BIG DATA

[It's changing how we do everything.]
Phyllis Schneck, PhD CS 99, and Andy Ozment, CS 00, help lead the U.S. Department of Homeland Security’s cybersecurity team tasked with defending our data and infrastructure from the crooks, hackers and worse desperately trying to get their hands on them.
When the power first went out in Ukraine last December—on an otherwise ordinary weekday afternoon—the loss of heat and lighting proved to be an annoyance for those living in the 250,000 or so households affected, but not necessarily alarming. The outage then spread throughout several regions of the country, lasting as much as six hours.

Inside the country’s power plants responsible for distributing the electricity, operators were distressed and confused. In three different locations, control center workers had lost access to their computers. Their equipment was suddenly unresponsive while cursors on their screens moved around seemingly of their own accord. Operators watched helplessly as unseen hands navigated through computer windows and cut off power to hundreds of thousands of people.

Hackers had remotely accessed the electrical system—using previously stolen usernames and passwords—and the cyber intruders were shutting down whole sections of the grid. Two of the power plants subsequently lost backup power. The operators were left literally in the dark.
The extraordinary feat of leaving hundreds of thousands of people without access to heat or light—in the dead of winter—was still not a sufficient exploit for these malevolent meddlers. While workers at the control centers witnessed their systems being manipulated right in front of their eyes, the hackers also secretly triggered a tool that destroyed the power grid’s automated capabilities. Computers could no longer be used to return power to those cold, dark homes. The electric company had to send out technicians to restore people’s power manually.

At present, more than five months later, Ukraine still has not fully restored its automated operations. But they have a greater understanding of what happened and how, and are better prepared to address such threats, in part thanks to a visit by a United States Department of Homeland Security (DHS) team overseen by two Georgia Tech graduates.

WHO YOU’RE GOING TO CALL

These two data defenders, Phyllis Schneck, PhD CS 99, and Andy Ozment, CS 00, are based in the Washington, D.C., area, but operate out of a multitude of undisclosed locations. This day, Schneck is at her Virginia office. “I was in the [White House] situation room just 48 hours ago,” she says. “Any given day, I have about eight meetings.” Schneck speaks in the breathless cadence of someone whose mind is in many places at once. Her thoughts seem to be always in motion, yet still on target—a requisite characteristic for her role as deputy undersecretary for cybersecurity and communications for the National Protection and Programs Directorate (NPPD).

The DHS is enormous, made up of multiple components, including the U.S. Coast Guard, the Secret Service and the Federal Emergency Management Agency (FEMA). NPPD is the component that focuses on our networks and systems. Its mission is to protect the country’s critical physical and cyber infrastructure—including the communications backbone that makes our phone calls, banking transactions, electrical grid and our water system work. Since 2013, Schneck has been the top cybersecurity official for the DHS, drawing from a blended background of public and private sector work. Previously, she was chief technology officer for the global public sector at McAfee Inc., and was vice president of Research Integration for Secure Computing.

“WHEN I SIT IN A POLICY OR BUDGET MEETING, THOSE OF US WITH TECHNICAL BACKGROUNDS BETTER UNDERSTAND HOW MONEY IS SPENT, HOW AN ADVERSARY WORKS OR HOW OUR PROGRAMS COULD BE DEVELOPED.”

- PHYLIS SCHNECK
Schneck’s charge may be difficult—and no doubt daunting—but her technical foundation gives her an edge. “When I sit in a policy or budget meeting, those of us with technical backgrounds better understand how money is spent, how an adversary works or how our programs could be developed,” she says.

In addition to situation room discussions with President Barack Obama and leaders from other agencies, Schneck also manages about 2,000 people. Her goals for the vast office fall into three main categories. First, on the technical side, keep the infrastructure secure. Second, communicate often and openly, in ways that make sense to the intended audience. (Her office works with a diverse customer base: federal, state and local government agencies, as well as the private sector, including academic institutions and businesses of all sizes.) And third, raise awareness with customers and policymakers—at the White House, on Capitol Hill and to U.S. citizens.

Schneck knew quickly upon joining the DHS in 2013 that she was going to need some help to fulfill these goals. And, thankfully, she knew just where to find it.

