

[www.volumatic.com/stolen-knowledge](http://www.volumatic.com/stolen-knowledge)



STAFF

# Stolen Knowledge

Issue No 5

## *Insider fraud*

Is it the last taboo?

### The Cloud: what you must know

Our cyber-security guru answers your questions



### Streamlining the cash cycle

How Morrisons have made our oldest payment method the most efficient



### Online is golden

But multi-channel is forever for Reeds Jewelers



## Contents



### Insider fraud

Why we need to open up about employee theft

p3



### Streamlining cash

Bringing certainty to the cash cycle is great for retailers and their banks

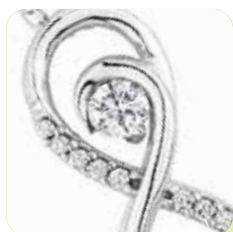
p6



### Morrisons and cash

Counting the benefits of new cash handling technology

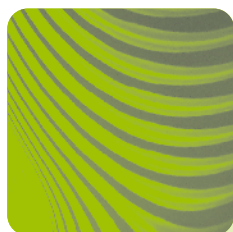
p8



### Multi-channel is forever

How Reeds Jewelers, and their customers, embraced multi-channel

p10



### Performance, performance

Big data can make a Chief Audit Executive's dream come true

p12



### What you must know about the Cloud

Clear thinking on Cloud Security from Neil Fisher

p13

## *A word from our sponsor...*

The material contained in this edition of Stolen Knowledge embraces thought and innovation beyond what might be described as historically the territory of the LP department. Today the business of loss prevention requires contributions from finance, operations, HR, IT and logistics departments as well as others like never before.

As businesses have developed their operations to offer their customers an omni-channel retail experience, criminals have been quick to exploit opportunities afforded by those new channels. As a result, the work of effective loss prevention now demands high levels of inter-departmental collaboration.

Furthermore, the recession has forced every retailer to look repeatedly at their operations, to see where savings can be made to protect their bottom line. Consequently "shrink" is no longer just about criminals and crime, but about streamlining processes and avoiding waste. To address these wider issues effectively, businesses are adopting a cross-functional approach.

I hope you enjoy this latest edition of Stolen Knowledge and the wider ambit of the material. The intention, as always, is to create debate, promote best practice and help the good guys to beat the bad guys.

### **James Harris**

Commercial Director, Volumatic Ltd

# *Insider fraud... the last taboo?*



*Are employees becoming less scrupulous about stealing from their organisation?  
Or are we finally just admitting that it happens...*

Phil Mullis is an experienced fraud professional, FCCA and Senior Statutory Auditor. He has investigated and reported on business frauds at all levels. He believes fraud would be better tackled if it were brought out in the open and discussed more in the workplace.

"Internal theft is, of course, embarrassing," he says. "It's like the last taboo to turn around and accuse your own people of theft."

But retailers have got customer theft on the run. "It is becoming harder and harder for customers to steal due to technical developments in CCTV, security tags and so on. But it's the employee who is around when the security is switched off. That's when things can go walkabout. Also cash, ringing up incorrect sales... There are more opportunities for employees. It can be low level across the whole organisation."

"Sometimes the cost of prevention outweighs the cost of theft. A certain level of theft can be almost

accepted. But unfortunately it sets the tone for the organisation. I come across it at all levels, people 'feathering their nest'."

"While we all like to think we have absolute moral standards, whether or not we choose to commit a crime is all about opportunity and whether we can justify it to ourselves", says Phil. "Tighter budgets at home and people feeling the pinch can make them less scrupulous."

## **So how do you press the reset button?**

What can you do in your organisation to reset standards of honesty? "When we are looking at higher level fraud in senior management and IT departments it can be helpful to brainstorm the matter amongst teams," Phil says. "Discuss how you would commit a crime. What do you think the opportunities and loopholes are in the system that allow it?"

**But it's the employee who is around when the security is switched off. That's when things can go walkabout. Also cash, ringing up incorrect sales...**

## Embed Fraud Risk awareness within your organisation

"You need to reset the tolerance levels, also make it easier for whistleblowing to take place."

"There needs to be more openness about the impact that even low level dishonesty has on the organisation - let's get everyone talking about it. It includes lack of opportunities for a pay rise, lack of trust among colleagues... it doesn't make for a great working environment. In the end everyone pays."

