ISRM

INSTITUTE OF STRATEGIC RISK MANAGEMENT

ISRM GLOBAL JOURNAL 2024

WICKED PROBLEMS

July 2024

PUBLISHING INFORMATION

First published in Australia in 2024 by the Institute of Strategic Risk Management Australia New Zealand Limited (ISRM ANZ).

A catalogue record for this book is available from the National Library of Australia.

ISBN 978-1-7635587-0-0

DISCLAIMER

Facts and opinions in articles appearing in this publication are solely the personal statements of respective authors. Authors are responsible for all content in their article(s) including accuracy of the facts, statements, citing resources, and so on. This publication and its editors disclaim any liability of violations of other parties' rights, or any damage incurred as a consequence to use or application any of the contents of this publication. Material submitted to this publication must be original and not published or submitted for publication elsewhere unless previously agreed. Consideration by ISRM ANZ is based on membership and interest in the activities of the association. The author is responsible to get permission from previous publishers or copyright holder if an author is re-using any part of paper (i.e. figure or figures) published elsewhere, or that is copyrighted. The editors in good faith consider that Authors of all material have full permission to publish every part of the submitted material including illustrations. ISRM ANZ cannot be held liable for the use of misuse of any information contained in this publication and users should seek expert opinion before applying any of the contents.

JOURNAL EDITOR

WELCOME

Recent events have reminded us of the VUCAD world in which we live – one in which we are regularly confronted with, and called upon to address, a wide range of "wicked problems". A term which is often misunderstood by "outsiders to the risk world", wicked problems are typically defined as…

"…those problems for which any resolution that could be proposed only generates further issues, and where solutions are not true or false or good or bad, but merely the best that can be done at the time based on the available evidence."

(ISRM Centre for the Study of Wicked Problems)

In recognising the centrality of being able to address such issues, and indeed to acknowledge the recent launch of the **ISRM Centre for the Study of Wicked Problems (CSWP)**, this particular publication is concerned with "wicked problems", and to exploring the range of associated considerations. Not surprisingly, a review of the featured articles would seem to indicate that we best try not to "manage" wicked problems in the regular sense, let alone trying to actually solve them. A core principle that becomes clear is that in order to address wicked problems, we need to adapt our traditional problem-solving approaches and paradigms – we need to reconsider how we frame, approach, and manage them.

I trust you will enjoy reading the articles in this issue, and encourage you to reflect on the key concepts raised as we continue to enhance our understanding and application of the same.

