A special report from GovConnection™ tools for higher learning™

SECURITY FOR A 2.0 WORLD

IT professionals discuss how to protect information in a world in which the rules have changed.

WITH THE PROLIFERATION OF mobile devices, telepresence, virtualization, and more, security has never been a greater challenge to IT professionals in education and the corporate world. That's why GovConnection partnered with Cisco and the University Business Leadership Institute to host an event to discuss the challenge and offer assistance, guidance, and understanding in managing and mitigating security risks. What follows are highlights of the event.

New Approach to Security Needed in Mobile Age

The ability to have anytime anywhere access to information fluidly and without friction will change the way people work. Indeed, the change will be so profound that many people believe that the borderless network will propel productivity in the next two decades in the same way that networking propelled productivity in the past two. But with this increased access to information comes increased security concerns.

"The way that we build and deploy security is going to be dramatically different five years from now than the way we do it today," said featured speaker Tom Gillis, vice president and general manager of the Cisco Security Technology Business Unit.

Gillis, author of *Securing the Borderless Network: Security for the Web 2.0 World*, said that the underlying technologies of the network are outdated when it comes to dealing with the new technologies. As a result, security mainstays, such as firewalls, are difficult to adapt to these changing requirements.

"The whole notion of how firewalls work, based on IP protocol, has to change. It gets really complicated to express policy based on IP protocol," Gillis said. "It can be done, but it creates ballooning rule sets. What we need is a new language for describing security in this new age."

The proliferation of new tools to access the network means a corresponding increase in the amount of information and data being generated. This is especially true in the university setting. "But what we really need are tools that will allow us to tackle this mountain of data and make our jobs a little easier," Gillis said.

The proliferation of new tools to access the network means a corresponding increase in the data generated.

"We've seen more innovation on the endpoint, with devices like the iPhone and iPad and Android, than we have in the past decade. As we begin to get our arms around these new devices as productivity tools, they will enhance our ability to get our jobs done. They will allow us to access and process this information that is the lifeblood of the university or enterprise.

"The mobile Internet is having a revolutionary impact on user productivity. It's bigger than we think." While mobile devices may increase productivity, they will also mean a greater burden on exisiting security systems.

"If you look at the combination of a mobile device such as the iPhone and a SaaS [software as a service] application like Salesforce [a CRM application], that's a real security challenge," Gillis said. "When you check your Salesforce report on the iPhone, there is no traditional firewall."

Cisco is working to provide users with the tools they need to help control this influx of technology, he said.

Another example is the popularity of social networking tools such as Facebook, which is used as much as a marketing tool as it is a communication tool in the university setting.

"The first instinct in many enterprises is to just block it," Gillis said. "We can't just block this stuff anymore, we need intelligent controls that are based not just on the underlying infrastructure, but that understand who you are, what applications you are accessing, and what you are trying to do with those applications. Basic things like access control and accountability get complicated in this new world, which is coming whether we like it or not," he said.

Q&A with Tom Gillis on *Securing the Borderless Network*

UB: In your book *Securing the Borderless Network*, you talk about the proliferation of a wide range of devices trying to access the network. How has security changed in this environment?

Gillis: In the past, security happened in two places. It happened on the endpoint, which was relatively well controlled. You could put up your anti-virus software, and you could manage the configuration. And it happened at the perimeter, which was something that was quite tangible. You could touch it. You had this thing called the DMZ where you could put an IPS, and a web proxy, and a firewall.

With the explosion of new consumer devices, the endpoint is sort of this ephemeral thing. The point at which you touch the internet is breaking down—the deperimeterization of the network. Security used to be at the beginning and end, but now the beginning and end are gone. So security has to go in the middle. It has to go into the network itself.

Cisco is uniquely suited to address this trend. We can put security scanning on the network. We can have multiple layers of anti-virus and data loss prevention. We have very advanced, intelligent policies around Facebook usage, for example. Not just blocking it, or turning it on and off. We can do fine grain controls.

UB: With cloud computing, do the same rules apply?

Gillis: I view cloud computing as the evil twin of mobile devices. With iPads, Androids, and so on, the *user* is on the move, but cloud computing means that your *data* is on the move. Your data may be in your data center, or in someone else's data center, or it could be moving between two data centers. It is getting harder and harder to say "my data resides here." That's why you need to put security in the fabric of the network itself.

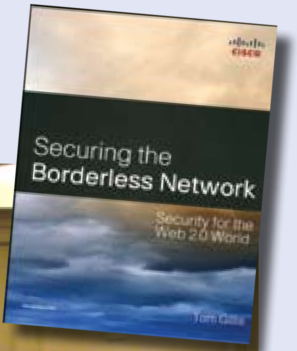
UB: Cisco employees can choose and use their own devices, which are then supported by the company. Are universities as flexible in this regard?

