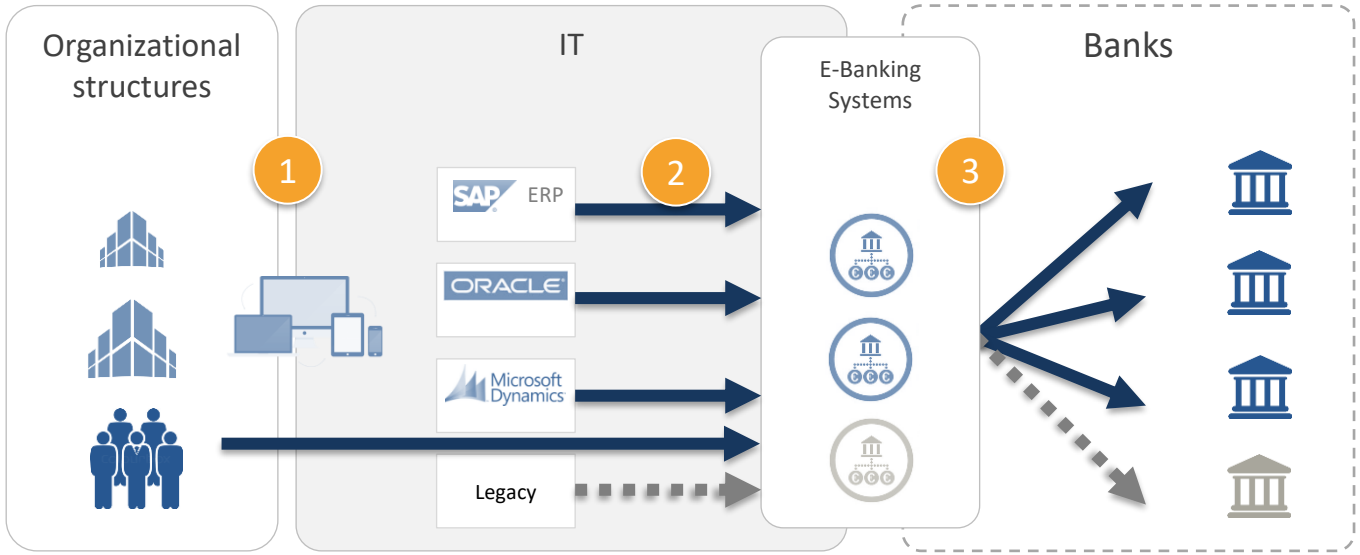
JOURNEY TOWARDS BETTER PROTECTION AGAINST PAYMENTS FRAUD

YOUR WORLD OF PAYMENTS. ONE LOGIN.
Leading cloud platform for managing corporate payments and cash flows

