SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER NO. 2017-002

PILOTING THE EXCHANGE OF INSIDER THREAT REPORTS: INFORMATION SHARING CHALLENGES TO PROACTIVE CYBER FRAUD IDENTIFICATION

ELIZABETH (Beth) M. PETRIE

CASEY EVANS

PUBLICATION DATE: 9 May 2019

Piloting the Exchange of Insider Threat Reports:

Information Sharing Challenges to Proactive Cyber Fraud Identification

Elizabeth (Beth) M. Petrie
Citi, Managing Director
Technology/Cyber Risk Management Frameworks

Casey D. Evans, Executive-in-Residence
American University, Assistant Dean
Kogod School of Business

Table of Contents

List of Figures

Acknowledgements

The authors wish to thank the SWIFT Institute's research sponsorship program for funding this research and the expertise provided by SWIFT's technical group. Special recognition goes the individuals from each of the financial and investment services organizations, who participated in this year-long pilot. The authors would like to extend our gratitude for your time and commitment to explore new approaches to information sharing in our united front to fight cyber fraud. The authors also wish to acknowledge Dan Carroll for his contributions in customizing the branding for all of the presentation and written materials.

The views, opinions, and/or findings contained in this report are those of the authors and should not be interpreted as representing the official views or policies of Citi or American University.

Key Words

Cyber, Fraud, Intelligence, Indicators, Insider Threat, SWIFT, Information Sharing

Abstract

Research published by the SWIFT Institute in August 2017, titled "Sharing Insider Threat Indicators: Examining the Potential Use of SWIFT's Messaging Platform to Combat Cyber Fraud" proposed a protocol for sharing insider threat activities between financial institutions. Building from the assumption that cyber criminals work off a shared services model to give them access to infrastructure, tools, targets and options for monetizing their exploits, the research asserted the strengthening of communication channels for defenders to share real time threat information is essential to pre-empting cyber fraud. A pilot to test this information sharing protocol through the development of an Insider Threat Report (ITR) message type was initiated in late September 2017. The pilot ran for 12 months during which time participants from financial and investment services firms worked together to validate a set of insider threat indicators based on actual use cases from internal investigations and customized the ITR fields for transmitting the information over the SWIFT messaging platform. The pilot concluded with a number of findings on key challenges to this level of information sharing that, until resolved, will prevent member organizations from formalizing their engagement on this effort.

1. Summary of Findings

Insiders often operate under a shared services model giving them access to infrastructure, tools, targets and the ability to monetize their exploits. As a result, organizations across industries must enhance communication channels to share threat information to preempt cyber fraud schemes. Financial institutions have a common interest in protecting against insider threats and therefore in sharing anonymized information about risks. However, it's challenging to do in practice, which was confirmed in the information sharing pilot discussed in this paper. While there were some legal hurdles around sharing information, the most significant findings related to data access and technical issues, cultural constraints for internally sharing data, inconsistencies between financial institutions around data collection, and a lack of a universal call to action for sharing insider threat activity.

The establishment of a dedicated insider threat program within financial institutions has been evolving over the last decade. As a result, institutions are at different stages of maturity when it comes to data collection on insider threat activity. Standards do exist for establishing programs; however the standards are intended to be used as guidance and financial institutions are not required to implement these standards. For example, the extent to which insider activity can be monitored varies depending on technical capabilities. As a result, there was a variance among pilot participants in the use of surveillance tools because of the uniqueness of each organization's network. Therefore, developing universal use cases that could be easily reported on by all institutions was a challenge. Without universal use cases, this presented an obstacle to using behavioral analytics to identify new patterns of fraudulent activity.

The pilot further highlighted the need for a common lexicon for standardizing the classification of threats so when threats are reported, a comparison can be made with internal case information to see if there are similarities. In many instances, case information was deemed to be highly sensitive and therefore tightly held by multiple departments within each participating firm. The pilot found internal silos to be the biggest hurdle to obtaining the data needed. Additionally, domestic policies and procedures walled off access to some data sets, such as human resource information. Data that was approved for submission still had to be securely transmitted. These security protocols intended to prevent security breaches inadvertently provided barriers for participants to use tools needed to analyze the information received.

There were also cultural, legal and regulatory considerations around sharing information, and the cultural norms were found to be as important as the legal and regulatory restrictions. These cultural practices frequently superseded legal and compliance requirements because even though protocols for information sharing were provided in procedural manuals, buy-in by the data owners was still needed for the pilot to proceed.

For example, participating in this pilot required a manual review of case data for each use case; however the case data was not owned internally by one department. This required participants to gain an additional level of internal agreement to access the relevant data despite the firms having obtained legal permission to exchange information.

