Alliance Security Newsletter

Spring 2018

Welcome to the 2018 edition of the Alliance Security Times Newsletter. Every year is exceptional and very different in the life of the company and the year 2017 has turned out to be a stimulating year with hard won interesting security projects coming our way. We all look forward to an equally exciting 2018.

The Management, Brian, Daniel and Peter would like to send a huge thank you to our staff including our support security officers for their commitment and hardworking efforts during 2017. It is much appreciated.

You may have noticed that we recently have just launched a new website. We do have plans for this website to expand and become more interesting and for it to become a 'must visit' site which will be a 'shop window' to be proud of. It is planned for it to evolve and become required reading for our clients as well as all our staff who will have their own section.

A 'Lifesaver' on your smartphone
In this year's issue of the Newsletter we do have items which I hope will be of interest!

St Johns Ambulance Free App
At John's Ambulance have made available a free app for your smartphone. It could be a 'lifesaver' for yourself, your colleague or your family. Accidents do normally happen without warning.

Phantom Fraud (would you believe it!)

There is also a Warning from Action Fraud about Phantom Debt. Once you have read the article you will know exactly what to do if you were being set up as a victim of such a scam plus you know what to do if your family or friends became a victim of it.

Acid Attack advice

We have included the very serious SIA advice on responding to acid attacks. With the current vogue in such attacks it is a must said that everyone should be aware or what to do in the event of an acid attack either upon themselves or those around you.

European Data Regulations GDPR

GDPR New European Data Regulations GDPR are coming in force in May 2018 (Explanatory Doc) This will in different way have an impact on us all although it is new European Regulation which the UK has signed up for.

Security Officer Of The Year Nominated!

The Alliance Security officer of the year has been nominated: Yes it is you: Miles Davis who was adjudged by his peers to be a thoroughly dependable security officer, who can always be relied upon to carry out his duties diligently with good humour and have the well-being of the client and Alliance Security in mind. Well Done Miles!

What more can I say Miles, but Thank you and your reward is in the post.

Good Security – The ultimate balancing act!

Although we say it ourselves, and we mean it, we are a security company with a good reputation for being totally professional, trustworthy, effective and cost efficient. Our clients are well aware that when there is need to resolve security difficulties, they find by using our services these difficulties get settled very quickly!

The ultimate balancing act arises for us, with on the one hand the continued delivery of consistent professional management of quality security services, which we are known for. Where, on the other hand, where excellent services are being stressed with serious demands on price reduction for supply of regulated security manpower where vital overheads, including support management, on-site supervision and skills training, are stripped out to reduce operating costs. There is the ever present danger in this balancing act of creating a discriminatory two tier security industry which if it happens may make us complicit in the dumbing down of what is, and what should be, a vital professional service.

In meeting this challenge head-on, it must be said that security professionals within the industry need to work harder and run faster than anyone else at communicating the values of a fully managed service.

There is also an urgent need for better and more appropriate measures which we can to judge ourselves by. It has been said the ACS is perfectly fine as an entry level standard which needs only to be used by procurement teams as the very minimum standard for either style of service. However, there is nothing tangible and measurable currently in place that defines the higher standards of a professionally managed service. In short, those trying to offer such a service have no easy way of differentiating themselves from the market at large.

Have no fear! Alliance Security will continue to provide the best quality managed professional security available, whatever the 'Brexit' future may bring us all.

.....

Phantom Debt Fraud - Alert

The information contained within this alert is based on information gathered by the National Fraud Intelligence Bureau (NFIB). The purpose of sharing this information with law enforcement partners and key stakeholders is to assist in preventing/detecting crime, bringing offenders to justice and increasing awareness of enablers currently being utilised by criminals.

ALERT CONTENT

Action Fraud has recently experienced an increase in the number of calls to members of the public by fraudsters requesting payments for a "phantom" debt.

The fraud involves being cold-called by someone purporting to be a debt collector, bailiff or other type of enforcement agent. The fraudster may claim to be working under instruction of a court, business or other body and suggest they are recovering funds for a non-existent debt.

The fraudsters are requesting payment, sometimes by bank transfer and if refused, they threaten to visit homes or workplaces in order to recover the supposed debt that is owed. In some cases, the victim is also threatened with arrest. From the reports Action Fraud has received, this type of fraud is presently occurring throughout the UK.

