



# Global threats to the insurance industry

**Branko Bjelobaba FCII**  
Regulation & Compliance Consultant



## Branko Ltd


### FCA compliance consultants


- \* BIBA Compliance Manual
- \* Engaging Events
- \* Tailored Solutions



## Today's event

- Thank you to your LI for hosting
- Interaction, debate and questions welcome!
- Please complete the feedback survey
- You will get the slides

brankobjelobaba 

brankoinsurance 



## Learning outcomes...

**By the end of this event you will have gained an insight into:**

- The key risks facing UK insurers and brokers;
- What can be done to effectively respond to these risks;
- How can firms manage the regulatory onslaught in particular;
- Artificial intelligence - is this a threat or an opportunity?



**Tell me in chat what you  
consider is the  
biggest challenge?**



# **Insurance Banana Skins 2023**

**The CSFI survey of the  
risks facing insurers**



**The London Institute  
of Banking & Finance**

**CSFI**  
Centre for the Study of  
Financial Innovation

## Introduction

- The Centre for the Study of Financial Innovation
- 9<sup>th</sup> survey of risks facing the global insurance sector
- Last edition was 2021 and then covid was of principle concern
- This time it's war, weather and cost of living
- Survey undertaken May to August 2023 with 589 responses from 39 countries (52% European)



- Top four have not changed:-
  - **Cyber crime**
  - **Regulation**
  - **Climate change**
  - **Technology**
- Optimistic about poor corporate governance and management
- Failing to attract the right human talent but this is a concern across all other sectors



## Composite insurers

1. **Cyber crime**
2. **Climate change**
3. **Regulation**
4. **Technology**
5. **Human talent**
6. Macro-economy
7. **Artificial intelligence**
8. Interest rates
9. Security risk
10. Cost reduction



## Brokers

1. **Regulation**
2. **Human talent**
3. **Cyber crime**
4. **Climate change**
5. **Technology**
6. Quality of management
7. Change management
8. Corporate governance
9. **Artificial intelligence**
10. Cost reduction



## Three things to highlight

1. What's the issue
2. The threat
3. What's to be done

Naturally, with an insurance angle!



BBC For you Home News Sport Weather iPlayer Sounds Bitesize Search BBC

# NEWS


Home | InDepth | Israel-Gaza war | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politics More

England | N. Ireland | Scotland | Alba | Wales | Cymru | Local News

**LIVE**

## Planes grounded as mass worldwide IT outage hits airlines, media and banks

The cause of the outage is unclear - but Microsoft says it's taking "mitigation actions".




BBC For you Home News Sport Weather iPlayer Sounds Bitesize Search BBC

# NEWS

Home | Election 2024 | InDepth | Israel-Gaza war | Cost of Living | War in Ukraine | Climate | UK | World | Business More

England | Local News | London

## Fix NHS gaps or face more attacks - ex cyber chief



BLAVATNIK SCHOOL OF GOVERNMENT


Claran Martin, former head of the National Cyber Security Centre said hack was "one of the most serious cyber incidents in British history"


### Top Stories


- LIVE** Starmer says defence spending pledge 'cast iron' as he arrives at his first Nato summit
- Biden pledges air defences for Ukraine as Nato summit begins  
1 hour ago
- Israeli air strike kills 29 people at Gaza camp for displaced  
8 hours ago

### Features

**INDEPTH**



 National Cyber Security Centre


ABOUT NCSC CISP REPORT AN INCIDENT CONTACT US 

Home Information for... Advice & guidance Education & skills Products & services News, blogs, events...

**NEWS**


# The NCSC and partners issue alert about evolving techniques used by China state-sponsored cyber attackers

APT40 is one of the cyber actors that has embraced the trend of using SoHo devices to launch attacks

 Branko

Home News Sport Weather iPlayer Sounds Bitesize Search BBC


**NEWS**

Home | Israel-Gaza war | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politics | Culture 

Technology

## AI could worsen cyber-threats, report warns

8 hours ago





GETTY IMAGES

**By Chris Vallance**  
Technology reporter



Artificial intelligence could increase the risk of cyber-attacks and erode trust in online content by 2025, a UK government report warns.

The tech could even help plan biological or chemical attacks by terrorists, it says.

