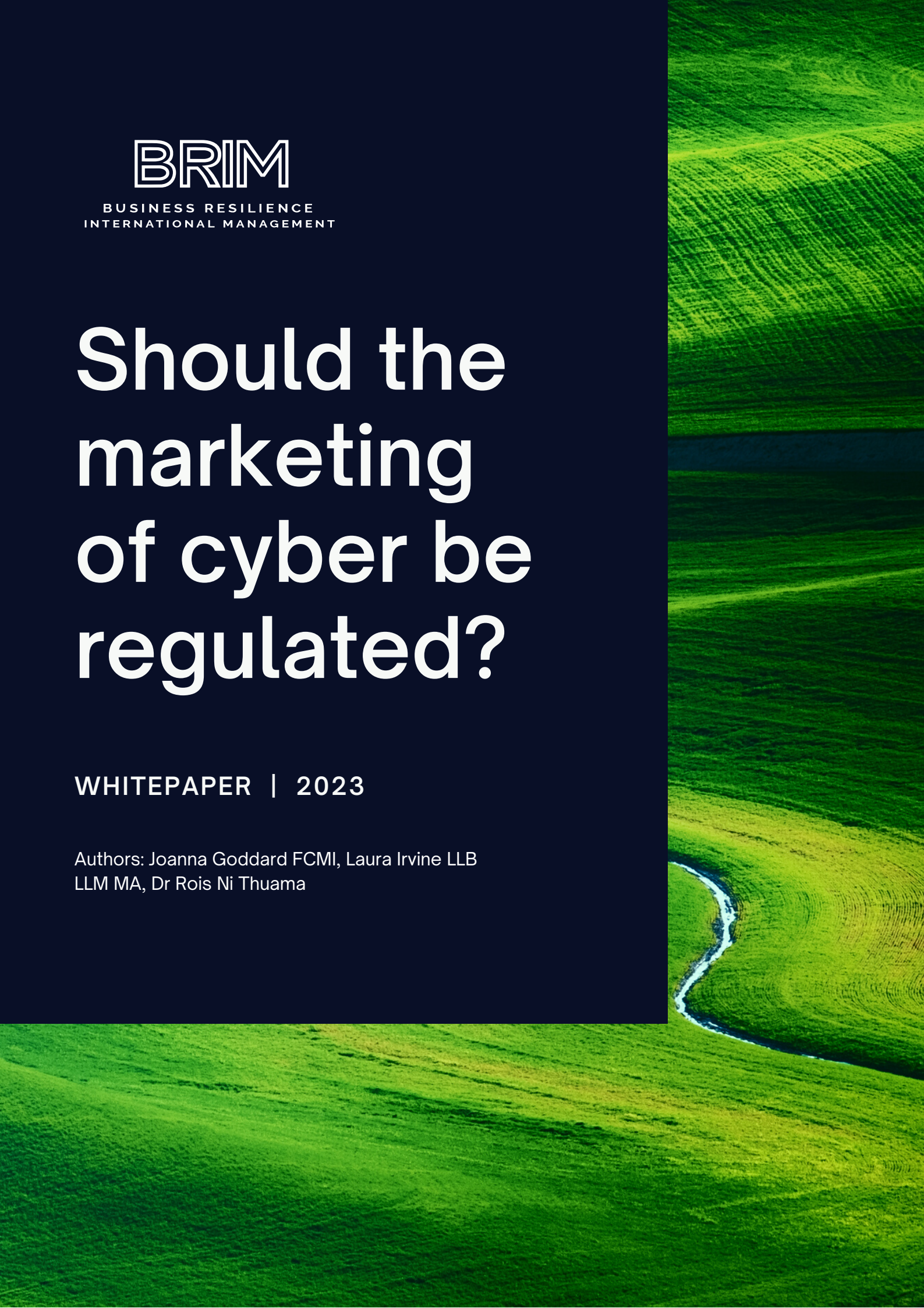
BRIM

BUSINESS RESILIENCE
INTERNATIONAL MANAGEMENT

Should the marketing of cyber be regulated?