Phil Mullis



"After all, we talk openly about sales and how to boost them. We should be discussing losses and how we can do things differently. Because Health & Safety is a legal obligation, all employees are briefed on it regularly. Why not Fraud Risk? Employees are trained to spot customer fraud, after all. They should be similarly briefed and reminded about the company's Fraud Risk. It needs to be embedded in the organisation." <sup>sk</sup>

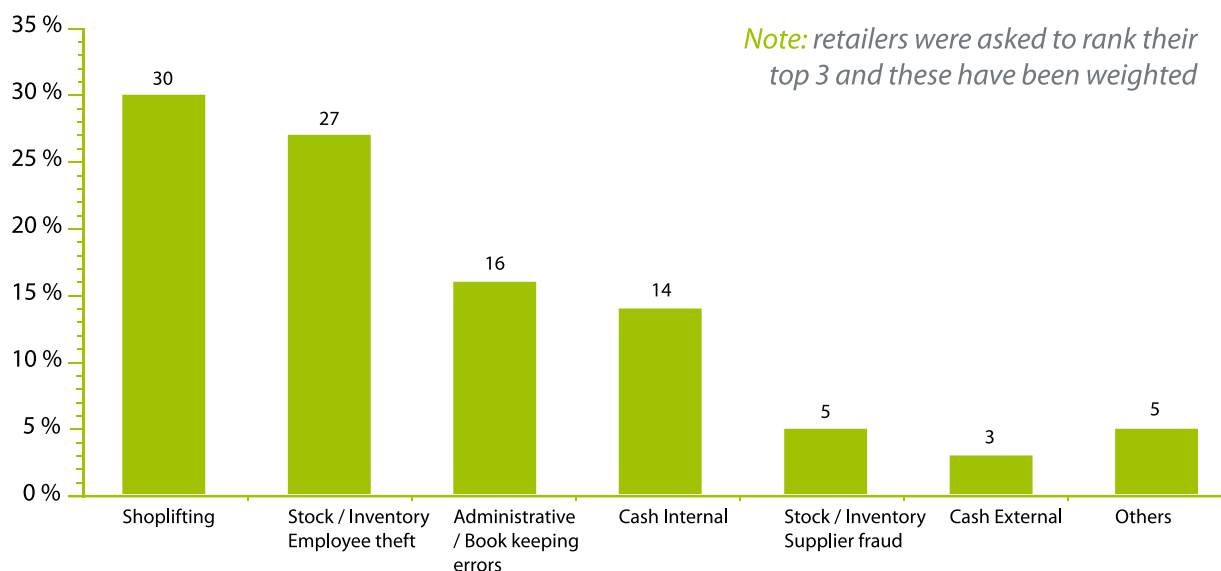
## US retail is upfront about insider theft

Dr. Read Hayes is the Crime Prevention Research Team Co-ordinator at the University of Florida, and Director of the retailer coalition Loss Prevention Research Council. He has conducted extensive research into insider fraud and is a co-creator of the theft triangle (motive to steal, opportunity to steal, low risk of detection).

"US studies indicate employee deviance is often the largest source of store loss, greater than customer theft. Culturally the US seems to be more willing to talk about it than in the UK. Our studies here are explicit about it and so maybe retailers are more desensitised!" Dr Hayes admits.

"Employers cannot afford to ignore this large-scale problem and should do everything in their power

% of retailers



### UK: Top Areas of Store Loss in the Business

*Note: retailers were asked to rank their top 3 and these have been weighted*

Source: The Volumatic Kount UK Retail Fraud Survey 2013



to create a workplace atmosphere that promotes honesty and encourages and rewards good behaviour. They need to make it clear that dishonest behaviour will be quickly detected and severely punished."

From deliberately damaging merchandise and marking it out of stock to colluding with suppliers, employee dishonesty can take many different forms. And while most often it can be out of need or desire, it is not always. "Committing crimes against an employer can also partially result from feelings of anger toward a supervisor, co-worker, or the company as a whole", Dr Hayes says.

In his work on insider fraud management, Dr Hayes recommends a rigorous system of diagnostics, prescription, testing and refinement. And, he says, employees generally welcome the 'zero tolerance' approach.

He cites recent research he has carried out with a major US theme park. "We carried out consultations among employees through focus groups in which employees say they prefer it if the organisation shines a light on the problem by rigorous monitoring techniques such as controls on cash registers. They don't feel uncomfortable about this. What they say they do feel uncomfortable about is the interrogation and investigations that have to be carried out when their employer does NOT properly detect dishonesty



using surveillance. They are aware that there are people in their midst who are stealing and would prefer that these individuals are identified and called to account." **SK**

**Read Hayes**, PhD has conducted independent research and consulting since 1984. He has over 30 years hands-on crime and loss control experience with Robinson's, Sears, JByron's and Ross Stores, and has provided loss prevention solutions to a large number of organisations across the US and globally.

