BRIM
BUSINESS RESILIENCE
INTERNATIONAL MANAGEMENT

The UKs response to cyber risk in SMEs and supply chain

July 2021

Background

In January 2020, the UK Home Office began a transformational UK Cyber Resilience Centre Programme in rapid response to an exponential rise in international cybercrime and risk to UK societal resilience, business trade and supply chain. Now, 15 months into the delivery of that programme, the depth of that engagement has led to sufficient comfort and confidence by UK Government Cyber Security Services (NCSC) for the introduction of a formal Memorandum of Understanding with the Cyber Resilience Centres directly. The programme ensures that the latest threat intelligence and expert cyber knowledge from these national entities is applied at a focus point where vulnerable businesses need it most. The CRC model drives engagement with smaller and/or vulnerable organisations that believe they have no need or are afraid to engage cyber resilience support and supports a nations cyber resilience by positively and effectively impacting supply chain resilience.

The programme is delivered through several Police led, not for profit, regional Cyber Resilience Centres (CRCs) and a national cyber talent pipeline developed in association with leading academic institutions. The cyber talent pipeline takes students from leading universities and augments their development with recognised industry training and qualifications ensuring they are also ready for deployment into Policing, Defence, Critical National Infrastructure (CNI) and the private sector at the end of their academic journeys. This development has been recognised as a critical factor for economic recovery and societal resilience in protecting rapid post pandemic national business growth and in the development of national work-ready cyber capability.

International law enforcement and the World Economic Forum have expressed interest in this transformational UK Cyber Resilience Centre Programme, which, despite the escalation and duress of pandemic and lockdown has been delivered ahead of schedule. The Programme continues to grow in scope as additional UK Government stakeholders seek to bind their own strategic development goals to the programme deliverables. As economic recovery now emerges as a Government critical mission, notable support through this model for the protection and resilience of start-up, spin out and high growth IP and trade secrets is gaining notable attention internationally.

The UK CRC Programme has secured high profile interest for its immediate success and long-term sustainable approach to improved country cyber resilience, supporting economic growth, through implementation of an innovative, entrepreneurial led model. Delivery has been managed efficiently and cost effectively through remote working. Acknowledged by the Home Secretary in her speech to CyberUK Conference 2021, this model has potential to export globally and profile the UK as the leading innovator and global leader in solving the supply chain engagement in cyber resilience challenge swiftly, at a pace akin to the rapidly evolving cyber threat.

The International Threat Landscape

INTERPOL published an initial COVID-19 cyber threat report in April 2020 and launched their Purple Notices strategy to alert countries of high-risk cyber threats, provide technical guidance for victim recovery and survey to understand cyber threat developments. Ongoing collaboration by the INTERPOL Cybercrime Experts Group with international key stakeholders, such as the United States Homeland Security investigations (HIS) joint statement on vaccine related cybercrime in March 2021 has allowed the UK Cyber Resilience Centre Programme to adopt and interpret this latest cyber threat intelligence into cyber resilience services for UK business.

INTERPOL has addressed a strategic two strand approach to countering cyber enabled crime and cybercrime for Small to Medium Size Enterprises (SME) and supply chain, stating that this requires essential collaboration with the private sector. Both law enforcement and private sectors are challenged globally to fulfil demands of cyber skills required. The INTERPOL New Year address (published in Dec 2020) highlighted the profound global disruption to law enforcement that the pandemic has created. With a substantial pre-pandemic cyber skills shortage, the risk remains extremely high, especially where the perception is that cybercrime remains a problem only for larger and international business.

Third sector organisations such as medical charities and international aid foundations require access to affordable cyber resilience services to support their critical supply chain and logistics operations. The CRC programme engages directly with SMEs including self-employed and third sector organisations to support resilience and reduce risk for these organisations that are critical to a nation’s wider economic recovery. The Cyber Resilience Centre Programme has proven to fully support that recovery. The release of HM Government's Integrated Review of Security Defence, Development and Foreign Policy, March 2021, further demonstrates the need and impact of this highly transferrable model in support of international trade and security developments, with particular attention to Indo-Pacific.