PROTECTION / PREVENTION ADVICE

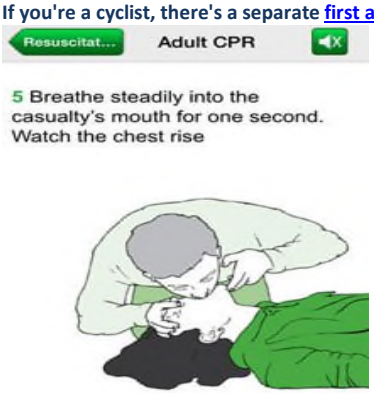
Protect Yourself

 Make vigorous checks if you ever get a cold call. Bailiffs for example, should always be able to provide you with a case number and warrant number, along with their name and the court they are calling from; make a note of all details provided to you. If you receive a visit from a bailiff, they must always identify themselves as a Court Bailiff at the earliest possible opportunity. Ask to see sight of their identity card which they must carry to prove who they are, this card shows their photograph and identity number. They will also carry the physical warrant showing the debt and endorsed with a court seal. If you work for a business and receive a call or visit, be sure to speak with your manager or business owner first. Never pay the debts yourself on behalf of the business you work for; some fraudsters have suggested employees make payment suggesting they can then be reimbursed by their employer when in reality the debt is non-existent.

FREE FIRST AID APP

Free First Aid Advice on your Smartphone

The free app (download for Apple/iOS, Android or BlackBerry) provides step-by-step guides, both in illustrated form and as voice instructions to keep your hands free for giving first aid.
If you're a cyclist, there's a separate first aid for cyclists app to keep with you while out on the road.



FREE REMINDER WHEN YOUR MOT IS DUE

Try This free Gov App to remind you when your vehicles MOT is due.

https://www.gov.uk/mot-reminder Sign up your **MOT** is due. ... You'll get another before your **MOT** is due.

to get free **reminders** by text message or email when **reminder** if you still haven't had your vehicle tested 2 weeks

……

A few mentions from Daniel

Firstly, congrats to Miles Davis on your recognition, providing your time & services on other assignments when called upon and your attitude to work is well deserved.

Client Contracts:

Please remember; whilst carrying out your roles on assignments, your duties, and requirements have been contractually specified with our customer. It has become increasingly noticeable; some staff members have been unable to carry out their duties due to situations beyond their or our control but have not made the Alliance Control Room aware. It is a fundamental requirement, any situation, incident or condition that prevents you from carrying out your role to its fullest, should be first communicated to the control at your earliest opportunity. Control will then notify the acting Duty Manager accordingly for guidance on the situation. Without these vital notifications, we cannot convey the problems onto our customer and provide preventative action going forward. I am sure we can rely on your cooperation on this matter. Any incident should be communicated to the control room followed by a logbook entry and FULL incident report.

TelMe:

Do remember, Alliance provides you with a portal so you can see your work schedules both historically and in the weeks ahead. Tell me comes in the form of an app you can download to your smartphone on both IOS and Android. Simply search the app store or play store for Gallinet and download the TelMe application. Enter the company name "alliance" followed by your name and followed by your pin number. This will provide you with some useful information.

Anti Terrorism:

The NCTSO National Counter Terrorism Security Office should be a website known to some of you already but I would encourage those that haven't looked at it, to certainly take a look. It provides a wealth of information and educational facts on what advice to follow in such instances as a terrorist attack and indeed, recognising one. The videos available to watch are – Identify and respond to suspicious behaviour – Identify and deal with suspicious items – How to react to a firearms or weapons attack & an Introduction to counter terrorism awareness. All of this can be found at https://www.gov.uk/government/organisations/national-counter-terrorism-security-office

You're Pay

The team at Alliance work very hard to ensure the pay you receive at the end of each month is not only delivered to you in a timely manner, but also that it is correct. We have a very good track record with regards to minimal wage discrepancies however I would urge everyone, when you receive your wages, payslips and time sheets, to check them and anything your unsure of or you think you have been paid incorrectly, to contact Alliance Security during office hours at your earliest convenience so we can handle your query immediately.

