TenInsight

TenIntelligence

www.tenintel.com | January 2018 | Issue 2

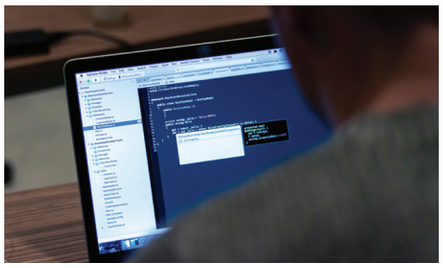
Insight from the top

As we consider what 2018 will bring, one thing we know for certain is the implementation of the new Europe-wide General Data Protection Regulations (GDPR). If you have not heard of it, or started your internal audit process, then you have until May this year to meet the GDPR.

The legislation is clear and concise, introducing new procedures and tougher rules on how personal information must be handled and protected.

It carries substantial financial penalties for non-compliance. But where do you start? The Information Commissioner's Office is an excellent resource, highlighting the key changes.

Assess your current policies, identify where your organisation keeps and processes personal information and look for gaps in your data protection compliance.



In November 2017, TenIntelligence appointed former Transport for London Chief Information Security Officer, Richard Bell, to head up our Security & Privacy Division. In this pivotal leadership position, Richard is responsible for supporting clients with security risk and compliance consulting services on GDPR, privacy and security planning, reviews and audits. Contact us if you need help starting your GDPR preparations.

In this edition of TenInsight we also examine the use of Industry Insight in due diligence investigations; providing clients with real insight into an individual's professional character and background.

Cate Wells, our Managing Director in Dubai, also shares some recent anti-counterfeiting investigations, successes and brand protection news from our UAE Office.

Neil Miller
CEO, Ten Intelligence Limited

Cyber Security, GDPR, Incident Response - You and Your Business

1 March 2018: 09.00

Venue: 80 Churchill Square, Kings Hill, Kent, ME19 4YU

Agenda includes networking, presentations and a Q&A session

Search 'eventbrite TenIntelligence' to book your FREE ticket.

Industry Insight: Providing a new level of Due Diligence

We have recently seen a substantial increase in requests for Industry Insight research and interviews complementing our background checks and due diligence. The driving force behind this seems to be an increase in regulatory requirements and scrutiny as well as "good governance". A large proportion of the Industry Insight interviews we conduct are in relation to senior executive hires or directors of listed companies; as well as listed companies themselves.

But what does Industry Insight entail and why is it such a vital part of enhanced due diligence? Industry Insight is a qualitative research tool that complements and adds value to quantitative data and information in respect of individuals, entities and markets. It provides clients with deepened understanding and valuable context in respect of people, entities, and events/circumstances. It is especially valuable when trying to capture sensitive or adverse information; such as previous litigation and bankruptcy.

Conducting Industry Insight interviews requires skill and a great deal of preparation, including full and proper background research to enable the interviewer to gain maximum benefit. To obtain quality responses the interviewer needs to know when and how to adapt lines of questioning or probe for further information or explanations.

A standard list of questions is not sufficient.

It is also important the credibility and relevance of the interviewee is thoroughly researched beforehand.

The interviews can be face-to-face, although telephone interviews are more common as they are more time/cost effective and not restricted geographically.

In most cases the individual will consent. However, in light of the new GDPR provisions, where an imbalance of power exists, this needs to be carefully considered. Discreet or covert interviews can also be conducted, when required.

GDPR – Get Data Privacy Ready!

With the introduction of the most comprehensive Europe-wide data privacy legislation to date in the form of the General Data Protection Regulations (GDPR) that come into effect on 25 May 2018, the main question in most business owners' minds is "are we ready"?

This legislation replaces most of the provisions of the UK's Data Protection Act 1998 (DPA) and other local data protection laws across the EU. Yes, it is a game changer; no, we shouldn't fear it.

GDPR is designed to give individuals greater and better control over their personal data, establishing a single set of rules across Europe. It also finally provides organisations with a concise approach to managing, processing and protecting personal data.

The continued and unstoppable growth of cybercrime means organisations of all sizes need to rethink their approach to the security of information and data. Thinking you are 'too big or too small' to suffer a data breach or hack isn't enough and GDPR is a timely reminder of how important it is. Did you know at least 60% of small businesses never recover after a serious data breach or cyber-attack? Everyone knows the importance of staying safe and secure in a digital world; under GDPR the consequences of a breach could result in fines of up to 4% of annual turnover.

Attacks are becoming increasingly more sophisticated and stealthy, targeting people, networks and devices. There are many questions you should be asking yourself now, but to start: Do you know where your data is? Do you meet your legal obligations, including the new GDPR, to keep data secure? Do you have a breach response plan?

With the introduction of our new Security & Privacy Division at TenIntelligence, our primary focus is to help businesses be resilient, to protect themselves and their customers and to swiftly recover and resume operations if an attack or breach is suffered.

