TenInsight

TenIntelligence
London | Dubai
Due Diligence | Investigations | Protection

www.tenintel.com | June 2019 | Issue 6

How resilient is your organisation?

A recent financial research paper suggested 58% of UK small and Medium sized Enterprises (SMEs) have invested in some form of resilience during the past 12 months.

It is clear from these figures that business owners and managers are taking the necessary steps to protect themselves against new challenges – including Brexit, cashflow problems and financial uncertainty. In times of financial difficulty, recession or uncertainty, business owners should look to cut costs to help their company become resilient. One key area to look at is within the organisation itself.

Expense fraud is the most common type of fraud and is a significant threat to a business.

Fabricated expenses can often be an easy way for an employee to get reimbursed for personal purchases, by inflating their mileage, client entertainment costs, or submitting multiple reimbursements for the same thing. The amounts are usually little and often, enabling the employee to subtly fly under the radar.

The preventative answer is to design and implement an expenses policy with clearly defined guidelines – one that requires a dual signature process, questions expenditure and requests original receipts.

Using your time wisely during uncertainty is a good opportunity to stabilise your financial position and review your audits, processes and expenditure. Keep a keen eye out for details or anomalies – in our experience, suspicions of fraud are normally well founded.

It has been a year since GDPR officially went into effect – how was your GDPR journey? Our journey continues daily, and we consistently test our data security compliance.

A year has passed since the legislation for GDPR and the Data Protection Act 2018 was officially implemented in the UK.

After an extensive annual audit by the British Assessment Bureau, I am pleased to confirm our ISO 27001 Information Security accreditation has been renewed.

If your organisation needs increased resilience, whether it be fraud, cyber or data related, then please let us help you.

Neil Miller
CEO, TenIntelligence
neil.miller
@tenintel.com

ISO 27001 certification gained by TenIntelligence for another year

Neil Miller, Chief Executive Officer, commended the team's effort in maintaining our high standards of excellence and said: "Confidentiality, integrity and the protection of data continues to be of paramount importance to our clients, and our successful re-certification demonstrates TenIntelligence's commitment to data security. My thanks to our compliance team, for coordinating, implementing and improving our procedures over the last year."

Richard Bell, Chief Operating Officer, added: "TenIntelligence has a strong commitment to adopting and enforcing the highest standards in our Information Security Management System (ISMS) for our clients, staff and partners. It is very important we practise what we proclaim – I am delighted by the efforts of all our team."

The company was assessed across several fields including relevant documentation, the scope of our ISMS, business continuity, risk assessments and internal procedures, as well as control checks appropriate to our business and service provisions.

Compliance will continue to be one of the core values of TenIntelligence. We have an integrated compliance programme for every process, which continues to provide assurance for our clients. TenIntelligence always strives for excellence and we are currently working towards ISO 9001:2015 Certification that sets out the criteria for our quality management system and assurance.

How do geopolitical cyberattacks affect the average UK SME?

It is not unusual these days to hear about a corporate or public entity being subject to a cyberattack or losing large quantities of data. The attacks garnering most attention are, characteristically, not perpetrated by a bored teenager (a so-called "script kiddie") but are instead state-sponsored and geopolitical in nature.

One of the more recent attacks includes the Australian government cyberattack in February 2019, linked to Iranian cyber espionage group 'Iridium' – a group also believed to be responsible for a similar attack against the UK government in 2017.

Other geopolitical cyberattack examples include the WannaCry ransomware in 2017, the supposed Russian interference in the US 2016 presidential election, North Korea's attacks against SWIFT and Bitcoin, and the numerous Russian assaults on Ukrainian infrastructure.

The effects of these geopolitical cyberattacks are often under-estimated always seem to be misunderstood, as people often forget about the incident after a couple of days of bad press. The long-term ramifications of such an event are often not truly comprehended by smaller businesses in the UK.

The 2019 Cyber Security Breaches Survey shows 31% of micro and small businesses have encountered breaches or attacks in the last 12 months. Despite the statistics, most SMEs feel they are not at risk of being a target – there is a general air of unrealistic optimism that being a small company is a form of protection. After all, they think, why would China want to know how many rats were caught by a small Kent-based pest control business?

At the ITC Annual Security Conference, Paddy McGuinness, former UK Deputy National Security Adviser for Intelligence, Security and Resilience, highlighted that China's attacks characteristically target big data sets and bounce off others by hacking through a service provider.

