MATTER OF TECHS AND BALANCES

**DIGITALISATION** allows operators to cut costs and improve safety, but it also opens doors to new types of cybersecurity threats, writes Anamaria Deduleasa.

For example, one source tells Upstream the equipment that enables remote monitoring and data gathering on installations such as floating production, storage and offloading vessels could be hacked.

"For remote monitoring you need to install sensors, a multitude of them, to keep an eye on things. These sensors are easily hacked."

While a compromised sensor in itself may not pose much of a threat, it could potentially "provide a sort of doorway to other parts of the main framework", the source says.

Another source points to the continuous development of digital technologies that increasingly push work previously done manually to the virtual sphere.

While this offers considerable benefits, it also creates never-ending race towards updating cybersecurity measures.

"The more the digital aspect evolves and companies in this industry use it to support their business, the further we dive," he says. "There is no way we can get ahead of this potential problem. We just can't."

Cybersecurity companies are always developing new ways to secure assets, but hackers are always coming up with new ways to breach systems.

"It's less about 'full protection', and more about managing risks," Duncan Greatwood, chief executive of cyber security company Xage, says: "The key thing is to shift cybersecurity from the limited forms of security in place today. For example, an anti-virus on a device or a firewall is a good thing, but the reality is that you can't assume that any one measure is going to protect you."

He advises a strategy of "control every interaction between every different system component, so not to allow communication unless it has been authenticated".

"You should never have a situation where someone, just by being on the network, would be allowed to do anything," Greatwood says.

He suggests a strategy of "strength in numbers" — a digitalised environment in which the more components you have, the more complicated it becomes for hackers.

"Every interaction needs to be controlled, every identity needs to be managed, and that's how you actually get a secure system. However, in oil and gas, we have quite a distant network before we get to this point," Greatwood says.

"Cybersecurity has moved to the top of people's agenda. There are measures being taken, around 20% of what needs to be done, but still, these initial measures are worthwhile. A lot more will be done over the next few years."