**Top Stories**

-  **LIVE** Hundreds of police search for Maine gunman as 16 feared dead
-  **LIVE** Israeli army conducts 'targeted raid' inside Gaza with tanks
- Humanity blasted and broken: Gaza through a medic's eyes  
9 hours ago

**Features**

-   
How two 4-year-olds were killed and social media dented it
-   
Humanity blasted and broken



Insurance **POST** My account

Post Learning Commercial Personal Claims Insurtech Risk Management Regulation Broker Insurance Matrix Market Access Events


Highlights | Top 100 UK Insurers 2023 | Top 75 MGAs 2023 | Top 30 European Insurers 2023 | Best Insurance Employers 2023 | Power List 2023 | Interview: Ombudsman's Rachel Lam | More

NEWS

# Insurers must bridge the knowledge gap of 'especially dangerous' malware

The implications of these breaches are far-reaching. They're not just about data theft; they could lead to **extensive operational disruptions, significant data breaches, and a multitude of lawsuits and legal challenges.**


By Scott McGee  
@SKPMcGee  
15 Mar 2024  
Indicative reading time: 3 minutes



POPULAR NOW

- Axa's schemes directory;
- McLarens' UK entertainment team;
- Markerstudy rebrands broker platform

# Aviva: SMEs 'woefully underserved' for cyber cover



Cover against damage from cyber attacks against SMEs has been branded as "woefully underserved" at an Aviva event.

Government data shows that just 37% of businesses report being insured against cyber security risks in some way.

POPULAR NOW

- View from the top: Aviva's Jason Storah on flood-proofing the UK
- Diary of an Insurer: Zurich's Amy Brettell
- Q&A: Martin Langhorst, Davies

## Cowbell research...

- 81% did not have a cyber incident response plan
- 77% did not maintain any in-house security
- 32% said that they were confident a cyber attack would not impact their ability to do business
- But only 10% said they did not need to improve their position regarding cyber risk
- 87% did not consider reputational damage as a significant risk to business
- Only 23% considered cyber as their biggest risk
- 500 UK SMEs spoken to September 2023



## What are the 10 most common types of cyber attacks?

Malware  
Denial-of-service  
Phishing  
Spoofing  
Identity-based  
Code injection  
Supply chain  
Insider threats



## What's the issue?

- The risk posed by cyber crime is the greatest threat facing the global insurance industry over the next 2-3 years as per the report
- Respondents worried most of all that a successful cyber attack could jeopardise **business continuity**, and that the theft of sensitive data (particularly health) could have **disastrous reputational consequences** for individual firms and the entire industry
- Criminals finding it easier to **monetise** stolen data



## The threat

- A major theme this year was about the growing sophistication of cyber attacks, as hackers and other criminals use a **wide variety** of methods for attackers to break into IT systems to exploit vulnerabilities in defences
- Risk is only going to increase as use of AI increases and can be used to mimic real people
- Cybersecurity in a world of geopolitical upheaval where professional hackers move in a shadowy world (and denied by Russia, Iran, etc)
- Assigning clear blame becomes difficult



## What's to be done?

- Cyber criminals seem to always be one step ahead - the need to invest in cyber security continues to increase
- Investing in defences is seen as more difficult – and expensive (and will it work?)
- Leakage of cyber-risk information from business partners in addition
- What actions have you taken and advised your clients to take and how can **insurance** respond?
- What's a better attack - banks or this sector?



### Cyber and data insurance

Policy summary

Policy wording ref: 19029 WD-PIP-UK-CCLEAR(5)

#### Key benefits: what risks are you protected against?

Hiscox CyberClear cyber and data insurance is designed to support and protect you from evolving cyber threats and risks associated with data, whether electronic or non-electronic. We will pay for claims and investigations made against you during the period of insurance arising from your cyber or data liability, up to the limit of indemnity in the schedule, and including your legal defence costs for covered claims and investigations. We also pay for your own losses arising from cyber or data incidents discovered during the period of insurance, up to the limit of indemnity shown in the schedule. The policy may also be subject to further limits for certain items, details of which are stated in the schedule.

**Please check your policy schedule to see which of the following sections you benefit from.**

#### 1. Your own losses

We will pay for losses incurred by you if you suffer:

- the unauthorised acquisition, access, use or disclosure of personal data or confidential corporate information;
- a failure by you, or others on your behalf, to secure your computer system against unauthorised access or use;
- a threat to damage your systems or disseminate sensitive information, following unauthorised access to your systems;
- a digital attack designed to disrupt access to or the operation of your computer system.

