Cybersecurity Perspective For The Financial Industry

Zach Jones, Security Project Manager for The Mako Group

Hacking. A term used to describe a myriad of activities perpetrated by a number of different actors, some benevolent, some malicious and others simply curious. Today, a would-be hacker needs to only download some malware from the internet and watch a few tutorials on YouTube to begin causing mischief. The subject of hacking and hackers can become quite complex with shifting definitions, technical jargon and a never-ending stream of new concepts. For the sake of clarity, the problem should be approached from the opposite perspective; not who is doing the attacking or how they are doing it but, rather, what is being attacked.

Information and the systems used to create, manipulate and store data are the target of hacking. To characterized exactly what is being attacked, industry and government alike have adopted the three concepts of Confidentiality, Integrity and Availability with respect to information. Confidentiality speaks to who can access information, integrity, the accuracy of the information and availability, when the information can be accessed. Hackers, whether for financial gain, public disruption or personal amusement, seek to interfere with information and information systems in one of these three areas.

In terms of financial markets and firms, cybersecurity defends organizations and mitigates risk from a variety of threats to the confidentiality, integrity and availability of information. The information targeted is a very real monetary asset beyond the obvious customer data or employee passwords that are usually assumed to be the target of hacking. The confidentiality of corporate data like quarterly reports or news releases, if accessed prior to public release by the PR department, could give hackers a huge advantage in the stock market (New York Times). The integrity of code and other information represents a huge risk whether through hacking or simple coding errors. Knight Capital Group lost $440 Million in 45 minutes (Forbes). The availability of information has become one of the most prolific concerns recently as banks are being targeted by DDoS attacks that can make the average person's money unavailable (ComputerWeekly).

The financial industry is one of the biggest in the world but unlike others almost all of its value is digital. Financial institutions of all sizes represent a daily part in the life of most Americans and with cyber-crime on the rise appropriate actions must be taken. While customer information should be of concern to organizations, it is hardly the most valuable asset or the most damaging risk. As such, cybersecurity in the financial industry is of paramount importance and must be approached with an appreciation and understanding for the risk to and monetary value of information.

Written based on insights shared at the Cybersecurity and Financial Markets Forum on November 29th, 2016 in IIT's Stuart School of Business. The panelists during this forum were:

- *Greg Benson, Incident Response, Planning and Cybersecurity Instructor, University of Illinois, Aurora University and College of DuPage*
- *Andy Kumiega, Ph.D., Vice President, Director of Financial Engineering, Calamos Investments; Adjunct Professor, School of Applied Technology, Illinois Institute of Technology*
- *Peter Van Loon, Manager of Information Security, Eddie Bauer; Board Member, ISACA Chicago Chapter*