DR PAUL JOHNSTON FARPI FISRM CHFINSTP RPP
JOURNAL EDITOR

TABLE OF CONTENTS

ISRM WORLD CHAPTERS

Abuja Chapter
Chair
Rueben Odum
rueben.odum@theisrm.org

Vice Chair
Blessing Igbankwe
blessing.igbanwe@theisrm.org

Antigua Chapter
Chair
Amanda Peters
amanda.peters@theisrm.org

Australia & NZ Chapter
Chair
Gavriel Schneider
gavriel.scheider@theisrm.org

Vice Chair
Joe Saunders
joe.saunders@theisrm.org

Bangalore Chapter
Chair
Rajiv Shah
rajiv.shah@theisrm.org

Vice Chair
Vandana Verma
vandana@infosecvandana.com

California Chapter
Chair
Brian von Kraus
brian.vonkraus@theisrm.org

Delhi Chapter
Chair
Garry Singh
gary@iirisconsulting.com

Vice Chair
Shraddha Bhandari
shraddha.bhandari@theisrm.org

Dubai Chapter
Administrator
Nikolaos Gkionis
nikolaos.gkionis@theisrm.org

Administrator
Steven Flaherty
steven.flaherty@theisrm.org

France Chapter
Chair
Bruno Sechet
bruno.sechet@theisrm.org

Houston Chapter
Chair
Ken Smith
ken.smith@theisrm.org

Indonesia Chapter
Chair
Basil Gouge
basil.gouge@hill-assoc.com

Ireland Chapter
Chair
Jenn Ciolfi
jenn.ciolfi@theisrm.org

Vice Chair
Garry Bergin
garry.bergin@theisrm.org

Israel Chapter
Chair
Ivor Terret
ivor.terret@theisrm.org

Jamaica Chapter
Chair
Julian Wilson
julian.wilson@theisrm.org

Japan Chapter
Chair
Scott McQueen
scott.mcqueen@theisrm.org

Kenya Chapter
Chair
Robert Christie
rabc@takuheconsultants.com

Kuwait Chapter
Chair
Ben Griffin
ben.griffin@theisrm.org

Malaysia Chapter
Chair
Piers Dixon
piers.dixon@theisrm.org

Manchester Chapter
Chair
Alan Cain
alan.cain@theisrm.org

Nordic States Chapter
Chair
Christian Fader
christian.fader@theisrm.org

Oman Chapter
Chair
Ali Al Harthy
ali.alharthy@theisrm.org

Philippines Chapter
Chair
Sergio Diasana
sergio.diasana@theisrm.org

Port Harcourt Chapter
Chair
Bryan Roberts
bryan.roberts@theisrm.org

Vice Chair
Gloria Ayika
gloria.ayika@theisrm.org

Singapore Chapter
Chair
Julian Tan
julian.tan@theisrm.org

South Africa Chapter
Chair
Brian Kennedy
brian.kennedy@theisrm.org

Vice Chair
Marisa Taino
marisa.taino@theisrm.org

South Eastern EU Chapter
Chair
Zoran Kekovic
zorankekovic@yahoo.com

Trinidad Chapter
Chair
Tessa Drayton
tessa.drayton@theisrm.org

EXPLORE MEMBERSHIP

The Institute of Strategic Risk Management has been established in order to create a global centre where practitioners, academics and policy makers can come together to share information, help progress and promote the underlying understanding and capabilities associated with strategic risk and crisis management, and develop their own personal and professional networks.

Visit www.theisrm.org for more information.

NAVIGATING THE CHAOS: TACKLING WICKED PROBLEMS IN THE MODERN RISK ENVIRONMENT

BY CHRIS DOUGLAS

You may have heard this term before, but what exactly are “Wicked Problems”? Well, they are complex, interconnected issues that are difficult to define, and even more difficult to solve. They can range from climate change, to poverty, to cybersecurity threats. These problems are so challenging because they involve multiple stakeholders with different perspectives and interests.

So why are we talking about Wicked Problems today? Because they are becoming increasingly prevalent in our modern risk environment. As society becomes more interconnected and technology advances, the risks we face become more complex and uncertain. It's important for us to understand these challenges and work together to find solutions. That's what we'll be exploring in this particular article.

Characteristics of Wicked Problems

Wicked Problems are complex issues that are difficult to define and even more difficult to solve. They are characterised by their interconnectedness, which makes it hard to isolate individual components for analysis. Wicked Problems are also highly uncertain, as there is often no clear solution or outcome that can be predicted with certainty.

Additionally, Wicked Problems are ambiguous, meaning that they can be interpreted in different ways, depending on the perspective of the person analysing them. This ambiguity can make it challenging to develop a shared understanding of the problem and its potential solutions. Overall, the characteristics of Wicked Problems make them some of the most difficult challenges facing society today.

The Modern Risk Environment

The modern risk environment is complex and constantly evolving, with new threats emerging all the time. From cyber-attacks to climate change, we face a wide range of challenges that require innovative solutions. One of the key factors that makes these challenges so difficult to address is the concept of Wicked Problems. These are complex, multi-dimensional issues that resist easy solutions and require collaboration across different sectors and disciplines.

One example of a Wicked Problem in the modern risk environment is the issue of cybersecurity. With so much of our personal and professional lives taking place online, the threat of cyber-attacks is more pressing than ever. Hackers are becoming increasingly sophisticated, and it can be difficult for organisations to keep up with the latest threats. This is just one example of how the modern risk environment is affected by Wicked Problems, and why we need to work together to find solutions.

Examples of Wicked Problems in the Modern Risk Environment

Climate change is one of the most pressing Wicked Problems facing the modern risk environment. Rising temperatures and sea levels threaten to cause widespread damage and disruption, while extreme weather events such as hurricanes and wildfires are becoming more frequent and severe.

Cybersecurity is another Wicked Problem that poses a major risk to individuals, organisations, and governments. As our lives become increasingly digitised, the potential for cyber-attacks and data breaches grows, with potentially devastating consequences. Public health crises such as pandemics also fall into this category, as they are complex and difficult to predict or control.

Cultivate situated humility, scope your needs honestly, and develop trusted partner relationships.

The Role of Technology in Addressing Wicked Problems

Technology has the potential to play a crucial role in addressing Wicked Problems in our modern risk environment. With the help of advanced technologies such as artificial intelligence, big data analytics, and blockchain, we can gain new insights and develop innovative solutions to complex challenges.

For example, in the field of public health, technology has been instrumental in tracking and controlling the spread of infectious diseases. During the Ebola outbreak in West Africa, mobile apps were used to collect and analyse data on the disease's spread, helping to identify and isolate infected individuals. Similarly, in the fight against climate change, technologies such as renewable energy and carbon capture and storage are key to reducing greenhouse gas emissions and mitigating the effects of global warming.

The Importance of Collaboration

Collaboration is essential in tackling Wicked Problems, because no single organisation or individual can solve them alone. Successful collaborations require trust, communication, and a shared vision for the future. One example of successful collaboration is the Global Polio Eradication Initiative, which brought together governments, non-governmental organisations, and private sector partners to work towards eradicating polio worldwide. Through this collaboration, the number of cases of polio has decreased by over 99% since 1988.

Another example of successful collaboration is the Paris Agreement on climate change, which was signed by 195 countries in 2015. This agreement sets targets for reducing greenhouse gas emissions, and provides a framework for international cooperation on climate change. The success of this agreement depends on continued collaboration between countries and other stakeholders.

Look at the whole system, bust silos and treat your people and contractors as though they are part of the solution.

