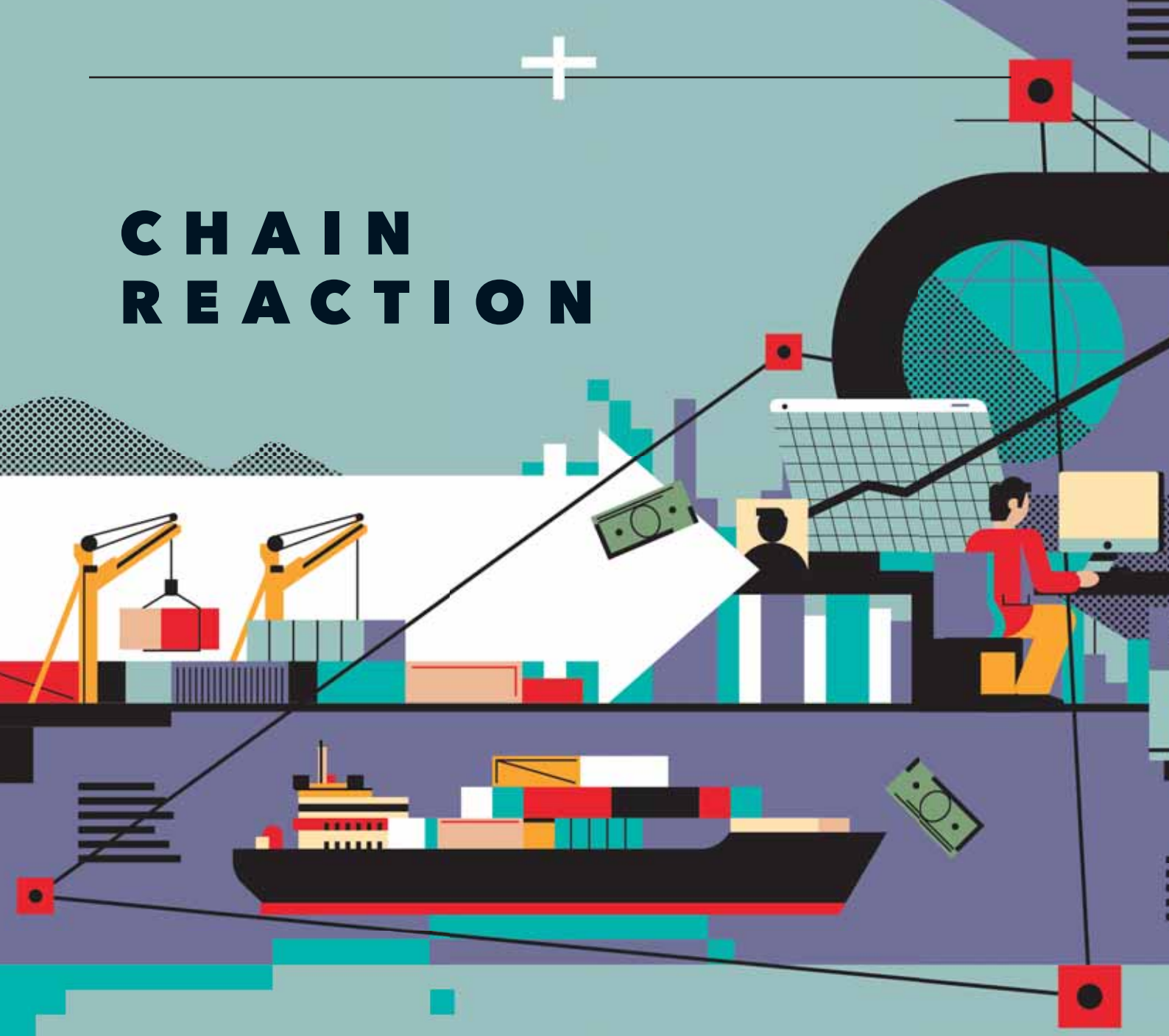
CHAIN REACTION



As businesses are becoming increasingly reliant on longer, more complex supply chains, the opportunities for fraud are increasing. Tim Philips looks at what can be done to prevent it

ILLUSTRATION BY ALEKSANDAR SAVIC

For 23 years, Rob Holmes, a private investigator at IP Cybercrime, has been travelling the world on behalf of multinational companies to investigate fraud. "The crimes never go away," he says, "but the medium changes."

In the 1990s, globalisation and the development of longer, more complex supply chains changed the scale and scope of crimes he investigated. Recently, Holmes investigated how organised criminals have been purchasing genuine goods and returning them for a refund. A footwear manufacturer hired him after discovering thousands of pairs of shoes that, according to its records, shouldn't have existed. The returns were fakes, only discovered by the retailer when the items were retagged and resold. "They were leaving the overseas warehouse early, before they were tagged for shipment," he says. "That happens a lot when you're dealing with a manufacturing supply chain. You're often dealing with a factory somewhere else that you don't know much about."

