flyingpenguin

COLONIAL PIPELINE SPILLS DETAILS ON FIRST CISO

DAVI OTTENHEIMER

FEBRUARY 28, 2022

Let me begin by saying the first ever chief information security officer (CISO) hire anywhere ever was a PR invention of Wall Street back in 1994.

This position was officially rolled out in a news campaign by Citicorp in order to offset panic when they disclosed their security breach.
From a computer terminal in his apartment in St. Petersburg, Russia, a Russian software engineer broke into a Citibank computer system in New York and with several accomplices stole more than $10 million by wiring it to accounts around the world, according to court documents and the U.S. attorney's office. Citibank said all but $400,000 of the stolen funds have been recovered. Six hacking suspects have been arrested, including the engineer, Vladimir Levin, who is being held in Britain and is fighting extradition to the United States.

Citicorp sounded bullish talking about law enforcement and government actions. Yet they were far more subdued about technology and management changes made, phrasing it in papers like this.
…the bank has upgraded it security since discovering the intrusions in June, 1994.

The bank upgraded.

Behind closed doors, meanwhile, Citicorp customers were being invited to meet with a chief of security, someone who had been running JPMorgan security since 1985; and he was recruited without being told that they were going to drop the whole thing on his lap, along with a blank check.

You can imagine how easy it was for someone with a decade of experience and a blank check on his desk to give people future leaning statements about how he intends to fix anything and everything.

Thus in terms of history a CISO is mostly a political act of creating a rug for things to be swept under, run from the marketing side of the business. In that sense it's not unlike other C-level

roles, however it has the important distinction of being tied to *externally established public policy* (safety).
Remember that phrase.

Now fast forward to this week…a somewhat related announcement is that Colonial Pipeline hired their first ever CISO, nearly a year after disclosing a massive mishandling of security. Allow me to rewind the Colonial breach just a little so that we can end on an interesting footnote about their CISO announcement text.

Colonial, an awkward name for a power company to say the least, was founded 60 years ago in 1962 as a joint venture of nine oil companies (political extremist Koch Industries today holding the largest stake).
About four years ago Colonial received at least one scathing 90 page audit report for its rather typical American energy habit of running a "patchwork of poorly connected and secured systems", as reported later by the Associated Press (AP).
We found glaring deficiencies and big problems. I mean an eighth-grader could have hacked into that system.

The AP also buried its lede in reporting that Colonial's chief information officer (CIO) Marie Mouchet sat on the advisory board of the firm that Colonial hired to be an "independent" security auditor. Mouchet is non-technical, with a background that reads like decades of evading regulations.
Mouchet began her career with Southern Company in 1981 as an assistant analyst for the company's rate and economic services division. She progressed through positions of increasing responsibility before being named supervisor of regulatory research in 1986. A year later, she became supervisor of market intelligence and was later named as manager of market intelligence in 1988. In 1990, Mouchet was named assistant to the vice president of public relations. She transferred to Southern Company's Georgia Power subsidiary in 1992 to serve as a senior regulatory affairs representative.

Assistant to the VP of PR and lobbyist is who Colonial hired to be their CIO? And she was in charge of security too? Predictable disaster.

When asked about the conflict of interest with a CIO on the board of an outside firm auditing the information systems, the firm said it didn't pay Mouchet to advise them. Talk about missing the point.

Hint. Hint. Corruption. Bias.
Unlike electrical utilities, the pipeline industry is not subject to mandatory cybersecurity standards…

Uh-oh. So the industry with no security standards or established public policy has this giant company that hires a anti-government lobbyist to be their CIO overseeing security?

We should also keep in mind that the risks here go far beyond information security and gets into a lack of basic standards of care about humanity.

Smallwood's study was not a cybersecurity audit. It focused on ensuring smooth operations… He cited, for example, Colonial's inability to locate a particular maintenance document. "You're supposed to be able to find it within 15 minutes. It took them three weeks." Locating such a document could be crucial in responding to an accident or keeping up-to-date pipeline inspection records to prevent leaks, Smallwood said. Colonial experienced one of the worst gasoline spills in U.S. history last August, contaminating a nature preserve north of Charlotte . After it was discovered by two teenagers, the spill's severity was not immediately clear as Colonial's initial reports indicated a far lower volume. North Carolina environmental regulators angrily called the company's failure to promptly provide reliable data unacceptable.