INTRODUCTION

Erol Bozak
CPO & Co-Founder
Treasury Intelligence Solutions

WEAK POINTS AND RISKS

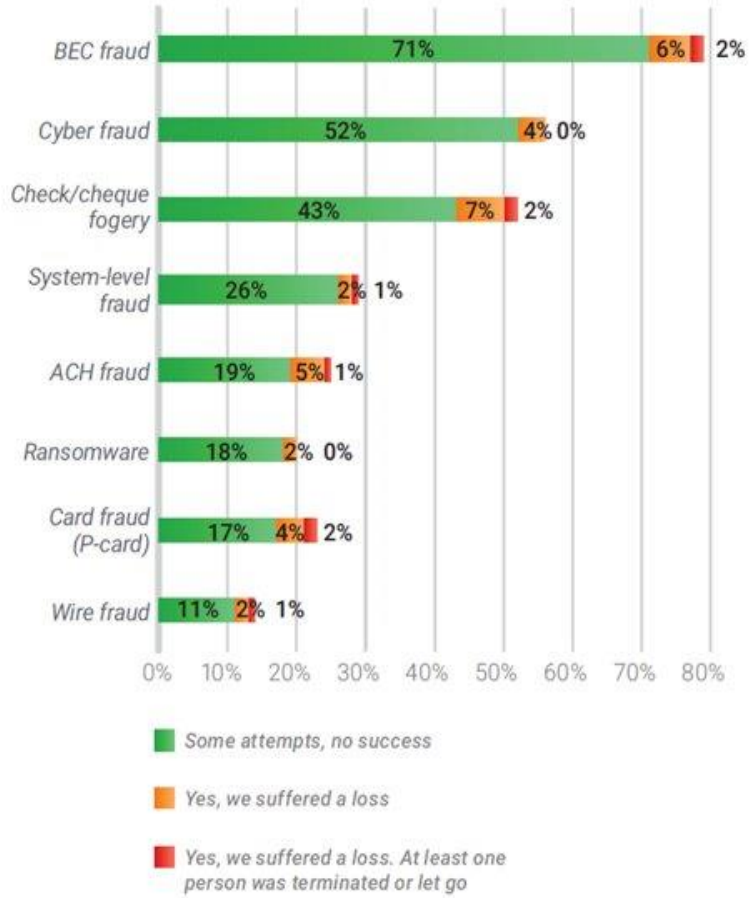


1. Complex organization, lack of processes, non-educated employees, devices are not secured properly
2. Missing integration, no STP (straight-through processing)
3. Manifold interfaces and formats as well as heterogenious security measures

- Like in other IT systems which contain economic processes there are different risks and weak points. In payments, those risks directly lead to financial loss.
- Attackers usually use several weak points
- The highest risk factor is the human being.

SOME STATISTICS

Corporates: Thinking of the last 12 months, please label your company's experience with each of the following:



Tips to Prevent:

BEC Fraud

1. Use multi-factor authentication on all email/messaging systems
2. Train employees on how to identify and respond to suspicious emails or requests

Cyber/Data Theft

1. Encrypt data, both at rest and in transit
2. Install & maintain updated antivirus & firewall software

Check Forgery

1. Stop using checks, convert to e-pay methods
2. Adopt Positive Pay
3. Reconcile bank accounts daily

Source: [2019 Treasury Fraud & Controls Survey Report, Strategic Treasurer]

PREVENTION VERSUS DETECTION

Fraud prevention is a corset which aims at standardizing behavioral processes by applying controls

Prevention by risk reduction and control of attack vectors

Detection by learning and identifying unusual behavior

PREVENTION MECHANISMS

- Workflow / process (e.g. 4-eye-principle, different approval processes)
- Secure ways of authentication
- Centralization and STP