There remains goodwill amongst firms to cooperate but action to do so effectively is unlikely without some strong external push, such as public sector pressure or a change in the perception of the urgency of a threat. It was particularly difficult to justify the allocation of resources to this pilot when some procedures do already exist for communicating insider threat information between institutions, such as through email. Given the current market climate, without an event occurring that has a systemic impact across the sector, investing resources in promoting new information sharing exchanges may actually take away from addressing the current threat environment.

2. Introduction

In November 2017, the SWIFT Institute awarded a research grant in support of a pilot to customize a SWIFT message type for sharing threat indicators between a group of financial and investment services firms leveraging the SWIFT messaging platform. This pilot was based on research published by Petrie and Evans in October 2017[1] , which asserted cyber criminals operate on a shared services model to gain access to infrastructure, tools, targets and opportunities for monetizing their exploits. This shared services model relies upon communications channels to provide cashout options. It was therefore concluded that if organizations strengthened communications channels to share real time threat information, the potential for pre-empting cyber fraud could be realized.

In September 2017, a kickoff workshop was held to bring together pilot participants. The pilot objectives were to deliver a list of validated insider threat indicators, which have been assessed for legal and privacy implications; to format a threat report that could be customized into a standardized SWIFT message type; write procedures for issuing insider threat reports; and make recommendations as appropriate to expand the pilot if deemed successful. The pilot ran for 12 months during which a set of validated indicators was created, a threat report template customized, development of a set of use cases achieved, and data collected for information sharing. It was determined at the conclusion of the 12 months that expansion of the pilot was not feasible; therefore transmission of the Insider Threat Reports (ITRs) was not tested and procedures for filing the ITRs were not written.

Although expanding the pilot concluded without successful transmission of the ITRs, there were several observations captured that may contribute to information sharing trials in the future. It was noted during the pilot that the financial sector community in general fully supports discovering ways to automate the exchange of insider threat activity between financial institutions, which goes above and beyond what is currently being accomplished in the various information sharing forums worldwide. These forums focus on best practices for establishing insider threat programs without full disclosure of insider threat activity, similar to the automated exchange of indicators of compromise (IOCs), which now occurs on a daily basis. The exchange of IOCs was at one time considered a bridge too far to cross as IOCs can indicate exploitation of existing vulnerabilities. However, over time, the community has seen the benefit to IOC exchanges in order to deactivate attacker tactics. The results of this pilot are being published as a call to action for the financial sector community to initiate programs which overcome the internal challenges of information sharing so that communication between organizations can be enhanced to pre-empt cyber fraud activity committed by insiders.

[1] Petrie, Elizabeth M., Casey D. Evans, SWIFT INSTITUTE WORKING PAPER NO. 2016-003 titled, “Sharing Insider Threat Indicators: Examining the Potential Use of SWIFT’s Messaging Platform to Combat Cyber Fraud.” SWIFT Institute. Published October, 2, 2017.

3. Use Cases

After establishing the objectives of the pilot, participants worked to validate the insider threat indicators identified in the October 2017 whitepaper titled, "Sharing Insider Threat Indicators: Examining the Potential Use of SWIFT's Messaging Platform to Combat Cyber Fraud."

To validate the indicators, each of the participants ran the indicators against a body of known insider threat cases from their organization within the preceding 12 months. To be considered valid, the indicators were ranked based on the number of recurring instances they appeared in the investigations. The indicators were further evaluated to determine whether or not the organization had the ability to monitor for the activity. In some cases, organizations had indicators of insider threat activity captured in investigations, which could not yet be captured and monitored through automation or due to legal issues.

Of the 54 insider threat indicators identified, 19 were used to create four use cases. The pilot participants decided to produce use cases versus collecting against a general list of indicators because for the purposes of the pilot, the use of behavioral analytics was not planned. It was decided use cases would give the participants a sense of the volume of information that could be collected to simulate what a behavioral model might look like. Of the four use cases, only one was determined to be viable because the other three relied heavily on access to fraud investigations to gather the additional information against all the use case indicators.

Pilot participants constructed the use cases by brainstorming a set of scenarios based on their knowledge of typical insider cases. They then refined these scenarios by cross referencing the activities with the list of validated indicators. Activities that could not be paired with an indicator were eliminated from the scenario. Finally, the group discussed the justification for sharing the indicators between their institutions to determine if sharing these indicators would close knowledge gaps in the scenario. It was decided that each of the resulting use cases provided necessary insights into insider tactics for circumventing controls as well as new tools being used to capture and transmit insider information.

In order to demonstrate how these use cases could be automated to retrieve desired sets of information in response to indicators, a set of rules in SQL and Virtual Basic for Applications (VBA) programming languages were created for one of the indicators sets under use case #4 regarding the discovery of external financial institution information posted to the Darkweb. Appendix A contains these simple set of rules.

