TenInsight

THE YEAR AHEAD.

I am an optimist and always look ahead. Yet, I also learn from past events, to help build success for the future.

Last year, political uncertainty dominated the UK headlines. Confidence in British business was low, financial markets were turbulent and there was indecisiveness within the political party ranks. British business took a blow, all whilst the outside world was watching us.

Political uncertainty will continue as our geo-political Analyst, Mariya Babikyan, highlights in her "Ask an expert" briefing. But as our regular readers and followers will know, TenIntelligence continues to build a solid platform, providing our clients with continued confidence and assurance.

These are just some of our highlights over the last year that we take forward into 2020:

Business Expansion

- Invested in the recruitment of new talent, including marketing, analysts, brand protection, compliance and business support positions
- Introduced new advisory board members, Mrs. Mendy Ghaleb (UAE), Ms. Patty Melamed (USA), Mr. Zach Bracchitta (USA) and Mr. Colin Culleton (UK)
- Created CyberSimplified – a new Cyber Division for TenIntelligence
- Invested in new office space in Kings Hill (Kent), Moorgate (London) and Business Bay (Dubai)
- Invested and officially launched the Digital Forensics Division
- Initiated the development of our Strategic Intelligence and Geo-Political Risk service offerings
- Continued to build relationships with Kent, Warwick and Hereford (NMiTE) Universities
- Partnered with Santander and the University of Kent's Intern programme

Personal development

- Introduced mentoring relationships with board advisors
- Invested in team building exercises, bringing the team together
- Investment into training, memberships and certifications
- As a team, we continue to work together to help monitor and improve our working processes

Continuous recognition and high security standards

- Continued accreditation with ISO27001 Information Security Management certification
- Formed a partnership with Dell to provide increased security and operational performance
- Protect our own and clients' data by improving our compliance and security standards
- Gained Cyber Essentials Plus accreditation, the Government's "Gold Standard" in Cyber Security

We have a team of colleagues who are dedicated in delivering excellence to help safeguard your reputation and protect you from fraud, brand infringement, regulatory risk and data breaches.

I wish all of our readers a prosperous and healthy new year.

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

In this issue....

Forensics in the workplace - a simplified approach

As part of our educational promise to our clients and local organisations, TenIntelligence recently presented its first awareness event of 2020.

Our Chief Operating Officer, Richard Bell and Cyber and Forensics Associate, Sean Nichol, provided local Kent businesses with an insight into the digital forensics examination process, the different types of forensic investigations and how they can support different organisations.

Identifying and gathering digital evidence is key to successful litigation and dispute resolution. During the presentation, our Certified Forensic Practitioners discussed how to recover and investigate material found in digital devices, including hard drives, servers, laptops, smartphones, networks and storage media devices, for further analysis and evidence review. The team also shared different scenarios that highlighted how digital forensics techniques can be utilised to aid fraud and Intellectual Property investigations or provide assurance for data compliance and protection.

If you are interested to have our cyber forensics team at your company for a presentation, please contact us at info@tenintel.com or visit our website at https://www.tenintel.com/digital-forensics/ for more information.

TenIntelligence gained Cyber Essentials Plus accreditation for 2020 and beyond

The team at TenIntelligence is delighted to announce that we successfully gained the Cyber Essentials **Plus** accreditation for 2020 and beyond.

Our team strives to protect ourselves and clients against different cyber risks and vulnerabilities. We continue to maintain the highest security standards, applying them across the board, ensuring the whole company fully applies and shares the same ethos.

Cyber Essentials is a UK Government assurance standard (led by the National Cyber Security Centre), designed to improve the resilience of UK businesses to prevent most cyber security threats.

Cyber Essentials **Plus** is an advanced level of assurance which includes an internal workstation vulnerability assessment carried out on-site by an independent CREST certified body.

As part of our certification process, a technical review and evaluation of our security processes and policies was completed by an external certifying body, Armadillo Security.

