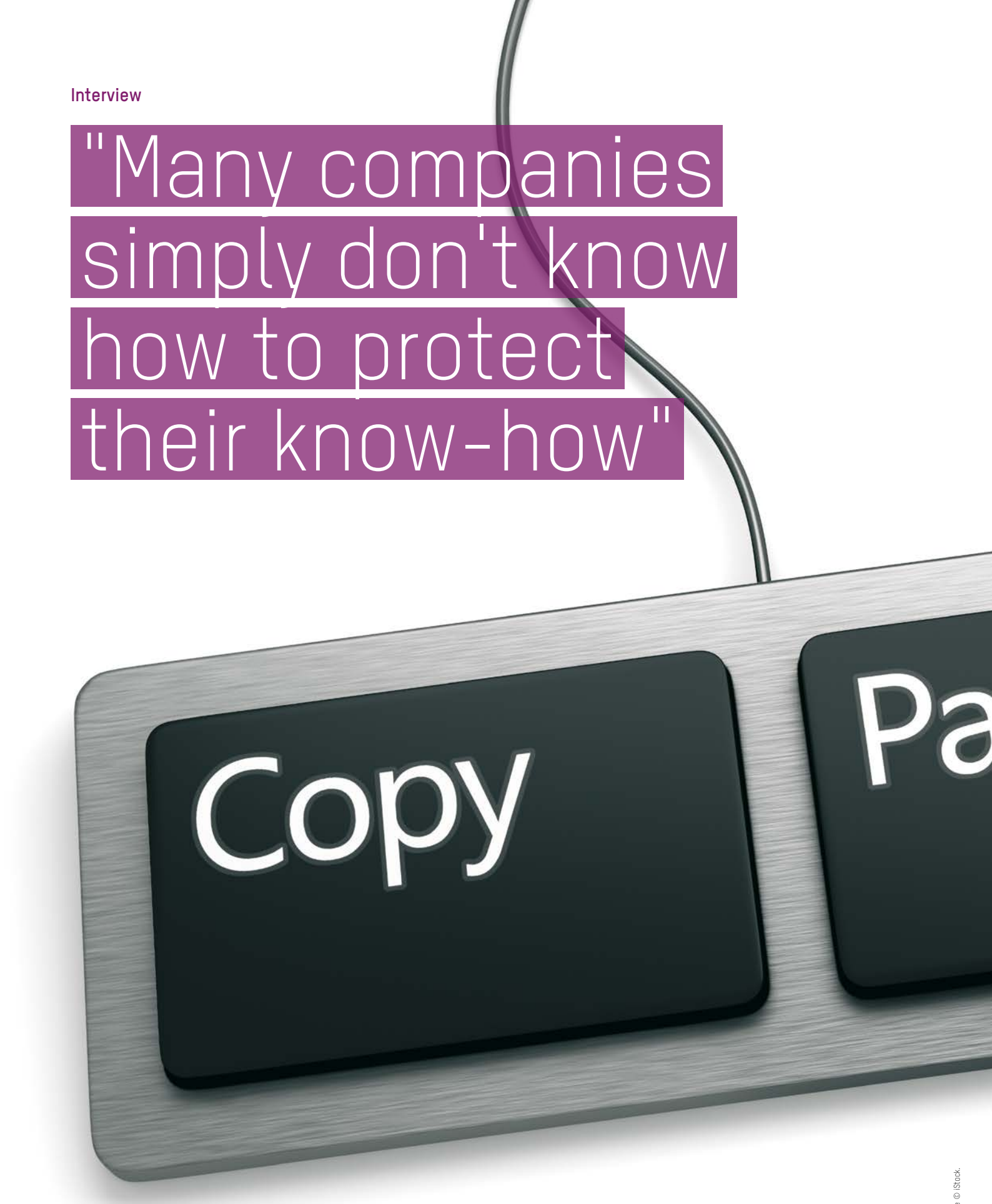
"Many companies simply don't know how to protect their know-how"



Photoe © iStock.

Year after year, manufacturing and processing companies suffer damages in the billions due to their products being produced illegally, both at home and abroad. Manufacturers and owners of production machinery and equipment need to take measures to protect their products and their intellectual property. Oliver Winzenried, from the German Engineering Association VDMA, explains what this type of security might look like in practice.

What are the potential risks of intellectual property theft for manufacturers of machinery and equipment?

Each year, VDMA members experience estimated damages of around €7.9 billion – or about 4% of their total revenue. These are the results of the most recent product piracy survey held by the VDMA every two years. Nine out of ten companies with over 1,000 employees are affected. More then 50% of them report having had entire machines or products reverse engineered.

Are these companies aware of the potential threat?