If you suffer any of the above, we will pay:

- the costs of computer forensic analysis to confirm a data breach;

### Significant or unusual exclusions and limitations

We do not pay for any claims, losses, breaches, privacy investigations or threats due to:

- your breach of duty in the provision of products or services to your client, other than claims made directly against you by data subjects in respect of their own personal data;
- the failure of service provided by an internet service, telecommunications or utilities supplier, or any other infrastructure provider;
- breach of intellectual property rights, other than where arising due to a any claim under the Online liability section;
- personal injury or damage to tangible property, other than where covered under Online liability, Your losses from crime or Cyber property damage;
- war or due to cyber operations carried out by, at the direction or under the control of a state; ★
- degradation or deterioration of your computer system, other than due to operational error;
- the use of any outdated or unsupported software or systems; ★
- anything you knew or ought reasonably to have known about before the policy started;
- any acts or omissions you deliberately or recklessly commit, condone or ignore;
- any post from a social media account that does not belong to your business; ★
- online liability claims brought by your current or former employees;
- the use of any credit, debit, access, convenience, smart, identification or other card, other than losses caused by the dishonesty of an employee who uses a card that you have issued to them for the payment of valid business expenses incurred for or on behalf of you;
- any purchase, use or development of blockchain or any other distributed ledger technology, however this does not apply to covered cyber ransom losses;
- any pollution;
- any criminal, civil or regulatory fines, other than PCI charges and regulatory awards where legally insurable; or
- any actual or alleged monitoring, tracking or profiling of an individual without their authorisation, including, but not limited to, web-tracking, session recording, digital fingerprinting, behavioural monitoring, eavesdropping, wiretapping or audio or video recording by you or by a third party.

Additionally, we do not pay your losses from crime due to:

- any act, breach or omission committed by any employee after you first discovered any crime being committed by or in collusion with that employee;
- any act, incident or event occurring, or any loss suffered before the crime retroactive date;



## Is your business protected against cyber crime?

Use our cyber safety tool to get a free tailored action plan.

[Start now](#)



## Cyber insurance

- 59% of SMEs have had an incident in the last 12 months + typical loss £15,300
- 80% could be prevented with good hygiene
- What's covered/not covered?
- Benchmarking/consistency/clarity
- How does cover evolve/adapt as there are constant new threats?
- How are premiums calculated?
- How will claims be handled?
- Sharing of good practice?



## Cyber insurance

- Big market - \$16.7bn in global written premiums in 2022 to an estimated \$33.4bn in 2027
- Critical risk management and crisis recovery tool for many businesses, big and small
- FCA are concerned that uncertain cyber policy wordings may result in firms not meeting their customers' needs and policies should meet those needs and provide value
- **What are you exactly covered for and have any claims ever been met?**



- Firms offering cyber insurance must make sure their policy wordings are clear and that customers **understand** the coverage they are buying
- Firms to manage cyber claims handling in a fair and timely way
- Market to continue improving their knowledge of cyber so firms will have sufficient expertise to understand the risks involved and ensure appropriate product oversight
- FCA will continue monitoring the cyber insurance market and take action on firms we deem to be outliers



## What's the issue?

- Volume of rules and regulations continues to multiply
- Cost and distraction of compliance
- Stifling impact on product development, innovation and competition
- “Excessive, overlapping and sometimes inappropriate or outdated regulation is not a risk, but a reality that burdens companies’ agility, innovation, efficiency, profitability and moreover often deteriorates the customer experience”.



## The threat

- Growing area of non-financial risk reporting brought on by the environmental, sustainability and governance agenda, which can entail reputation risk
- Inability to attract new talent to the industry is seen as a recent negative outcome of regulatory excess
- Solvency II and UK vs EU
- Commission as a continuing method of remuneration for brokers?





## What's to be done?

- Perceived failure by the government to seize the initiative post-Brexit and tackle the regulatory legacy from the EU
- The continued burden of regulatory scrutiny and a limited appetite to make the UK more competitive against European markets
- 42% of global marine, aviation and energy is placed in London
- Lloyd's £3.9bn profit at half year 2023
- Is the industry doing it's very best?