Don't fall into the trap of security and risk theatre, manage biases and seek assurance via testing and exercising.

Innovative Approaches to Addressing Wicked Problems

TDesign thinking is an innovative approach to problem-solving that focuses on understanding the needs of the user. This approach involves empathising with the user, defining the problem, ideating solutions, prototyping, and testing. By focusing on the needs of the user, design thinking can help address Wicked Problems by creating solutions that are more effective and sustainable.

Systems thinking is another innovative approach to addressing Wicked Problems. This approach focuses on understanding the complex systems that underlie Wicked Problems and identifying leverage points where interventions can have the greatest impact. By taking a holistic view of the problem, systems thinking can help identify solutions that address the root causes of Wicked Problems rather than just treating the symptoms.

A burgeoning term within the "Wicked Problem" arena, which focuses on collaboration and thought leadership is Presilience. Presilience is "the process of successfully preventing where possible, preparing for, responding to, and recovering from adverse, major business interruption events".

Presilience represents the mindset that is needed to address issues such as Wicked Problems, and encompasses key areas such as adaptability, leadership and continual learning, as well as focusing on both opportunities as well as risk exposures.

The Importance of Adaptability

Adaptability is crucial when it comes to addressing Wicked Problems. Organisations and individuals who are able to adapt to changing circumstances are better equipped to find solutions to complex challenges.

For example, during the COVID-19 pandemic, many businesses had to quickly adapt to remote work and virtual communication in order to continue operating. Those that were able to adjust quickly were more likely to survive, and even thrive, during this difficult time.

The Role of Education

Education plays a crucial role in addressing Wicked Problems by providing individuals with the knowledge, skills, and tools needed to tackle complex challenges. For example, educational programs focused on sustainability can help individuals understand the impact of their actions on the environment and develop strategies for reducing their carbon footprint. Similarly, educational initiatives focused on public health can provide individuals with the information they need to make informed decisions about their health and well-being.

Though often thought of as being a focus of a more senior academic discipline, Wicked Problems, can often be multi-faceted/multilayered and require diverse levels of understanding and integration from stakeholders at all levels. Indeed, The Institute of Presilience holds educational courses, from a skills-based program through to senior academic consideration with its Graduate Certificate and Graduate Diploma programs, that reflect the layered (and practical) approach that is needed.

In addition to providing individuals with knowledge and skills, education can also promote collaboration and innovation. By bringing together individuals from diverse backgrounds and disciplines, educational programs can foster an environment of creativity and problem-solving. For example, interdisciplinary programs that combine engineering and social sciences can lead to innovative solutions for addressing climate change or improving public health outcomes. Overall, education is a key component of any strategy aimed at addressing Wicked Problems.

Conclusion

In conclusion, we have explored the concept of Wicked Problems and how they relate to the modern risk environment. We have defined Wicked Problems and explained why they are so challenging to solve. We have discussed the characteristics of Wicked Problems, including complexity, uncertainty, and ambiguity. We have also provided specific examples of Wicked Problems in the modern risk environment, such as climate change, cybersecurity, and public health crises. We have discussed the role of technology, collaboration, leadership, education, and adaptability in addressing Wicked Problems. Finally, we have explored innovative approaches to addressing Wicked Problems, such as design thinking and systems thinking.

It is clear that Wicked Problems are complex and difficult to solve, but they require urgent attention from all of us. We must work together, across disciplines and sectors, to find solutions that address these challenges. We must be adaptable and innovative, and to be willing to try new approaches and to learn from our mistakes. And we must be committed to educating ourselves and others about these issues, so that we can take action and make a difference.

1. *Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. Policy sciences, 4(2), 155-169.*
2. *Head, B. W. (2008). Wicked problems in public policy. Public policy, 3(2), 101-118.*
3. *Snowden, D. J., & Boone, M. E. (2007). A leader's framework for decision making. Harvard business review, 85(11), 68-76.*
4. *Brown, T. (2008). Design thinking. Harvard business review, 86(6), 84-92.*
5. *Meadows, D. H. (2008). Thinking in systems: A primer. Chelsea Green Publishing.*
6. *Schneider, G., Young, L. (2022). Presilience as a unifying practice to change, thrive and grow. ISRM ANZ Journal 2022 Autumn Edition: 20-23.*

AUTHOR BIO

CHRIS DOUGLAS

Having worked in the training industry for well over 10 years, both as a trainer and a Company Director of one of the largest regional training providers in the security industry, he has developed and implemented training standards that have set both “Brand” and Industry standard. Based on his extensive experience in security, Federal law enforcement, entrepreneurial skills, and educational acumen, he is accustomed to meeting and achieving goals.

He is client-focused, developing business and educational strategies to help and develop outcomes. Chris has experience in the corporate, state, and federal sectors, with experience in tailoring results to align with agency and legislative requirements.

