Bauerle's Bank Notes

Darkness Visible, Part I

Lit Up Like a Christmas Tree

September 12, 2016

Speaking before Labor Day with an OCC executive, I asked, "What is top of mind at the OCC these days?" "Cyber," came the instant response.

Last week, Congress and the President gave additional credence to the executive's reply. Thursday, the House Committee on Oversight and Government Reform released a scathing 231 page report, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation" (the "OPM Report").[i] Friday, President Obama named retired Brigadier General Gregory J. Touhill as the first Federal Chief Information Security Officer "to drive cyber security policy, planning and implementation across the federal government."[ii]

The OPM Report chronicles the U.S. Office of Personnel Management's chronic and ultimately calamitous failure to secure personally identifiable information, or PII. Four million current and former federal employees' personnel files were exposed. So were security clearance background investigation files on 21.5 million Americans who do business with the federal government and fingerprint data of 5.6 million of those persons.[iii] For two years, hackers systematically explored and looted OPM's computer network. Media reports attributed the attack to the Chinese government.

The OPM Report is a sunbeam cast on the otherwise dark subject of cyber heists, a witch's brew of espionage, financial chicanery and stealth warfare. This broader context is compellingly presented in Dark Territory: The Secret History of Cyber War, the latest book by Pulitzer Prize-winner Fred Kaplan.[iv] An Oberlin College classmate of mine, Kaplan earned a Ph.D. degree at MIT and worked for U.S. Rep. Les Aspen when Aspen chaired the U.S. House Armed Services Committee. For the last 30 years, military strategy has been Kaplan's beat as a writer for leading periodicals and the author of five books.

In Dark Territory, Kaplan reprises a White House briefing May 16, 2007, at which Director of National Intelligence Mike McConnell explained that economic damage from the terrorist attack of September 2001 would have been far worse had the perpetrators targeted a big Wall Street bank's computer systems instead of the World Trade Center buildings.

> [President] Bush turned to Henry Paulson, his treasury secretary. "Is this true, Hank?" he asked.
>
> McConnell had discussed this very point with Paulson in a private meeting a week earlier. "Yes, Mr. President," he replied from the back of the room. The banking system relied on confidence, which an attack of this sort could severely damage.
>
> Bush was furious. He got up and walked around the room. . . .
>
> "McConnell," he said, "*you* raised this problem. You've got thirty days to solve it."

Continues Kaplan, McConnell was "shocked at how little progress had been made" in the ten years since he served at [the National Security Agency] in the Clinton years. "[P]rivate companies didn't want to spend the money on cyber security, and they resisted all regulations to make them do so; meanwhile federal agencies lacked the talent or resources to do the job, except for NSA, which had neither the legal authority nor the desire."[v] The OPM Report reveals that another decade later, McConnell's assessment remains depressingly accurate.

Beyond lack of talent and resources, the OPM Report chronicles a half-hearted, over confident and CYA-infused culture concerning data security. Attack perpetrators roamed at will within the agency's computer network. They mapped the system's topology, constructed attack vectors, and captured "crown jewels material" in the words of Joel Brenner, former NSA senior counsel. Said FBI Director James Comey, "My SF-86 [the federal form used as a starting point for background checks] lists every place I've ever lived since I was 18, every foreign travel I've ever taken, all of my family, their addresses. So it's not just my identity that's affected. I've got siblings. I've got five kids. All of that is in there."[vi]

Alerted to an attack by the Department of Homeland Security in March 2014, OPM enlisted the aid of specialists from DHS, NSA and FBI. Within weeks, the interagency cyber SWAT team identified the perpetrator as the Axiom Group and set up counter-surveillance to monitor the hack in progress. When they believed there was little additional counter-intelligence to be gathered, the team sprang a trap they called "Big Bang" and shut down the attack in May 2014.

The full measure of damage done came to light 11 months later. In April 2015, OPM had two private contractors test on OPM's network their malware detection and attack mitigation software, one tool called Cylance and the other CyFIR. When the tools probed for the presence of "Trojans," which allow an attacker to bypass network security controls, the network "lit up like a Christmas tree."[vii] Within 24 hours of its deployment, CyFIR revealed that although the federal interagency team believed they had outfoxed the hackers, a second campaign continued undetected. Worse, in the months following Big Bang, the second campaign bored deep into the mother lode of the OPM network environment: the security clearance and fingerprint files. So the interagency experts' smugness about their Big Bang countermeasures compounded rather than solved the problem.

The OPM Report concludes by quoting Rep. Will Hurd: the OPM case "is just another example of the undeniable fact that America is under constant attack. It is not bombs dropping or missiles launching; it is the constant stream of cyber weapons aimed at our data."[viii]

It would be a mistake to conclude cyber crime is the government's problem alone, or that the government alone should solve it. The OPM Report should be required reading for every bank executive and director. The report describes in plain English the ways and means of cyber espionage. It lays bare how system administrators' fears for their jobs and technical experts' narrowly focused tactics trump effective risk assessment and response. And it shows how financial constraints and operational and human failures coalesce to create institutional barriers that inhibit anti-cyber crime strategies in complex organizations. Banks and other financial companies are no exception.

Next, Part 2: Endless End Points: the Banking Industry Challenge.

[i]https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

[ii]https://www.whitehouse.gov/blog/2016/09/08/announcing-first-federal-chief-information-security-officer

[iii] OPM Report at p. v. "There is some overlap between the 4.2 million individuals impacted by the personnel records breach and the 21.5 million individuals impacted by the background investigation breach. . . . The aggregate number of individuals impacted by this breach totals 22.1 million." Id. at fn 1.

[iv] Kaplan, Fred M., Dark Territory: The Secret History of Cyberwar, New York, NY: Simon & Schuster (2016)(cited below as Kaplan).

[v] Kaplan at p. 176.

[vi] OPM Report at p. iii.

[vii] OPM Report at p. 103.

[viii] PM Report at p. 226.

James F. Bauerle
Keevican Weiss Bauerle & Hirsch
Three Gateway Center
401 Liberty Avenue, 3rd Floor
Pittsburgh, PA 15222
phone - 412-355-2605
fax - 412-355-2609

email - jbauerle@renaissance-partners.com

Keevican Weiss Bauerle & Hirsch, 1001 Liberty Avenue,
11th Floor, Federated Investors Tower, Pittsburgh, PA 15222-3725