Protecting what's ours

Global Privacy works to strengthen safeguards of personal information

By Susan Birkholtz

Boeing has accomplished a lot in its continuing efforts to protect personally identifiable information (PII) since two Boeing laptops containing unencrypted PII were stolen in 2005 and 2006. This information can be used to identify, contact or locate an individual; examples of PII include a person's name, Social Security number, date of birth, home address, credit card number, driver's license number or bank account information.

Immediately after each laptop theft, the company took swift measures to prevent the lost personal information of the current and former employees and retirees from being used to harm their financial standing. Affected people were immediately offered the opportunity to sign up at no cost to them for credit monitoring through Experian, a major credit bureau, to alert them to any suspicious activity. Thankfully, there have been no reports of identity theft or misuse of this data to date, and the laptop lost in 2006 was recovered, with data intact.

Perhaps the best evidence of the strides that have been made is that, although Boeing laptops unfortunately continue to be lost or stolen on a daily basis, no PII loss has recurred.

"The 2005 and 2006 incidents led us to take a close look at the processes, policies and controls related to how—and by whom—sensitive data like PII is handled in the organization and protected from potential loss and misuse," said Rick Stephens, senior vice president, Human Resources and Administration. "We knew we had to assure our employees as well as our customers that we were putting the right safeguards in place to protect the information they entrust with us. I think we have come a long way in a relatively short period of time."

This "close look" included an external audit by a world-class information security vendor to assess Boeing's privacy practices. The company also conducted an international risk assessment of privacy-compliance practices. And, to underscore the seriousness of its commitment, in 2006 Boeing established a Global Privacy Office as well as a chief privacy officer position, currently held by Deb Overlin, reporting to Stephens. Overlin works closely with Information Security as well as Shared Services Group's Security and Fire Protection organization, whose many duties include information and computing security and export compliance monitoring.

Overlin and this extended team have taken a number of corrective actions, the first being successfully mitigating the loss of PII resulting

"Each of us is personally responsible for protecting sensitive information by clearly understanding and strictly adhering to all company policies and procedures related to data security."

– Deb Overlin, Boeing chief privacy officer

from the stolen laptops. Here's a look at some of their many actions.

- An incident response procedure was updated and formally documented so actual and suspected incidents involving the theft, loss, compromise or unauthorized use of Boeing or non-Boeing information are reported promptly.
- As of 2006, any work activity associated with PII must be performed only on company premises. Downloading and saving PII to transportable devices such as laptops, PC hard drives or thumb drives is no longer permitted.
- To build employee awareness about the importance of protecting sensitive data, new training modules were introduced and others were expanded or revamped.

Boeing in 2005 introduced "Boeing Privacy Directions–Awareness," which is mandatory for managers and HR and Information Technology teammates—groups that typically need to have access to PII and other sensitive information in their daily jobs. In addition, Boeing introduced an Information Protection training module in 2006 and revamped its Computing Security and Laptop Protection module in 2007. Also in 2007, Boeing introduced training for the handling of employee personal data in the European Union.

Existing Information Security training, mandatory for employees and non-Boeing individuals with access to company computing systems and networks, is updated every year; the 2008 update has been rolled out.

- Global Privacy in 2007 identified and categorized PII users into high, medium and low risk according to their ability to access this information in various Boeing systems. PII users are subject to certain requirements based on their risk level. Employees can determine their PII user risk level and associated system names by clicking on the My Profile tab in TotalAccess. Managers can review their employees' risk level through Manager HR Services on TotalAccess.
- The number of employees with access to PII was significantly reduced. In addition, the number of applications containing PII has been cut by 75 percent.
- In 2007, all employees were required to upload Whole Disk Encryption (WDE) software on their laptops and PCs, regardless of their PII user-risk level. WDE encrypts system hard drives, thereby protecting all stored data by preventing unauthorized access to systems.
- All current and former users of employee data were required to delete any PII from their PC or laptop hard drives or move it to a secure server. To assist in this task, Information Security deployed a self-scanning tool for employees to perform a self-check to identify any residual PII.
- Global Privacy is updating PRO-98 Personal Information Protection Practices, which describes the company's employer-employee information practices related to personal data. To access Boeing Policies and Procedures, look for the POLs, PROs and Processes icon on either http://my.boeing.com (look for the Boeing Web links box in the left column) or http://inside.boeing.com on the Boeing intranet.
- An earlier update to PRO-98, consisting of the addition of "Directions for use of PII," was made in 2006, and includes information that specifically relates to the use, access, visibility, storage and destruction of PII.

