New year, new beginnings and new ideas
At the beginning of the new year it is traditional to look ahead and make fresh plans. If you do have new plans underway or a new campaign waiting to take off, then please also remember to speak to us and let us know how we can support you.

We have a broad range of means available ranging from mail-outs for members, through to newsletters in print and online and our own social media activity.

We start this year with 4 events of our own following in quick succession – the first of these is our Metal Theft Summit on the 23rd of February, our annual cyber conference on the 9th of March, our annual Best Bar None National Awards on the 24th of March and then leading to our 2nd National Anti-Ilicit Trade Summit in May.

You will see details of all of these events and once again we are offering membership discounts on the booking fees in order to make these as accessible as possible. All of the team have worked really hard since the end of last year to bring some genuinely outstanding speakers to these events so we hope that you will find them attractive and helpful.

On the digital side we are still involved in the research work with Glasgow University, asking small companies why digital security messages are not working for them currently and what would make security advice more relevant to them. If you can spare time to go through this, then we would be hugely grateful – just email us.

What obstacles will you face? How will you take your staff forward and develop them? Alas, we don’t have a crystal ball but we know that fraud and cybercrime is going to increase this year. After the terrible weather flooding so many homes and businesses, resilience plans for such disruption must be a priority to everyone. Take advantage of your membership, make the most of it, and make it work for you. You are our member and it is our priority to provide as much help as you need. Our workstreams cover all the issues you may face and we have a wealth of knowledge and experience that cannot be found anywhere else - and it is all here at your disposal.

**Tracy Hope, Head of Marketing & Membership, SBRC**

---

**EU set to agree new data privacy law with stiff penalties**

The new EU laws are coming your way!

One of the most worrying consequences will be large fines for businesses who lose customer data. Hackers, of course, increasingly attempt to gain access to your customer data.

Some of the new policies expected to be approved:

- Allow national watchdogs to issue fines, potentially totaling the equivalent of millions of dollars, if companies misuse people's online data, including accessing information without individuals’ consent.
- Enshrine the so-called right to be forgotten into European law, giving people in the region the right to ask that companies remove data about them that is either no longer relevant or out of date.
- Require companies to inform national regulators within three days of any reported data breach, proposals that go significantly further than what is demanded by American authorities.

Karen Renaud is a Computer Scientist from the University of Glasgow (www.dcs.gla.ac.uk/~karen)

She is currently seconded to the Scottish Business Resilience Centre looking at how to support SMEs more effectively in terms of resilience to cyber attacks. She would really like to speak to folks in SMEs (small/medium businesses) (max 20 minutes). All interviews will be anonymised and can be done in person or over the phone. There is also an online survey if folks don’t have time to chat to her (should take 5 minutes): http://tinyurl.com/sbrc-survey

Karen’s email is karen.renaud@sbrcentre.co.uk, please get in touch with her.
CYBER CRIME DON’T BE A VICTIM

I grew up in an era when I was taught that crime does not pay, but sadly a new generation has come through the cyber arena believing that crime can pay and we make it easy for cybercriminals if we don’t take simple precautions.

We can protect our families, our businesses and ourselves if we are careful with things we use on a daily basis such as our primary email account, bank account, social media accounts and mobile phone.

Email:
- Add a recovery email address to your primary email account so that if someone changes your password or your personal details, you will be told and can take action before harm is done.
- Make your password complex, but not hard for you to remember, using special characters if you can. A passphrase might help you to remember. Iliketoplaybadmintonatcollege could be il2pb@coll.
- Change your password regularly, and don’t use the same password for all accounts. You could add TR to the end of your Twitter password and EL to the end of your email password.
- If your email supports it, use two-factor validation at login. You can set Gmail for example, to send a text containing a code to your mobile and this code is needed to complete the login. So even if someone gets your password, they can’t log in unless they also have your (unlocked) phone. It takes slightly longer to login, but is much more secure than a password on its own and so much easier than trying to recover a hacked email account.

Bank accounts:
Ask if your bank can set text or email alerts when changes are made to your account, particularly:
- When new bank cards are issued or your personal details are changed.
- When new payment instructions are set up.
- If the balance falls below a pre-set level. Also useful to avoid overdrafts as you can pay cash in to put the account back into credit.

These types of changes can be an indicator that criminals have access to your bank details. If you are concerned about any payment or instruction, phone your bank using a number you know to be correct such as the number on your bank debit card. If you use online banking, keep your system software and anti-virus software up to date whether that is on a PC, mobile or tablet. Log in regularly and check all transactions.

Social Media - Use it wisely:
- Check your privacy settings to limit what is public. Limit what you do share to people you trust (for example, only friends can see updates).
- Do not reveal personal information – keep it personal. Criminals can build up a picture of you from many sources and use it to steal your identity.
- When you post information, it can be there forever! Don’t rely on being able to delete it.
- Don’t tell people when you are away from home. Knowing your house or business might be empty is great news for burglars.