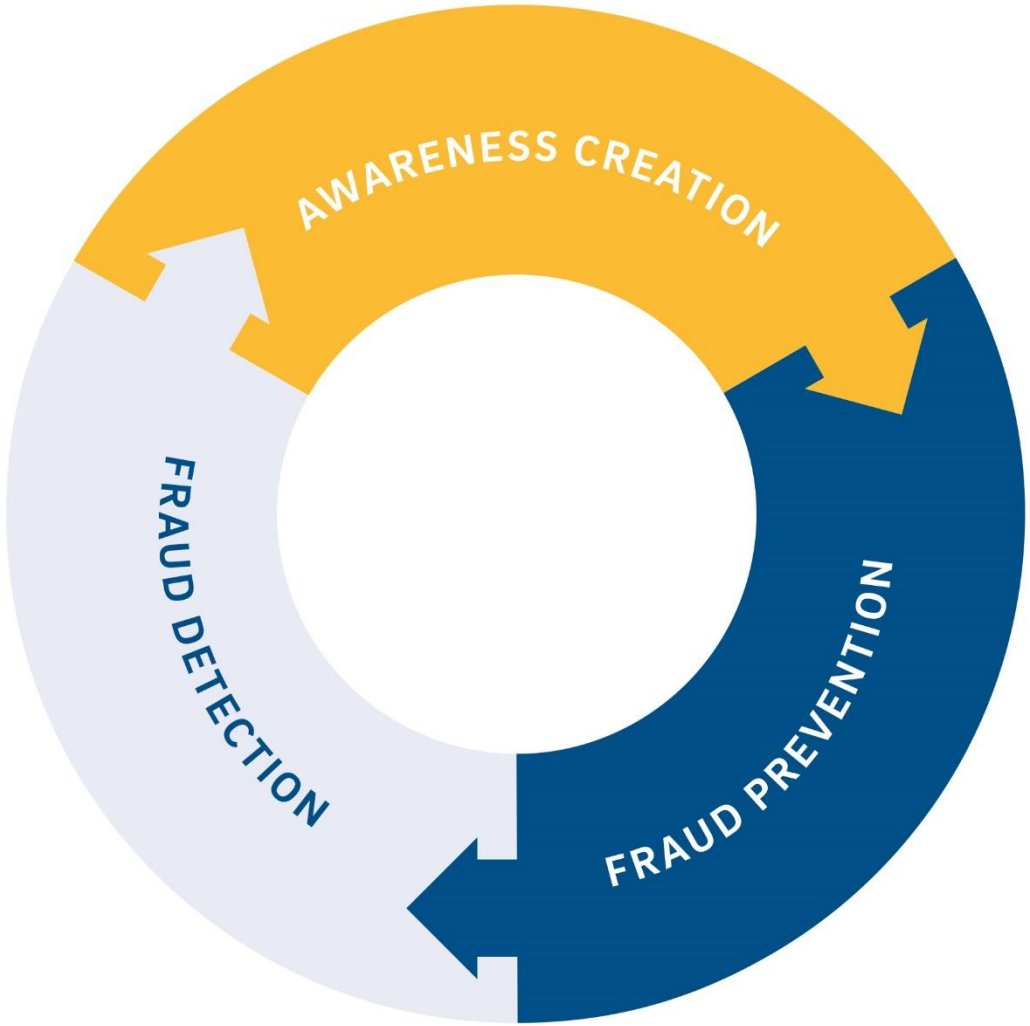
DETECTION

- Machine learning/ AI

PREVENTION MECHANISMS

- White / black lists
- Pre-approved payment templates for manual payments
- and much more

A POSITIVE CYCLE FOR PAYMENT SECURITY



STEP 1: SECURITY STARTS WITH PEOPLE

- An important step to tackle fraud is to make sure that your staff is aware of the common tactics developed by fraudsters.
- Guidelines need to be in place, so everyone knows how to act and who to contact
- Regular trainings for all team members to tackle the ever-changing TTPs (tactics, techniques and procedures) of fraudsters
- IMPORTANT! Fraud does not always come from an external source
- Since measures against fraud can be restrictive or require changes in the ways of working people are used to, it is important to create awareness across the organization so that everyone is on the same page

STEP 2: ENSURING AN EFFECTIVE DEFENSE

IDENTIFYING WEAK POINTS

- Complex organizational structure, usually decentralized
- Lack of standardized processes, usually with multiple people involved
- No integration of ERP systems or other backend systems
- No straight-through-processing for data integrity
- Multiple E-banking systems causing lack of transparency
- Different types of payment methods
- End devices for doing payments not properly secured
- No consistent security strategy or execution