WHITEPAPER | 2023

Authors: Joanna Goddard FCMI, Laura Irvine LLB LLM MA, Dr Rois Ni Thuama



Contents

Background

> The vision of the UK's National Cyber Strategy (NCS) 2022 is that the UK will continue to be a leading, responsible, and democratic cyber power, able to protect and promote its interests in and through cyberspace in support of national goals. The NCS 2022 set out how the UK will continue to adapt, innovate, and invest in order to pioneer a cyber future with the whole of the UK."
>
> - NCS 2022

This whitepaper is a response to that vision for leadership, protection, responsibility, and innovation, and it presents a set of pioneering conclusions that extend well beyond the borders of the UK. If the UK embraces these conclusions and our national agencies and forums engage with these recommendations, the UK will lead an innovative and pioneering evolution of regulation in the marketing of the cyber sector.

Marketeers are experienced in navigating regulation. In the UK in May 2018 the introduction of the GDPR strengthened existing PECRs rules and the direct relationship between marketing and legislation. Marketeers operating within heavily regulated industries such as manufacturing, retail, legal and financial sectors, are experienced in navigating communications considerate of legal challenge and interpretation of claims. Tobacco and pharmaceutical companies operate under security and challenge. However, this paper focuses primarily on Professional Services.

We approach this issue within the context of cyber's emergence as the third Board professional adviser, joining legal and financial advisers. It addresses the marketing challenge of unsubstantiated claims from the cyber industry. Identifying this as an obstacle to improving the nation's cyber resilience.

First raised publicly through a CyNam webinar in March 2021, Joanna Goddard a partner of BRIM has continued to raise the profile of the challenge of 'marketing cyber' to an uninformed market, through unregulated assurance.

At the National Cyber Security Conference for the Energy sector in September 2022, Joanna addressed the issue to a legal panel featuring Rois Ni Thuama, EU Cyber Woman of the Year, who discussed the development of C-suite responsibilities for cyber accountability.

This white paper, "Should marketing within the Cyber Sector be regulated?" is the result of a dynamic collaboration between three recognised cyber trailblazers who co-authored it.

After several years of guest masterclass lectures by Joanna at the University of St Andrews, the Post Graduate Course in HR Management will include an assessment of the HR leader's role in an organisation's cyber resilience beginning in February 2023. As HR is so intrinsically linked to the marketeers fulfilling the roles, including HR within this ecosystem is imperative.

In April 2023 the Cyber Leaders Summit, sponsored by Cyber News Global, OPS Cyber, Police Scotland, FBI and CIISec, invited the Co-authors to officially launch their white paper at the summit.

Co-Authors of Collaboration

Joanna Goddard, award winning specialist data-informed growth Consultant to the UK cybercrime programme for SME and supply chain cyber resilience for Business Resilience International Management (BRIM); Laura Irvine, Partner and Head of Regulatory Law at Scottish law firm, Davidson Chalmers Stewart (DCS), and former Board Members of Scottish Business Resilience Centre; and Rois Ni Thuama , EU Cyber Woman of the Year, and Head of Cyber Governance, boasting an in-house Doctor of law specialising in Cyber governance at UK based cyber provider, Red Sift collaborated to co-author this whitepaper.

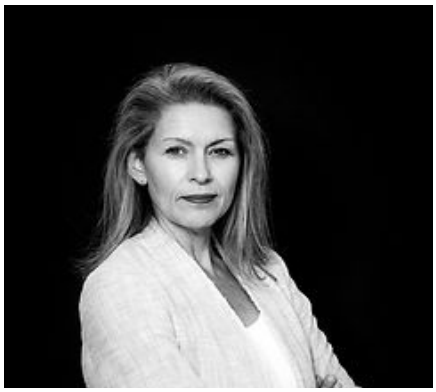
The conversation following the 2022 National Cyber Security Conference for the Energy sector was the catalyst.

Whilst the 2022 conference panel addressed the imperative of C-suite leaders becoming more educated on their cyber resilience risk and accountabilities, Joanna of BRIM raised the topic of dual responsibility by legislators, to make the selection process more protected once C-suite leaders become educated, and ready to engage and invest in Cyber resilience measures. Notably imperative for small businesses where they are unlikely to have in-house security or security expertise within their IT supplier.

