www.NEWSBASE.com

NorthAmOil

North America Oil & Gas Monitor

Issue 524 06 • September • 2018 Week 35

Approval overturned

A Canadian court has overturned the approval that had been granted to the Trans Mountain pipeline expansion project.

Hitting new highs

US crude oil production hit record highs in June, according to data from the country's Energy Information Administration.

Back to normal

Energy companies in the US Gulf of Mexico have begun taking steps to resume normal operations after Tropical Storm Gordon made landfall.

Oil sands sale

Total and its partners are selling their interests in the Joslyn oil sands project in Alberta for US$171 million.

Keeping systems online

Georgia Tech is poised to help US oil, gas and power operators face significant risks in the area of cybersecurity, writes Jennifer DeLay

US

WHAT:
The university has created an online degree track for its graduate cybersecurity programme, which allows students to specialise in energy systems.

WHY:
The stakes are higher, given the increasing computerisation of the energy industry and the DHS' recent revelations about Russian attempts to hack US power grids.

WHAT NEXT:
The expansion of Georgia Tech's programme could help oil, gas and power companies secure the personnel they need to counter cyberattacks.

EARLIER this year, the UK-based risk management consultancy Marsh released a report showing that cybersecurity was moving up on the list of top priorities for the energy industry. Citing data from a survey conducted in partnership with Microsoft, Marsh stated that fully 59% of the energy executives involved in the survey had listed cybersecurity as one of their organisations' top five priorities. It also said that another 2% had identified cybersecurity as their number-one priority.

The consultancy further noted that no less than 76% of the executives had expressed concern about the possibility of their business operations being interrupted as a result of breaches in cybersecurity. But at the same time, it reported that 54% of respondents had not quantified or were unsure of the impact of potential losses from such interruptions.

Although the Marsh/Microsoft survey targeted executives from energy companies around the world, it seems safe to assume that cybersecurity issues are looming large on the horizon of US operators. The US Department of Homeland Security (DHS) reported in July that hackers employed by Russia's military intelligence agency had been showing increasing interest in the US power transmission grid. Over the last year, it stated, Russian hacking teams have mounted hundreds of attacks on US utilities – companies involved in power generation and transmission.

According to some sources, the problem is much more extensive. Speaking on condition of anonymity, US intelligence officials told the New York Times in late July that the DHS had significantly understated the number of attempts to upload Russian malware to networks involved in power systems. Technology and tech security executives have voiced agreement with this assessment, the newspaper said.

Closing the gap

Addressing the threat will not be easy, given shortages in the number of cybersecurity professionals available to address security challenges in every industry, not only energy. IT experts have estimated that the global shortfall in trained cybersecurity personnel may reach 2 million by the end of 2019.

But efforts are being made to close the gap. One such initiative is coming from the Georgia Institute of Technology, a public research university in Atlanta.

Last month, the university, known as Georgia Tech, expanded the scope of its graduate cybersecurity programme by announcing the launch of an online degree track in collaboration with edX in 2019. Like the traditional programme, the Online Master of Science in Cybersecurity (OMS Cybersecurity) degree track will offer students the opportunity to choose between three areas of specialisation, one of which is energy systems.

In short, Georgia Tech is set to play a role in closing the cybersecurity skills gap of the North American energy industry. *NewsBase Intelligence (NBI)* spoke recently with the faculty lead of the OMS Cybersecurity programme, Raheem Beyah, about the matter. Beyah – an industrial control cybersecurity specialist who serves as a professor in Georgia Tech's School of Electrical and Computer Engineering and is the co-founder of Fortipyhd Logic, an industrial control security company – provided an overview of cybersecurity issues in the energy sector and described the university's approach to overcoming current challenges.

Growing concern

Beyah noted that cyberattacks were hardly a new concern for energy operators around the world, pointing to past incidents such as the Stuxnet attack on Iran's nuclear energy scheme. Nevertheless, he said, the statements from the DHS in July make it clear that North American companies face major risks.