Mobile phones:
Many security systems rely on your mobile phone rather than email for sending you alerts, so it is important to protect your phone.
- Make sure you have a SIM lock code (and don’t make it your birth year or anything anyone could guess easily)
- Set up an auto screen lock after a minute or two of inactivity. This reduces the chance of someone finding your phone being able to see your data or make expensive telephone calls at your expense. If your phone company supports bill capping, ensure it is set for the amount you wish.
- Switch on ‘Find my phone’ services if you can – it makes finding and recovering phones so much easier.
- If you can, set your phone to securely erase itself after a number of wrong attempts to enter the passcode – but make sure you have regular backups. Many phones can automatically back themselves up each night.
- Use anti-virus software and keep it up to date.

Trust:
Trust is a great thing, but many criminals rely on you being trusting – too trusting! Emails are not secure and there are many examples of emails, purporting to be legitimate, telling people that bank details for a payment due to be made have changed. Don’t rely on these ‘instructions’. If a payment has to change, speak to the person you are due to pay and confirm the payment instructions, and use a phone number you know to be correct – don’t rely on a contact number in an email as it could be false too.

Finally, and especially for businesses:
Make sure your staff know that if they get an email purporting to be from a senior person in the business insisting an unusually large payment or several smaller ones are made immediately, they should ALWAYS check before making the payment, or perhaps set up a pre-determined code that needs to be in an email before they follow the instructions. Criminals give very plausible reasons to create a sense of urgency so that staff over-ride their normal common-sense checks, but if managers or owners make it clear to all staff that they must check if a payment is over a certain amount, then the chances of this type of fraud are reduced. It can be almost impossible to recover the money when it has gone, despite the best efforts of banks.
Make it harder for criminals. Don’t let crime pay. You know it makes sense.

Brian Barbour, Information Security Consultant
70% of employees can’t spot a phishing site

Phishing attacks have dramatically increased over the past few years and are fast becoming a cyber criminal’s weapon of choice.

But would your employees know how to spot the signs or could they be exposing your organisation to an attack? Through our phishing simulation tool, Piranha, we found that 70% of employees at large organisations cannot tell a legitimate website from a phishing site, Protecting against phishing attacks is crucial and a 70% success rate for an attack with relatively low sophistication puts the importance of employee education and the need for cyber resilience into perspective. Over 500 emails were sent over a two month period, and 22% of recipients clicked through to a malicious site, and of these 70% then went on to supply credentials. Armed with this information, an attacker could gain a foothold within an organisation’s infrastructure. The emails were tailored to each target organisation but were not personalised for each individual. Phishing of this sort is the tool of choice for a number of threat actors – particularly organised crime rings and state sponsored attackers that want to infiltrate a target organisation. Once they’ve obtained valid credentials they can quickly move deeper into the organisation’s infrastructure in order to often obtain access to sensitive data and then look to retain access. We discovered through the use of Piranha that the minimum time it takes for an organisation to be breached by a phishing attack is 1 minute and 29 seconds. We launched Piranha to help customers who wanted to bolster their staff awareness training efforts as well as their technology at the gateway. Piranha allows them to create and send their own simulated emails to an unlimited number of their internal staff members, which, for large organisations is very cost effective compared to some other tools on the market.

TransAtlantic Trade and Investment Partnership – what does it mean for the Food & Drink Sector?

The proposed treaty between the US and EU is intended to open up both markets to increased exports from the other and the reduction in tariffs and bureaucracy with associated harmonization of regulatory requirements opens up some exciting possibilities.

Proponents of the treaty have suggested that the European economy could be increased by more than €100 billion or 0.5% GDP there is however increasing ground level hostility to the treaty. Some of this hostility seems to be motivated by distaste for “globalisation” or concerns about the “secrecy” of the negotiations or the investor state dispute resolution mechanism. Surely however one would expect treaty negotiations to be conducted in confidence and in fact there has been unusual openness around TTIP. Regular updates on the discussions can be found at http://ec.europa.eu/trade/policy/in-focus/ttip/index_en.htm. Similarly most free trade treaties include a special arbitration clause for investor disputes however in this case the Commission is proposing a special court with publically appointed judges, rights of intervention and very public processes. One still might argue why such disputes cannot go to the normal courts but the proposal goes a long way to meet concerns about the arbitration model and is at least worthy of some discussion.

In fact there are a number of much more controversial aspects of the proposed treaty for food and drink producers. The US is generally believed to have much less stringent regulations on health and safety and so there is concern that “harmonisation” may mean lowering EU standards as has alleged to have already occurred around endocrine disrupting chemicals. Areas that have received particular publicity include the chemical washing of meat, the use of antibiotics and hormones as growth promoters, the acceptance of genetically modified crops, reduced port of entry checks and animal welfare. There is also concern about the different approaches to the use of chemicals as pesticides and in packaging materials – the US approach is that a material is acceptable unless proven to be dangerous whereas the EU precautionary approach has been that chemicals must be proven safe before use. The result is that around 80 more chemicals are in general use in these areas in the US than in the EU. Another area of concern for this sector specifically is the potential undermining of the geographical indication schemes that protect products particularly associated with specific places like champagne or Cornish pasties. Contrary to its TRIPS obligations the US does not have a general scheme to protect products of this type and with few exceptions prefers to rely on the very different trademark laws. As with the recent Canadian treaty (CETA ) it is unlikely that all EU registered products will be accorded protection under the treaty. It should be noted that while other governments are lobbying to ensure their regional specialities are specifically protected the UK government does not seem to be seeking protection for UK specialities. The Scottish food and drink sector is an amazing success story and the US our largest market. This treaty could lead to more opportunities for the ambitious but there are risks with the current plans. Rather than throwing away all the potential benefits by rejecting the treaty as a whole what is perhaps needed is careful targeted lobbying to ensure that the voice of this important sector is heard and its interests addressed.

