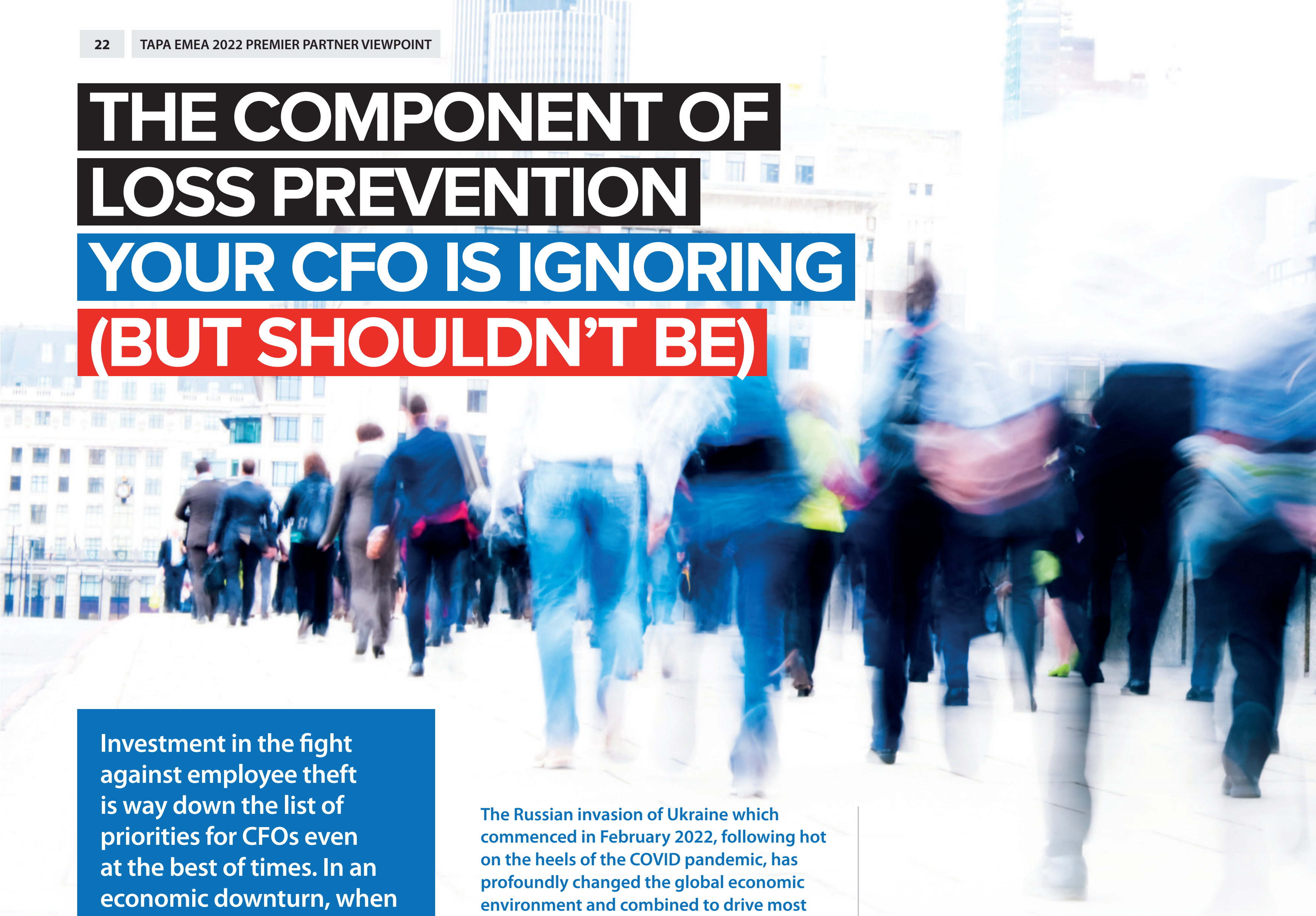
THE COMPONENT OF LOSS PREVENTION YOUR CFO IS IGNORING (BUT SHOULDN'T BE)



Investment in the fight against employee theft is way down the list of priorities for CFOs even at the best of times. In an economic downturn, when margins are squeezed and cash is tight, the chances of security and loss prevention professionals persuading their organisations to back them financially are next to nil. But what if we're thinking about this all wrong? What if you could make the case in such a way that the investment which you desire is a no-brainer for your CFO? Ben Graham, VP Commercial, and Glenn VanLandingham, VP Solutions Consulting for Thruvision believe they have the answer...

The Russian invasion of Ukraine which commenced in February 2022, following hot on the heels of the COVID pandemic, has profoundly changed the global economic environment and combined to drive most Western economies to the brink of recession. Whether you work for a FTSE100/Fortune 500 company or a small enterprise, the impacts of inflation on your energy costs, transportation costs and staff wages are dominating the thinking of your Finance departments.

Most capital expenditure is normally discretionary, and when times are tough or businesses are not performing to expectations, it is natural to put some of that spend on hold. Our experience, dealing with large corporations on a daily basis, is that CFOs have largely made the decision to continue investing in digital transformation, which is deemed essential to adapt to the post-COVID e-commerce world and in order to remain competitive. Everything else? Well, unless it's preventing you from doing business, you're just going to have to sweat those assets longer than normal. That machinery that is approaching end of life and could do with replacing? See if you can make it last another year or two.

