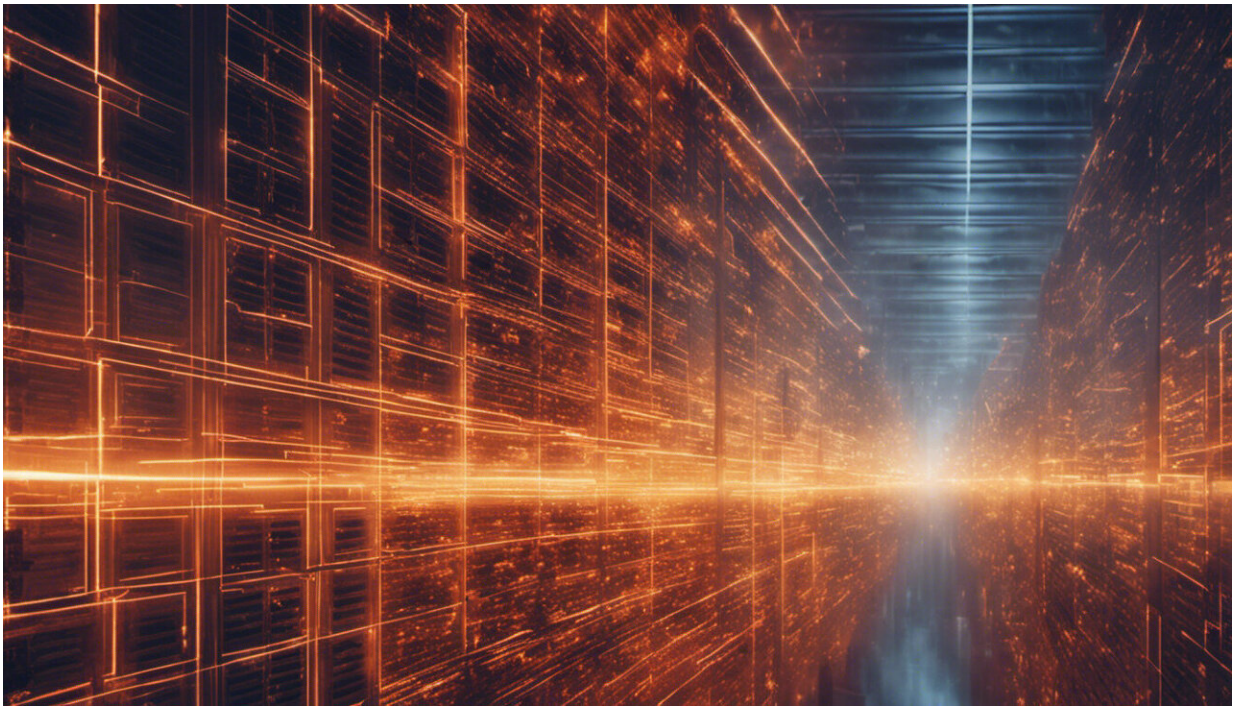
Electricity grid cybersecurity will be expensive – who will pay, and how much?

May 8 2019, by Dominic Saebeler And Manimaran Govindarasu



Credit: AI-generated image (disclaimer)

Recently, a neighbor asked one of us whether Russia, China, North Korea and Iran really are capable of hacking into the computers that control the U.S. electricity grid. The answer, based on available evidence , is "Yes." The follow-up question was, "How expensive will it be to prevent, and who will end up paying for it?"

The answers are: Likely tens of billions of dollars, and probably us, the electricity customers. This is a major – and, in our view, vital – investment in community and national security. But as scholars of grid cybersecurity, we understand it's not very clear what consumers will be getting for their money, nor whether utility companies themselves should bear some share of the cost.

Paying for reliability

In the U.S., the electricity grid is a ubiquitous system that's highly reliable. Most consumers expect the lights to turn on when they flip the switch, and don't think much more about it – except when paying the monthly bill.

Electric power companies' high levels of performance depend on interconnected computer systems, which are vulnerable to cyberattacks. Hackers took down portions of Ukraine's electricity grid in 2015 and 2016, cutting power to hundreds of thousands of people. U.S. officials regularly report that foreign agents are working to infiltrate critical infrastructure systems, like computers that control the power grid. An as-yet-unspecified "cyber event" affected the power grid in California and Wyoming in March 2019, according to the U.S. Department of Energy.

While media coverage and neighborly conversations have increased public awareness of the risks to the grid, most people's thinking hasn't changed much. People regularly evaluate how much they pay for car insurance, whether they need to buy life insurance, what the risks are of a recommended medical procedure or whether they feel safe flying in a Boeing 737 Max 8 airliner. But they rarely consider whether they're paying the right amount to ensure that the lights come on when they're needed.

Credit: AI-generated image (disclaimer)

But what about protection?

It can be difficult even for experts to keep track of all the potential risks to the grid, an interconnected set of industrial control systems. There are big threats from very rare events, like massive solar flares. And there are relatively minor threats from nearly certain incidents, like trees falling on wires. In between are cybersecurity concerns – which themselves can range from one individual hacker playing around to a national government orchestrating intrusion attempts into the national grid.

Now consider how much we, as consumers of utility service, might be willing to pay to protect against those dangers. Making a system more secure and reliable costs money, but often the economic benefits are hard to quantify. How much was saved by preventing a citywide

blackout? Was it worth millions – or billions – of dollars invested in protection? Even if that could be calculated, it's not easy to communicate effectively to the public, who regularly face many difficult choices about where to spend their limited money.

Recouping the costs

Collectively, utility companies in the U.S. are already planning to spend billions of dollars a year on grid cyber defenses. Those investments will include securing locations and equipment, improving the security of the utility supply chain, and continuous training and workforce development. This spending in turn brings up another complication: Most electricity utilities are highly regulated by the government, so they have to provide a certain level of service and spend money on required compliance activities. In return, those utilities are permitted to recover a certain return on their investment.

When utility companies' costs rise, they typically ask for permission from regulators to raise the prices they charge customers. What those customers can ask for, and in our view what regulators should insist on, is clear information about what those charges will be paying for.

Right now there is ongoing research exploring what the best practices are for cyber defense of public utilities, but there is only limited useful information about what those measures should cost. Ultimately, consumers can reasonably expect to shoulder some of the cost – but should get as much information as possible about the benefits that will result from the rates they're paying.

Provided by The Conversation