Patricia Barclay, Bonaccord. The author is proud to represent a number of innovative food and drink brands. www.bonaccord.eu
Rail pastors aid revellers at Falkirk

Network Rail in Scotland and British Transport Police have joined the Safer Streets partnership in Falkirk to help identify and support vulnerable people at night and highlight the dangers of misusing the railway.

- who routinely patrol Falkirk in search of vulnerable people requiring assistance around pubs and clubs at closing time - will now include Falkirk High and Falkirk Grahamston stations as part of their route on a trial basis. Advised by British Transport Police, it is hoped their presence will deter people from potentially engaging in anti-social behaviours in and around the railway and encourage them to get home safely after a night out while identifying and supporting vulnerable individuals who may require further assistance and guiding them to a place of safety.

The pastors will also be given TACTICS cards designed to be placed in a lanyard holder. These provide guidance on how to intervene if you meet a vulnerable person considering suicide and include key support telephone numbers.

Senior communications manager for community engagement Mark Henderson said: “Street pastors are an invaluable resource for the local community and emergency services, providing a recognisable presence for people who may require minor first aid or who are suffering from more serious problems such as poor mental health.

“Their presence at Falkirk High and Falkirk Grahamston stations is a welcome support that we hope will prevent tragic incidents and antisocial behavior from happening on the railway by moving people to a place of safety where they can receive the care that they need.

“We are now looking at ways to enhance the existing street pastor programme and are working with BTP and charity Street Pastors to introduce dedicated rail pastor roles in to the Scottish network.”

Network Rail’s involvement in Safer Streets and the Safe Base initiative is supported by the Edinburgh Glasgow Improvement Programme (EGIP) that will electrify the Edinburgh Waverley-Glasgow Queen Street line from December 2016 to deliver faster, longer and greener trains. Alongside Network Rail and BTP, there are several Safer Street partners including Street Pastors, British Red Cross, Police Scotland, Scottish Fire and Rescue, Falkirk Delivers and the Scottish Business Resilience Centre as part of their Safer Areas initiative.

Branded emergency packs containing water, a foil blanket and even flip flops for people who have had to remove their shoes because of sore feet will be distributed to those who need them over the coming months.

Working with service providers and volunteers on a project called Safe Base, on busy winter nights, the partnership will try to enhance safety while reducing crime and anti-social behavior to make the town a more enjoyable place for partygoers, businesses and the wider community.

As part of the initiative, voluntary street pastors

European Commission (EC) - Changes to the European Data Protection Rules

The European Commission is currently undertaking a reform of its data protection rules to strengthen the rights and expectations of citizens including online privacy rights as well as providing clearer “modern” rules to boost Europe’s digital economy.

The Commission’s objectives include two key legislative proposals: a Regulation setting out a general EU framework for data protection and a Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

The British Security Industry Association have a copy of the latest press release from the EC, which provides an update on an agreement on the EU data protection reforms and how it is expected to benefit companies / businesses reducing costs of compliance. The press release also contains some useful links to the background information on the ECs aims to achieve a Digital Single Market and Privacy - by - Design principals in standardisation. The final texts are expected to be formally adopted by the European Parliament and Council early 2016 with the new rules becoming applicable 2 years thereafter. If you would like a copy of the press release please contact Willie Clark, Scottish Regional Representative, BSIA at w.clark@bsia.co.uk or contact via SBRC.

The BSIA is the trade association for the private security industry in the UK and its members provide over 70% of UK Security products and services and adhere to strict industry standards.
BBN Scotland launch exclusive Insurance product to accredited premises

Best Bar None Scotland has partnered with Insurance Brokers Harper Stairmand to bring Best Bar None accredited premises an exclusive insurance discount which will result in potential savings of between 10% and 20% annually. To find out more please read the information below.

At renewal of your venue’s insurance consider:

- **This Exclusive benefit** to Best Bar None Scotland Accredited Premises
- Applies to pubs, bars, hotel bars, social clubs, sports clubs, music venues, night clubs and late night venues.
- Contact Harper Stairmand Insurance Brokers on: graeme@harperstairmand.com – Mobile No: 07889-499312
- Your dedicated point of contact is: Graeme Harper
- Harper Stairmand will visit you and do a full consultation in relation to your Insurance cover
- Harper Stairmand will deal direct with you and complete the full administration process with you
- Harper Stairmand will provide all documentation direct to you
- Harper Stairmand will maintain contact with you direct to manage your Insurance provision

**POTENTIAL SAVINGS OF BETWEEN 10%-20% ANNUALLY**

Don’t Forget! The Best Bar None Scotland National Awards will be taking place in Glasgow this year on the 24th of March.

