Security – a Major Focus for Treasurers

An Executive Interview with **Martin Bellin,** Founder and Managing Director, BELLIN Group

In this edition, we welcome Martin Bellin, founder and managing director of BELLIN Group, a global leader in providing web-based treasury software and services for multinational corporations headquartered in Germany, with offices in North America and the UK. In this interview with Helen Sanders, Editor, Martin discusses the issue of security, which has become front of mind for corporate treasurers and finance managers globally.

Why has security become such a major focus for treasurers recently?

Over the past year or two, we have seen a series of significant security events around payment execution, from Leoni in Germany through to ABB in South Korea and SWIFT in Bangladesh, together with many lower profile fraud events in many other organisations, both successful and attempted. These events are taking place at the same time as a new payments landscape takes shape, creating not only potential challenges but also opportunities.

Many organisations are taking advantage of new opportunities to centralise and standardise their payment flows, including payment factories and shared service centres, but they are doing so to different degrees, with some decentralised responsibilities and multiple systems still remaining in many cases. To be clear, any company that is using more than one payment platform across the group is unnecessarily exposed to additional fraud risk. Every access point represents a risk, and a new challenge in maintaining and enforcing consistent processes and controls.

While five years ago there were limits in corporate treasurers' and finance managers' ability to consolidate payment platforms, these obstacles have been swept away, and companies that do not seek to take advantage of these opportunities neglect the risks that a fragmented payments technology infrastructure presents.

Martin Bellin

What are treasurers and finance managers doing to address this risk?

The way that each corporation deals with this risk depends largely on the individuals involved and their awareness, experience and appetite for embracing the possibilities that now exist in payments technology. Given the pace of change, keeping track of emerging opportunities can be difficult, particularly with a large number of stakeholders and commentators in the market offering different opinions and following different strategies. Furthermore, treasurers and finance managers have a variety of calls on their time and budgets, so it can be difficult to prioritise payment technology projects. However, the business case is compelling given the risk of significant financial and reputational damage, as well as delivering improvements in efficiency, automation and cost-effectiveness.

Can you give an example of the opportunities in payments technology that you've mentioned?

Recently, we announced that we had connected our 100th corporate customer to SWIFT via our platform, a process we started in 2014. Clients can now connect directly to any SWIFT-enabled bank that supports corporate access and exchange a wide variety of message types. While SWIFT connectivity has traditionally been the domain of large multinational corporations, as it was complex and expensive, this has changed radically over the past three years. A growing number of smaller and mid-cap clients are now using our solution to connect to SWIFT and benefit from the efficiency and automation, bank coverage and security previously enjoyed only by larger companies. For example, we recently connected a Japanese client to SWIFT via our service located in Germany, which would have been difficult to envisage three years ago.

> *A growing number of smaller and mid-cap clients are now using our solution to connect to SWIFT and benefit from the efficiency and automation, bank coverage and security previously enjoyed only by larger companies.*

What other issues should treasurers be focusing on, in addition to payment platforms?

Although it is an essential step, implementing a central payments processing platform will not completely eliminate risk in the payments process.

For example, all users need to be aware of ways that third parties – and potentially internal staff – could seek to compromise security, including techniques such as CEO fraud and spearphishing which are becoming increasingly sophisticated. Companies may also choose to implement white lists, where all payments are validated against details held in securely stored data repositories.

The right payment processes are essential, and while many corporations have developed sophisticated processes, they are not always applied or enforced consistently. This is often a particular challenge for smaller, remote business units that have less sophisticated systems and smaller teams, so it can be difficult to achieve the appropriate segregation of duties. Lack of awareness of external fraud threats is also a problem in these cases, and as a result, these teams are particularly vulnerable to both internal and external fraud attempts.

Increasingly, corporations are addressing this vulnerability by centralising payments processing onto a central platform, so that all parts of the business observe the same processes and controls even if payments remain the responsibility of local business units. They may also choose to separate the transmission stage from execution and approval, to provide an additional layer of validation. Implementing techniques such as dual-factor authentication strengthens payment security further, but corporations need to determine how they want to balance payment speed and convenience with security. Currently, we are developing an app that offers an additional layer of security due for release later this year that ensures that approvals are performed on a separate device from execution. This breaks the process chain and avoids the risk of the originating device being accessed remotely.

Do SaaS solutions offer any specific security risks, or indeed benefits, compared with installed solutions?

Firstly, it is important to identify precisely what the security risks are. A hacker, for example may try to access an application – and indeed every large organisation has been hacked whether they are aware of it or not – and potentially delete data, modify existing data or insert fake data. The question, however, is what they are trying to achieve, and this is where the focus should be. For example, if the risk is that a hacker makes or redirects a payment, what controls beyond the system itself can prevent this?

In reality, a SaaS system is really no more or less 'secure' than any other system, although SaaS providers have sophisticated security infrastructure and protocols. However, the security of every system depends not only on access restrictions, but also on the processes, user controls and training around it. In this respect, there are some clear advantages to using a SaaS solution. Firstly, by consolidating the systems environment within the organisation to a single platform, there is only one external access point, such as to banks, which can be overseen by a central department. Secondly, processes and controls can be standardised and routinely enforced across the business. Thirdly, the treasurer can achieve the balance of convenience and security that is appropriate to the business, and establish the right levels of security according to the type, currency, value (etc.) of payment.

What advice would you give to treasurers and finance managers?

Securing the payments process is not rocket science and the opportunities exist for every organisation to achieve a high level of process and technical security, even if they lack specialist IT resources in-house. Before looking at the more sophisticated security tools, corporations need to get the basics right: many corporations still do not have controls on password usage, for example. The risk of security breaches, including the potential for significant financial and reputational damage, is not an issue that applies to other businesses, it is an essential issue for every organisation. Therefore, in an environment of increased risk on one hand, and increased opportunity on the other, no treasurer or finance manager can afford to delay. ■

> ***The security of every system depends not only on access restrictions, but also on the processes, user controls and training around it.***