The Rise of Ransomware – and the Fall in Taxes?

Janet Gooi - Senior Counsel - Tax
j.gooi@tamimi.com - Dubai International Financial Centre

Shiraz Khan - Partner, Head of Taxation - Tax / Corporate / Mergers and Acquisitions / Family Business
s.khan@tamimi.com - Dubai International Financial Centre

High-profile ransomware attacks have been recently grabbing headlines – and millions of cash. Major US fuel pipeline Colonial Pipeline, meat processing giant JBS, and GPS technology company Garmin were the latest organisations to have fallen victim to the increasing onslaught of ransomware attacks.

Amidst the threat of severe economic damage and operational disruptions brought on by these cyberattacks, businesses face the difficult choice of whether to pay these unwarranted amounts – and the tax consequences of their decisions.

How does ransomware work?

Ransomware, as its name suggests, is a type of malware that holds a user's files as "hostage" by encrypting these files and making them inaccessible until the ransom demanded is paid. Ransomware attacks occur through the downloading of software or opening of attachments with malicious codes, typically sent through email phishing, social media and suspicious websites.

Once the malicious code enters a machine, the ransomware can encrypt files across the entire

organisation’s network, flash drives or even cloud storage. To make matters worse, the ransom demands with specific payment instructions pop up – along with a countdown clock.

Corporate Tax in the GCC

Four out of six GCC countries have a corporate tax regime. Currently, there is no corporate tax in the UAE at the Federal level. However, at the Emirate level, some individual Emirates impose a limited form of corporate tax on businesses engaged in the exploration and production of oil and gas and branches of foreign banks in the UAE. Similarly, in Bahrain, only businesses that operate in the oil and gas sector are subject to corporate tax.

With the exception of the UAE and Bahrain, businesses operating in Saudi Arabia, Qatar, Kuwait and Oman have to grapple with corporate tax issues.

A tax deduction enables businesses to reduce a portion of their taxable income, through the deduction of allowable expenses. Claiming a tax deduction may seem like a simple matter of just deducting expenses from your gross income on the tax return. However, the determination of whether an expense is deductible is not always straightforward – not all expenses are automatically eligible for a tax deduction. Unsurprisingly, the tax deductibility of expenses is a common major source of controversy between tax authorities and taxpayers in the GCC region.

In order for an expense to be tax deductible, the big question is this: Is the expense is an ordinary and necessary expense to generate income?

Tax and Ransomware Attacks

The attack on Colonial Pipeline shut down systems that supply 45% of the fuel in Eastern United States. The ransomware attack on JBS resulted in a shutdown of its meat processing operations, with workers being sent home and shipments of cattle having to return to ranches. JBS reportedly paid an equivalent of USD 11 million to hackers to restore its system.

With the mounting ransomware attacks, such payments become increasingly common and appear to be a necessary expense to continue generating income. Businesses that are attacked usually have no option but to pay these hackers, or risk losing all their data. If organisations are unable to access files that are crucial to carrying on their business activities, organisations are unable to generate any income. Arguably, the alarming surge of ransomware attacks and its devastating consequences provide strong justifications for these expenses to be considered an ordinary (or regular) and necessary expense for business continuity.

Despite the apparent necessity of ransomware payments, businesses will also need to take a closer look at whether these expenses are restricted or fall into the non-deductible category. Many countries, such as Saudi Arabia for example, restrict taxpayers from claiming a tax deduction for any amounts that are considered illegal or a criminal offence under domestic law.

Similar parallels exist between ransomware attacks, kidnapping and robbery. By “kidnapping” data and extorting money from businesses, there is no doubt that ransomware attacks contain the essential ingredients of a criminal activity. However, a distinction should be drawn between ransomware attacks and making ransomware payments. Whilst the former activity is clearly illegal, the potential illegality of the latter activity is not so clear cut. The little-regulated aspect of the cybersecurity industry presents a further

challenge in assessing whether the tax deductibility of ransomware payments is restricted.

Governments around the world have been cautioning businesses from giving in to the demands of cybercriminals. And there is a rationale for that – the more businesses settle ransomware demands, the more incentivised these cybercriminals will be to carry out attacks. No business will voluntarily fork out millions to meet ransomware demands. However, the refrainment from paying the ransom demand is not an easy decision to make particularly when it boils down to the survival of the business. Not only would businesses suffer from financial loss and operational chaos when attacked, businesses may have to take a double hit to their accounts if a tax deduction for ransomware is disallowed, in addition to penalties. On the other hand, the ability to benefit from tax deductions for such payments may unintendedly open the floodgates to abuse by organisations.

On top of satisfying the "ordinary and necessary" expense condition, robust documentary evidence is generally required in order for the expense to be tax deductible. In the GCC region, in practice, taxpayers are typically denied from claiming a tax deduction if the tax authorities consider that the supporting documents in place are insufficient to substantiate the taxpayer's expenses. Documenting a ransomware payment can be tricky though, particularly with the emergence of Bitcoin – the preferred currency of ransomware attackers. The only information displayed by Bitcoin wallets are a long, complex string of letters and numbers. The anonymity and lack of traceability of Bitcoin may make the substantiation of the ransomware payment a complex task.

Concluding thoughts

As we have seen above, the failure to meet ransomware demands may translate into catastrophic implications for the business and the economy. When the survival of the business is at stake against a ticking clock, there may be little option but for the business to pay. Even then, businesses will need to carefully consider the tax repercussions of their difficult but pragmatic decision. The tax deductibility of ransomware payments is a complicated and delicate affair – especially when tax deductions are a common major source of controversy between tax authorities and taxpayers in the GCC region.

Al Tamimi & Company's Tax Team regularly advises on corporate tax, VAT and other tax matters. For further information, please contact Janet Gooi.