Washington's disclosures represent "one of the most significant announcements" made to date with respect to the security of US power transmission networks, Beyah said. "Nothing actually, from what we were told, was triggered or modified or executed, but there's evidence that Russian hackers are inside of our systems, inside of our power grid," he added. "It could have tremendous consequences if we're not able to detect and disrupt the various attackers that infiltrate our grid."

Thus far, he said, the cybersecurity programme's energy track has mostly focused on the threats faced by conventional power generation and transmission companies. He noted, though, ▸▸

"IT experts have estimated that the global shortfall in trained cybersecurity personnel may reach 2 million by the end of 2019.

Source: Georgia Tech

that Georgia Tech was not overlooking other US energy concerns. The programme also addresses the problems faced by renewable energy companies, as well as oil and gas producers and pipeline operators, he said. Indeed, he said, all of these enterprises face similar problems with respect to cybersecurity.

According to Beyah, the power transmission sector has come under close scrutiny for reasons that go beyond concerns about Russian hackers. Many grid operators have drawn attention because they make extensive use of operational controls and IT systems that are connected to the internet, he explained, and because their failure would cause widespread and immediate damage.

But this vulnerability is also a problem for renewable energy firms and oil and gas companies, he stated. Energy operators that use online technologies must treat every networked computer, every terminal and every smart device as a potential point of access for hackers, he added. They must also be prepared to expand the scope of their efforts, since production, storage and transportation activities are becoming increasingly computerised, he said.

Faculty and student synergies

The energy track of Georgia Tech's cybersecurity programme takes these similarities into account, Beyah said.

More specifically, he explained, the curriculum focuses on the physical systems that professionals are likely to encounter and use in the fields so that students will be able to make an impact wherever they land in the energy sector. "At a high level, it's a combination of networking courses, security courses and power systems courses, and [also] cyberphysical security systems courses," he said. "It's kind of an amalgam of different areas."

One reason the programme is in a good position to teach all of these skills is that it has fostered synergies among university faculty members from different departments, he added. "If you think about energy security the way I look at it, then it can be approached from two different perspectives," Beyah commented. On the one hand, he said, the programme makes use of energy specialists who have added cybersecurity to their portfolio of skills. On the other hand, he said, it includes cybersecurity specialists who have taken an interest in the physical systems used in the energy industry.

"The really nice thing is that here [at Georgia Tech] we have both," he said. "I fall in that latter camp. I'm a cybersecurity person. I've picked up [knowledge on] power and other cyberphysical systems and applied that and used different techniques to secure systems. And we work with the power people who've done exactly the same thing, but they've picked up cybersecurity."

Beyah indicated that the university was taking a similar approach to students. Georgia Tech hopes to draw applicants with a strong IT background, including "a BA or a BS in computer science or electrical engineering, some backgrounds in systems and controls [and] good programming skills." These students can use their time in the programme to gain familiarity with the energy industry, he said.

At the same time, though, the university is keen to attract applicants who have worked for power utilities or oil and gas companies, he commented. "[We] also are really interested in folks who have past experience in the area – work experience, for example, which would cover some of the requirements," he said.

The more, the better

As noted above, Georgia Tech is not addressing a new problem. Cyberattacks have been a challenge for the energy sector for years – that is, ever since power, oil and gas operators began using internet-connected devices.

Nevertheless, the DHS report indicates that the stakes are rising. At the same time, energy companies are not seeking to disconnect from the internet. Rather, they are likely to continue taking steps such as increasing the use of smart devices for purposes such as monitoring environmental and geological conditions at oil and gas production sites or optimising renewable energy use amidst variations in conditions such as wind speed.

As such, Georgia Tech's move to expand its graduate cybersecurity programme – and to sustain that programme's energy track – has the real potential to help US companies secure the personnel they need to address the issue. Beyah certainly hopes the university can accomplish this goal. "We see it as a national priority, and it's really important," he said. ❖

> "Cyberattacks have been a challenge for the energy sector for years – that is, ever since power, oil and gas operators began using internet-connected devices.