With no standards to prevent 'false promises' in that any single product or service can make an organisation 'cyber secure', procurement can result in a false sense of security, resulting in *increased risk of, rather than improved resilience, though increased ignorance*. Contravening the NCS 22.

Red Sift and DCS responded in support of this proposition.

Research showed no one was addressing it.



Joanna Goddard FCMI

Partner - Growth Specialist, BRIM

Laura Irvine LLB LLM MA

Partner and Head of Regularory Law, Davidson Chalmers Stewart

Dr Rois Ni Thuama

Head of Cyber Governance, Red Sift

International Assurance Landscape

In March 2023, the Securities and Exchange Commission (SEC) proposed new rules aimed at addressing cybersecurity risks in the US Securities Markets.[1] [2] In a press statement, SEC Chair Gary Gensler emphasised the significant growth in the nature, scale, and impact of cybersecurity risks in recent years. He highlighted the need for investors, issuers, and market participants to be confident that these entities have appropriate safeguards in place for the digital era. This, in turn, would contribute to fulfilling the SEC's mission, particularly in terms of protecting investors and maintaining orderly markets.

As part of this initiative, the proposed cybersecurity rules require companies to disclose the level of cybersecurity expertise possessed by their boards of directors. The objective is to provide market participants with transparency regarding a company's cybersecurity measures and its resilience to cyber threats. Understanding a company's cybersecurity and cyber resilience posture is now regarded as essential after a significant increase in its importance.

In order to address this urgent corporate issue, a growing number of organisations are opting to outsource their cybersecurity expertise, similar to outsourcing a financial director or legal counsel service. However, the issue arises: what qualifications qualify an individual as a 'cyber expert'?

In the UK, there are mandatory law society memberships and associated regulations and disciplinary procedures in place to protect the selection of certified and accredited legal practitioners. Similarly, equivalent bodies exist for accountants. Currently, there is currently no regulatory body governing cyber professionals.

Various developments including the UK Cyber Security Council are evolving policy and standards to address this for delivery practitioners. However, without equivalent marketing regulation of said practitioners, services, and products from within the Cyber sector, how will B2B and B2C end users select suppliers with confidence and assurance? The Cyber Security Council is developing certification and accreditation and exploring routes to standardise recognised roles and related skills and experience. However, no protection on how these services are marketed exists.

We would like to instigate the sector to address this in tandem to enable full sector assurance.

In a world where recognised ‘experts’ agree it is impossible to achieve a ‘cyber secure’ posture, but cyber resilience measures can be identified and implemented, often only effective due to aligned policy, process, and continuous development, assurance is now required for the marketing of products and services.

This would mirror the evolution of advertising regulation. The evolution in consumer protection throughout the last few decades setting a precedent. For example, in the UK, the Solvite advertisement is a case in point: https://youtu.be/4h5mErP1E6A

The history of the Advertising Standards Agency (ASA) stretches over half a century. Notably in 2010, following a period when the internet became the second most complained about medium for advertising, websites and social media content became obliged to adhere to advertising rules also.

> In September 2010, CAP announced the extension of the ASA's online remit to cover advertiser's own marketing communications on their own websites and in other non-paid-for space under their control, such as social networking sites like Facebook and Twitter. Journalistic and editorial content and material related to causes and ideas - except those that are direct solicitations of donations for fund-raising - are excluded from the remit.
>
> - Our history - ASA | CAP

Therefore, the framework to promote, support and govern marketing regulation already exists.

These milestones are also reflected in the history of legal marketing and regulatory evolution.

Advertising, often referred to as touting, in the Scottish legal sector was banned in the 1930s. It was only reintroduced in 1985 but in a very restricted way. There has been a gradual relaxation of the restrictions but if the solicitor claims to be a specialist in any field of law, then the onus of proof is on the solicitor to prove that it should be challenged.

Legislation states that advertising should not contain any inaccuracy or misleading statements or anything that could reasonably be regarded as bringing the profession into disrepute, as well as a ban on it being defamatory or illegal.

Compare claims about making your system 100% secure or indeed claims about 'zero trust technology' both of which are patently untrue, yet we have all heard claims of this nature.