3.1. Use Case # 1 Student Account Activity

Justification Statement: The basis for sharing this information could lead to proactive identification of cashout activity at other financial institutions as well as possible mule activity.

Figure 2.1: Use Case #1 Student Account Activity

Scenario A

A foreign exchange student with a visa (J-1 or other student visa) opening a student account with an active volume of incoming and outgoing electronic funds transfer (EFT) activity followed by an extended dormant period. Activity in the account resumes after a long period of dormancy, defined as 9-12 months.

Indicators of Insider Activity:

- Insider turning off alerts
  - Fraud alerts
  - Transaction alerts
  - Limit alerts
- Privacy options modified to lowest settings
- Account being accessed with internal credentials

Scenario B

Account that suddenly begins to receive and send Electronic Funds Transfers (EFTs).

Indicators of Insider Activity:

- Account profile of activity deviates from its norm, i.e. sudden big wire transfers
- Activity is structured to be under wiring limits and skirt other bank reporting requirements

3.2. Use Case #2 Separated Employee Accesses Client Information

Justification Statement: The basis for sharing this information is to potentially identify victim bank if the competitor identifies unknown incoming files. In addition, the competitor bank would know that they hired a questionable employee.

Figure 2.2: Use Case #2 Separated Employee Accesses Client Information

Scenario A

Separated employee unnecessarily access, copies and shares client information to a competitor. Employee does not have authorized rights to share client information. The competitor is the separated employee's future employer.

Indicators of Insider Activity:

- Separated employee
- Client information accessed by employee who does not have approved account access
- Encrypted files emailed to competitor institution

3.3. Use Case #3 Current Employee Alters Customer Information

Justification Statement: The basis for sharing this information is to increase knowledge on how account controls are overcome to prevent customers from being notified their account information has been changed. Sending and receiving institution are both impacted by a fraudulent transfer of funds.

Figure 2.3: Use Case #3 Current Employee Alters Customer Information

Scenario A

An employee changed a customer's contact information on an account; an action unrelated to the employee's duties. An EFT occurs immediately after the change.

Indicators of Insider Activity:

- Employee is not an approved change agent
- Account contact information modified
- Notification of account changes deactivated
- Account contact information changed within 24 hours of an EFT occurring

Scenario B

Changing a customer account attribute and reverting it back within a specific time period.

Indicators of Insider Activity:

- Employee is authorized to make an account change, but peer analytics reflects employee is making changes to accounts more than his/her peers
- Customer account changes are reverted within a short period of time, defined as 24-48 hrs

3.4. Use Case #4 Separated or Current Employee Takes Categorized Company Data

Justification Statement: The basis for sharing this information is to automate a practice already engaged in by financial institutions to inform one another when internal company information is discovered in a public repository. Can also provide insights on new tools being used to extract company information undetected and identify new sites information is being posted for disclosure or for sale.

Figure 2.4: Use Case #4 Separated or Current Employee Takes Categorized Company Data

Scenario A

Mass emailing or posting of sensitive company data to suspicious locations, such as personal email or cloud based storage.

Indicators of Insider Activity:

- Company information marked as such, i.e. customer, internal, restricted, etc.
- Sent to external site, such as:
  - Personal email
  - To a customer and BCC to personal email
  - Uploaded to cloud storage services
    - Site is uncategorized or blocked by company policy
  - Darkweb
  - Authorized external site being used for unauthorized purposes ie.
- File is encrypted
- No business exception provided for this activity
- Multiple attempted uploads
  - Frequency of attempted uploads
  - Number of channels attempted for upload

4. Challenges: Information Sharing Between Member Organizations

Findings in the August 2017 research paper, "Sharing Insider Threat Indicators: Examining the Potential Use of SWIFT's Messaging Platform to Combat Cyber Fraud" suggested the infrastructure and capabilities of the SWIFT message platform were well suited to transmit threat information between member organizations. During the pilot, participants discussed what fields would be necessary to capture information from each of the use cases and then met with their respective legal counsel to determine what information would be permissible to share. Using Microsoft Excel, a spreadsheet was customized to simulate the format of an Insider Threat Report SWIFT message type. This was done to expedite the information sharing exchange process during the data gathering phase of the pilot.[2]

In order to gather data against each of the use cases, pilot participants reviewed their organization's insider threat investigations from January 2017 to June 2018. While partial data was obtained for use cases #1-#3, the majority of data was available across all participating firms for use case #4. It was determined that the fraud investigative units within the participating firms would have the remaining data needed to complete use cases #1-#3; however because internal systems are not interconnected, the insider threat groups couldn't access the relevant cases. Discussion with the fraud teams resulted in a verbal confirmation the data existed; however in order to use the data, a secondary review by legal counsel for the fraud units would have been required. It was decided not to pursue this secondary review as the pilot focus was to test the information sharing protocol of at least one use case.

