First Person—EPRI'S Cyber Security Guru Goes to Europe

The Story in Brief

EPRI's Annabelle Lee has gained international recognition for her wide-ranging experience in cyber security dating back to the early 1980s before the term had been coined. In this interview with EPRI Journal, she shares insights from her career, describes the cyber security threat in the electric sector, and discusses her role on a panel to inform regulations in Europe.

EJ: The European Commission selected you as the only American on its Energy Expert Cyber Security Platform–Expert Group, a 14-member panel providing cyber security guidance to the Commission. How did you become such an internationally recognized cyber security expert in the electric power sector?

Annabelle Lee

Lee: I began my career as a programmer in the mid-1970s working for a number of consulting firms on computer systems design, development, and analysis. I started in computer security in the 1980s at the MITRE Corporation, with a focus on law enforcement. I worked on-site at the FBI on computer systems design and cyber security for two of its very large systems, and I led a cyber security effort for the Drug Enforcement Administration. In 2004, I moved into power sector cyber security, first for the Department of Homeland Security, then the federal agency National Institute of Standards and Technology (NIST), and finally EPRI.

EJ: What got you into computer security?

Lee: In the early 1980s, I was doing computer system design and analysis at MITRE. A co-worker said that MITRE was starting a group on computer security and asked me if I was interested in joining. My response was 'I don't know anything about that,' and his response was 'Neither does anybody else.'

“As we modernize the grid with renewables and other new technologies, interconnectedness makes cyber security more challenging, and it’s hard to predict consequences of cyber security events….”

EJ: What did you do at the Department of Homeland Security and NIST?

Lee: At the Department of Homeland Security for four years, I worked on security for control systems in the electric sector—the hardware, firmware, and software that operate and monitor the energy delivery systems.

I was at NIST when it was starting the Smart Grid Interoperability Panel, and set up a team to develop NIST’s Guidelines for Smart Grid Cyber Security. This was the first cyber security guideline for control systems in the electric sector. Grid control systems are focused on availability—when they go down, people may lose electricity. This is different from the majority of information technology systems—think of banking and finance systems—that focus on confidentiality. The smart grid guidelines are used by organizations around the world to develop cyber security specifications. More than 100 technical experts authored the document.

EJ: What aspects of cyber security does EPRI focus on?

Lee: EPRI collaborates with utilities internationally to identify critical cyber security research in two main areas. I lead the first area—information assurance. This includes cyber security risk management, creating security metrics for the industry, designing security into products, and identifying and assessing technical solutions for compliance with the North American Electric Reliability Corporation’s (NERC) Critical Infrastructure Protection Standards, with international standards, or with utility requirements.

The other research area focuses on testing of cyber security technologies in EPRI’s Knoxville laboratory. One example is our research on Secure Substation Systems. EPRI worked with utilities to develop security requirements for five common uses of these systems. Five vendors made adjustments to their password management and other software products to comply with these requirements. EPRI’s involvement helped enhance security and solutions available for the entire electric sector.

To make sure we don’t duplicate research, we collaborate and coordinate with other industry stakeholders, and participate in conferences and workshops.

“Technologies and threats are constantly changing, and that makes cyber security a constant work area.”

EJ: Drawing on your pioneering and extensive work in cyber security, what primary insights are you bringing to the discussion in Europe?

Lee: One is that technologies and threats are constantly changing, and that makes cyber security a constant work area. Five years ago no one would have considered that everyone would have one or more mobile phones. You can’t just say, ‘Okay, I’ve done a risk assessment, I’ve implemented my security controls, and I don’t have to worry about it for the next year or two.’

In this environment, grid reliability is paramount. The grid must be resilient in the wake of a cyber security incident. Maintaining electricity availability today while simultaneously planning for future cyber security controls is extremely difficult. Utilities have to be conservative. You don’t just deploy security technologies and then say 'Oops, guess what? I shouldn't have done that.' IT departments have accidentally shut down systems when they performed vulnerability scans. If you do that in the electric sector, people could lose their electricity. EPRI works with utilities to support reliability and resiliency in this constantly changing environment.