Even now there is draft legislation in Scotland to stop unqualified persons using the title "lawyer" if they are not qualified solicitors or advocates. The proposal is to criminalise this type of assertion.

In the UK marketing in general is regulated by the Advertising Standards Authority (ASA). The ASA is independent of the UK Government and the advertising industry; however, it is recognised by them both as the body to manage complaints about advertising. In addition, it proactively monitors markets, industry, and adherence to regulation.

Our view is that the cyber sector itself needs to take the lead on the standards that businesses and consumers can expect, identifying what is misleading advertising and what is responsible advertising. And then lead developments with the marketing and advertising industries.

The National Cyber Security Centre (NCSC), the cyber division of GCHQ could play a key role in defining what is technical or educational content as a point of difference to marketing content to engage businesses in a customer journey.

[1] See https://www.sec.gov/rules/proposed/2022/33-11038.pdf
[2] https://www.sec.gov/news/press-release/2023-52

UK response and current context

In the UK, law enforcement has led strategic partnerships with the government, the private sector, and academia to deliver The CRC Network, a highly innovative nationwide initiative to engage SMEs in cyber resilience.

Due to its significance in resolving the difficulty of attaining a cyber resilient supply chain, this has evolved and developed since 2019 with multi-national enterprise companies engaging. As a result, National CRC Group was established and private partners such as Microsoft, KPMG, CGI, Very Group, NatWest Group, and Mastercard have joined, recognising that this is an impactful solution.

With a data analysis informed growth strategy across nine regional Cyber Resilience Centre's (the CRCs) to support SME engagement in cyber resilience, it is additionally supported by academic research in cyber resilience engagement influences. [3]

National CRC Group published its first report providing a measured engagement and research informed platform with UK SMEs that is unparalleled, **it offers a mechanism for consultation that is directly informed by the end user, the SMEs.**

In 2020 Ticketmaster was fined £1.25 million by the ICO for a breach of the security principle under the GDPR for allowing a vulnerability in a third party chatbot, Inbenta, to access customer payment details. Contractual terms were in place with Inbenta requiring that their software be free from malware.

It was not. Ticketmaster had placed the chatbot on its payment page which allowed the malicious code to scrape the user-inputted data back to the attackers. This included personal and financial data such as names and payment card numbers, including the expiry date and the CVV number.

Inbenta had been alerted to a potential issue and had provided Ticketmaster with reassurance about malware and stated that had they known that their software was being used by Ticketmaster on a payments page, they would have advised against it as a security risk. This was not explored further by the ICO and Inbenta was not fined for the security breach as a supplier/processor.

The possibility of issuing fines to processors was introduced by the GDPR in 2018 but the ICO has, to date, not exercised this right. Ticketmaster did initially challenge the fine and claims for compensation and we understood that part of this challenge was to submit that Inbena was at least partially liable. However, this potential litigation settled without the need for any court hearings and so without any guidance from the courts about what is expected of suppliers in terms of data security and how this is reflected in their legal and marketing materials.

The relationship between accountability in the supply chain underlines the requirements for assurance in the marketing of promises made.

[3] https://nationalcrcgroup.co.uk/ncrcg-annual-report/

The sector and marketing imperatives to be addressed

An assurance process is required to prevent the current practice of overpromising, which increases risk due to miss-selling, over selling, and misleading by providing a deceptive sense of security. In addition, to prevent 'poor experience', which often results in a subsequent reduction in cyber resilience engagement thereafter. Positive experience generates referrals. We know that SMEs accept referrals and recommendations of what not to do from other SMEs.

What do we mean by **over promising**?

The use of the term 'secure;' promises to make you 'Cyber secure' using one product or service.
The use of the terms 'guidance' and 'advice' requires definition. For example, drawing upon the requirements within legal and financial markets whereby it is a requirement that published generic marketing content applies advertising and marketing disclaimers i.e.

- Advice must be given under contract to a specific organisation and by a relevant qualified specialist. Guidance can be generically shared information, open to interpretation at the reader's own risk.

- Legal risk may be incurred by organisations (both public and private) if they present any generic marketing collateral positioned as 'advice'. This could be later presented by an organisation with a legal claim to damage that the 'advice' followed did not sufficiently protect them from a cyber-attack.