**NATIONAL AWARDS 2015/16**

Thursday 24th March 2016
at The Grand Central Hotel, Glasgow.
Girl Geek Scotland was formed in 2009 to create a network for women working with “Creativity, Computing and Enterprise”, in Scotland. GGS aims to develop a network of women, who are able to support each other at entry-level, and throughout their careers, working at the intersection between these areas.

It is very much hoped that this work will link into the Scottish Business Resilience Centre (SBRC) by promoting innovation and business improvement support, working in partnership with the business community. As such, Girl Geeks shares the objective of SBRC in promoting a ‘Secure Scotland for Business to Flourish in’. In effect, creating a secure environment where business can trade and prosper securely, regardless of size and sector. This encompasses everything from premises and employee safety to cyber security.

Although Girl Geek Scotland markets its products towards women, it welcomes people of all gender identities, and particularly encourages men to be involved, who can offer support in working towards a gender balanced, career ecosystem.

Girl Geek Scotland knows that to develop a healthy ecosystem to support women, it needs to focus on different ‘market segments’ or audiences that make up the ecosystem: women in corporates and established technology based businesses, women going through career transitions, students of technology or enterprise, female entrepreneurs, and women who work with technology, such as developers.

This all ties in with the Scottish Government aims of creating a wide range of business security services and advice, establishing hubs of innovation and business improvement, as well as addressing the gender gap in ICT to meet that demand; the Scottish Government recognises the digital sector as key driver of economic growth.

Girl Geek Scotland aims to:

- Consolidate Links with USA & London
- Develop new International Links
- Support Female Startup community with network & skills acquisition
- Support Industry in growing need for Data Science Specialists and encourage talent to Scotland

Projects:

- MSc Scholarships in Data Science
- Girl Geek Dinners
- Entry level workshops in coding and startup skills

Edinburgh Napier University’s School of Computing and Bright Red Triangle (BRT) are delighted to announce their partnership with Girl Geeks Scotland (GGS), hosting a launch in February 2016 with First Minister Nicola Sturgeon.

Collection of Interviews and Articles for an eBook

Core Themes:

- Thinking Big, Growing Business
- Big Data and Analytics
- Global Connections With a Focus On India

Proposed Girl Geek Dinner Speaker Panel Events:

- Thinking Big, Requires a Change of Mind
- International and Technology Startup Cultures
- The Global Supply Chain

As part of the Gender agenda Edinburgh Napier University with BRT, are also working with Investing Women to facilitate their nationwide pitching competition AccelerateHER; a competition for female-led businesses; closing date 31 January 2016: www.investingwomen.co.uk/accelerateher-pitch-competition/

This links into the Investing Women Conference being held 7-8 March 2016, Dynamic Earth, Edinburgh: www.investingwomen.co.uk/ambition-growth-conference16/

For more information, please contact Jane Grant, Bright Red Triangle, Edinburgh Napier University: j.grant@napier.ac.uk
Skills rather than technology

The threat landscape is complex and dynamic. Without a doubt we can expect more stolen customer information, so there still needs to be an ongoing education and awareness around security configurations, passwords and access policy. The BYOD (Bring Your Own Device) trend is showing no signs of slowing and continues to challenge security managers with both the active management of policies and training of staff and suppliers. Throw into this mix the increasing sophistication of hackers and the broad adoption of cloud-based storage and security. Organisations of all sizes are faced with a complex and evolving challenge to maintain business continuity and protect their data, employees, customers and business partners.

Forward looking business leaders are beginning to realise that cyber-crime in all its guises is no longer the sole responsibility of the IT department, particularly where supply chains are interdependent. The lessons learned from some of the most publicised events from 2015 such as Talk Talk and Ashley Madison must be to adopt a ‘not if but when philosophy’ and consider how your organisation will react to a high profile security incident. Cyber resilience is not a line that is crossed but an ongoing program which starts with education and training and must permeate through an entire organisation.

Last year’s cyber breaches and their victim’s lethargic reactions to the fallout from high-profile hacks reveal how unprepared most organisations are for coping with the immediate aftermath.

Education and Training – Cyber Essentials in 2016?

In the last few weeks there have been a plethora of surveys of UK business leaders, assessing their capability to respond to a data breach, hack or other security incident. The common theme to the response is one of being poorly prepared, poorly trained with a recognised experience and knowledge gap and distinct lack of competence to deal with some of the likely challenges in 2016.

Whilst we can definitely expect more coordinated and organised ‘hacking attacks’ and ‘data leakage’ through social networks and social engineering some of the basics need to be addressed including data encryption and employee training and enforcement of security policies. Education of employees to reduce human error through deliberate or accidental negligence must be a key focus.

All companies should be focused on reaching a minimum standard such as Cyber Essentials, a UK Government initiative, complemented by Cyber Essentials+. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Forward thinking organisations of all sizes and in every sector are upskilling staff to address this gap. Whilst the IT department may be at the forefront of these initiatives, we might increasingly expect the HR and Executive teams to be taking on some of the burden.