It's hard to accurately estimate the extent of supply chain fraud, not least because of the wide range of

crimes it encompasses. Kickbacks on raw material purchases, intellectual property theft, counterfeiting, fraudulent certificates of origin, quality assurance fraud, and inventory fraud are just a few. According to PwC, food fraud alone costs the global economy more than $40bn a year, which adds around $5 to the price of an average weekly shop. The extent of food fraud has pushed many retailers and suppliers to consider radical technology solutions, notably blockchain (see *Blockchain and Food*).

SPOT THE PROBLEM

In 2017, Deloitte surveyed 3,200 supply chain professionals in the US and found that three out of 10 had reported at least one instance of supply chain fraud in the last 12 months. If you have not found supply chain fraud in your organisation, this may not be good news as it may mean that you simply haven't found it yet. KPMG's 2016 survey, *Global Profiles of the Fraudster*, found that 61% of frauds benefited from weaknesses in internal controls that allowed the criminals to remain undetected. Additionally, two out of three frauds were done by, or were carried out with help from, employees who were able to exploit this lack of control.

"Supply chain fraud is not something that a firm would advertise, so we don't know the exact nature and extent of the crime," admits David Clarke, a director at the Fraud Advisory Panel, and group head of anti-corruption and due diligence services at Today Advisory. "Also, the reason the firms haven't got these controls is that they have put supply chain fraud in the too difficult tray."

Clarke admits that much of the supply chain fraud he has uncovered is "not Sherlock Holmes stuff". It ranged from contractors being added to the payroll; suppliers claiming to have shipped more goods than they have to hit target; fraudsters pretending to be existing suppliers and submitting fake invoices; and contracts being awarded to friends and relatives. One example was a case he investigated involving a fraudster impersonating a supplier. The fraudster convinced the supplier's accounts department to change its address and bank details, and supplied fake invoices for two years before being discovered. "It wasn't sophisticated. They were even using an out-of-date logo," he says.

Clarke points out that while all your employees, and the employees of your partners and suppliers, superficially have the same goal; many of them have the incentive to exploit lack of control and processes. He says that a clear statement that suppliers will be audited and a firm commitment to procurement standards and processes is the first step. You can introduce them alongside a temporary amnesty to help uncover existing problems.

"Just the fear of getting caught changes behaviour," he says. "I have investigated this all over the world and if you don't have the tone from the top, you get the scandals that we have seen in the last few years. If a leader says that they will not tolerate this, then we immediately see changes."

COUNT THE COST

Risk management firm Kroll has investigated many examples of supply chain fraud for its clients. Matthew Weitz, associate managing director in the firm's investigations and disputes practice, explains that in some boardrooms supply chain fraud may be accepted as a cost of doing business, especially if the supply chain is very long and international, where different standards may apply. The problem is that there is unquantifiable reputational risk too: for example, from tolerating poor working

61%

Number of frauds that benefited from weaknesses in internal control

"THE ORGANISATIONS THAT HAVE GOOD VISIBILITY ARE TWO-AND-A-HALF TIMES MORE LIKELY TO BE LEADING PROCUREMENT ORGANISATIONS THAN THE REST"

conditions or even modern slavery somewhere within the supply chain.

"Measuring the true cost of supply chain fraud can be a challenge, so assessing the prevalence of it can often only be done by measuring perceptions of fraud, which is not always the most reliable measure," Weitz says. "In some cases the revenue lost may not be material to the business, but the damage to the brand can potentially be devastating."

The fight against fraud will also be undermined if the entire organisation is not aligned against it. "There can be a disconnect sometimes between people in the business who are selling or buying, and people who are trying to keep the supply chain clean. So talk to the business leaders around the organisation and make sure you understand who they are dealing with. Use that knowledge to design your processes with the resources you have. Don't drive it from a textbook, your risk management must be driven by, and integrated with the business," he says.

Given alignment, what can businesses do to investigate potential fraud? A proportionate response, he explains, is to use some basic data analytics to investigate the information that the organisation holds, or can easily access.

"There is a vast universe of data both within your organisation and externally in the public record," he says. "But there is a risk of drowning in the noise from all this data. There's so much data it can be a challenge to standardise it in a way that means you can get something out of it. The best detection is crosschecking datasets against each other. Analysing payments to suppliers over time with a geographical split can be one tool in the box. But to be more effective, it should always be complemented by on-the-ground risk assessment, which allows the business to put the data in context, rather than analysing data in isolation."

