Export Trading Group (ETG) June 2019

ACT MIDDLE EAST BREAKFAST BRIEFING:

Liquidity Performance & Payment Fraud

19 June 2019 | Dubai | 08:00 - 11:00

09:50 Case study 2: Treasury as the function to detect and prevent payment fraud

Featured speaker: Anish Jain
Chief Treasury Officer,
Export Trading Group

ETG Group Overview

Operations across 45 countries on 5 continents, with 150+ entities in these countries.

Importing and exporting soft commodities form 26 African countries

Dealing with 70+ global and local banks in Africa and ROW. 20+ currencies dealt with,700+ account globally

1000+ customers around the world incl. farmers, government, institutional buyers, retailers, wholesalers & independent suppliers

Importing and exporting soft commodities form 26 African countries

ETG

Cyber Crime and Cyber Fraud

As custodians of an organization's cash, treasurers have a key role to play in the fight against cybercrime. By being strategic about this issue, treasurers can go a long way to mitigating the threat

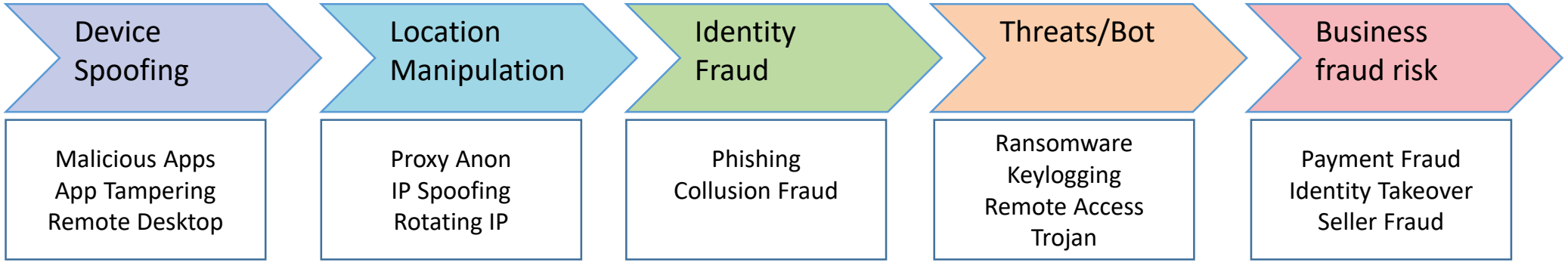
- Cybercrime and the cyber fraud landscape are constantly shifting with an ever-growing range of attack mechanisms and increasingly sophisticated tools. Two attack vectors in particular stand out:
  - the use of ransomware
  - treasury fraud
- Cybercrime and cyber fraud in the news

ETG

Cyber Crime and Cyber Fraud

- Treasurers have an ultimate responsibility for many of the areas most commonly targeted by cybercriminals, including cash balances, global bank connectivity, high-value payments processing, and maintenance of repetitive payment instructions.
  - Based on the Marsh/Microsoft Global Cyber Risk Perception Survey, 70% of organizations have not developed a cyber incident response plan, and 43% of organizations do not have board-level responsibility for the review and management of cyber-risk.