### Consumer Duty implementation: good practice and areas for improvement

Good and poor practice | Published: 20/02/2024 | Last updated: 22/02/2024

- [1. Next steps](#)
- [2. Culture, governance and monitoring](#)
- [3. Consumers in vulnerable circumstances](#)
- [4. Products and services](#)
- [5. Price and value](#)
- [6. Consumer understanding](#)
- [7. Consumer support](#)

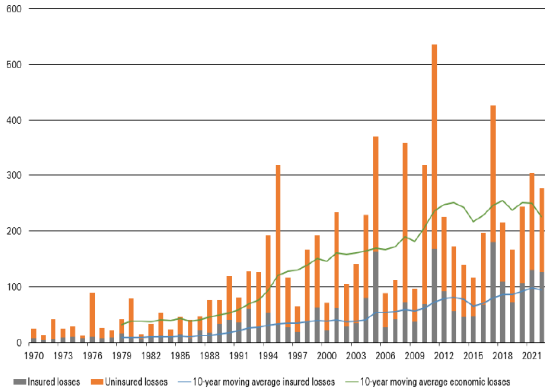
**Copy available – please message me if wanted**



### 3. Climate

### Insured vs. Economic losses

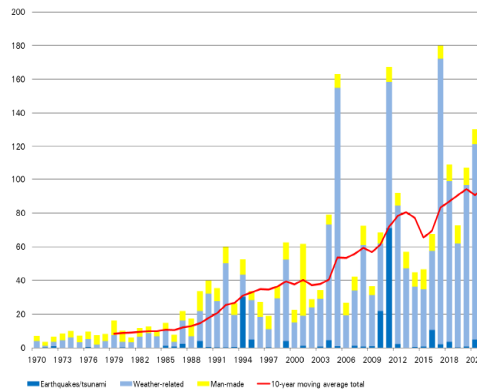
Insured vs uninsured losses, 1970 – 2022, in USD billion at 2022 prices



## Up-trend of nat cat losses reaffirmed in 2022, and set to continue

- USD 132bn: **4th highest ever**
- **Hurricane Ian**, costliest event of the year (USD 50 to 65bn) and **2nd costliest ever**
- Floods in Australia and South Africa, costliest natcat events in the respective countries
- Hailstorm losses in France, the country's costliest ever
- **Growth driven by loss severity** from growing exposures due to economic development, urbanization, often in high-risk areas

Global natural catastrophe insured losses, in USD billion (2022 prices) and number of events



Source: Swiss Re

Standards. Professionalism. Trust.

## What's the issue?

- Insurers face growing claims as natural disasters become more prevalent
- Uncertainties in how to price policies
- Increase underwriting risks
- Epidemics - can insurance even cover them?
- Investments in vulnerable assets face devaluation
- Serious financial, social and regulatory implications for the industry (can it/should it be insured?)



## The threat

- Long-term impacts of climate change is changing the frequency and severity of weather events showing in the increase in wildfires, convective storms, droughts impacting crop yields and flooding of agricultural land
- Impact on claims is becoming more severe and apparent and the industry faces challenges related to assessing risks accurately, pricing policies, and managing claims
- Climate risk is global and rates are hardening and more exclusions are coming in



## What's to be done?

- Insufficient collective action?
- Climate change has impacted the claims experience in an unpredictable way, with the result that catastrophic losses are becoming more prevalent
- Insurers are struggling to price the risk appropriately and reinsurers not as willing as before as they continue to bolster the sector
- Moves to exit higher risk markets will reduce capacity and put more pressure on governments to pay out of taxation domestic losses





### What's the issue?

- The insurance industry is seen by many as being rather behind when it comes to technology when compared, for example, with the banking and investment fund sectors
- The ability to fully address the digital challenge and adjust business models
- Some digital initiatives have been launched but far too slowly compared to what is required to remain relevant in the future
- What does this say to new entrants?



## The threat

- Sector are not able to meet these requirements with their legacy systems (previous mergers)
- One of the main obstacles to tech modernisation is cost, particularly when it isn't clear how long new IT systems will remain relevant
- Technology world is moving very fast and the amount spent to implement chosen technologies may not generate returns on investment, leading to increased cost of operations



## What's to be done?

- Higher costs of doing business than more technologically savvy peers and will some fall behind and not be able to catch up?
- Long implementation times and uncertain outcomes
- Regulatory interventions/reporting and links with cyber, ICO, etc
- Do we just have to bite the bullet?
- Think how far we have come – EDI, quote engines, customer portals, no paper!