[2] Appendix B provides the details of the Excel template.

5. Survey Overview and Results

To better understand the importance of this work to the community, a survey was created to share with a panel of experts. The goal of the survey was to receive feedback from a panel of insider threat experts on the importance of gathering and sharing insider threat information. Additionally, it was hoped the survey results would help provide insight into what tools, mechanism/functionality, or processes that were used to get data out of institutions. To increase the response rate, the questions were streamlined and the survey was condensed so that it took an average of five minutes to complete.

The Financial Services Information Sharing and Analysis Center ("FS-ISAC") was one of the first ISACs to be established in 1999 and has nearly 7000 members.[3] Their mission is to share physical and cyber security threats and vulnerabilities among both private and public sector entities to protect the financial critical infrastructure. The FS-ISAC has a North American Insider Threat Working Group, which is a committee of insider threat experts, charged with approaching the insider threat programmatically, identifying best practices for management. The group also helps facilitate in-person meetings and calls, as well as dealing with issues specific to the region.[4]

5.1. Constructing the Survey

The survey questions were developed with the assistance of this pilot's members. Survey participants were asked to evaluate the questions to indicate if the information would further the knowledge base of the participant's insider threat program were it to be shared between financial institutions. The following questions were intended to enhance insider threat monitoring, for example, by sharing techniques being used by insiders to attempt to circumvent monitoring, or the use of new sites to sell proprietary information. It was noted that the sharing of the following information would not include identifying information on the employee or any specifics on their employment, such as job title or grade, employing institution's name or job description.

- Internal company information sent to an external site (ie. personal email), without a valid business need, using means to attempt circumvention of monitoring (Y/N)
- Identification of another financial institutions' data on an underground site (Y/N)
- Current employee who uploads encrypted internal company information to an external site without a valid business need (Y/N)
- Employee who has been notified their position has been terminated uploads encrypted internal company information to an external site (Y/N)

[3] Financial Sector-Information Sharing and Analysis Center. Accessed October 12, 2018 from https://www.fsisac.com/about/mission
[4] Financial Sector-Information Sharing and Analysis Center. Accessed October 12, 2018 from https://www.fsisac.com/about/committees#ITWG

- Employee who has been notified their position has been terminated uploads internal company information with a file capture/upload tool (ie. uses screen captures and uploads using CURL) to a categorized site for atypical business purposes (ie. use of GitHub to publish proprietary information v. open source code) (Y/N)
- Employee who has been notified their position has been terminated attempts to upload internal company information on multiple occasions using a variety of channels (Y/N)
- In your experience, what tools does an insider use to encrypt data sent outbound (ie: 7zip)? (Free narrative)
- What sites do insiders use to upload internal information for unauthorized external use (ie: Github, Dropbox, etc)? (Free narrative)
- What mechanism/functionality or processes have you seen insiders use to get the data out for unauthorized external use (ie: Office 365 flow)? (Free narrative)
- What other information would you find useful if shared between financial institutions to proactively identify insider threat tactics? Please only list types of information that you would be willing to share with other financial institutions. (Free narrative)
- Do you want to be considered as a partner in a pilot currently underway to establish a secure platform for exchanging insider threat indicators between financial institutions? (Y/N)
- Are you currently exchanging insider threat information on a secure platform internally (ie. between the insider threat team and investigations team)? (Y/N)
- Does your organization use the SWIFT platform? (Y/N)

The survey was created on www.surveymonkey.com and participants were emailed a link to take them directly to SurveyMonkey's website. The survey was emailed to the Chair of the FS-ISAC's North American Insider Threat Working Group, who then circulated it among the group's members. Of the members surveyed, there was an approximate 50 percent response rate.

5.2. Survey Results

100% (8/8) of the survey participants agreed that sharing of the following would increase the knowledge base of their institution's insider threat programs:

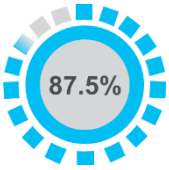
Question 1 - Internal company information sent to an external site (ie. personal email), without a valid business need, using means to attempt circumvention of monitoring.

Question 3 – Current employee who uploads encrypted internal company information to an external site without a valid business need.

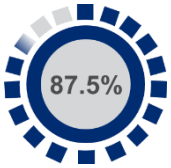
Question 4 - Employee who has been notified their position has been terminated uploads encrypted internal company information to an external site.