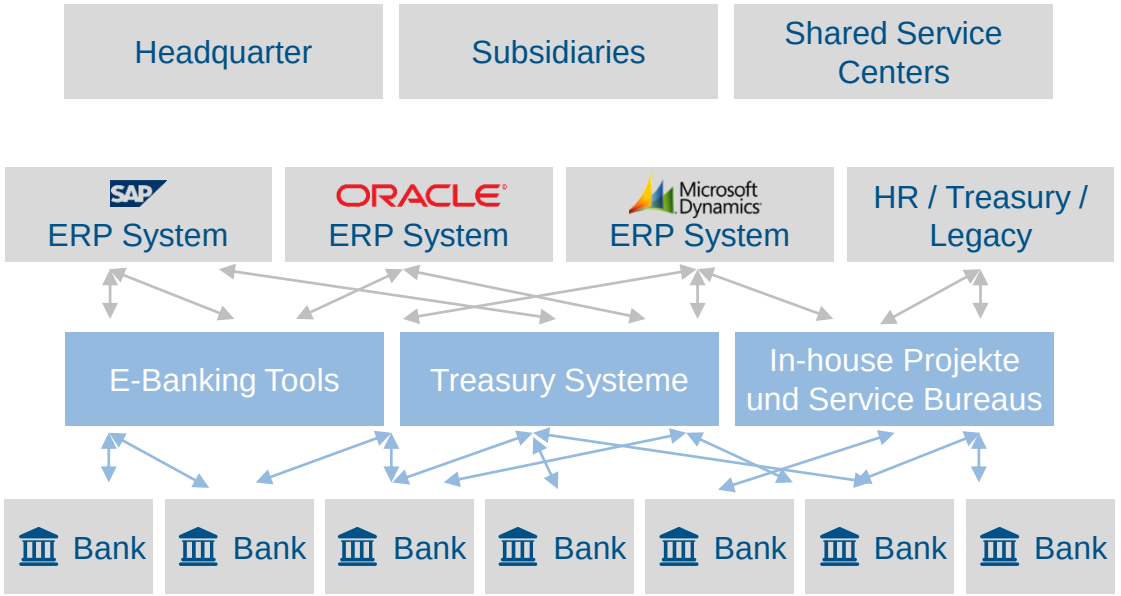
If one or more of the above are present in your current payment processes, it is a good time to revisit your setup and make necessary changes.

USING THE RIGHT TOOLS

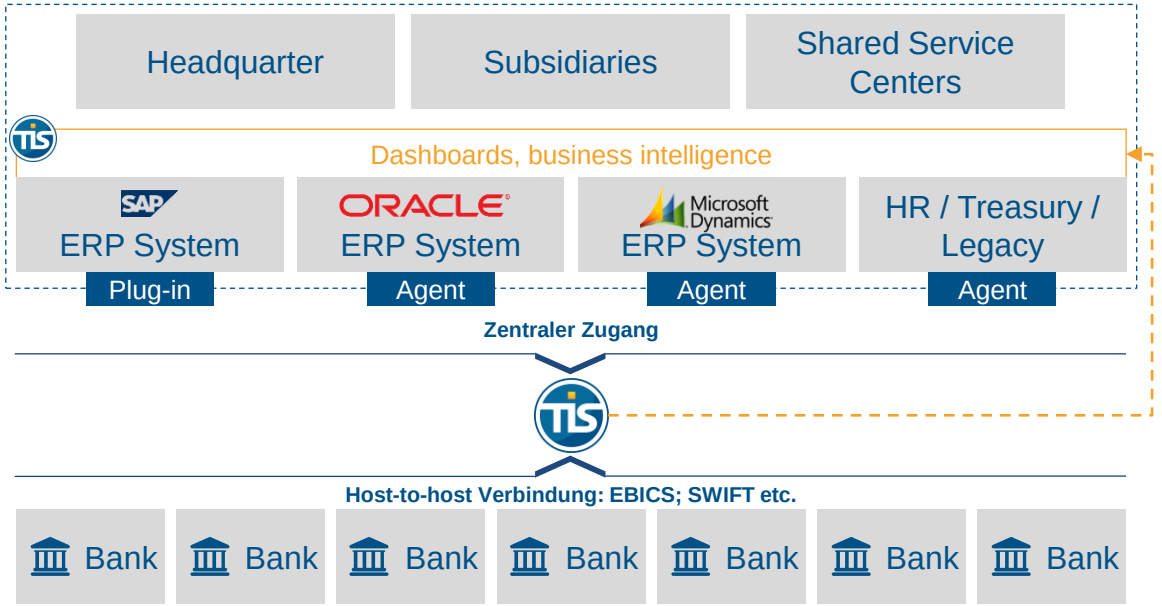
- At TIS, we help many international companies mitigate payments risks.
- Cloud-based platform where all payments processes will be standardized
- All payment data centralized for visibility and accessibility
- Approval processes and workflows with multiple approvers can be established quickly
- TIS has designed four building blocks for its cloud-based platform

