sibos TORONTO 16 - 19 Oct 2017

SWIFT INSTITUTE

Sharing Insider Threat Indicators: Examining the Potential Use of SWIFT's Messaging Platform to Combat Cyber Fraud

sibos TORONTO
16 - 19 Oct 2017

SWIFT INSTITUTE

Elizabeth Petrie

Director Cyber Threat Risk Management
Citi

Casey Evans

Executive in Residence, Accounting
American University's Kogod School of Business

Presentation Overview

- Problem Statement
- Research Goals & Methodology
- Defining Insider Cashout Indicators
- Threat Indicator Sharing Tool
- Legal and Privacy Implications
- Future of Threat Information Sharing
- Q&A

Business Impact of Cyber Threats

Systemic Loss of Confidence in Business Functions

01 **LOSS OF DATA**

02 **LOSS OF FUNDS**

03 **COMPROMISE**

By the Numbers

73%

of observed attacks in 2016 were Financially Motivated

$800 billion

Value of intellectual property theft – February 2017

$2.1 trillion

Global cost of cybercrime by 2019

Verizon Data Breach Report 2017 - https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf
**Forbes, "*Cyber Crime Costs Projected To Reach $2 Trillion by 2019", January 2017
The National Bureau of Asian Research, "The Commission on the Theft of American Intellectual Property" , February 2017

Shift to the Financially-Motivated APT Actor

GOALS

- Intelligence Collection
- Destructive or Disruptive Attacks
- Financially Motivated

TACTICS, TECHNIQUES, PROCEDURES

- Multiple vectors-leverages significant resources
- Maintains access and adapts to resistance
- Erases tools; wipes tracks

Information Sharing-A National Security Issue

Failures of 9/11

- Poor information systems prevented recall of bad intelligence
- The community was not networked to receive early warnings, which would have enabled corroboration of reporting
- Legal and policy barriers

Not a Competitive Advantage-Critical Infrastructure

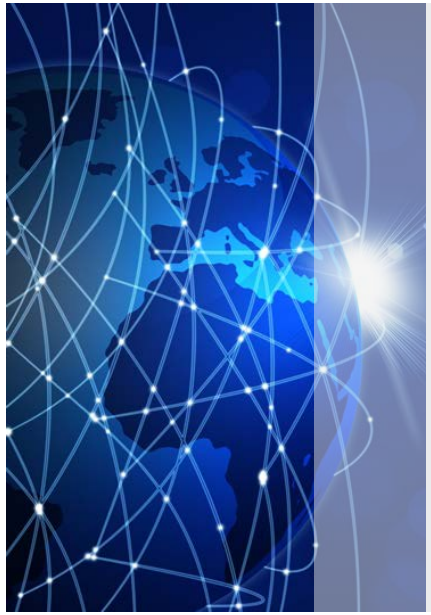
- Historically no incentive to share
- Exposure of vulnerabilities
- Loss of customer confidence

Operational Losses

- Operational and financial interconnectedness-a cyber incident or failure at one interconnected entity may also impact the safety and soundness of other financial entities with potentially systemic consequences
- Exceeding tolerance levels

Present Day Information Sharing

Looking Forward-The WMD Commission Final Report



- Centralized management of intelligence information
- Processes for sharing intelligence information governed by risk management principles that balance protection of the source of information with sharing
- Expansion of the information sharing environment
- Breakdown of technical barriers to information sharing by implementing uniform standards
- New culture to share as a rule, withhold by exception

Information Sharing and Analysis Centers

- Financial Services (FS-ISAC)
- Financial Systemic Analysis & Resilience Center (FSARC)
- National Cyber-Forensics & Training Alliance (NCFTA)

U.S. Industry Threat Information Sharing Tools

Financial Crimes Enforcement Network (FinCEN) Suspicious Activity Reports

1. Bank Secrecy Act requires financial institutions in the U.S. to assist U.S. government agencies to detect and prevent money laundering
2. Suspicious activity reporting is a cornerstone to combating financial crimes, terrorism financing, money laundering and now-cyber enabled crime and cyber events
3. Includes cyber related information to describe technical details of electronic activity
4. Electronic filing through Bank Secrecy Act E-Filing system

Intelligence Information Reports

1. Intelligence reporting vehicle to disseminate raw intelligence
2. Driven by collection requirements, which may or may not be levied by the collecting agency
3. Shared reporting within the organization, between intelligence agencies and law enforcement communities
4. Teletype to IIR Dissemination System

Research Goals

- **To leverage existing telecommunications platforms** to communicate cyber fraud threat information by establishing indicators of insider cashout behavior, which could warn of cyber fraud activity.