The UK’s response and how success has been achieved in the UK

The framework that the UK CRC Programme has used is transformative, yet highly adaptive to ensure it can adopt and implement the national country requirements. The programme governance structure also benefits from engagement and funding from global brands as well as strategic regional organisations. It has proven attractive to highly innovative, entrepreneurial companies and welcomed by global technology companies.

The framework was a development following a 9-year success programme, followed by an initial trial of two Centres in England, (one City and one regional) then rolled into the first full network of regional Centres across England and Wales through extensive European procurement from January 2020. Acclaimed for its success in the Scottish Parliament, the architect of the model has since won a European SC Security award for the success in this field. Comprising of country specific scoping, implementation and support framework, its robust and proven mechanisms embed a sustainable model for improved and responsive cyber resilience in SMEs and supply chain. With a convergence approach, it also has inclusivity, ethics and governance established as key tenets.

The CRC model, designed by Founder of Business Resilience International Management (BRIM) has led an escalated implementation programme in the UK on behalf of the Home Office and National Police Chiefs Council (NPCC). Early reporting within 15 months, saw significant uptake of engagement by SMEs with 65% from micros, a traditionally hard to reach segment of the market.

Strategically informed and tracked engagement enables threat intelligence to drive educational and preventative guidance at speed, improving resilience across the right organisations at the right time. A recent example of this has been in the UK educational sector.

The model has exceptional potential to swiftly support Overseas Territories and Crown Dependencies. It is efficient, smart, agile, and responsive.

The business and security imperatives model adopted

The CRC model addresses business and security imperatives:

- Takes national and international threat intelligence, and interprets and implements these for SMEs, vulnerable organisations and third sector charities through affordable baseline cyber resilience solutions

- Building societal resilience to withstand unexpected cyber threats and risks, including future environmental and global health emergencies.

- Cyber resilience solutions delivered by a nation's own developing cyber and academic resources, using tight and transparent service governance, a controlled and protected central service platform and internationally recognised skills and knowledge.

- Cyber resilience education and protection embedded for start-up, spin out and high growth IP and trade secrets, critical to economic recovery.

- Rapid dissemination of guidance and support to counter emerging national and international cyber threat intelligence and to provide the nation's security services with a live picture of the security and risk stance of SMEs, vulnerable organisations and third sector.

- Focus for implementation of national technical visions and emerging strategies, including affordable technical solutions and technical innovations.

- Development support services for regional, state, and national infrastructure projects.

- Engagement and education for hard-to-reach market segments.

- Support to improve resilience of regional and national law enforcement, CNI and supply chain.

- Workplace ready talent pipeline escalation for law enforcement, CNI and business cyber skills.

- Robust and structured engagement with law enforcement, public and private sectors at strategic level, tailored by region, for reporting of regional cybercrime.

- Trusted route to cyber support and provision in an unregulated market.

- Service delivery platform based on skills and knowledge, secure accredited tooling, and service governance.

IMPACT

How the model impacts cyber resilience and skills development

A Cyber Resilience Centre model provides relevant regional resources and protection for business operations and IP, supply chain and third sector organisations and ultimately all business communities in the digital era. It creates and implements proven solutions using trusted and best information from law enforcement and Government.

There is growing international interest in the success of this model.

"Intelligence sharing between stakeholders is a defining feature of the cyber security community and one of its most important shared challenges."

- World Economic Forum October 2020

Economies and communities rely on resilient commercial and third sector organisations. In a digital era, the combined threat to operations and service delivery from cyber attack, social engineering and digital fraud means that at national and regional level, law enforcement agencies, Government, academia, private and third sectors have had to find new ways of working together. COVID-19 and lockdown impacted cybercrime has escalated this demand.

The priorities of the Cyber Resilience Centre model include reducing risk, building effective cross-sectoral capability, applying new resiliency measures at pace in an affordable way as well as developing a high calibre talent pipeline. The BRIM Cyber Resilience Centre model addresses all these factors.

"Learnings and insights from these case studies will help inform law enforcement and the private sector around the world. We look forward to learning from BRIM's work and the network of Cyber Resilience Centres."

