RESILIENCE AND FLEXIBILITY

CORPORATE TREASURERS HAVE TO NAVIGATE A VOLATILE LANDSCAPE MADE OF REGULATORY DEVELOPMENTS, GEOPOLITICAL RISKS AND MOUNTING CYBER THREATS. THEIR ORGANISATIONS AND TEAMS WILL HAVE TO LIVE UP TO THE CHALLENGE, SAYS VIKTOR IVANOV

Regulation and cyberthreats are now firmly among the top factors that will impact the corporate treasurer's strategy in the years ahead. Add to that sudden geopolitical changes, which have abounded recently, and the risk equation for treasury teams could sometimes become overwhelming.

What is required from corporate treasury departments to cope with this fast-evolving and particularly challenging context?

This is one of the important questions discussed in the second edition of the *Journeys To Treasury* report, jointly published by BNP Paribas, the European Association of Corporate Treasurers (EACT), PwC and SAP in October 2017. The report takes stock of a survey and interviews with more than 100 treasurers who attended the 2017 EACT Summit.

Among the various themes in the report, one will resonate for sure with the corporate treasurers in the Middle East who manage their fair share of regulatory, geopolitical and cyber challenges – their organisations have to grow even more flexible and risk-resilient.

The regulatory avalanche

"There are moments, Jeeves, when one asks oneself: 'Do trousers matter?'"

"The mood will pass, sir."

Quite certainly there are moments in the professional life of a treasurer when one feels like talking to Jeeves as in the above quote from *The Code of the Woosters* of the great comic author PG Wodehouse. Admittedly, the link with treasury may not be obvious at first sight, so simply replace 'trousers' with EMIR, SEPA, BEPS, PSD2, GDPR, MiFID II or any other regulation acronym that has the capacity to put your organisation under a certain amount of stress.

During the past few years, rules and regulations have been coming in droves. Corporate treasurers have raised their game and have reinforced the preparedness of their departments to handle the practical implications of this ever-increasing variety of regulatory, compliance and accounting requirements.

However, new developments are emerging that will further complicate the tasks and raise the stakes for corporate treasury departments.

New trends, higher stakes

Attempts to mitigate or partially reverse some past reforms have been visible recently. Deregulation is a priority of the Trump administration in the US, yet even the EU is considering ways to limit the burden of certain onerous regulations. And while part of the treasury workload is removed, this brings along a growing regulatory fragmentation, and hence another headache for companies operating on a global scale.

At the same time, upcoming regulations are more often than not accompanied with significant penalties in case of non-compliance. For instance, the General Data Protection Regulation in the EU will carry significant fines (up to 20m or 4% of annual turnover) and potential public disclosure in cases where privacy laws are breached.

There is also a new propensity for authorities to take action, including inflicting penalties, against corporates for non-compliance in the areas of financial crime and sanctions. Beyond the financial cost, associated negative news can lead to tarnished reputations and damage relationships with banks.

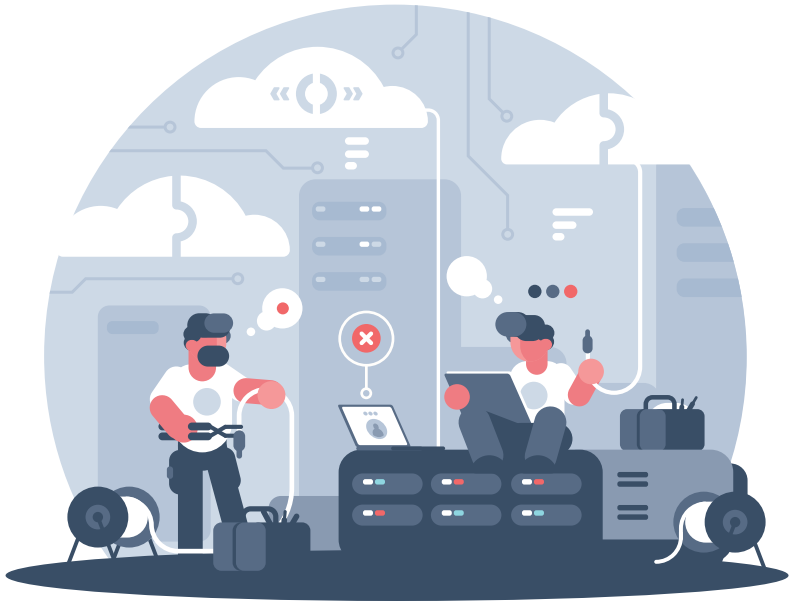
These developments have attracted attention at the highest levels of the corporate organisation. Executive management, and sometimes even the board, closely monitor the matter and increasingly look at their treasury departments for help with strategic advice.