## Comparing UK and US figures on insider theft

The Volumatic Kount UK Retail Fraud Survey 2013, which looks into the concerns of 100 of the UK's top retailers, has revealed that alongside online fraud and return fraud, internal theft is a major area of concern for retailers and the biggest area of store loss.

Concern about employee theft of stock has risen from 18% last year to 27% in 2013. While recognition that cash theft is a problem has increased from 11% to 14% this year.

Meanwhile, in the study's new North American counterpart, the Volumatic Kount US Retail Fraud Survey 2013, retailers are less reticent about the problem. Employee fraud comes out top with 37% of retailers reporting inventory theft by employees. In third place a fifth of retailers report cash losses through internal theft and then in fourth place is shoplifting with 13%. So internal losses count for the majority of fraud - 57% of the total in North America.

# Streamlining

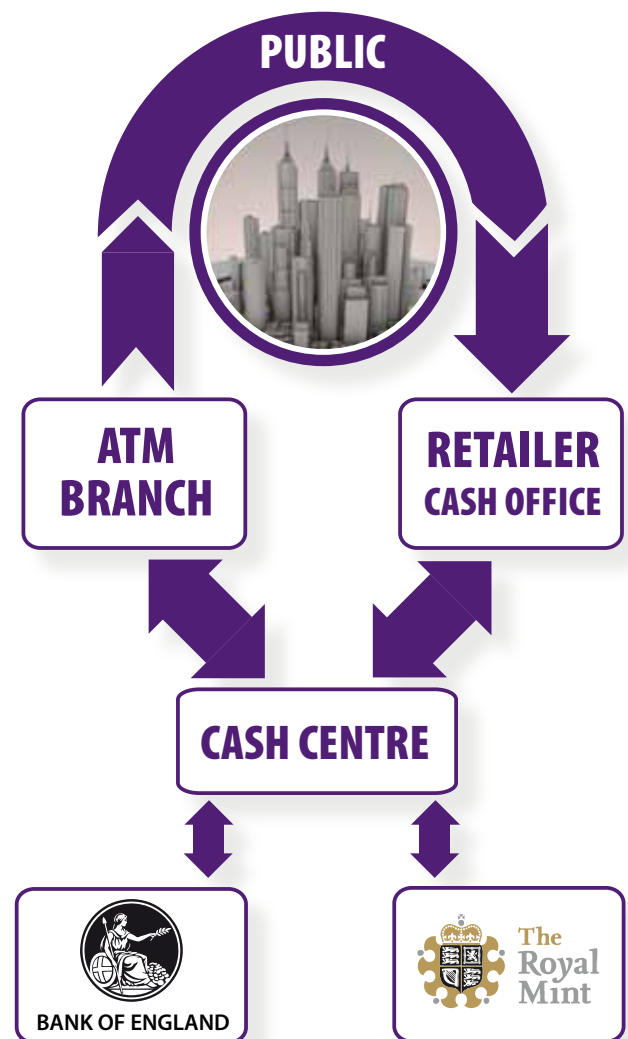
*Cash is still the cheapest and fastest method of transaction. How can retailers make the most of it? Ross Knight considers the emerging solutions that are ironing out some of the traditional drawbacks associated with managing large amounts of cash.*

Cash is alive and well. Despite almost constant claims to the contrary, the oldest, cheapest and most reliable payment mechanism still accounts for more than half of all retail transactions (BRC, 2012) – and the day we see a cashless high street feels as far away as taking a flying car to get there.

Indeed, the number of retail cash transactions increased by one billion from 2010 to 2012 (BRC, 2012), albeit with a reduced value as the profile of cash transactions continues to shift towards lower value purchases. Note and coin in circulation continues to rise, and the 44 million ATM users in the UK each withdraw an average of £360 per month (Payments Council, UK Payment Statistics 2013) – a large portion of which will go on to be spent in retailers.

This is good news – and not just for sentiment. Customers like cash and as well as being the most trusted payment, it is also the most cost effective for retailers. According to figures from the BRC, the cost of processing cash in 2012 was £81m, at an average 1.5p per transaction. Debit card transactions cost 9.4p, whilst those made using a credit card cost a staggering 38p. Doing some rough maths reveals that moving all cash transactions to debit cards would cost the industry an extra £426m a year – and moving to credit cards would cost an extra £2bn – an almost unbelievable 2,400% rise.

As well as being the cheapest, it's also much faster than the immediate alternative of the card payment. A difference of nine seconds per average transaction may not sound much, with 31 seconds for cash and 42 for card, but over an hour, week, month or year a cash-only till can make 28% more transactions than a card equivalent – critical at peak times.



