Cyber Crime vs Commercial Crime – What are you seeking to protect?

As business transactions are increasingly conducted online, most businesses are aware of the need for some sort of protection against potential losses, thus this has forced such entities to seriously consider the need to protect themselves against perils intrinsic within these spaces.

An article from Harvard Business Institute (1) published 18th February 2021 highlights how Kenya has seen a boom in usage and setup of Financial technology owing to heavy investment in the countries telecommunications infrastructure, with more Kenyans having access to Mobile Phones, thus performing their daily banking transactions on the go. The same behaviour is also common within Kenya's commercial sectors, both public and private, of whom have exploited these changes in order diversify business scope and maximise customer leverage. Naturally, this has brought technological related crime and the means of protection against it, to the forefront of risk management in these regions.

Whilst principally having two distinct functions towards protecting a business's balance sheet and general operations, it does seem apparent that there is a confusion within the local market between the intended offerings of Commercial Crime and Cyber insurances, and how each are designed to protect a business from financial or reputational harm, but in different ways.

Cyber Crime (Liability)

Cyber Crime (or Cyber Liability) is generally defined as any criminal activity involving a computer or network, usually perpetrated by an external agent. It is the unauthorized access to, interference with and/or fraud of **data.** Cover is often afforded to the insured on both a first and third party basis either in the forms of Business Interruption & Data Recovery (amongst others) and Liabilities incurred against the mishandling of customer data (especially Personal Protection Information or PPI) respectively.

Commercial Crime

Commercial Crime Insurance covers companies against their financial losses incurred through fraud, theft or dishonesty committed by their employees, with the intended result being the embezzlement of **direct funds** from the company, or in other words, an **intended direct financial loss to the insured**. This makes Commercial Crime insurance an exclusively first party loss policy. In some instances, crime insurance policies also cover frauds perpetrated by third parties (non-employees). Given that a company's internal controls should cover much of the risk associated with third party fraud, cover for this type of crime is often quite specific and usually endorsed subject to underwriter approval on a case by case basis.

The Confusions

Like Cyber, Commercial Crime insurance is sectioned in the respective wordings to cover various perils associated with the intended consequence of the perpetrated fraud/act (Cyber – access of Data, Commercial Crime – access to company/trustee money). The confusion tends to lie within the Electronic Computer Crime (ECC) section of a Commercial Crime policy (or Bankers Bond depending on the industry concerned) which runs the risk -by implication of its name - of being misunderstood by its policyholder and potentially bleeding into Cyber Crime. It is important to remember that ECC is intended to cover the misuse of internal computer systems from employees or third parties who use them to funnel insured funds, and not an external hack of company or customer data. The same

blurring of the lines is the case for Social Engineering which is an endorsed section of a Commercial Crime policy and is designed to cover against a confidence scheme that intentionally misleads an employee into sending money or diverting a payment based on fraudulent information, which in many respects, tends to involve the use of computer of digital based systems. To make matters more confusing, some Cyber reinsurers have now begun to include extensions within their wordings as a sublimit against the annual aggregate to cover an external party's access to direct funds of the insured, once again blurring the lines between these two covers further. However it must be stressed that this is not a common inclusion and is not covered in an isolated form nor does it cover internal infidelity cases, thus a Commercial Crime policy would still be a more viable solution if this is the intention behind the procurement of insurance

The Solution

It is evident from speaking to our client's across the African Continent that there are misapprehensions on what their policyholders are seeking for their coverage, and it is all too common for the perils that are at the forefront of buyer's mind to be absent from the solution that is sourced because it is the wrong product in the first place. The key question to ask your client is 'What are you seeking to protect?' should an enquiry for Cyber ever be forthcoming, as it may be the assured's actual intention to protect themselves against the nefarious access of monies via digital means, which in practice, would make a bespoke Commercial Crime policy a more viable solution for their demands and needs. It's important to assert, both policies have their merits, and in a world where computer fraud is increasing in severity and prevalence, the optimal remedy is for your client is to try and purchase both for a complete risk managed solution against digitally related criminal activity.

For more information on this article or to discuss with us further solutions within these spaces, please contact Michael Knight at Afro Asian Insurance Services.

(1) https://hbr.org/2021/02/kenya-is-becoming-a-global-hub-of-fintech-innovation