- World Economic Forum October 2020

Indicators of success in the UK 2020-2021

BRIM is one of the fastest growing and most highly respected cyber resilience engagement specialists companies operating from the UK. With a global network across law enforcement, academia, and the private sector, this has resulted in a contract extension and an expansion from UK law enforcement. The expansion and visibility of the contract has drawn requests from law enforcement in the United States, Bermuda, INTERPOL and one of the largest UK business management consultancies.

UK work to date has seen a significant multimillion pound investment by the UK Government. The programme has been delivered ahead of schedule and in an expanded capacity in light of its positive impact evidenced to date throughout COVID-19 and lockdown impacted cybercrime rates. A unique Memorandum of Understanding (MoU) was agreed between NCSC and the client network supported by the data-informed engagement success with hard-to-reach SMEs embedded as part of delivery.

The UK project is now developing plans for Phase 4, Sustainability. This stage is focussed on the creation of a National company which will centralise support for the entire network of Regional Centres and is a significant piece of work in its own right, for the UK.

Stakeholder engagement has been a key tenet in the delivery of the Cyber Resilience Centre programme, including Home Office, NCSC and NPCC. BRIM core consultants have also been asked to support wider stakeholder engagement, through related consultation with the UK Department for Culture, Media and Sport (DCMS) with regard to impact and collaboration across other strategic projects with Home Office and NCSC. This includes developing a national educational and communication framework, and a support service for the national civil aviation industry aligned with the UK Aviation Regulator.

Conclusions

1. Focus on protecting and improving cyber resilience in the entire national supply chain to support post COVID-19 pandemic recovery, societal resilience and support business growth through increased IP and operational protection.

2. Takes national and international threat intelligence, and interprets and implements these for SMEs, vulnerable organisations and third sector charities through affordable baseline cyber resilience solutions.

3. Cyber resilience solutions delivered by a nation's own developing cyber and academic resources, using tight and transparent service governance, a controlled and protected central service platform and internationally recognised skills and knowledge.

4. Rapid dissemination of guidance and support to counter emerging national and international cyber threat intelligence and to provide the nation's security services with a complete and live picture of cybercrime and the security stance of SMEs, vulnerable organisations and third sector.

5. The CRC model solves the engagement challenge of smaller and/or vulnerable organisations that believe they have no need or are afraid to engage cyber resilience support but who need help to manage cyber risk to their own businesses.

6. The CRC model provides effective solutions for SMEs to choose and engage suppliers with knowledge, confidence and trust, solving problems short term and building legacy trust in quality provision by this emerging unregulated sector for the future.

7. The internationally recognised skills and knowledge delivered through the programme ensure a high quality, escalated workplace ready talent pipeline to accelerate talent supply into law enforcement, defence and CNI as well as the private sector.

8. Investment and support from large entrepreneurial and tech focused companies who want to be associated with economic recovery programmes and national academic and talent development.

9. Programme implementation has proven resilient throughout pandemic and can be deployed remotely.

10. This innovative transformational model is adaptive to be designed and implemented to align with in country key stakeholders, threat intelligence imperatives, technology and development strategies and key academic and skills development initiatives.

11. It is tried, tested, and trusted by UK Government. Early-stage progress is being monitored for additional impact specifically with supply chain to CNI.

About the Authors

Joanna Goddard

Partner

Business Resilience International Management

Joanna is an award-winning business consultant, specialising in rapid engagement for hard-to-reach markets. Certified in Business Analytics by Judge Business School, Cambridge University and one of less than forty consultants in the UK trained in ISO20700 by ICMCI, The International Council of Management Consulting Institutes.

Her extensive international commercial network and multi sector experience, enables law enforcement and Government to effectively structure working with and engaging with the business and third sector communities.

Prior to the security industry Joanna successfully founded her own niche business, delivering internationally, recognised as a ‘go to’ expert, advising a Channel 4 TV series from inception for over four years. Additionally, experienced in leading a not for profit (Town Centre Management) and consulting on the introduction from North America of the BID system, a local tax scheme to support troubled town and city centres, and its introduction to the UK. As a former director of a law firm, Joanna also has a good grasp of coordinating governance and legal implications across different jurisdictions with legal advisory teams.

As well as delivering the national programme of Centres for Policing, Joanna is also now working directly with national and international business leaders on the creation of a single National entity which will support the network of Regional Cyber Resilience Centres.

