FINANCIER
WORLDWIDE corporatefinanceintelligence
www.financierworldwide.com
Issue 203 November 2019
THIS ISSUE:
FEATURE
IA today: plotting a roadmap to success
SPECIAL REPORT
Corporate tax
ROUNDTABLE
Corporate fraud
Emerging trends in cyber security
Companies need to adapt their cyber security strategies as new risks threaten networks.

Acuris Risk Intelligence

Published by Financier Worldwide Ltd

TALKINGPOINT November 2019

Proactive fraud risk management

FW discusses proactive fraud risk management with Nick Parfitt at Acuris Risk Intelligence.

THE PANELLIST

Nick Parfitt
Head of Market Planning
Acuris Risk Intelligence
T: +44 (0)20 3741 1300
E: info@acuris.com

Nick Parfitt is responsible for determining Acuris Risk Intelligence's approach to the market and building subject-matter expertise. He has 18 years' experience in project and programme management, business process change and in implementing technology and business solutions at financial services, telecoms and public sector organisations. His experience in the financial crime sector spans seven years, helping tier one financial institutions assess and improve anti-money laundering (AML), know your customer (KYC) and sanctions operations. Mr Parfitt has worked for several tier one banks and holds an MBA (Distinction) from Cardiff University, and a BA (Hons) in Biochemistry from Imperial College.

FW: How would you describe the current level of fraud risk facing companies? What recurring themes are you seeing in the types and methods of fraud being committed?

Parfitt: Companies are facing more fraud risk challenges today than at other period in recent history. Electronic commerce, information technology (IT) connectivity and the internet provide huge opportunity for fraudsters to gain access to businesses and to defraud them directly, through fraudulent customer transactions and even via employee identify theft or ransomware-type attacks. And let us not lose sight of fraud that is committed internally. How big is the fraud problem overall? The Association of Certified Fraud Examiners reports that US businesses will lose an average of 5 percent of their gross revenues to fraud. Phishing attacks are increasingly popular for targeting senior staff with 'CxO' frauds that encourage businesses to pay fraudulent invoices or change their banking details. Identity theft that leads to fraudulent customers being able to order goods or take out financial products is also increasing every year. According CSO UK, 56 percent of IT decision makers say targeted phishing attacks are their biggest security threat.

FW: How important is it for companies to take a proactive rather than reactive approach to fraud risk? What are the key principles of effective fraud risk management?

Parfitt: If companies rely on a reactive approach to fraud prevention, then it is unlikely that they will survive the initial attack. But not all fraud risks are equal. The challenge lies in identifying material risks and applying appropriate controls, and this is an ongoing process. Organisations first need to understand the fraud risks to which they are susceptible and how these risks would impact the business. If a company is the subject of a ransomware attack and does not pay up, what then? Can the company recover everything from back-up systems? Is customer data also compromised and would that result in General Data Protection Regulation (GDPR) issues? Once the risks are understood, it is important to know what governance and reporting mechanisms are available to identify, assess, action and then mitigate known or potential fraud threats, and to assess whether these controls are enough to address inherent and residual risk. Inherent risk is risk that exists without controls; residual risk is the risk that remains once current controls have been applied. Do companies have the systems and data to support the required controls – would they know if they did not? Fraud risk management should also consider supply chain risks, a growing problem in our increasingly interconnected world.

FW: How important is it for companies to build a risk management model tailored to address the specific fraud risks they may face?

Parfitt: Building an appropriate risk management model is crucial. Businesses vary so much in operational scale, the nature of what they do and where they operate, their culture and legal entity structures, and with whom they do business. With a detailed risk management model, a business can look at its scope and vulnerabilities, rate risk based on the material impacts of control failures, and then implement a roadmap to harden controls. This also ensures a continuous approach to improved defences. For example, training that is relevant to how an organisation operates should be highlighted within any framework, as should measuring its effectiveness.

FW: Having identified and prioritised the risk they face, how should companies go about integrating anti-fraud initiatives into their broader risk management function?

Parfitt: Companies must look for synergies with other initiatives or systems that overlap with identified higher-risk issues as a way to accelerate implementation. Where there are gaps, these must be highlighted through existing governance structures, and prioritised. A key factor is the level of senior sponsorship applied to these initiatives and how that plays out with the broader management function. It is possible, even likely, that current governance and process implementation mechanisms will need to be changed in order to improve the effectiveness of implementation and adoption. It is also important to be able to measure the effectiveness of progress and governance approaches for unblocking challenges or issues.

FW: Where should responsibility for managing fraud risk sit within a company's hierarchy? Is it important to designate oversight to a department or individual, for example?

Parfitt: We need to be careful in relation to the type of fraud, because on its own, it is too broad. For customer fraud, whether that is for actual customers being exposed to fraud by bad actors or themselves deliberately defrauding the organisation, it should sit with the business line owner with board oversight as it impacts the profit/loss ratio. Internal fraud or threats from external sources, such as hacking or phishing, would necessarily reside with the chief information security officer (CISO), again with board-level visibility and sponsorship. Accountability should be to individuals and not at department level, and we should look to leverage the Financial Conduct Authority's (FCA's) Senior Managers and Certification Regime (SMCR) for best practice.

FW: What can companies do to ensure their anti-fraud processes do not stifle their ability to meet their strategic, operational and financial objectives?

Parfitt: Companies must understand their fraud risks and exposure implications and prioritise accordingly. A business that makes widgets in the UK with a staff of a few hundred and turnover of a few million pounds does not need to locate its operations in an underground hardened bunker. But a nuclear power station, social media giant or financial adviser to ultra-high net worth families would have very different priorities around fraud. In practice, business should assess the control gaps that pose the most risk today and put in place a roadmap to close them.

FW: How do you envisage the nature of fraud risk developing in the years ahead? With this in mind, do companies need to be forward-thinking, to manage their exposure and reduce their chances of falling victim?

> “IN PRACTICE, BUSINESS SHOULD ASSESS THE CONTROL GAPS THAT POSE THE MOST RISK TODAY AND PUT IN PLACE A ROADMAP TO CLOSE THEM.”
>
> NICK PARFITT
> Acuris Risk Intelligence

Parfitt: We can only see fraud risk going one way, and that is toward greater risks, increasing fraud typologies and financial and reputational risk challenges for both businesses and individuals alike. As ever more devices are connected to the internet, security vulnerabilities and hacking risks increase. Companies can protect themselves by being highly aware of where the risks lie and building security into everything they do. However, this poses real challenges to large, global organisations that will have a plethora of IT systems, thus increasing their exposure risk. Companies must stay on top of fraud typologies and look to protect themselves by being proactive and leveraging specialist tools and data sets that provide an early warning of breaches and attacks, and whether data is already in the hands of criminals with fraudulent intent. ■

This article first appeared in the November 2019 issue of Financier Worldwide magazine. Permission to use this reprint has been granted by the publisher. © 2019 Financier Worldwide Limited.

FINANCIER WORLDWIDE corporatefinanceintelligence