Duty Manager(s)

As you're all aware, we dedicate ourselves to the smooth running of the business, 24 hours per day, 365 days per year, Brian, Peter and I, work to a duty manager schedule, ensuring the company has a dedicated decision maker available during all hours of business being a 24 hour company. As always, during normal office hours Monday to Friday between 0830hrs – 1800hrs, do call the office on 0344 800 6898 and someone will be able to take your call. **Outside of these hours**, if your situation is urgent, please call the control room and they will contact the scheduled on call manager. Please do not call Manager's directly on their mobile phones outside of office hours, like you, we all enjoy our time away from work when not on call, and we don't always have our work phones with us. So to avoid disappointment, please call the control room and they will pass on your message accordingly.

Peter Moss's Corner

I have now been with Alliance for around 18 months and I must add it has been a busy, challenging but most of all, an enjoyable time. I would like to thank all staff members for all their hardwork and commitment over last year However, may I take this opportunity to highlight some areas where I feel everyone needs reminding on;

WEBSITE: Alliance have a new website, www.Alliancesecurity.co.uk which features a staff resources section where you can view the following;

- Training: A list of online courses available to all employees via citation
- Human Resources: A link to your citation log in area
- A copy of the Alliance employee handbook
- The latest Alliance newsletter

BOOKING ON AND OFF: Can I please remind all staff to ensure you book on at the start of your shift and book off at the end of your shift.

CHECK CALLS: If checks calls are in place on site, please ensure these are made on time. They are in place for your own safety part of your duties as a security officer.

COMMUNICATION: Can I please remind all staff if for any reason you are running late for your shift or are unable to attend work you must inform our 24-hour control room on 01384 215384 as soon as possible.

INCIDENT REPORTING: It has been noted of late, numerous site incidents are not being reported in the correct manner, and key information is being either delayed in reaching us or not at all. I would respectfully ask all staff members, if an incident occurs, you are required to notify Alliance via its 24-hour control room on 01384 215 384 and a Duty Manager will be contacted and briefed accordingly. An incident report must then be completed in full and faxed/emailed to Alliance. If fax/email is not available on your site, please leave the complete report in your logbook and a member of the management team will collect the incident report at the next available opportunity.

HOLIDAY: Can I ask all staff to try and spread their holiday our over the year and give Alliance as much notice as possible, this will then give us a much better chance of finding suitable cover.

UNIFORM: Can I please remind you whilst on duty you MUST ensure you are in FULL clean and pressed uniform at all times, this includes;

- White Shirt
- Alliance Tie
- Black Trousers
- Black Shoes
- Hi vis jacket/vest (if applicable to your site)
- Your valid SIA licence – Remember if you fail to display your licence this can result in your licence being revoked, six months imprisonment and/or a fine of up to £5,000
- Your valid Alliance ID Card

Should you feel you need any new uniform please contact the Alliance office during normal working hours.

Paula and Terry from finance

The department continues to be staffed by Paula Sabine who is a qualified MAAT Book-keeper and Terry Henshaw who handles payroll and finance administration.

Last year, Paula took part in the 46-mile London Cycle Ride event which she completed in approximately 4.5 hours and raised over £650 for the Princess Alice Hospice. She even managed to cycle up Wimbledon Hill without stopping! At the end of May 2018, she is running the Vitality Health 10K in London.

Terry continues to ride and assist with the training of horses. She has just spent 6 weeks in Australia visiting her family.

We share the finance duties and, although not full-time employees, we try to ensure that at least one of us is in the office Monday to Friday, to answer any queries. The Finance Department is very much a 'back room' function providing information and support to the other departments and the Directors.

Terry and Paula are responsible for the invoicing of clients, the payment of suppliers, and the preparation of monthly accounts for the Directors and, of most interest to employees, we operate the payroll system.

Please remember if you do have any queries concerning the hours you have worked these should be referred to Peter Moss or Daniel Harper for clarification. Should you have a query concerning general payroll related matters then Paula or Terry will be happy to help you.

You will appreciate that it is extremely important that any change to your address should be notified to the payroll department in writing as soon as possible, just as you should notify the SIA immediately of any changes. We also require any alterations to banking details to be notified in writing in order to ensure that pay is forwarded to the correct bank account. Processing of the wages takes place on the 21st of each month and any alterations must be received before this date.

SIA ADVICE: Responding to Acid Attacks

We are asking licence holders and security businesses to familiarise themselves with the available guidance on responding to acid attacks. This is in response to recent acid attacks against members of the public, and a very small number of such attacks against licence holders.

An acid attack involves a corrosive substance being thrown or sprayed on a person or people as part of a violent attack or robbery. Although 'acid attack' is the phrase most people use to refer to such incidents, they can involve acidic, alkaline or caustic chemicals. Household cleaners, drain un-blockers and industrial chemicals might all be used by perpetrators.

