Cybersecurity: living dangerously

From pipelines to refineries, oil and gas companies are responsible for critical infrastructure that is a prime target for cyberattacks. But cybersecurity experts say the industry has been worryingly slow to respond, write Katherine Dunn and Herman Wang
But for a coding error, an attempted cyberattack last year on a petrochemical plant in Saudi Arabia could have led to a catastrophic explosion.

Malware implanted into the control system to sabotage the plant accidentally triggered a shutdown, but investigators say the attack was one of the most technologically advanced they had ever seen. Chillingly, they say the assailants — still not publicly identified — have likely already fixed the glitch and are lying in wait to target their next facility.

That close call and several others have many experts convinced that the oil industry, even as it invests millions of hours on safety procedures, is ill-prepared on the cyber front.

“The sector is becoming fair game. [Hackers] are seeing opportunities to attack the sector, and facility operators believe they are very well-protected,” a Washington-based cybersecurity analyst at FireEye and former oil industry consultant, Marina Krotofil said, “It is not a good combination.”

Much of the focus on energy-related cybersecurity has been on power plants and grids, but authorities say oil and gas companies — responsible for critical infrastructure including refineries, pipelines and ports — are ripe targets for hackers to implant malware that can disrupt operations, endanger public safety, wreak havoc on markets and disclose sensitive information.

Spending on security measures is insufficient by and large, and collaboration among companies on best practices is woeful, given the secretive and competitive nature of the oil business, according to people in the field.

Often, national security can be at stake. In the Middle East alone, which accounts for more than a third of global crude production, cyberattacks cost the oil and gas industry $1 billion last year in outages and loss of confidential data, according to a March report by industrial services provider Siemens and the Ponemon Institute. However, only 47% of Middle East oil and gas companies surveyed in the report said they prioritize continually monitoring all infrastructure for cyber threats and attacks.

“In general, the oil industry is conservative in nature,” said Gary Williams, a senior director for Schneider Electric, which installs control and safety systems in refineries and other critical infrastructure often targeted by hackers. “The industry tends to take an ‘if it ain’t broke, don’t fix it’ approach to how we operate. But we must change this model, and our culture, when it comes to cybersecurity.”

Some experts warn it may take a major successful cyberattack for the industry to fully grasp how great the danger is. “Organizations need to invest in cybersecurity, but they don’t see it’s a major threat,” senior research fellow with Chatham House’s International Security Department Beyza Unal, said. “We haven’t seen an event where an entire critical infrastructure got taken out. But it will happen. So how do you get companies to invest in that?”

More complex, more often

Across the industry, energy companies spend less than 0.2% of their revenues on cybersecurity, according to a recent analysis by consultancies Precision Analytics LLC and the CAP Group. That is less than a third of what banks and financial services companies spend protecting their businesses from hackers.

Some experts warn it may take a major successful cyberattack for the industry to fully grasp how great the danger is.
Meanwhile, hackers targeting the industry don’t discriminate by size. Spanish oil company Cepsa is a relative minnow compared with giants like Saudi Aramco or ExxonMobil, but still finds its network targeted about 20 times each day. “Both the range and number of potential attacks are increasing,” Cepsa spokeswoman Marta Llorente Señorans said.

None of the attacks has succeeded, to its knowledge, according to company officials. Its facilities have not failed, and its operations have remained unscathed by any cyber-related outages.

The company, which operates two refineries with a throughput of 430,000 b/d and holds working interests in upstream projects with an output of about 100,000 b/d, is increasing cybersecurity spending by a minimum of 25% annually.

Eni, the Italian energy giant, said it has fended off several cyberattacks targeting its industrial control systems, including at the company’s refineries. “Cyberattack is one of our corporate top risks,” Eni spokesman Roberto Carlo Albini said. “We have developed a specific security architecture for industrial control systems, we perform vulnerability and security assessments on our infrastructure regularly, and we have a dedicated team for security monitoring and incident response.”

Cepsa and Eni’s acknowledgement of the problem is unusual. Many oil and gas companies contacted by S&P Global Platts for this story — ranging from state-owned companies to integrated majors, independent refiners and terminal operators — declined to comment on the issue or disclose cyber defense spending. Few disclosed any assaults on their systems.

**Unknown unknowns**

But experts say that known attempts account for likely just a fraction of the assaults launched every day – and it’s the ones that remain undetected that are the most worrying.