THE BUILDING BLOCKS

THE OLD WORLD



THE NEW WORLD



Segregation of Duties	A Single Payment‘s Gateway	IP Whitelisting	Beneficiary Address Book	White-/Blacklist
SSO	Multi-Factor-Authentication	Real-time Monitoring	Inventory Process	Business Audit Logs

THE BUILDING BLOCKS (2)

BUILDING BLOCK 1

The basics are vital to maintaining proper control of payment security

- Segregation of duties
- Designation of signature authority
- Single Payment Gateway

BUILDING BLOCK 2

Transparency and visibility are the enemies of fraud

- Real time monitoring of transactions
- Business audit log
- Inventory process
- Duplication check on payments

THE BUILDING BLOCKS (3)

BUILDING BLOCK

3

Advanced tools to support safety, security and ease in the payment process

- File forwarding configuration
- Single Sign-On (SSO)
- MFA (Multi-factor authentication)

BUILDING BLOCK

4

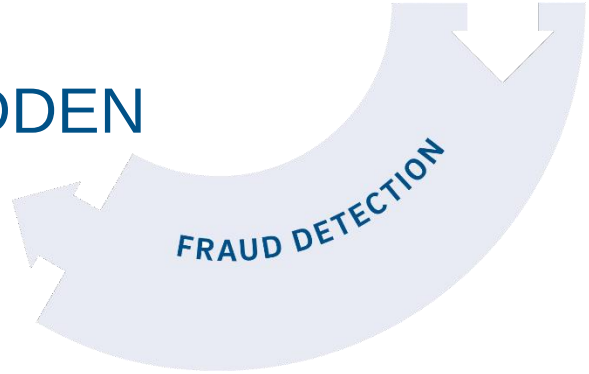
Specific tools designed for fraud prevention

- IP white-listing
- Beneficiary address book
- Whitelist beneficiaries for manual payments
- Blacklist

THE BUILDING BLOCKS (4)

Capabilities	Category
1. Segregation of duties	Workflow design principle
2. Business audit log	Auditing and reporting
3. Payment approval process	Process standardization
4. Payment approval with token (currently hardware token is offered)	Extra layer of security
5. Payment process standardization	Process standardization
6. The n-eyes principle for master data	Security principle
7. The 4-eyes principle for administrative workflow configurations	Security principle
8. Duplication check on payments	Configurable payment rules
9. Inventory process (automated audit proof internal control)	Auditing and reporting
10. IP white-listing	Extra layer of security
11. MFA (Multi-factor authentication)	Enhanced password security
12. Single Sign-On (SSO)	Enhanced password security
13. Real time monitoring of transactions and account movements	Monitoring and controlling
14. File forwarding configuration	Configurable payment rules
15. Straight-through processing of payments (STP)	Process standardization
16. Beneficiary address book	Beneficiary management
17. Whitelist beneficiaries for manual payments	Beneficiary management
18. Blacklist	Beneficiary management

STEP 3: SPOTTING THE UNKNOWN AND THE HIDDEN



Data input	Pattern recognition	Alarm triggering	Human review
The AI is given location, time of transaction, etc. for each payment and is told whether it was fraudulent.	The AI learns to recognize patterns that often go hand in hand with payments fraud, like an unusual time of day.	After sufficient training, the AI can flag suspicious transactions in new data it is given.	Suspicious transactions should then be reviewed to make sure there are no false positives.

