social machines

CYBER RISK CULTURE:
CURRENT ISSUES AND PRACTICES

Researchers	Midori Nishioka, Manuel Cañas
Project Technical Lead	Justin Hempson-Jones
Lead Reviewer	Felipe Costa Sperb
Published online	26 November 2024

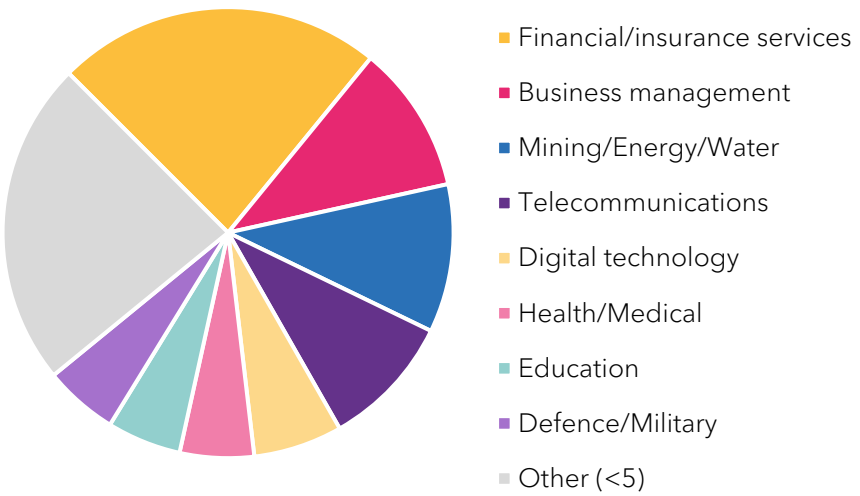
Overview

A critical aspect of cyber security is managing cyber risks. Cyber risk culture can be conceptualised as a subculture or subset of a broader concept of cyber security culture, and a group's (e.g., an organisation's) shared norms, beliefs, knowledge, values, attitudes, and behaviours relating to cyber risks. Understanding how cyber risk culture can be embedded within organisations is important for securing organisations across all sectors and industries in the United Kingdom (UK). However, cyber risk culture is a relatively novel and potentially multi-faceted concept, which poses a challenge for organisations looking to strengthen their own cyber security, and for organisations supporting this journey (e.g., consultancy, professional bodies, government organisations).

Aims and Methods

Social Machines conducted research to identify the barriers, enablers, worst practices, and best practices regarding effective cyber risk management and embedding cyber risk culture. The method began with a scoping literature review in order to identify key themes in this problem space and to establish an evidence base from which to expand upon through primary data collection. The research team then conducted semi-structured interviews with 29 subject matter experts, such as cyber security professionals and risk practitioners, in order to elaborate on and modify the initial set of themes.

All interview participants had experience working in the private sector, 19 had experience in the public sector, and 3 participants had experience in charities or the third sector. They had experience in a range of industries (see the figure to the right).



social machines

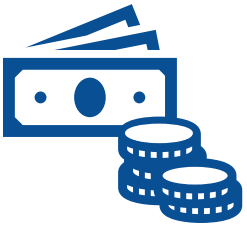
Findings

Cyber security has not built solid and standardised best practices, which can diminish outsiders' perceptions of the field's credibility. The strong focus on technological expertise and solutions in cyber security can come at the expense of understanding how people and organisations work. Embedding cyber risk culture requires working with, not against, organisations' goals and their people. "Soft" skills that would support this endeavour, such as communication and relationship-building, are not valued enough in the cyber security field.

Buy-in from leadership is critical, but middle and lower management and staff members are also important for ensuring that top-level priorities trickle down and translate to action. Cyber risk should be represented at the top, but the Chief Information Security Officer (CISO) does not need to sit on the board; what is more important is for cyber security to have an independent voice that is channelled to the senior leadership and the board.

"Non-cyber" people's engagement is impeded by competing priorities, including the need to deliver fast and maximise benefits to oneself and the organisation. The trade-off between speed or reward and security is not well-understood by organisational leaders. High-profile cyber incidents can motivate organisations to act, but interest and investment in cyber security may wane over time. Regulations are important for encouraging organisations to invest in cyber risk management, but organisations may resist over-regulation and some cyber security professionals may be sceptical about the effectiveness of existing regulations.

A negative overall organisational culture is a barrier - e.g., toxic, bullying, non-inclusive, or discriminatory culture makes it challenging to embed a sustainable cyber risk culture and may enhance threats and vulnerability. Disharmonious or uncoordinated organisational structure and governance may also pose a challenge to cyber risk management.

