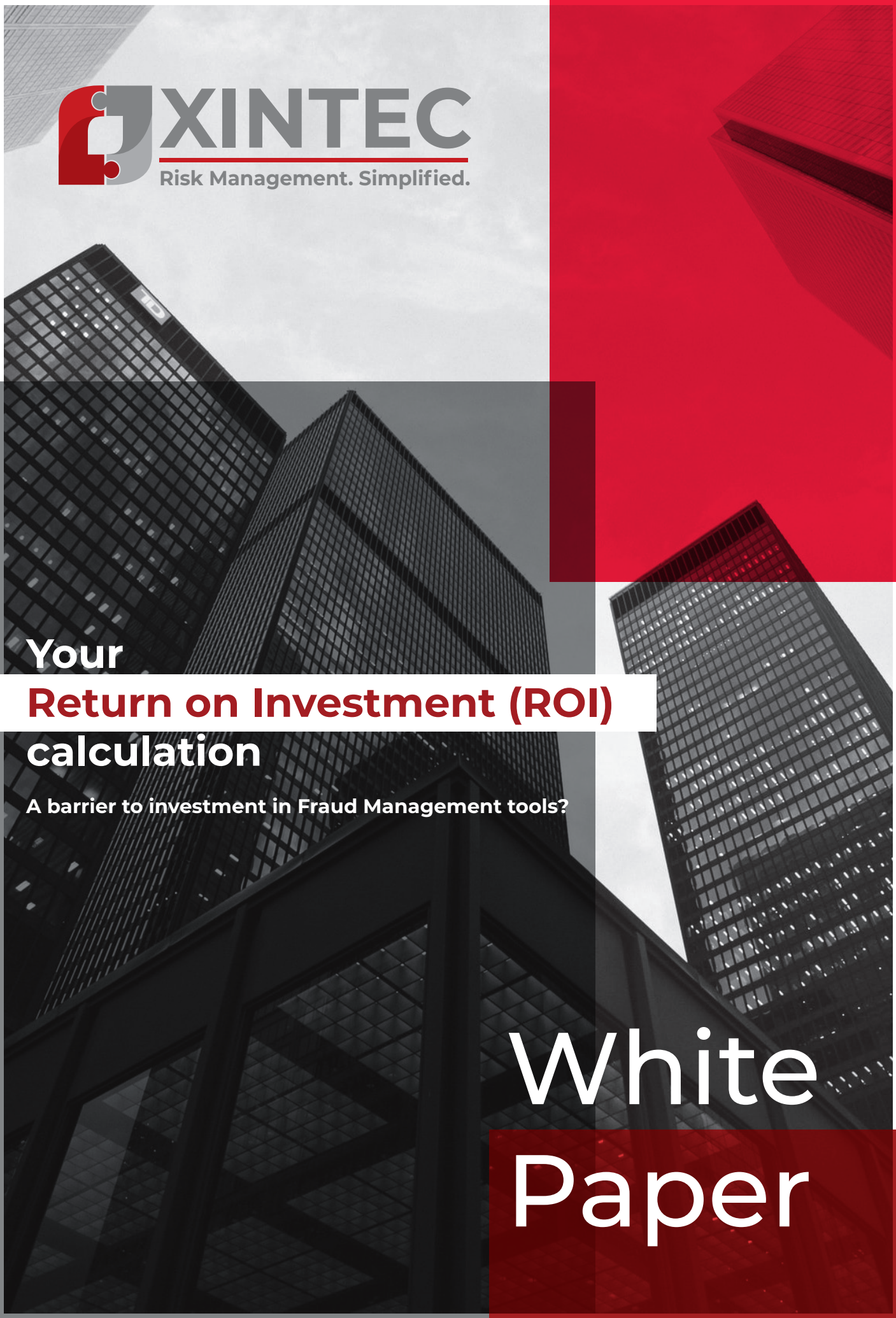
XINTEC

Risk Management. Simplified.



Your Return on Investment (ROI) calculation

A barrier to investment in Fraud Management tools?

White Paper

Your Return on Investment (ROI) calculation

A barrier to investment in Fraud Management tools?

Today's standard business practice would demand that any application for capital budget be accompanied by an ROI calculation. The ROI relates to the profit from an investment. If you invest money in a part of your business, the ROI tells you how much of that investment you got back, or how much new income was generated, in relation to what you put in. This will show you the profitability of your investment.

The ROI is calculated by subtracting the initial value (or beginning value) of the investment from the final value of the investment, including improvements, increased revenue etc, and this equals the net return. The net return is then divided by the cost of the investment, and then multiplied by 100. It is generally accepted that a good marketing ROI is 5:1, although achieving a ratio higher than 10:1 is possible.

