James McJunkin
GSIS Cybersecurity Principal
June 2022

Defining the Cyber Threat and Defending Small and Mid-Sized American Companies

Nation-State Threat Actors:

China, Russia, North Korea, Iran, Etc.

- Extensive technical capabilities, unlimited funding, heavy Research and Development, Strategic Targeting

Criminal Organizations:

Sophisticated and Highly Organized - Located Primarily in Eastern Europe and the African Continent

- Closely Affiliated with Nation-State Threat Actors
- Benefit Directly From This Affiliation (i.e. Extensive technical capabilities, unlimited funding, heavy Research and Development)

Less Sophisticated -World-Wide (including U.S.)

- Prone to Rely on Malware Purchased on the DARK Web
- Target-Of-Opportunity and Profit Motivated

Issue-Based Causes:

Environment/Climate, Animal Welfare, Left/Right Political Extremism, Etc.

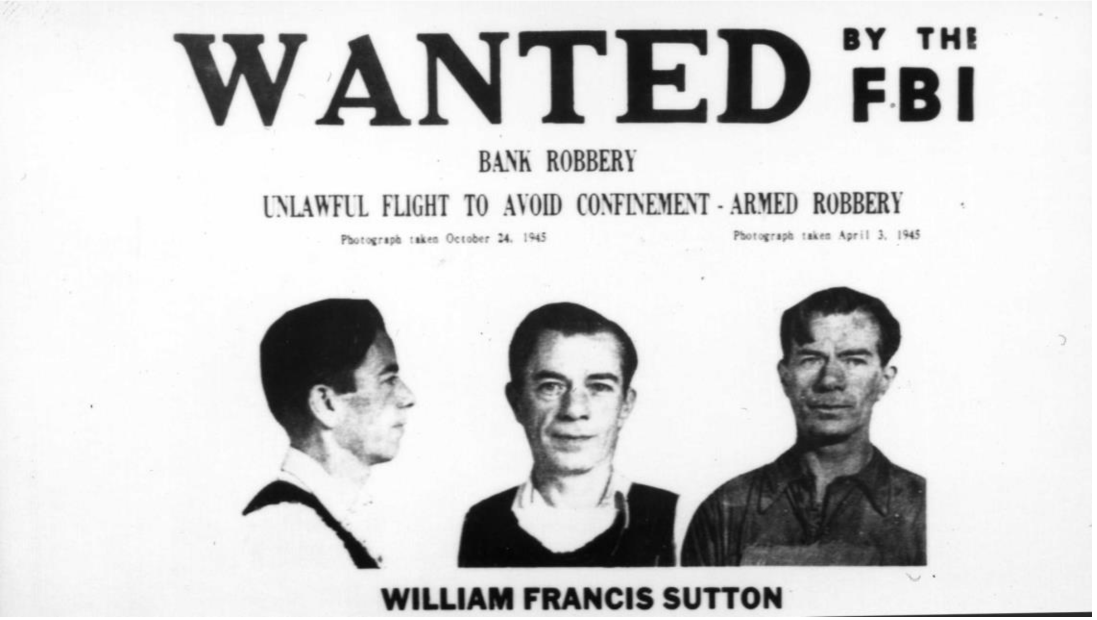
- Higher degree of Victim Targeting

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Anthem.

EQUIFAX

The Face of Cyber Threat Actors?



WANTED BY THE FBI

BANK ROBBERY

UNLAWFUL FLIGHT TO AVOID CONFINEMENT - ARMED ROBBERY

Photograph taken October 24, 1945

Photograph taken April 3, 1945

WILLIAM FRANCIS SUTTON

REPORTER: Willie! Why do you rob banks?

SUTTON: Because that's where the money is"

The Craft:

- First choice to choose the most obvious route
- Hid in plain sight
- Impersonated a postal telegraph messenger, police officer, messenger, maintenance man

"Go where the money is ... and go there often"

" Why did I rob banks? Because I enjoyed it. I loved it. I was more alive when I was inside a bank, robbing it, than at any other time in my life. I enjoyed everything about it so much that one or two weeks later I'd be out looking for the next job. But to me the money was the chips, that's all."

Information Technology (IT) focuses on the systems that store/transmit digital information. Cybersecurity focuses on protecting electronic information stored within those systems.

CYBER POSTURE RATING

- Non-intrusive scan to provide a critical view of technical assets exposed to potential criminals/hackers via the internet.

CYBER SECURITY RISK ASSESSMENT AND STRATEGIC IMPLEMENTATION PLAN

- Cybersecurity assessment determines system and program proficiency against established industry frameworks. Roadmap for improvement is developed to further reduce cyber risk.

TECHNICAL SERVICES

- Internal and external network vulnerability scanning, web application vulnerability scanning, external and internal pen testing, phishing training and testing, and web application firewall, cloud configuration, and code reviews.

EXECUTIVE CISO SERVICES

- Strategic plan implementation project management, SOCaaS technical monitoring and oversight, and cybersecurity advisory services.

GSIS

DISCUSSION/QUESTIONS

GSIS™