Evolving attack vectors



ETG

Cyber Crime-Data

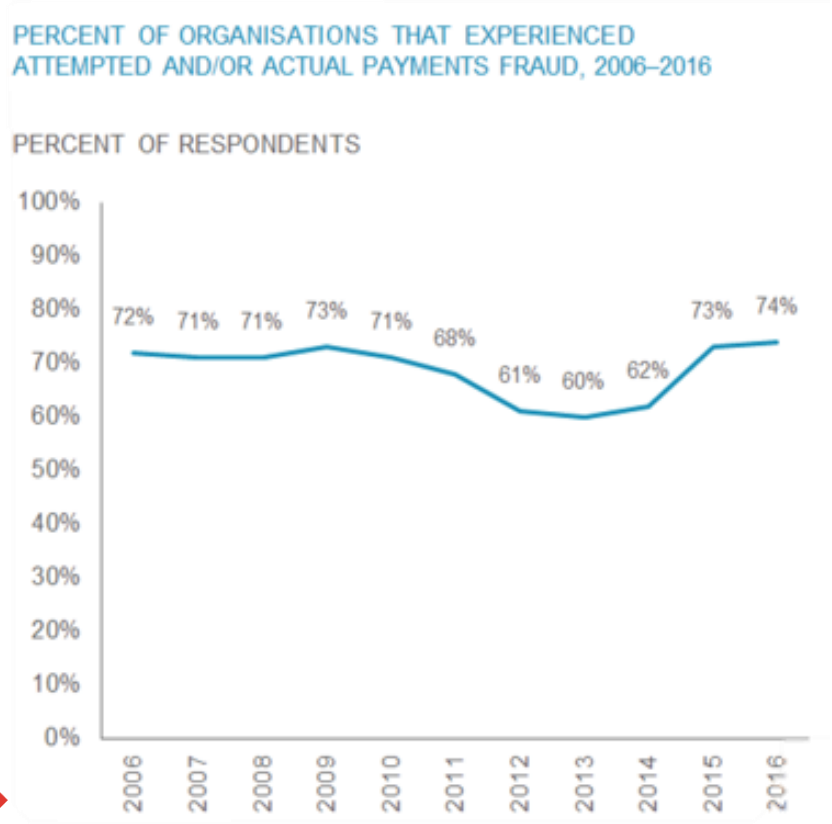
A survey conducted by the AFP shows that 78 % of companies were targets of payments fraud last year demonstrating the crucial need for cybersecurity protocols and strict control governance. Additionally, the survey reveals that in 2017:

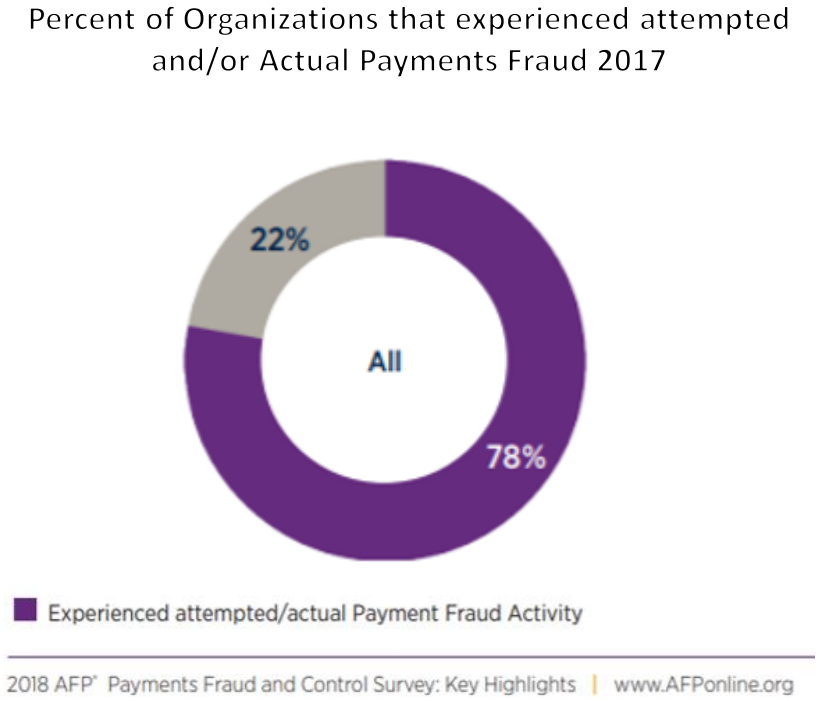
- 77 % of organizations experienced Business Email Compromise (BEC)
- 54 % of BEC scams targeted wires, followed by checks at 34 %
- 77 % of organizations implemented controls to prevent BEC scams
- 74 % of organizations experienced check fraud, a slight decrease from 2016
- 28 % were subject to ACH debit fraud and 13 % were subject to ACH credit fraud
- 67 % of payments fraud was discovered by the organization's treasury staff