This measure is certainly applicable to projects that have an impact on busines growth, customer satisfaction, customer acquisition/ retention, new products and services etc, where ROI is reasonably easy to predict and quantify. Business Analysts will be able to survey and analyse customer behaviour to predict the success or failure rate of any pending project, and accurately predict the ROI. After a period, typically 6 months or 1 year, the predicted ROI will be validated by measuring the business growth or increased revenue/ customer satisfaction that it has created and applying the standard ROI formula. The result of this ROI validation will then determine whether not the project is considered a success, or if that is not the case, discontinued.

The CFO at centre stage

For these types of investments, decisions up to a certain financial level are delegated to the CFO or Finance Director. Investments with a value over the CFO's delegated financial authority will generally go before a Finance Committee to make a recommendation.

This process works well with a project investment that clearly identifies opportunities to increase revenue or increase customer satisfaction and is supported by a robust and credible ROI. This is not so easy when the budget application is to implement Fraud or Security controls to protect the business against a malicious threat that may or may not occur within the next 1, 6 or 12 months.

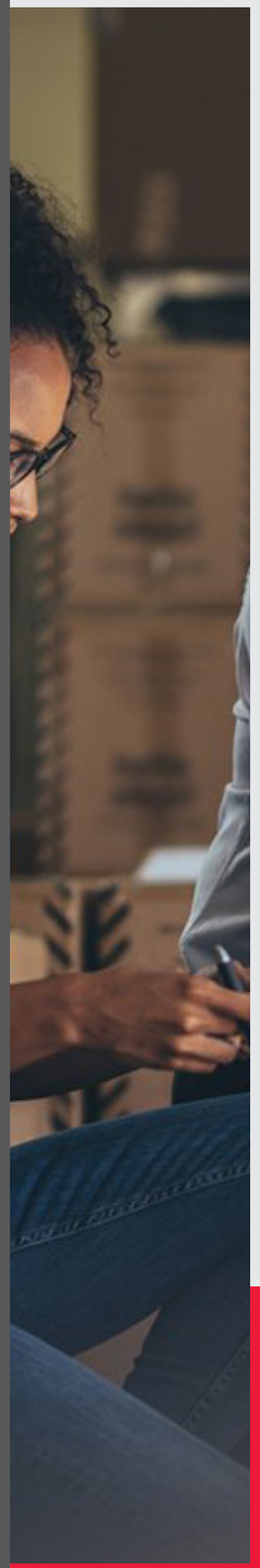
After 30 years working in the Telecoms Fraud, Risk and Security field, the writer has had many experiences where a budget request for fraud or security resources has been declined by a CFO who has stated that he will 'take the risk' that they will not suffer any major malicious attack.

Despite the financial and reputational risks being clearly identified the CFO has elected on such occasions to decline the budget request without fully understanding what the impact of nothing doing could be.

This thought process is quite understandable when considering that the CFO has, in one hand, a budget request for a marketing project that will generate significant benefits to the company against the fraud/ risk project that will only deliver value if the company is targeted by criminals.

In some instances, the CFO will not see the impact of this decision for a period, but those of us in this field know that sooner or later fraud and security attacks always migrate to the weakest link. The writer has experienced incidents where the decision to decline a budget request for a fraud or security prevention initiative has resulted in losses to the company far in excess of the budget requested.

XINTEC Risk Management. Simplified. 5-6 Castle Demesne House, Ivy Terrace, Tralee V92 Y4DC, County Kerry, Ireland I +353 (0) 1 2930260 I info@xintec.com I www.xintec.com /company/XINTEC /XINTEC /XINTECGlobal



Case Study – highlighting one of many real-world examples

One of these situations that always comes to mind – where the CFO has declined a budget request – is an incident the writer was involved with a few years ago. A Telecom Operator implementing a new Customer Management system made the decision that to stop cost overruns, they would remove fraud and security controls from the project. This resulted in the new Customer Management System going live with a number of known security, audit and access weaknesses.

These vulnerabilities were known to the Fraud and Security team within this Telecom Operator, and over a 3–4-year period, 3 or 4 requests for budget to enable the system access to be hardened were declined, despite warnings from the document authors of the risks the current insecure system imposed on the business. The budget requested ranged from a few hundred thousand dollars to implement some basic security to about 3 million dollars to implement more rigid controls.

