tis

WHITEPAPER

Cyber Security as a Top Priority for the C-Suite in 2022: The Challenges Keep Growing.

Learn more at tispayments.com »

INTRODUCTION

2022 data shows that *Cyber Security* is a major priority on the agendas of C-level executives in 2022, and is ranked as the 2nd largest priority behind Digital Transformation. In fact, the newest issue of the annually conducted study by the international management consultancy Horvath found that while most financial service and insurance companies have been dealing with cyber security for some time and are better prepared to manage it, the topic has become increasingly important across other industries as well, such as Manufacturing. This whitepaper will use data captured through Horvath Consulting's recent "2022 CxO Priorities" to highlight why cyber security has become so important and evaluate how recent innovations in payment fraud prevention can help protect companies today.

FROM ZERO TO SECOND PLACE:
Cyber Security is the Strong Newcomer on the C-level Agenda in 2022.

Digital Transformation is a topic that has gained significant momentum for companies of all sizes and in all industries, especially as a result of the pandemic. For finance, treasury, and accounting teams, a wide variety of new digital solutions and workflows that were a minor focus just a few years ago have now been prioritized in full force. Although some of these solutions were implemented as strategic tools as part of ongoing, long-term digitization projects, many others came about specifically because of the rapid shift to remote working setups that was required circa 2020. But due to an extremely short implementation time, many of these projects have created loopholes or vulnerabilities that potentially expose companies to digital attacks on payment systems and transactions.

Yet pandemic-related objectives alone do not fully explain the results of Horváth's recent study on C-suite priorities and perspectives, in which *Cyber Security* catapulted into one of the top priorities.[1]

Earlier in 2022, management consultancy firm Horváth held in-depth discussions with 280 C-Level executives from 17 different countries, primarily in Europe, on the topic of strategic priorities and industry trends. The results showcase a rapid rise in the prioritization of cyber security and fraud prevention.

General Study Information

Source: Horváth, CxO Priorities 2022. Managing Overlapping Crises, June 2022, p. 4

1 Horváth: CxO Priorities 2022. Managing Overlapping Crises, June 2022.

FROM ONE CRISIS TO THE NEXT:
Companies are Facing Ever More Challenges.

The elevated presence of cyber security on the agenda of C-Suite executives can be largely attributed to the current global political situation, which does not hold out the prospect of any relief. In addition to supply chain bottlenecks and geopolitical conflict, volatile markets and fears of a global recession are causing massive uncertainty worldwide. As a result, concerns about the risks of digital attacks have risen significantly,[2] while constantly changing sanctions and sanction lists are creating additional compliance challenges for companies.

Strategic priorities 2022 to ensure steady mid- and long-term growth

	Rank 2020	Rank 2021	Rank 2022	△ '21 vs. '22	Score 2020	Score 2021	Score 2022
Digital Transformation	1	1	1	=	3.6	3.6	3.6
Cyber Security			2	NEW			NEW 3.5

Source: Result of the Study: Horváth: CxO Priorities 2022. Managing Overlapping Crises, Juni 2022, p. 18

While banks, insurance companies, and financial service providers have been confronted with the issue of *Cyber Security* for several years now and have been implementing or at least evaluating appropriate countermeasures, it is now other industries like manufacturing that are facing these challenges head-on.

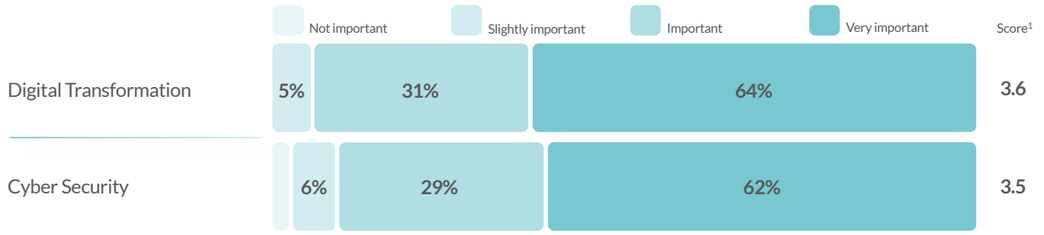
Cyber Security – the Rising Star of 2022

Source: Horváth, CxO Priorities 2022. Managing Overlapping Crises, June 2022, p. 4

2 Horváth: CxO Priorities 2022. Managing Overlapping Crises, June 2022, p.18

According to Horvath's data, ninety-one percent of the 280 CxOs surveyed consider *Cyber Security* to be important or very important. There is therefore just a small gap to the front-runner, *Digital Transformation* – rated as important or very important by 95 percent of respondents and still number one on CxOs' list of priorities, as it was in 2020 and 2021.