A second level risk is incurred if any guidance or advice presented featuring technical content, was not signed off by a technical specialist. This is high risk for marketing content published in the cyber sector.

Impact on skills and sector growth

There is risk and opportunity growing in related roles including HR and recruiters operating within sales and marketing for the cyber industry.

Risk

The use of open-source intelligence gathering as a benchmarking tool is of utmost importance when evaluating the level of security competency. One notable tool in this regard is BIMI radar, which[4] conducts a global survey and monitors 71 million domains. It offers valuable insights to businesses by identifying those that have strong email authentication practices. However, the findings are concerning, as less than 2.8% of businesses among the surveyed domains conform to globally accepted standards, and a mere 0.00202% include essential indicators for email recipients.

Failure to comply with well-established email configuration standards exposes businesses to the risk of brand impersonation. This, in turn, can result in reputational damage, diminished consumer confidence, and disruptions to business operations. It is therefore crucial for organisations to prioritise the adoption and[3] implementation of these standards to protect their brand, foster trust among customers, and maintain smooth business operations. These are business concerns that marketing and HR directors should be aware of if they are to meet their legal obligations.

As exemplified by the[5] University of St. Andrews, it is crucial for universities to incorporate cyber resilience into Marketing and HR courses. This proactive measure would provide additional protection to organisations over time and contribute to enhancing national cyber resilience.

Opportunity

Sectors devastated by the pandemic and/or struggling in economic recovery may see an opportunity for the government to support the upskilling of experienced marketeers from other sectors, into cyber, with training in a Code of Good Practice from the outset.

Bringing engagement experience from hospitality and retail could further boost online service levels.

Equally, sectors with marketeers experienced in navigating regulated marketing where redundancies exist due to the increased use of automation, such as the legal sector, offer a significant opportunity to bring discipline and value to the cyber sector's marketing.

[4] https://bimiradar.com/glob
[5] Section 172 (a), (c), and (e) Companies Act 2006

Indicators of sucess

What would indicate progress and success within 12 months, i.e., by the Cyber Leaders' summit 2024?

1 Code of Good Practice established

The word security is dropped, 'informally banned' within a 'Code of Good Practice' for marketing cyber products and services, created and promoted by an independent body from cyber and/or marketing for engagement marketing. (i.e., why to use it). This ideally would include the UK and Scottish Cyber Security Councils, The Chartered Marketing Institute, and The Advertising Standards Authority (ASA) Committee of Advertising Practice (CAP).

2 Marketing education available

A diploma or recognised qualification that links marketing and an understanding of cyber resilience for technical content creators is established by a UK university. (i.e., technical guidance or tips.)

3 Standards established

A professional road map for developing standards for marketing personnel within the cyber industry is created and adopted by the UK and Scottish Cyber Security Councils. Aligned with the Professional Registration Road map for cyber practitioners and deciding if a regulatory framework is required to align with the National Cyber Strategy 22 delivery timeline.

3

Evidencing progress

Establish an annual benchmark of research statistics from UK companies on the adoption of best practice for email configuration within marketing using BIMI radar.

Scaling impact

The UK CRC Network , run by UK Law Enforcement and supported by Home Office, is being prepared to scale and could then deploy awareness to UK SMES in partnership with enterprise, their SME supply chain, customers, and academia on the new Code of Good Practice and emerging additional developments within the marketing industry for marketing cyber products and services.

Simultaneously, UKC3, the UK cyber cluster network supporting the developments in the cyber industry with academia could deploy the Code of Good Practice to cyber practitioners within their networks.

Conclusions

1 Ban 'Secure'

By establishing a Code of Good Practice, mapping with legal and financial marketing regulation because cyber is also a professional service, and an undereducated client base has growing demand to find, adopt and deploy its products and services. A Code of Good Practice for marketing of cyber products and services is an immediate progress point that could mitigate growing risk. It's creation must involve Technical/Operational/Legal and Marketing expertise. It must not stifle innovation in the cyber resilience supply chain; however, it should protect misleading buyers from believing one product or service stand alone will ensure the security of their organisation. It should be established in consultation with UK and Scottish Security Councils, The UK CRC Networks, UKC3, Marketing bodies as well as legal, technical and HR contributors.

