SECURITY

Cybersecurity focuses on phishy business

Trade secrets, **infrastructure** and **safety** are on the line in the **digital age**, and the oil and gas **industry** is as **susceptible** as any sector

ANAMARIA DEDULEASA
London

AN AUTOMATED machine dispenses fish food once a day in a fish tank in a casino in Las Vegas. The chip controlling the system is hacked, and, once hackers are in, the dispenser provides access to the entire system operating in the casino.

The widely circulated anecdote is used as a warning of the vulnerabilities of an increasingly digitalised business world, including upstream oil and gas.

"We don't want to be the casino with the fish food," says Duncan Greatwood, chief executive of cyber-security company Xage.

Greatwood's point comes as the oil and gas industry dives into the digital world, one in which people and devices are more connected than ever, but also increasingly susceptible to cyber attacks.

The benefits of digitalisation for the industry are undisputed, as it creates cost cuts for companies, creates a wave of new highly skilled jobs, improves safety and cleans up operations in a world bent on cutting emissions.

While there is a lot that distinguishes the oil and gas industry from other sectors, when it comes to information security it is like any other — perhaps even more vulnerable, as the physical distribution of oil and gas operations creates additional risks, experts say.

Cyberattacks against the industry were reported in 2017, when Russia's Rosneft and Denmark's Maersk Oil were hit by a virus called Petya, an example of ransomware, in which hackers demand money for the return of sensitive information.

While companies continue to prioritise cyber-security, they are more worried than ever about the complexity of the threat landscape.

Connectivity: the energy industry is seeing a growing reliance on digital and remote control
Photo: BP

Last year, services giant Petrofac suffered an IT breach following the discovery of malware in its systems in the Middle East, while Italy's Saipem was hit with a variant of the so-called Shamoon malware.

Aramco incident

A previous version of Shamoon was used to attack Saudi Aramco in 2012 and wipe clean around three-quarters of its computers, leaving only images of a burning US flag behind.

A recent survey by consultancy EY of more than 1200 industry professionals shows that 60% of respondents have had a recent "significant" cybersecurity incident.

The industry increasingly operates in a digital world, with more and more data stored in the cloud and a growing reliance on automated equipment controlled digitally and remotely.

Trade secrets, vital infrastructure and safety are on the line, experts say.

A broad overview, based on research from multiple consultancies and cybersecurity experts, suggests the sector is vulnerable to attacks at all stages, from exploration and production, processing and refining, distribution and trading.

This should not come as a surprise to anyone who understands that anything connected through the internet of things is open to potential breaches.

Viruses can spread from one infected machine to other computers on a network. Once a system is infected, the virus continues to compile a list of files from specific locations within the system, upload them to the attacker, and then erase them.

Finally, the virus overwrites the master boot record of the infected computer, making it unbootable.

While companies continue to prioritise cybersecurity — and are making good progress in identifying and resolving vulnerabilities — they are more worried than ever about the complexity of the threat landscape, EY says in its report.

The findings revealed that 78% of respondents still consider a careless member of staff as the most likely source of an attack, with more than half concerned about phishing — fraudulent emails disguised as trustworthy sources but meant to obtain sensitive information.

Often used in conjunction with phishing, RAT (remote-access Trojan) programmes are implanted into industrial machines and remain dormant until activated.

Response plan

According to EY, a cyber breach response plan (CBRP) is essential to minimise the impact of such cyberattacks.

"An effective CBRP will encompass every point of interface, internally and externally. It should be regularly put on trial, and, when an attack occurs, it should be able to identify and isolate the invasive processes," EY says.

Nevertheless, new types of incidents are now lurking, with consultancy PwC pointing to the potential risks to workers' health and safety and massive potential environmental damage.

"The inherently risky nature of offshore oil and gas exploration and production activity... is exacerbated by the risk of cyberattack, whether that be nation state led, corporate espionage or even terrorist activity," PwC says.

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 a 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. So, 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 are good things, but the reality is that you can't assume that any one measure is going to protect you."

He advises companies to "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 distance to travel before we get to this point," Greatwood says. "(Cybersecurity) has moved to the top of people's agenda. There are measures being taken — probably 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."