Andy Ozment was working at the White House as President Obama’s senior director for cybersecurity in 2013. (Since getting out of Georgia Tech, he had moved to the United Kingdom on a Marshall Scholarship, where he earned a master’s degree in international relations from the London School of Economics and a PhD in computer science from the University of Cambridge.) The White House gig was going well. It was a policy-heavy position where internal education was a key mandate. Ozment was asked to increase attention to cybersecurity—it was already an important issue, but not one easily understood by senior leaders.

When Schneck phoned Ozment about joining her team, he saw an opportunity to act on network protection, rather than be in the business of describing it. Schneck wanted someone who had walked the walk, a tech type who could communicate complex ideas. “I wanted strong leaders who had done the job in the same way,” Schneck says.

Ozment adds: “DHS is the place where we help companies and government protect themselves against bad guys. It’s where my heart is. And Phyllis is very persuasive.”

Since they often aren’t working in the same location, both Schneck and Ozment have each other on speed dial. Schneck focuses on leadership, building relationships with other agencies, customers and governments, and ensuring resources are available, while Ozment manages engineering teams and traditional security operations, and works directly with

“COMPANIES CAN BE RELUCTANT TO DISCUSS THEIR INCIDENTS, WHICH CAN HAVE THE RESULT OF SUSTAINING CYBERCRIMINALS LONGER. OUR IGNORANCE IS THEIR BLISS.” - ANDY OZMENT
The partnership is not a hard science. Sometimes, impromptu meetings with interagency partners jettison carefully crafted schedules. Once, they caught up over “lunch”—the first meal either of them had enjoyed in 12 hours. Often it’s all hands on deck, especially when a customer asks them for help. That’s one thing about the cybersecurity office.

“DHS doesn’t just walk onto a site,” Schneck says. “We have to be invited. Does the customer want us there? Do they want our guidance? We have to deliver answers in a way that the recipient can hear it and act on it, and we have to do it fast.” Such was the case in Ukraine following the power grid cyber attack. The U.S. was invited to help.

WHO SHOWS UP TO HELP

If the speed of a 911 emergency met in the cybersecurity world with the skills and resources of a cyber-CSI crew, you’d have a layman’s sense of the DHS’s Industrial Control Systems Cyber Emergency Response Team capabilities. The ICS-CERT, according to Schneck, is made up of “hard-core techies” who respond to incidents and mitigate cyber threats, and communicate with 200-350 teams throughout the world. They, along with representatives from the U.S. Department of Energy and the FBI, went to Ukraine following the December incident.

“Ukraine trusted us to come in and help,” Schneck says of the relationship between the two countries. The U.S. team helped review what happened, then published an advisory online to help educate other nations and entities about the attack and what could be done to thwart a similar one.

When big companies discover they’ve had a cyber incident, they will frequently ask the DHS’s Office of Cybersecurity and Communications for help. Ozment says his office’s technical response is often the easiest part of the process. “I hire a lot of responders and I take the best technical people around,” he says. “But the people who really excel are not just great technically, they have the skillset of a therapist.” His teams go into companies and organizations on what might be the worst day of a chief security officer’s life. “That person may fear for their job,” Ozment explains, “or they’re worried about the consequences for their company.”

Naturally, corporate lawyers are next in line to express concern. They want to know what happens once they ask the government for help. Ozment explains that the DHS has lawyers to reassure companies about their protections. DHS will not release any information about an incident without permission, most often requested strictly for the purpose of raising awareness in an industry. No one will reveal the company’s name, nothing can be accessed through Freedom of Information Act requests, no information can be disclosed in litigation, and DHS cannot even share the slightest detail of the case with a regulating body.

“The first all-nighters on an incident response are usually pulled by the lawyers, not the techies,” Ozment says. Once the paperwork is done, which happens quickly once worries are quashed, a team goes onsite to investigate, support and provide a framework for what the company or agency can do next. “We don’t send a lot of people to a given incident, maybe five to eight,” Ozment says. “Too many and the customer gets overwhelmed.”
The cybersecurity office has a “war room,” a 24/7 situational awareness center where data is monitored by the millisecond. “It’s a dark war room with huge screens and lots of people,” Schneck says. “Just like you picture it in the movies, I promise.” Officially, the war room is the National Cybersecurity and Communications Integration Center. “I call it the NCCIC,” Schneck adds, pronouncing it like en-kick.