RISK BASED LEADERSHIP

TODAY'S EVOLVING ENVIRONMENT – LEADING THE SAME WAY AND EXPECTING DIFFERENT RESULTS

BY DAVE OWENS AND DAVE DONOHUE

In the ever-evolving environment that leaders currently operate in (natural hazards, business or political), the acronym VUCA, (Volatility, Uncertainty, Complexity and Ambiguity)[1] has been used for decades, but do we fully understand what it means and how it impacts on today's leaders?. VUCA can be defined as:

Volatility: Change and dynamics of that change including the speed of the changing forces and turbulence within the operating environment.

Uncertainty: Unpredictability (ability to confidentiality predict the future), surprise and awareness of an issue/event. Inability to understand what is going on.

Complexity: Concurrent and complex events (number of factors operating concurrently). The more complex, the more difficult to analyse. Ambiguity: Potential to misread the event or a lack of clarity as to how to interpret due to past experiences.

Ambiguity: Potential to misread the event or a lack of clarity as to how to interpret due to past experiences.

Whilst this simplifies the VUCA approach, you will often hear the term, "Leadership in a VUCA World". In a VUCA world, strong, effective and adaptable risk-based leadership becomes even more critical. How do we engage with and produce effective risk-based leadership? In the development of, or training of current and future leaders we will need to consider and include the following attributes to ensure that the leaders of tomorrow are future proofed[2]:

a. Inspiration through a clear and compelling vision that will guide their teams through uncertainty. Effective communication skills, communicating the vision along with setting the purpose and direction.
b. Agility in a changing environment. Decision making that is agile, flexible and adapting quickly to the changing circumstances.
c. Thinking strategically and making sound decisions on the available data.
d. Leaders that are resilient – it's a stressful environment that will be challenging to all involved. Building resilience through the support of the agency to change decisions or direction during an event along with the ability to bounce back from any setbacks.
e. Collaborative Leadership. Instil a collaborative approach that reaches across all agencies to solve complex issues that ultimately will drive innovation across all areas.
f. Continuous learning through researching new technologies, trends and practices within industry and incorporating and adapting changes without feeling threatened by them.

The 2019/20 bushfire season and 2022 floods challenged many conventional assumptions.[3] Many of the tried and tested strategies and techniques did not work as events were compounding and concurrent in nature. Climate change is also impacting on and changing the frequency and severity of events. In this changing global landscape, what are the new norms that leaders can expect and how do they prepare themselves for what is to come?

Historically, leaders have been held to account through compliance against systems and processes. However, in an unstable or evolving environment, how do we prepare leaders to be flexible and adaptive in their decision making, but still hold them to account?. In order to do this, an agency must mature and be equally willing to evolve.

The current Whole of Government approach to Risk, Emergency/Crisis Management is PPRR (Prevention/Mitigate; Preparedness; Response and Recover)[4] as demonstrated in Figure [15.] Whilst PPRR is viewed as a theoretical framework, it is meant to address all aspects of an event through a cycled approach. Whilst in theory this is good, in reality it is not working because in many instances, the same mistakes occur again and again without any learnings. The Lessons Management Framework has been adopted by the NSW Government[6], however putting those lessons into practice is a painstaking process and rarely successful.

The PPRR model assumes that there is effective coordination of risk across all agencies, unfortunately this is not the case[7]. A number of agencies still operate in isolation believing that as the designated 'Combat' Agency they can undertake all of the required functions.

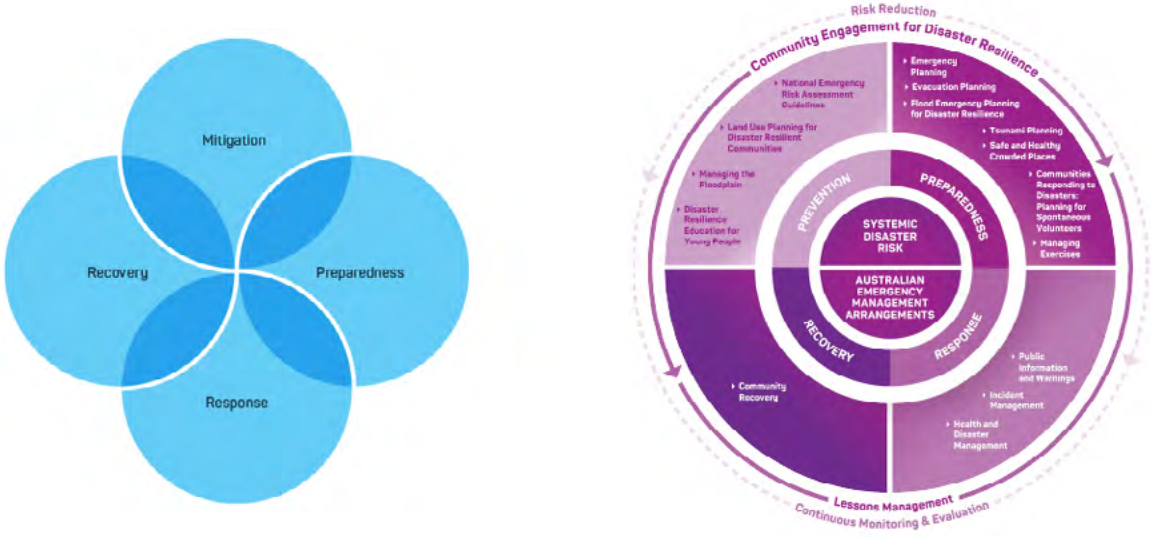


Figure 1: The emergency management cycle is represented as interrelated phases and as a 'policy landscape'. Source: AIDR (2021) .