Here comes the taxman

Tax authorities have contributed their share of the burden, with increasing transparency requirements or new taxes. In the aftermath of several scandals and information leaks, anti-tax avoidance measures are now being enforced and reinforced. The Foreign Account Tax Compliance Act from the US, BEPS from the Organisation for Economic Co-operation and Development and, more recently, a string of regulations and fines from EU authorities are raising the stakes for global corporations operating in multiple jurisdictions.

In the Gulf Cooperation Council (GCC), often (wrongly) presented as a tax-free region, the introduction of VAT represents a significant milestone. Saudi Arabia and

Cybersecurity is now recognised as a strategic priority not only for the treasury department, but also company-wide



the United Arab Emirates are leading the way, while the other GCC countries are to follow suit within 12 months, as per the previously agreed framework of a VAT union.

At a company level, the VAT introduction has mobilised significant resources spanning treasury, sales, procurement, IT, legal and indeed tax. CFOs and treasurers have been working intensively with their teams to analyse and anticipate all the practical implications, and to maintain sufficient lead time for a proper implementation. This is critical to avoid the tax audits and penalties that could be triggered in case the company is unable to fulfil its VAT obligations.

Geopolitical events

The past 18 months have seen an increased frequency of high-profile geopolitical events, with sometimes significant consequences for treasury departments.

In Europe, Brexit has been in the headlines for more than a year now. Still, on the treasury side, a number of critical aspects are yet to be determined, such as whether the UK will remain part of the Single Euro Payments Area zone or whether it would be convenient to keep euro-driven cash pools in the UK.

In the Middle East, the Qatari situation has brought a number of questions for treasurers to think about, ranging from contingency plans on treasury operations to sensitivity analysis on FX or interest rate exposures, without forgetting the need to provide regular updates and advice to their head offices.

Such situations offer a welcome opportunity for treasury teams to raise their profile within the company and play a proactive role in addressing strategic questions. Geopolitical shifts, however, pose an arduous challenge to treasurers who need to build and maintain cost-efficient, yet very flexible, organisations.

Cyberthreats

Cybersecurity is now recognised as a strategic priority not only for the treasury department, but also company-wide.

The hacking, phishing or ransomware schemes have grown in sophistication and scale, and are today capable of inflicting costs similar to a large natural disaster. In a recent report published by Lloyd's and Cyence[1], the potential losses under certain possible large-scale hack events have been modelled in the range of a few billions to a few tens of billions of US dollars. This is comparable to the cost of a hurricane, such as the 2017 Irma[2].

The financial impact of the Petya[3] cyberattack in June 2017, while not yet fully known, has certainly reached multibillion-dollar levels. In their earnings reports, some impacted large firms in Europe and the US have reported damages of hundreds of millions of US dollars each.

In this context, efforts and money are mainly spent on security tools and staff-awareness programmes, both meant to prevent cyber incidents occurring. Yet, similarly to hurricanes, cyberattacks cannot be prevented. Therefore, another very important aspect is the capacity to respond and to implement time-sensitive measures in case of a breach. A cyber-incident plan is critical to protect the corporate assets and, as such, is a key component of a resilient organisation.

Building resilience

Today, the case is stronger than ever for building resilient and flexible treasury departments, capable of managing and adapting to a vast array of risks, many of which can be difficult to predict, anticipate or even formulate. There is no standard formula for achieving that. Treasurers need to be able to identify the right combination of levers to activate within their organisations. Yet one aspect will be a key success factor in all cases – the ability to engage with internal and external stakeholders to bring diverse perspectives together, to create awareness and share knowledge. The purpose of the report is exactly that.

1 *Counting the cost – cyber exposure decoded*. Emerging Risks Report 2017. Lloyd's, Cyence, 2017
2 Irma was one of the strongest Atlantic storms on record; it caused damages estimated in the range of several tens of billions of dollars
3 Later renamed to 'NotPetya' to distinguish it from earlier versions of the ransomware

Viktor Ivanov is head of transaction banking CEEMEA at BNP Paribas