The second insight: We have to be right with our cyber security strategies and controls 100% of the time; the bad guys only have to be right one time. That makes this work very challenging.

I'll add a third: Cyber security is just one area utilities need to address. They have other important areas such as financial risk and safety risk. Utilities cannot spend all their resources on cyber security, so they have to prioritize systems and vulnerabilities. This is risk management.

EJ: Characterize the current cyber security threat in the electric power sector.

Lee: Before 9/11, I was managing NIST's cryptographic module validation program where I'd be lucky to have 20 or 30 people in the room for a speaking engagement. After 9/11, I spoke on September 30th and had 100 people in the room. The next day I had 300.

As we modernize the grid with renewables and other new technologies, interconnectedness makes cyber security more challenging, and it's hard to predict consequences of cyber security events—or any grid events, for that matter. Utilities are concerned about the potential for cascading failures, such as the one that occurred in the Northeast blackout in 2003. In 2011, more than two million people in the U.S. Southwest lost power after the loss of a single 500-kilovolt transmission line that led to cascading outages in Arizona, Southern California, and Baja California. Nobody could have anticipated that shutting down a 500-kilovolt line would have led to such a widespread blackout.

Some grid devices are 30 to 50 years old. Even though you cannot put cyber security controls on these old devices, you are not going to replace them unless they break because they can cost millions of dollars and require 18 months to two years to replace. So you are addressing an environment that has modern and old technologies and figuring out the best way to address threats and vulnerabilities.

Articles in the media about power sector security typically focus on data breaches. Utility control systems are not typically accessible via the Internet. NERC has specific requirements about how various grid devices can be accessed. So you can't just call up or connect to these devices and bring down the grid. Some people think that it's very easy to hack the grid, but it's not.

A couple years ago, a utility had its customer and billing information compromised, but that's the information technology side, not grid operations.

> "Maintaining electricity availability today while simultaneously planning for future cyber security controls is extremely difficult."

EJ: What's the status of cyber security in the European electric power sector?

Lee: Europe's power sector is different from the United States. In the United States, there are roughly 3,000 utilities—municipal utilities, co-operatives, investor-owned utilities, all different sizes, some vertically integrated, some not. In Europe, there are only a few major utilities in each country. These utilities make our large utilities look very small. They do not have mandatory cyber security standards as North American utilities have through NERC.

The European grid uses some different communication protocols than the U.S., but grid devices, vendors, and security requirements are the same internationally. So they're going to have the same cyber security challenges.

EJ: How might a utility's size affect its ability to secure the grid from cyber threats?

Lee: That is a huge issue. Let's say you decide to deploy an upgrade or a patch to a device in customer meters. You'll have to manage that with millions of meters, and those meters may be out of communication during the upgrade. The large scale of the European utilities will impact their decisions on cyber security solutions.

EJ: Describe the activities and plans of the European cyber security panel.

Lee: This group is providing guidance to the European Commission as the European Union looks at the potential of developing cyber security regulations for the energy sector in Europe. The Commission selected 14 individuals to provide input and recommendations and will take those to the European Union. All panel members are from Europe except me. We've had two meetings—one last December and one in March—and two more meetings are later this year.

I chair the working group called Practices and Gap Analysis. We've been requested not to publicly divulge information about our deliberations, even when we turn our reports over to the European Commission. They will determine what to make publicly available.

Cyber security in the energy sector is a small community. It's an impressive group of people, and the discussions are very technical. That makes it a lot of fun for me.

I'm also learning about the priorities and concerns of the other panel members and their organizations.

EJ: What lessons from your cyber security experience can you transfer to Europe?

Lee: When you work in cyber security, it's important to understand the requirements and needs of the specific application. I've written cyber security standards and guidelines for many different applications such as law enforcement, homeland security, and the federal government. Through these experiences, I've learned how to delve into an application and figure out its unique requirements. That's the fun part of this work.