THE HUAWEI STOR

Kacy Zurkus reflects on the ongoing dispute between the US and the Chinese telecoms company Huawei, and asks what the future might have in store

Confused about the status of Huawei and the impact of the US ban on American companies selling technology to the Chinese telecommunications giant? Well, it's with good reason, particularly since President Trump has started to waiver on his once firm position that American companies will no longer be allowed to sell goods to Huawei.

On May 15 2019, President Trump signed an executive order restricting companies in the US from using telecom equipment made by companies that were suspected of posing threats to national security, according to *Reuters*.

As Huawei had already been identified as a potential threat that had allegedly conspired to steal trade secrets from global organizations, the company was added to Trump's 'Entity List,' "in part, because it could build undetectable backdoors into 5G hardware and software, allowing the Chinese government to spy on American communications and wage cyber-warfare," *Bloomberg* reported.

Despite all the hype, President Trump has started to soften on his prior stance with regard to the Chinese telecommunication giant. Following talks with China's President at the end of June, Trump reportedly said that he would allow Huawei to buy products from US firms.

Still, the future remains murky at best given that lawmakers have introduced legislation that would prevent the administration from relaxing export restrictions on Huawei, according to *World Trade Online*. Even though President Trump indicated that the US would begin lifting some restrictions on Huawei, Senators Marco Rubio and John Cornyn are seeking to block companies on the 'Entity List' from buying products from US companies, the *Wall Street Journal* reported.

Why is Huawei an Issue?

This issue is at the heart of the concerns about Huawei products, but there are also hundreds of manufacturers that use Chinese components, so there is a trickledown effect that many fear would pose national security risks.

Why foreign companies are placed on the US 'Entity List' is something that many ordinary US citizens can't really understand. The main reason Huawei has been banned is because its devices could potentially be used to spy on anyone using them.

"It could be used for spying on individual people. Maybe it could be used for industrial espionage," says owner and chairman of ProPrivacy, Pete Zaborszky. "Worst case scenario, it could be used to spy on the government."

Many accusations have been made against Huawei, including the suggestion that there are hardware compromises that, in some way, are able to take data and send it to the Chinese intelligence community.

The Ripple Effect

As US-China relations become more strained, companies outside of the scope of tariffs are beginning to feel the effects, with Huawei suffering major blows from the US government.

As the ban has most notably impacted the global telecommunications provider, Huawei filed a lawsuit against the US government for violating the Due Process Clause and the Separation-of-Powers principles enshrined in the US Constitution. In the case of the latter, because Congress is "both making the law, and attempting to adjudicate and execute it," as *Infosecurity* Magazine reported.

Tensions continued to mount as US companies have also been impacted by the ban. FedEx filed a lawsuit in response to the federal restrictions. In a statement explaining the suit, FedEx claimed that the "prohibitions contained in the Export Administration Regulations (EAR)...unreasonably hold common carriers strictly liable for shipments that may violate the EAR without requiring evidence that the carriers had knowledge of any violations. This puts an impossible burden on a common carrier such as FedEx to know the origin and technological make-up of contents of all the shipments it handles and whether they comply with the EAR."

Even though Huawei products have long been difficult to buy for US consumers, the company produces more than consumer phones. "They also do telecoms equipment, which is something Sprint of Verizon would use. Now the ban has expanded to everything that is Huawei," points out Zaborszky. Given that the ban restricts the use of Huawei in Google apps, that's going to have a significant impact as the phones will be virtually unusable for Android.

Y: AN ANALYSIS

The Industry's Quiet Reaction

Some voices in the tech industry have recognized the potential security risks that could result from the ban along with the impact of Huawei no longer using the Google Play store, but Zaborsky thinks the industry has been strangely quiet about the whole ordeal.

"From a handset standpoint, Huawei is a lot more popular in Asia than it is in the US, so the market response from the consumer side has been relatively muted," agrees Clay Miller, CTO of SyncDog.

As Huawei is a provider of telecoms equipment, US cellphone providers and tower providers are likely going to have a more negative reaction to the ban, especially since Huawei is a major 5G provider on a global scale, Miller adds.

The security issues brought to light because of the hype around Huawei have had a more indirect impact, argues Brian Egenrieder, SyncDog's chief research officer. "People are being more introspective and asking 'If Huawei is doing it, who else is doing it?'" Egenrieder says.

Rather than speaking out in reaction to the ban's impact, Egenrieder insists more people are stepping back and questioning everything they are doing around mobile devices and mobile technology.

> ***"From a handset standpoint, Huawei is a lot more popular in Asia than it is in the US, so the market response from the consumer side has been relatively muted"***

Though the ban is not baseless, there is reason to question whether the cybersecurity market's reaction to the tech giant is the right one when it comes to concerns of national security. Data security is at the heart of the Huawei debate, but Egenrider points out that it wouldn't be at the forefront of these retaliatory actions if companies practiced strong endpoint security policies in the first place.

"The industry has not really reacted to the market in terms of responding to the trust issue. Banning one provider is not going to solve that problem," Miller says.

Huawei & the Future of Modern Technology

The ban is limited to network infrastructure that the US assumes has a high risk of being compromised, but what about other providers or other players in the industry that also have backdoors that nobody knows about?

What the security industry can learn from the current debate is that everyone with a mobile device is vulnerable to being compromised, Miller explains. "We have to assume that from point A to point B, we may send data over a compromised network. We can't trust that our devices are not being backdoored, or that our network hardware going over a cell tower is secure."

Assuming that modern technology is vulnerable forces the industry to see what steps can be taken to protect data even if it is sent over compromised networks. "You have to assume there is a non-zero possibility that data exchange is going to travel an insecure network in one way or another," Miller says

Huawei has revealed that modern technology isn't really intended to secure the data being exchanged. The reality is that Huawei has only brought to light the fact that we have been trusting that mobile and network hardware installed in service providers is secure.

"Now we have to move forward, separating the data from the device. Assume the device is compromised, so protect that data no matter what device it's on," concludes Egenrieder END