The Cyber Essential **Plus** scheme requires TenIntelligence to implement five key controls: secure configuration, boundary firewalls and internet gateways, access control and administrative privilege management, patch management and malware protection.

Our Chief Operating Officer, Richard Bell, welcomed the accreditation, "Cyber Essentials **Plus** is an important certification for us. It clearly demonstrates our ongoing commitment to continually ensure that TenIntelligence is at the forefront of applying the best security standards. Security is crucial to everything that we do and achieving this certification along with our well-established ISO27001 certification, allows us and our clients to operate with confidence."

Neil Miller, CEO and Founder added, "Our continued mission is to help protect our clients, colleagues and their livelihoods from harm through effective due diligence, investigation and protection. We are really pleased to receive the accreditation and extend our cyber security services to our clients. As with our other ISO accreditation and processes, this was again a team effort and I congratulate them on this success."

The unstoppable growth and dynamic of cyber-enabled crime mean organisations of all sizes need to rethink their approach to security. Everyone knows that security is important, and we all rely on the Internet, IT and other connected systems, all of which without the appropriate protection could be at risk from a cyber-attack. These attacks are becoming increasingly more sophisticated and stealthier, targeting people, networks and devices.

TenIntelligence provides jargon-free, cyber simplified advice and services to all organisations. For more information, please visit our website https://www.tenintel.com/cyber-security/. You can also email us at info@tenintel.com.

Cyber security trends to look out for in 2020

As cyber attacks continue to evolve, organisations need to be prepared for future cyber security challenges.

The Cyber Security Breaches Survey 2019 *(GovUK, 2019)* demonstrates that cyber attacks are a continuous threat to businesses and charities. The number of phishing attacks and ransomware reported by organisations has been increasing since 2017.

When it comes to becoming cyber resilient, organisations need to prioritise cyber security training to everyone, not only to the IT department. It is a joint effort to protect the organisation's data. Going back to basics in terms of fostering ongoing cyber security awareness is one of the simplest yet most effective ways to keep an organisation secure.

Especially when ***50%*** of the UK workforce are projected to be working remotely by 2020 (Office of National Statistics, 2017), personal devices will become the backdoor for cyber criminals to bypass corporate defences *(ONS, 2017)*. It is important for organisations to provide adequate training to everyone in the team.

Enforce a baseline for cloud-based security

The UK is the sixth largest cloud user among European Union (EU) countries in 2018 *(Eurostat, 2018)*. It is not unusual to see small-medium enterprises utilising cloud services, such as Dropbox, to store data or customer relationship management (CRM) providers, like Salesforce, to support day-to-day operations. With ***41.9%*** of the UK enterprises adopting some form of cloud service, organisations must understand thoroughly the intended use of cloud service, identifying how data will be processed, stored and transported, will allow relevant security measures to be implemented.

The emergence of Artificial Intelligence and the need for cyber talent

The World Economic Forum reported a shortage of people trained in cyber security in 2017. It has also been projected that there will be ***3.5 million*** unfilled cyber security jobs globally by 2021. As the cyber security skills gap continues to grow *(Cybersecurity Ventures, 2019),* more organisations are exploring the possibility of utilising Artificial Intelligence (AI). In the long run, organisations should recruit talent to stay on top of the trend and experiment how AI can slowly be embedded into the foundation of security, to detect threats and other potentially malicious activities.

Ask an Expert

A glimpse into uncertainty: 2020 geopolitical risks

Before the discovery of Australia, people were convinced all swans were white, entirely confirmed by empirical evidence. No one had ever seen a black swan, writes Nassim Taleb, a risk analyst who works on randomness, probability and uncertainty. To refute this theory, it only took for one person to see a single black swan as proof. Much like the times we live in today, the "black swan theory" illustrates events of high improbability which leaves a lasting impact on our lives.

Last year was undoubtedly a very turbulent one from a geopolitical standpoint, and while 2020 might look like mainly having negotiations on the table. We have prepared a list of 5 risks surrounding geopolitical uncertainties:

Brexit

Britain is set to leave the European Union on 31 January 2020. While this puts an end to a long period of political and business uncertainty, risks stem from the short 11-month window for the UK and the EU to formulate bilateral agreements. There is even less time to agree a negotiating mandate, and to seek ratification for the final trade terms.

