TenInsight

Becoming certain in uncertainty

The political landscape has been a real distraction recently and it is no surprise that uncertainty often leads to financial strains and subsequently, workforce lay-offs. If your organisation has the unfortunate ordeal of laying off employees, be prepared.

Recent research highlighted that **58%** of former employees still retained access to IT networks including financial and customer information; whilst **24%** of UK businesses alone have experienced data breaches instigated by former employees.

To avoid further burden and costs because of disgruntled former employees, now is the time to implement the necessary steps to help prevent fraud and data breaches.

Our Forensics Lab is now open

Many fraud investigations that I have presided over the years have been solved via digital forensics. Evidence found in computers, digital devices and networks have often been the key to uncover the perpetrators and true mechanics of fraud and computer misuse.

So, it is with great pleasure, that we can announce that our internal Digital Forensics Laboratory is open. There are many different scenarios whereby digital forensics can help an investigation, data breach or safely recycling laptops back into an organisation's operations – please call us for an introductory no-obligation conversation.

Identifying a fraudster in your organisation

Besides potential data breaches, uncertainty is often preceded with an increase in corporate fraud. A massive **US $7 billion** was lost to corporate fraud alone last year, these were just the reported frauds and this figure is likely to be the tip of the triangle. In our "Ask an Expert" feature, Valeryia outlines some practical advice on building an anti-fraud environment; as well as giving tips on how to spot a fraudster.

University of Kent – a collaboration

Education, awareness, collaboration are all values which we at TenIntelligence like to share with our networks. As you will read below, it is our responsibility to guide younger generations with the awareness they need to secure their physical and cyber lives. We work closely with the University of Kent on a variety of cyber awareness campaigns, helping their students move into adult working life with the necessary knowledge to protect themselves for their future.

Reducing the counterfeiters' purse

Besides ongoing political uncertainty and cyber threats posed to society, we cannot forget about other dangers across the globe. Profits from counterfeiting are often used to fund serious organised crime, such as human trafficking, money laundering and child pornography. I would like to take the opportunity to congratulate our Dubai team, led by Cate Wells, who are continuing to win the counterfeiting fight and enjoy some substantial raids depleting the purse of the counterfeiters.

Neil Miller, CFE
Founder & CEO
neil.miller@tenintel.com
in @Neil Miller, CFE

In this issue....

Ten On Tour

University of Kent , Canterbury

Physical and Cyber Security Convergence

According to research by Intel IDC, the number of Internet of Things (IoT) devices are growing exponentially, from 2 billion IoT devices in 2006 to a projected 200 billion by 2020. It means every human being on the world will own an average 26 smart objects. Yet, lack of convergence will result in failings to provide both secure physical and cyber environment in the long term.

As the boundaries between physical and cyber security continue to blur, it is important for future generations to understand extensively the challenge and develop inter-related skills.

The convergent approach should minimize the skills gap between the two fields and pave the way for a mutual understanding, awareness and knowledge of both sectors.

TenIntelligence, as a leading influence in the security sector, have the knowledge and experience to share with the security experts of the future. We are delighted to meet the students from different courses at the University of Kent and hopefully have inspired, encouraged and educated the students to take on responsibility in building a more secure online environment for everyone.

How using forensics can help protect your organisation's digital assets

What is the right thing to do when you encounter the following scenarios?

92% of UK businesses do not have an automated procedure in place for when an employee leave the business. *(OneLogin, 2017)*

58% of past employees retained access to the corporate network. *(OneLogin, 2017)*

24% of UK businesses have experienced data breaches by former employees. *(OneLogin, 2017)*

55% of UK businesses failed to encrypt removable devices such as USB pen drives. *(ESET & Kingston research, 2019)*

45% of businesses do not use a Security Information and Event Manager to audit for application usage by former employees. *(OneLogin, 2017)*

1. A senior employee has announced their resignation and is moving to a competitor. Allegations arise surrounding the theft of sensitive organisation data by this employee. There are a several ways in which digital data can be transferred out of an organisation including USB memory devices, email, or cloud-based file hosting services.

   Do you have any policies in place to avoid former employees stealing confidential data?

   Did you know our team can forensically track the movement of data through a multitude of digital devices?

2. Your organisation has a high turnover of staff and the devices are often recycled back into the organisation.

   Are you aware that resetting the device does not wipe the data?

   What process does your organisation utilise to securely recycle or decommission the devices?

   What GDPR security obligations do you have when recycling devices?

   Have you considered a forensic analysis of the device to understand an employee's activities before leaving the organisation; and whether any information has been stolen or leaked?