Source: Vaultex

## The competition

So why would cash go? It's inescapably true that its share of the overall payments market is declining – with card usage continuing to steadily grow and mobile and contactless technology on the rise – but cash is not forecast to lose its place at the top of the payments tree until at least 2020, according to the Payments Council (UK Payment Statistics 2012), and the shift will be longer term in the retail market in particular.

# *the cash cycle*

The almost stereotypical demographic which has historically distrusted bank accounts and card payments is slowly shifting, and there is no doubt that the 47 million card holders in the UK are using their plastic more than ever, as even the smallest rural stores are installing chip and pin terminals. Credit and charge cards are not seeing the same growth, reflecting an increased consciousness of the risk of debt following the recent austere times.

With 32 million contactless cards in circulation (UK Cards Association, 2013) and over 40% of manned tills having the capability to accept them, contactless technology is undeniably on the rise – and both of these numbers are growing rapidly. A similar influx of mobile payments could be seen in the near future, as flagship smartphones are launched with pre-installed NFC chips and Visa prepares to launch its mobile payments application by the end of 2013 (Visa Europe, 2013).

And cheques? Whilst they still refuse to disappear completely, cheque usage dropped by 12.5% in 2012 (UK Payment Statistics, 2013). Despite the Payments Council's well-publicised reversal of its decision to phase out usage from 2018, the manual nature, fraud risk and clearing time is continuing the inexorable bounce of the cheque into the history books.

## **Cash USPs**

So in the face of a changing payments landscape in 2013, and some innovative and potentially game-changing technology, cash still has a part to play for the customer with selling points as robust as ever:

Anonymous, untraceable and completely transferable in a climate of distrust of banks and mega corporations, and their visibility of our lives

Universally accepted and available from any one of 66,000 ATMs plus countless businesses and branches

Payable for any amount, no upper or lower limits for spending

Independent of technology

Self-imposed spending control (you can't spend £15 if you only have £10 in your pocket)

As long as cash remains important to the customer, it's important to the retailer... but the differentials in cost of collection and transaction time sweeten the deal. All the facts show that cash payments are still critical to the customer – and it's no coincidence that many of the retail segments seeing significant growth presently, including value supermarkets and price-point retailers, are heavily dependent on cash usage.



It's clear, then, with usage stable and benefits clear to both retailer and customer, that the world still needs cash. The past 12 months has seen significant investment in enhancing technology from some of the high street's biggest names, and the question for retailers now is how to optimise the cash cycle, get cash in accounts quickly and minimise cost and risk.

### Cash challenges

Historically, there have been a number of core challenges which retailers face when dealing with cash:

**Forgeries:** a constant presence in any cash-issuing economy, forgeries range from the ridiculous to the sublime. Unfortunately, whilst many are detected at the POS, many more are found only at cash office, bank or cash centre level leading to a charge – direct or indirect – to the retailer.

Each and every element of the cash value chain is in a constant battle with the criminal production of forgeries, from technology updates and staff training to the design and manufacturing of the issuing bank's security features... and if the good guys were to ever

lose the upper hand, the results would devastate the economy.

**Resource:** counting, checking, balancing and reconciling multiple tills into prepared deposits is a time consuming activity which can demand specialist teams in medium stores upwards. Counting errors occur frequently and the resulting discrepancies may take days or longer to investigate and reconcile. As technology develops and links in this chain can be automated, retailers could see effective redeployment of staff into more revenue-generating positions.

**Security:** the holding of significant sums in tills and vaults on a retail site creates a risk to staff and customers of external theft, and creates a temptation – to a very small minority – of internal theft.

**Working capital:** as credit is harder to come by with a renewed sense of responsibility from financial

## Morrisons has employed in-store technology which removes the traditional drawbacks of handling cash

Transaction for transaction, cash is cheaper and quicker than plastic. But a somewhat slow and clunky cash cycle has, until now, diminished its benefits for retailers.

In a supermarket, with cash being handled typically by a dozen people in-store before it is banked, the cash counting process has been cumbersome and with an element of risk. Any discrepancies identified by the bank are therefore usually laid at the door of the retailer who bears the loss. And there has been the (until now) inevitable time lag while value of the cash taken is credited to the retailer by the bank.



Morrisons this year caused a stir by adopting new cash counting technology which, in a stroke, banished these drawbacks.

Called CounterCache™ Intelligent, or CCI, the system counts and validates cash with 100% accuracy, eliminating forgery, discrepancies and staff involvement after the cashier. The money goes straight into



institutions, organisations need to make their money work quicker, with many cash cycle models taking at least two days to give the customer credit from collection.