Negotiations will potentially focus on pressing issues where no unilateral measures could easily be set to replace current arrangements. Risks to the volatility of the pound sterling remain as Prime Minister Boris Johnson has ruled out an extension to the transition period, which leaves the possibility of a No Deal Brexit. The manufacturing industry losses of 2019 will probably remain substantial during the year ahead and will have to be factored in during negotiations in Brussels.

Presidential Elections in the US

US Presidential elections set for 3 November 2020 bear twofold importance in terms of geopolitics. President Trump, like many of his predecessors, will most likely enjoy an incumbency advantage in the elections, which brings little surprise for US and global market security as the political platform is at home since the first mandate. However, President Trump's ongoing impeachment trial puts a question on the legitimacy of a second term in office. Contestation of the result risks the continued decrease of public sentiment in democratic institutions in the US and creates a prolonged political vacuum. A re-election of a polarising figure like Donald Trump has immediate consequences on business, investment, and climate agreements.

US - China Trade Deal

A First Phase trade deal was signed on 15 January 2020 between the US and China, drawing a current pause on trade tensions. The US looks to develop economic relationship with China in the areas of intellectual property, technology transfer, agriculture, financial services, currency, and foreign exchange.

However, reshaping the trade relationship between the two biggest economies included sanctions, export controls, and boycotts in the past months. This leaves little room for transnational corporations to maintain geopolitical neutrality in the coming year.

The US-China trade war will likely focus on spheres of influence, as evident from the launch of the new 5G technology.

With the UK negotiating trade deals until the end of 2020, the US-China tensions add another layer of complexity for the financial markets.

Conflicts in the Middle East

The continuously growing tensions in the region are set to continue in 2020 - on the one hand, between the US and Iran, and on the other, between the Gulf countries and Iran in a clash for regional influence. The escalation of tensions with Iran saw the brief detention of the British Ambassador, followed by the Office of Financial Sanctions designation of Iran-backed political and military wings of Hezbollah on the list of terrorist entities.

The risks to security remain volatile in times of tensions and 2020 might see proxy activity in retaliation to the growing isolation of the Iranian regime. Prolonged unrest in Lebanon and Iraq, alongside the growing tension in Libya and post-war Syria reconstruction will likely pose security risks and will remain on the political agenda in 2020.

The Green Deal

In 2020, "The Green Deal" debate will risk deepening geographic and socio-economic divisions within Europe as it is already prompting populist campaigns against the deal and giving platform to climate change deniers.

In Eastern Europe, many countries largely use and rely on coal for energy, so when it comes to talks on carbon neutrality, Eastern Europe feels left behind and part of a two-speed Europe. "The Green Deal" not only creating interstate divisions, but also purveys political divisions within the majority of EU member states.

France's attempt to raise taxes on fuel in 2018 sparked the yellow vests movement. Deeply divisive across Europe, the deal will likely also see backlash from corporations which might struggle meeting the new rules.

We, at TenIntelligence, are committed to protect clients, people and their livelihoods from harm. We know investing or operating in adverse business environments or foreign jurisdictions is a daunting proposition for businesses. Environmental conditions, shifting regulations, political fluctuations and cultural changes are all risks that an organisation will face over time.

To find out more about the way we incorporate geopolitical insights with our due diligence work, ensuring you have a contextual understanding of risks for your business, please visit our website at https://www.tenintel.com/strategic-intelligence/ or email us at info@tenintel.com.

Mariya Babikyan
Analyst | Due Diligence
mariya.babikyan@tenintel.com
in @Mariya Babikyan

UPDATE FROM DUBAI اخبار جديدة من دبي

Counterfeiting in 1997 vs 2020

In **1997**, the US Customs seized Intellectual Property infringing goods worth **USD 54 million**. The top five suppliers of counterfeit goods to the US, were China, Korea, Taipei, Hong Kong and the Philippines. The main sources of fake good imported to the European Union were Poland, Thailand, Turkey and the US. The most common counterfeit products were CDs, videos and computer games *(The economic impact of counterfeiting ,1998)*.