Question 5 - Employee who has been notified their position has been terminated uploads internal company information with a file capture/upload tool (ie. uses screen captures and uploads using CURL) to a categorized site for atypical business purposes (ie. use of GitHub to publish proprietary information v. open source code).

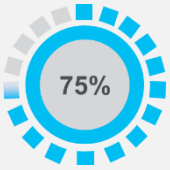
Figure 4-1: Survey Results



87.5% (7/8) of the survey participants agreed that e*mployee who has been notified their position has been terminated attempts to upload internal company information on multiple occasions using a variety of channels (Question 6)* would increase the knowledge base of their institution's insider threat programs.

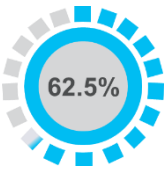


87.5% (7/8) of the survey participants provided information about *the mechanism, functionality or processes they have seen insiders use to get the data out for unauthorized external use (Question 9)*. The processes provided were Outlook, hand carry, uploading information to a vendor site and then download from home using the same credentials, printing, personal email, personal phones plugged into work laptop, unapproved software, FTP, and proxy redirects.

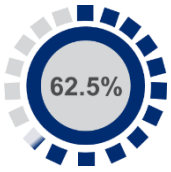


75% (6/8) of the survey participants agreed that *identification of another financial institutions' data on an underground site (Question 2)* would increase the knowledge base of their institution's insider threat programs.

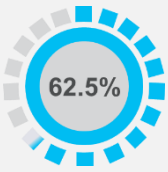
75% (6/8) of the survey participants *provided information about what tools an insider uses to encrypt data sent outbound (Question 7).* The tools listed were 7zip (2/6), Winzip (5/5), Application whitelisting (1/6) and Gzip (2/6).



62.5% (5/8) of survey participants provided information about *the sites insiders use to upload internal information for unauthorized external use (Question 8).* The sites provided were Dropbox.com (5/5), Onedrive (3/5), docs.google.com (3/5), Amazon Drive (1/5), Box.com (2/5), Any other public file shares (1/5), GitHub (2/5), Live.com (1.5).



62.5% (5/8) of survey participants provided information about *what else would be useful if shared between financial institutions to proactively identify insider threat tactics (Question 10)*. The suggestions were lexicon search words, tactics used, information targets, intel on compromised customer information, specific systems targeted, method of exfil, gaps identified, general lessons learned, and exchange of file types used by insiders to transmit proprietary information.



62.5% (5/8) of survey participants are SWIFT members. None of the SWIFT members volunteered to participate in an expansion of this pilot**.** One non-SWIFT member volunteered to participate in an expansion of this pilot.

50% of survey participants are currently exchanging insider threat information on a secure platform internally.

6. Pilot Reflections

Pilot participants were interviewed to get their feedback on how well the pilot objectives were achieved and their insights on any learnings. Overall, their experience was positive despite the obstacles faced. According to the pilot participants, the level of communication, willingness to share ideas, and collaboration within the group were highlights of the project. They felt pleasantly surprised that big competitors could work together towards a common goal. All believed the use cases that were developed and then refined were strong, and noted an appreciation for the opportunity to learn about the processes to investigate insider threats within each institution.

While their overall experience was positive, our pilot participants noted the many challenges that were faced during this project. While there were some legal hurdles around what information could be shared, the most significant findings related to data access, cultural constraints for internally sharing data, inconsistencies between financial institutions around data collection, technical issues and a lack of a common call to action.

6.1. Data Access

Internal silos were universally noted as the biggest hurdle to obtaining the data needed to support this project. Access to data was limited for each pilot participant due to the hurdles that exist internally within each organization. All of our pilot participants were members of the Insider Threat Group within their organization. Much of the data needed to support the pilot use cases was “owned by” the fraud department or investigation groups at their respective institutions. Since the pilot participants were not technically in the fraud or investigation groups, they lacked proper credentials to access the data and, therefore, were kept from collecting pertinent data supporting all of the use cases, not just use case #4. For example, data held by the fraud department was subject to review and approval for sharing by the fraud department’s legal team, such as Anti Money Laundering (AML) information, which was stored in systems separate from the insider threat group. In many cases, there was already a protocol in place to share information from fraud investigations with outside parties; therefore the fraud department found sharing information via the Insider Threat Group to be redundant. Therefore, the onus would have been on each pilot participant to create buy-in from each of their fraud teams around the need for a standardized, automated approach to share this information. Once automated, the benefits would have been creation of a capability to track sharing as well as ensuring sharing occurred whether or not relationships currently exist between financial institution fraud departments.