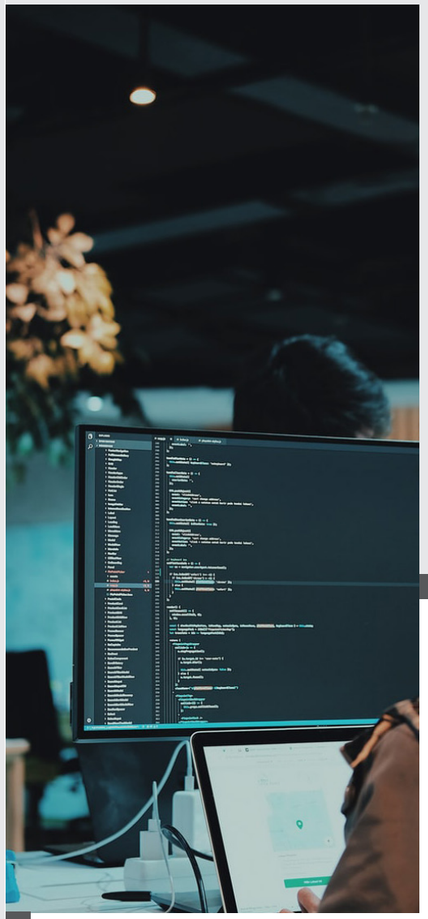
"...the risk of doing nothing to manage the vulnerabilities created by a system of weak controls was putting the company at significant risk..."

This issue became known in the public domain when a member of the public was able to use his laptop in a café and obtain access into the back end of the Telecom Operator's customer management system. In doing so, he could set up an account for himself, and also access other customer accounts to view their personal information. He then took evidence of this to the media, and the issue was reported in the country's daily newspapers every day for the following week. This resulted in Government and Law Enforcement intervention and the damage to the company's reputation was devastating.

When the writing is on the wall

A system audit found that over a period of several years, almost $4 million had been added to customer accounts by organised crime members through International Revenue Share Fraud (IRSF) and account takeover. In addition to refunding these fraud charges to customers, the Telecom Operator also had to pay the interconnect charges for the fraud calls. As a result of the adverse publicity through the media, and the lack of confidence in the Telecom Operator by customers, over 100,000 customers cancelled their services with the Telecom Operator during the following month. With an average ARPU of $34.00 per month ($408.00 per customer per year), this represented a loss of income for the first year of $40.8 million.

Budget requests seen by the writer made it quite clear that the risk of doing nothing to manage the vulnerabilities created by a system of weak controls was putting the company at significant risk, particularly considering that during the same period a budget request to purchase and implement a Fraud Management System had also been declined. When later questioned about his reasons for his continued refusal to approve budget to harden this system, the CFO claimed that the risks had not been explained to him in enough detail.



If the estimated $3 million originally applied for to complete the robust security requirements on the customer management system had been applied towards a revenue generating project that could have generated revenue equal to the value of the fraud losses, along with the lost revenue due to customer churn that followed, this would have generated revenues of 15 times more than the initial $3 million investment in the first year. To achieve this return from the investment required no sales input, no customer acquisition and no marketing expenses, just a modest investment to manage a known risk.

This is not the only case the writer is aware of where budget requests for Fraud and Security projects have been declined, because there is insufficient evidence to show that there will be an acceptable ROI from this investment.

Many of the challenging budget arguments I have experienced involve much more modest funding requests than the incident detailed above. We operate an International Premium Rate Test Number database which has become highly effective at identifying IRSF incidents when used as a hot number called list. We also use this database to assist Law Enforcement agencies, such as Europol, in their investigations of IRSF incidents. This is provided as a pro bono service and is remarkably successful at identifying who may have provided numbers used in any IRSF attack. We would generally find a match between the called numbers from any incident, and our IPRN database with 60 to 80% of these numbers.

XINTEC Risk Management. Simplified. 5-6 Castle Demesne House, Ivy Terrace, Tralee V92 Y4DC, County Kerry, Ireland I +353 (0) 1 2930260 I info@xintec.com I www.xintec.com /company/XINTEC /XINTEC /XINTECGlobal

