Unsung *guardians*

Information Security, an organization few people know, ensures that Boeing's data is safeguarded. And that helps keep the company working smoothly.

By Jay Spenser

Boeing's most precious asset is the unique expertise of its employees, and the information they generate is its lifeblood as an aerospace company. Maintaining competitive leadership demands that Boeing properly safeguard this information.

Fortunately, Boeing Information Security is on the job. Responsible for protecting the company's data and computing assets, this small but vital organization also ensures that company employees and their external business partners can collaborate as needed with timely, secure data flows.

With Internet-based technologies advancing rapidly, meeting this mandate is never easy for any company. In Boeing's case, the challenge is far greater because of the variety of its global operations, the scale of its data flows, and the differing computing needs and habits of its highly diverse and distributed workforce.

"Boeing Information Security is fortunate to have some of the most talented and resourceful IT professionals in the world," said Vice President of Information Security Linda Meeks, the company's chief information security officer. "As a result, our industry peers, as well as our commercial and military customers, often turn to us for advice on security issues."

CAT VS. MOUSE

Information protection is a cat-and-mouse, measures-versus-countermeasures world where things quite literally change daily. Boeing has a team in place to carefully monitor all of the company's computing systems.

Majed Barbar is manager of End User Devices, Technical Controls, a part of Information Security informally called Desktop Security. A 28-year Boeing employee with a background in computer science, Barbar leads the team of experts who are the company's first line of defense against Internet-based external
attack.

"You have to have a passion for this line of work or you risk getting burned out," Barbar observed. "Every virus is differ-

ent so you also need to be nimble and knowledgeable, and a lifelong learner. Ours is a competency model because we have to deal real-time with whatever shows up. In this sense, we're more like doctors at a hospital shock-trauma center than your average aerospace worker."

Ben Norton, director of technical controls, Information Security, likens this defense to a behind-the-scenes war being waged in cyberspace.

"Majed and his team keep Boeing one step ahead of people seeking illegal access to our information or trying to disrupt our operations," Norton said. "We're constantly adjusting our desktop and network components to counter these emerging threat patterns, leaving Boeing employees free to concentrate on their work."

SYSTEM AND DATA PROTECTION

Information Security provides protection to Boeing on two fronts. The first is system protection, which seeks to ensure all employees' computers and the Boeing Intranet itself remain unaffected by external Internet-based threats. The second is data protection, which addresses the privacy and integrity of the information within this distributed computing infrastructure.

Firewalls, anti-virus protection, anti-spyware, credentialing, remote access and rights management protections are among the tools Information Security uses. The team also ensures that all attachments entering the company via the Boeing e-mail system are automatically screened.

This comprehensive suite of protections operates quietly in the background and is all but invisible to Boeing computer users. Information Security is committed to preventing hindrances and disruptions that might compromise productivity. And like the company's information technology community as a whole, the professionals of Information Security believe that even one infected Boeing laptop is too many.

In the past year, new measures implemented by Information Security further enhance this protection. For example, Digital Rights Management allows employees to send encrypted e-mails that recipients cannot copy, print or forward. DRM can also be invoked in Microsoft Office applications including Word, Excel and PowerPoint to impose similar restrictions to those applications' documents.

Another recent example: thumb-drive encryption. Complementing the whole-disk encryption that is today standard for Boeing computers, thumb-drive encryption allows users to protect the data on removable thumb drives and other external USB storage devices. Then there's the companywide screen saver that was recently deployed to protect computer users against data exposure and loss.

COLLECTIVE RESPONSIBILITY

Boeing prides itself on fostering an open and collaborative environment that values, respects and protects information. Although Information Security's practices, processes, applications and infrastructure facilitate data protection and security, proper protection still requires the active and knowledgeable participation of every person at Boeing.

A focus on enhanced awareness is under way, educating and enabling employees to better recognize when they possess sensitive information, understand which protections are required for it, and to protect it accordingly.

Plain old common sense is just as important. Never opening a suspicious e-mail, exercising good judgment when checking your personal Web-based e-mail account from a Boeing computer, and never letting your laptop out of your sight in public settings are all examples of practices that will help keep Boeing information safe. Employees also can rely on Information Technology support to answer questions.

"Information Security is vital to the continued success of Boeing. I am pleased with the progress we've made in this important area," said Boeing Chief Information Officer John Hinshaw. "We will remain vigilant in our efforts to protect Boeing computer systems and information." ■

jay.p.spenser@boeing.com

PHOTO: Carolyn Loew (from left), Tim Boisvin, Liz Crowley and Sonja Floyd of End User Devices, Technical Controls, are part of the Information Security team that protects Boeing from "malware," or malicious software threats.

BOB FERGUSON/BOEING