Pilot participants also noted internal policies and procedures that walled off their access to the data needed for collection. None of the pilot participants were using a common data lake model wherein various departments across the enterprise share sets of data for a

broad range of analytics. In some cases, this is due to regulatory requirements stipulating access to certain data sets must be auditable. In other instances, there were legal considerations, such as the use of human resource data, that is oftentimes necessary to adequately monitor employee behavior, but can be prohibited from sharing depending on where the data resides, such as in countries with stringent privacy restrictions. Collaboration across legal groups is necessary to find a common ground for setting rules for data sharing as well as better tagging of data classification to ensure restricted data is appropriately protected.

6.2. Cultural Constraints for Internally Sharing Data

During the data gathering phase of the pilot, without access to data from investigations across the fraud and cyber investigation teams, there was no seamless way to review cases and identify data against the indicators for each of the use cases. In addition, each of the cases needed to be reviewed manually, so without a dedicated resource from each of the participant organizations to support this effort, it was difficult to get a rich body of data to populate sample ITRs for each use case. While the participants felt they had proper support from their management to work on the project, the day to day demands on their time limited their ability to review the dense volume of case information for indicators to substantiate the identified use cases. Although it was demonstrated rules could be created for each use case to automate the identification of applicable data sets, each pilot organization had a different case management system for which extensive coordination was required to obtain approval by the case manager to implement an automated search of records. This challenge was deemed to be more of a cultural rather than a legal obstacle.

Each of the pilot participants were invited based upon a particular organizational profile to enhance the probability of success in collecting the data necessary for this pilot. The participants were global; had mature, dedicated insider threat groups; were headquartered in the U.S. in order to equalize any legal issues; and were SWIFT members with access to the SWIFT network. Each participant organization had a complex environment where multiple legacy systems had been merged. The merging of these systems created business practices which, over time, instilled cultural practices that now govern information sharing practices. These cultural practices oftentimes supersede legal and compliance requirements because traditional practices of information sharing are recorded in procedural manuals that are rarely challenged for their relevancy to the current threat environment. Upon reflection, the pilot participants agreed that outdated protocols within these procedures, if removed, would enable a level of communication between departments that could bridge critical information sharing silos.

6.3. Inconsistencies on Data Collection Between Institutions

The establishment of a dedicated insider threat program within financial institutions has been evolving over the last decade. As a result, institutions are at different stages of maturity when it comes to data collection on insider threat activity. Standards do exist for establishing programs; however they are not required. Recognizing the potential of insiders to harm national security, the U.S. Government has published a number of reports on optimizing insider threat program capabilities to better deter, detect and mitigate insider threats. Most recently the National Insider Threat Task Force under the Office of the Director of National Intelligence published a report in October 2018 on the "Insider Threat Program Maturity Framework."[5] This framework builds upon the basic requirements necessary to establish an insider threat programs, as mandated in Executive Order 13587, which was published October 7, 2011. There are 19 elements in the framework which address how to govern and staff the program, provide employee training and awareness, enable access to information, monitor user activity, and integrate information, perform analysis and improve response capabilities.

During the pilot it was discovered each participant organization had programs built upon similar elements of this framework. Specifically, under the umbrella of integration of information, analytics and response capabilities[6], all of the participants used advanced analytics to detect anomalous activity based on a composite of data inputs. In some cases, participants were also using risk scoring based on workplace factors and baseline activity to inform mitigation response plans. These response plans have been used selectively as inputs to exercises based on cyber events involving insiders. However, the extent by which insider activity can be monitored varied depending on technical capabilities. As a result, there was a variance among participant programs in the use of surveillance tools because of the uniqueness of each network. Therefore, developing universal use cases, ones that can be easily tracked by all institutions, was a challenge. This challenge will continue to impact the use of behavioral science methodologies to identify new patterns of activity to assign indicators to for the purpose of proactively identifying insider threats.

6.4. Technical Challenges

The Insider Threat Report used for the pilot was built in Microsoft Excel. This proved challenging because it required a manual process to input the data results. Furthermore, when the Excel template was emailed to the participants for use, participants were unable to activate the "Enable Content" option due to security controls each participant firm has in place to prevent users unintentionally enabling malicious macros. Without the macros, participants entered data in free form, which resulted in report submissions that were not

[5] Office of the Director of National Intelligence-National Insider Threat Task Force. "Insider Threat Program-Maturity Framework." Accessed November 20, 2018 from https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf
[6] Ibid.

standardized. Functionality was built into the Excel template to also enable data aggregation of the reports, but because the macros could not be used, it was not possible to use the aggregation function. If the aggregation of results had been automated, it may have been possible to establish basic patterns of behavior. It was recognized by the participants that the security protocols designed to protect their organization were equally preventing proactive activity to exchange information that could stop attack activity.