Leave it to the experts

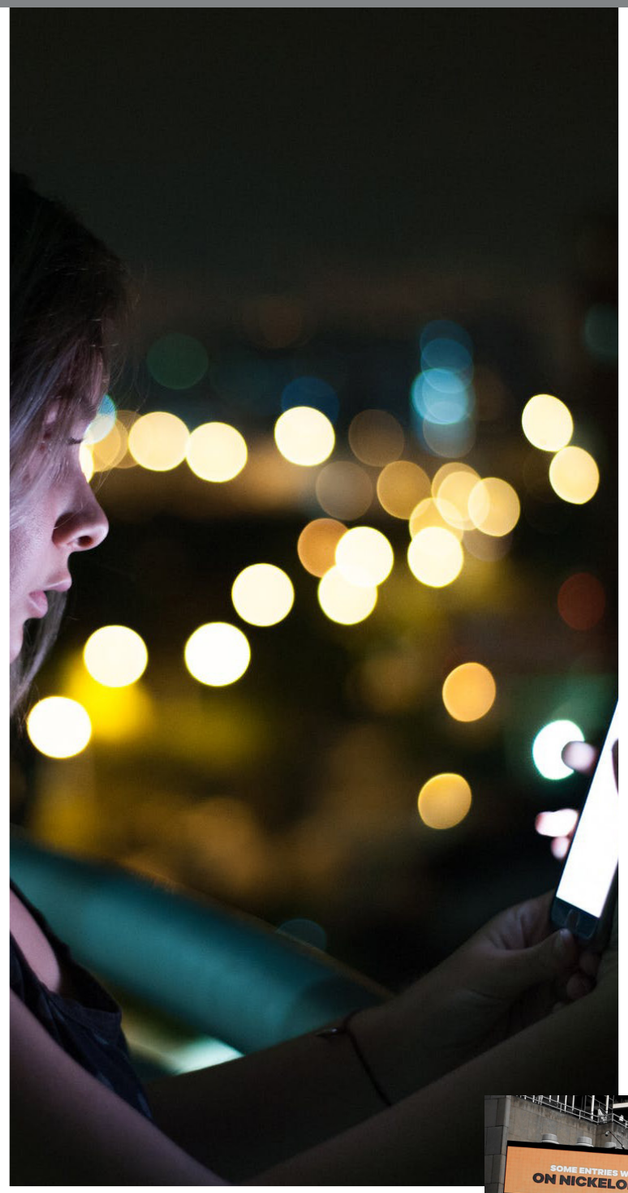
Law Enforcement will advise the complainant Telecom Operators of the success of this number match, and from this information, the Fraud Manager can identify at what point during the fraud attack it could have been discovered, and further calls prevented, had the IPRN Database been in use at the time of the attack. This information makes a very compelling business case and ROI as the annual cost of subscribing to this database is generally less than 10% of the cost of a modest IRSF attack. In two cases during 2020, we have the same Telecom Operator suffering 3 different IRSF attacks at different times with each showing 60 to 80 % of the numbers used in our database. Despite this, and a strong ROI being available, budget requests to implement our database to prevent further losses were declined.

Fraud and Security Managers understand that securing budget to provide tools to make their task of protecting the business easier is always going to be a challenge, so any budget request will only be submitted when they consider such tools are absolutely necessary to counter any current or emerging risk. In this second case, the requested budget was less than $US10,000 and the Business Case and ROI was very compelling, showing a huge net return.

A Chief Risk Officer role

So how do we overcome the historical reluctance of CFO's to look more favourably on budget requests to provide tools to better protect the business. The writer has a very strong view that if a budget request relates to a 'non-revenue generating initiative' and particularly one that will help protect the business from serious fraud, revenue or data loss, particularly one that could have a negative impact on the brand or share value, then this should be considered first by the Chief Risk Officer, who should then make representations to either the CFO (up to the level of financial authority of the CFO), and if a higher value is requested, to the CEO and Board.

There should be an expectation that the CRO will be very convincing in his or her argument for the budget allocation, while ensuring that the CFO, CEO or Board are in no doubt of the financial and reputational risk that could threaten the organisation if the budget is not approved. Any application that is still declined, should be raised again in 6 months to allow additional information to be added to the request if this is available.



Conclusion

In the current climate of reduced revenues caused by the global pandemic, and other influences such as new disruptive technologies, ringfencing an organisation, and protecting it's revenue streams from fraud, financial leakage and other issues (such as churn) that inevitably result in brand damage, is critical.

Fraud, Revenue Assurance and Risk Managers are retained by the organisation to enable the business by providing a secure and risk-free operating environment through which the rest of the business can offer superior services to customers. Like all customer delivery areas of the business, from time to time they require budget to keep the business safe.

Colin Yates
Director and Principal Consultant
Yates Fraud Consulting Limited

About the author: Colin is a telecommunications professional with some thirty years' experience, specifically in the areas of Fraud, Investigations, Revenue Assurance and Threat Management. Colin specialises in the areas of Telecoms Fraud (Internal and External) and Investigations. He also has considerable experience with Personnel and Physical Security, Law Enforcement Agency Liaison, Intelligence Management, Regulatory Compliance, Revenue Assurance and Policy development. In 2012/13 Colin researched the use of Test Numbers being used prior to an International Revenue Share Fraud attack and fostered the development of a database of known Test Numbers in use. This database has grown from 17,000 numbers in 2013 to over 7 million numbers today, and has proven itself as a key defence against IRSF for its many customers.

XINTEC Risk Management. Simplified. 5-6 Castle Demesne House, Ivy Terrace, Tralee V92 Y4DC, County Kerry, Ireland I +353 (0) 1 2930260 I info@xintec.com I www.xintec.com /company/XINTEC /XINTEC /XINTECGlobal