the breach.
- **Strengthen.** Identify and plan for improvements that will reduce the likelihood of similar risks.

INCIDENT RESPONSE DOS

- **Have a plan.** Decision-making authority (and accountability) must be clear to enable decisive action in the event of an incident.
- **Have a team.** This is a multi-disciplinary problem. Legal, the privacy office and IT are key stakeholders. You will also often need IT security and crises communications expertise. Identify the key players in advance.
- **Take what appears to be small seriously.** Incidents occur frequently. Every incident will not justify the same approach and the same commitment of resources. Be very careful in the initial assessment; what looks like a minor incident may be turn out to be a big incident.
- **Beware of conflicting interests.** People in the company will protect their interests and may even hide facts. Develop a fact-gathering process with this in mind. Use a skilled investigator to conduct interviews.

INCIDENT RESPONSE DON’TS

- **Rush to notify.** You may be criticized for being slow to notify potentially affected individuals, but you will also harm your credibility because you have misappreciated the scope of a breach.
- **Be slow in investigation.** Conduct a reliable and expeditious investigation.
- **Expect perfect knowledge.** Expect to make some decisions and make some statements with a less than ideal grasp of the facts. Do your best. Communicate carefully given the lack of knowledge.
- **Think over e-mail.** Set a communication protocol for the team involved in managing the breach. Even if communications are structured to be privileged, the risks of thinking over e-mail usually exceed the benefits. Communicate facts by e-mail. Meet to discuss what to do about the facts – i.e., to plan. Use e-mail to implement your plan.

- **Give an opinion on the risk.** In communicating with potentially affected persons or the public, provide a balanced description of all material facts, including facts that tend to lessen the risk of harm. The circumstances in which you will be able to give a reliable opinion about the degree of risk will be rare.

GET READY TO ANSWER THESE QUESTIONS

From the start, examine an incident from the perspective of potentially affected individuals. Think of the questions they will have. For example:

- Was the information taken, lost or merely exposed?
- When?
- What information?
- Am I one of few or one of many?
- Anything else that informs my risk?
- What have you done?
- What are you going to do?
- Where can I go for help?

WHY LIABILITY FOR PERSONAL INFORMATION LOSS IS NOT A FOREGONE CONCLUSION

Things can seem grim when you are in the middle of the incident response process. Bear in mind that liability for personal information loss is not a foregone conclusion for the following reasons:

- **No strict liability.** The legal duty is to take reasonable precautions. Though defending your practices in hindsight of a breach can be challenging, you can meet the standard of care and still lose data.
- **Causation requirement.** If a breach of the standard of care can be established, liability only follows if the breach caused damage. It may be hard for plaintiffs affected by identity fraud to establish how the fraud caused economic damage, particularly if individual plaintiffs have been lax in keeping their personal information secret.
- **Damage claimed must be compensable and not too remote.** There is case law that suggests a plaintiff seeking damages for psychological injury must prove that (1) the psychological injury was a foreseeable consequence of the defendant's negligent conduct and (2) the psychological injury is a "recognizable psychiatric illness."

If you have any questions regarding data breach prevention or data breach response, please contact Frank Cesario at 416. 864.7355 or your regular Hicks Morley lawyer.
