March 28, 2018

MULTISECTOR CYBER-DEFENSE COLLABORATIVE (MCC)

Purpose

MCC is a membership group formed to identify and share the most effective practices being used by financial services institutions and service providers to combat the threat of cybercrime.

Members meet periodically and ad hoc to learn what other members are discovering, testing and implementing to defend against new and old cybercrime threats.

MCC was conceived as the way to focus the combined efforts of all members to benefit each member. The scope is limited to financial services sectors that have similar characteristics and exposures and which therefore require similar defenses.

MCC members agree to use the defenses discussed for their institution's own advantage and use their best efforts to maintain privacy so as not to alert villains of the details of practices being implemented.

The financial services sectors represented in MCC are listed below. Membership can include product manufacturers as well as firms that provide services involving retention of sensitive data, holding assets or execution of transactions (Service Providers).

- ✓ Investment Management
- ✓ Life and Annuity Insurance
- ✓ Retirement Plans
- ✓ Broker/Dealers
- ✓ RIAs

DALBAR, Inc.
Phone: 617-723-6400
303 Congress Street
Boston, MA 02210
Fax: 617-624-7200

MCC Defense

Defending against cybercrime requires an understanding of who the cyber-villains are, their objectives and deployment of strategies to thwart these objectives.

The Cyber-villains

Cyber-villains that present the greatest threat are those that have the knowledge, expertise and motivation to steal or corrupt data and to use that stolen data to infiltrate and steal assets. The most dangerous threat groups are ex-employees, ex-advisors and ex-clients ("Ex's") conspiring with crooked technical experts to manipulate systems. Ex's are intimately familiar with practices and vulnerabilities so defenses must contemplate villains with such knowledge.

The Villain's Objectives

Cyber-villains who attack financial services recognize three potential targets:

- Data… that can be corrupted or sold to other villains
- Assets… that can be destroyed or stolen
- Transaction Systems… that can be disabled or misused

Defensive Strategy

Defenses must protect against the two basic forms of attacks:

- Attacks to steal or corrupt data
- Attacks that use stolen data to infiltrate and steal assets

The MCC defense is based on three actions by each member:

- Adopting and maintaining effective practices to protect all relevant points of access (Websites, Mobile Devices and Apps, IVRs, Contact Center Reps and Online Statements). Members recognize that all points of access are vulnerable to the same attackers using the same attacks.
- Privately notifying all members, through MCC, of attacks, whether prevented or not. In this way, new attacks are quickly prevented from spreading and the effectiveness of defensive practices are monitored.
- Publicly support MCC and its mission of defense of financial services against cybercrime. This deters would-be villains from pursuing financial services.

DALBAR, Inc.
Phone: 617-723-6400

303 Congress Street

Boston, MA 02210
Fax: 617-624-7200

Access Methods

It is the intent of MCC to include all access to data, assets and transactions that present a material threat to financial institutions and service providers. The following list represents the initial areas of coverage but is expanded and changed as situations and concerns change.

- ✓ Websites
- ✓ Mobile Devices and Apps
- ✓ Contact Center IVRs
- ✓ Contact Center Reps
- ✓ Online Statements

Member Benefits

MCC Members have the opportunity to meet online monthly and in-person annually. Each meeting has one or more themed topics planned in advance as well as member's reports on developments, incidents and changes underway. Members answer questions from other members.

Members are free to reach out to other members or the membership group as a whole any time the need arises. The outreach may require a simple answer, prolonged discussion or an online meeting.

Membership includes a copy of the "*In-Depth Analysis*" from the "*State of Authentication in Financial Services Study*". The "*In-Depth Analysis*" provides the rationale for using individual practices and the reasons some have been abandoned.

Through these exchanges, members gain access to the combined knowledge of MCC members and stay abreast of the latest developments in the defense against cybercrime in financial services.

Member Requirements

Members must represent a recognized financial institution or service provider so as to avoid infiltration by cyber-villains.

Member skills and knowledge in a number of areas bring value from different points of view and are welcomed:

- ✓ General Management… with an overall perspective of institution's business and profitability
- ✓ Technology… providing a perspective of the scale and complexity of various practices
- ✓ Risk Management… is expected to weigh in on the imperative nature of certain practices
- ✓ Compliance… provides guidance on practices that may be outside of existing regulations and mandates

Firms may include as many members as desired.

DALBAR, Inc.
Phone: 617-723-6400
303 Congress Street
Boston, MA 02210
Fax: 617-624-7200

MCC PRELIMINARY AGENDA -2018

The following topics are proposed for coverage by MCC during 2018. The specific schedule of coverage is determined by members' votes. Members may add and schedule other items of interest on an ongoing basis.

Experts in specific topics will be invited as appropriate.

Common Threats

Financial services institutions look remarkably similar to a cyber-villain. This enables the villain to repeat the same approach with a number of high value targets. By banding together, institutions can construct defenses that protect all as quickly as the villains can invent the threats.

- Structural Similarities
- Common Data
- Valuable Data
- Theft, Misuse, Hostage and Destruction

Understanding Cyber-villains

Cyber-villains do not have a simple profit motive. The motivation is as likely to be doing harm as it is to be monetary. Methods used are not limited but defined by where opportunity and access exists.

