2d Lt James Marvin

CTC #1

The Financial community within and outside of the Air Force deals with some of the most sensitive information. They have Personally Identifiable Information such as Social Security Numbers, bank numbers, account information, age, race, credit score, and many more that are sensitive to your identity. “Cyber” for this community means protecting this information and insuring that only the correct financial operations are taking place. The financial community is under a barrage of attacks because the information gained is so valuable to the attacker.

Gordon Snow the Assistant Director for the Cyber Division of the FBI spoke before the House Financial Services Committee to illustrate the cyber terrain for the financial services. He painted a grave picture of the current state of affairs back in 2011. He highlighted numerous pain points and I will highlight a few. The first being account takeovers. He said that cyber criminals have been able to exploit financial systems such as the Automated Clearing House that processes direct deposits, card payments, and market trades 1. They can use this access to create false financial transactions that can deplete the resources of the affected entity. If the Air Force fell to this type of attack money that was supposed to go to various government contracts could easily be whisked away to an offshore bank account that is virtually untraceable or untouchable. The next threat would be a release of sensitive information. The government is no stranger to this attack. In 2015 the Office of Personnel Management was breached compromising the PII of 21.5 million federal employees 2. The SSNs that were stolen in this breach can be used to set up fake debit cards. Mr. Snow also touched on the even more sinister reality of insider threats. No amount of external protection can stop a motivated attacker who has been given privileges to the system 1. The only partial solutions to this issue are close system monitoring and good vetting during the hiring process.

It is crucial that this community place a high importance on cyber resources because the price of not preparing could be devastating.

Sources:

1. Gordon M. Snow, “Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit Washington, D.C” (address September 14, 2011)
2. Office of Personnel Management, “Cybersecurity Incidents”, OPM, accessed 2 October 2018, <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>