Helping to secure the industrial Internet of Things with KPMG and Microsoft

KPMG's experience can help manufacturers make decisions on connected device security, according to **Ronald Heil**, Global Cyber Security Lead for Energy and Natural Resources, KPMG International & Partner, KPMG in the Netherlands; **Motoki Sawada,** Partner, KPMG in Japan; and **Norikazu Hosaka**, Director, KPMG in Japan.

Internet of Things (IoT) devices are being increasingly employed in industrial sectors, including energy and manufacturing.

An energy company can install thousands of internet-enabled rust sensors along the length of a pipeline to monitor its condition regularly, as long as they can connect to a network. Power networks can use IoT in the shape of smart meters to manage temporary local demands, such as many drivers recharging their electric vehicles in the early evening. Manufacturers can use IoT to monitor factories for potential problems and to track output in real time.

What are some of the security risks to industrial users of IoT technology?

IoT devices are often inexpensive pieces of rapidly developed commodity hardware with little to no security built in. However, this situation is improving in some countries and industries. For example, Singapore has set guidelines for IoT in critical infrastructure; similar standards are developing for healthcare devices; and automotive companies are exerting pressure on IoT component makers to secure connected vehicles.

But there's currently little investment in security by IoT device makers, increasing the risk that cyber attackers could use them to interfere with or halt manufacturing processes. These security risks can be reduced by using IoT devices for monitoring rather than controlling processes and connecting them to the internet through 5G networks rather than internal networks. Larger companies often do both, but even then, an attacker could cause damage through false alerts or blocking flows of data which could, for example, shut down a factory during a Christmas manufacturing rush.

Organizations should not introduce IoT technologies just because they exist. One port operator considered replacing the steel blocks used to stop rail-mounted crane gantries falling into the water with IoT sensors which would cut the power if a gantry got too close to the edge. But this could open the possibility of a cyber attacker trying to push a crane off the dock or freezing it when unloading containers by blocking its signals or manipulating its sensors. You can't launch a remote attack on a steel block, so it doesn't make sense to replace it with technology.

There can be a clash of cultures within organizations over the use of IoT. Younger workers are used to everything being networked and are more willing to take risks and hit reset buttons if anything goes wrong. Older staff who are used to industrial operational technology (OT) are likely to be more cautious. There are good reasons for this, particularly when considering how to control processes. However, completely ruling out IoT could mean ignoring a useful technology. In our view, a better option is to use IoT appropriately and securely.

What does Microsoft offer to secure IoT devices?

Given its insecurity, it makes sense to manage IoT devices at a network level. Microsoft's Azure Defender for IoT, which incorporates technology from CyberX (acquired by Microsoft in 2020) is designed to carry out three processes: asset management so you know what devices are connected to your network; checking the state of its security; and detecting interference. Moreover, the advantage of Microsoft security services is that they span both IoT and IT.

KPMG in Japan already had several years of experience with CyberX before its acquisition, using the product to provide risk analysis services to major manufacturing customers. CyberX's advantage was that it was 'agentless' — it didn't require software to be installed on industrial OT, avoiding changes to essential equipment that could risk disrupting production. Microsoft has adopted the same model for Azure Defender for IoT.

Other suppliers can provide a similar range of services to Azure Defender for IoT, but it has the advantage of integrating well with other Microsoft products, including the enterprise-wide security analytics tool Azure Sentinel. This can help detect attacks involving other Microsoft products, such as with compromised IoT devices spreading malware across other devices.

It's important to realize how much modern factories and industrial processes depend on IT. For example, a large train station considered to be one of the busiest segments of the railway in Europe with many tracks has around 2,000 servers installed for managing the industrial side of its tracks. This is the same number of servers one Dutch bank uses across its entire organization.

What does KPMG offer?

Some clients involve KPMG purely in their security risk assessment, but we have broader capabilities to help secure IoT with the goal of increasing protection, improving detection and readying organizations to respond to attacks. We have significant expertise in supporting OT, which has substantial differences from IT, and in addition to our experience with Microsoft products, we work with products and services from multiple vendors. We can also run training, including simulation exercises.

KPMG firms can help multinational manufacturers use IoT to help run overseas factories remotely and securely from their headquarters. For example, KPMG firms in Japan, Thailand and Vietnam work together to support Japanese companies that operate factories in South East Asia. We believe this area is set to grow, given long-term trends towards manufacturing goods closer to consumers, and more recently, COVID-19 making travel more difficult. Manufacturers in Japan are struggling to find specialist staff to run IT networks, which can make it more efficient to use IoT to remotely control systems from a hub rather than try to recruit for every factory. But centralizing like this underlines the need for security.

What first steps can organizations take to help improve IoT security?

It is vital to know both your organization and your likely adversaries. Technologies such as asset management can help with the first, but assessing your adversaries is a judgement call. Each organization has their own security needs, so it is important to spend time and money on any potential threats relevant to you. This also presents a dilemma — if you over-assess the threat, you could waste resources on overly tight security.

There are basic decisions to make, such as whether IoT devices should be connected to internal networks or the internet, or whether they should be used for controlling versus simply monitoring. You also should work out the current level of your security before setting your ambitions. One option is to meet an industry baseline, such as the International Electrotechnical Commission's series of IEC 62443 standards,[1] then work out what needs to be done to achieve this.

There is often a gap between what managers think is the case versus reality, such as believing that a factory's systems are segregated for security purposes when they're not. OT users may have weaker security practices, such as not setting passwords or using weak ones. Speed is important, so this might have been acceptable in a physically secure location, but that may no longer be the case when such equipment is online. One incident involving a country's national power grid saw operators switching off virtual servers, but attackers turned them back on remotely. Experienced industrial workers may not expect that, but if you are to take appropriate advantage of IoT, it is vital to know what can go wrong and subsequently determine how you can help protect your organization against threats.

[1] https://www.iec.ch/blog/understanding-iec-6244

What comes next is driven by KPMG

To find out more contact:

Ronald Heil
Global Cyber Security Lead for Energy and Natural Resources, KPMG International & Partner, KPMG in the Netherlands
T: +31 (20) 656 8033
E: heil.ronald@kpmg.nl

Motoki Sawada
Partner, Technology Risk Services
KPMG in Japan
T: +81 (0)80 8000 4088
E: motoki.sawada@jp.kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Designed by Evalueserve.

Publication name: Helping to secure the industrial Internet of Things with KPMG and Microsoft
Publication number: 138698-G
Publication date: March 2023