NHS Guidance

NHS England and the British Association of Plastic, Reconstructive and Aesthetic Surgeons (BAPRAS) have issued first aid guidance on how to ensure victims of acid attacks get the right help fast. They are asking people to remember the 3 R's:

- **Report** the attack: dial 999
- **Remove** contaminated clothing carefully
- **Rinse** skin immediately with running water

NHS Choices has also issued more detailed guidance for the public on how to treat acid and chemical burns.

Equipment

Employers and venue owners should be aware of their responsibility to conduct risk assessments associated with acid attacks and plan for how to respond to them subject to the Health and Safety Act 1974 as well as the Control of Substances Hazardous to Health Regulations 2002. This includes supplying appropriate equipment for responding to an acid attack. We cannot recommend individual equipment items, but you may want to consider the following equipment which is carried in Metropolitan Police Service (MPS) vehicles for police officers to use.

- 1 x high density recycled plastic box with seal - the MPS use this to hold their equipment safely in transit or in situ.
- 2 x chemical resistant gloves - basic latex gloves will only provide a short (20-30 seconds) of protection against a corrosive substance. For longer term use, laboratory suppliers sell thicker, purpose-built gloves.
- 2 x anti-fog, chemical-resistant goggles - these can also be sourced using websites that provide safety equipment for laboratories.
- 1 x 5ltr water bottle - this is the minimum amount to be used on a victim, there is no maximum, and is enough for 10 minutes of constant dousing of water.
- 2 x bottle shower caps to control the rate of water pouring from a bottle. These essentially turn a bottle of water into a shower and you can find these online under the title “bottle shower head".
- 2 x good quality scissors capable of cutting through clothing - these are the sort of scissors you can find in larger first aids kits and being used by paramedics. They often go by names like tough cut scissors, tuff cut scissors or paramedic shears.
- 4 x face shields recommended by the Health and Safety Executive - these can be purchased from reputable chemical suppliers.

The police, fire brigade and ambulance service will bring their own, more specialised equipment when they respond to an acid attack.

Getting bottles or jugs of tap water from the bar might be the quickest and easiest method to do the 'Rinse' of the 3 R's in a licensed premise like a pub or nightclub.

We will update the above information when further guidance on how to prevent and respond to an acid attack becomes available.

.....

General Data Protection Regulation (What is it & How does it affect all of us?)

What is the GDPR?

The EU's General Data Protection Regulation (GDPR) is the result of four years of work by the EU to bring data protection legislation into line with new, previously unforeseen ways that data is now used.
Currently, the UK relies on the Data Protection Act 1998, which was enacted following the 1995 EU Data Protection Directive, but this will be superseded by the new legislation. It introduces tougher fines for non-compliance and breaches, and gives people more say over what companies can do with their data. It also makes data protection rules more or less identical throughout the EU.

Why was the GDPR drafted?
The drivers behind the GDPR are twofold. Firstly, the EU wants to give people more control over how their personal data is used, bearing in mind that many companies like Facebook and Google swap access to people's data for use of their services. The current legislation was enacted before the internet and cloud technology created new ways of exploiting data, and the GDPR seeks to address that. By strengthening data protection legislation and introducing tougher enforcement measures, the EU hopes to improve trust in the emerging digital economy.

Secondly, the EU wants to give businesses a simpler, clearer legal environment in which to operate, making data protection law identical throughout the single market (the EU estimates this will save businesses a collective €2.3 billion a year).

When will the GDPR apply?
The GDPR will apply in all EU member states from **25 May 2018.** Because GDPR is a regulation, not a directive, the UK does not need to draw up new legislation - instead, it will apply automatically. While it came into force on 24 May 2016, after all parts of the EU agreed to the final text, businesses and organisations have until 25 May 2018 until the law actually applies to them. While the overwhelming majority of IT security professionals are aware of GDPR, just under half of them are preparing for its arrival, according to a snap survey of 170 cyber security staff by Imperva. Just 43% are assessing GDPR's impact on their company and changing their practices to stay in step with data protection legislation, Imperva found. While the respondents were mostly US-based, they would still be hit by GDPR if they handle - or contract another firm to handle - EU citizens' personal data. Despite this, nearly a third said they are not preparing for the incoming legislation, and 28% said they were ignorant of any preparations their company might be doing.