The biggest data threat to U.S. security is the risk to our critical infrastructure, Schneck says. So the overarching idea that governs her team’s work is looking at how someone would make a computer do what it’s not meant to do. “If you own or operate a piece of critical infrastructure, good morning—you probably have BlackEnergy malware on it,” she says.

The NCCIC monitors millions of events, allowing the DHS to see when patterns arise. One event in one place isn’t usually a big deal. But 100 events on random machines is a different story. Schneck has spearheaded the Weather Map project: The work aims to build a map which future cyber responders will look at and know if a “raincoat” is needed.

Buoyed by President Obama’s Executive Order 13636, which among several directives, created new information-sharing models and civil liberty protections that encouraged companies to share threat information, DHS can use these vast troves of data to identify indicators. Lots of indicators lead to trends. And trends in data can stimulate action. Once events are detected, the DHS distributes advisories via their protocol, which is open to the public. The potential impact doesn’t just stop at a bunch of techies. Those decisions can hit as high as the CFO and CEO of major companies—the folks who are accountable to shareholders in various organizations.

“We’re using Big Data in ways that not only respect privacy and civil liberties,” Schneck says, “but we can use the speed of computing to detect events that were never before visible in all the noise of the Internet.”

Everyday citizens and their many devices—connected via the Internet of Things—also contribute to those data points. All those connected phones, cars, medical devices, washing machines and home security systems also expose consumers to greater risk. It’s true, Schneck says, every new connected item potentially introduces a new vulnerability. The key is to manage it and be vigilant. To that end, DHS launched the Stop Think Connect initiative, encouraging consumers to reconsider before downloading mysterious files, clicking on ads or following links to unsolicited websites.

But data points only go so far. This is where communication can matter the most, Ozment says. Companies can be reluctant to discuss their incidents, which can have the result of sustaining cybercriminals longer. Our ignorance is their bliss. To help shift the culture around discussing unseemly cyber incidents, the NPPD sponsored a workshop for the insurance industry in late April.

“Insurance does a lot to drive the economy to better secure itself,” Ozment says. “We wondered what data companies would be willing to share with insurers, and what data insurers would find useful in crafting their policies.”

This is the softer side of how DHS sees itself in cybersecurity—bringing parties together and hoping that they help each other. But that’s the job, Ozment says. “That’s the experience of being day-to-day defenders. We inform the conversations that shape the broader market and economy.”

Schneck and Ozment agree, those conversations began with the technical foundation they received at Tech.

Ozment cites the varied opportunities to research and explore as crucial to his development. “I realized that as a programmer, I could build complicated things in a precise way, but could shape those things in a way that suited my personality,” he says.

“My education has given me an edge every time,” Schneck adds, “from the Situation Room to a casual phone call. It’s not just knowing the software, it’s understanding how stuff works at the metal level.” She credits College of Computing founding Dean Peter Freeman as a business mentor, helping aim her in the right professional direction. Schneck says she also received priceless advice from Rosalind Meyers, former vice president of auxiliary services. “She told me to volunteer to get good experience. When the FBI approached me to run the Atlanta branch of InfraGard, it was scary, but I took it.” There, she learned about leading large groups and was able to give back to things that were important to her.

The Tech alumni family doesn’t stop at the DHS staff. As part of Schneck’s outreach to companies to better understand what they need, she recently invited serial entrepreneur Tom Noonan, ME ’83, to her office to speak to her staff. Noonan contributed funds to help open the cybersecurity office where Schneck worked as a graduate student, and they’ve remained friends.

She intends to leverage relationships like this to bring “the best of innovation” into today’s new government, one that’s focused on customer service and speed—which looks nothing like it did a few decades ago. Back then, “a typical company’s security methodology was to buy a firewall and network gear and if there was any money left, you got a color printer,” Schneck says.

The reality is that Schneck, Ozment and the rest of the DHS cybersecurity team are working to make the Internet more self-healing, so when devices notice something awry, it gets reported instantly, creating a track record of actionable indicators.

“Our mantra is months to milliseconds,” Schneck says of the shift. If the worst happens, the general public doesn’t have to stay up all night worrying about the outcome. Someone with a DHS badge is doing that already.