How Boeing turned theft of personal information into a privacy awareness campaign

One laptop is stolen each day at Boeing on average. The company's HR Data Privacy Director **Debra Overlin** explains how the company addressed two privacy incidents resulting from such thefts and used the process to build its privacy awareness campaign.

Theft of company laptops is, unfortunately, a common occurrence in the world today and is potentially highly damaging to those whose information resides on these computers and the companies that own them.

In November 2005, before the Thanksgiving holiday, a payroll department employee's work laptop was stolen from a hotel room. In Boeing, a laptop computer is your desk. It has everything you need to do your job, as Boeing employees work predominately in virtual environments. The stolen laptop contained information on about 161,000 current and former US Boeing employees. Data included names, Social Security numbers and, for some, bank account details, home addresses, home phone numbers and dates of birth.

Privacy legislation in the USA

In the US, privacy is only regulated at the state level, and then only in some states. There is some movement at the federal level potentially to enact a federal privacy statute. Some states require that when personal information is placed at risk, such as through theft, the individual whose personal information it is must be notified. Boeing decided that rather than notifying some employees and not others, it would notify all those whose personal information had been on the stolen laptop.

The company spent a over a week determining what personal information was on the stolen laptop before notifying current employees via internal e-mail and former employees by post about the data stolen. The media and Attorneys General were then also notified.

As part of the notification process, Boeing used its internal employee portal to communicate to employees their individual status as to whether or not they specifically were impacted, what information of theirs had been stolen, if any, and that they could place a fraud alert on their credit information file. They were also advised to contact the Federal Trade Commission if they needed more information.

Boeing then paid the three major credit reporting bureaus in the US to give its employees free credit monitoring for three years. Additional call centres with extended hours were also placed into operation. On one day, Boeing received 22,000 calls, mainly from those employees affected by the theft. An internal and external website was created with FAQs, and privacy/security employees were made available to employees to answer questions.

The incident cost Boeing $1.5m to $2m, covering the cost of the credit alert services in the first year, employee overtime and printing/mailing costs to notify former employees.

Loss was the best awareness programme

A positive outcome of the loss resulted in increased employee awareness about identity theft, fraud protection and the risks in handling their own and others' personal data. It is unlikely any planned privacy awareness programme could have reached everyone as effectively.

Boeing had not felt the risk before and, importantly, had not expected employees' reactions. There were many unhappy employees with many questions, which Boeing addressed through its subsequent communication strategies with its employees as outlined above. Managers and staff necessarily took a few days to notify the many thousands of affected employees of the theft due to the time needed to identify what information was on the files, who was affected and how employees should be contacted and given support.

Lessons learnt

Trust takes a long time to build, but can be lost in the blink of an eye. Regaining trust comes from ongoing diligence with proper follow up. Education and awareness of privacy risks is vital. Employees need to take responsibility for the data they access, whether it be their own or others, and management needs to ensure that employees take proper precautions. Policies and processes created to minimise the risk of privacy breaches need to be continuously audited for compliance. Having a disaster plan in place to allow for immediate response to a privacy incident is also helpful.

Tips to minimise unauthorised exposure of data on laptops

- Remove data that is not needed;
- Encrypt data;
- Store data on a server, rather than on the laptop; and
- Secure or lock the hard drive or the laptop or both.

Second privacy incident six months later

In April 2006, a Boeing employee had a laptop snatched at an airport after briefly setting it down on the ground to put on a coat. Since the first incident had occurred, this laptop owner had deleted data that was not required and had encrypted other files. However, an old file existed in the temporary folder that was not encrypted. This file contained

The stolen file contained information on 3,600 people. It also included information on 800 non-Boeing employees. Data included names, Social Security numbers and home addresses

information on 3,600 people, 2,300 of whom had been affected in the first incident. It also included information on 800 non-Boeing employees which was related to a recent acquisition. Data included names, Social Security numbers and home addresses.

Boeing deployed the same mitigation process as in the first incident and further strengthened data security and privacy requirements, including immediate purging of data on laptops, audits to ensure encryption software was loaded onto all laptops and that mandatory training was completed. Employees were also required to sign a statement advising that appropriate privacy/security steps had been taken and thus take responsibility.

Further steps that Boeing is taking to prevent data risks:

- Ongoing desk checks;
- Disabling access levels that employees do not require;
- Removing the use of Social Security numbers to identify employees and replacing it with a Boeing identifier;
- Investigating technological solutions, such as automated scanning of data, locking hard drives and tracking laptops.

Conclusion

Prevention is better than cure. Assess your company's risks and prioritise them. After identifying risks, remove them or minimise them. Employees and management need to appreciate the value or liability of data and the risks posed when personal information is exposed to unauthorised individuals. Should your company be unlucky enough to be subjected to a privacy incident, use it to create privacy awareness and educate management and employees on privacy and security.

INFORMATION

This report is based on a presentation given by Debra Overlin when she came to Cambridge for this year's PL&B Annual International Conference.
Boeing is one of the world's leading aerospace companies and is the largest manufacturer of commercial jetliners and military aircraft combined. It is headquartered in Chicago and employs some 154,000 employees in 70 countries.

AUTHOR

Report by Annelies Moens, LLB (Hons), BSc, BA, who attended this year's PL&B conference after completing her international MBA (with distinction) at the Vlerick Leuven Gent Management School, Belgium. Prior to her MBA, Moens was Deputy Director, Compliance at the Office of the Privacy Commissioner, Australia.
E-mail a.moens@lycos.com.