**Wastage:** with fixed Cash In Transit (CIT) scheduling, cash collections and deliveries are often not used to their full potential – particularly when considering ATM replenishments. In a utopian, just-in-time world, cash would be collected just before the vault or insurance limit is reached, and delivered just before peak sales time (or just as the ATM is emptying). The technology and infrastructure is not currently in place for dynamic CIT scheduling, and as a result retailers waste millions each year through sub-optimal collections.

**Visibility:** in the past, there has been no sight of a client's cash from the moment it's collected up until credit. At any one time, a large retailer may have several millions of pounds sitting on neither its premises

nor its balance sheet. Of course, in most cases there is no need for any increased visibility, but in cases of shortages and significant forgeries, conflicts could easily arise between client, CIT, cash processor and bank.

**Flexibility:** similarly, it was typical for retailer's cash to be collected, processed and credited as per the standards set by the providers – not the retailers. The guidelines on presentation of cash and paperwork create a resource-hungry task – resource which again could be used to generate further sales for the business.

### Emerging Solutions

To manage some of these challenges, the cash industry is using developments in technology to implement a range of solutions.

"Intelligent" tills and safes have been available for

# *Morrisons and cash*

pouches, which are sealed and tamper-evident. 'Back end' software displays the figures and this information drives the bank's figures.

We wanted better visibility of cash... We decided to look at technology and the relationship with our bank," says Malcolm Mackie, Retail Improvement Manager at Morrisons. "We had looked at all areas where we can control cost... it was only cash handling left! We are a customer focused retailer. We want our staff at the frontline with customers, not counting cash."

"We trialled the system extensively, to prove that we could eradicate mistakes and to prove that we could reduce labour and refocus. We wanted a local level of control too", Malcolm says.

Having satisfied themselves that the CCI ticked all these boxes for them, Morrison rolled the system out to 10,000 points of sale.

The benefits of this greater visibility of cash are evident across the entire cash supply chain and Morrisons use of CCI is praised by their cash processing company Vaultex and bank, Barclays.

Sameer Dubey of Barclays: "I must congratulate Morrisons on this first large-scale implementation of the technology in the UK. Other retailers will go this way."

He is echoed by Mark Trevor of Vaultex: "It is beneficial to the industry as a whole, by reducing the cost of transactions."

a number of years, but have only recently seen the tipping point of benefits outweighing investment. The features offered vary broadly between devices, but can typically link with the POS to automate counting, recording transactions on a network to remove in an instant the manual end of day cashing up process. Cash is held in a secure, tamper-proof pouch or bag and forgeries are detected on receipt – removing two of the costliest risks in the supply chain.

Each transaction recorded can automatically be uploaded to a central database, where it can be viewed by management at company, region, store, shift or till level. With the right integration, this could be matched to CIT and processing data to provide a single data warehouse for all cash information, with drill-down, dynamic MI for speedy analysis and query resolution – all available to customers through a portal solution.

Early value, or provisional credit, has been offered by the cash industry based on a percentage of forecasted deposits, but the technology also exists to offer credit based on the deposits known to have been taken by a device. Through either mechanism, the retailer sees an increase in working capital and a decrease in the funding costs of cash held on the balance sheet.

It's through enhancements like these and others, in the reporting, crediting, counting and holding of retail cash, that the cash cycle can work more efficiently than ever.

### Summary

Despite its many challengers and its imperfect nature, the benefits to both seller and buyer are strong enough to keep cash as a key component of retail payment for many years to come.

The same issues which have always affected cash remain, amplified by the recession – but mitigated by developments within the industry which can offer retailers significant long-term savings through new products and solutions. So, in a changing world of ever-new technology and payments to match, only one thing is certain: cash is here to stay. **Sk**

**Ross Knight is Product Development and Marketing Manager at Vaultex UK Ltd**



**For US jewellers**  
Reeds, the benefits of going multi-channel have fulfilled all expectations and business is booming. Mark de Causmeaker, Director of Multi-channel Sales at Reeds Jewelers, told Stolen Knowledge about their journey to multi-channel.

Reeds Jewelers is a family-owned jeweller based in the US with thriving e-commerce, catalogue, and bricks-and-mortar operations. They've been trading online since 2001 but full integration between stores and online came with the launch of their 'direct to customer' programme two and a half years ago. It's worked wonders for the business.

"We have a standard e-commerce platform which stands alone, and also our bricks and mortar stores", Mark explains. "It wasn't until around two and a half years ago when Reeds implemented its 'direct to customer' programme that the internet was effectively brought in store. Our sales associates have embraced the 'direct to customer' programme because our multi-channel offering means we are able to operate a never out of stock policy."

