If South Korea's nuclear plant staff are vulnerable, then so are the reactors

December 23 2014, by Alan Woodward

South Korea relies heavily on nuclear power. Credit: Barbara Walton/EPA

Claude Shannon, who many consider the father of modern information theory, wrote a paper in 1949 in which he pointed out that security should never be based upon your enemy's ignorance of how your system is built. This is known today as the mantra: "There is no security through obscurity". Does it matter then that a South Korean nuclear plant was hacked and plans of the complex stolen? That rather depends on what

happens next.

As it is South Korea that's the subject of this latest attack everyone tends to assume it must have had something to do with North Korea. With a target as sensitive as a nuclear power plant, not unreasonably people are asking if safety could be compromised by a cyber attack. Could hackers cause the next Chernobyl or Three Mile Island? The South Korean authorities have sought to reassure the public, making it clear that no "core systems" – those computers that control the reactor and safety systems – were compromised.

If it was North Korea – and there is no evidence it was – then one might imagine it was actually the technical details and blueprints of a modern nuclear reactor that was the intended target. But sadly there is secondary security implication: the plans reveal the role of the human operators in running the reactor, and when it comes to hacking into critical infrastructure it is people that are the weakest link.

Weakest link in the chain

For example, when Iran's nuclear reprocessing plant at Natanz was hacked with the infamous Stuxnet virus, it should not have been possible as the computers affected were not connected to the outside world. There was a very distinct "air gap" maintained between the reactor computer controllers and any other network. But that air gap was relatively easy to bridge, by leaving USB sticks where curious people would find them, plug them in, and transfer the virus to the systems.

Imagine that – now you know which computers operate a nuclear power plant, and who uses them, which departments they work in, and at what times. Suddenly it's possible to design a very targeted attack on the operators themselves, aimed at fooling them into breaching their own security. Information about people and processes that operate a

technology is as valuable to a hacker as knowledge of the technology itself. Not only did Stuxnet damage equipment, it caused the computers to falsely report that all was well to the operators. It doesn't take much imagination to see how the same could happen to a nuclear power plant – with devastating consequences.

And so although it's great to hear that the plant operators are running safety drills I really hope they make sure that their security drills include the vital triad of people, processes and technology.

The 'soft target' of civilian infrastructure

This again points to an important and infrequently discussed problem, the vulnerability of critical national infrastructure. Cyber-attacks like these are a great way of levelling the playing field: why invest in massively expensive nuclear weapons programmes if you can simply shut down your enemies' power, gas, water, and transportation systems? Increasingly more and more infrastructure is connected to the internet, with all the security risks that entails.

And many of these systems – hardware and software – are old, updated far less frequently than a desktop computer at home or at work. Computer security flaws that may have ceased to be a problem in data centres or on desktops years ago might still affect an embedded system running a gas pump, sluice gate or electricity sub-station somewhere.

The UK government at least has been on the case for some time, having established the Centre for the Protection of National Infrastructure (CPNI) to focus on infrastructure resilience to cyber-attacks. Bringing together various government agencies and businesses, it has made significant progress in at least establishing what might be vulnerable, which is the first step in knowing where to focus your efforts.

There is no room for complacency, however, as every day more systems become internet-connected, and more security vulnerabilities are discovered. This trend of attaching everything and anything to the internet – such as with the growing Internet of Things, but not limited to that – is embraced even more enthusiastically in Europe and the US. Take a look at search engines like Shodan or Thingful which show locations of online devices, and see just how widespread the Internet of Things has already become.

This problem will not go away. It is a fact now and will only grow in the future. Security is possible only by including people and processes as well as technology. And anyone who relies solely on security through obscurity is doomed to fail.

Source: The Conversation