Video Transcript for "Cybersecurity Strategies"

online at https://spice.fsi.stanford.edu/multimedia/cybersecurity-strategies

On-screen text:
Cybersecurity Strategies
a discussion with Herbert Lin

On-screen text:
How do we defend ourselves from cybersecurity threats?

On-screen text:
Herbert Lin
Senior Research Scholar for Cyber Policy and Security
Center for International Security and Cooperation, FSI

Herbert Lin: So, you ask "how do we protect ourselves from these bad things that can happen to us in cyberspace?" Well, there are only a handful of ways of doing it, and you really can't think of much else that doesn't fall into one of several buckets.

So the first thing is: Don't use the Internet, or don't use a computer, when you don't have to. Good example of this: There are power plants that generate electricity that are controlled by the Internet—by commands sent over the Internet. So these power plants are vulnerable to being hacked over the Internet. Now, if you disconnect them from the Internet, can they still be hacked? Yes, but it's much harder to. Why are these guys making it easier for people to hack these power plants? The answer to that is economics. It's cheap to put the command pathways to these power plants on the Internet. You don't have to build a special purpose communications infrastructure, and so you can buy off-the-shelf hardware that will do all the connecting. It's all really cheap. Now, is this a good thing? Is it good that it's cheap? Yes. It's absolutely a good thing. But does it come with security risks? You bet. Should somebody be thinking carefully about whether it's worth it? Yes. Do people think carefully enough about it? No.

Second thing: You can detect. Instead of not using the Internet, you can do what's essentially knowing that you're under attack. So you have a computer at home. Haven't you ever experienced the problem where it froze? Did somebody attack your computer? Or did just some lousy software foul up your computer? Well, the fact of the matter is you don't know. You might know if you were a real hacker yourself. Even hackers often don't know that. There's a question mark; there's an element of doubt. But I got to tell you: Most of the time that happens, it's some crappy software that you're using or a mistake that you made. You weren't under attack; nobody attacked. It's just some bug that happened on you, and your machine froze up, and you just rebooted the thing and started over again, and everything was fine. But, you know, that could have been an attack. It might have been an attack. How do you know?

So there's another domain, another area where you have to pay attention. How do you know that you're under attack? Knowing that you're under attack is a big deal—being able to recognize—even if you can't do anything about it. I'd rather know that somebody was draining my bank account rather than not know that somebody was draining my bank account. Even if I can't do anything about it, I'd rather know than not know. Because if I know, then at least I can complain to somebody. So those are two things.

Third thing you can do is you can defend your computer. This is what most people think about when they talk about cybersecurity. They can put up an antivirus software, or something like

that, that checks your machine for incoming malware—bad software that will screw up your machine. And they can run checks. It turns out that those checks don't do very much; they only protect about 40 or 50 percent—some percentage—but by no means 100 percent. Not even 90 percent; not even 80 percent. But it's better than nothing. And so what I actually do is I run two or three virus protection [software programs]. There are some of them [viruses] that they all catch, and there are some that only one catches, and I get a little bit better protection that way. So that's good. But I'm more paranoid than most people about this, so I take that extra trouble. Does it cost me more? Yes. Does it interfere with the performance of my computer? Yes. But it's worth it to me to do that. So there are ways of protecting your own computer that you can do. Antivirus software is just one of many measures that you can take.

You could also, from the vendor's side, write better software that is more security conscious—that doesn't have the problems in it that cause security vulnerabilities that the bad guy can take advantage of. It turns out that this is very expensive to do. To write really good software that has very few bugs in it costs a lot of money—ten, fifteen, a hundred times as much as it does to write regular old software. And so you, as the vendor, you have to say, "Is it worth it?" In some cases, it is worth it. For example, the airlines spend a lot of money on airplanes. The airplane manufacturers spend a lot of money to develop software that really works. I don't want ordinary software running my plane in the sky; I want something that I know works, that I have high confidence that [it] works. And they really get that, and they pay through the nose for it. It's very, very expensive, but it's worth it. I mean, it's also worth it because they wouldn't get certification to fly if they didn't do that, but that's a different point. It's certainly worth it to invest that money in really critical applications.

So those are two things. There's a third thing that you can do, which is that you can configure your system in such a way that is more secure rather than less secure. For example, use a complicated password. Don't use the word "password" for password. Don't use "123456" as your password. It turns out that those two are among the most commonly used passwords. By "commonly used," I mean maybe five or ten percent of people use them.

They give you advice about how you should have a password [and] what password you should [choose]. Here's the advice they give you: Make it a password that's difficult to guess. And remember [it]. And don't write it down. Is this very sensible advice? Well, yes, it's good advice from the standpoint of passwords. If you're just looking at the password problem, those are good rules to follow. But if you can follow that advice in any meaningful way, you're better than I am. No human being can follow all those rules and still remember [them]. Passwords are a 50-year-old computer security technology, and we're still using it. There are many advantages. But we're still using it.

You can configure your system to require more complicated passwords. That might help. But, of course, then there's a tradeoff with operability, with usability. It makes it harder for you to use your system. So that's the defending part.

The fourth bucket is recovery. What does recovery mean? And resilience? Recovery means that you give up. You don't really give up, but you realize that eventually you're going to be compromised. When was the last time you did a backup on your files? If you're like most people, [it was] a long time ago. And you worry about that. You worry that somehow something bad has happened and something weird is going on, and you want to go back to a backup file. You want to go get it, and you say "oh no, I didn't do that. I didn't back the thing up." Be prepared for needing to recover. This is an important thing to do. Everybody should be backing up files.

Anticipate being compromised, and act accordingly. So, for example, that might mean having a backup plan. Just recently the U.S. Naval Academy just started again teaching its cadets how to shoot the stars—that is, to navigate by sextant. Why? Because people were getting too dependent on GPS. GPS is a computer-operated system, and if GPS goes down, these ships will have no idea where they are. That's bad. So that's the recovery part—recovery and resilience.

Then there are things that are somewhat more controversial. Such as: If you know a bad guy is coming after you, can you punch him out? In real life, if you were coming after me, can I punch you out? Well, if you attacked me first, I can certainly punch you out. But if I punch you out and then you run away, I can't run after you. What's the right law in cyberspace? Should attackers in cyberspace be vulnerable to being punched out? That's a very interesting question. Because now…you mean, you're going to do the same sort of stuff to the bad guy as the bad guy did to you? You can see where this goes. It's not clear you should be able to do that. But that is another way to do it. You have to impose a cost on the bad guy. Because otherwise, they'll just come after you, and will come after you and will come after you, and he won't suffer at all. When he gets bored, he'll stop. But if he doesn't incur a cost, there's no incentive for him to stop. So how do you do this? This is a question of "active defense," and it usually means doing something to the bad guy that he doesn't want you to do. And it's very controversial.

And then there's the last way of doing it. [It's] to think of who the bad guys are, who your adversaries around are, and you just go around trying to intimidate them. You slap them around a bit—maybe in cyberspace, maybe not in cyberspace. Maybe you threaten them with economic sanctions or whatever. You just establish the fact that you're king of the hill, and that nobody dares attack you. I leave it to you whether you think that that's feasible in today's environment, but that's a different point. That's another approach—you weaken the other guy, and then you theoretically make him less willing to attack you because now he's scared. Those are the ways… that's how you deal with cybersecurity. And how, the ways…you asked "How do you defend yourself?" And that's a rough breakdown of the kinds of ways you can do it.