The Cyber Essentials program aims to help organisations implement basic levels of protection against cyber attack, demonstrating to their customers that they take cyber security seriously. Whilst there are numerous standards associated with the management of cyber security, experience has taught us many common cyber-attacks were successful due to simple technical controls not being managed.

The UK government is keen that all companies, including those who already have accreditations such as ISO27001, gain certification to the Cyber Essentials program, and indeed for certain areas such as the MOD and Critical National Infrastructure this is becoming mandated.

It all starts with getting the basics right, recognising the immediate and emerging risks and becoming more cyber aware, in most instances it’s definitely not just a question of buying in expensive cyber security software or professional advice, around 80% of cyber-crime can be prevented by simply getting the basics right through an ongoing program of education and training.
GLA continues fight to protect vulnerable workers

More than a decade has passed since the world was rocked by reports that 23 Chinese workers had drowned collecting cockles on the treacherous sands of Morecambe Bay. In the wake of that tragedy, new legislation was introduced – along with the Gangmasters Licensing Authority (GLA) to enforce it.

The aim then, and now, is to work with other organisations to protect vulnerable and exploited workers – like those who perished on the sands in Morecambe. The GLA regulates the supply of labour into agriculture, horticulture, shellfish gathering and all associated processing and packaging. Any company providing workers for these areas is classed as a ‘gangmaster’ and must hold a valid GLA licence. Operating without one is a criminal offence and carries a sentence of up to 10 years in prison. Entering into an agreement with someone who has no licence is also an offence for which a sentence up to six months can be imposed.

So what forms does the exploitation take and how does the GLA set about tackling it?

Increasingly, the authority uncovers instances of ‘forced labour’. Criminals are aware that within the GLA-regulated sector are large numbers of workers, mostly migrants with little or no English, who represent easy pickings for the unscrupulous. Consequently, just as the licensed companies with multi-million pound turnovers are well-run and sophisticated outfits, so are the criminals.

Their victims come to the UK lured by the prospect of decent wages, accepting the work may be hard and monotonous. Controlling such vulnerable individuals, their bank accounts and wages, while at the same time exerting fear and control is the trafficker’s standard tactic. It may begin with one individual who has learnt the system and spots an opportunity to cash in – but it can quickly escalate into a complex criminal network handling scores of workers a year.

The GLA encounters potential trafficking victims on a regular basis. It knows how to spot victims and - as an official ‘first responder’ - how to deal with them. The Authority has produced a booklet called Spotting the Signs, (available online), which highlights common trafficking indicators. GLA officers are often requested to act as ‘tactical advisors’ to the police in trafficking cases and also assist with interviews and gathering evidence.

The GLA is able to help potential victims if they contact the GLA. It can also assist with victim or witness interviews and evidence gathering. The GLA works closely with the UK Human Trafficking Centre, the Salvation Army and Migrant Help and advises on forced labour issues to labour providers, labour users, retailers, the police and other partners. The GLA will work alongside businesses to raise awareness of the risk of worker exploitation and modern slavery and tackle any exploitative practice identified.

Anyone who suspects they may have discovered an exploited worker, unlicensed activity or a victim of forced labour should call the GLA on 0345 602 5020 and select ‘option 2’ for the intelligence team. Alternatively, there is a Freephone number – 0800 432 0804.

For more information on the GLA visit www.gla.gov.uk
The Summit this year will highlight the successful and ongoing work of Operation Scandium and start to look at the upcoming changes to the legislation and how this will impact on the organisations and authorities of Scotland. It will also continue to discuss the way forward in the fight against metal theft.

Inputs on the day include Chief Superintendent John McBride who will provide an overview on Operation Scandium and its successes. Guy Jefferson, Director of SP Energy Networks will highlight the current threat businesses face from metal theft. Robin Edwards from Onis Consulting limited will also be at the Summit discussing the pros and cons of the recent legislation change in England.

If you would like more information or would like to book a place please email claire.melville@sbrcentre.co.uk

The start of the new year sees the SBRC continuing its campaign against metal theft.

In the last 3 months there has been a reduction of around 32% in the amount of metal related incidents. This is predominantly down to the pro-active work of British Transport Police and Police Scotland in conjunction with other partners including the SBRC that have been participating in OP Scandium. We may also be seeing a reduction in some areas due to the drop in the price of scrap metal.

The Metal Theft Scotland Sub Group had their quarterly meeting in December of last year. This group is chaired by Chief Superintendent John McBride from BTP. The group includes representatives from Police Scotland, Scottish Business Resilience Centre and a large number of partner agencies affected by metal theft throughout Scotland. The aims of the group are to implement a strategy for tackling metal theft, as well as producing an action log designed to assist law enforcement and partner agencies in tackling this issue. One of the main issue’s on the agenda was the implementation of the Scrap Metal Dealers legislation, which now looks likely to go live in the middle of 2016. On the 23rd of February 2016 the SBRC is hosting Scotland’s 2016 Metal Theft Summit. The summit will look to draw on a number of industry experts and enforcement agencies to raise awareness of the metal theft issue in Scotland, how it can affect everyone and how partnership working can make a real impact in assisting Scotland’s economic recovery and in creating a hostile environment for metal thieves.

