Sights on cyber

By Michelle Roby and Jenna McMullin
Photos by Fred Troilo

Boeing division takes on cybersecurity

In the movie *Hackers*, amateur and professional computer hackers crash thousands of systems, influence a significant drop in the New York Stock Exchange and discover a computer virus that threatens to put a global oil company on the brink of ecological disaster.

The movie, which came out nearly 15 years ago, was way ahead of its time. Today, computer networks and systems are an attractive target for rogue "coders," or hackers, who seek to disrupt operations, shut down systems or cripple information-sharing. The more valuable the information or more critical the asset, the greater the risk—if hackers can access it—to a nation's economic prosperity and national security.

Some have described the cyber threat as an emerging adversary.

"In short, America's economic prosperity in the 21st century will depend on cybersecurity. … For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation," President Barack Obama stated in May in conjunction with the release of a White House Cyber Policy Review.

Current events show the cyber threat already is very serious. For example, several South Korean Web sites were attacked in July, bringing much of the country's network traffic to a halt. At a Cyberspace Symposium in April, U.S. Army Brig. Gen. John Davis, deputy commander of Joint Task Force Global Network Operations, said: "In the last six months we spent more than $100 million reacting to things on our networks after the fact. It would be nice to spend that money proactively to put things in place so we'd be more active and proactive in posture rather than cleaning up after."

Realizing the urgency of the threat and the importance of supporting and protecting customer missions, Boeing is working to design solutions in the cybersecurity arena.

PHOTO: Integrated Defense Systems' Cyber and Information Solutions organization integrates real-time network situational awareness with tools to identify and respond to threats, as shown in this command center scenario.

> "Our military and government customers have stated that protecting vital information networks against cyberattacks is one of the nation's highest priorities, and Boeing is responding to the call."
>
> *– Jim Albaugh, then president and CEO of Integrated Defense Systems and now president and CEO of Commercial Airplanes*

"Our military and government customers have stated that protecting vital information networks against cyberattacks is one of the nation's highest priorities, and Boeing is responding to the call," said Jim Albaugh, at the time president and CEO of Integrated Defense Systems and now president and CEO of Commercial Airplanes.

Specifically, Boeing Intelligence and Security Systems (I&SS) formed its Cyber and Information Solutions organization last year to develop and integrate comprehensive cybersecurity capabilities.

The new division designs, integrates and operates cyber defense solutions on U.S. Department of Defense and other government agency platforms and networks. The organization also provides analysis and operational support to cyber networks around the world through a suite of interactive tools and services.

Boeing's own networks are also a focus. "Our ongoing priority—given the size and activity across our internal and external networks, with more than 2 million logins each month on our external business network alone—is to develop improved capabilities for protecting those networks," said Steve Oswald, I&SS vice president and general manager.

"Cybersecurity is everyone's business," said Barbara Fast, vice president of Cyber and Information Solutions. "It's an economic and national security issue for both the U.S. and the rest of the world. Government and industry networks are only as strong as the weakest network link. Accordingly, Boeing is addressing these challenges with the art and science required to meet this type of threat."

Fast worked with industry leaders and the National Security and Homeland Security Councils in providing comprehensive recommendations on what aspects of cybersecurity the White House should consider as part of the U.S. national strategy. The 60-day review culminated in numerous recommendations; a key finding was the need for government-industry partnership, a need Cyber and Information Solutions stands ready to address.

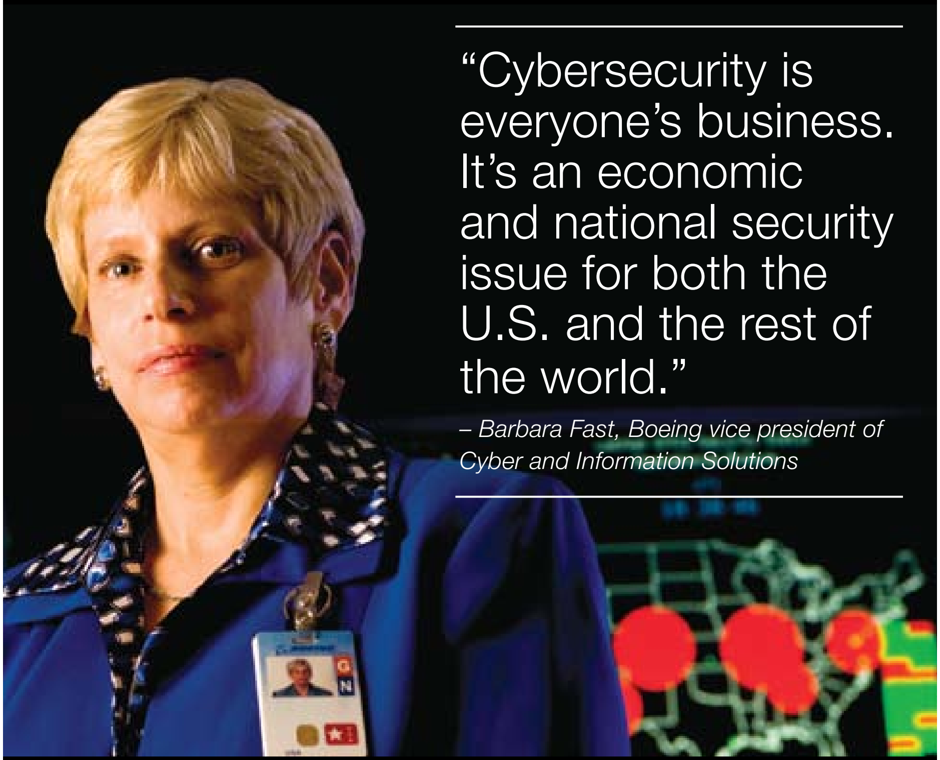
"Innovation is key, and ensuring that companies large and small are able to freely innovate, hand in hand with government, will help mitigate and overcome this dynamic threat," Oswald said.

