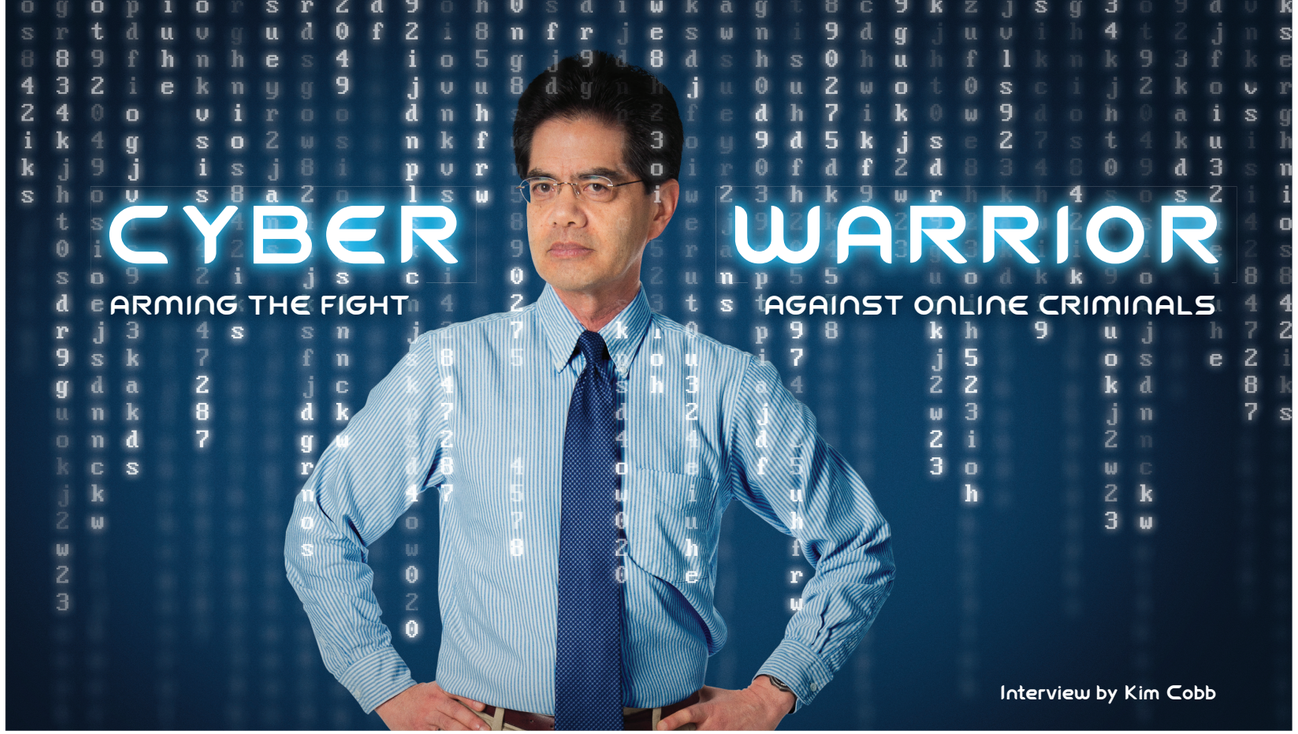

***The Dallas Morning News* described Fred Chang as a "cyber warrior" when he joined SMU in September 2013.** His roles at SMU reflect the breadth of his expertise, as well as his goals – Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, computer science professor in the Lyle School of Engineering and senior fellow in the John Goodwin Tower Center for Political Studies in Dedman College. Chang says he plans to tap as many SMU resources as possible to develop a multidisciplinary program aimed at tackling significant cyber challenges facing individuals, businesses and government. By November 2013, he was testifying before a congressional committee examining concerns about lack of privacy protection for people using healthcare.gov as it was being rolled out. And in January 2014, SMU announced the establishment of the Darwin Deason Institute for Cyber Security with Chang as its director. After a year on the Hilltop, Chang discusses cyber issues.

The past year has been marked by numerous global cyber security problems. How are those issues shaping the Darwin Deason Institute for Cyber Security?

The many cyber security incidents over the past year have underscored to the public just how widespread the problem is. Unfortunately, the headlines also have demonstrated that the cyber defenders continue to trail the cyber attackers. It has proven difficult for the defenders to get ahead of the problem.

From day one, a primary goal of the Darwin Deason Institute for Cyber Security has been to conduct high-quality research that will contribute to the creation of a science of cyber security. We are working with industry partners to move from being reactive to proactive, and the creation of a science of cyber security with these same partners is a critical step in the process. Creating a science with universal standards and methods of measurement will take some time, but we've got to start. We expect that the research we conduct at the Institute will make important contributions to this new science.