So who does the GDPR apply to?
'Controllers' and 'processors' of data need to abide by the GDPR. A data controller states how and why personal data is processed, while a processor is the party doing the actual processing of the data. So the controller could be any organisation, from a profit-seeking company to a charity or government. A processor could be an IT firm doing the actual data processing. Even if controllers and processors are based outside the EU, the GDPR will still apply to them so long as they're dealing with data belonging to EU residents. It's the controller's responsibility to ensure their processor abides by data protection law and processors must themselves abide by rules to maintain records of their processing activities. If processors are involved in a data breach, they are far more liable under GDPR than they were under the Data Protection Act.

When can I process data under the GDPR?
Once the legislation comes into effect, controllers must ensure personal data is processed lawfully, transparently, and for a specific purpose. Once that purpose is fulfilled and the data is no longer required, it should be deleted.

What do you mean by 'lawful'?
'Lawfully' has a range of alternative meanings, not all of which need apply. Firstly, it could be lawful if the subject has consented to their data being processed. Alternatively, lawful can mean to comply with a contract or legal obligation; to protect an interest that is "essential for the life of" the subject; if processing the data is in the public interest; or if doing so is in the controller's legitimate interest - such as preventing fraud.

At least one of these justifications must apply in order to process data!

How do I get consent under the GDPR?
Consent must be an active, affirmative action by the data subject, rather than the passive acceptance under some current models that allow for pre-ticked boxes or opt-outs. Controllers must keep a record of how and when an individual gave consent, and that individual may withdraw their consent whenever they want. If your current model for obtaining consent doesn't meet these new rules, you'll have to bring it up to scratch or stop collecting data under that model when the GDPR applies in 2018.

What counts as personal data under the GDPR?
The EU has substantially expanded the definition of personal data under the GDPR. To reflect the types of data organisations now collect about people, online identifiers such as IP addresses now qualify as personal data. Other data, like economic, cultural or mental health information, are also considered personally identifiable information. Pseudonymised personal data may also be subject to GDPR rules, depending on how easy or hard it is to identify whose data it is. Anything that counted as personal data under the Data Protection Act also qualifies as personal data under the GDPR.

When can people access the data we store on them?
People can ask for access at "reasonable intervals", and controllers must generally respond within one month. The GDPR requires that controllers and processors must be transparent about how they collect data, what they do with it, and how they process it and must be

clear (using plain language) in explaining these things to people. People have the right to access any information a company holds on them, and the right to know why that data is being processed, how long it's stored for, and who gets to see it. Where possible, data controllers should provide secure, direct access for people to review what information a controller stores about them.

They can also ask for that data, if incorrect or incomplete, to be rectified whenever they want.

What's the 'right to be forgotten'?
Individuals also have the right to demand that their data is deleted if it's no longer necessary to the purpose for which it was collected. This is known as the 'right to be forgotten'. Under this rule, they can also demand that their data is erased if they've withdrawn their consent for their data to be collected, or object to the way it is being processed.

The controller is responsible for telling other organisations (for instance, Google) to delete any links to copies of that data, as well as the copies themselves.

What if they want to move their data elsewhere?
Controllers must now store people's information in commonly used formats (like CSV files), so that they can move a person's data to another organisation (free of charge) if the person requests it. Controllers must do this within one month.

What if we suffer a data breach?
It's your responsibility to inform your data protection authority of any data breach that risks people's rights and freedoms within 72 hours of your organisation becoming aware of it. The UK authority is the Information Commissioner's Office. Information commissioner Elizabeth Denham believes the authority needs more resources to cope with policing GDPR, and responding to organisations who notify it of breaches. In March 2017, she told the EU Home Affairs Sub-Committee that more funding was necessary to recruit and retain skilled people. That deadline is tight enough to mean that you probably won't know every detail of a breach after discovering it. However, your initial contact with your data protection authority should outline the nature of the data that's affected, roughly how many people are impacted, what the consequences could mean for them, and what measures you've already actioned or plan to action in response.
But even before you call the data protection authority, you should tell the people affected by the data breach. Those who fail to meet the 72-hour deadline could face a penalty of up to 2% of their annual worldwide revenue, or €10 million, whichever is higher.

If you don't follow the basic principles for processing data, such as having a legal basis for doing so, ignore individuals' rights over their data, or transfer data to another country, the fines are even worse. Your data protection authority could issue a penalty of up to €20 million or 4% of your global annual turnover, whichever is greater.