Still, Boeing faces tough competition in the cybersecurity market, including Lockheed Martin, Northrop Grumman and General Dynamics.

Acquisitions are vital in the company's strategy to expand its presence in the cyber and intelligence markets. Boeing's decision to acquire eXMeritus, announced in June, complements last year's acquisitions of Digital Receiver Technology, RavenWing and Kestrel Enterprises. eXMeritus products are certified and accredited by the U.S. government to secure networks on its most trusted systems.

"The addition of eXMeritus to our team is a strong enhancement to the Boeing capabilities developed through years of experience on secure networks for some of the most complex systems in national security today," Albaugh said. ■

michelle.roby@boeing.com
jenna.k.mcmullin@boeing.com



> "Cybersecurity is everyone's business. It's an economic and national security issue for both the U.S. and the rest of the world."
>
> *– Barbara Fast, Boeing vice president of Cyber and Information Solutions*

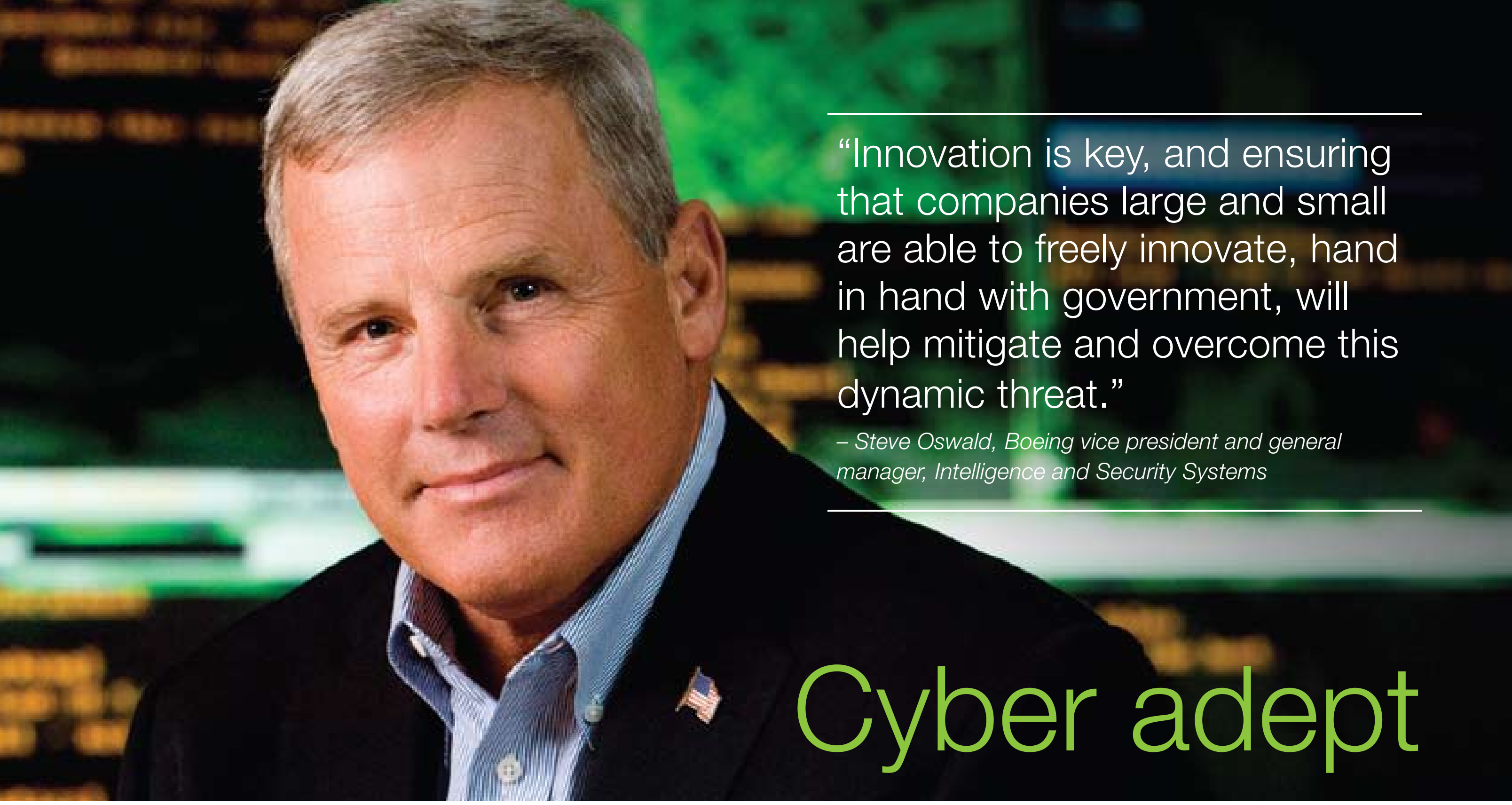
Cyber defenders

Cybersecurity curriculum changes almost as quickly as it's written. In addition to keeping technology up to pace with the threat, cybersecurity is a training challenge. To react quickly, the experts behind a network need substantial practice at detecting and foiling would-be hackers situated anywhere around the globe, and Boeing is doing its part to develop future cyber professionals.

In March, Boeing served as a key sponsor for the Western Regional Collegiate Cyber Defense Competition. The three-day event provided these up-and-coming experts the opportunity to address cyber challenges in a simulated environment, focusing on managing and protecting an existing commercial network infrastructure from intruders. Students tested their knowledge and skills as they worked with experts on developing protective measures to defend their networks. Boeing Technical Fellow Alan Greenberg helped judge the competition.

"These students did an outstanding job in learning how to defend their networks, and also in articulating their actions," he said. "Students like these are our future cyber defenders."

– Michelle Roby and Jenna McMullin



“Innovation is key, and ensuring that companies large and small are able to freely innovate, hand in hand with government, will help mitigate and overcome this dynamic threat.”

– Steve Oswald, Boeing vice president and general manager, Intelligence and Security Systems

Cyber adept

While Boeing is better known for its aerospace products and services than for cybersecurity, the company has actually been a leader in this arena for years, according to Steve Oswald, vice president and general manager of Boeing Intelligence and Security Systems (I&SS). Boeing builds cybersecurity into many of its products, including information assurance (the guarantee that the information being sent reaches the correct recipient and in the form the sender intended) and network defense (keeping the right users in and the wrong users out).