Certainly. Others quickly become aware once they see an imitation first-hand or face warranty claims for counterfeit products. Only upon closer inspection does it become clear that they are dealing with an illegal copy rather than their own product.

"Manufacturers and operators of industrial equipment need to safeguard their know-how and their products," says Oliver Winzenried, chairman of the VDMA consortium on product and know-how protection.

Are there any sectors that are affected more than others?
There are indeed. The most heavily affected are wood processing, textile and agricultural machinery.

Where do the counterfeits typically come from?
The main source of counterfeit machinery and products continues to be China. Although the number has gone down slightly from our previous survey, at 72% it is still very high. Many are surprised to learn that second place for pirating goes to Germany.

How do these counterfeiters generally operate?
The most common approach – again at 72% – is reverse engineering. They take apart the machine or product and analyze it. Then they copy the mechanical components and decompile the software. The final step is to figure out the processes performed by the machine. These can then be implemented on the counterfeit machine without any significant development expenses or years of field experience. In a way it's not strictly counterfeiting, because they actually understand and apply the processes themselves. However, it does constitute infringement of any patents that exist on the equipment.

Why don't we see more protective measures in place?
Many companies simply don't know what technical options are available, or which measures are appropriate for their machinery or products.

What about techniques that have proven themselves in IT applications?
Protective measures used in an office environment have limited application in industrial machinery. You can't ask a processing plant, for example, to reboot or run a virus scan that locks up the system for minutes at a time. The requirements are simply very different.

What options are available for OEMs?
Manufacturers of integrated systems can't be expected to develop and implement security measures for each individual component themselves. That must be the responsibility of the component supplier. Still, the machine manufacturer faces a considerable challenge in ensuring that these functions are integrated into the overall system and used properly.

What are the security needs of plant owners?
If you own a clothing brand with production

sites in Asia, you want to be sure that those sites are only producing the specified quantities and are only delivering them to you. You want to prevent those sites from producing excess items and selling them on the gray market for their own profit. With appropriate measures in place, this kind of unauthorized production will not go unnoticed. These measures have applications in every industry, but are still in their infancy. With the onset of Industry 4.0 and big data in production, cybersecurity is becoming increasingly critical.

Are there any standards that can provide manufacturers a frame of reference?
National and global standards, like those established for safety equipment, do not yet exist for cybersecurity. Emerging standards such as IEC 62443 and ISA-99 attempt to define Security Assurance Levels (SALs). These account for the protection of products and intellectual property as well as protection against manipulation and modification.

What criteria should a manufacturer consider when selecting a supplier?
Manufacturers and operators should ensure that they will be able to protect their know-how. If you select suppliers who use open communication standards, you can be assured that interoperability won't be a problem. This is fundamental if you're integrating components from various suppliers into an overall system. And if these open standards also support cybersecurity, this is clearly a huge advantage for the user.

Some examples include OPC UA and IEC 62541, which enable safe communication between components. Intelligent protection opens up new business models for machinery and equipment manufacturers by allowing functions implemented in their software to simply be enabled or disabled for a given machine configuration. ←

Safeguard your know-how with Technology Guarding

Technology Guarding provides reliable protection for B&R customers' products and know-how. The required USB dongle is installed by B&R during assembly.

With B&R's Technology Guarding, manufacturers of machinery and equipment can reliably safeguard their process data and know-how. They can manage licenses easily and monitor hours of operation reliably.

Technology Guarding offers a way for B&R customers to manage the growing portfolio of options they offer for their machines. On the one hand, equipment owners generally don't want to pay for functions that they won't be using. On the other, the manufacturer of the equipment doesn't want to hand out valuable functionality for free.

The result is that options have to be managed on a customer-by-customer basis. B&R's license management system has the answer. Each customer's licenses are managed on a central license server and implemented on the machine using a USB dongle.

USB dongle included in hardware assembly
Technology Guarding is programmed in Automation Studio and applied to the hardware using a USB dongle. B&R installs the Technology Guarding dongle during hardware assembly, allowing the customer to have components delivered directly to their panel maker. And of course it's no problem if the hardware ever needs to be swapped out in the field. Simply insert the USB dongle in the new component and it immediately resumes its function.

Secure monitoring of operating hours
Technology Guarding helps machinery and equipment builders protect not only their own interests, but those of their customers as well. It is possible, for example, to monitor a machine's hours of operation in a way that cannot be tampered with. This prevents unauthorized products from making their way to the market illegally.

Technology Guarding provides the perfect technical basis for a leasing business model, allowing manufacturers to ensure that operating hours are counted and documented accurately and free from tampering.

The advantages
- Safeguard product know-how and process data
- Secure monitoring of operating hours
- Manage machine options efficiently