TenInsight

TenIntelligence

www.tenintel.com | February 2019 | Issue 5

Welcome to 2019

We're beating the January blues by sharing with you our ambitious plans for 2019.

In the last edition of the TenIntelligence newsletter, our CEO Neil Miller talked about defining our vision and how, as an investigation and protection consultancy practice, we want to be the playmaker in our field; recognised for our diligence, integrity and excellence.

We have been working determinedly to achieve this, spending several months reviewing our current practices, organisational structure and range of services. We have successfully made significant improvements and devised a series of ambitious and exciting strategies for the near future.

We recognise that our unique selling points are built upon the diversity and expertise of our global team in the UK and UAE. Not only will we continue to utilise these advantages, we will further expand and develop our global teams in the upcoming year.

Our young, dynamic and enthusiastic team possess different skill sets including: languages; legal; security; brand protection; corporate fraud; investigation and compliance experiences. By growing this team, our current and future clients will receive better, bespoke services.

It is important for our clients to know we are always here to serve them discreetly with commitment, excellence and professionalism.

Everybody at TenIntelligence is excited about the future. In 2019, we promise to recruit more talent, spend more time building trustful relationships with our clients and continue to provide them with quality services. We will always reflect on ourselves and aspire to not only be a better company for our clients, but an exemplar for the industry.

In this edition, we highlight our due diligence, investigation and protection service provisions; we examine the latest 'sextortion' cyber scam hitting our email inboxes and provide tactical advice around protecting your organisation from internal security breaches.

Richard Bell
Chief Operating Officer, TenIntelligence
richard.bell@tenintel.com

Phishing scam

In recent years, we have been contacted by numerous clients regarding 'sextortion' scams. Sextortion scams are a type of phishing attack whereby people are coerced to pay a Bitcoin ransom because they have been threatened with sharing the video of themselves visiting adult websites. These scams are made to appear even more credible because they provide seemingly plausible technical details about how this was achieved. The phish can sometimes also include the individual's password.

Phishing scams are designed to play on people's emotions so that they will behave in a way which is out of character, and scams such as this are no different. The phisher is gambling that enough people will respond so that their scam is profitable; they do not know if you have a webcam, have visited adult websites, or the means by which you communicate with people – in short, they are guessing. The phisher hopes to emotionally trigger people so that they will 'take the bait' and pay the ransom – a typical modus operandi. If you have been contacted by a phisher, remember do not fall into their emotional trap and you can always contact us immediately. Continues on p2

What to do?

- As with other phishes, our advice is not to engage with the phisher, to delete the email and report it to Action Fraud: **www.actionfraud.police.uk/report-phishing**
- Do not be tempted to pay the Bitcoin ransom, doing so will likely encourage more scams as the phisher will know they have a 'willing' customer
- Do not worry if the phish includes your password; in all likelihood this has been obtained from historic external or third party breaches of personal data. You can check if your email address or account has been compromised and get future notifications by visiting: **www.haveibeenpwned.com**
- If the phish includes a password you still use then change it immediately. Advice on how to create suitable passwords and enable other factors of authentication is available from Cyber Aware: **www.cyberaware.gov.uk/passwords**
- If you have been a victim of a sextortion scam and have paid the Bitcoin ransom, then report it to your local police force by calling 101
- If you need emotional support, this is available from charities such as Victim Support by calling 0808 168 9111 or visiting: **www.victimsupport.org.uk**

Example phishing 'sextortion' email

Email Title - THIS IS NOT A JOKE - I AM DEAD SERIOUS!

Hi perv,

The last time you visited a pornographic website with teens, you downloaded and installed software I developed. My program has turned on your camera and recorded the process of your masturbation. My software has also downloaded all your email contact lists and a list of your friends on Facebook. I have both the 'Euk.mp4' with your masturbation as well as a file with all your contacts on my hard drive.

You are very perverted!

If you want me to delete both the files and keep the secret, you must send me Bitcoin payment. I give you 72 hours for payment.

If you don't know how to send Bitcoins, visit Google.

Send 2.000 USD to this Bitcoin address immediately: xxxxxxxxxxxxxxx

Do not try to cheat me!

As soon as you open this Email I will know you opened it. This Bitcoin address is linked to you only, so I will know if you sent the correct amount.