Top Priorities: *Cyber Security* close behind *Digital Transformation*



¹ *Importance of priorities on a scale of 1-4: 4 - very important, 3 - important, 2 - less important, 1 - not important, 0 - not applicable*
Source: Horváth, CxO Priorities 2022. Managing Overlapping Crises, June 2022, p. 17

CONSISTENTLY MINIMIZING RISK
with the Right Digital Solutions

Cyber Security and *Digital Transformation* clearly top the strategic agenda of C-suite executives in 2022. As such, many companies are attempting to address both digitalization and security priorities with the same tools and strategies that can mutually optimize each other:

> "As part of our consulting activities in the treasury environment, we emphasize the importance of a clear organizational structure and integrated processes that promote a high degree of standardization and harmonization.
>
> This is especially true for such a sensitive topic as payment transactions, and here we see clear potential for greater transparency and efficiency in our projects.
>
> When implementing digitization strategies, companies are looking for suitable technical solutions for processing payment transactions and, in addition to typical requirements such as process support, automation, and monitoring, they are increasingly making demands aimed at flexibility and security. This is underlined by the results of our CxO study from this year, and we expect the trend to continue in the future."
>
> ***Marco Meyer, Principal Treasury at Horváth***

For *Cyber Security* in general and payments in particular, this could mean establishing resilient and robust processes with the help of innovative and secure digital solutions. Such processes do not just take place here and there; rather, they are harmonized at a global level and across all entities. A holistically optimized standardization and automation of processes, systems, and authorizations, such as a consistent n-eyes principle or IP safelists and blocklists, can play a significant role in the successful operation of a company and strengthen its resilience in times of crisis.

Yet securing these basic processes and procedures is only the first step. Since digital threats are constantly evolving and new fraud scenarios are always emerging, they are best countered with digital solutions that are also constantly evolving and comprise a broad set of basic tools against both internal and external security threats. They must also have the necessary flexibility to support organic and externally-driven corporate growth in a way that is time-efficient and future-oriented, without lengthy implementation processes.

SANCTION SCREENING & PAYEE COMMUNITY SCREENING:
New Features of TIS

As a cloud-native solution with advanced banking and ERP connectivity, TIS has the flexibility and scalability needed for docking new corporate entities globally in a short space of time. While their **RiskOptix** product suite already includes several essential security functionalities such as automated workflows, secure logins, clear distribution of roles and rights, and data security and encryption on ISO 27001 and SOC1&2 certified servers, there are two newer solutions in RiskOptix that may prove particularly valuable to enterprises in light of current global political challenges: **Sanction Screening** and **Payee Community Screening**.

Today, violation of sanction lists can result not only in severe fines, but also in long-term reputational damage, meaning a mistake in payment transactions can potentially threaten a company's existence. Meanwhile, the volume of sanctioned countries, parties, and individuals – OFAC alone lists more than 20,000 entries – and the speed of changing sanction requirements pose a challenge.