Many malware programs are intended to gather information on a plant, not necessarily launch an imminent attack, and they may lurk inside a system for months or even years before their creators gain enough intelligence to develop and unleash custom-built viruses that can take down an entire facility.

Hackers who have gained access to a system may just be waiting for the right moment to do their worst, said Daniel Quiggin, a research fellow at Chatham House who specializes in energy systems. “A lot of reconnaissance has gone on,” he said. “To what end, we don’t know, and that is why everybody is so concerned.”

In the case of the Saudi petrochemical plant incident, hackers implanted malware into the facility’s Triconex safety control system — hardware and programs manufactured by Schneider Electric — which regulates voltage, pressure and temperature. But rather than forcing a shutdown or disruption of the plant, the malware sought to reprogram the safety system, so that fail-safes would not be triggered when a subsequent piece of malware caused the plant to overheat, explode or otherwise catastrophically malfunction, according to FireEye.

Hackers who have gained access to a system may just be waiting for the right moment to do their worst

Given the sophistication of the malware involved and the likely long development time and cost it would have taken to build, authorities say only one kind of actor could be behind the intrusion: a nation state.

Investigators continue to look into the incident and have neither named the facility nor identified the attackers, though officials suspect they were backed by Saudi Arabia’s longstanding geopolitical rival Iran, a charge Tehran has denied.
With tensions rising in the Middle East, Krotofil said to expect more incidents targeting oil and gas operations there. “It’s strategic,” she said. “It’s countries where their ability to produce or not produce oil has a huge impact on global oil markets. Therefore, there are continuous, multiple attempts to disrupt operations in the Middle East.”

Iran has been steadily building its hacking capabilities, and the fear among US security experts is it could then turn a volley of attacks on the US, as it withdraws from the nuclear deal and re-imposes sanctions that bite at Iran’s oil exports.

“There are legitimate reasons to be concerned that Tehran’s intention in targeting critical infrastructure is to hold social and economic assets in adversarial countries at risk in the event it needs to escalate or retaliate during conflict,” the Carnegie Endowment for Peace warned in a recent report on Iran's cyber threat.

But Iran, too, has been a cyberattack victim. In 2010, the Stuxnet virus struck Iran’s Natanz uranium enrichment plant, manipulating its computers to send its centrifuges spinning at dangerous speeds. That incident occurred in the lead-up to an Iranian presidential election, and media reports later attributed Stuxnet to the US and Israel.

**Late to the game**

As the scale and complexity of malware has exploded in recent years, cyberwarfare has emerged as a new front in the battle to gain geopolitical supremacy. Governments and companies are scrambling to stay ahead of hackers and protect vital assets and resources.

But maintaining adequate cyber defenses is costly, as systems must be constantly updated to stay ahead of hackers as they innovate.

The industry has yet to agree on common standards, though trade associations, such as the International Association of Oil & Gas Producers and US refineries group American Fuel and Petrochemical Manufacturers have fostered discussion among their members, in concert with governmental bodies.

However, oversight is uneven and restricted by an inability for national governments and companies to keep pace with the rapid development of malware threats, consultancy Oxford Analytica said in a recent report. Many governments are already late to the game and hampered by a skills shortage.

**Attacks in recent years have become far more sinister**

“Although leaders might acknowledge the growing importance of the issue, few understand how to proceed,” the report said.

Also troubling is a growing relationship between state actors and criminal groups, with countries providing funding to low-level cybercriminals, as well as access to sophisticated hacking resources via encrypted dark web sites.

“I think what’s interesting that we’ll see in maybe five, 10 years’ time is the nexus between organized crime, terrorist organizations and hackers on the dark web,” Chatham House’s Unal said.

In the past, cyberattacks on oil facilities typically involved cybercriminals seeking proprietary information such as production levels, which they could use for market manipulation, said FireEye’s Krotofil. But attacks in recent years have become far more sinister, ambitious and potentially destructive.

Cyberattacks “have become much, much more complex, much more dramatic,” she said. “Attackers right now are trying to attack everything and see how far they go.”

It is a risk that oil and gas producers can no longer ignore.
In October, four South Korean hackers in Shanghai spent seven hours attempting to infiltrate an oil refinery’s corporate network to gain access to its control systems and shut the facility down.

Another 15 minutes or so, and they likely would have succeeded.