"'Direct to customer' means that if a customer wishes to purchase a piece of jewellery not available in store they are still able to purchase the piece there and then and have it shipped directly to their home, very often by the next day. This is done via our in-store iPads which work on our e-commerce platform."

### The 'multi-channel feel'

"Having this 'multi-channel feel' to our business offers yet further benefits though – a good example is our family jewellery which includes a choice of stone and often engravings. What our multi-channel process allows us to do is to allow a customer to be in store, look at the stones and the physical pieces of jewellery and then, when it comes to the building of the piece to their specifications and getting the engraving right, our sales associates are able to help them through the process on the iPad. This allows them to try different things out on the screen with the benefit of the expertise and advice of our sales associates in store. Plus there are the full benefits of the e-commerce aftersales process: order confirmation, tracking and shipping details all via email – they also can sign up for our newsletter. It really offers us the best of both worlds."

# Online is golden but multi-channel is forever



## The business benefits

"As well as the increased sales opportunities and superior customer experience offered by this approach, there are also significant cost benefits to us as a business," Mark explains. If you have the option of integrating a hugely expensive EPOS system or adopting a similar approach to us - which involves the purchase of a handful of iPads allowing access to our e-commerce platform - it is a no-brainer really! And perfect for SMEs, also, I would imagine. "The cost benefit of iPads with our sales associates versus a fully-integrated POS solution will be increasingly important as leases or contracts run out on the systems in place today with retailers."

## Fraud prevention

Installing the correct technology to enable true information sharing underpins the multi-channel process. "We'd been operating a multi-channel approach to profit protection since we went online 12 years ago. In that time there was a certain amount of intelligence sharing, but there was no technology implemented and a lot of manual labour in reviews, etc., was required."

"With our 'direct to customer' programme we implemented Kount's online fraud prevention technology which enabled us to do all this."

## Advice for those embarking on multi-channel

"Always do what works best for you. But always work with experts. Choose people who have a similar business ethos to you. For me it is all about partners and we found a partner against fraud in Kount. Reeds prides itself on serving the customer above and beyond the call of duty. In the same way we got this from Kount, the sales team there were more than just a fraud tool sales team but problem solvers, too."

"And, be ready to listen... for the relationship to work it is not just about employing the experts, you have to listen, process and act upon any intelligence in front of you."

## The future of multi-channel

And what about the future of multi-channel? "The future of this sort of approach is not an overnight boom, it will be gradual and may take 15 years. The benefits we have seen mean that this style of trading cannot be ignored. In the first year of integrating this 'direct to customer' programme and using Kount we saw a reduction in bad debt by 35%, with an additional 10% reduction over the last year and still counting... So we are thrilled from that perspective", Mark says.

"The automation of the fraud prevention process has freed up time which was otherwise taken up manually reviewing our orders. This is down by 90% compared to before the implementation of this solution. And the multi-channel approach means that these benefits have been stretched into our bricks and mortar offering too." **Sk**

# PERFORMANCE, PERFORMANCE, PERFORMANCE



Continuous auditing using Big Data is a powerful tool to control shrink, before it happens, says Orlando Sousa, Chief Audit Executive of Portuguese retail giant the Sonae Group.

Sonae has 1000 stores across Europe and the Middle East, spanning grocery, consumer electronics and sporting goods, and generating more than 5 billion euros in revenue annually. The Group has moved from a traditional audit process to one of continuous auditing with remarkable success says Orlando Sousa.

28% of global PLCs that failed over the past 36 months are reported to have failed due to operational factors that could have been under control of the organisation, ranging from cost overrun and supply chain issues to employee issues, including fraud

## A whole organisation approach

Continuous 'systemic' auditing involves the whole organisation, scrutinises every form of loss to the business – and, crucially, operates in real time exposing weaknesses as they arise. "This contrasts with the reactive approach of traditional auditing", he says.

"Retail is characterised by a huge volume of transaction data. Today we have the technologies (hardware and software) and skills to audit this volume of information on a continuous basis. With continuous auditing, Internal Audit has been evolving from reactive to a proactive approach regarding fraud prevention."

## Fraud prevention

He cites the example of returns monitoring: the system monitors for the incidence of multiple returns with the same receipt. "If there is more than one return for the same receipt we get an alarm. Analysing the detail we can identify the stores and items involved."

