Bauerle's Bank Notes

Darkness Visible, Part II

Endless Endpoints: Banking in the Era of Ubiquitous Computing

September 26, 2016

At the beginning of the 1985 movie *Spies Like Us,* we meet Austin Milbarge (Dan Akroyd) holding down a civilian desk in the bowels of the military, having just parsed triple-encrypted Chinese military communications with a Drogan's decoder ring. "Put it through the machines," barks his commander. "I already did," replies Milbarge, handing him the computer printout. "Then clean up your desk," orders the boss.

Today, code cracking is no longer top secret or a movie punch line. It is a fixture of the daily news cycle. For computers are as common as kids' plastic decoder rings. In 2015, The Economist wrote, "The third windfall [of computing's ubiquity] is economic. Some studies find that in developing countries every ten extra mobile phones per 100 people increase the rate of growth of GDP-per-person by more than one percentage point-by, say, drawing people into the banking system."[i]

The fly in the ointment is new responsibility accompanies new opportunity. The $40 computer qua smart phone enables remote capture of bank deposits. It also enables remote theft of bank deposits. So an attack on a bank vault can come from anyone, anywhere.

"Endpoint detection and response" (EDR) is the name business research company Gartner (NYSE: IT) coined in 2014 to identify emerging cyber security countermeasures. Billions of dollars of venture and private equity capital are being spent to develop complex adaptive systems to identify and defeat remote attacks against critical infrastructure, including our banking system. Among the tools available today is CyFIR[ii], one of the two EDR applications that cracked the OPM data breach discussed in the last installment of this column.

In the realm of electronic financial services, three dimensions of the problem must be addressed: recognition, response and regulation. These are the Three R's of cyber security.

Recognition and the Importance of Education. Software development during the last thirty years has made computers easy for consumers to use, sometimes too easy. People publish information on social media without considering the consequences. They transfer money with no real understanding of the risks. They indiscriminately click "I accept" on terms of service that commit them to contracts containing terms they do not understand until after they suffer losses. They get suckered responding to con artists posing electronically as legitimate businesses or banks. Rather than prosecute John Stumpf and Wells Fargo for faking customer accounts, the Consumer Financial Protection Bureau should educate consumers about how to recognize their own unsafe Internet banking practices and reduce the risk they will be victims.

Response and the need for Systems Engineering. CyFir and similar tools are network operators' best available means to identify and mitigate cyber attack risks. By the nature of their business, banks are especially vulnerable. The size XXL economic opportunity to create effective cyber security is likely to continue to attract sufficient capital to outgun the crooks at least most of the time.

The OPM Report described in our last installment highlights negligence of multiple federal agencies, not just the Office of Personnel Management. In the annals of failed banks, there are already cases in which computer technology was an instrument of fraud and deception. There will be more. Collaboration between public and private technical experts is vital to building better systems of detection and response. The nature of banks and the agencies that regulate them is to be insular and self-referential. This is a behavior that must be tempered if we are to have an effective net for preventing cyber crime.

Wall Street banks are currently conducting trials of blockchain technology, also called distributed ledger systems. This software is the foundation for crypto currencies like Bitcoin. In blockchain systems, artificial intelligence-equipped computers trade financial contracts with one another according to established protocols. A key premise of the systems is that the actors will not cheat one another or that the cheating will be detected if tried. This premise is sure to be undermined somewhere by someone. Already, crypto currencies are a preferred means of payment among criminals because the currencies function outside the bank transaction reporting requirements of U.S. federal law. For blockchain technology to succeed, security systems will need to be built in to promote data integrity and data security. As more users join the networks being created, the need for security countermeasures will grow commensurately.

Regulation to Promote Safe Cyber Financial Services. "Lock 'em up," is conventional wisdom for how to deal with bank larceny. More effective, and needed, are

law changes that promote banks' investment in cyber security and disinvestment in obsolete brick and mortar delivery channels.

For example, in financial accounting for mergers, banks have often allocated much of the purchase price to brick and mortar assets, which bank buyers can then depreciate for accounting purposes. The practical problem is many purchased brick and mortar assets are no longer worth their carrying values. So they cannot be sold without eroding earnings and profits. This dilemma leads banks to continue operating obsolete brick and mortar assets. Why not enact a one-time tax holiday that would allow banks to shed obsolete assets without penalizing earnings? After all, states in the 1990s enacted sales tax holidays on computer purchases by consumers to encourage them to become computer savvy. What's the difference?

Alternatively, tax effects associated with selling obsolete assets could be offset against tax credits or accelerated depreciation schedules enacted to promote investments in cyber security technology.

Retraining personnel who are no longer needed as tellers, credit analysts or loan administrators should also be encouraged by legislation. The current Wells Fargo drama reminds us that we all respond to financial incentives. Teaching current employees new skills for the era of ubiquitous computing has more social and economic utility than bonuses for opening new accounts.

Blockchain is impossible without regulation. Like letters of credit, distributed ledger technology is most useful in international transactions, where it creates a new lingua franca and transcends differences in culture and local practice. A necessary corollary is that jurisdictional limits of legal sovereignty require a pre-agreed set of rules governing trading and dispute resolution. The Uniform Customs and Practices for Documentary Credits has been an effective framework for banks that deal in letters of credit. A parallel framework for blockchain technology must be created before the system goes live.

At the end of *Spies Like Us,* Austin Milbarge, Emmett Fitz-Hume (Chevy Chase) and their Russian collaborators save the world from nuclear catastrophe. Daily life for most of us is more mundane. Cyber risk, however, is here to stay. The sooner we take it seriously and act accordingly, the better we and our world will be for the effort.

[i] http://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones

[ii]https://www.cyfir.com/