Recovery has evolved from the historical approach of building back or restoring the business to the way it was before the event/crisis. Now Recovery is focused on building back better! Building the operating system back better, building a sustainable, resilient recovery after Covid19.

1. *Harvard Business Review (Feb 2014)*
2. *Robert Johansen - https://www.axelos.com/resource-hub/blog/vuca-prime-the-answer-to-a-vuca-dynamic Ronald Heifetz - https://www.hks.harvard.edu/publications/practice-adaptive-leadership-tools-and-tacticschanging-your-organization-and-world*
3. *NSW Independent Bushfire Inquiry https://www.dpc.nsw.gov.au/assets/dpc-nsw-gov-au/publications/NSWBushfire-Inquiry-1630/Final-Report-of-the-NSW-Bushfire-Inquiry.pdf '*
4. *NSW Government. State Emergency Management Plan. https://www.nsw.gov.au/sites/default/files/202104/state-emergency-management-plan-emplan.pdf*
5. *https://knowledge.aidr.org.au/resources/ajem-july-2022-pprr-and-aiims-a-whole-of-government-strategy-innsw/*
6. *NSW Government, Resilience NSW: A Lessons Management Framework for the NSW Emergency Management Sector (2020).*
7. *NSW Independent Bushfire Inquiry https://www.dpc.nsw.gov.au/assets/dpc-nsw-gov-au/publications/NSWBushfire-Inquiry-1630/Final-Report-of-the-NSW-Bushfire-Inquiry.pdf*

19[8] or building flood/fire resilient premises in specified areas. Traditionally under the PPRR approach, we have concentrated our efforts on development of improved processes to Response to the detriment of the other phases. **Future leadership needs to be constant, risk based, ethical decision making so that it is able to engineer outcomes through constant learning and adaptability across all four integrated areas.**

Traditionally effective leadership has always been 'labelled' into a specific category of leadership. That being Charismatic, Contingency, Transactional and Transformational leadership to name a few[9]. The traits within each category were known and understood. Staff knew the difference between Leadership and Management[10]. In a time of great risk or crisis, the leader stood at the head of the table or at the scene of the event and gave orders for others to follow. There was a clear hierarchical relationship.

We then moved away from this approach to what we would call 'group think'. It is important to obtain the facts from as many sources as possible, particularly where there are subject matter experts involved. However, we moved away from decisive leadership to group think, where the consensus of the group would be followed. This is a process where team members work as a group and agree to support whatever decision is made in the best interests of the whole. This is sometimes referred to as Facilitative decision making where everyone in the group has an equal say[11]. In the high-risk changing world that we now live in, decisions are required immediately to ensure action is taken, sometimes on limited or uncertain information.

We have found that when working with engineers for instance, that they readily adopt the facilitative decision-making model. They will want all of the facts and then go 'around the table' to consider everyone's opinions and input. They know that the decision is important and would rather take their time making the decision as they would in a business-as-usual situation. In a crisis however, where there is sometimes limited time to decide, they sometimes cannot come to a consensus within the given timeframe.

Today's leaders need to be adaptive and flexible within their 'normal' or everyday business practices. Their leadership skills also need to develop and mature so that they are able to 'switch' from 'Business as Usual' to crisis situation seamlessly. Risk based leadership needs to also be linked with evolving technology and processes that can enhance the leader's decision-making ability and adaptability in this ever-changing environment.

In times of 'Business as usual', businesses and leaders need to take the time to reflect and think about what are the 'known knowns' and 'known unknowns' that may affect them during a crisis and not be taken by surprise time and time again by similar events. The difficulty is that during 'Business as usual', it is difficult to get people attention to focus on a potential risk or crisis that may affect them in the future. It is often difficult to gain Executive support for the release of funds to undertake exercises that will enhance leadership skills as there are no visible risks during this period of time. Therefore, why should funds be allocated to a nonexistent risk.

Agencies and businesses should know the nature of the risks (present and future) that may confront them. They should firstly plan and exercise for these 'known knowns'. This is the simplest type of risk to plan for and yet businesses continue to make the same mistakes and be taken by surprise. You should know these risks and therefore be able to measure and qualify those risks[12]. Today however, businesses and leaders are faced with constant uncertainty and as such there are many 'known unknowns'. If leaders prepare correctly, they can identify many of the 'known unknowns' and have plans to deal with them. These are actually predictable events; you just don't know when or where they will occur or you may not have all of the information.[13] We should be aware of the gaps in our knowledge and understanding, not continually surprised by these events. This is best demonstrated in Figure 2 below. For the model or business to improve or better prepare themselves for the future, they need to make the 'unknown unknowns' into 'known knowns'. This is best commenced through working out your 'known unknowns' and stepping through the process. Some businesses embrace this progressive thinking, many others are too concerned with the daily running of their business to consider events that haven't yet occurred.

