The digital fortress

The world has witnessed a series of significant security events recently around payment execution, from Leoni in Germany, through to ABB in South Korea, and SWIFT in Bangladesh – to name a few of the major headlines. Aside from these, there have been countless unreported, lower profile fraud cases in other organisations, both successful and attempted. *Martin Bellin*, Founder & CEO of BELLIN, explains how these events are taking place as a new payments landscape takes shape.

> *"Where there is money, there is fraud: an open door could tempt a saint"*

FINANCE departments are at the heart of any corporation: they safeguard liquidity, manage and steer cash flows and ensure there is a strategy to underpin all financial operations. At the same time, however, finance departments can be a 'gateway' to cyber-crime and internal fraud.

Back in the Middle Ages, rulers built fortresses to protect their treasures. However, despite their best efforts, these fortifications were still destroyed by fire and invaders. Metaphorically speaking, today's finance departments are doing the same to protect their 'treasures' by building digital fortresses, including fully integrated treasury management solutions that systematically eliminate vulnerabilities. However, even the most fortified systems can still fall victim to attack, from both external and internal forces, if all three pillars of cyber-security are not considered: people, technology and governance.

The people factor

Where there is money, there is fraud: an open door could tempt a saint. Employees can be an organisation's greatest asset in fraud prevention – or the weakest link. Fully integrated systems

offer authentication methods that ensure business-critical systems and data are only ever accessible to those employees who have been given the corresponding permissions. Two-factor authentication represents state-of-the-art security technology for treasury management systems and meets the most stringent requirements. In addition, Single Sign-on technology (SSO) enables a number of authentication methods that can be used on their own or in combination with other username and password standards in use at a company.

But what good is the best technology if employees don't know how to use it properly? For this reason, a holistic solution strengthens security considerably; a fully integrated solution represents a consolidated payment platform, unlike the use of several different banking portals. It is possible to set up a series of approval rounds for all payments, to save trusted account connections in a whitelist and to conduct Cyclic Redundancy Checks (CRC).

The technology factor

As cyber-crime has increased in the last few years, hacker attacks have become increasingly bold and professional. Enterprise-grade firewalls and intrusion prevention systems provide optimum protection from external threats. Network access encryptions increase security, but only if they are subjected to rigorous penetration tests by certified third-parties, ensuring that cloud solutions are protected from hacker attacks at all times.

"As cyber-crime has increased in the last few years, hacker attacks have become increasingly bold and professional. Enterprise-grade firewalls and intrusion prevention systems provide optimum protection from external threats"

The governance factor

Every company is different, meaning that requirements also differ when it comes to compliance with international legislation and regulations, guidelines and best practices. Moreover, these requirements are subject to constant change, again calling for a comprehensive, technology-based approach that ensures security system compliance at all times.

With a fully integrated system, companies have the option of making changes subject to an approval process with multiple levels (from dual approval to involving six approval levels). This means that any changes need to be checked and authorised by at least one other administrator before being approved and implemented. This way, approval processes can be aligned with internal governance guidelines.

From a system point of view, it is also possible to define daily limits for account transactions and intercompany transfers, or to set them up for specific employees. Blacklists can help meet all compliance requirements with regard to sanctions and embargoes.

The digital drawbridge

Security can be boosted enormously by combining the use of a system with additional components, like an app. This creates a separation of hardware between the user of the application and the software itself, making it impossible for potential fraudsters and attackers to retrace the entire process on one single device and to copy it. BELLIN recently launched a new app to complement the tm5 treasury management system – BELLIN Connect. Using the app, corporates benefit from the added security of two-factor authentication and the ability to split payment authorisation between different devices. The app essentially acts as a 'pulled up drawbridge' across the security moat, ensuring the finance department treasures are fully protected.

MARTIN BELLIN is Founder & CEO of BELLIN Group. After studying business administration at the University of Mannheim with a focus on finance and computer science, he worked as a treasurer for notable companies. Today, BELLIN is a global leader in providing web-based treasury software and services for multi-national corporations. In 2015, he was recognised as 'Entrepreneur of the Year' by World Finance, and again in 2016 by European CEO Entrepreneur Awards.