CYBERSECURITY AND THE FINANCIAL INDUSTRY

Businesses are under siege from cybercriminals bent on stealing or destroying sensitive data, interrupting critical digital operations, or causing reputational damage. Financial services firms, which handle a wealth of sensitive customer information and have access to crucial trading platforms, are particularly juicy targets.

WHO ARE THE HACKERS?

The landscape of threat actors includes cybercriminals whose objective may be to steal money or information for commercial gain, nation-states that may acquire information to advance national objectives, and hacktivists whose objectives may be to disrupt and embarrass an entity.

NATION-STATES

HACKTIVIST COLLECTIVES

ORGANIZED CRIME SYNDICATES

INDIVIDUAL "HOBBY HACKERS"

FINRA "Report on Cybersecurity Practices," February 2015

HOW BIG IS THE PROBLEM?

Broker-dealers are increasingly exposed to cybersecurity risks, and breaches at a broker-dealer could entail adverse implications for investors, firms, capital markets and even broader swaths of the financial system.

THE HIGH FINANCIAL COST OF CYBERCRIME:

PwC, Global Economic Crime Survey 2014, February 2014

In a sweep of 57 registered broker-dealers and 49 registered investment advisors, most reported that they have been the subject of a cyber-related incident.

INVESTMENT ADVISORS

BROKER-DEALERS

FINRA "Report on Cybersecurity Practices", February 2015

WHAT ARE THE BIGGEST CYBERTHREATS TO FINANCIAL SERVICES FIRMS?

Threats vary by firm and business model. Online brokerage firms and retail brokerages are more likely to rank the risk of hackers as their top priority risk. Firms that engage in algorithmic trading were more likely to rank insider risks. Large investment banks or broker-dealers typically ranked nation-states or hacktivist groups more highly than other firms.

HACKERS PENETRATING SYSTEMS	NATURAL DISASTERS AND POWER FAILURES TAKING SYSTEMS OFFLINE	EMPLOYEES OR OTHER AUTHORIZED USERS STEALING OR MANIPULATING SENSITIVE INFORMATION	OTHER
33%	22%	22%	23%

FINRA "Report on Cybersecurity Practices," February 2015

WHAT DO THEY WANT?

Dangers include email hack attacks, improper transfer or theft of customer assets, and misuse or even theft of customer data and other types of confidential information.

BANK OR BROKERAGE ACCOUNT INFORMATION

PASSWORDS OR PINS

SOCIAL SECURITY NUMBERS AND OTHER SENSITIVE INFORMATION

FINRA "Investor Alerts: Cybersecurity and Your Brokerage Firm," February 3, 2015

WHERE ARE FIRMS VULNERABLE? (AND WHAT ARE THEY DOING ABOUT IT?)

A variety of factors drive a firm's exposure to cybersecurity threats—and firms are likely to take a risk-management approach to avoid attacks. Some examples of threats and risk mitigation include:

MOBILE DEVICES

- Limiting access to work materials on approved devices
- Using secured networks when accessing work materials on personal device
- Protecting access with passwords

EMPLOYEE THEFT

- Limiting access to sensitive information on a "need to know" basis that's frequently re-evaluated
- Heavily monitoring employee usages of sensitive information

MALWARE AND PHISHING EMAILS

- Training employees not to click on phishing emails or visit suspicious websites
- Filtering access to harmful sites and emails

THIRD-PARTY VENDORS

- Ensuring that subcontractors have vigorous data protection systems in place

HACKERS POSING AS CLIENTS

- Incorporating robust client identity verification

Need attribution - not sure where this came from.

WHAT CAN I DO?

As an investor, you should understand your firm's cybersecurity policies and take personal precautions to safeguard your brokerage accounts and personal financial information.

GET TO KNOW YOUR FIRM'S CYBERSECURITY PRACTICES AND POLICIES

- What **safeguards** do they have in place to protect personal information and assets?
- Do they **monitor your personal information** to determine whether it has been stolen or misused?
- How do they **handle an account intrusion** or other malicious cyber event?
- Do they **reimburse you** if your assets are compromised by a cyberattack?

PRACTICE CYBER SAFETY

Use up to date firewall and anti-virus programs. Log out of all online sessions. Password-protect your device—select the highest security setting.

DON'T FALL FOR PHISHING SCAMS

Watch for spam email or a fake websites. Beware of emails that request personal information. Don't reply to, or click on a link in, an unsolicited email that asks for your personal information.

READ YOUR ACCOUNT AND CONFIRMATION STATEMENTS

Make sure that all transactions that are shown are ones that you actually made or authorized. Report mistakes immediately and follow up in writing.

FINRA "Investor Alerts: Cybersecurity and Your Brokerage Firm," February 3, 2015