LOOKING OUTSIDE BOEING

Boeing also applies the same strict requirements on partners, vendors and suppliers who perform work on Boeing's behalf. Global Privacy and SSG Information Protection have shared the lessons the company has learned with these vendors and suppliers so they can improve their policies and guarantee the security of Boeing's information.

Global Privacy also has worked with Boeing Supplier Management and Contracts to develop standard contractual language on information protection requirements for PII, and has drafted supplier/vendor requirements for notification of any data loss incidents to Boeing and affected individuals.

Additionally, between August and November 2007, an SSG Information Protection and Information Security team conducted assessments of Boeing's top 10 benefits providers to ensure they have adequate data protection practices in place and that they are meeting Boeing's expectations.

The team began assessments of another 12 suppliers on April 1; these are expected to be completed in late July. The risk potential of the remaining 55 suppliers will be evaluated to determine if additional assessments are required. Also under consideration: assessments of Boeing subsidiaries' privacy practices.

A LOOK AHEAD

Currently, Global Privacy is partnering with Information Security to make more secure the way PII users access this information. Within the next year or so, Boeing employees whose job descriptions require that they access PII will be required to use the applications and files containing this information through a secure remote desktop environment. Also in the works is a hard-drive-free device from which PII users can access this information; this route eliminates the possibility of downloading and storing PII.

While much has been done since those first laptops were stolen, Overlin recognized that even more can be done to make employee PII more secure—but employees need to do their part as well.

"Each of us is personally responsible for protecting sensitive information by clearly understanding and strictly adhering to all company policies and procedures related to data security," said Overlin.

"As we move forward, we must make these practices part of our culture by actively applying the training to the work we do each day, and by remaining informed about our company policies and resources that are available to us. I'd like to say thanks to those employees who do their part every day to keep Boeing information safe." ■

susan.l.birkholtz@boeing.com

How not to lose your laptop

As the days get longer in the United States and the rest of the northern hemisphere, everyone's in a hurry to enjoy the additional hours of daylight. But good weather can bring increased risk to protecting your Boeing equipment and Boeing information.

"It is imperative that you take a few extra minutes to really secure your company-issued laptop," said Deb Overlin, Boeing chief privacy officer. "Nothing can ruin a good evening faster than coming back to find your entire work-world has been stolen."

Here are a few common-sense tips:

- Don't leave your equipment in your vehicle parked in a public lot. Even if your laptop is locked in the trunk, the vehicle remains a target for thieves.
- Don't leave your equipment in an outside parking space overnight. Take the time to take it into your residence.
- Don't leave your gear in your locked garage. Make a habit of taking it inside your residence before continuing on with your evening. A few seconds of prevention is worth it.

Overlin noted that the loss of any portable equipment, including BlackBerrys and thumb drives as well as laptops, must be reported to Boeing Security immediately to ensure that valuable company information does not fall into the wrong hands. "This equipment is your responsibility; treat it as you would your wallet, purse or car keys," she said. "It's just as valuable."

Safe at home

There are plenty of things you can do at work to help safeguard personally identifiable information (PII). But what about at home? Here are some tips from the U.S. Federal Trade Commission on how to keep this information secure at home.

- Avoid using easily available information for passwords such as your mother's maiden name, your birth date, the last four digits of your Social Security number or phone number, or a series of consecutive numbers.
- Secure personal information in your home—especially if you have roommates, employ outside help or are having work done in your home.
- Ask about information security procedures at businesses you frequent, doctor's offices or other institutions that collect your PII. Find out who has access to the information and verify that it is handled securely. Also, ask about the disposal procedures for those records.
- Don't give out personal information on the phone, through the mail or on the Internet unless you've initiated the contact or are sure you know that you are dealing with a legitimate organization.
- Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox.
- Tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.
- Keep your purse or wallet in a safe place at work. Do the same with copies of administrative forms that have your sensitive personal information.
- If you have a home computer, regularly update your virus-protection software. Also, install patches for your operating system and other software programs to protect against intrusions and infections that can lead to the compromise of your computer files or passwords.
- Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know.
- Use a firewall program, especially if you use a high-speed Internet connection, to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.
- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password—a combination of letters (upper and lower case), numbers and symbols.
- Before you dispose of a computer, delete all the personal information it stored. Use a "wipe" utility program to overwrite the entire hard drive.