The latest industry trends indicate that insider attacks are supported by too many users with excessive access privileges and the availability of sensitive data on a multitude of devices. [7] This pilot aimed to, in this example, analyze how insider threat activity makes use of an excessive entitlement to transact with another financial institution. By sharing this information between institutions, it may have resulted in understanding how to close the gap on detection of fraud activity before it occurs. Similarly, the pilot sought to include information on what an institution uses to monitor specific insider threat activity that may have led to cyber fraud, such as Data Loss Prevention, encryption or identity and access management solutions, so each institution can assess how best to reinforce their defensive approach.

We conclude that had a tool that interfaces with case management software been available, it would have improved the reporting mechanism used for this pilot. Even the use of a simple tool, such as an Excel spreadsheet, came with security constraints which created significant obstacles to automating the aggregation of results. As organizations mature their insider threat programs, it will be critical to develop a capability to extract data from cases not only to model internal insider activity to learn what changes need to be made to enhance internal control effectiveness, but also to be able to share these models of behavior with other internal teams, such as the fraud and cyber investigative units. Learning from fraud and cyber investigations will enhance the insider threat models.

6.5. Lack of a Common Call to Action

As the response in the pilot survey indicated, only one of the organizations was willing to volunteer to expand the pilot despite the favorable responses indicating increased sharing of insider threat information is needed. Pilot participants reported a similar conflict in continuing to resource the pilot due to competing demands. It was particularly difficult to justify allocation of resources when some procedures do currently exist for communicating insider threat information between institutions, such as through email or a phone call. Given the current market climate, it was decided that without an event that has a systemic impact across the sector, investing resources to promote new information sharing exchanges could not be justified against a return on investment for each of the participating organizations.

[7] Cybersecurity Insiders. “Insider Threat 2018 Report.” Accessed December 1, 2018 from https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, pg. 4

The after action review of this pilot revealed that there was a critical need for a central sponsor in order to promote the sharing of data as a channel to enhance security. For example, if FS-ISAC or SWIFT was providing a central repository for data to be collated and analyzed, it may provide the needed incentive for organizations to dedicate resources to support data collection and aggregation. This type of central entity would provide the necessary environment for data analytics to be performed to produce behavioral models, which could lead to the development of new indicators to proactively identify cyber fraud activity. However, it was acknowledged a significant level of effort would be required to implement protocols for masking data shared with an independent entity as well as consideration of security implications of bringing so much information into one data lake.

7. Looking to the Future

As the observations from this pilot reveal, internal sharing is harder than peer-to-peer sharing. Short of a significant global event that would force change, the laws/rules/regulations that are currently in place prevent internal departments from sharing information from investigations in a common data lake where data analytic tools can be applied. For example, cross silo sharing exists between fraud and insider threat groups as well as human resource cases with corporate investigations; however this sharing is on a case by case basis and oftentimes lacks a defined process for routine sharing of information. This begs the question that if legislation can be enacted for organizations to enable the sharing of information externally with one another, is legislation needed to enable sharing *within* an organization? The results of this pilot point to a need for legislation that enables global organizations to overcome country legal constraints in order to effectively communicate within its ecosystem as it was designed to do. Within the U.S., this type of legislation was enacted when Anti Money Laundering terrorist financing laws were passed, designed to facilitate communication between financial institutions to thwart terrorist financing activity.

The pilot participants agree that this effort still has merit; however, it was noted that the internal silos that made this pilot a challenge would require a more coordinated internal effort in order to overcome. Since the data that is needed to effectively test the information sharing proposal needs to come from a variety of departments across an organization, any future work would require multiple representatives from each pilot organization. In addition, a full body of use cases would need to be developed in order to obtain the volume of data necessary to formulate any patterns of behavior. It is recommended that organizations progress on the development of these use cases internally by engaging multiple lines of business. This work would be similar to what financial institutions are currently required to do in formulating threat scenarios to adequately prepare for possible future losses. These insider threat use cases could then be tested to determine the critical inputs. Once identified, each department could then

develop their own internal process for contributing information, to include any necessary review and approvals.

Externally, more work can be done in the sector to create scenarios that test how the use of communication platforms, as described in this pilot, could mitigate the global impact of a significant event involving an insider threat. This could be included in a sector wide exercise, such as Quantum Dawn. Quantum Dawn is a series of cybersecurity exercises that enable financial institutions and the sector to practice and improve coordination with key industry and government partners to maintain equity market operations in the event of a systemic cyber-attack.[8] Given the number of participants in these exercises, a test of a peer-to-peer communications platform may provide the needed validation to resource automating the exchange of insider threat information.