Let's be honest. One of the worst gasoline spills in U.S. history was discovered by some kids and completely mishandled by Colonial. That was serious breach news of 2020 (that nobody heard about) and in retrospect offers some ominous foreshadowing.

You may recall a far more public outcry in May of 2021, when Colonial tripped over their clown shoes into a basic ransomware attack. It's what allegedly prompted them to make a highly political decision to shutdown 5,500-miles of pipeline (nearly half the fuel supply on the East Coast of the U.S.) and donate 75 Bitcoin ($4.5m) as ransom to the "DarkSide" Russian cartel. That ransom payment was widely criticized not least of all because the decryption key it produced was too slow to be useful, especially relative to Colonial's own restore process from its backups. This complete failure of common sense came after long-time advice from the FBI to never pay the ransom.
The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data.

Colonial would have been far better served giving $5m to the FBI to investigate Russians, instead of to the Russians. Except there's at least two problems with the logic of such a company helping the federal government to help protect Americans.

First, the ultra-right political organization Koch Industries is the majority holder in Colonial and paid nearly $100K to Devin Nunes to undermine FBI investigations into Russian crimes.
[Nunes argued] the FBI's process was not a good-faith attempt to investigate Russian influence; rather, the memo says, it was a politically motivated operation to spy on someone affiliated with the Trump campaign.

Seems unlikely that those running Colonial were going to be cooperating with the U.S. government when their wealth comes largely from fighting with the U.S. government.

Second, Koch is the name derived from Fred Koch who made his fortunes in the Soviet Union building oil refineries for Stalin (1929 to 1931) and then in Nazi Germany for Hitler. This family is notorious for its alignment with anti-American hate groups.
You know what else looks bad? Financing the publication of Holocaust denial literature over the course of several decades. Which is exactly what Charles Koch did between the 1960s and the 1980s. […] Fred hired a dogmatic Third Reich sympathizer to nanny his sons at home [who today run Koch Industries]. […] In 1977, Charles Koch founded the libertarian Cato Institute think tank, and brought in his brother David Koch as a shareholder. […] Barnes, who called Jews "swindlers of the crematoria" who "derive billions of marks from non-existent, mythical

and imaginary cadavers," had died back in 1968. But the Cato Institute resurrected his work and published it again anyway.

Speaking of resurrecting work, their father Fred Koch returned to Russia in 1956 to continue his business ties there, while becoming a founding member of the notorious American hate group known as John Birch Society.

John Birch Society Leader Villifies Jews at Rally

Smear Speech Casts Doubt Society Rejects Hatred of Jew

BOSTON —(JTA)— An openly anti-Semitic rally here at which a key spokesman of the John Birch Society vilified Jews cast considerable doubt on the repeated insistence of Birch Society leaders that the organization rejects hatred of Jews.

The main thesis of Birchers tends to be they fear government is going to steal a god-given privilege from white men, while claiming they don't believe in the very things that they say they are losing. It's really fascism, a modern variation of the more latent "let white men rule" KKK platform of the 1868 Presidential campaign.

And speaking of notorious hate groups, I couldn't help but notice this line promoted by Colonial in their otherwise fluffy CISO announcement:

[Colonial's new CISO] Tice earned a Bachelor of Science degree in Information Systems Management in 2000 from Bob Jones University in Greenville, South Carolina.

Graduating in 2000 from Bob Jones "garbage" University is not something to be proud of or mention in public… unless maybe you're trying to impress Koch Industries or their Cato Institute?

President Bob Jones III said Wednesday [March 2000] he wanted to show that nothing had changed about his views on Catholicism [by calling it a cult]… "Unfortunately they still treat Catholic bashing as an intramural sport," Patrick Scully, spokesman for the New York-based Catholic League for Religious and Civil Rights, said Wednesday. Scully says Jones "has an absolute right to teach this type of garbage, but we have the right to shine the light of truth on it."

