Hackers for hire put corporate security systems to the test

April 23 2012, By W.J. Hennigan

Most weekdays, Jarrad Sims and Tin Tam, a pair of college buddies, ride their bikes to a computer center and try to hack into computer security systems belonging to Boeing Co.

Rather than having them arrested, Boeing is paying them to do it - a situation that the car-loving, video-gaming friends have pronounced "awesome."

For two years, the young engineers have worked side by side in a secluded unit where they design and thoroughly test ironclad security systems for the largest aerospace company in the world. Boeing's systems need to be capable of staving off hackers and keeping safe some of the nation's most prized intellectual property.

Like many of their colleagues in surrounding cubicles, Sims, 25, and Tam, 24, spend much of their days devising, revising and analyzing complicated security programs that they then use their well-honed skills to attempt to crack.

The pair from California State University-Pomona were hired after they aced a cyber-security competition held by Boeing, in which the aerospace giant urged students to consider careers in cyber security and, of course, scouted for fresh talent.

As computer threats become more coordinated and complex, Boeing and other defense contractors are bolstering their cyber-security staffs.

Increasingly they are turning to unlikely characters like Sims and Tam, who as students had distinguished themselves more on simulated cyber battlefields than in classrooms.

"As long as there are computers, there will be somebody trying to attack them," said Sims, adding that teamwork at the office pays off. "We trust one another to stay on top of the threats."

The damage from hackers to consumers is well known, but the potential for corporate sabotage is far greater, and the need for cyber sleuths like those at Boeing is huge and growing.

Corporate computers serve thousands of employees engaging in different tasks and require layer upon layer of sophisticated security protection.

Those workers need access to the Internet. Although that access enables employees to get the information they need to do their jobs, it also opens a door for hackers to sneak through.

It's not just monolithic corporations at risk. Even small businesses are liable for lost or stolen data, said Scott Hauge, president of Small Business California, a small-business advocacy group.

"I recently had a client who owns a restaurant where credit card information got released to the public," he said. "As a result, MasterCard is looking to collect $200,000 in fines and he is also looking at numerous credit card holders bringing action against him."

Visa recently stated that 95 percent of credit card thefts originate at small businesses, Hauge said.

Such liability has driven demand for cyber-security expertise, said Richard A. Clarke, a former chief counter-terrorism advisor for the

National Security Council and author of "Cyber War."

"There's an arms race in cyber right now," he said. "And the talent isn't just found at the MITs or Stanfords anymore. It's a whole new skill set."

A generation ago, the brightest engineers in the aerospace industry were typically recruited from Ivy League universities and other prestigious institutions.

Now defense contractors are broadening the hiring pool as they hunt for savvy young computer whizzes at local colleges.

Lynn A. Dugle, Raytheon Co.'s president of intelligence information systems businesses, said last year at a conference that her company's most impressive cyber-security hires have come from outside of traditional recruiting outlets.

One recruit was a man who didn't have a college education and didn't graduate from high school. He had a GED and worked at a pharmaceutical plant stuffing pills into bottles.

At night, he participated in online hacker competitions and outperformed others, Dugle said.

"That person would have not gotten through the normal Raytheon recruiting process," she said.

Boeing hired Sims and Tam more than two years ago along with four other Cal Poly-Pomona classmates, most of whom have since left for other cyber-security jobs.

Each morning around 9 a.m., Sims and Tam, who live as roommates in Huntington Beach, Calif., ride their bicycles to work.

There they must flash a federal government-vetted identification, wind their way through a corridor and then gain access to the secluded cyber unit only after entering a special code.

Inside, not much distinguishes the cyber unit from any other office.

It's a 3,000-square-foot room with cream-colored walls and floor-to-ceiling windows on a far wall that lets the afternoon sun stream in on row after row of slate-gray cubicles.

Their work space is a mini-fort of sorts, with 6-foot walls on four sides and small video cameras mounted near the entrance that enable team members to see who is coming their way.

It resembles the chaos of a college dorm room. Inside, a tangle of computer wires lies on the floor and papers are strewn about on desks, along with a half-eaten burrito or two. Sims and Tam each have their own corner, where they sit hunched over PCs.

Their world is full of colorful terms to describe lurking computer threats.

They try to stop "Trojan horses," which enable a hacker to gain access to computers when people click on dangerous links.

They try to squash "worms" that replicate, spread and corrupt computer files.

And they fight "logic bombs" that hide in computers and delete files at a specific time.

Cyber-security professionals have identified tens of thousands of threats aimed at Microsoft Windows programs over the years. If Windows

vulnerabilities are found on Boeing's security system, they fall under Tam's purview to fix.

Sims, meanwhile, is proficient in providing protection for Boeing's customers, virtual data centers and networks, making sure that even if malicious software is downloaded, no data are corrupted.

They're self-professed computer geeks, devouring operating system manuals, the latest software program codes, and white paper reports on recent hacks as if they're glossy magazines.

On a recent weekend, Sims and Tam went out for pizza and rounds of beer.

They ended up spending most of the time talking computers.

"Working with my friends makes the job easier," Sims said. "I trust their abilities."

But just as they close one threatening door, others may open. Just as they lock up one set of secrets, more may leak out.

"It's a never-ending battle," Tam said.

If one employee makes a mistake - forgetting to download a security update or clicking a suspicious link - hackers may get all the access they need to cause trouble.

For example, an employee may receive an email with an attachment that appears to be an Excel spreadsheet but in reality is malicious software. Once opened, the file can embed a virus that will record and send back key strokes or other data, such as credit card numbers.

Boeing's cyber-security workers need to know how to counter that attack so even if the virus is launched it will not infect the system. They determine whether the newest, most harmful viruses - which when activated may damage or delete files, cause erratic system behavior, display messages or even erase data - would work on the system.

Sims and Tam stay current on hackers' affairs by spending time looking at what they're saying in hacker chat rooms. Then they take what they've learned to the lab environment.

Boeing's cyber-security team can spend weeks prodding the system on a platform they designed called "cyber range in a box" that simulates the Internet without actually going live on it. They comb through the security system, seeing whether there are new ways to inject harmful code that would change the database content or dump information like credit card numbers or passwords to a hacker.

In this controlled environment, the team can apply what they learn in real-world situations.

Once they find security lapses within the systems, they plug them.

"We have one main goal here," Tam said, smiling, "to keep private information safe."