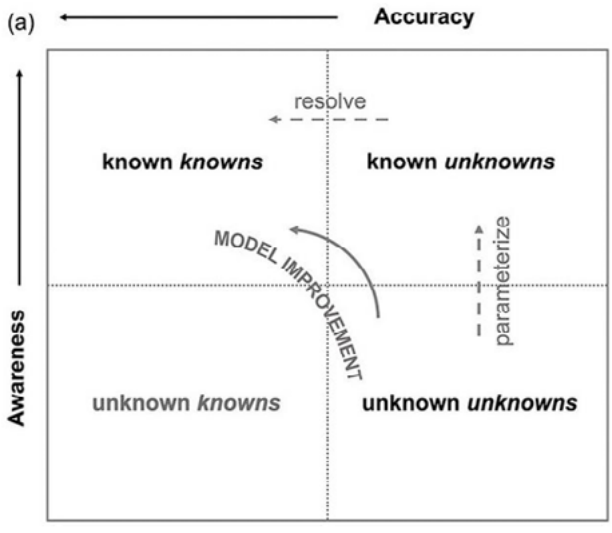
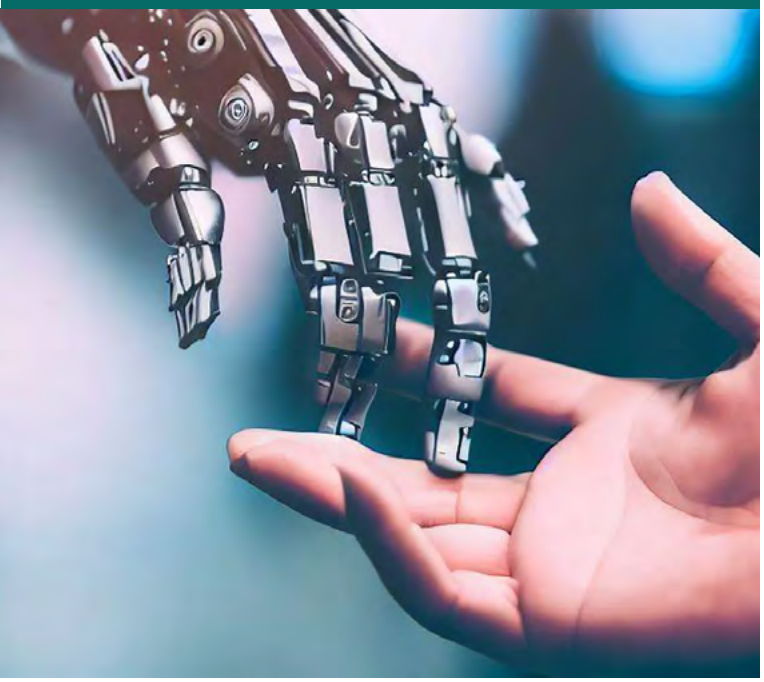


Figure 2: The Rumsfeld Matrix[14]

We should be aware of the gaps in our knowledge and understanding, not continually surprised by these events.



So, what are some of the known unknows?

- **Climate change** (Severity of events, closer together)
- **Emerging global threats** (cyber security and terrorism in its different forms)
- **Impact of social media** (all forms of instant news and opinions)
- **Artificial intelligence** (skills and interactions within the workforce)
- **Changing work practices** (historical practices no longer acceptable; remote working).

In a crisis, leadership needs a combination of clear communication, decisive action and empathy. Leaders are looked to for reassurance and guidance, and they need to provide the direction to the team. However, they also need to understand and be sensitive to the needs of the communities. The question must be asked, how does an adaptive leader operate in the environment of 'Political correctness' which is behaviour that avoids offending marginalised or vulnerable groups[15].

In an emergency there may be a need to use direct language to communicate the urgency of the situation even if the language is not perfectly politically correct[16]. However, we would stress that it is possible to communicate clearly and effectively without using language that could be viewed as discriminatory.

Communities are now very well informed and demand that agencies are held to account for their actions during a crisis. Therefore, it stands to reason that leaders will also be held to account through Inquiries, Royal Commissions or the Coroners Court.

Leaders should not be terrified by the prospect of being held accountable. Instead, leaders should constantly exercise their leadership skills in different situations, collaboratively working across agencies to identify other individuals of high calibre that are willing to adapt to changing environments. Building up a resilience and maturity to accept that a constantly changing environment will occur and the need to prepare yourselves to operate in such an environment. Learn the ability to change direction as more information is available on a situation. It isn't admitting defeat or a mistake, it shows a maturity of learning and leadership that on the available information at that time the decision was made it was a good decision. Now new information is available so the decision/s can change. It is not about blame; it is about achieving the most positive outcome for the community that we serve.