- **Insider cashout** is part of broader cyber or fraud rings. A ring is defined as two or more people colluding to conduct illicit activity. Based on this assumption, by reporting insider activity to other financial institutions, the identification of a ring may be possible before significant losses are suffered due to cyber fraud schemes.

  - To further narrow the definition of insider cashout activity, insider activity must involve **abuse of trusted access to compromise the confidentiality, integrity or availability** of an organization’s data or its systems.

Polling Question #1

Do you see a need for ***more*** information sharing on cyber fraud?

a) Yes

b) No

Research Methodology

- Identification of insider behavior indicative of theft of PII, trade secrets and/or cashout activity (54 indicators of insider behavior identified)

- Identification of the source of the identified indicators such as network access data, customer account activity, email, human resource records, phone records, and internet browser history

- Developed the Insider Threat Report to communicate insider threat behavior:
  - Reporting Bank
  - Insider Threat Activity
    - Type of threat
    - Threat action (54 indicators were culled down to the 10 most common)
    - Financial and non-financial impact of the threat
    - Actions taken to remediate or contain the threat
  - Designated point of contact for the case and date filed

- Worked with SWIFT to convert the Insider Threat Report into the MT 998 and XML format

Indicators of Insider Cashout Activity

Insider Indicators of Cyber Fraud

- **Examples of Theft of PII**
  - Unnecessarily accesses and copies customer materials
  - Emailing customer files to personal or web-based email
- **Examples of Theft of Trade Secrets**
  - Employee staying at the office after hours and accessing sensitive data following termination notice
  - Laptop that has been wiped when returned after termination

Insider Cashout Indicators

- **Examples of Money Laundering**
  - Offering to aid placement of illicit funds on the dark web in exchange for payment
  - Access to dormant accounts followed by sudden activity in the dormant accounts
  - Regularly changing customer attributes (i.e. address)

Polling Question #2

Is sharing insider threat behavior feasible?

a) Yes

b) No

DRAFT: Insider Threat Report

Reporting Bank

Legal name of business

Address

City | State | Zip Code

Insider Threat Activity

Threat (select all that apply)

- ☐ Theft of PII
- ☐ Theft of Trade Secrets
- ☐ Cashout Activity

Threat Action (check all that apply)

- ☐ Accessed sensitive data after termination notice
- ☐ Conducts unauthorized searches
- ☐ Short trips to foreign countries for unexplained reasons
- ☐ Calls with known high-risk personnel or external parties
- ☐ Interest in matters outside the scope of their duties.
- ☐ Unexplained affluence
- ☐ Complaints of hostile, unethical or illegal behaviors
- ☐ Remotely accesses the computer network at odd times
- ☐ Working odd hours without authorization
- ☐ Network access data: web browsing history, network crawling, data hoarding, copying from internal repositories

Severity of Threat

Date or date range of threat ____ to ____

Account used/compromised

- ☐ Corporate
- ☐ Individual
- ☐ Not applicable

DRAFT: Insider Threat Report (continued)

What instruments were used to facilitate the threat? (check all that apply)

☐ Not applicable	☐ Structuring	☐ Credit/debit cards
☐ Wire transfers	☐ Shell companies	☐ Stored value cards
☐ Trade instruments	☐ Bonds/notes/stocks	☐ Digital currency
☐ Correspondent accounts	☐ Money orders	☐ Other: (describe below)

	YES	NO
Is there any potential or actual financial loss associated with the incident?	☐	☐
If yes, what is the amount? $ 1.00		
Were other financial institutions affected by the threat?		
If yes, which one?		
Is the incident likely to result in notification to a regulator?	☐	☐
Has any action taken place to remediate or contain the incident?	☐	☐
If yes, please describe:	☐	☐

