The Philadelphia Inquirer

PhillyDeals: Cybersecurity worries spawn business, academic opportunities

By Joseph N. DiStefano

February 15, 2015

When **Starnes Walker** was a newly minted physicist and Navy electronic-weapons veteran in the 1970s, his job at **Phillips Petroleum Corp.** included finding ways to replace human oil-refinery operators, who once hand-checked miles of pipes, with digitally networked monitors and switches.

"So that, now, valves are controlled by computers," Walker says, from his office in a converted Chrysler factory, where he heads the University of Delaware's new Cybersecurity Initiative.

That digital technology had far-reaching results:

It's part of the reason the brightly lit refineries that still line the rivers near Houston and Philadelphia now employ hundreds of workers each, not thousands.

And it's why energy systems, like so many other industrial, financial, water, government, and small-business systems, have become vulnerable to software attacks and other computer failings. "That's why we are concerned about the critical infrastructure of the U.S.," Walker told me.

Once a preserve of specialists at big computer-dependent companies, specialty software vendors, and scholars at high-powered schools like Massachusetts Institute of Technology, cybersecurity worries since the 9/11 terrorist attacks have fed a proliferation of Washington bureaucracies - and created business and academic opportunities.

Walker has held a succession of jobs setting up Navy, Defense Department, and Homeland Security agencies to cope with digital security threats.

Federal demand and government mandates have helped spawn consultant firms staffed by well-connected government veterans. **Michael Chertoff**, the former Homeland Security secretary, visited Delaware last week to give a speech for Walker's program. Services such as bank and retail cyber-compliance departments, designed to limit personal data leaks, have been created. So have specialized units, such as the glass-walled room at **GE Water & Process Technologies** headquarters in Trevose, where a dozen engineers watch client systems to spot data and operating problems at remote locations.

With the CIA claiming a deficit of tens of thousands of cybersecurity specialists in the U.S. workforce, universities are scrambling to offer courses to help students train for promised jobs.

Is all this necessary?

"Zero people have died, so far, from cyber-terrorism," points out **Benjamin Friedman**, a "cyberskeptic" at the **Cato Institute** in Washington, which warns against exaggerating strategic threats or costly national responses to computer challenges that are, for most firms, a cost of doing business.

But Friedman agrees it makes sense for schools like Delaware to "try to meet market demand," focusing on basic business problems of network security and personal data hygiene.

Delaware president **Patrick Harker** says Walker's program, which currently offers a cybersecurity minor across the university's seven undergraduate colleges, is well-positioned to meet both corporate and government needs.

There are local demands for data security and analysis at Delaware businesses, such as **JPMorgan Chase & Co.'s** consumer-lending units. Walker sees other clients as well.

"We're halfway between the center of government, intelligence, and military institutions, and the financial center in New York," Walker noted.

The university is even closer to - and has landed contracts with - Aberdeen Proving Ground in Maryland, where the U.S. military concentrates cybersecurity efforts.