Gillis: They are being forced to be. The cultural environment is one of openness and, especially in the student population, it's silly to even talk about it. They are going to hook up that Xbox to the network anyway so trying to stop that is like trying to hold back the ocean. It just can't be done. The rest of the world has a lot to learn from the university environment, because you're already dealing with it.

We are trying to give people the tools to allow them to deal with it. This type of disruptive change is difficult to respond to. I would even argue that our tools are still nascent. They are still in relatively early days of development and will be refined substantially over the next few years.

UB: You said that you are passionate about the user experience. How passionate are campus CIOs?

Gillis: When it comes to student access, many campus CIOs are in the position of just minimizing the pain. It's not about delivering an excellent experience; it's about minimizing the cost of supporting it. You have such a broad constituency that you can't please everyone. They are trying to deliver good service without rocking the boat. They are being asked to provide a spectrum of services from the Wild West to the Army Special Intelligence Facility. In that world, it is difficult to be a fanatic about delivering a consistent end-user experience everywhere.


cisco
Securing the Borderless Network
Security for the Web 2.0 World
Tom Gillis

Mobile devices will continue to increase productivity—while also being a burden on older, existing IT security systems, noted Tom Gillis of Cisco.

For faculty and staff, especially at research institutions, you have much higher levels of security. You have an incredible spectrum of missions that you need to accomplish with a single team that is usually massively under-resourced. It is not an easy task.

UB: You referenced the film *Minority Report*, with its vision of total access to information. How far are we from that future?

Gillis: The thing that is still missing is the ability to navigate through all this data. We'll see more business logic tools and tools that help you get insight faster. Our mission at Cisco is to make access to information frictionless, so it "just works" and you don't need to know about the underlying tunnels and connections.

Learn more about Securing the Borderless Network *by Tom Gillis at www.securingtheborderlessnetwork.com*

Roundtable: What is on CIOs' Minds

Following the presentation by Cisco's Tom Gillis, CIO Summit attendees participated in a wide-ranging roundtable discussion about the disruptive technologies currently affecting their institutions.

Several CIOs mentioned the use of game consoles—particularly those found in residence halls—not just for games, but as another kind of general-purpose computer for web browsing, and in authenticating them.

"It's an example of consumer devices coming into the enterprise," said Rich Pickett, CIO at **San Diego State University**. His campus has up to an estimated 60,000 wireless devices registered with IT, with up to 18,000 or so simultaneously connected.

SDSU has terminated all the wired jacks in the residence halls and started charging students for a hard-wired port. Several attendees noted that it is not the first time they have heard of schools doing that.

Some institutions offer free cables to keep devices off the wireless network and provide better service.

It is also common for students to think that the IT department is responsible for making all of their devices work. An IT administrator at another institution noted seeing "every device known to man" brought to the helpdesk. Administrators try to push people to the wired connection.

Some institutions are even giving away free cables, which will keep some devices off the wireless network as well as provide better satisfaction to student users.

One participant suggested that while, for practical reasons, campuses may have to resist providing access to meet every request, a long-term strategy has to encompass new technologies.

But what can IT administrators do to be more proactive, rather than reactive?

Michael Berman, CIO of **California State University, Channel Islands**, commented that Cisco's strategy is the right one: any device to any application. "That's what we have to move toward."

"Unless it's illegal, we don't limit access on our wireless network," added Pickett.

Educating users about the realities of network traffic is crucial. "If somebody sells you an automobile, the person can't promise you you're never going to get into a traffic jam," says Bill Balint, CIO at **Indiana University of Pennsylvania.** (IUP) "There are so many points of failure now. You have to get your users savvy enough so they can find their own path."

Another CIO likened the challenge to having a lot of security for your home, but then your son leaves the door wide open. "You can have every technology piece in place, but if that end user doesn't know not to send their password to that guy in Israel, that's a point of failure for us. It's not our technology," he said.

Balint's colleague, Tom Rodgers, a senior technology analyst, explained that IUP uses social media, including Facebook, to try to push security common sense out to users. "We say, 'As a technology group, we'll never ask for your username or password.' "

For San Diego State University constituents, completing a web training course on security awareness was required, Pickett says. Telling faculty he would terminate their network access if they did not complete the training resulted in 100 percent compliance, he added.

On the other hand, in Berman's experience, administrative staff are "just hungry for knowledge," he shared. "They say they want to make sure they're not the one who releases student data. The staff working with student records really want to help in keeping this secure."