## The challenges

Orlando does not deny there are huge organisational challenges in making this happen, including:

- Complexity of the business environment
- Inadequate business processes design
- IT Architecture (lack of integration)
- Data Quality (no unique key, no consistent naming convention, spelling errors, missing values, data in wrong fields, data cleansing...)
- Lack of skills and knowledge for effective use of technology

## Do we have a choice?

Yet overcoming these challenges is vital in today's complex business environment. "28% of global PLCs that failed over the past 36 months are reported to have failed due to operational factors that could have been under control of the organisation, ranging from cost overrun and supply chain issues to employee issues, including fraud", says retail business transformation specialist Ana Cunha who has worked with Sonae.

## A positive culture of efficiency

Sonae's Store Operations are delighted with the results of the transformation program, Orlando says. Store associates feel proud of what they have achieved with stores being run at a very high standard of efficiency. People are encouraged to contribute with ideas on a daily basis. Often ideas are simple and drive an improvement towards a simpler process. Once tried and tested in one store, the idea is shared for the benefit of other stores. **SK**

## Stable doors and horses

**Auditing in real time draws on Big Data and demands cross functional co-operation to achieve new levels of scrutiny and efficiency.**

» Auditing large quantities of data in real or near-real time and then establishing a workflow to ensure that critical information reaches the right person and provides metrics during the follow up and closeout of cases.

» Providing a continuous sequence of snapshots of the retail business processes, showing exactly how the core systems are performing and exactly what to do about them in a process view. It makes the bridge between the way things should be done and the way things are actually done.

» When irregularities are found, workflow functionalities will be fundamental to assure case resolution. In cases of fraud, it is critical that an immediate action plan or special audit be conducted with the support of the legal department.



# What you *MUST* know about the Cloud

*We spoke to cyber-security guru Neil Fisher.*

*The Cloud is, of course, a Great Thing. We are moving our data and processes into it, transforming the way we do business. But how much do those of us outside IT departments really know about it? And how safe is it?*

## *Let's cut to the chase: is it safe?*

Neil This is the major question. The Cloud has been talked about since the beginning of the internet but it was too easy to lose data to the bad guys. The three questions to ask are: Where is my data (mainly for State jurisdiction over access), is my data protected (in transit as well as at rest in the server, wherever that may be) and who has access to my data (should only be you and whoever the company rules allows). Hence data location, data encryption and identity management and access control become the big issues for a safe and secure Cloud.

## *What should I know about encryption?*

Neil This is the trouble with IT – Information Technology. It's been designed by technologists for technologists. Hence it uses a lot of jargon that the ordinary user doesn't understand. Encryption is just a way to keep the data safe, secure and unable to be read unless it recognises who the right recipient is. You don't need to know how it is done, just that it is done. Common three letter acronyms that have entered the lexicon would be SSL (used a lot on the internet and gives low level protection), PKI which gives a much higher level of protection.

## *What should I know about Identity Management?*

Neil Identity Management is the main key to a safe and secure use of the Cloud, along with encryption. Once you know that the data that you send and where it rests is protected, then the next step is to ensure only those with the right permission can access it.

Identity Management has two main stages; enrolment and then authentication. Enrolment is when you register

Neil Fisher has a background in military cyber-security and counter terrorism at the UK MoD and is now VP Global Security at Unisys.




to use a service – could be just accessing company data. Authentication happens when you actually try to access that data. The simplest level of authentication is the username and password. This is a basic level of authentication called 'Something You Know'. For ordinary, low value data it is good enough but not for higher value data such as accessing your bank account. For that you would need at a minimum a second level of authentication as well – 'Something You Know' along with 'Something You Have'. The 'Something You Have' may well be a company access card or a bank's smart card – two things that, on their own, can't gain access but can when they come together. This also means that you don't have to remember lots of different passwords – the same personal credentials can be used to access all Cloud services.

Many Identity Management systems in use in the Cloud use this and you will hear them referred to as Federated Identity Management, or Single Sign On (SSO). Having a strong Identity Management system means the same system can also be used for access to the physical world – so using the same authentication for entering a building or going through certain doors. There is a third level of authentication which is 'Something You Are', known also as a biometric such as a finger print, a face or iris pattern recognition. This was used usually for high value or high risk transactions where there had to be almost no doubt over who the user was. Now technology, with cameras and touch screens on mobile devices, is making biometrics a preferred way of authenticating because it is quick, easy, doesn't need a password and is very strong from a security point of view.

## *What should I be worried about?*

Neil From an individual point of view be worried about how your data moves through the network – is it protected? Worry about the protection of your "End Point" – the technical term used to describe the platform you access your



data on – could be a laptop, desk top, mobile phone, iPad. If you lose it and you haven't protected access – through a strong second or third level authentication process – you may lose everything. And back up your important data onto an accessible storage device – there are plenty

## CLOUD JARGON-BUSTER

SaaS? IaaS? Waas? Explain the jargon.