I'll say it again, graduating in 2000 from Bob Jones "garbage" University is not something to be proud of especially when talking about safety and security.

There was a tradition in the hate-filled Jones family, apparently, that became the fundamental ethos of their education system.
Jones was not only a purveyor of fine painting but also of the hoariest anti-Catholic tropes, calling the church of Rome "a satanic counterfeit," for example, and "drunk with the blood of the saints."

Bob Jones University thus is perhaps best known for overt acts of hate, such as the fact that exactly zero black students were admitted to this "deep South" school between 1926 and 1971… by design!
…the 76-year-old Jones—who was born five years after the completion of Reconstruction and who was the son of a Confederate soldier—took to the airwaves on Easter Sunday [in 1960] to make his case from Scripture about why [Civil Rights for Black Americans] was not something to be welcomed and celebrated but rather to be rejected and condemned. After the address aired, Jones had the talk transcribed and printed as a booklet, which became the school's primary statement on race and integration throughout the 1960s and 1970s, and into the 1980s.

Why were Blacks finally admitted in 1971? The school's founder had died three years earlier.

Even then, the school strictly prohibited Blacks socializing with whites, actually requiring all Black students to be married to a Black person before they could "mix" with whites.

The racist school fought hard to continue promoting hate, attempting to falsely litigate that integrity failures should be protected under the Constitution (Bob Jones University v. United States (461 U.S. 574)[1983]).
Chief Justice Warren E. Burger, writing for the eight-justice majority, found that … the government's purpose of eliminating discrimination in education was so fundamental to public policy that it overrode Bob Jones University's religious convictions.

Such hate-driven litigation to promote racism ended with the Supreme Court declaring Bob Jones University a place of worship that is "contrary to established public policy" and thus technically the opposite of "charitable".

One more time, graduating in 2000 from Bob Jones "garbage" University is not something to be proud of especially when talking about safety and security.

Only in 2008 (!) did Bob Jones University weaken its hate, by claiming their racism was due to *them* being "victims" of the American culture of racism that they fostered.

I swear I am not making any of this up.
For almost two centuries American Christianity, including BJU in its early stages, was characterized by the segregationist ethos of American culture. Consequently, for far too long, we allowed institutional policies regarding race to be shaped more directly by that ethos than by the principles and precepts of the Scriptures. We conformed to the culture…

These wealthy white men claiming to be "victims" of racism had used their huge endowments and giant legal teams to fight bitterly all the way to the Supreme Court *to preserve and expand racism*.
To be fair, they did also then finally confess to the system of education at Bob Jones University lacking integrity, being intentionally hurtful.

…failed to accurately represent the Lord and to fulfill the commandment to love others as ourselves…we allowed institutional policies to remain in place that were racially hurtful.

And this is exactly how America remains extremely racist, despite believing that it is not racist.
Psychologists refer to this kind of broad bias in perception as "motivated cognition" — that is, most Americans want to live in a society that is more racially equal, and so they engage in mental actions that ignore, discount or downplay contradictory evidence to maintain coherence between belief and reality.

I am imagining Colonial to someday soon announce that they allowed institutional policies to remain in place that were hurtful, because they were victims of an American culture of weak security practices (one that they fought hard to promote).

Colonial believed it was operating safely, despite copious evidence proving the opposite. It even hired people to taint external reports and block regulation rather than make significant change to its unsafe practices.

See now why it seems weird as a PR exercise to announce a CISO has been appointed with a degree from a school dedicated to increasing harm by operating "contrary to established public policy"?

It begs the question of why Colonial took so many years to hire someone technically qualified and capable in security. Were the Koch brothers holding the line, insisting on someone who would reject basic concepts of public safety let alone justice?

Why list Bob Jones on any announcement related to leadership or integrity? That just doesn't make sense. Had Colonial not mentioned it, this blog post probably never would have been written to ponder why a CISO is being promoted as a Bob Jones believer.

And thus it all begs the question of whether this CISO is someone who can take to heart the poorly-worded mea culpa of his school in an attempt to change, in some way using a blank check in order to stop Colonial from being intentionally hurtful in the ways he was taught (no longer transferring large cash donations to fascists, even those in Russia).