2 Investment in skills development

Security is illusory but resilience is not. There is a requirement to introduce discipline into the language applied across the marketing of cyber products and services. Marketing should not be technical in isolation, it should be engaging and supporting relevantly qualified expertise. It should help buyers navigate relevant products with ease to make informed decisions. The Marketing and HR knowledge gap needs to be closed with education and campaigns. Vast opportunity lies in upskilling highly experienced marketeers from other marketing regulated sectors.

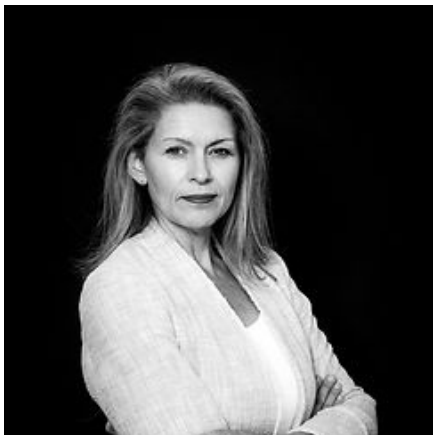
3 Create policy for change

Recommendations identified to be policy led for change. Skills development specifically within marketing for the cyber sector needs Government support to create and educate on standards. Aligning with the focus form World Economic Forum on the subject of demand; Reskilling and upskilling talent help shrink cybersecurity skills gap | World Economic Forum (weforum.org) CPD for cyber marketeers needs to be established. CPD for cyber marketeers needs to include recent case law examples.

About the Authors

Joanna Goddard FCMI

Partner for BRIM Business Resilience International Management



BRIM
BUSINESS RESILIENCE
INTERNATIONAL MANAGEMENT

Joanna leads growth advisory to the Home Office and UK law Enforcement for BRIM, on the development and delivery of the national cybercrime programme.

She specialises in data informed strategies for rapid risk management and engagement in hard-to-reach markets as an award-winning business growth consultant. In addition to being a Fellow of the Chartered Management Institute (CMI), she is certified in Business Analytics by Judge Business School, Cambridge University, and trained in ISO20700 by ICMCI, The International Council of Management Consulting Institutes.

Her extensive international commercial network and multi sector experience enables law enforcement, the government, and the business community to effectively structure collaboration with a return on investment (ROI) that is efficiently managed.

Prior to working in the security industry Joanna founded her own business, delivering internationally, was recognised as a ‘go to’ expert, and advised a Channel 4 TV series from inception for over four years. As a former director of a law firm, Joanna is also adept at coordinating governance and legal implications with legal advisory teams across multiple jurisdictions.

In addition to expanding the reach of the national network of Cyber Resilience Centres across at-risk SMEs for UK law enforcement, Joanna works directly with national and international business leaders.

Joanna is passionate about the importance of a positive culture and wellbeing within the Cyber community. She is a guest lecturer at the University of St Andrews and a member of the Strategic Advisory Board member of Converge, which supports the development of Scotland's Universities' start-ups and spin outs from Scotland’s universities.

Laura Irvine LLB LLM MA

Partner Davidson Chalmers Stewart

LLB (Hons) (Edinburgh); LLM in Human Rights (Strathclyde); MA in Criminology (Keele); Solicitor (Scotland) 2000; Law Society of Scotland Accredited Specialist in Freedom of Information and Data Protection.

As a former procurator fiscal depute with COPFS, with 20 years of working throughout the court of Scotland, Laura knows her way around the criminal justice system and provides clients with invaluable insight into what to expect from regulators and the Crown.

She is passionate about data protection, privacy and information law and was part of the only legal team in the UK to have successfully overturned a data breach fine imposed under the Data Protection Act 1998 – see Scottish Borders Council v the Information Commissioner.

Laura provides clients with contentious and non-contentious data protection advice having spent 2017 and 2018 advising clients across all sectors on how to implement the changes that the General Data Protection Regulation and the Data Protection Act 2018 brought in. She is the Convenor of the Law Society of Scotland's Privacy Sub-Committee and recently gave evidence to the Public Bill Committee at Westminster considering the Data Protection and Digital Information (No 2) Bill.

