# The trans-Alaska pipeline fights off 22 million cyber attacks. Daily.

By **Elizabeth Harball, Alaska's Energy Desk - Anchorage** - March 14, 2018

*Bill Rosetti, Alyeska Pipeline Service Company's chief information officer, at the company's Anchorage headquarters. (Photo by Elizabeth Harball/Alaska's Energy Desk)*

The symbol of a well-known caped crusader is taped to the door of a secure room at Alyeska Pipeline Service Company's Anchorage headquarters. The sign reads: "THE BAT CAVE."

Listen **now**

My guides don't know why the sign's there. Maybe it's the lack of windows. Or maybe it's because the people who work in this room see themselves as undercover crime-fighters, like Batman — because they sort of are. This is the office of Alyeska's cybersecurity team.

The trans-Alaska pipeline has dealt with its share of problems — earthquakes, declining oil flow, even gunfire. But today, the pipeline is facing another, more modern threat: cyberattacks. Energy infrastructure is a tempting target for hackers, and the trans-Alaska pipeline is no exception. Alyeska, which operates the pipeline, now ranks cyberattacks as one of its top three risks.

In the room where part of the pipeline's cybersecurity team is stationed, Alyeska's Bill Rosetti points at a wall of data flowing down three giant screens hanging above the cubicles. It's all totally incomprehensible to a layperson. But for Rosetti and his staff, weird activity on one of the colorful charts rippling across the screens could indicate something serious.

"The idea here is that we are looking for things to be normal," Rosetti explained. "And anything that's not normal is something that needs to be investigated."

Rosetti is Alyeska's chief information officer. He's in charge of keeping cyberattackers at bay. Rosetti takes that job seriously, because the trans-Alaska pipeline is getting hit by cyberattacks all the time — and not just a few.

"We see about 22 million attacks a day," Rosetti said.

And that's an average.

"It can be six or seven million some days and 45 million the next," Rosetti said. "I wish I could tell you why it changes that way, but I really don't know."

Of course, there aren't millions of people carrying out these attacks individually. These are mass, automated attacks, often coming from servers overseas.

Rosetti said so far, none of the cyberattacks have been successful; Alyeska has never been breached. But the challenge is growing. Rosetti said the rate of cyberattacks has roughly doubled in the last five years.

So how are hackers going after the trans-Alaska pipeline, and why? Rosetti says they have all kinds of goals, and all kinds of techniques. There's phishing, for example:

"Some are very focused — that's called spear-phishing — where they're aimed at our CFO, trying to get people to wire them money," Rosetti said.

And then there are attacks that threaten the trans-Alaska pipeline itself. As the energy industry settles into the Internet age, more of its machinery is controlled remotely by computers. If someone manages to breach those systems, there could be dangerous real-world consequences. I asked Rosetti what the worst-case scenario would be if there was a major cyberattack on the trans-Alaska pipeline.

"We think about what the worst case is so we can protect against the worst case. And I don't want to share what that is," Rosetti said.

Throughout the interview, Rosetti was very vague and careful with his words, because, he said, he didn't want to give hackers any clues. But he did acknowledge that a successful cyberattack could interrupt the flow of oil down the pipeline. It could even result in people getting hurt.

The growing cyber threat to pipelines and other infrastructure is worrying the topmost levels of government — late last year, the Department of Homeland Security and the FBI issued a warning that sophisticated cyberattackers have targeted the U.S. energy sector, in particular.

Jim Guinn leads the company Accenture's cybersecurity business for the energy, utilities, chemicals and metals and mining industries. Part of Guinn's job is to help energy companies prepare for cyberattacks. As far as he's concerned, the potential consequences of a major cyberattack should be the No. 1 thing keeping energy executives up at night, if it isn't already.

"It could be anywhere from a spill, to loss of the command of the plant itself, to explosion, to loss of life. It would be no different than losing a platform in the Gulf of Mexico or in the North Sea," Guinn explained.

Guinn said the threat level to America's energy system hinges on two factors: the bad guys' capability to pull off a cyberattack and the bad guys' desire to actually inflict damage. So far, those two factors haven't lined up.

But… "there are those in the intelligence community that have openly said that they believe that an attack at scale could occur on U.S. soil, or against a U.S. company within the next 12 to 24 months," Guinn said.

Guinn couldn't speak specifically to the cyber threat facing the trans-Alaska pipeline. But he said one thing's for sure: the risk isn't going away.

“The reality is, as long as these assets are attached to networks and they are managed the way that they are today, there is a real threat that they could be manipulated for malintent,” Guinn said. “It’s just the unfortunate world that we live in.”

---

**Elizabeth Harball, Alaska's Energy Desk - Anchorage**

Elizabeth Harball is a reporter with Alaska's Energy Desk, covering Alaska’s oil and gas industry and environmental policy. She is a contributor to the Energy Desk’s Midnight Oil podcast series. Before moving to Alaska in 2016, Harball worked at E&E News in Washington, D.C., where she covered federal and state climate change policy. Originally from Kalispell, Montana, Harball is a graduate of Columbia University Graduate School of Journalism.