None of this is new, but until we develop individuals, teams and organisations that are willing to embrace the fact that they operate in a changing risk environment, that have the capability and willingness to learn from others and adapt, we will continue to undertake the same tasks the same way and achieve the same results. The community however will no longer accept that leadership model.

8. https://www.oecd.org/coronavirus/policy-responses/building-back-better-a-sustainable-resilient-recoveryafter-covid-19-52b869f5/
9. Miller, P and Dalglish C. The Leader in You. Developing your leadership potential (2011)
10. Mitchell, M and Casey J. Police Leadership and management (2007)
11. University of Florida https://leadership.hr.ufl.edu/wp-content/uploads/sites/15/2019/02/ConsensusDecision-Making.pdf
12. Management Study Guide https://www.managementstudyguide.com/known-unknown-classification-ofrisk.htm
13. https://www.forbes.com/sites/forbesbooksauthors/2021/06/21/managing-known-and-unknownunknowns/?sh=4dfab769d02e
14. The Rumsfeld Matrix – Degrees of knowledge. https://www.cambridge.org/core/books/abs/climatedemon/rumsfeld-matrix/7AAED1029A4F13B0467FF7E9165B9A90
15. Wooten, S.L. The Importance of Communication During a Crisis (2018) 16 Lind, W. Political Correctness. A Short History of an Ideology (2017)

AUTHOR BIOS

DAVE OWENS

Risk-e Business was founded by David in 2012 as an Executive Level Consultancy Service after leaving the NSWPF at the Rank of Deputy Commissioner after over 30 years' service.

David held the position of State Emergency Operations Controller and oversighted APEC Leaders week, World Youth Day, Christchurch Earthquake, Japanese Tsunami and the United Nations USAR accreditation in Turkey. In the private sector for the last 12 years, he chaired the NSW Government Loose Fill Asbestos Taskforce, NSW Independent Bushire Inquiry and rewrote the Hawkesbury Nepean Valley Flood Plan.

David was Chair of the Westpac Rescue Board (6 years); Ambulance NSW Board (current) and the NSW Reconstruction Authority Advisory Board (current). David was a professor/lecturer Rabdan Academy UAE (2012-23) & the National Centre for Emergency Management studies. In 2023 David was the Risk Management Institute of Australasia Consultant of the Year.

Qualifications:

2012 Masters of Emergency Management Charles Sturt University

2011 Masters of Leadership and Business Charles Sturt University

2009 National Executive Institute Session XXXIV, Federal Bureau of Investigation

1998 Diploma in Criminology

DAVID DONOHUE APM

David has smoothly transitioned from the NSW Police after over 30 years of Service and 4 years in the private sector. David held Commander positions for over 13 years.

David was a Board Director at Westpac Life Saving Rescue Helicopter Service, leading them through a complete restructure of service provision and implementation of a new operating model. David has undertaken Gateway Reviews for the WA Government for the 2012 Commonwealth Heads of Govt and in 2016 WAPOL Optimisation Program. During a career break, David was the Security & Risk Manager for DHL, Oceania and the Loss Prevention and Investigations Manager for Qantas.

David joined Risk-e Business as a business partner in 2022. David has a passion for innovation and combining risk and emergency management practices to ensure the communities safety.

Qualifications:

2012 Masters of Emergency Management Charles Sturt University

2011 Masters of Leadership and Business Charles Sturt University

THE WICKED PROBLEM OF WVA: EXPLORING THE LITERATURE AND LANDSCAPE OF WORKPLACE VIOLENCE AND AGGRESSION IN HEALTHCARE

BY KALLAN GRIFFIN

INTRODUCTION

In the sanctuaries of healthcare, where compassion and healing intertwine, a wicked problem lurks beneath the surface: workplace violence and aggression (WVA). This menacing issue, acknowledged as a global concern, significantly impacts the daily operations of healthcare workers, patients, and visitors, inflicting not just physical harm but psychological trauma as well. The reverberations of WVA penetrate the very core of the healthcare system, exacerbating staff burnout, diminishing job satisfaction, obstructing staff retention, and ultimately, compromising the quality of patient care.

WVA is a complex and multifaceted enigma, encompassing a broad spectrum of actions and behaviours that pose significant risks to the health and safety of those in its path. This encompasses both verbal and non-verbal, physical and non-physical acts, whether intended or accidental, inflicting physical or psychological harm on those directly involved or witnessing such behaviour. The prevalence of WVA in healthcare settings originates from its intricate complexity and the interplay among numerous stakeholders and contributing factors across the health system, with only a limited number of these stakeholders having formal decision-making authority to counter or manage WVA.

This essay will explore the labyrinth of WVA, highlighting the necessity of a holistic and collaborative approach that empowers all stakeholders to contribute to prevention and management efforts. It is argued that the key to effectively mitigating WVA lies in systemic reform, calling for the development of a system-wide risk profile that encompasses operational, project, program, strategic, infrastructural, and workplace health and safety risks. By synthesizing these factors into a unified risk overview, we aim to pave the way for a series of targeted interventions that foster a safer, more harmonious healthcare environment for all.