3. An employee has allegedly viewed or downloaded pornographic material on their work device.

   Did you know you can utilise digital forensic techniques to view an employee's browsing history, even when they are utilising private browsing?

4. An employee complains that their line manager is bullying them via an organisation-owned instant messaging app.

   What level of logging does the organisation-owned instant messaging app contain?

   Have you considered recovering deleted messages via a forensics investigation?

If you wish to discuss the any scenarios in detail, please contact us at forensics@tenintel.com.

Introducing our Digital Forensics Laboratory

We are delighted to announce that our new in-house digital forensics laboratory at our Kent Headquarters is now in operation and conducting forensic examinations.

Time is often crucial to an investigation, and our new laboratory allows our team to follow a set of streamlined procedures, preservation standards and technical competence to preserve, examine and analyse the evidence collected.

Our Certified Forensic Practitioners, led by the company's Chief Operating Officer, Richard Bell and Cyber and Forensics Associate, Sean Nichol, are trained to recover and investigate material found in digital devices, including hard drives, servers, laptops, smart-phones, networks and storage media by imaging these devices for further analysis and evidence review.

We have a forensic team that has a mobile unit, allowing us to travel to the source to preserve the evidence. We have been assisting clients on cases such as the following:

- unauthorised access to company/client information
- transfer of confidential files to personal devices/storage and non-company emails
- origins of fraud, perpetrators and suspects examination of synced text messages, call logs from company phones
- identification of data breaches which may have been unreported under the recent GDPR obligations
- recycling of devices for re-introduction to the company infrastructure

To find out more about our digital forensics service, visit our website at www.tenintel.com. Alternatively, you can email us at forensics@tenintel.com.

Ask an Expert

How to identify a fraudster and build an anti-fraud environment?

At a time of geopolitical uncertainty, staff are often anxious about their futures, resulting in the temptation to commit fraud or more vulnerable to falling victim to scams. It was reported by a recent Brexit survey, where **80%** of UK business leaders are fearful of job losses as a result of Brexit, with **66%** of them being concerned about employees committing fraud due to the lack of job security.

Data also shows that employees are more likely to be able to commit fraud, compared to people outside of the organisation. This is because employees are more familiar with the internal system and points of vulnerability, as well as unchallenged opportunities within an organisation.

Fraud can bring negative impacts to the organisation's financial health, image and reputation. **$7 billion** was reportedly lost globally in 2018 due to corporate fraud. Therefore, by recognising and understanding behavioural red flags can help organisations to detect, prevent fraud and avoid monetary and reputational damage.

The Association of Certified Fraud Examiners ("ACFE") outlined 6 behavioural red flags of fraud in their Report to the Nations in 2018. In **85%** of the 2,690 cases of occupational fraud studied by the ACFE, it was identified that fraudsters exhibited at least one behavioural red flag and that **multiple red flags** were evident in **50%** of cases. These include the following:

- living beyond one's means - lookout for lifestyle changes, purchasing of expensive cars, houses, and luxury goods
- financial difficulties - check for the history of debt and be aware of any arising financial problems, consider addictive behaviours such as gambling
- unusually close association with a vendor/customer
- excessive control issues or unwillingness to share duties
- divorce or family problems
- "wheeler-dealer" attitude involving shrewd or unscrupulous behaviour

Gender and positions dependent

The report also stated that these warning signs varied by perpetrator's position within the organisation, as well as gender. To illustrate:

- 24% of owners or executives were found unusually closed with vendor or customers, compared to 14% of employees
- "Wheeler- dealer" attitude is more commonly found in owners or executives than employees, as well as in women than men
- Financial problems are generally discovered in male fraudsters than female
- Instability in life circumstances is a more common behavioural flag found in men than women
- However, more women were found in a close relationship with vendors or customers

However, simply meeting the profile outlined above does not mean that an individual is going to commit fraud, nor should someone who falls outside the profile be immune from suspicion.

Build an anti-fraud environment

50% of all reported corporate fraud in 2018 was caused by deficient internal control. To avoid corporate fraud from happening in the long run, it is important to take some of the following steps to create an anti-fraud environment and culture to limit fraud risk:

1. *employee training* - create awareness of what constitutes fraud, and promote education in fraud detection and prevention methods
2. *employment and pre-employment screening* - prevent the organisation from hiring people who have a greater tendency to commit fraud
3. *regular risk assessments* - gauge the nature of risks to your organisation
4. *open communication*- beating fraud should be everyone's business. Establish convenient and secure methods for employees to report fraud concerns
5. *internal and external controls* – setting policies and procedures

Fraud prevention becoming the first line of defence as bad news travel fast

Lastly, in this era of absolute transparency, organisations are often in a passive position when an issue becomes a crisis. Public opinions have been a deal-breaker to an organisation's reputation. An efficient crisis response was rated highly by **76%** of the employees surveyed by a US Marketing firm. This suggests how crucial reputation is to an organisation and how an effective fraud risk management can help.