Hypothetically speaking, if the UK government used Amazon Web Service (AWS) to store its data, China could target large data sets in AWS to seize this. As a small pest control business in the UK, using AWS cloud to store all personal data relating to your clients, your company's data could be compromised in the attack. Would you have a plan in place for this scenario?

It is important to understand that although you may not be the direct target of a nation-state hack, it is possible to be affected indirectly – having a plan in place will help mitigate the consequences of the breach.

Primarily, you need to understand your own cyber vulnerabilities: does your company adhere to the most basic cybersecurity principles? In their Cyber Essentials programme, The National Cyber Security Centre (NCSC) has useful guidelines for making sure you are safe – the information is written plainly and is accessible for most.

Undertaking third-party risk management is also important. Ask yourself and your team – how well do you know the provider of your cloud-based security solution? Do you know where in the world your data is stored? What security protocols does the company have in place? What is their reputation like? Do my third parties use other third parties? If a data breach occurs, how do I communicate externally and internally?

According to the 2019 Cyber Security Breaches Survey, the number of businesses reporting cyberattacks decreased from 43% the previous year to 32% this year. However, it appears that businesses and charities that have been targeted now appear to be experiencing more attacks than in prior years.

Such a high percentage of attacks suggests it is not a case of if you will suffer a data breach, but when.

Most importantly, do not underestimate the effects of a cyberattack on your company and employees, and never undervalue the importance of a thorough and up-to-date company plan in minimising the effect of a macro-scale cyberattack. Be prepared – you never know if you will be the next target.

At TenIntelligence, we provide a range of services and jargon-free advice to organisations who require assistance to protect their company. If you would like to have a conversation about your security position, or need help in reaching an applied standard, contact us via info@tenintel.com.

Sean Nichol
Associate (Cyber and Forensics)

Useful links:

1.The 2019 Cyber Security Breaches Survey: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

2. Cyber security advice for SMEs by the National Cyber Security Centre https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations

Is your company taking due diligence seriously?

When 75% of our background checks identify flags, a simple Google search isn't enough.

In 2002, Yahoo discovered that CEO Scott Thompson could not have obtained a bachelor's degree in computer science from Stonehill College, as the course was not offered until four years after he graduated. In 2018, the world's largest luggage maker, Samsonite, also announced its CEO had stepped down following allegations he lied on his resumé.

These are just two high-profile examples, whereby both companies, as market leaders in their sectors, overlooked the details of their most senior executives' CVs. This resulted in not only financial losses but, most importantly, it had an embarrassing impact on the company's public image. Skeletons can be found in even the safest closets.

How much due diligence is enough?

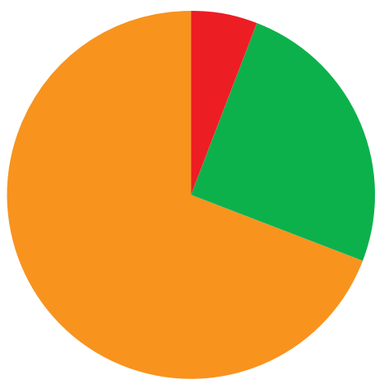
Having the right background information allows organisations to work with confidence, compliance and assurance. Our Due Diligence Team completed over 600 background checks during 2018. As part of our analysis into these checks, we implemented a simple traffic light system, giving each background check a status of Red, Amber or Green. Red showed a significant red flag had been found; Amber confirmed that discrepancies were identified; whilst Green meant there were no issues identified on their CV or application form. From our research, a total of 75% cases were identified as an Amber (69%) or Red flag (6%). This means during the open source phase, a further investigative phase is required, or the scope might also need to be expanded into additional jurisdictions.

During this research we identified a number of near misses, where clients had been poised to appoint a professional who, at first glance, seemed like the ideal candidate but turned out to be less than desirable. Our findings included allegations of insider trading, sexual harassment, fraud, drug taking, undeclared insolvencies, court litigation, ties to sanctioned individuals and companies; all of which clearly demonstrate the need for background checks before employment to help safeguard your organisation's reputation.

No more Google searches

Whether it's through an in-depth interview with a former colleague which reveals criminal activity or undeclared financial issues identified through official records, relying on a Google search to identify these kinds of risks is unwise – none of the red flags we identified during the 600+ background checks in 2018 were found through a Google search.