“aaS” is invariably “as a Service” since everything in the Cloud will be accessed by you as a service to you. It may be the use of software – Software as a Service (SaaS), or actual infrastructure (think a telco providing connectivity as you need it as you expand ((or contract!)) as a business), Infrastructure as a Service (IaaS). It may be the whole working experience accessed in the Cloud as described above but provided not to you as an individual but to your whole business, wherever it is, whenever it needs to be – this would be Workspace as a Service (WaaS).

PaaS is Platform as a Service which could be the functionality of a sophisticated laptop brought to, say, your iPad – think of those online calculator apps for smart phones and tablets which can be as sophisticated as you want for hardly any money and compare to the cost of a Texas Instrument or HP calculator that was the “must have” appliance for exams when I was at school. Now scale that up for entire businesses. This is the sort of transformation happening now and why life in the Cloud, provided it is safe and secure, is utterly and compellingly exciting.


around or use the Cloud again to backup. I was burgled last year and lost my iMac which had all my photos on it. The iMac was well protected so I wasn't worried about the thieves hacking in and the insurance company replaced the device within the week. Fortunately I had backed up all my Office documents onto a separate storage device (one of those terabyte eBook things) and all my email and photos were backed up in the Cloud. They were still there when I activated the new machine.

### *What other questions should I be asking a Cloud provider?*

Neil Ask them where their data centres are. UK and Germany are good places to have them. Ask them how do they backup your data – what are their Business Continuity/Disaster Recovery plans? How often do they practice them? If you are a business ask them about Identity Management – actually it will be evident how much care they take over this by the way they ask you to authenticate. Ask them how they protect your data at rest and especially in motion. Amazon Web Services (AWS) is a good example. They provide Cloud Services. They can create a working space for you that looks and feels as if it is in your computer, but actually it is in their many servers around the world (joined together by the internet and the speed of light). They use second level authentication and your data can be protected by Unisys STEALTH encryption system. Once setup you have the confidence to know that, even if you are burgled or lose your “End Point”, the data hasn't been compromised or lost as well.

### *What about other products that say they are ‘using the Cloud’ – how do I check these out?*

Neil Check out which ‘Cloud’ they are talking about. If it sounds as if it is too good to be true then it probably is. Use the three security questions above – where is the datacentre, what is the Identity Management system, is the data protected and how? Do shop around and compare with established and trusted services such as AWS. **Sk**



Life in the Cloud, provided it is safe and secure, is utterly and compellingly exciting

# What is the Cloud?

Using the Cloud, putting data and processes into the Cloud, means that you have removed the hardware and software you used to own and had to buy for yourself and are now using computers and servers that don't belong to you but you can access through a low cost communication medium such as the internet. Smart phones and tablets such as iPad have revolutionised this aspect making the Cloud an irresistible way of conducting all business; personal, private or public.

## *Where is it?*

Anywhere and everywhere would be a flippant answer. For some big companies – say a global corporate that spans several countries – they have probably consolidated all their private infrastructure and servers into one location and, as an employee, you access them as if they still were located in the IT room in the basement of the building. This would be what is called a Private Cloud. In the email example above, as a private individual, you would be accessing your email through a Public Cloud since it uses the internet. Some companies use a bit of both and this is called a Hybrid Cloud. Where the servers and data centre is located is important since the data that resides on those servers will be subject to the laws of the country that the data centre is located in.

## *Why do people keep putting things in it?*

If you don't need to own the hardware – the servers and data centres – and only need to lease a service or disc space as and when you need it the cost of doing business is dramatically reduced. And the flexibility the Cloud provides transforms the way business can be conducted. If you understand this you will undergo an epiphany that questions, for instance, why you commute to work every day when you could just as easily work from wherever you are and save journey time and cost.

## *How do I know if my company information is now in the Cloud?*

Ask your IT manager. The chances are that some low risk or low level transaction services have been moved to the Cloud but some important and business critical functions have been retained under the control of your company. Hence payroll and HR functions are often the first to go, as are CRM functions (from a company owned Siebel CRM licence to a Cloud provided Salesforce.com licence) but you may have retained control of the development of Intellectual Property, sales figures, merger and acquisition plans and so on.





# Take the “handling” **out** of your cash handling process...

From the moment a till operator accepts a note and feeds it into CCI, **nobody** touches that note again until it is received by the bank.

The mere action of feeding the note into the CCI sees it validated, counted, stacked and secured in a tamper evident pouch.

- ▼ Billions validated over 4 years - zero errors
- ▼ Stops forgeries dead
- ▼ Cut operational costs by as much as 75%