Contact for Assistance

Designated point of contact (Investigator's First Name, Last Name)

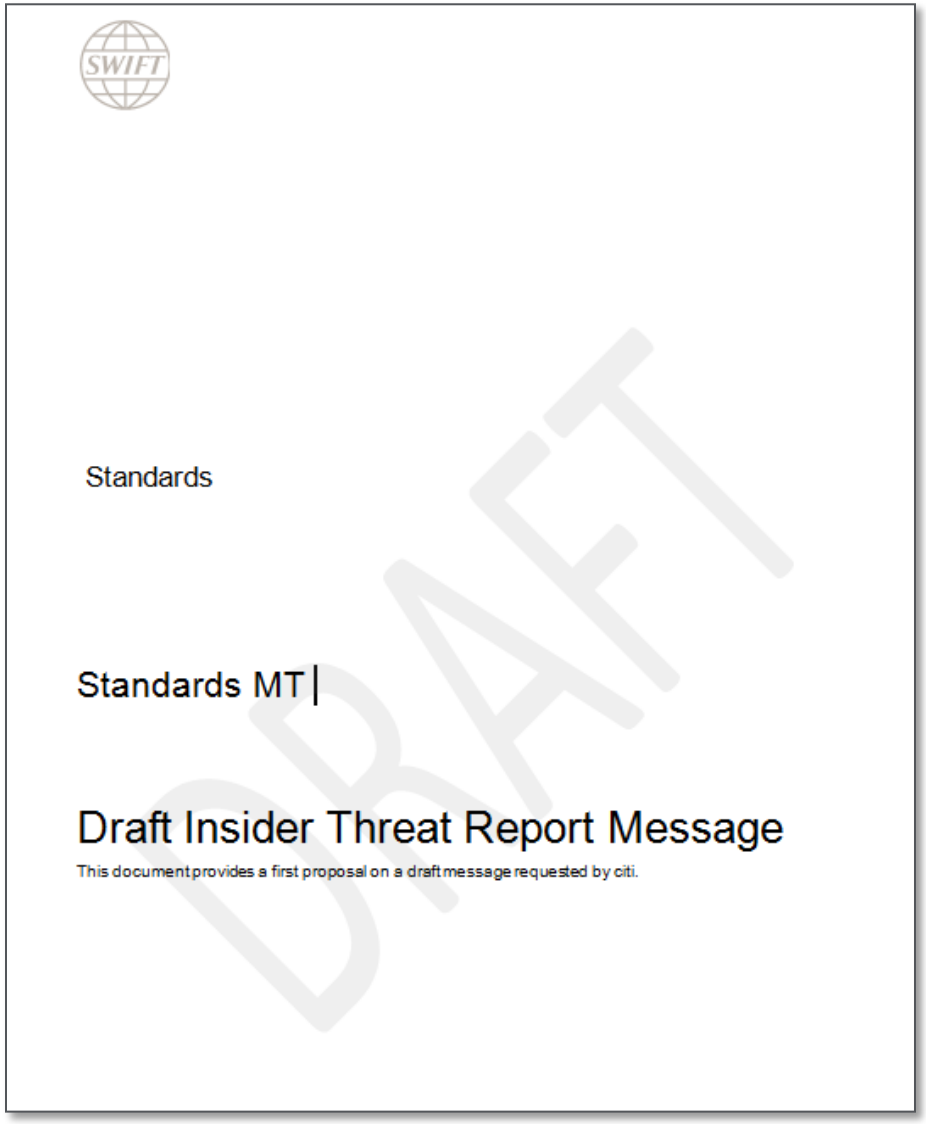
Designated phone number

Designated email address

Date Filed

Draft Insider Threat Report Message

This document provides a first proposal on a draft message.