The summit hopes to attract delegates across a wide range of sectors from those affected by metal theft to those who work to prevent it i.e. Police Scotland and Scottish Fire and Rescue Service, security companies, licensing authorities, local authorities, the insurance industry, SEPA and any business that is a victim of metal theft.

Further details of this event can be found below, on the SBRC web site and also the Metal Theft Scotland site. You can also contact Jim Scott, SBRC Metal Theft Lead on: James.scott@sbrcentre.co.uk

METAL THEFT SUMMIT 2016

THE SCOTTISH BUSINESS RESILIENCE CENTRE IS HOSTING OUR ANNUAL METAL THEFT SUMMIT ON TUESDAY 23RD FEBRUARY 2016 AND WE ARE DELIGHTED TO ANNOUNCE THAT THE EVENT IS BEING SUPPORTED BY OUR CLOSE PARTNERS SP ENERGY NETWORKS AND TRANSPORT SCOTLAND.

The Summit this year will highlight the successful and ongoing work of Operation Scandium and start to look at the upcoming changes to the legislation and how this will impact on the organisations and authorities of Scotland. It will also continue to discuss the way forward in the fight against metal theft.

Inputs on the day include Chief Superintendent John McBride who will provide an overview on Operation Scandium and its successes. Guy Jefferson, Director of SP Energy Networks will highlight the current threat businesses face from metal theft. Robin Edwards from Onis Consulting Limited will also be at the Summit discussing the pros and cons of the recent legislation change in England.

TICKET PRICES: SBRC MEMBERS £25+VAT, NON-MEMBERS £30+VAT. EXHIBITOR OPPORTUNITIES: £250+VAT.
But now a new firm has been launched that aims to change this. From their base in Dumfries, Harper Stairmand is making waves and winning business.

Founding Directors Graeme Harper and Kevin Stairmand have plenty of experience of how the industry works, having learned their trade in both independent and international brokers over the past 20 years.

What makes Harper Stairmand different?

“Our clients are really important to us”, says Graeme Harper. “It’s very much a personal service that we deliver. We go the extra mile for clients and wherever possible we do things face to face. We’ve found that our clients really appreciate this”.

Many of those clients have stayed with Graeme & Kevin as their careers have developed, and joined them on the journey from independent brokers, to the national firms, and then finally on to their own business.

“We’ve taken the best bits from both the independent and national brokers, and blended them together to create a unique proposition. Our business is designed to be client centric, everyone within the team is committed to understanding our clients needs and then delivering solutions that meet those needs”, says Kevin Stairmand.

“It means that our clients get the best of both worlds, but without any of the bureaucracy that comes from dealing with the big firms. Our clients trust us to manage the insurances on their behalf, as we say in our logo, We Get The Small Print.”

Specialists in General Broking

“People often ask what we specialise in, and our answer is usually Everything!”, says Harper. As a firm, Harper Stairmand provides insurance cover to clients in a wide range of industries, across the whole of the UK.

As a result of their reputations and strong relationships within the UK insurance market, this isn’t as scattergun as it sounds. The firm has a depth of knowledge of most industries, and particular expertise in property, liability, transport, farming, licensed trade, construction, manufacturing, professional indemnity, and retail. But as Harper says, they’re happy to talk to anyone about their insurance needs.

When things go bad

Given the winter we’ve had, Harper Stairmand have been helping clients with flood claims. They are experts in the Government’s new Flood Re scheme, the not for profit flood reinsurance fund, and would be happy to meet with anyone who'd like to find out more about this.

For those who have suffered flood damage, they would also be happy to provide free support and advice on how best to manage their claim, in addition to offering a free risk survey of the business.

A change from the norm

It’s refreshing to hear about such a forward-thinking approach from a broker. Stairmand summarises it well, “With everything we do, we try to see it from the client’s perspective. The world of insurance can be confusing, and the majority of brokers don’t make it easy for their clients to understand. By standing in the shoes of our clients, it helps us to understand insurance as they see it. We keep things simple and deliver our service in a way that our clients tell us they want.”

It seems that listening to clients, and seeing things as they do, is working well for Harper Stairmand. Maybe it’s time that you put your own broker to the test?

Please feel free to contact Graeme on 07889 499312 or graeme@harperstairmand.com
CAP has a unique approach to tackling underage drinking and has been very successful in reducing harm in over 90 local communities across the UK using a combination of enforcement, education, business engagement and provision of appropriate diversionary activity for young people.

Tommy Sheppard, MP for Edinburgh East, recently visited his local CAP to see the great work CAP partners are doing to reduce opportunities for young people to purchase alcohol in the area as well as learning about some of the innovative ways the CAP is educating young people about alcohol misuse.

He learned that since the CAP was set up in East Edinburgh in 2013, there has been an 18% reduction in alcohol related crime, a significant drop in calls to police to report alcohol-related anti-social behaviour and a 25% reduction in confiscations of alcohol from young people. Surveys of local residents show that they feel safer since the CAP was set up and retailers report that they feel more confident in dealing with attempted underage and proxy purchase.