- Goals
  - Mischief or Fame
  - Monetary
- Methods
  - Accessibility
  - Technical Skills
  - Overcoming Defenses
  - Industry Specialists
- Scale
  - Account by Account
  - Volume Villains

DALBAR, Inc.
Phone: 617-723-6400
303 Congress Street
Boston, MA 02210
Fax: 617-624-7200

Uniformity of Defense

Unlike other threats, the threat of cybercrime exists in all lines of business and all means of access to data, transactions and systems. It is a tragic error to limit defensive thinking to one's own firm, department or function. It is the firm, department or function with the weakest defense that presents the greatest risk. Villains are continuously searching for new ways to "break in" and their past performance is no indication of future results!

- Folly of Designated Turf
- Integrated Strategies
- Responding to New Threats
- Use of Threat Levels

Frequent Changing of Practices

In recognizing the threat from Ex's (ex-employees, ex-advisors and ex-clients) it is necessary to continuously change defensive practices to make the knowledge held less threatening. The awareness of the fact that defensive changes are ongoing also presents a challenge to villains to find out what to expect. On the other hand, defensive practices that remain unchanged for years provide an opportunity for villains to find ways around them.

- Frequency of Changing Practices
- Indicators of When Practices Need Change
- Communicating Changes
- Scale of Changes
- Cost of Changes
- Effect of Changes on User Experience

Username and Password Standards

Username and passwords are the almost universal method of controlling access to data, transactions and systems. The complexity of the username/password protocol can also create a negative user experience that is injurious to business.

- Types of Threats to Password Protection
- Various Standards in Use
    - Nature of Protection Achieved by Each
    - Required User Practices
    - User Experience
- Types of Access Covered

DALBAR, Inc.
Phone: 617-723-6400
303 Congress Street
Boston, MA 02210
Fax: 617-624-7200

- Response to Password Denial
  - Single Denial
  - Multiple Denial Practices

Alternatives to Username and Passwords

Alternatives to commonly used username and password protocols are also used for compatibility with existing technology and to enhance the user experience. These alternatives are viable until cyber-villains are able to overcome them.

- Strengths and Weaknesses of Alternatives
  - 4 digit "PIN"
  - Social Security Number
  - e-mail Address
  - Account Number

Multi-tiered Authorization

The risk associated with certain data, transactions and systems may require different levels of authorization. Top clearance is burdensome and unnecessary for most users. This detracts from the user's experience.

- Tiers by User Classification
  (Advisor, Individual Client, High Net Worth Client, Plan Sponsor, Plan Participant, Third Party Recipients)
  - Password protocol used
  - Data Access Permitted
  - Transaction Permitted
- Tiers by Content
  - Public Information
  - Account Summaries
  - Statements
  - All Account Information
  - Limited Transactions
  - Full Array of Transactions
- Access to Unrestricted Data
- Event Dependent Permissions

DALBAR, Inc.
Phone: 617-723-6400
303 Congress Street
Boston, MA 02210
Fax: 617-624-7200

- Existence or Non-existence of Previous Transaction
- Existence of Specific Conditions

Response to Data Loss

Data loss requires a response about the specific loss as well as other vulnerable areas and other institutions. Response regarding recovery is limited to the loss itself but the loss requires identifying and defending other vulnerable areas within the institution and at other institutions.

- Loss of Firm's Own Data
  - Access point and data
  - Password/Username Reissue
  - User Notification/Actions
  - Upgrade of Protection
- Loss of Other Financial Institution's Data
  - Identify data held in common… names, addresses, e-mails, phone numbers, social security numbers, passwords, security questions
  - Self-examination
  - Upgrade Protection
- Loss of Data from Non-financial Entity
  - Determine level of threat from potential crossover of data held in common

Protection from User Exposure

Users may inadvertently permit unknown villains to see or record their interaction with various devices. Information stored on the user's own devices can also be accessed by villains. Such knowledge can later be used for illicit purposes.

- Exposure by Types of Access
  - Villain Observing or Recording User
  - Compromise to User's Computer or Phone
  - Limits to Prevent Exposure by User
- Display of Key Data (Social Security, Account Numbers, etc.)
  - Omitted
  - Truncated
  - Masked
- Key Data Use by Display Medium

DALBAR, Inc.
Phone: 617-723-6400
303 Congress Street
Boston, MA 02210
Fax: 617-624-7200

  - Statements
  - Websites
  - IVR
  - Mobile Devices
- Protections with Paper Communication
  - Envelopes Used
  - Test for Valid Addresses
  - Procedure for Fraudulent Mail Scams

Automated Threats

Automated tools permit villains to use technology to make millions of attempts to find ways into systems to extract data, execute transactions and corrupt systems. Defenses include detection and protection from such automated attacks.

- Phishing Protections
- Automated Password Generators
- Interpretive Screening (Image or Voice)

Biometric Identification

Biometrics are rapidly becoming a preferred alternative to username and password because of its high reliability and positive user experience.

- Fingerprint
- Voice
- Facial Recognition
- Iris Recognition

Threat Level Changes

Threat levels rise when new breaches of data, transactions or systems occur. These threat levels are lowered when adequate defenses are put in place.

- By Type of Access
- By Activity
- Factors Affecting Threat Level

DALBAR, Inc.
Phone: 617-723-6400

303 Congress Street

Boston, MA 02210
Fax: 617-624-7200

Ransom Demands

One particularly dangerous form of cybercrime is the ability of a villain to prevent access to critical systems. This villainous denial of access is accompanied by one or a series of demands for payment in order to permit access.

- Protection
- Response to Demand

Third Party Services

Third party services are available to validate identities and other security measures.

- Review of Services

DALBAR, Inc.
Phone: 617-723-6400
303 Congress Street
Boston, MA 02210
Fax: 617-624-7200