It's also important that we take a multidisciplinary approach in addressing the problem. The focus of our programs ranges from hardware and software security concerns to economic and social sciences issues to consideration of policy and law factors. That's why SMU is such a good home for this program – the University has expertise in so many disciplines. I have had the good fortune to collaborate with Josh Rovner, the John Goodwin Tower Distinguished Chair of International Politics and National Security, associate professor of political science and director of studies at the Tower Center for Political Studies, as well as Amit Basu, chair of the Information, Technology and Operations Management Department in Cox School of Business. And within the Computer Science and Engineering Department in the Lyle School, I am working with a team of truly committed people, including, among others, Mitch Thornton, who specializes in hardware security, Tyler Moore, whose research focuses on the economics of information security, and Suku Nair, department chair.

You frequently say that cyberspace is getting to be a bad neighborhood. What keeps you awake at night as you think about strolling through "the neighborhood"?

Cyber attacks on the nation's critical infrastructure are a constant worry. Attacks that would lead to a disruption of communications networks, health care, public safety, financial services, transportation and the like are unthinkable. Indeed, the federal government has made the protection of critical infrastructure from cyber attacks a major priority. And here's another concern that I've had more recently: As security breaches and data exposures are becoming the new normal, I worry that we are all suffering from "security fatigue."

We are constantly learning about some new data breach that may compromise our personal security and requires, for example, that we change our passwords as a defensive measure. I worry that people, upon hearing about the latest compromise, might think: "I just changed my password three weeks ago – I'm not going to do it again." Are we going to become numb to the warnings? I'm certainly not advocating an overreaction to every new breach report, but I do worry that when a credible warning is issued, it may not be taken seriously.

What is SMU doing about these problems?

In the classroom, we want our students to have the right balance of technical implementation details, adversarial thinking and fundamental principles. On the one hand we want them to be "front-line qualified" when they graduate, but at the same time we want to ensure that they are well prepared for the future, because we know the specific attacks that they witness today will be very different two and five years from now. Undergraduate and graduate students gain valuable theoretical and practical skills that prepare them for additional formal training in cyber security or for positions in the job market.

We've been ramping up our research capabilities, focusing on world-class "problem-driven" research through the Deason Institute. We are working with research clients to produce tangible solutions – and by that I mean prototype software – to pressing, difficult problems within a shorter time frame. Another goal of the Institute is our interest in helping to solve the "skills gap." Because there is a large shortage of highly skilled cyber security professionals, employers in the private and public sectors worldwide can't find enough trained workers in the field to fill their openings. This problem will persist for a long time, but we are determined to help close the gap with well-trained, innovative graduates in cyber security from the Lyle School. And because our students have the opportunity to participate in industry-driven research through the Deason Institute, they graduate with industry-focused skills.

> "THERE ARE TWO TYPES OF COMPANIES – THOSE THAT HAVE BEEN HACKED AND KNOW IT, AND THOSE THAT HAVE BEEN HACKED AND DON'T KNOW IT."
>
> – FRED CHANG

For most people, the question of cyber security comes down to personal security. Is there really anything that individuals can do to protect themselves from cyber thugs?

Just like when you drive your car, you can't guarantee that you won't get into an accident. But like buckling your seat belt and adjusting your mirrors, there are some things you can do to help defend yourself in cyberspace. Let me mention three approaches:

- ***Update software*** – it's a good idea to regularly and frequently update the software running on your machine. The software vendors are constantly providing updates that contain improvements, including security patches that will close a security vulnerability that exists in the software.
- ***Be vigilant*** – be smart when you're on the web and when processing email. It remains all too easy for your machine to inadvertently download malware – nasty software that damages or takes control of computers.
- ***Use difficult passwords*** – people continue to use passwords like "password" or "123456." It's not convenient, but people are well served to use harder passwords.

You receive many requests for speaking engagements. What do people want to learn about cyber insecurity – especially in industry, where problems are occurring faster than many experts can form a response?

A lot of people find the cyber security problem both surprising and alarming – they realize the problem has become widespread, and they either know somebody who has been affected or they have been affected. There's a saying that has been going around the business world as it relates to cyber security: There are two types of companies – those that have been hacked and know it, and those that have been hacked and don't know it. So that's our challenge, and we are embracing it. We're very excited about the research momentum we are building at SMU. We believe we are making a difference in the field of cyber security by helping to solve some challenging problems, and our positive outlook is being validated by an increasing number of research sponsors approaching us for assistance. We're off to a fast start and we don't plan on slowing down.

What does it mean for your work, overall, to hold a centennial chair and lead a new institute dedicated to solving global cyber security issues?

It was very clear when I joined the University that SMU intended to provide significant resources to make a real impact in the field of cyber security. The beauty of a centennial chair is that the donor has had the foresight to provide several years of operational support until the endowment matures. And the opportunity to develop an institute that reflects the priorities I have embraced through work in government, business and academia will provide important resources for important work.

For more information, visit www.smu.edu/Lyle/Institutes/DeasonInstitute.