BIZCOMMUNITY

Why investing in due diligence now will save you money later

By David Loxton

12 Dec 2019

Just a few years ago, the only security a company need worry about concerned physical measures; measures which could be easily quantified and reviewed. However, with the steady online migration and greater emphasis and reliance on data, cybersecurity is gaining prominence, which means that due diligence is becoming increasingly important too.

The number of companies which overlook this simple fact is astounding – not that it's restricted to cyberspace. In fact, according to a recent report by Refinitiv, as many as 43% of new employees admitted to organisations were not subject to due diligence checks. This runs contrary to a trend that sees 5% of global turnover invested in third party and client due diligence checks. It also flies in the face of another of the report's findings, which states that 76% of the organisations included in the survey were aware that financial crime had taken place within their global operations within the past 12 months.

Basic checks

A simple check seems like an obvious undertaking. It's also unlikely to be particularly onerous. The problem is that the details that make all the difference between an honest transaction and a fraudulent one might be so small as to be almost unnoticeable – especially if the check runs short of being completely thorough.

A case in point: recently, a client's procurement team conducted a due diligence check on a potential client. They did this by consulting the Companies Intellectual Properties Commission, which holds the details of every company. They found that the details on the prospective client's invoice seemed entirely legitimate, except for one tiny thing: while CIPC listed the details as, say, Joe Soap, inscribed on the invoice was the name 'Joe Soap and Company'. Not really worth investigating – except that, had more attention been paid, the procurement department would have noticed that different bank accounts were given. This would have stopped them from losing money, as happened when they accused their customer of failing to pay. The fact is that money has been paid, just not into the right account – and, as the original supplier rightly points out, that's not really the payee's problem.

Does your company follow a due diligence checklist?
LexisNexis 28 Nov 2019

No shortcuts

This kind of practice is on the increase. So, what's the solution? Unfortunately, there are no shortcuts here. It's all about making sure you know your customer, and the only way to do this is by conducting a comprehensive due diligence.

Every member of your team has to be involved in this process, even if their role is not directly related to finance. Because fraud is so rife, every single person on the team has to think like a forensic specialist. And, yes, it will be time consuming – hours will be spent checking invoices against the original documentation. But the alternative is to lose those funds when you are forced to pay twice.

Cyber security

The issue becomes even more complex when we're dealing with the cyber environment. Plus, the stakes are higher. Just think of how much data is online, and you'll see that information is one of your organisation's most important assets; not only because it may be leveraged to enhance your organisation's competitive edge, but also because there's much to be gained from monetising it. Loss thereof may have dire consequences, from financial loss to reputational damage as it emerges that you have put your customers' private details at risk. You might even find yourself facing a fine because of this.


The objective of due diligence is to entrench value
Lerato Thekiso 9 Jul 2019

That's why, just as you go to great lengths to protect other assets, so you must ensure that your cyber security cannot be breached.

The problem is that, in a world of shared offices and fibre lines, this isn't always easy – hence the need for an eagle eye when it comes to identifying the information that requires protection, and a thorough investigation of the technology, people and processes that are required to do this properly. Above all, it is crucial to bear in mind regulatory requirements and best practice.

Due diligence is one of those areas where a significant upfront investment is critical – but putting in the time and money

upfront will save you a great deal of both later on.

ABOUT THE AUTHOR

David Loxton is CEO of Africa Forensics & Cyber, specialists in fraud, online and white collar crime. He also practises for his own account at Loxton Attorneys, which focuses on employment law.