Fast forward to **2013**, the international trade of counterfeit products has increased to **USD 461 billion**, represented **2.5%** of the world trade. It was then increased to **USD 509 billion** in **2016**. Types of counterfeiting goods have also expanded to include footwear, clothing, leather goods, electrical equipment, medical equipment, toys, pharmaceuticals and more.

The continuous growth of counterfeit goods can be explained by the rapid digital transformation. With the widespread adoption of digital technologies, it enables firms to internationalise at a lower cost, allowing more small parcels to cross borders. As a result, counterfeit and pirated products can be shipped by virtually every means of transport. To illustrate, small parcels accounted for **69%** of global total customs seizures by volume over **2014-2016**, up from **63%** over the **2011-2013** period.

Compared to **1997**, more countries have become the top producers and transition points for trade in counterfeit, such as India, Malaysia, United Arab Emirates and Turkey. Four transit points – Albania, Egypt, Morocco and Ukraine – are of particular significance for redistributing fakes destined for the EU. Finally, Panama has also become an important transit point for fake products to the United States *(Trends in trade in counterfeit and pirated good, 2019)*.

Counterfeiting and trademark infringements are serious Intellectual Property (IP) crimes. For consumers, "fake" or "forged" products pose a significant threat to their safety, by unsuspectingly putting their health in jeopardy each time they use counterfeited products. For businesses and IP rights holders, the rise in counterfeiting results in revenue loss and negative brand image. For governments, it also means huge losses in tax revenues and increase in unemployment.

Counterfeiting has yet seen slowdown, compared to 25 years ago. The amount of counterfeiting globally has reached to **USD 1.2 trillion** in 2017 and is bound to reach **USD 1.82 trillion** by 2020 *(Global Brand Counterfeiting Report 2018-2020, 2018)*. To protect your brand and keep your customers safe, contact our brand protection team in Dubai at ***dubai@tenintel.com***, so we can work collaboratively for the identification and safe removal of counterfeit products.

Member of the AIPPI

We have become an active UAE member of the International Association for the Protection of Intellectual Property, generally known as the AIPPI.

The AIPPI is a politically neutral, non-profit organisation, domiciled in Switzerland, which currently has over 9,000 members representing more than 100 countries. As the world's leading international organisation dedicated to the development and improvement of legal regimes for the protection of Intellectual Property (IP), its objective is to improve and promote the protection of IP on both an international and national bases. It pursues this objective by working for the development, expansion and improvement of international and regional treaties and agreements and national laws relating to IP.

Learning is Key

To keep abreast of all the developments, updates and services provided by Interpol in the region, members of our team recently attended the Interpol and the Emirates Intellectual Property Association (EIPA) Crime Conference held in Dubai.

The conference provided a forum to discuss ways to address the challenges brought about by IP crimes and current practices deployed in the region. Our attendance at such an event allows us to continue our strong collaborative links with Dubai Police, Dubai Customs and brand owners.

Sharing Success

In early December, Dubai Police confiscated counterfeit fire prevention products worth **Dh2.5 million (around USD 680,000)** in a police raid. The anti-counterfeit operation was conducted by the Department of Combating Economic Crimes of the General Department of Criminal investigations at Dubai Police in association with technology security firm UL (Underwriters Laboratories) and our TenIntelligence team.

Following our success in 2019, our team will continue to work alongside with Law Enforcement Agencies (LEAs) in the different Emirates for the safe removal of counterfeit products. For more updates, you can follow us on LinkedIn and Twitter **@TenIntelligence**. You can also visit our website at **www.tenintel.com/brand-protection**, where you can find out how we support clients in the identification, gather intelligence and the execution of enforcement notices on counterfeit branded goods found in the UAE.

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