Therefore, traditionally fraud prevention and detection has progressively become an organisation's first line of defence. Identifying fraudsters with the above signposts are the first of many steps in creating a comprehensive prevention method.

If you think your organisation might be a victim of fraud, please get in contact immediately. We can help you to analyse the evidence, circumstances surrounding the suspicion and set out clear objectives in an investigation plan. We can also help strengthen your defence model.

Alternatively, you can utilise our due diligence service, where our analysts conduct thorough background checks into senior executives and new hires, looking for adverse information and risk, including undisclosed red flags, conflicting findings, false or exaggerated statements. All of which can prevent corporate fraud from happening.

For more information, please visit https://www.tenintel.com/corporate-fraud/ and email us at info@tenintel.com

Valeryia Dockrell
Senior Associate | *Investigations*
valeryia.dockrell@tenintel.com
in @Valeryia Dockrell

TEN facts on counterfeiting products

- **2.5 million** jobs are lost globally due to counterfeiting. *(Frontier Economics)*
- In the first half of 2019, a total of **£5 million** counterfeit banknotes were taken out of circulation. *(Bank of England, 2019)*
- **1 in 3** UK residents, the equivalent of 18 million people, have mistakenly purchased a counterfeit electrical item online. *(Electrical Safety First, 2018)*
- Less than **10%** of people aged 55 or above have received a counterfeit electrical products, compared to **55%** of millennials. *(Electrical Safety First, 2018)*
- Counterfeits account for **10-30%** of the market of drug sales. *(World Health Organisation)*
- **25%** of British consumers had knowingly bought one or more counterfeit products online during 2017-2018. *(European Commission, 2018)*

Illicit goods, from designer handbags to luxury watches accounted for 3.3% of total international trade in 2016, up from 2.5% ($461bn) in 2013. *(OECD & EUIPO, 2016)*

The number of counterfeit tobacco products detected, mostly cigarettes, has been decreasing for 4 years consecutively. *(Intellectual Property Crime Threat Assessment, 2019)*

Profits made from counterfeiting are often used to fund other serious organised crime such as, people trafficking, money-laundering and child pornography. *(Interpol, 2019)*

Counterfeiting costs the UK cosmetics sector more than £200 million per year. *(Journal of Trading Standards, 2018)*

UPDATE FROM DUBAI اخبار جديدة من دبي

TenIntelligence has recently partnered up with multiple brands and organisations to carry out raids in both emirates of Sharjah and Dubai, with the assistance of law enforcement agencies.

Two successful raids were carried out in July, where 25,056 counterfeit products were seized from two warehouses in the first operation and over 43,000 substandard goods were captured by working with various well-known brands in the second operation. Both raids have resulted in the seizure of counterfeit goods worth 19,000,000 AED/ Emirati Dirhams (approximately 4million GBP).

TenIntelligence is delighted to work with the local and global law enforcement authorities and contribute to apprehend and prosecute counterfeiters who break the law. The monitoring of counterfeit goods or intellectual infringement in the physcial and online market places, aims to discourage fraudsters. As a leading influence in the brand protection community, we are committed to assisting companies with the safe removal of counterfeit products, protect intellectual property and help facilitate successful innovation.

Cate Wells, Managing Director (Dubai) said, "TenIntelligence have been working alongside different UAE Law Enforcement Authorities (LEA's) for many years for the identification and safe removal of counterfeit products in different sectors. Counterfeiting, piracy and infringements of intellectual property rights are a constantly growing phenomena. The money raised from selling fake products is well documented in supporting other criminal activities. We are inspired to continue to work collaboratively with brands and LEAs to prevent the sale and distribution of dangerous and inferior goods. Thank you to all involved!"

To know more about the brand protection services we provide in the UK and Dubai, please visit our website https://www.tenintel.com.

You can also learn about the company and receive advice by following us on LinkedIn, Twitter and Facebook @TenIntelligence.

Our Intelligence | Your Assurance

ذكائنا هو ضمانك

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

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

Dubai
+971 (0) 4 425 3002
dubai@tenintel.com

@TenIntelligence