Due diligence results



Red	Green	Amber
6%	25%	69%

Detailed examination of databases, online resources, and interviews with carefully chosen individuals and sources, is the only way companies can be certain to minimise risks when engaging with a new senior hire, partner or business. Interestingly, there are several mechanisms in place online for people to hide their backgrounds: for example, companies which bury negative online profiles for a fee, as well as the Right to be Forgotten law codified in the EU's General Data Protection Regulation (GDPR).

It further proves that using standard search engines will not recover scrubbed data, however, an experienced due diligence analyst is trained to spot the signs and collect factual information.

Due diligence is a very complex and challenging undertaking. A thorough background check into senior executives and new hires should entail rigorous interrogation and analysis of information gathered from a range of open sources, such as: subscribed databases; press articles; company registries; court searches; public records and documents; reference checks; employment and education verifications, as well as social media platforms. It is critical to identify all the possible risks, as the additional cost for the supplementary phases is minimal compared to the possible losses incurred from a bad business decision.

For more information regarding our due diligence service, please email us via info@intel.com. Our team is looking forward to providing assurance and help your organisation make informed decisions.

Katie Frodsham
Litigation Support and Assurance Director
katie.frodsham@tenintel.com

اخبار جديدة من دبي

Update from Dubai

Anti-fraud learning – a personal perspective

Attending the Association of Certified Fraud Examiners (ACFE) anti-fraud masterclass organised by the Open Thinking Academy in Dubai was beneficial for me to learn more about becoming a fraud examiner, and an opportunity for me to be introduced to other professionals in the field, as well as presenting TenIntelligence to a wider audience.

As fraud investigation is one of our core services, attending the masterclass was a great opportunity to gain contacts and build relationships. I was really pleased to receive positive feedback from one of our existing clients and interest from another masterclass visitor – both were very keen for us to contact them.

The anti-fraud masterclass was divided into two sessions. The first session focused on the Certified Fraud Examiner (CFE) exam requirements. The second session of the class concentrated on interviewing techniques that fraud investigators should apply when interviewing someone suspected of fraud or wrong-doing.

With the help of visual aids, the speaker was able to elaborate on how an investigator should create the right environment to reassure any suspect rather than intimidate them. The session ended with a guest speaker from a well-known accounting firm – his talk gave a good insight into how a fraud investigator should conduct an interview, with real-life examples. I particularly enjoyed his presentation as it showed how psychology can really help investigators when dealing with somebody suspected of fraud, which can significantly change the outcome or course of an investigation.

I look forward to putting some new learning into practice and building upon that knowledge.

And if you are interested in knowing more about the workshops and lectures we attend, please follow us on social media @TenIntelligence.

Reem Ramadan
Analyst (Dubai)

Counterfeit goods seized

TenIntelligence, in partnership with Underwriters Laboratories (UL) and Sharjah Criminal Investigation Department (CID), has successfully carried out raids on counterfeit electronic products.

Our Dubai team worked with UL, a global independent safety science company, to assist officers from Sharjah CID in identifying almost AED 4 million worth of counterfeit products and items that featured unauthorised trademarks.

TenIntelligence provided Sharjah CID with evidence of the counterfeit products and their locations, as well as additional assistance during the raids.

Items with a total value of AED 3,997,667 were confiscated, including 30,546 illegal lithium-ion batteries, AC adaptors, chargers, keyboards, hard drives and LCD screens.

TenIntelligence is pleased to work with local and global law enforcement authorities and contribute to apprehending and prosecuting counterfeiters who break the law. It is also important to recognise that this successful collaboration has protected the public's safety and prevented the spread and sale of illegal and dangerous counterfeit goods across the Emirates.

The operation was the latest in a series of ongoing collaborations between UL, TenIntelligence, police and local authorities in the UAE designed to target sellers and manufacturers of such goods.

Cate Wells, Managing Director (Dubai), said: "This joint approach proves we can prevent the sale and distribution of hazardous and substandard commodities. For clients like UL, it is their utmost desire to prevent harm to consumers and they are concerned with much more than the financial value of the goods that have been removed from the markets. Congratulations to all involved – our Dubai Team, Sharjah CID and Natalie Wong and Hamid Syed at UL."

To learn more about the brand protection services we provide in the UK and Dubai, visit www.tenintel.com.

LONDON
+44 (0) 203 963 1930
info@tenintel.com

KENT
+44 (0) 173 252 5810
info@tenintel.com

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

@TenIntelligence