For more information on GDPR, please visit www.tenintel.com/audit-assessment/

GDPR – the basics:

- **GDPR introduces greater rights and choice for individuals, while imposing tighter controls and requirements on data controllers and processors.**
- **GDPR has world-wide application. It will cover all organisations, wherever located, which hold or process personal data of EU citizens.**
- **Brexit will not affect the application of GDPR in the UK.**
- **GDPR broadens the definition of 'personal data' to include, inter alia, web-based identifiers and IP addresses.**
- **It will introduce much stricter rules for obtaining valid consent from data subjects.**
- **Newly introduced, mandatory Privacy Impact Assessments will have to be conducted by organisations.**
- **Organisations will be required to apply the principle of 'Privacy by Design' to all their processes and systems.**
- **Data subjects will acquire a new 'Right to be Forgotten'.**
- **Data Breaches will have to be reported to the relevant authority within 72 hours of an organisation discovering a breach.**
- **Penalties are hefty and substantial – it could amount to the greater of 4% of an organisation's annual worldwide turnover or €20million.**

Insights from th

As always, the conference provided invaluable insights into current fraud trends as well as prevention initiatives and activities by government, law enforcement and the private sector. It is evident that the partnership between these bodies in combatting fraud is growing and strengthening.

City of London Police Update

Commissioner Ian Dyson highlighted three significant things that are affecting the fraud landscape in the UK: The Crime Survey for England and Wales, the Joint Fraud Taskforce and the National Cyber Security Centre.

It was interesting to note that according to the Crime Survey (an independent survey accepted by the Office for National Statistics), fraud and cybercrime now make up approximately half of crime in the UK. Commissioner Dyson also commented that the Joint Fraud Taskforce is growing in capacity.

The launch of the Banking Protocol to protect vulnerable people has seen a good response and is now live in around 35 forces across the UK. The Taskforce is now setting its sights on "cardholder not present" fraud. He concluded by saying the National Cyber Security Centre shows the government is serious about cybercrime.

Action Fraud, run by the City of London Police, also has a new system coming in that will make it better and easier for users to report crime.

Cybercrime

Mike Hulett of the National Cyber Crime Unit, part of the National Crime Agency, gave some interesting statistics: 47.5% of all UK crime involves cyber and 68% of large UK businesses had identified a cyber security breach or attack in the past 12 months. He cited the UK's sophisticated internet infrastructure as the main attraction for online business, luring in cyber criminals and fraudsters.

Mr Hulett explained the 4P approach in tackling cybercrime: Pursue, Prevent,

he London Fraud Forum Conference 2017

Protect and Prepare. Regarding prevention, it was both interesting and alarming to learn that boys between the ages of 11 and 14 are perpetrators and continue to be a specific focus group. Mr Hulett touched on the different types of cyber attacks and gave tips on how to manage risk. He emphasised this involves the whole business, not just the IT department, and that processes, systems and people, should be continually evaluated.

The London Digital Security Centre

Jon Unsworth, Chief Executive of the London Digital Security Centre (LDSC), gave an overview of how they are helping SMEs in London to operate and grow their businesses online in a secure digital environment. Membership is free and the LDSC delivers masterclasses, workshops, consultations and digital security clinics across London. They also provide affordable and appropriate products for SMEs.

General Data Protection Regulations (GDPR)

Keith Dewey of DataGRC, provided an overview of the key requirements of GDPR, with a specific focus on the implications for anti-fraud practitioners. He simplified it by stating that GDPR is "basic privacy" and a regulation for "decent behaviour", adding that businesses should not process data unnecessarily or against the will of an individual. Unfortunately, the provisions of GDPR read far less simply. In addition, businesses in the UK will have to contend with the new Data Protection Bill currently going through Parliament, which will add addendums to the GDPR.

For fraud prevention, the provisions of GDPR Article 32 ("Security of Processing"), set measures which will assist, including "pseudonymisation and encryption of personal data" and the implementation of "appropriate technical and organisational measures". More generally, for a business to have a defensible position under GDPR, it must be able to demonstrate it has adequate governance, legal agreements, data management processes and privacy operations (including data subject access rights) in place.

Article 6 sets out the requirements for lawful processing of personal data. Where consent of the data subject is absent, specifically in covert investigations, fraud investigators may have to satisfy the "legitimate interests" criteria, i.e. that the processing is necessary for purposes of a legitimate interest – it is thought a fraud investigator relying on this criteria will have to show that the processing of the personal data was strictly necessary for purposes of "preventing fraud". It is, however, not yet clear whether this extends to the "detection and investigation" of fraud.

Mr Dewey stressed the importance of documenting all processes relating to data; including how it is collected, where it is stored and how consent is obtained. Privacy and consent statements also form part of the evidentiary paper trail. Agreements with clients, customers and third parties are key.