A particularly innovative feature of the Edinburgh CAP is an alcohol peer mentoring project called “AlcoLOLs” which is being offered to local high schools in the area. Tommy got a chance to speak to Professor Emma Wood from Queen Margaret University, who developed the project, as well as some of the teenage volunteers or “AlcoLOLs” who have been specially trained to lead structured dialogue sessions with younger people on the topic of drinking and drunkenness. A total of 2,000 young people have been involved in these ‘no adults allowed’ conversations. So far, it would appear that youngsters who have been involved in the project are starting to question the need to drink or get drunk to gain peer group acceptance.

The CAP has also worked closely with the Piershill Project, the City of Edinburgh Council and other local youth services to ensure the community – and youngsters in particular - are aware of diversionary activities in the area. Young people are encouraged to use sports facilities, youth cafés, youth clubs, drop-in centres and the ‘Buz Bus’ (North Edinburgh Mobile Youth Project) as places for young people to meet in a supervised, safe environment.

Tommy Sheppard and partners went on a joint patrol starting at Portobello Police Station and stopping off at a number of local retailers. The patrols are a regular CAP feature and provide an opportunity for police to check display of Challenge 25 signage and refusal registers and for retailers to talk to partners about any recent issues relating to attempted underage purchase or proxy purchase. Extended joint patrols also take on selected Friday evenings throughout the year (e.g. beginning of school holidays) to known anti-social behaviour “hot spots” where youngsters are known to congregate. Any alcohol found in possession of Under 18s is confiscated and supportive follow up interventions are put in place involving the appropriate CAP partners.

Speaking of his visit, Tommy Sheppard said: “The CAP in Edinburgh is clearly making a big impact in Portobello and Piershill. It’s fantastic to see such a wide range of services working together and sharing their expertise and ideas to tackle alcohol abuse and anti-social behaviour in the local area. Hearing from young people themselves who are involved in changing the dialogue around alcohol is inspiring. I hope this type of model can be extended to other areas of the city and beyond.”

Pictured above, from left to right are Tommy Sheppard MP, Ian MacKenzie, Sales Assistant; Ian Lovie, ScotMid Licensing and Compliance Manager; and Derek Lewis, Chairman of CAP.
This event is one not to be missed and is guaranteed to be a high impact event. The conference will provide access to some of the newest state of the art developments and technical innovation. We are excited to announce our support for this event comes from the NCC Group who are a global information assurance specialist firm. The NCC Group are one of the many stakeholders involved in helping Scotland become more cyber resilient.

Speakers for the event include world renowned James Lyne from Sophos who will be delivering our keynote address, Glenn Wilkinson from Sensepost who will be bringing his drone “Snoopy” to show how our mobile devices are betraying us. Also confirmed to speak is Richard Hollis from Risk Factory who will be showing businesses how to protect themselves and their data.

Ticket Prices: Non-members: £60 + VAT, members £40+VAT. Exhibitor opportunities are also available and are competitively priced at non-members £500+VAT and members £400+VAT. For more information and to book please contact Claire Melville, Events Manager on claire.melville@sbrcentre.co.uk
SSAIB, the UK and Ireland’s leading security, fire and telecare certification body, recently completed an audit of Community Safety Glasgow’s Public Space CCTV (PSCCTV) activities, located within the new multi-functional Glasgow Operations Centre (GOC), and judged them to be compliant with the 12 guiding principles of the Surveillance Camera Code of Practice (in accordance with the Protection of Freedoms Act 2012). This is notable, since the Surveillance Camera Commissioner’s remit covers England and Wales and does not officially include Scotland.

The pioneering GOC brings together Glasgow’s urban traffic management services (Land & Environmental Services Traffcom) and Community Safety Glasgow’s Public Safety & Security services all under one roof. The co-located services also include CSG Security Services (security for the city council’s museums and art galleries), CSG Enforcement Services, Urban Traffic Management and a Police Scotland CCTV Liaison unit.

This combined operation now gives Glasgow one of the most modern and advanced CCTV and traffic management control rooms in Europe. One of the key benefits of bringing together these key services in one location is the delivery of a more joined up approach for service delivery and the sharing of information and intelligence. CSG believes that a more coordinated approach will help it to identify, prevent and tackle crime and antisocial behaviour more effectively. This approach will, in turn, make the communities safer, stronger and help to reduce the fear of crime, CSG adds.

Importantly, the PSCCTV network for Glasgow is the first operation in Scotland to comply with the Surveillance Camera Code of Practice and to mark the occasion Tony Porter, the Surveillance Camera Commissioner, was recently on hand to officially present the certificate to Johann Watson, Head of Security and Business Development at Community Safety Glasgow, and GOC Operations Manager Kalim Uddin. They were joined by Regional Auditor Richard Deacon, representing SSAIB.