ETG

Cyber Fraud Data

- The percentage of organizations that experienced attempted and/or actual payment fraud, 2006-2016 – payment fraud is INCREASING





ETG

CYBER LOSS SCENARIOS

1 Business working with a foreign supplier	A business that typically has longstanding relationships with suppliers where an invoice payment is received to remit funds to a fraudulent account.
2 Business executive receiving or initiating a request for a wire transfer	A request for a wire transfer from an employees compromised account is sent to a second employee within the company who is typically responsible for processing payments
3 Business contacts receiving fraudulent correspondence through compromised e-mail	Request for invoices to be paid to fraudulent accounts emails are sent from a hacked employees account to multiple vendors.
4 Business executive and attorney impersonation	Victims may be pressured by fraudsters identifying themselves as lawyers to act quickly in handling transfer of funds.

ETG

CASE STUDY – PAYMENT FRAUD

Fraud Scenario

- Email received from a senior colleague close to cut off to change account no to remit funds to an unregistered account as the rates negotiated with said bank is more favorable and the same needs to be executed on and urgent basis so as to take advantage of the situation

Risk Factor

- Unusual behavior to change accounts close to cut off
- Remitting funds to account which is not registered with Treasury team

Controls/Precautions taken

- Fraudulent e-mail detection to indicate mails initiated from out of organization
- Educate staff that no payments to be made to unlisted accounts
- Call back confirmation to check and see if the following account is correct and obtain other details

ETG

Leveraging Technology

Enterprises can leverage technology to sustain a risk-based approach to cyber-risk management. This requires technology that enables organizations to monitor complex and large volumes of data and run advanced data crunching analytics to identify potential vulnerabilities, incidents, and their impact. Firms should seek dedicated expert partners with advanced technical capabilities to assist with the role out and implementation.