# 5. Human Talent



There's a problem with talent...

Competition for talent will remain fierce in the UK despite economic uncertainty



CII survey shows skills shortage in UK general insurance

70% of insurance CEOs see skills shortage as a threat to growth

## The War For Talent In The 'New Normal'

The Great Resignation is spawning a talent war. Who will win it?

A new report argues that firms must change how they view workers to compete in the war for talent.

War for talent will be won with culture over salary, report finds

Experts warn many businesses 'will not make it' if they champion salary over a toxic working environment



**INSURANCE**  
Business publications in the last few years have noted the 'leakage of talent' leaving the insurance sector, with The Bureau of Labour Statistics (BLS) predicting that over the next 10 years, 50% of the current insurance workforce will retire.

Leaving the sector in a talent crisis if we do not act now.

It seems opportunities simply are not meeting the talent needs, according to Accenture (2022) 'Less than 20% of the insurance industry is under 35 years old'. Exposure to the market is low for a lot of young people.

From peer to peer chats it is clear our industry has an external brand perception issue. Simply put young people have a lack of knowledge of what our sector does and are unaware of the diversity of roles and opportunities it holds for degree and non-degree holders through apprenticeships and in industry training through the CII.

This research was conducted to get an updated post-covid world view from those aged 18-28, to identify gaps to work on and to quantify assumptions into facts.



## What's the issue?

- Acute difficulty of finding appropriate talent in technical roles, particularly technology-related
- Low supply and high difficulty in recruiting highly qualified employees in the areas of pricing, advanced and flexible IT systems, advanced analytics and financial expertise
- Is the industry sexy and innovative enough to attract people with these much-needed skills
- In 15 years time half of the current workforce will be retired...



## The threat

- War for talent - defining issue is not just levels of pay but whether the sector can appeal to the broader expectations of younger generations in the workforce, particularly after the normalisation of hybrid work during covid
- Younger generation loyalties are harder to obtain, and what motivates them harder for current leaders to understand
- Impact on developing future leaders as the basis of learning a complex industry has largely been on the job - which is much more complex in the current environment





## What's to be done?

- Losing key people with the right knowledge/skillset is a major risk - how can they be retained?
- Improving work life balance impacts social cohesion at work
- Increase focus more on retraining existing employees
- Are offices a thing of the past and what's the current expectation of employers and employees?





A screenshot of a Hiscox press release page. At the top left is the Hiscox logo. To its right is a navigation menu with links for 'About Hiscox', 'Careers', 'Investors', 'News', and 'Responsibility'. In the top right corner, the share price '1,058.00' is shown with an upward arrow. Below the navigation is a search bar with a magnifying glass icon. The main content area has a breadcrumb trail: 'Hiscox &gt; News &gt; Press releases &gt; Hiscox and Google Cloud Collaborate on AI in lead underwriting for the London Market'. The headline reads 'Hiscox and Google Cloud Collaborate on AI in lead underwriting for the London Market'. Below the headline is the date '12th December 2023'. The sub-headline is 'Augmented underwriting in Hiscox London Market could reduce the time for lead open-market quotes from three days to three minutes'. The main text starts with 'London, UK (12th December, 2023) Hiscox, the specialist global insurer, has collaborated with Google Cloud to create the first AI-enhanced lead underwriting model in the London Market insurance industry.' The final paragraph states: 'The collaboration combines Hiscox London Market's recently built technology platform, Hiscox AI Laboratories (Hailo) with Google Cloud's generative AI technology to automate lead algorithmic underwriting from submission to quote.'

**BBC** Branko LIVE Home News Sport Weather iPlayer

**NEWS**

Home | Israel-Gaza war | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politics | Culture

UK | England | N. Ireland | Scotland | Alba | Wales | Cymru | Isle of Man | Guernsey | Jersey | Local News

## Sadiq Khan says fake AI audio of him nearly led to serious disorder

11 hours ago

Remembrance Day



**By Marianna Spring**  
BBC disinformation and social media correspondent

London Mayor Sadiq Khan says deepfake audio of him supposedly making inflammatory remarks before Armistice Day almost caused "serious disorder".