Fortunately for the industry, the attack was not real. It was performed in a live-televised cybersecurity competition put on by Internet security firm Kaspersky Lab. The competition pitted teams from around the world against each other in a race to breach a model of a real oil refinery that is one of the company’s clients.

None of the three teams in the final managed to bring the refinery down; the South Korean team came closest and won the contest. But as the organizers note, real-world hackers do not operate under such tight time restrictions.

“The contest demonstrated once again that, by exploiting weaknesses in the corporate network’s protection and network configuration faults, a remote threat actor can gain unauthorized access to the industrial segment of the network,” Kaspersky’s industrial control system vulnerability research group manager, Vladimir Dashchenko, said.

This was the third annual cybersecurity competition that Kaspersky has held. The 2016 contest invited hackers to penetrate the network of a model power plant.

The competition highlights the vulnerabilities of critical infrastructure, including oil refineries, as the stakes of cyberwarfare grow. The environmental and human toll of a cyber-induced disaster could be significant, to say nothing of the disruption to oil and gas markets.

“Oil and gas is one of the industries that is essential to how societies and economies function,” Dashchenko said.

The Moscow-based company earlier this year said it discovered malware infecting a control system installed at more than 1,000 gasoline stations that would have allowed hackers to shut down fueling systems, change fuel prices and cause leakages, among other acts of sabotage.

Kaspersky itself has faced allegations of helping the Russian government spy on its customers, as the US has banned the use of its products on federal networks and reportedly is weighing sanctions against the company.

The company denies the charges and says it is “caught in the middle of a geopolitical fight” between the US and Russia.

Malware lurking

Most sophisticated cyberattacks on oil refineries and other critical infrastructure are multipronged.

Hackers will first try to infiltrate the facility’s distributed control system (DCS) or supervisory control and data acquisition system (SCADA) by installing malware that collects intelligence on its operations, security features and other sensitive information.

They will often also try to gain access to the plant’s independent safety control system, usually with the intention of being able to override automatic shutdowns.
The malware installed to gather this data can lurk on systems for years undetected. Then, when assailants have gleaned enough information on the facility’s vulnerabilities and the time is right for an attack, they will unleash the targeted, sophisticated code they have developed to bring down the refinery – or worse, cause a catastrophe, such as an explosion that was narrowly averted at a Saudi petrochemical plant last year.

Investigators say that attack was foiled because of a glitch in the malware that had targeted the plant’s safety system.

“Most of the activity seen has been reconnaissance penetrating systems to try to understand these SCADA systems, such that when the attack is made, it’s effective,” said Daniel Quiggin, a fellow at Chatham House who studies energy systems.

To reduce the risk of being hacked, many facilities are “air gapped,” or isolated from public networks. But air gapping is not foolproof, as hackers can still use creative methods to exploit security holes and access secure internal networks. For example, they could steal personal information from an on-site vending machine that uses a wireless internet signal to transmit data and use it to breach the refinery’s secure operating and safety networks, or program a security camera’s infrared LEDs and sensors to transmit information.

“It’s good to have isolation, but there’s no such thing that could secure you with isolation,” said Beyza Unal, a senior research fellow with Chatham House’s International Security Department. “Now we are in an age where the legacy systems can’t cope with today’s needs. There are so many cases where we know air gapping wasn’t enough.”

Once the air gap is breached, facilities are as good as hacked. Companies are largely focused on protecting the perimeter of a plant from hacking, but have relatively few tools to detect or prevent an attack once the hacker is inside the system, experts say.

The event did not reveal any previously unknown security holes, known as zero-day vulnerabilities, as happened in Kaspersky’s previous two contests. But these exercises, known as “capture the flag” or CTF, are a crucial step for testing the security of computer systems, as the conditions closely model real-life scenarios.

“Everything that happens at a CTF site can also happen to real critical infrastructure and industrial systems,” Dashchenko said. “Cybersecurity risks [for oil refineries] are still high, and the industry should still take proper security measures for better infrastructure protection.”

Capture the flag

In the Kaspersky contest, the teams had to solve several tasks to breach the perimeter of the model refinery’s corporate network. Once they had accomplished that, they would be required to figure out the internal industrial system’s communication protocols and command the refinery to shut down.

The South Korean team was at the final stage of the corporate network level, the most difficult part of the competition, when time expired.

Had they gotten past it, the rest of the job would have been “very easy compared to the previous tasks,” Dashchenko said. “Based on our estimation, they were just 15-20 minutes away from completing it.”