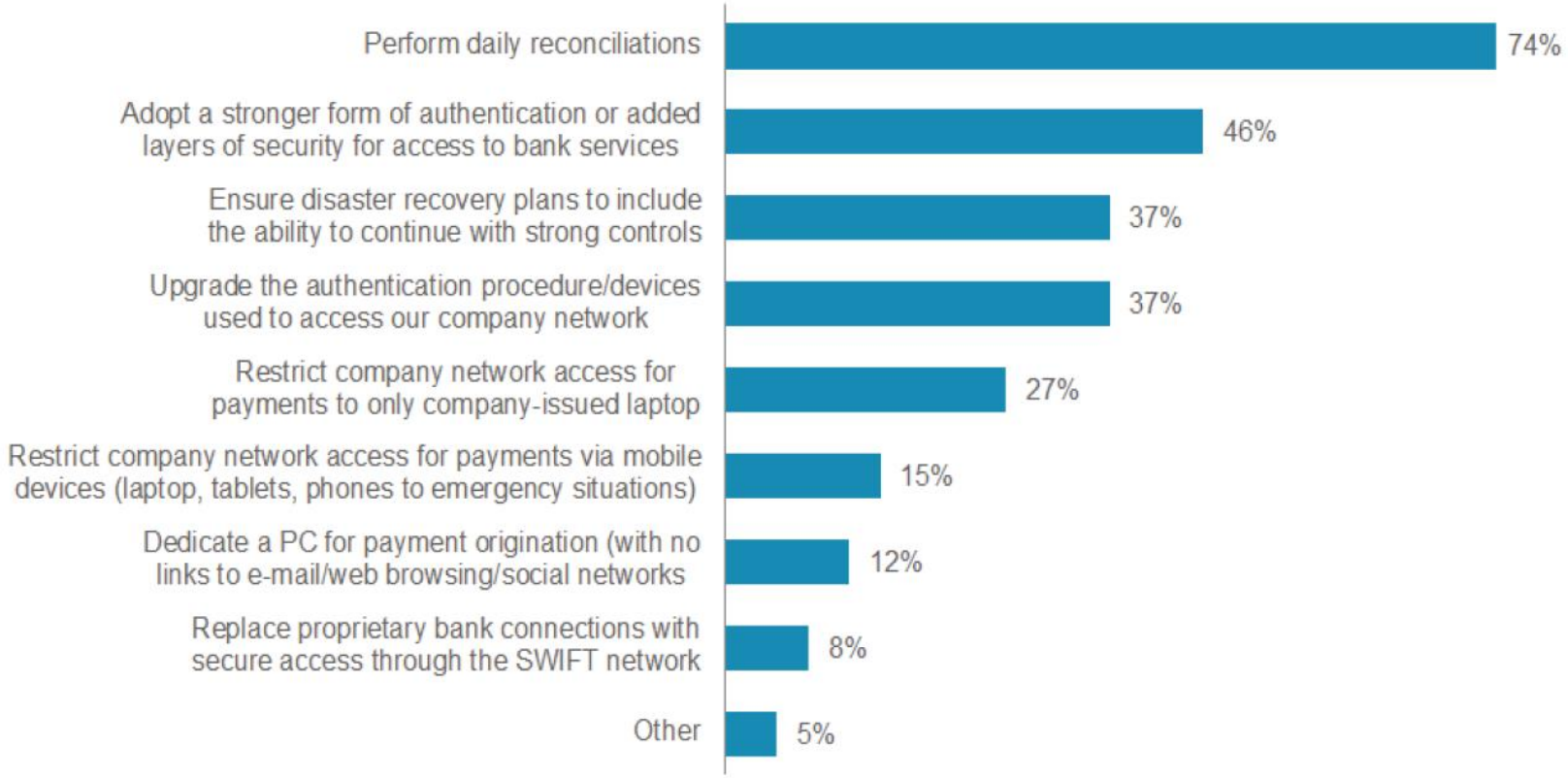
Kyriba's Payment Fraud Detection

- Has the capability of setting pre-defined rules to screen for suspicious payments – create scenario based determinations to stop or flag payments
- The ability to create workflows allow for segregation of duties – allow non-treasury personnel to over view payments
- Audit trail – to be provided for internal audit review

ETG

Best Practice

ACTIONS TAKEN TO DEFEND AGAINST ATTACKS THAT WOULD COMPROMISE SECURITY



Source: 2017 AFP Payments Fraud and Control Survey.

ETG

Confidentiality & Disclaimer

IMPORTANT NOTICE

- The information contained in this presentation is strictly confidential for Export Trading Group (the "Company"), and is provided by the Company to you solely for your reference because you are one of the esteemed bank in our portfolio. Any reproduction, dissemination or onward transmission of this presentation or the information contained herein is strictly prohibited. By accepting delivery of this presentation you acknowledge and agree to comply with the foregoing restrictions.

- The information contained in this presentation is subject to change without notice, its accuracy is not guaranteed and it may not contain all material information concerning the Company. Neither the Company nor its Management makes any representation regarding, or assumes any responsibility or liability for, the accuracy or completeness of, or any errors in or omissions from, any information contained herein.

- In addition, this presentation includes projections and forward-looking statements that reflect the Company's current views with respect to future events and financial performance. These views are based on assumptions and are subject to various risks. Such forward-looking statements are not guarantees of future performance and no assurance can be given that any future events will occur, that projections will be achieved or that the Company's assumptions will prove to be correct. Actual results may differ materially from those projected and the Company does not undertake to revise any such forward-looking statements to reflect future events or circumstances.

- This presentation does not constitute or form part of any offer for sale or subscription of or solicitation or invitation of any offer to buy or subscribe for any securities, stocks, equity including in the subordinates interests, nor shall it or any part of it form the basis of or be relied on in connection with any contract or commitment whatsoever.

ETG