Testimony of

Jason Healey

Before the

United States House of Representatives

Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit

Hearing on

"Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats"

19 May 2015

Chairman Neugebauer, Ranking Member Clay, and distinguished Members of the Committee, thank you for the honor of testifying before you on the finance sector's response to cyber threats.

Over the past nearly twenty years, I have been involved in cyber operations and policy in the military and Intelligence Community, the White House, and finance sector. I created the first cyber incident response capability at Goldman Sachs and was an early Vice Chairman of the Financial Services Information Sharing and Analysis Center. Now as an academic, serving both as a Senior Research Scholar at Columbia University's School of International and Public Affairs and as Senior Fellow at the Atlantic Council, I may be less involved in the day-to-day cyber tumult than my colleagues here today, but with a bit more freedom to analyze where we have come from and what might be next.

Regarding the cyber threat, it is surprising how little has changed. We've been concerned about the same basic threats – nation-states' warriors and spies, hactivists, terrorists, insiders, and criminals -- for twenty, thirty, even forty years. It has been clear that banks are in the crosshairs since at least 1994 when Vladimir Levin took Citibank for over $10 million.

But of course the massive expansion of those threats, and the myriad way come at the sector, is astounding.

Those early hacks were mostly from lone individuals or juvenile groups until a bit over a decade ago, when we saw what we call the "Rise of the Professional." In the years since, amateurs like Levin were no longer the norm, pushed aside by organized crime and nation states like Russia, Iran, and China who were increasingly swimming in the same waters.

Today, according to the Verizon Data Breach Investigations Report, the finance sector is hit mostly with web-application attacks (27% of the total attacks on the sector), such as phishing, to take over the user interface to a banking application.

Other important categories of attacks were payment-card skimmers (22%) and denial of service attacks (26%). The financial sector tended to have far lower levels of insider abuse than other sectors (only 7% of the total compared to 24% in the public sector and 37% in real estate) and strikingly low levels of cyber espionage, at under 1% of the total attacks compared to 40% in mining and about 30% for professional services and manufacturing.

AMAZING PROGRESS TO DATE

Fortunately, in the past twenty years the finance sector has led the way on many key technology innovations, such as firewalls and intrusion detection systems. At least as important have been the process innovations. After the Levin hack, Citibank created the world's first Chief Information Security Officer (CISO) position, held by our colleague Steve Katz.

Other process innovations that have made a real difference include working from a presumption of breach - assuming there is already a sophisticated heist underway and trying to find evidence; operationalizing the cyber kill chain to stop intrusions as early as possible; intelligence-driven operations; and, of course, effective information sharing.

Only one year after President Clinton called on the private critical infrastructure sectors to create Information Sharing and Analysis Centers, the finance sector had responded with the FS-ISAC which is still going strong today.

Based on my intelligence background, I formed the ISAC's Intelligence and Threat Working Group and am happy to say that under Byron Collie of Goldman Sachs, the group has blossomed beyond anything found in other sectors. The finance sector has, for example, launched the Soltra Edge platform to help standardize and automate the flow of real-time cyber threat information.

The finance sector has much else to brag about, such as .bank and .insurance as well as the Account Takeover Task Force (ATOTF) established in 2010. Another factor contributing to the relatively low rate of insider attacks against banks are the tremendous efforts taken by banks to implement effective controls – even as one of the watchers on the information security team, I knew my actions too were being watched. In fact, I have little doubt Edward Snowden would have been thwarted or arrested had he tried his shenanigans at a major bank rather than the National Security Agency.

It is true that point-of-sale attacks on credit cards have been getting worse, but more secure technologies are on the way, such as chip-and-pin or token-based systems.

Of course it is not just the financial institutions themselves that are making progress. During my time at the White House from 2003 to 2005, it was clear that the finance sector regulators were on active and that cooperation between the financial institutions and the government was exceptional, especially compared to other sectors.

Twelve years ago, the finance sector instituted one of the great critical infrastructure governance innovations. The financial institutions, industry association, and exchanges created the Financial Services Sector Coordinating Council on Critical Infrastructure Protection and Homeland Security, known as the simpler FSSCC, while the government created its counterpart, the Finance and Banking Information Infrastructure Committee. These twin pillars have been the foundation of effective information sharing and mutual trust to the extent that the Department of Homeland Security tried to copy the idea to other sectors with, it should be said, mixed results.

The "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" issued by the Board of Governors of the Federal Reserve in 2003 was one of those relatively simple documents that really helped shift the industry. I often tell my students that finance did resilience before it was cool.

Few remember it now, but the FS-ISAC would likely never be as strong as it is today if it hadn't received a grant twelve years ago from the Department of the Treasury. The FS-ISAC used this to recapitalize on the condition that it would provide service to all regulated American financial institutions, not just those who paid a membership fee.

Cooperation has continued to be effective, particularly through efforts like the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity and Critical Infrastructure Working Group (CCIWG) and Financial Sector Cyber Intelligence Group of 2014.