Draft Insider Threat Report Message (continued)

1 MT 998 Insider Threat Report

1.1 Scope

The Insider Threat Report message is the message a financial institution (branch/department) sends to either another branch/department of the same financial institution or to another financial institution reporting on information about a threat identified in the banking industry. It includes the details of the threat, the action(s) linked to it, the severity and assistance details from the reporting bank that is sending the Insider Threat Report.

1.2 Format Specifications

The MT 998 consists of two sequences:

- Sequence A Threat Activity is a single occurrence mandatory sequence and contains information linked to the threat identified
- Sequence B Assistance Details is a repetitive mandatory sequence and contains information of one or more contact person(s) that can be contacted regarding the Threat Activity described in Sequence A.

Status	Tag	Field Name	Content/ Options	No.
M	20	Transaction Reference Number	16x	UHB
M	12	Sub-Message Type	3!n (= 999)	UHB
M	77E	Proprietary Message	73x [n*78x]	UHB
Fields within field tag 77E:				
Mandatory Sequence A Insider Threat Activity				
----->				
M	23H	Category	4!c	1
-----|				
----->				
M	24H	Action	4!c	2
-----|				
Mandatory SubSequence A1 Severity				
M	30B	Date Range	6!n[/6!n]	3
----->				

Draft Insider Threat Report Message (continued)

DEFINITION

This field contains the category code to indicate the kind of threat reported.

CODES

One of the following codes must be used:

TPII	Theft of PII	The threat is the theft of Personally Identifiable Information
TTRS	Theft of Trade Secrets	The threat is the theft of Trade Secrets
CAOA	Cashout Activity	The threat is cashout Activity

EXAMPLE

:23H:TTRS

2. Field 24H: Action

FORMAT

Option H 4!c (Code)

PRESENCE

Mandatory and repetitive in mandatory sequence A

DEFINITION

This field identifies the type action involved in the threat.

CODES

One of the following codes must be used:

SENS	Sensitive Data	The threat action is accessing sensitive data after termination notice.
CALL	Calls	The threat action are calls with known high-risk (personnel or external parties).
BHVR	Behavior complaints	The threat action are complaints of hostile, unethical or illegal behaviors.
SENS	Sensitive Data	The threat action is accessing sensitive data after termination notice.
NDAA	Network Data Access	The threat action is access to network data: web browsing history, network crawling, data hoarding, copying from internal repositories.
SRCH	Searches	The threat action is conducting unauthorized searches.
OOSI	Out of Scope Interest	The threat action is interest in matters outside the scope of their duties.
REMA	Remote Access	The threat action is remotely accessing the computer network at odd times.
UFCT	Unexplained Foreign Country Trips	The threat action are short trips to foreign countries for unexplained reasons.
UAWH	Unauthorized Working Hours	The threat action are odd working hours

Camt.998.999.01 Example

Camt.998.999.01 example

```
<InsdrThtRptMsg>
    <MsgId>
        <Ref>THREATREPORT170328</Ref>
    </MsgId>
    <PrtryData>
        <Sb-MT>999</Sb-MT>
        <PrtryMsg>
            <GrpHdr>
                <CreDtTm>2017-03-28T10:26:10</CreDtTm>
                <InstgAgt>
                    <FinInstnId>
                        <BICFI>BANKUS33BOS</BICFI>
                    </FinInstnId>
                </InstgAgt>
                <InstdAgt>
                    <FinInstnId>
                        <BICFI>BANKUS33CAL</BICFI>
                    </FinInstnId>
                </InstdAgt>
            </GrpHdr>
            <InsdrThrtActvty>
                <Ctgy>CAOA</Ctgy>
                <Actn>CALL</Actn>
                <Actn>OOSI</Actn>
                <Svrty>
                    <DtRg>
                        <FrDt>2017-01-01</FrDt>
                        <ToDt>2017-03-27</ToDt>
                    </DtRg>
                    <AcctTp>INDV</AcctTp>
                    <Instrms>
                        <InstrmCd>WITR</InstrmCd>
                    </Instrms>
```