Officially opened in February 2014, ahead of the Commonwealth Games held in the city that year, the GOC is managed by CSG on behalf of Glasgow City Council. Community Safety Glasgow is a limited company with charitable status and was established by Glasgow City Council and the Joint Police Authority for Scotland. Investment in the Operations Centre was funded by a mix of The Technology Strategy Board now called Innovate UK (part of the Department for Business, Innovation & Skills) and Glasgow City Council. The Council won a £24 million TSB Future Cities grant in 2013, beating 29 other metropolitan contestants, and aims to become one of the first ‘smart’ cities in the world. The Council demonstrated its ability to integrate transport, communications and other infrastructure to improve the city’s economy, quality of life and reduce environmental impact better than anywhere else in Britain. The GOC is one of the first fruits of that programme, with a number of other Future Cities Projects in development.

Glasgow Operations Centre’s success in gaining full certification with the Surveillance Camera Code of Practice shows a strong commitment to best practice as the Surveillance Camera Commissioner’s remit does not officially include Scotland. Community Safety Glasgow believes, nevertheless, that the Code of Practice’s value meant that voluntary assessment against it should be sought. “We are delighted to have attained this third party certification through SSAIB, which enables us to clearly demonstrate that we comply with the Code and follow best practice,” says Johann Watson. “We’re also very happy to be aligned with the Surveillance Camera Commissioner’s drive to raise standards across the industry through the recently launched third-party certification scheme.”

SSAIB Chief Executive Alex Carmichael describes the multi-functional Glasgow Operations Centre’s pioneering thinking and its role in helping Glasgow become one of the world’s first ‘smart’ cities.

SSAIB helps Glasgow Operations Centre achieve audit ‘first’ for Scotland

Have you got something you would like us all to read about? Here at SBRC we are always on the look out for articles which will be of interest to the Scottish business community. If you would like to submit an article to the SBRC newsletter then please contact Breige McBride on 01786 447 441 or at breige.mcbride@sbrcentre.co.uk

The submission deadline for our next issue is 5pm on Wednesday the 30th of March.
Protecting your business

December saw a prolonged period of extreme weather, resulting in many businesses across Scotland being affected through road closures and buildings flooding, leading to damaged stock and evacuation of premises.

SEPA issued 271 Flood Warnings and 4 Severe Flood Warnings during the same period, giving people time to get prepared for potential flooding.

You too can check the current situation 24/7 by visiting our website or by calling Floodline on 0345 988 1188 to get access to live flooding information and advice on how to prepare and cope with the impacts of flooding.

In December registrations to receive free direct warnings from SEPA’s Floodline service increased by over 1900, and our website received over 250,000 unique visits to our live flood update page.

As a business owner you may be responsible for staff, multiple properties, storage facilities and distribution networks, so receiving free advanced warning of potential flooding from Floodline could give you and your business valuable time to:

- consider and communicate potential weather impacts with your staff;
- put your flood plan into action;
- access your flood kit;
- protect your stock;
- contact suppliers and customers to inform them of possible delays;
- minimise disruption by altering distribution routes to avoid affected areas;
- put in place any flood protection products;
- check your insurance policy, do you have the correct level of cover?;
- save your hard earned money, flood damage can be costly!

It is estimated that approximately 29,000 non-residential properties are at risk of flooding in Scotland, this includes outbuildings and garages. To find out if your business or access routes are at risk you can view our flood maps at http://map.sepa.org.uk/floodmap/map.htm

---

Be Wise

How many people/areas across your business work to ensure resilience throughout your business?

Board / Crisis Management team
Risk and audit committee
Health and safety committee
Security management team
Estates/ and Facilities Management team
IT Incident and escalation management team / project teams
Business Continuity team
Project management teams
Do these independent areas proactively talk to one another / recognise the dependencies upon each other?
Do the right people get the right information at the right time to make informed decisions?
Do the work streams in each area complement each other? / involve each other in decision making?

Businesses across Scotland are utilising the fundamental principles of Enterprise Risk Management (ERM) to ensure:

- risk and opportunities are effectively managed
- risk information is shared
- resilience is strengthened

The ERM framework adopted by businesses, while based on the same principles, will be unique to that organisation’s culture, processes, skills, systems, etc.

Ask is risk always bad? NO!

What happens to an organisation that takes no risk?

Unfortunately, many organisations approach ‘integrating’ and ‘embedding’ risk management by imposing generic risk management tools and processes (like the ubiquitous matrix). True integration required the adaption of the tools to suit the needs of the organisation, the people using it and the decision makers.

Effective risk management fuses with internal controls so organisations are better placed to deal with anything impacting on objectives and strategies. Establishing the context is essential to ensure that appropriate risk assessment is conducted to the benefit of the organisation.

The risk management process should provide a systematic, effective and efficient way by which risks can be managed at different levels throughout the organisation. It should be a continuous undertaking by the organization and its units as an integral part of their decision making, and be operated in accordance with the parameters that are set out by the risk management framework.

Risk identification
What might happen (the event)?
Risk analysis
How likely is it to happen?
If it does what might the impact be?
Risk evaluation
So what?
Is it within our risk appetite and tolerance?

KRisk’s team of risk and communications professionals work with organisations across Scotland to evaluate their current approach to risk and resilience, identifying opportunities to implement those elements required to add value and meet the organisations objectives.

by Grant Kennedy & Nicola Brannan
KRisk Directors.