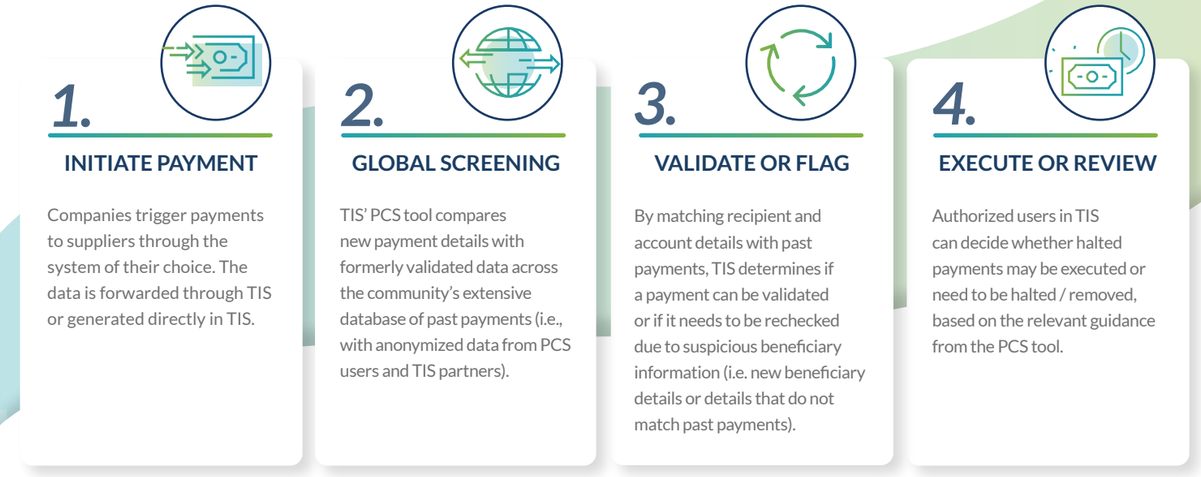
While individual banks and back-office systems such as Treasury Management Systems (TMS) often enable payments to be screened against sanction lists, compliance on a global level and for the entirety of payment transactions in all corporate locations is rarely guaranteed due to a lack of connectivity with all relevant systems, banks, and entities. Automation and global harmonization of sanctions list screening as an integral part of overall corporate payments, on the other hand, is something that TIS offers through its comprehensive system connectivity. Daily updated sanction lists, such as those of the UN, EU, and OFAC, can be supplemented with customizable safelists and blocklists, so that all payments can be screened around the clock based on a company's niche requirements. Alert management is also carried out in a globally uniform and clearly documented manner, and suspicious cases are easily resolved with definable responsibilities. This enables maximum compliance not only for the payments themselves, but also for the processing of suspicious cases.

> "Risks and vulnerabilities in the payment process often arise from insufficient data exchange between systems in different corporate entities. For such sensitive topics as digital security and sanctions screening, these gaps can have serious consequences for a company. TIS provides crucial support with global compliance by combining automated processes with digital solutions. At the same time, the risks of internal and external fraud attempts are minimized throughout the entire payment process."
>
> ***Jörg Wiemer, CSO of TIS***

In addition to **Sanctions Screening**, TIS has recently expanded its product range with another innovative fraud prevention solution in **RiskOptix** – **Payee Community Screening (PCS)**. PCS works by leveraging a global repository of historical beneficiary data from the TIS community of companies and banks – of course in compliance with the strictest data protection requirements – in order to authenticate new transactions made through the network. Through a strong partnership with Deutsche Bank, the amount of accessible data is significantly extended: PCS can access approximately 100 million bank account data points. This partnership also enables access to SWIFT's extended Pre-Validation Service, where approximately 9 billion anonymized transaction data points can be utilized across 4 billion global bank accounts annually.

PCS leverages this aggregated data to screen all payments against known and validated account information. Where there are discrepancies, alerts indicate possible violations in real time. Invoice fraud, for example – a form of fraud that has increased sharply in recent times – can be combatted efficiently in this way, as invoices made out to beneficiaries that are not recognized by the network are quickly halted and flagged.

Today, one of the main benefits of PCS is that it is continuously self-improving. The enormous data volume is constantly growing thanks to the tens of thousands of payments made daily by participating companies and banks within TIS. The intelligent collection, linking, and evaluation of this data accelerates the detection of attempted fraud, thus making payments even more secure and providing an iteratively more robust and comprehensive tool.