Mr Khan says the law is not "fit for purpose" in tackling AI fakes, as the audio creator "got away with it".

TECHNOLOGY

## Zurich reveals it has found more than 160 use cases for AI

By Harry Curtis  
18 Mar 2024  
Indicative reading time: 3 minutes



Zurich has deployed more than 160 artificial intelligence-powered solutions across its business around the world, the insurer's group chief information and digital officer Ericson Chan has said.

POPULAR NOW

- Scale of motor insurance quote manipulation laid bare
- Aviva and Howden partner; Ecclesiastical's Cockrem to retire; Eurochange to launch travel insurance
- Aventum founder 'extremely proud' as son impresses on Formula One debut

The Insurance Charities  
for the things you can't insure against


Post Learning Commercial Personal Claims Insurtech Risk Management Regulation Broker Insurance Matrix Market Access Events

Highlights | BIA 2024 shortlist | General Election | Interview: CFC's Louise O'Shea | Power List 2024 | Top 100 UK Insurers 2023 | Top 75 MGAs 2023 | More

NEWS

# Insurance influencer argues AI scares the 'antiquated' industry

By Damisola Sulaiman  
13 May 2024  
Indicative reading time: 4 minutes



POPULAR NOW

What Labour's landslide victory means for insurance

British Insurance Awards 2024

THE GLOBAL CITY LONDON


VISION FOR ECONOMIC GROWTH | SUSTAINABLE FINANCE HUB | THE UK'S OFFER | INNOVATION | INDUSTRIES | INSIGHTS

What is the AI Innovation Challenge?

The AI Innovation Challenge will provide a unique platform for collaboration between financial services (banking, payments, insurance) and technology companies. Participants from tech firms and financial services firms will work together to enhance innovative tech solutions to address a key security priority or "use case" for financial services.

The innovation challenge will:

- Accelerate the development of innovative AI solutions that meet FS and wider industry demand;
- Support cross-sector collaboration and information sharing on an Online fraud; and
- Provide thought leadership on catalysing online fraud innovation in the UK.





## What is AI?

- AI should help humans rather than work against us
- A report by investment bank Goldman Sachs suggested that AI could replace the equivalent of 300 million full-time jobs across the globe
- It concluded many administrative, legal, architecture, and management roles could be affected
- But it also said AI could boost the global economy by 7%
- The tech has already been used to help doctors treat cancers and to develop new antibiotics



## AI could be used to...

- Enhance terrorist capabilities in propaganda, radicalisation, recruitment, funding streams, weapons development and attack planning
- Increase **fraud, impersonation, ransomware, currency theft, data harvesting, voice cloning**
- Increase child sexual abuse images
- Huge amount of **cyberattacks**
- Erode trust in information and use 'deepfakes' to influence societal debate



## What's the issue?

- Introduced to the survey for the first time as AI is attracting a lot of attention
- AI may become a great opportunity, but a lack of regulation and security may become an even greater risk
- The potential for profound and rapid social change combined with a much less agile legal and regulatory environment creates a big potential for risks pools to rapidly emerge or shift where the insurance industry is unknowingly exposed



## The threat

- Using AI for good and controlling the bad is another very high risk. What happens when the underwriting data on which all other decisions are dependent is manipulated?
- Easy infiltration of financial services incl banking and insurance
- The types of risks posed will depend on how insurers choose to deploy this emerging technology
- How can insurance cover respond?



## What's to be done?

- How these models function can only be learned as you try to train them and while the opportunities are promising and exciting, the risks are significant
- Insurers need to have a clear vision of what they intend to achieve with the usage of AI and being driven by buzzwords and fuzzy trends can be noxious
- The conservatism of the insurance industry in adopting new technologies could reduce the threat



## **What have we covered...**

**By the end of this event you will have gained an insight into:**

- The key risks facing UK insurers and brokers;
- What can be done to effectively respond to these risks;
- How can firms manage the regulatory onslaught in particular;
- Artificial intelligence - is this a threat or an opportunity?



**Thank you for listening**

**Questions please**

**[www.branko.org.uk](http://www.branko.org.uk)**

**(0800) 619 6619**