Dr. Rois Ni Thuama

Head of Cyber Governance Redsift

RED SIFT

Rois is a Doctor of Law and subject matter expert in corporate and cyber governance, risk, and compliance. She is an award-winning cybersecurity expert and is the Head of Cyber Governance for Red Sift, one of Europe's fastest-growing cybersecurity companies.

Dr Ni Thuama works with key clients across a wide market spectrum providing expert insight to governments. Her most recent work was for the British Government for the Joint Committee on National Security Strategy (JCNSS) whilst her legal opinion has been sought by the US Government.

As an invited guest of the US Government, Dr. Ni Thuama delivered a presentation at Fort McNair, focusing on the legal implications of AI in future conflicts. The audience comprised military experts from the US Department of Defense. This presentation had a significant impact on shaping the understanding of AI in future conflicts, leading to the decision to discontinue the use of the term "autonomous" when referring to weapons and weapon systems.

She is an Instructor for Cybersecurity, and on the Joint Command & Staff Course (OF-3) with the Irish Defence Forces. She works with boards and management across legal, financial, energy, and banking sectors to spread a contemporary understanding of cyber threats, risks, liabilities, and resilience across diverse audiences and stakeholders to drive effective change.

3

Sponsored by

OSP CYBER ACADEMY

Research Reference Points

1. The UK Government National cyber Strategy 2022 National Cyber Strategy 2022 - GOV.UK (www.gov.uk)

2. The Cynam Webinar where Joanna Goddard first raised the topic publicly in 2021 https://youtu.be/zYC54hxh1wM

3. The security minister launches police led National CRC Group, in supporting of the success of regional Cyber Resilience Centres, addressing the need for SMEs to engage in cyber resilience, December 2021. Security Minister launches brand new National Cyber Resilience Centre Group (brimcentre.com)

4. University of St Andrews adopts Cyber Resilience as part fo assessed HRD Post Graduate Course. University of St. Andrews develops cyber resilience into HR Management student learning (brimcentre.com)

5. 2022 conference Cyber Resilience for National Security & the Energy Sector - OSP Cyber Academy]. This whitepaper was launched at the 2023 conference in response, to instigate developments to improve assurance within the sector. Senior Leaders Cyber Summit - OSP Cyber Academy

6. OPS Cyber invites the whitepaper co-authors to launch the white paper at the 2023 Cyber Leaders Summit, sponsored by Cyber News Global, FBI, Police Scotland, Robert Gordon University, CIISec,, Scotland IS and BRIM. Senior Leaders Cyber Summit Speakers - OSP Cyber Academy

7. Marketing and advertising: the law: Regulations that affect advertising - GOV.UK (www.gov.uk)

8. New vs Old Marketing Methods for Law Firms – Lawyer Monthly | Legal News Magazine (lawyer-monthly.com)

9. Board Certification in Cosmetic Surgery: An Examination of O... : Annals of Plastic Surgery (lww.com)

10. Advertising regulator to clampdown on greenwashing ads - BBC News

11. 18 False Advertising Scandals (businessinsider.com)

12. Our history - ASA | CAP

13. Professional Registration Roadmap by the UK CYber Security Council Professional Registration Roadmap (ukcybersecuritycouncil.org.uk)