Forensic Linguistics and Fraud

Dr Kate Haworth, of the Centre for Forensic Linguistics at Aston University, presented a case for the inclusion of forensic linguistics in fraud investigations. Dr Haworth asserted that language is a key element in almost any fraudulent endeavor, as it is used to impersonate, persuade or deceive.

One technique of forensic linguistics, which has proved useful in fraud cases, is forensic authorship analysis. This involves analysing language and punctuation use, spelling variations and other linguistic differences to distinguish the most likely author of a disputed text among a small number of suspects.

Dr Haworth also encouraged the intelligent use of language when interviewing suspects. She recommended the use of the PEACE framework (Planning and Preparation; Engage and Explain; Account clarification and challenge; Closure; Evaluation). This technique involves forming a rapport with the interviewee; explaining the reasons for the interview; listening; probing for details and verifiable information; challenging inconsistencies and asking for explanations; repeating until closure; and, finally, evaluating the information. Avoiding restriction and coercion is important, particularly when working with law enforcement. Keep questions open-ended and be aware of the function of the language you use.

The Kweku Adoboli Rogue Trader Case: The Investigating Officer's Perspective

Detective Sergeant Paul Curtis gave his account of the rapid investigation involving Kweku Adoboli, a former trader at UBS who lost $2 billion as a result of unauthorised trading.

DS Curtis' team was thrown into a complex case involving technical trading methods. In just a few hours, his team was forced to learn the intricacies of Adoboli's fraud. DS Curtis explained that fraud investigations have three areas of focus: material, assets, and people. His team had to work quickly to understand these.

In the end, Adoboli owned up and was convicted. The fallout was catastrophic for UBS. DS Curtis emphasised the necessity for strong internal controls, particularly in financial markets. Adoboli had been able to run his fraudulent trades without supervision, and when the first alert of losses came in, passed it off as a delayed return, before only doubling down on his fraud and making the situation worse. His fraud could have been easily prevented.

Updates from our Dubai office

Brand Owner's inaugural case for seizing diverted medical devices in the UAE

TenIntelligence's Brand Protection Team in Dubai recently completed a significant instruction for a multinational medical devices and pharmaceutical client, regarding the sale of diverted medical devices.

Diverted products can be described as the "practice in which genuine products intended for a particular market are diverted and sold in another, usually without the knowledge or permission of the brand owner".

What's the problem with original products being diverted?

When products are diverted to another jurisdiction, other than where they were originally intended, there is no "control" on how they are stored and handled.

Consider the impact of medical devices which may be affected by temperature, for example. What would the effect be to a medical device when exposed to high temperatures? Would the device work or would it have serious health and safety implications or repercussions? Who would be to blame if a patient used the product and it didn't work or caused a serious health problem – the retailer or the brand owner?

By performing due diligence, conducting site visits and making purchases of their branded products (which were not for sale directly in the shop), the client was able to thoroughly examine the packaging and cross check all reference numbers to confirm the products had been diverted.

Although the medical devices were original, they did not comply with local legislation, (GSO: 1943:2016).

With evidence provided and samples secured by our team, information was passed to a local law enforcement authority (Dubai Economic Department) and a complaint filed against the trader. The inspectors thoroughly checked the premises (and the secret storage area identified by our team), resulting in the seizure of approximately 240 boxes.

All cases are important; however, this was especially significant as it was the first time the brand owner filed a complaint in the UAE in relation to diverted products. It was also TenIntelligence's first task for this client – a nice win-win!

The Brand Protection Team attends the 7th Regional Intellectual Property (IP) Crime Conference, Middle East and North Africa

Each year, TenIntelligence attends many IP conferences such as the Regional Intellectual Property (IP) Crime Conference, Middle East and North Africa, as it provides the opportunity to meet with local law enforcement authorities across the region to discuss current trends, enquiries and re-establish links in one arena.

Such events also offer a relaxed meeting environment for both Brand Owners and Intellectual Property Specialists to discuss on-going and future projects.

Luxury fashion house successfully raids premises in Jebel Ali Free Zone and Secret Apartments in Dubai

TenIntelligence regularly provides intelligence to a well-known fashion power house; collecting precise and clear details relating to traders selling counterfeit versions of their products.

The information supplied includes layouts of showrooms, how to enter secret storage areas, and quantities available (as seen).

Think of it as buying a house, a buyer reviews the floor plans prior to purchasing – we draw these floor plans, indicating where the counterfeited products are located, and identify how to access these secret rooms (remote control, by a key stored in a specific cupboard, drawer, location etc.). The floor plans have assisted local law enforcement authorities in locating these "secret" areas, thus yielding a larger quantity of fake products.

December saw successful raids carried out at premises in Jebel Ali Free Zone and Dubai.

Contact Us

UK
+44 (0)20 3102 7720
info@tenintel.com

MIDDLE EAST
+971 (0) 4333 4669
dubai@tenintel.com

@tenintelligence