PREVENTION AND DETECTION AT A GLANCE

	FRAUD PREVENTION	(AI-BASED) FRAUD DETECTION
KEY FEATURE	Preventing fraud by reducing risks and monitoring attack vectors	Detecting fraud by learning and identifying uncommon behaviors
LIMITATIONS	New attack vectors need to be incorporated into the software	Strong variations in payment behavior can cause difficulties
ADVANTAGES	Easier implememtation, lower costs	Scope of protection is scalable
DISADVANTAGES	Too much controlling can slow down processes	- High costs - Difficult to realize because of complex learning processes - Company internal know-how needed
TYPICAL CUSTOMER	Every company	- Companies with huge amount of payments - Decentralized companies with heterogeneous structures - Companies with reoccurring payment patterns

TIS: JOURNEY TO THE PERFECT WORLD OF PAYMENTS

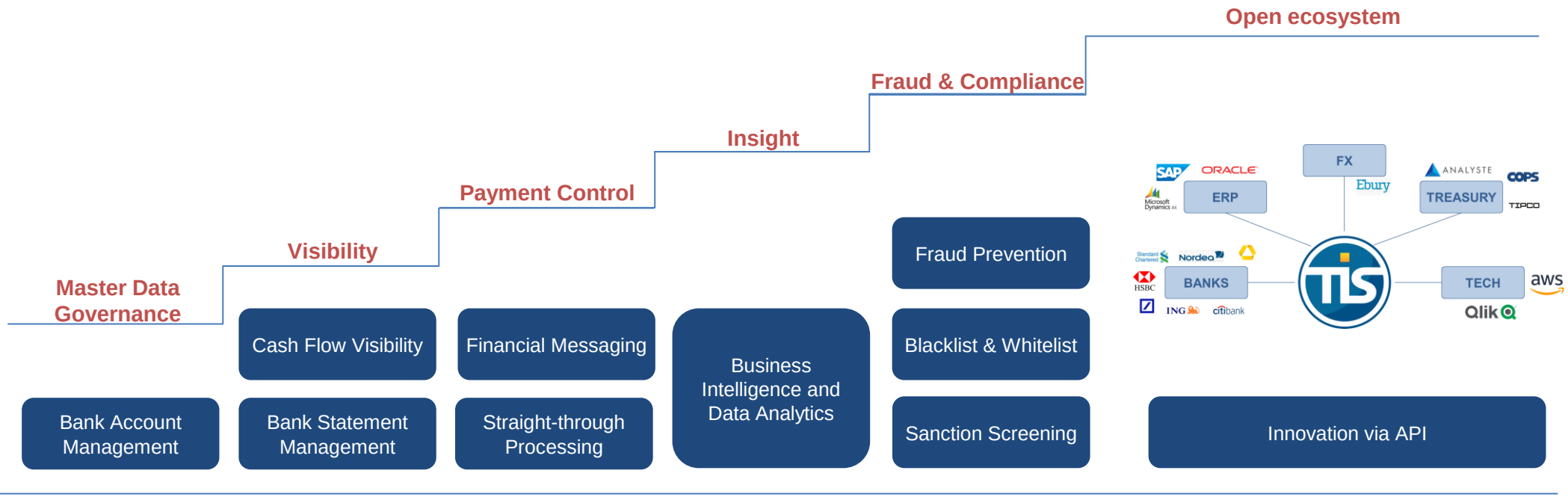
TIS defining payment trends

Since 2010: CLOUD PAYMENTS

Since 2014: MULTI-CHANNEL CONNECTIVITY

Since 2018: BEST OF BREED + API

TIS recommendations



Q&A

THANK YOU!

EROL BOZAK
CPO

TREASURY INTELLIGENCE SOLUTIONS
erol.bozak@tis.biz