Camt.998.999.01 Example (continued)

```
                                        <Instrms>
                                                <InstrmCd>MNOR</InstrmCd>
                                        </Instrms>
                                        <Instrms>
                                                <InstrmCd>CDCA</InstrmCd>
                                        </Instrms>
                                </Svrty>
                                <FinLossInd>true</FinLossInd>
                                <Amt Ccy="USD">5000</Amt>
                                <RgltnNtfctnInd>false</RgltnNtfctnInd>
                                <IncdntRmdlAndOrCrrctvActns>Employeedismissed</IncdntRmdlAndOrCrrctvActns>
                        </InsdrThrtActvty>
                        <AssstncDtls>
                                <Invstgtr>
                                        <Nm>Emma Jackson</Nm>
                                        <PstlAdr>
                                                <TwnNm>Boston</TwnNm>
                                                <Ctry>US</Ctry>
                                        </PstlAdr>
                                        <CtctDtls>
                                        <EmailAdr>Emma.Jackson@aol.com</EmailAdr>
                                        </CtctDtls>
                                </Invstgtr>
                                <Dt>2017-03-27</Dt>
                        </AssstncDtls>
                </PrtryMsg>
        </PrtryData>
</InsdrThtRptMsg>
```

Legal and Privacy Considerations

Legal

- Restrictions on Employee Monitoring (e.g., ECPA, CFAA, state laws)
- Employment discrimination (e.g., FCRA, EEOC, protected classes)
- Protection of personal and proprietary information (e.g., GLBA, FTC)
- Anti-trust and anticompetitive prohibitions
- Potential liability protection for cyber threat indicator sharing (CISA)

Privacy

- Notice and consent to monitoring, collection, use, sharing of personal information
- Purpose Specification
- Right of Access and Correction
- Collection and Access Limitation
- Data Quality
- Security
- Retention Limitation

Polling Question #3

What are the biggest challenges you see to sharing information using this method?