If you take recently issued fines issued by the ICO - which can hand out a maximum penalty of £500,000 - and scale them up under GDPR, you can see how much tougher the penalties for getting data protection wrong could soon become. So under GDPR, TalkTalk's record £400,000 fine would actually total £59 million - that's a pretty big chunk of the telco's third quarter 2016 revenue, which was £435 million. Meanwhile, the ICO's total issued fines for 2016, which amounted to £880,500, would become £69 million from 25 May 2018, according to risk mitigation firm NCC Group - 79 times higher. However, it's important to note that while the maximum fines that can be issued will become much higher under GDPR, the legislation stipulates that they must remain "proportionate" to the breach. Also, if you can demonstrate that you work hard to ensure your organisation is compliant with GDPR, the ICO would likely not issue as high a fine in the event of a breach as it would otherwise.

But what about Brexit?
Yes, the UK is leaving the EU - but because the UK government only triggered Article 50 in March, which sets in motion the act of leaving the EU within a two-year timeframe (though it could take longer), means the GDPR will take effect before the legal consequences of the Brexit vote, meaning the UK must still comply for the time being.

Karen Bradley, secretary of state for Culture, Media and Sport, said in October 2016: "We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."
A new Data Protection Bill, put forward by the UK government in August 2017, essentially replicates the requirements under GDPR. Once the bill is passed, it will help to clarify the regulations for protecting data once the UK leaves the European Union, by creating a British version of GDPR in all but name.
Much like the stipulations of GDPR, the bill sets out sanctions for non-compliant organisations, permitting the Information Commissioner's Office to issue fines of up to £17 million, or 4% of global turnover, whichever is highest (compared to €20 million and 4% of turnover under GDPR).

It also provides provisions for the right to be forgotten, adding the ability for data subjects to demand social media companies erase any posts they made during childhood, which will most likely be used in those cases where individuals are ashamed of historical comments.

The bill also acts to modernise current data protection regulations by expanding the definition of personal data to include IP addresses, internet cookies, and DNA.

By harmonising data protection laws, the UK is hoping to gain a "whitelisted" status from the EU, meaning that protections are robust enough to allow data to move freely between the regions. This is going to be essential for those businesses that operate in both the UK and the EU, as without that guarantee, organisations would need to choose whether to place their operations inside or outside of the UK.

Digital minister Matt Hancock said: "Bringing EU law into our domestic law will ensure that we help to prepare the UK for the future after we have left the EU. We are committed to ensuring that uninterrupted data flows continue between the UK and the EU and other countries around the world while the process has started to harmonise data regulations, what's unclear is whether the new legislation will be deemed compatible with GDPR once the UK leaves the EU. For example, under the UK's Investigatory Powers Act, ISPs are compelled to collect personal web histories and hold them for up to 12 months.

While GDPR does allow for organisations to collect and process data to comply with a legal obligation, national security laws are also a factor the EU will consider when deciding if the UK provides adequate (equivalent) protection for people's data when it exits the EU.The UK's new Data Protection Bill aligns with GDPR, and hopes to build an enhanced data protection mechanism that goes beyond the adequacy model the EU imposes on 'third' countries. But the European Union Committee has pushed the UK government on whether its controversial national security legislation might scupper such an agreement between the EU and UK following Brexit.

Matt Hancock, minister of state for digital, responded in October 2017 to say that such laws shouldn't prove an insurmountable obstacle, however.

"The UK is already compliant with EU law on data protection and is confident that UK national security legislation should not present a significant obstacle to data protection negotiations," he wrote. "The activities of UK security and intelligence agencies are governed by one of the world's most robust legal frameworks and oversight arrangements, which ensure UK intelligence activity adheres to strict principles of necessity and proportionality." The UK also wants the ICO to continue to play a role on the EU Data Protection Board, which comprises all EU member states' data protection regulators, and governs data protection rules. Hancock said in the letter that he is confident this can happen, writing: "Given the ICO's reputation as a highly regarded, pragmatic regulator, we believe that their continued participation would be invaluable to both the UK and EU's data protection regulatory frameworks."

.....

As a footnote to this year's Newsletter the editor would like to receive any news, gossip, photographs accompanied with articles or interesting security stories to be included in our next edition. We look forward to receiving your contribution. Do not be shy!"