FINAL THOUGHTS

The topic of *Cyber Fraud* has catapulted from zero to second place in the C-level's strategic agenda, according to Horváth's "CxO Priorities 2022" study. Manufacturing companies in particular are now focused on concerns about secure, compliant payments. Unlike many financial service providers and insurers, which have been frequent victims of fraud attempts in the past and have already grown better equipped to deal with these scenarios, manufacturers have often not yet implemented appropriate solutions. The rapidly evolving fraud scenarios are best addressed through clear organizational structures and processes supported by smart, digital solutions. These should have the flexibility and system connectivity to connect all entities and payment-related systems of a company, and quickly keep pace with organic growth as well as M&As. On one hand, it is important to enable seamless, compliant processes – and to do so on a global level, across all business units. On the other, these solutions should be automatically updated and continuously developed – such as the **Sanction Screening and PCS** from TIS – to make it possible to deal with new fraud scenarios of all kinds more quickly and efficiently.

ABOUT HORVÁTH

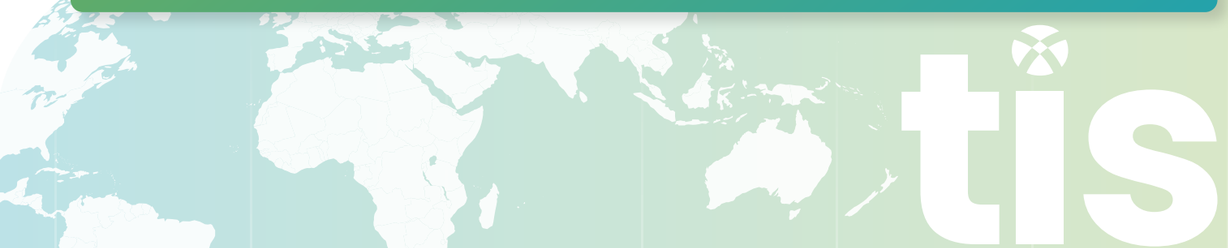
Horváth is an international, independent management consultancy firm with over 1,000 employees in locations in Germany, Austria, Switzerland, Hungary, Romania, Italy, the USA, Saudi Arabia, and the United Arab Emirates. We represent in-depth knowledge across different industries and top-level subject matter expertise in all company functions – with a focus on performance management and transformation. We carry out projects for our international customers around the world. In this context, we provide precise knowledge of, and take into account, the local conditions thanks to the cooperation with our partners of "Cordence Worldwide", a global network of truly connected consultancy firms with the ability to think and deliver together.

Our specialists support companies and top executives with extensive competence in business models, organizational structures, processes and systems to successfully align their organizations for the future. We combine passion and effective implementation to turn change into success across whole companies, in individual business areas or in functions such as sales, operations, procurement, controlling & finance, HR and IT. Horváth stands for project results which create sustainable benefits and value. That is why our consultants accompany their customers from the business management concept and anchoring in processes and systems through to change management and training of managers and employees.

ABOUT TIS

TIS helps organizations simplify and streamline their global payments and liquidity management operations. Our cloud-based platform empowers businesses to optimize critical functions surrounding cross-border and domestic payments, bank connectivity, cash forecasting, fraud prevention, payment compliance, and more. Corporations, institutions, and business vendors leverage TIS to transform how they connect with global banks and financial systems, collaborate on payment processes, execute outbound payments, analyze cash flow & compliance data, and promote working capital efficiency.

Ultimately, the TIS Enterprise Payment Optimization (EPO) Platform helps businesses improve operational efficiency, lower risk, manage liquidity, gain strategic advantage – and achieve enterprise payment optimization. Visit tispayments.com to reimagine your approach to payments and liquidity management



Learn more at tispayments.com »

TIS IN ZAHLEN

- **140+** COUNTRIES
- **250+** B2B CLIENTS
- **300+** EXPERT STAFF
- **30,000+** USERS
- **1k+ Systems** CONNECTED
- **100k+** PMT PROFILES
- **11k+ Bank** CONNECT OPTIONS
- **65k+ Bank** ACCOUNTS
- **~25 Million** UNIQUE PAYEES
- **$2 Trillion** ANNUAL VOLUME
- **99.95%+** SYSTEM UPTIME
- **100%** NATIVE CLOUD

All statistics represented are valid as of Q4 2022, unless otherwise noted.

Enterprise Payments reimagined.

Learn more at tispayments.com »

tis

TREASURY INTELLIGENCE SOLUTIONS GMBH

Germany (+49 6227 69824-0) | United States (+1 (617) 955 3223) | info@tispayments.com | tispayments.com