a) Implementation

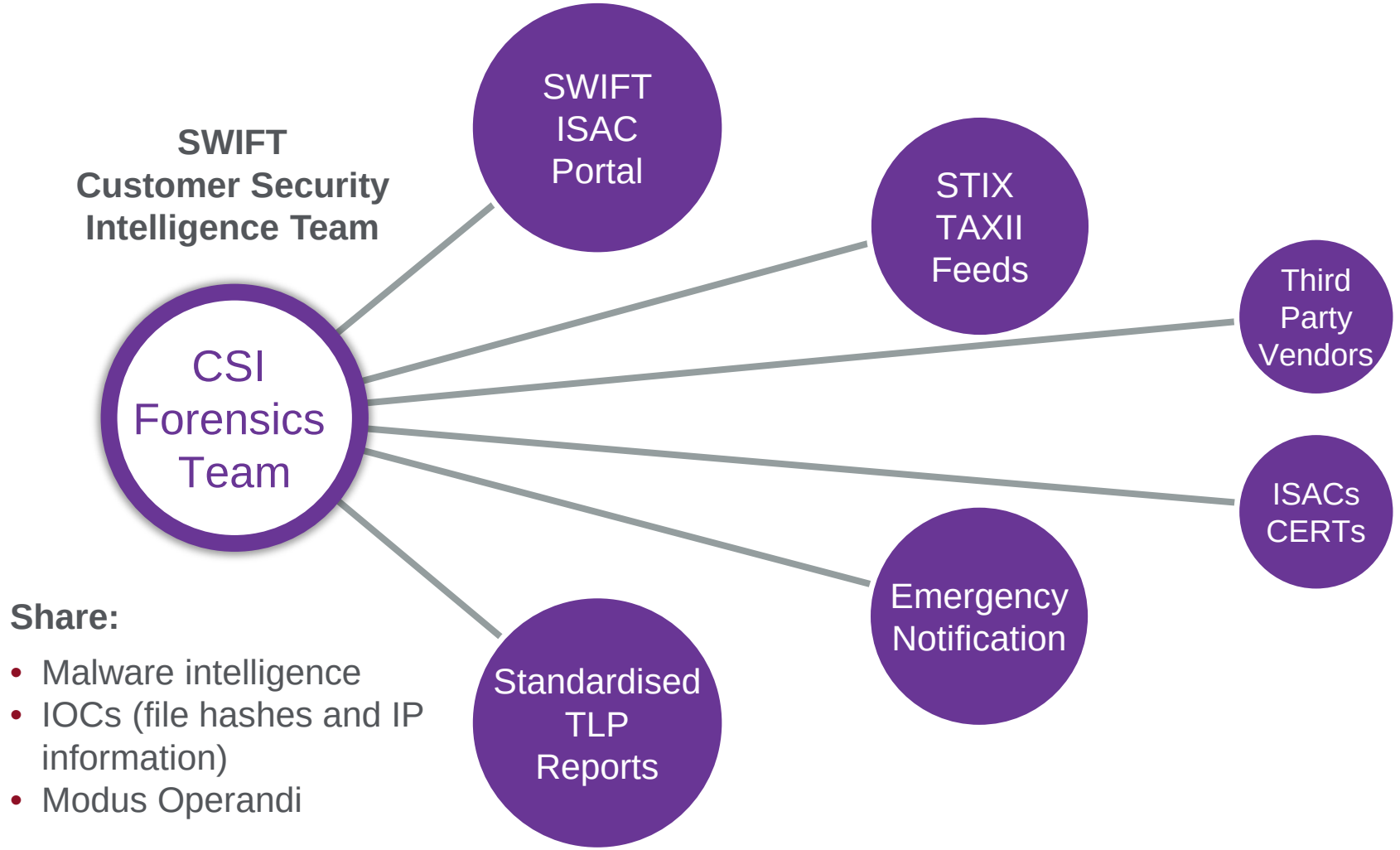
b) Privacy Concerns

c) Liability Issues

d) False Positives

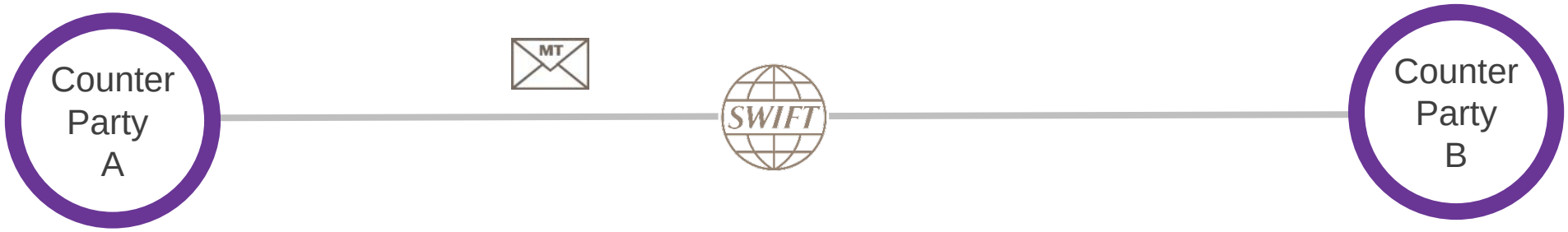
Possible Future of Threat Information Sharing

Sharing Malware Threat Information – *SWIFT ISAC*



Possible Future of Threat Information Sharing

Sharing Insider Threat Information



MT 999 Message Type

- Free-format message that is designed to flow over SWIFT network
- Payment derivation MT 199
- 2KB size, no attachments
- Widely used by customers

Possible Implementation Steps

- Either create a new, dedicated message type. Raising a standards CR with associated community consultation could take 2-3 years
- Or use the MT 998 with a pre-defined message structure, and market practice to guide usage with a closed community of interested customers. Could be done in a few months

Next Steps

- Validation of all insider threat indicators presented in the research findings.
- A sub-set of indicators would then be identified for use in a pilot based on capabilities to collect activity related to those indicators using existing tools.
- Finalize the message format for the ITR and begin exchanging the messages in a Closed User Group on the SWIFT platform.
- Develop procedures for writing and disseminating the ITR.
  - SWIFT would evaluate what standards would be required in order to implement an ITR message type and whether there is a broader community appetite for using such a mechanism for information sharing.

Questions

sibos TORONTO 16 - 19 Oct 2017

SWIFT INSTITUTE

Research paper can be downloaded from:

www.swiftinstitute.org