BUT WORRIES CONTINUE

The Committee need not be overly concerned about a large-scale disruptive attack taking down the finance sector. While the impacts could be terrible, these kinds of attacks are far more difficult to trigger than you may have been led to fear. Perhaps the first use ever of the term "electronic Pearl Harbor" was actually in testimony to the House Committee on Science, Space and Technology in 1991.

So even though Congress has been hearing for nearly twenty five years that a major cyber attack could cripple the United States, no major attacks have even come close.

During my work writing the first history of cyber conflict it became clear that is easy to take down a target using the Internet, but far more difficult to keep it down over time in the face of determined defenses. And as we saw after the attacks of September 11th, the finance sector can be *extremely* determined.

This should not mean the sector should rest on its successes to date. An optimist might say a digital Pearl Harbor will never come, while a pessimist will insist we're overdue. As a realist, I'd recommend work across several areas.

First, the sector should prepare not just for isolated incidents but conflict and shocks. I'm deeply worried that the finance sector will get caught up in what I believe is the most dangerous moment we've seen for cyber conflict.

From the earliest days of cyber intelligence, a rule of thumb was that "those with the capability to do us significant cyber harm lack the intent; those with the intent lack the capability." High-end adversaries simply did not launch major disruptive attacks as it frankly was not in their larger interests. Terrorists might want to cause a cyber 9/11, but haven't had the means.

But if the talks with Iran collapse, we might see a rapid spike in truly disruptive attacks by a dangerous cyber adversary, which no longer has a stake in a stable global financial system. This should not induce us to sign a deal which we may not have signed anyhow, of course, but it must be a contingency for which the sector is preparing.

Likewise, President Putin of Russia may feel that with his economic back against the wall, he would have little to lose and much to gain by throwing some just-deniable-enough cyber sand in the financial and economic gears of the West. Finance would be an obvious target for his little green bytes: mess with Russia's economy, and you'll feel pain too. He would never initiate such an attack out of the blue, but he already seems to feel he is in a conflict with us, a conflict he may see as increasingly existential.

This danger requires immediate contingency planning within the sector and with regulators and other Federal partners, along with coordination with our international partners particularly in Europe.

Second, what happened to Sony Motion Pictures last year could happen to any company in any sector. The best defended financial institutions operate under a presumption that they have already been breached, and might be able to thwart some of the worst effects. But the North Koreans have shown all of America's adversaries a new tactic, one which if used against a major bank would go far beyond cyber vandalism.

A next-generation Sony-style attack would not take down the sector as a whole, but could seriously disrupt a systemically important financial institution for days.

Last, a finance sector response will be challenged if a sector-wide emergency lasts more than a few days or weeks. Too many people who are key to the sector-wide response are also key to the response of their own financial institution. Some firms have been adding staff to give them more staying power, and a great sign of this weakness being addressed is the hiring of Greg Garcia to be the Executive Director of the FSSCC.

I suspect, though, that exercises like the Quantum Dawn series will show that there is still more to do. The sector must continue these exercises and as it is so international, the exercises must include foreign institutions and foreign regulators. The US-UK finance war game announced earlier this year is a great start.

WHAT NEXT

The best cyber regulations have not pushed security or information sharing. Rather, they have mandated transparency.

The early data-breach notification laws were true game changers and I'm pleased that Congress has been taking this topic seriously. And if a financial institution is not taking cyber risks seriously, its shareholders must be told so they can put pressure on their representatives, the board of directors.

Indeed, in this vein I believe that the Administration should do more to convince financial titans like Warren Buffett and activist institutional investors like CalPers to better understand cyber risks so they can pressure boards themselves, in their own long-term financial interest.

At least as important, the Federal government must lead from the front in three areas. The government pushes the need to share information, but too much remains government information on cyber threats remains classified. The Executive Branch has improved over the last few years, but there is much farther yet to go and the secretive national security and law enforcement agencies might need some oversight from this Committee and others for some added push.

Likewise, the Executive branch is quick to criticize others for lax security practices, even in the face of their own miserable FISMA scores.

And even though it is in the long-term interest of the United States to have a norm that financial infrastructure should be off limits to foreign attacks, the Department of Defense has not made clear statements to that effect. General Keith Alexander came very close in his

response to advance questions for his confirmation from the Senate in 2010, but Admiral Rogers did not repeat the restriction in his own response in 2014. This is likely an oversight, but it seemed to some watchers that perhaps US Cyber Command was putting finance sector targets back on the table.

This subcommittee might also usefully push the Department of Homeland Security and the Pentagon to think of a broader set of possible responses from the military to give the finance sector more staying power in a sustained conflict.

When I was working sector-wide incidents with the FS-ISAC, I can't remember pining for military cyber ninjas or wishing for the Pentagon to lay down suppressing fire. Usually, we simply needed a few more competent people who knew how to keep their heads together during a crisis, who could help wrangle the many details, tasks, sub-groups, and endless crisis teleconference calls. In short, the responses could have been far more successful not with cyber ninjas but with solid officers and NCOs ready to roll up their sleeves. We wouldn't want the sector to stumble simply for the lack of a few MOUs in place beforehand to make this possible.

Thank you for your time; this concludes my testimony.