On the current cyberwarfare front, “Boeing cyber experts deal every day with determined and intelligent adversaries who attempt to steal defense and commercial data and technologies,” said Linda Meeks, Boeing chief information security officer. “On average, we block more than 500,000 virus attacks per month on our network.”

In June, I&SS’ Cyber and Information Solutions organization demonstrated a sampling of its defensive capabilities at its Arlington, Va., facility. The Security Monitoring Infrastructure System, which detects and reports network anomalies and is used on multiple Boeing networks, was developed by Boeing’s Analysis, Modeling, Simulation and Experimentation group. The SMIS product has been in development for more than three years and has proved highly effective and efficient in numerous real-world situations, said Barbara Fast, vice president of Cyber and Information Solutions for I&SS.

During the simulation, SMIS reported suspicious network activity and alerted personnel so they could take appropriate action—the same as it does every day on Boeing’s LabNet network, Boeing’s internal network for distributed simulation, network evaluation, and network-centric operations testing.

The Boeing team also demonstrated the Common Open Research Emulator, a virtual, or cyber, “range” for mission rehearsal, exercise scenarios, training, modeling, simulation and testing. Together, SMIS and CORE represent how vigilance and training is enabled by technology.

“We have to become more predictive in defending our networks,” Fast said. “Products such as SMIS and CORE alert our Intelligence Community and government customers to potential dangers and provide the awareness to defend their own networks today, while collecting the information necessary to prepare and rehearse in order to better defend against future cyberattacks.”

Although customers gain advantages through defensive network tools, Fast said, behind every network is a person. When it comes to defending networks there is no substitute for a well-trained, educated work force, she said. Ultimately the best response is not just technical, such as blocking a virus, but in finding the individual or group behind the attack. Situational awareness and the ability to make decisions in incredibly short timelines are critical, Fast said.

– Michelle Roby and Jenna McMullin

“On average, we [Boeing] block more than 500,000 virus attacks per month on our network.” *– Linda Meeks, Boeing chief information security officer*