Another outcome of a downturn, one that has been extensively studied by economists and statisticians, is that some types of crime increase. In their 2012 study titled *'The Overall Effect of the Business Cycle on Crime',* Shawn Bushway and Matthew Phillips (University of Albany) along with Phillip Cook (Duke University) proved that robbery and property crime rates generally rise during recessions and fall during recoveries, whilst other crimes such as homicide are acyclical.

Employee theft is a classic example of a crime that is driven by economics. The 10-10-80 rule is well known in our world of fraud and loss prevention: that 10% of your staff will never steal from you, 80% will depending on the situation and if the opportunity presents itself, and 10% will steal regularly. When costs of living are increasing rapidly, it is likely that a greater proportion of that middle 80% will assess the situation and determine that the risks associated with getting caught are worthwhile for the opportunity to supplement

an income that suddenly doesn't stretch as far as it used to. That will be even more true for organisations who have limited security processes and ineffective staff search procedures. Across the board, the companies we talk to are telling us that they believe staff theft is increasing rapidly.

Let's not forget that 10% who steal regularly. Organized crime groups are always on the lookout for holes to exploit. They can easily embed agency staff inside a poorly protected warehouse and then steal to order. Aside from that, they set a bad example to their colleagues, they demonstrate the ease with which theft can be committed, and the methods for doing so.

All of this staff theft does directly affect something which your CFO most definitely does care about: inventory and the costs associated with inventory. Theft is a form of shrink and inventory shrink results in many negative outcomes for your company – margin reduction, stockouts affecting your ability to deliver to customers' expectations leading to future lost revenue, replacement costs of that missing stock, and management distraction, to name just a few.

Unfortunately, most security efforts aimed at reducing employee theft have a negative impact on staff churn. In this economy, that's the last thing any organisation needs. Recruitment and employee retention are as tough now as they've ever been. Finding staff for your warehouse is difficult and costly. Finding the untrustworthy members of your

workforce and removing them is important, but it could drive a big increase in the costs incurred by HR, especially if it is a continual occurrence.

The impact on the trustworthy and reliable employees is just as significant. Warehouse staff do not like security screening (no-one does). No-one likes to go to work somewhere where they feel as though they are treated like a criminal. No-one eagerly awaits the prospect of a pat down or wanding by a security guard, and no guard enjoys performing those searches – and that's before you even

CONTINUED ON PAGE 24 >

consider the potential financial and PR implications of any legal action brought as a result of improper behaviour by guards during such searches. Companies that find ways to make their security screening process more "user friendly" report much lower rates of staff churn. It becomes a selling point to recruit staff in a crowded marketplace. In the supply chain world, combating staff theft and staff retention are inherently related.

Why, then, do we persist with traditional security screening at all? After all, inventory shrink is "baked in" to the P&L. Within reason, losses are acceptable. It's simply a cost of doing business. It's also incredibly difficult to pinpoint the root cause of that inventory shrink, because there are so many possible reasons for shrink. Professor Adrian Beck, a Criminology expert at the University of Leicester, spent years researching the topic and developed the concept of Total Retail Loss. It shows the myriad ways in which shrink can occur. Internal theft is one of many reasons and unlike some of the other reasons, it is largely an invisible cost, so it does not get the attention it deserves.

Let's back up a step. Losses are acceptable and are simply a cost of doing business. Really? Why? As experts in security, asset protection and/or loss prevention, why should we accept this status quo? Should we not do everything in our power to bring this number down? Especially when that number is huge. Industry benchmarks such as the 2022 *National Retail Federation Security Survey* tell us that the annual cost of shrink to retailers is $100bn, a significant increase from the $62bn reported a year earlier. Asset Protection/Loss Prevention teams are growing in size, and their budgets and responsibilities are both increasing. Professionals in this space are increasingly being evaluated on the success of their shrink reduction initiatives. For a retailer carrying $400 million of inventory across their distribution network, as little as a 30% reduction in shrink from theft is worth $900,000 per year.

Security screening has undergone its own digital transformation. The physical search by security guards is no longer the only option. You can demonstrate to your CFO the financial impact that using advanced technology to fight employee theft has on your bottom line. You can reduce shrink and boost your staff retention at the same time. Working with your supply chain and HR colleagues on a cross-functional business case for a more user-friendly solution, that delivers immediate and measurable impacts and a rapid return on the investment, might just have your CFO sit up and take notice.

'Let's not forget that 10% who steal regularly. Organized crime groups are always on the lookout for holes to exploit. They can easily embed agency staff inside a poorly protected warehouse and then steal to order.'

Perhaps you might even find that your organisation, despite cutting capital expenditure budgets wherever it can, deems that a small amount of CapEx investment in a "digitally transformed" security solution is worthwhile because it gives your business a few basis points of EBITDA margin back, even more so because it can deliver those returns quickly. That extra margin might just enable you to hire that additional sales manager, or that new engineer, or invest in development of a new product or capability. It's a no-brainer.

About the Authors

This article, coordinated by Alex Brundle, Thruvision's VP Sales and Marketing Profit Protection, was written by Thruvision, lead manufacturer of security screening technology.

Addressing the urgent need for "safe distance" people security screening in the COVID era, Thruvision is uniquely capable of detecting metallic and non-metallic items including weapons, explosives and contraband hidden under clothing, at safe distances. Using patented passive terahertz technology, Thruvision completely removes the need for physical "pat-downs". Deployed in 20 countries around the world, Thruvision is used for aviation security, supply chain loss prevention, customs and border control. The company has offices in Washington DC, and near Oxford, UK.

www.thruvision.com