On-the-ground assessment means going out and seeing if the data you hold matches reality. Weitz argues that putting a clause in any supplier contract that you have the right to perform an audit is a useful deterrent, even if it is rarely used. "Educate the supply chain about your culture. Ask the suppliers to treat their suppliers that way as well. The discussion is that this is the way you do business, rather than being a threat to come and check every transaction."

RISK MANAGEMENT

One of the problems in managing the fraud risk from a supply chain is that most organisations know little about the other companies that are in it. Deloitte's *2018 Global Procurement Officer Survey* found that 65% of procurement leaders had limited or no visibility beyond their tier 1 suppliers. Financial services, with their cultural emphasis on risk management, came out best – but a majority still had little visibility of their supply chain below immediate suppliers (55%).

Lance Younger, EMEA head of sourcing and procurement at Deloitte, and the author of the report, says this has two effects: it increases risk, but also prevents firms from innovating to improve the way their supply chains work. "The organisations that have good visibility are two-and-a-half times more likely to be leading procurement organisations than

the rest," he says. "If you're in automotive, for example, and you're getting 50% of your innovation from your supply chain, then procurement has a critical role to play."

The problem may be that procurement is seen as a policing role with a role focused primarily on cost. While this gatekeeping function will always be a goal, cost cutting can also stimulate fraud further down the supply chain. Balancing this with a procurement role as "an enabler and an accelerator" can help cut fraud, says Younger. This might be by creating a common standards process, such as a blockchain ledger, or creating a shared ethical commitment.

Uncovering and investigating supply chain fraud has dominated the risk management agenda. But creating a shared culture of integrity, and backing that up with technology, may one day stop fraud before it develops. "Ten years ago, organisations might say they would just sort out their own issues. In the last 18 months, we have seen a huge increase in the number of organisations using shared or managed services to control risk in the supply chain," Younger adds.

Meanwhile, Holmes is not short of supply chain frauds to investigate. "As long as there's a dishonest person in the world, I have work," he jokes. ●

65%

Amount of procurement leaders who had limited or no visibility beyond their tier 1 suppliers

BLOCKCHAIN AND FOOD FRAUD

In January 2013, the Food Safety Authority of Ireland, alerted to the fact that some of the beef products on sale in supermarkets weren't all they seemed, found that many supermarkets had been conned by their suppliers. A Tesco "Everyday Value" burger it tested was 29.1% horsemeat and contained traces of pork. The scandal, known colloquially as "Horsegate", was traced back to Silvercrest Foods in Ireland and Dalepak Hambleton in Yorkshire. Further tests found other suppliers equally guilty: Rangeland Foods and Freeza Meats beef were 75% and 80% equine, and a Findus Lasagne made in France contained 100% horsemeat.

Chris Elliott, a food specialist and professor at Queen's University Belfast, wrote the official report into Horsegate. He concluded that weak regulation created an "incentive for criminals to pursue food crime".

Food fraud is a global problem that illustrates how modern supply chains rely on trust, and how difficult it is to find out when that trust has been broken. It is a global problem: together, Interpol and Europol co-ordinated Operation Opson against food fraud. The latest wave of raids at the end of 2017 took place in 61 countries and seized €230m of fake products, from stock cubes to caviar.

Today, it is very hard for retailers or consumers to find out the provenance of their food. With a European office in Belfast, arc-net is one of a small number of start-ups using blockchain technology to change that. "Horsegate started us off," says arc-net CFO Barry Millar. "Given supply chain complexity, trust among participants is critical and that is a natural application for blockchain technology."

At each stage in the supply chain, arc-net's blockchain application captures the relevant data, which is then available to anyone who queries it. Because the shared, distributed blockchain ledger cannot be changed, the entire history of every single item in a supply chain travels with the item. Blockchain creates, in Millar's description, a "chain of custody".

An example is the application arc-net created for the Downstream craft brewery (down-stream.io). By pointing your smartphone camera at the QR code on the side of the bottle, you can learn when it was bottled, when the fermentation took place, at what temperature, for how long and who did it. Arc-net is working with Scotch whisky distillers on a similar application and is talking to dairy farmers who would like to know where their milk goes after they sell it.

For retailers, even the best current technology makes a problem almost impossible to trace to one supplier, or one batch. This means when there is a problem with a good, all stock has to be recalled or taken off shelves. In 2016, Walmart traced the origin of a mango. It took six days, 18 hours, and 26 minutes to trace back to the farm. Now, Walmart is trialling blockchain applications and tracing the same product takes two seconds.

For arc-net's application to work every link in a supply chain needs to update the blockchain and everyone involved needs to use it. "The technology is only one part of it," warns Millar. "It's mostly about process."