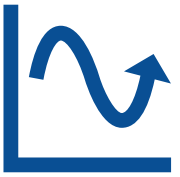


Issues with funding cyber security cut across industries and organisations of varying sizes. Whereas small and medium organisations and charities tend to lack sufficient funds to adequately manage cyber risks, budgets may be threatened in larger organisations due to difficulties justifying spending and evidencing value added.

social machines

Findings

Varied understanding of cyber risk, and risk in general, also poses a challenge; there are inconsistent definitions, approaches, and conceptualisations of risk. Poor measurements of risk are also popular and often misused. The global context in which cyber crimes are rewarded and go unpunished also poses a problem with managing cyber risks, given that the root cause of the risks may need to be addressed by governments, not individual organisations. Cyber risk is also dynamic and changing, yet organisations do not realise this, treating it as a static risk.



Interdependency and interconnectivity between and within organisations add to the challenge of managing cyber risk, yet organisations do not realise how much they rely on others, underestimating the propagation of risk.

Sharing information about issues and cyber incidents is helpful, but there are barriers to open and honest communication, such as damage to the organisation's and cyber security professional's reputation, legal confidentiality requirements, and the fear of regulatory penalties.

Current frameworks and standards are useful, but they are not sufficient or fit for purpose. Frameworks and standards have not kept up with rapid changes in cyber risks, including risks related to artificial intelligence. Most guidance tells organisations what they need to do, but not how to do it. Without expertise and experience, organisations struggle to select and tailor frameworks and standards to their specific needs and context.

Conclusions

Integrating cyber risk culture is important for cyber security. Cyber risk culture should not be isolated from the broader organisational culture, governance, and management.

Negative cyber risk culture may exist in two forms. First, in some organisations, cyber risk culture is absent due to immaturity, with no leadership support, personnel, budget, or policies for managing cyber risks. Second, organisations can have a dysfunctional cyber risk culture, in which cyber risk is poorly governed, limited to surface-level regulatory compliance, and disconnected from the organisation's decision-making and strategy.

Positive cyber risk culture is characterised by the involvement of well-trained professionals who connect cyber risks to organisational priorities, ensuring stakeholder engagement at all levels. Senior leaders support strategic cyber risk management that is integrated with other types of risks (e.g., financial risk). Organisations collaborate across sectors and with the government to share best practices and threat intelligence. Clear and evidence-based regulations and guidance support the smooth implementation of effective cyber risk management.

social machines

Recommendations

Based on the findings, the following recommendations were identified for organisations to embed an effective cyber risk culture, and for those looking to support this journey (e.g., consultancy, professional bodies, government organisations).

- Promote training that targets the weak areas: Cyber security professionals' training can be improved by promoting programmes that address critical yet under-prioritised areas. These include risk management, business and communication skills, leadership and influence skills, and basics of behaviour and culture change.

- Offer a playbook of cyber risk management: Many organisations know they need to manage cyber risks but require additional support that is tailored to their context. Consultancy services and guidance can offer case studies and tailored advice based on industry and organisation size.

- Support the development of knowledge-sharing networks: Cyber security professionals may prefer sharing sensitive information in small, trusted groups. Leaders within the community can help build connections for smaller, less established organisations, so that risks and best practices are widely shared.

- Enhance visibility and presence outside cyber security: Leaders in the community can promote cyber risk management in fields outside cyber security to enhance collaborations across disciplines. They can collaborate with professional bodies to integrate cyber risk frameworks and guidance with industry standards.

- Promote positive organisational culture: Organisations can foster a positive overall culture and leverage existing cultural assets to enable the development of a strong cyber risk culture. Consultancy and professional bodies can explore ways to implement positive cyber risk culture within negative organisational cultures.

- Offer guidance on integrating cyber risks with other risks: Resources that balance the uniqueness of cyber risks with comparability to other risks can be offered to organisations. For example, organisations may benefit from guidance on enterprise risk management.

- Support the informed use of cyber risk products and services: Guidance around products and services may be especially helpful for small businesses and charities that tend to outsource cyber risk management.

- Solidify evidence for regulations and guidance: Organisations across the UK can collectively participate in generating evidence to test the practical effectiveness of regulations, guides, and tools, as applied in the field.

social machines

For more information about Social Machines behavioural science research and innovation work and capabilities, please contact Nick Wilding at nickw@socialmachines.co.uk or go to www.socialmachines.co.uk.