[8] Securities Industry and Financial Markets Association. "Cybersecurity Exercise: Quantum Dawn IV." Accessed December 18, 2018 from https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-iv/

Appendix A

Rules for Identifying: External Financial Institution Data Posted on the Darkweb

Coding in SQL (preferred)

CASE WHEN (DATASOURCE.DarkwebFlag= TRUE AND DATASOURCE.FI Name <> 'Citi') THEN SENDMESSAGE ELSE NULL END

Darkweb Flag - This is a way to flag a darkwebsite prior to running above code. It is a pre-requisite and should be automatically scanning. The EXAMPLE A, B, C, references a hardcoded list of dark websites. If the user wants it to use additional criteria to determine if a site is a darkweb site – the user will need to develop that criteria and add it to the CASE WHEN statement.

Darkweb flag code: CASE WHEN (Datasource.WebsiteInfoFound = EXAMPLE A) THEN 'TRUE' WHEN (Datasource.WebsiteInfoFound = EXAMPLE B) THEN 'TRUE' WHEN (Datasource.WebsiteInfoFound = EXAMPLE C) THEN 'TRUE' WHEN (Datasource.WebsiteInfoFound = EXAMPLE D) THEN 'TRUE' ELSE 'FALSE' END

Darkweb flag code v2: WHEN ((OR (Datasource.WebsiteInfoFound IN ('Example A', 'Example B', 'Example C', 'Example D'))) THEN 'TRUE' ELSE 'FALSE' END

DATASOURCE – references where the data is actually being stored (website, data table, etc)

'Citi' – references "home" FI. Should be automatically pulled in from SWIFT license, identifier, etc.

Send Message – this is the command for an action if the prior criteria are met. If not, nothing will happen.

Coding in VBA (alterative)

```
Private Sub Worksheet_Change(ByVal Target As Range)
   If Target.Address(True, True) = External FI Data on Darkweb Target Cell Then
      Select Case Target
         Case "TRUE"
            Call SENDMESSAGE
         Case Else
            'Do nothing
      End Select
   End If
End Sub
```

External FI Data on Darkweb Target Cell Formula = Iferror(IF(AND(Match(Website info found, Reference of known darkweb sites, 0) >0, FI Target <> My FI) , "TRUE", "FALSE"), "FALSE")

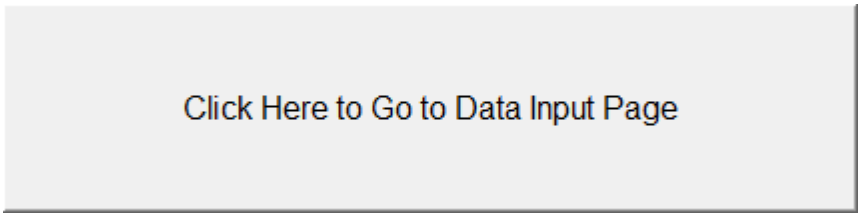
SENDMESSAGE – this "calls" the command for the action if the prior criteria are met. If not, nothing will happen.

MY FI - references "home" FI. Should be automatically pulled in from Swift license, identifier, etc.

Appendix B

Threat Information Exchange Template Final

Threat Information Exchange Template Instructions **The following information will assist with completing the threat information exchange template:**	
1	This template can only be completed with macros enabled. In order to enable macros - When the file is opened a pop up above the worksheet will say "Security Warning: Macros have been disabled". Please click "enable content".
2	Response data should be input into the Yellow Boxes.
3	Responses are either free form (submitter information, victim firm information, additional comments) or drop downs (all other questions). Drop down selections are limited and free text will cause an error message to appear and will not populate the answer box.
4	When you have filled out all yellow boxes, hit the "Submit Data" button. This will archive the information you have provided in an additional sheet for later consolidation.
5	Once the "Submit Data" button is clicked, the data is archived and information is cleared from the input tab. The next example can then be entered into the input tab.
6	Any questions left blank will be marked as "no response" in the data archive.
7	Once all examples have been input and archived, save the file as "Threat Information Exchange Template (Company Name)" with the company that is submitting substituting company name.



Threat Information Exchange Template	
Submitter Information	**Answers**
Business Name	
Address	
City	
State	
Zip Code	
Scenario Analysis	**Answers**
Which Scenario does this most resemble?	
Customer Information and Account Questions	**Answers**
Does the customer have a visa?	
Has there been unusual activity on the customer account?	
Was the activity structured to skirt bank reporting requirements? (ie under wire limits)	
Employee Action Questions	**Answers**
Were alerts disabled for this account?	
Was the employee recently separated from the firm?	
Did the employee send encrypted files outside of the Internal Network?	
Was customer account information changed?	
Victim Information	**Answers**
Which is the victim firm?	
Additional Comments	**Answers**
Please describe any additional information about the threat:	

Submit Data