When you pay in full, I will remove the files and deactivate my program. If you don't send the payment, I will send your masturbation video to ALL YOUR FRIENDS AND ASSOCIATES from your contact list I hacked.

Here are the payment details again: xxxxx

YOU CAN VISIT POLICE BUT NOBODY WILL HELP YOU. I KNOW WHAT I AM DOING.

I DON'T LIVE IN YOUR COUNTRY AND I KNOW HOW TO STAY ANONYMOUS.

Don't try to deceive me - I will know it immediately - my spy ware is recording all the websites you visit and all keys you press.

If you do - I will send this ugly recording to everyone you know, including your family.

I am waiting for your Bitcoin payment.

Anonymous Hacker

Security awareness

We have recently assisted several clients to ensure their technical security measures deployed are commensurate with identified risks such as GDPR, data and cyber security – listening to our clients revealed a forgotten yet crucial tool – staff.

Giving your staff the right information and setting parameters of operating through a clear set of processes and procedures is extremely important – it allows everyone to have the confidence to act when necessary.

All staff have a critical role in protecting the organisation – it's important that security rules and any adopted technology enables users to do their job as well as possible and not put the organisation at risk. This can be supported by a systematic delivery of awareness training that helps establish a security conscious culture and create accountability.

Actions and behaviour become second nature – a habit – like the steps you take before setting off in a car. It is just done and takes little thinking.

What are the risks you should consider?

Users must be able to do their jobs effectively. Organisations that do not successfully support staff with the right tools and awareness may be vulnerable to the following risks:

Removable media and personally-owned devices:
Without clearly defined and usable policies on the use of removable media and personally-owned devices, staff may connect unsafe devices to the infrastructure. However big or small the device, this might lead to the inadvertent import of malware or compromise of sensitive information.

Legal and regulatory sanction:
If staff are not aware and supported in how they handle sensitive information, the organisation may be subject to legal and regulatory sanction.

Incident reporting culture:
Without an effective reporting culture there will be a lack of quality dialogue between staff and those responsible for the systems (security team). It is essential to uncovering where gaps in technology and processes can be improved, as well as reporting actual incidents for legal reasons

The organisation should promote a security culture that empowers staff to voice their concerns about poor security practices and security incidents, without fear of recrimination for managers.

Security Procedures:
If the security procedures are not balanced to support how staff work, then security can be seen as a blocker, and thus ignored.

External attack:
Since staff have legitimate access and rights to the systems, they are usually the primary focus for external attackers and criminals. Attacks such as phishing or social engineering attempts rely on taking advantage of legitimate user capabilities and functions.

Insider threat:
Changes over time in an employee's personal situation could make them vulnerable to coercion, and they may release personal or sensitive commercial information to others. Unhappy staff may try to abuse their system privileges or coerce others to gain access to information or systems to which they are not authorised. Equally, they may just steal data.

How can you manage the risk?

Create a staff security policy:
Develop a user security policy, as part of the overarching corporate security policy. Security procedures for all systems should be produced with consideration to different business roles and processes. A 'one size fits all' approach is typically not appropriate for many organisations. Policies and procedures should be described in simple business-relevant terms with limited jargon.

Establish a staff induction process:
New staff (including contractors and third parties on system) should be made aware of their personal responsibility to comply with the security policies as part of the induction process. The terms and conditions for their employment, or contract, should be formally acknowledged and retained to support any subsequent disciplinary action.

Maintain user awareness of the security risks faced by the organisation:
All staff should receive regular refresher training on the security risks to the organisation. Consider providing the opportunity for staff to ask questions about security risks and discuss the advice they are given.

Monitor the effectiveness of security training:
Establish mechanisms to test the effectiveness and value of the security training provided to all users. This will allow training improvements and the opportunity to clarify any possible misunderstandings. Ideally the training will allow for a two-way dialogue between the organisation and its staff. Do not be afraid to work together and have difficult conversations about security risks.

Establish a formal disciplinary process:
Staff should be made aware that any abuse of the organisation's security policies will result in disciplinary action. Any sanctions detailed in the policy should be appropriate and enforceable at a practical level.