14. The Cyber Scotland Partnership Cyber Scotland – Up to the minute cyber services information across Scotland.

15. The CRC Network, by UK Law Enforcement supported by Home Office Homepage - National CRC Group

16. Uk CYber Custers UKC3 Home - UK Cyber Cluster Collaboration (ukc3.co.uk)

17. NCAC National Cyber Security Centre National Cyber Security Centre - NCSC.GOV.UK

18. World Economic Forum The World Economic Forum (weforum.org)

19. UK advertising in a digital age (parliament.uk)

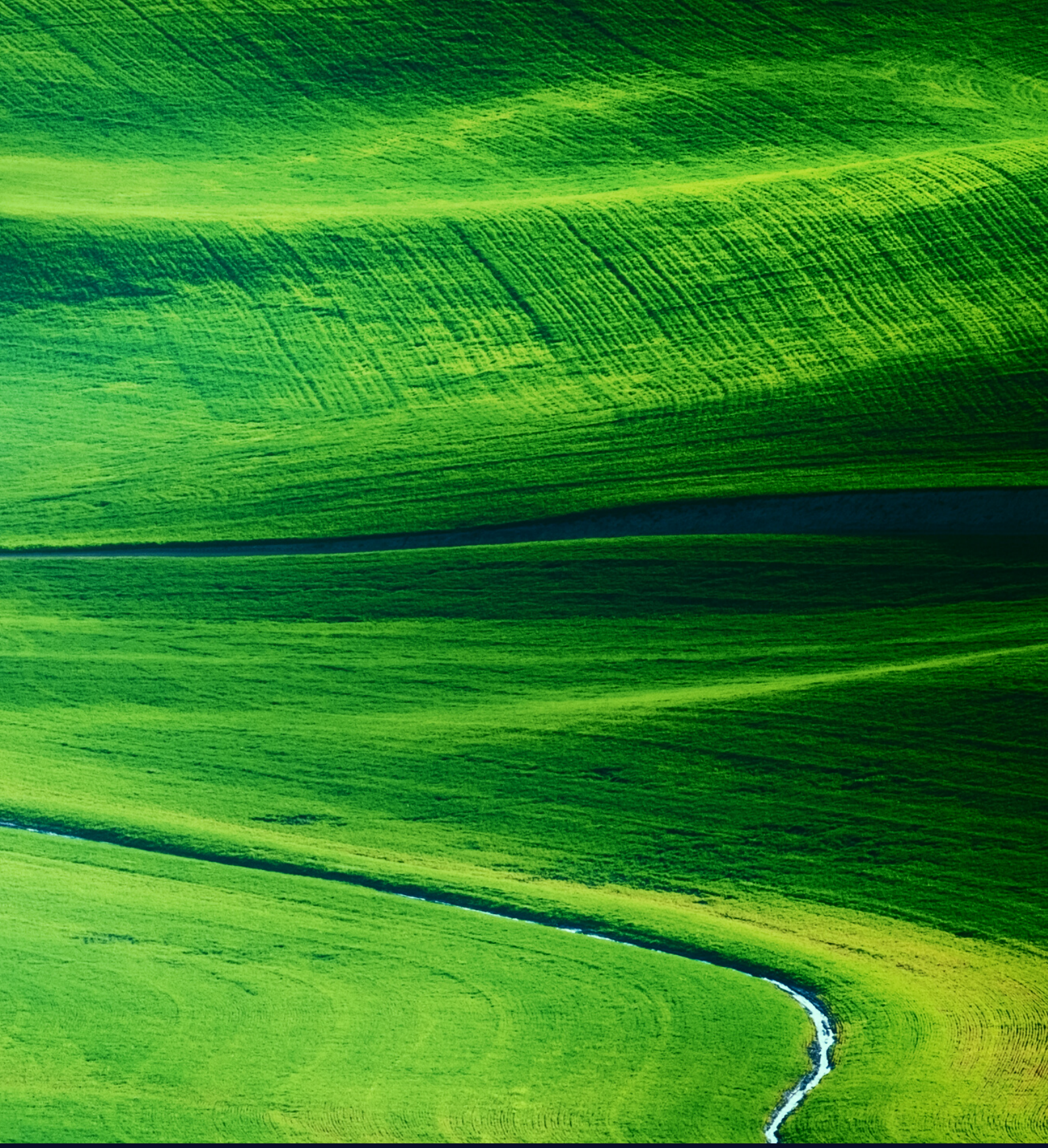
20. https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022

21. UK NIS – Get ready for expansion of the UK's critical national infrastructure cyber security laws – Privacy Matters (dlapiper.com)

22. Homepage - Cybersecurity Marketing Society

23. https://www.legislation.gov.uk/ukpga/2006/46/part/10/chapter/2/crossheading/the-general-duties

24. https://www.bimiradar.com



BRIM

BUSINESS RESILIENCE
INTERNATIONAL MANAGEMENT