Joanna is passionate about the importance of positive culture and wellbeing within the Cyber community. She is a member of the Advisory Council to the School of Management and guest lecturer at the University of St Andrews; a Fellow of the Chartered Management Institute; Strategic Advisory Board member of Converge, and Chair of Trustees at the ground-breaking Arctic exploration charity, The Polar Academy.

Paul Boam

Partner

Business Resilience International Management

As a former consultant for her Majesty's Government and a highly recognised technical consultant, working for international regulation bodies including the United Kingdom Accreditation Service (UKAS), Paul is an experienced security company director.

A Chartered Engineer and former CLAS consultant and CHECK team member, Paul is a specialist in Information Security Management Systems, Industrial Control Systems, Anti-Bribery, Asset Management, Supply Chain Security, and Business Continuity management systems. Paul is the only person in the UK considered technically competent by UKAS to assess Common Criteria bodies such as NCSC and other security laboratories.

His background as an OSINT and Dark Web trainer brings additional expertise to the talent pipeline that is of exceptional value to National Policing and the role out of the Cyber Resilience Centres.

Paul is passionate about cyber security engineering and the emerging challenges of defending Industrial Control systems. The blended attacks that critical national infrastructure now faces from foreign state actors are commonplace and bringing students the skills and knowledge to face these threats is a key focus for his work at BRIM on the CRC programme.

References

1. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

2. https://www.gov.uk/government/speeches/home-secretary-priti-patel-speech-to-cyberuk-conference

3. https://www.computerweekly.com/blog/When-IT-Meets-Politics/One-size-does-not-fit-all-current-Cyber-Security-Practice-as-revealed-by-DCMS-Breaches-Survey

4. https://policinginsight.com/features/innovation/the-cyber-resilience-network-an-insight-into-an-ambitious-programme-delivery-amidst-lockdown/

5.https://www.brimcentre.com/post/mandy-haeburn-little-wins-at-sc-digital-awards-europe

6.https://atos.net/en/expert/mandy-haeburn-little

7.https://www.cirmagazine.com/cir/2020072702.php?utm_source=jsrecent

8.https://www.csoonline.com/article/3533552/cyber-resilience-centres-a-new-model-for-uk-police-to-fight-cyber-crime.html

9.https://www.devopsonline.co.uk/cyber-resilience-centre-for-wales-to-help-businesses-improve-their-security/

10. https://www.brimcentre.com/post/interview-william-dixon-head-of-future-network-technology-world-economic-forum

11. https://www.brimcentre.com/post/the-list-of-big-brands-supporting-the-boards-of-national-cyber-resilience-centres-2021

12. https://www.brimcentre.com/post/nebrc-appointed-to-deliver-100k-cyber-support-programme-for-leeds-city-region-smes

13. https://www.brimcentre.com/post/mandy-haeburn-little-awarded-commendation-from-npcc

14. https://www.brimcentre.com/post/emcrc-welcomes-200th-core-member

15. https://www.brimcentre.com/post/the-crc-for-greater-manchester-launches-partnership-with-the-greater-manchester-chamber-of-commerce

16. https://www.brimcentre.com/post/nebrc-wins-outstanding-cyber-security-initiative-at-2021-uk-ospas

BRIM – There’s more to us

BRIM works in collaboration with the following agencies and is recognised and supported by UK Law Enforcement at national level:

- UK Government
- Home Office
- NCSC, Part of GCHQ
- NPCC
- Scottish Government
- Police Scotland

We provide you with:

- Best practice organisational models.
- Professional consultancy, highly experienced in the Cyber Resilience Centre model.
- Professional consultancy, highly experienced in the development of Talent Pipeline.
- Technical cyber resilience expertise, boasting former GCHQ and CNI consultants.
- Forensic style data informed engagement analysis.
- Highly skilled commercial leadership development skills.
- A global network of CISO, Law Enforcement, Ministerial, Government and strategic Commercial stakeholders in Cyber Resilience.

www.brimcentre.com

@BRIMCentres

Business Resilience International Management

Join Our Mailing List

BRIM

BUSINESS RESILIENCE INTERNATIONAL MANAGEMENT