Bringing all the facets of security together (People, Physical and IT) is what the team at TenIntelligence excel in. If you would like to have a conversation about your security posture or assistance in reaching an applied standard, contact us via **info@tenintel.com**

Our due diligence, investigation and protection services

Working closely with our clients, we will continue to:

- provide our clients with the core tools to prevent, detect and investigate fraud & infringement
- protect our clients' reputations from risk through effective due diligence and investigation
- keep our clients' digital and physical resilience through appropriate 'security by design'
- protect our clients, people and their livelihoods from harm
- and deliver the highest levels of professional support, often in difficult circumstances, by building and maintaining trusted relationships

OUR SERVICES

DUE DILIGENCE

Organisations enter into financial and operational arrangements such as mergers, acquisitions, joint ventures, tenders and partnerships based on trust, people, financial results, opportunities and reputation.

We specialise in identifying the hidden risks by reporting on adverse elements to avoid potentially expensive mistakes before a prospective deal, engagement or transaction is completed.

All organisations are different, but they all require elements of compliance, screening and assurance.

INVESTIGATIONS

The detection of corporate fraud usually arises from an internal audit finding, an anonymous tip-off, suspicion, complaint, whistle-blower or allegation. In our extensive experience, suspicions of fraud are normally well-founded, irrespective of the source. We trust our clients' instincts and consult with them in depth to develop a strategy and investigation plan that suits the suspicion.

PROTECTION

An organisation's resilience is the ability to withstand changes to its operational environment without having to permanently adapt. The capability to effectively address the issues of security, preparedness and risk determines its strength to withstand brand crises, to deflect cyber attacks, and works to improve its reputation with stakeholders and customers. All organisations are different, but they all require elements of brand, cyber and data protection to maintain a successful and thriving enterprise.

For more details, please visit www.tenintel.com

Update from head office

Cally Choy joins the TenIntelligence team as Marketing Executive

Cally Choy has recently been named the Marketing Executive of TenIntelligence. As part of our growth strategy, we recognise the importance of providing our clients with regular and insightful information, as strengthening our activities will provide better awareness.

In order to support our ambitious vision, Cally will be responsible for organising events, and developing, implementing and monitoring a wide range of strategies, such as planning regular information sharing and conversations across social media.

Please follow our social media pages @TenIntelligence on LinkedIn, Twitter and Facebook. Visit www.tenintel.com for further information.

Veriflo Limited appoints TenIntelligence as advising consultants

TenIntelligence has recently been appointed by Veriflo as its external service provider to deliver data and cyber protection services. It is our great pleasure to assist such a successful organisation with its compliance in data protection, cyber security and response.

Veriflo
Water Asset Management

Neil Scott, Managing Director at Veriflo, confirmed the appointment: *"We have a commitment to diligence in providing clients with clean water asset management services. As part of our commitment, we have engaged the services of TenIntelligence to strengthen our ability to protect ourselves from future cyber threats."*

Neil Miller, CEO at TenIntelligence, commented: *"We are delighted to be working collaboratively with Veriflo. This joint approach sends a positive message to their clients and suppliers, but also positions them in maintaining their compliance to complement their continued success and excellent reputation in the water asset management environment. We keep 'Cyber Simplified'."*

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

TenIntelligence attends Compliance Week Europe 2018

Delegates from TenIntelligence attended the 2018 Compliance Week Europe Conference in Amsterdam for a third consecutive year. Our delegates came away with a wealth of new insights gleaned from highly-regarded speakers, benefiting from valuable knowledge sharing with like-minded compliance professionals from various jurisdictions and industries.

The conference, last November, pointed out that there are still a lot of uncertainties and challenges faced by organisations when making these regulations part of daily operations, especially for smaller businesses.

A main underlying theme of the conference was that, ultimately, 'culture' within an organisation determines the effectiveness and success of any compliance function or programme. Compliance departments should not exist in isolation, seen as the 'enemy' or an 'obstacle', but incorporated in all aspects of a business to build a culture of ethics and compliance. However, it is also important to remember every business is different, and any compliance programme or function should be tailored to the specific needs of each organisation.

The topic of Brexit was also broached – in particular, how it might affect EU and UK companies alike. From a GDPR point of view, things will only be changed to a small extent, due to the UK's Data Protection Act. It is expected that the UK will be regarded as a jurisdiction that provides an adequate level of protection. However, it may also be that the one stop shop will longer apply and that UK businesses will have to deal with multiple Data Protection Authorities post-Brexit.

To view the full article, please 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