CERIAS
The Center for Education and Research in Information Assurance and Security

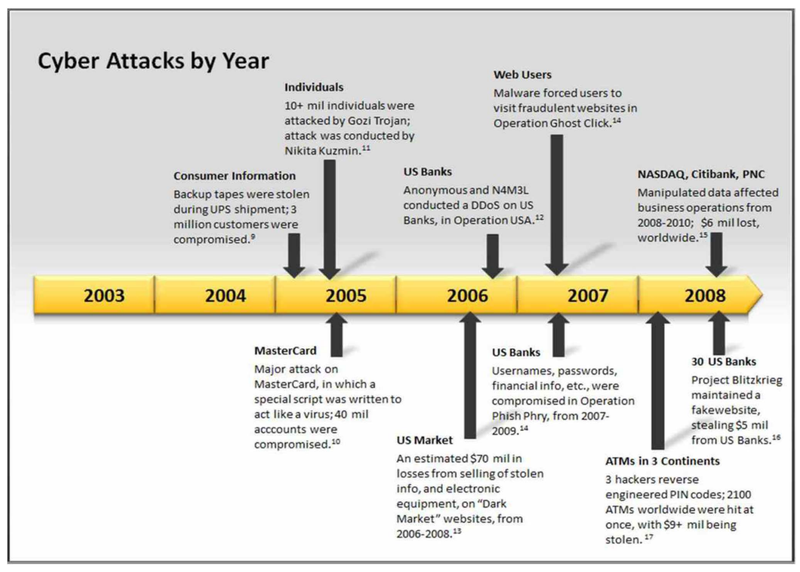
U.S. Bank of Cyber

An analysis of Cyber Attacks on the U.S. Financial System.

Danielle Crimmins, Courtney Falk, Susan Fowler, Caitlin Gravel, Michael Kouremetis, Erin Poremski, Rachel Sitarz Nick Sturgeon, Yulong Zhang under the direction of Dr. Sam Liles.

The technical report looked at past cyber attacks on the United States financial industry for analysis on attack patterns by individuals, groups, and nation states to determine if the industry really is under attack. An analysis explored attack origination from individuals, groups, and/or nation states as well as type of attacks and any patterns seen. After gathering attacks and creation of a timeline, a taxonomy of attacks is then created from the analysis of attack data. A Strengths, Weakness, Opportunities, and Threats (S.W.O.T.) analysis is then applied to the case study Heartland Payment Systems.

Portion of the time line:

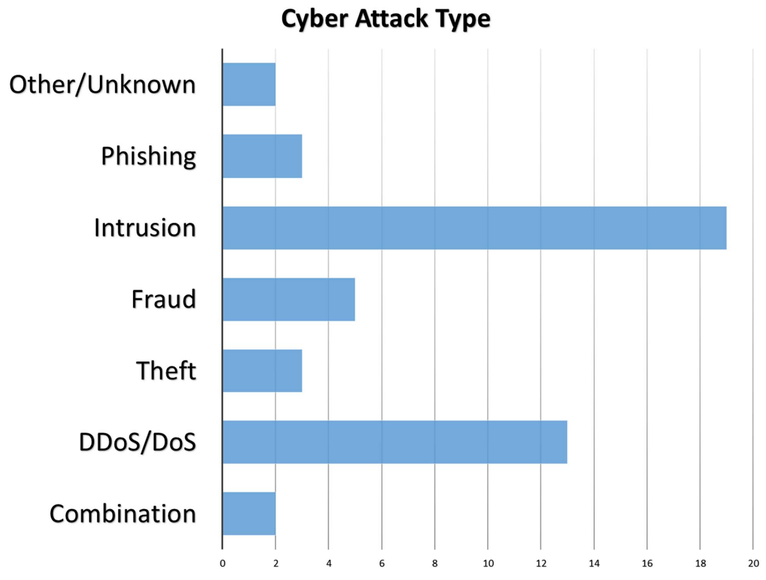


The time line developed showed that the cyber attacks on the financial industry are not new. Attacks can be documented back to the 1970's. What is new are the attack methods. These attack methods change as technology changes.

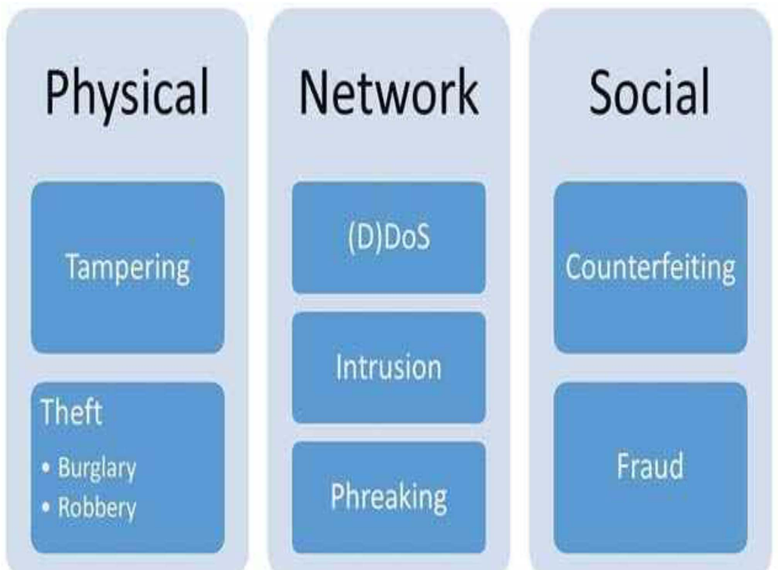
SWOT Analysis:

Strengths	Weaknesses
(1)Awareness Priority (2)End to End encryption is standard (Identity Based Encryption) (3)Expected Security Level (4)Experience	(7) Resources for implementing cyber security (8) Resources for dealing with aftermath of attack
Opportunities	**Threats**
(1)Create and follow better standards (2)Update and upgrade security audits	(9) Lucrative Target (10) Insider Attacks

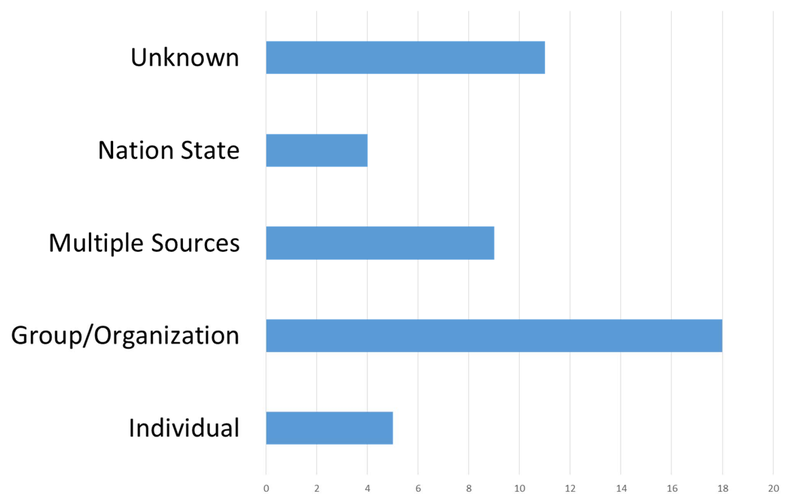
Cyber Attack Type:



Attack Taxonomy:



Source of Attack:



CERIAS

PURDUE UNIVERSITY
DEPARTMENT OF COMPUTER AND INFORMATION TECHNOLOGY

PURDUE UNIVERSITY