BIG DATA: AN ALTERNATE REASON FOR HACKS PAST AND FUTURE?

[Fracking sites, location unknown (Simon Fraser University via Flickr)]

On Monday, MIT's Technology Review published an interesting read: Big Data Will Keep the Shale Boom Rolling.

Big Data. Industry players are relying on large sets of data collected across the field to make decisions. They're not looking at daily price points alone in the market place, or at monthly and quarterly business performance. They're evaluating comprehensive amounts of data over time, and some in real time as it is collected and distributed.

Which leads to an Aha! moment. The fastest entrant to market with the most complete and reliable data has a competitive advantage. But what if the fastest to market *snatches* others' production data, faster than the data's producer can use it when marketing their product?

One might ask who would hack fossil fuel companies' data. The most obvious, logical answers are:

– anti-fossil fuel hackers cutting into

production;
– retaliatory nation-state agents conducting cyber warfare;
– criminals looking for cash; and
– more benign scrip kiddies defacing property for fun.

But what if the hackers are none of the above? What if the hackers are other competitors (who by coincidence may be state-owned businesses) seeking information about the market ahead?

What would that look like? We're talking really big money, impacting entire nation-state economies by breach-culled data. The kind of money that can buy governments' silence and cooperation. Would it look as obvious as Nation A breaking the digital lock on Company B's oil production? Or would it look far more subtle, far more deniable?

Technology Review's article on Big Data discusses how the shale oil and gas sector relies on increased efficiencies when oil prices have tanked. Shale oil producers find cost savings, or lose all their sunk costs in production to date. Shareholders will pitch a fit over the latter.

But OPEC and other non-shale oil producers must optimize their pricing. They must drop low enough to make shale oil (and fracking) untenable, while ensuring they make as much profit as possible. The break-even for shale is somewhere between $60 and $80 per barrel, depending on production location, financing, and facility's age. Over the last year, oil prices have fluctuated from more than $95 per barrel last July, to less than $50 per barrel this past March. The plummet in prices knocked much U.S. shale production offline to avoid operating at a loss.

It's easy to see how a nation-state oil producer can use asymmetric warfare – in this case, simple economics – to punish a competitor. A larger producer with more cheap oil can simply lower their prices or flood the market, knocking

out highest-cost producers.

But what if the highest-cost producers are dependent on Big Data analysis to reduce their costs? And what if the larger producer is running low on cheaply-produced oil, or needs more cash to keep production partners happy? The temptation to get as much information about the competitor is strong, and the potential for hacking is likely.

The amount of money in play makes this a foregone conclusion. At 10 million barrels per day, multiplied by $60 per barrel (the rough two-month average daily unit price), the daily gross revenue is $600 million. For relative comparison, this is two-thirds of Samoa's annual GDP; this scale of money makes or breaks countries.

At the same rate, a year's shale oil production is $219 billion. General Motors' multi-year $2.8 billion contract with its IT service provider looks like a bargain. Or even the federal government's one-year $1.2 billion contract with IBM (Y2013) looks cheap. Why wouldn't a producer (or even a well-capitalized trader!) with some loose cash pony up tens of millions to obtain hacked data?

If the stakes were higher – let's say $100 per barrel – how much incentive would there be to hack a competitor?

This is all pretty elementary; what's new is the proposition that data, not oil, has value worth fighting for. Data is what props up or crashes profits, makes or breaks a market.

The next new proposition is targeting: who else may be important to fast analysis of competitors' place in the market?

How about the companies safeguarding the data?

Which brings us to Eugene Kaspersky's op-ed in Forbes yesterday – published after his information security firm disclosed their Duqu infection. Whatever entity hacked Kaspersky was

looking for data. It wasn't destructive cyber weapon Stuxnet launched on the firm's computers. It was reconnaissance malware, designed to seek-collect-report.

Kaspersky is direct: "This was a case of industrial espionage, plain and simple."

To him the hacking doesn't make sense. Kaspersky guesses the hackers motives were to:

1) "steal our technologies, source code, know-how and ideas,"
2) obtain information about "the inner workings of our company," and/or
3) "ego-tripping…vengeance," in response to hackers being previously exposed by Kaspersky.

Kaspersky fumbles on customer information, though he calls their customer-related data part of the firm's "crown jewels." What clients Kaspersky protects and the status of content including Big Data stores is valuable. Such information may exist not in technical work files on air-gapped machines, but in networked accounting systems.

(This may explain why a "non-technical employee" in Asia-Pacific area was the index case of infection.)

The infosec company is willing to license their technology, Kaspersky points out. The hackers could simply buy the technology they need to subvert. But that's not what they want – the desired info is something Kaspersky wouldn't share if hackers had to breach their systems to access it.

Perhaps Kaspersky's right about the motives for hacking his firm. But with potential billions of dollars at stake –and we do know fossil fuel companies' networks have been breached – it's worth considering another possibility. Hackers may want something more valuable than Kaspersky's accounts receivable.

They may want to know much time and resources it will take to hack their targets' Big Data. How

long before they hit digital pay dirt – whether billions of dollars in fossil fuel revenues, or crushing a competitor into exiting the market?

Keep in mind, too, that Kaspersky Lab is a Russian company, and may have far more Russian clients than any other infosec firm. Russia is also the world's largest producer of oil, pumping 10.1 million barrels a day – more than second-place producer Saudi Arabia's daily output of 9.7 million barrels.

The possibility of hacking for oil-related competitive info certainly puts a new spin on "data mining."