"The reverberations of WVA penetrate the very core of the healthcare system, exacerbating staff burnout, diminishing job satisfaction, obstructing staff retention, and ultimately, compromising the quality of patient care."

"It is argued that the key to effectively mitigating WVA lies in systemic reform, calling for the development of a system-wide risk profile that encompasses operational, project, program, strategic, infrastructural, and workplace health and safety risks."

"This call to action is not merely a professional obligation, but a moral imperative for those vested in the sanctity of human well-being."

CONTENT

The complexity of this wicked problem is underscored when simply attempting to define it. WVA is a globally recognised issue, extensively researched by the international community. However, definitions of WVA vary, reflecting the scope of the research undertaken (Lanctôt and Guay, 2014). To facilitate a better understanding of the spectrum of challenges being addressed, the World Health Organisation (WHO) recommends a workplace violence definition is designed and adapted for local-level use, effectively capturing the issues faced by staff within a particular health service (Krug et al., 2002, Wiskow, 2003).

Description of the Wicked Problem

Focusing on Western Australia's health system, this essay considers the workplaces and the individuals within them, including staff members, patients, and visitors. The current Department of Health (DoH) definition for WVA does not encapsulate the complexities of the issue fully (Department of Health, 2021). It leans on outdated standards, omits essential legislation, and appears to be formed in the absence of a literature review. Consequently, it has been considered but not used as the primary definition in this essay.

For the purpose of this essay, workplace violence and aggression (WVA) is defined as;

"any action, behaviour, or incident occurring within any Western Australian (WA) health system workplace, including all healthcare environments and settings, where a staff member, patient, or any other individual associated with the service provision is subjected to acts of abuse, threats, assault, or harm in circumstances arising out of, or in the course of their work or interaction with the health services." (Griffin, 2023, Appendix A, p. 11).

The urgency of addressing WVA becomes apparent when considering its proportionality, having reached epidemic immensity (Adeniyi and Puzi, 2021). Its prevalence is terrifying, with a staggering 98% of emergency department (ED) staff admitting to experiencing some form in their workplaces (Cabilan and Johnston, 2019). This problem is not limited to international contexts as evidenced by the nearly 10,000 Code Blacks – urgent calls for security assistance to a violent emergency – reported in the Perth metropolitan area (Muir-Cochrane et al., 2020, O'Leary, 2019).

Delving deeper into the problem, the complexity of WVA is diverse and multi-factorial, making it a 'wicked' problem (Rittel and Webber, 1973). The multifactorial nature of the problem is magnified by the diverse stakeholders involved and the multiple layers of the healthcare system that influence the issue (Ramacciati et al., 2018). Staff faced with patients battling mental health issues, substance abuse, or cognitive impairments such as delirium and dementia often instigate such violence (Ferri et al., 2020, Nikathil et al., 2018, Wong et al., 2019). However, the problem extends beyond individual patient characteristics, intertwining with broader systemic issues.

This complexity is further amplified by the diversity of stakeholders involved, compounded by the lack of clear decision-making authority among them. This group includes healthcare workers, management, security personnel, patients, and their families or advocates, each bringing unique perspectives and interests (Gadegaard et al., 2018, Manier et al., 2017a). The ripple effects of WVA extend beyond immediate physical injuries, reaching into realms of psychological trauma, job satisfaction, staff retention, and the quality of patient care (Cranage and Foster, 2022,

Schablon et al., 2022). These profound impacts underline the urgent need for effective interventions to safeguard healthcare workers and ensure the continued delivery of high-quality patient care. This call to action is not merely a professional obligation, but a moral imperative for those vested in the sanctity of human well-being (Hassard et al., 2019).

Suggested Solutions to the Wicked Problem

In the quest to eradicate the pervasive issue of WVA within healthcare settings, the path is paved with multifarious and robust solutions. A wealth of resources currently exist, their core aim being the prevention and management of WVA. Nevertheless, the escalating frequency of WVA incidents casts a disheartening shadow, indicating that management, rather than prevention, is often the primary outcome (Raveel and Schoenmakers, 2019).

The systematic and scoping reviews of Morphet et al. (2018), Raveel and Schoenmakers (2019), Spelten et al. (2020) and Somani et al. (2021) serve as invaluable navigational tools, shedding light on the multifaceted approaches undertaken to combat this issue. Each offers a unique lens through which to examine the issue: Morphet et al. (2018) focus on policy recommendations, Raveel and Schoenmakers (2019) explore technological solutions, Spelten et al. (2020) consider the efficacy of staff training programs, and Somani et al. (2021) investigate the effectiveness of various security measures. This wealth of literature provides an intricate map of proposed interventions, enabling us to delve deep into their respective merits, limitations, and potential side effects.

Empowering healthcare workers with knowledge and skills to manage aggressive situations is critical as Somani et al. (2021) has identified. Training and education can enhance staff awareness and confidence, honing their abilities to de-escalate conflicts and communicate effectively. However, as Raveel and Schoenmakers (2019) point out, such initiatives often fall short of addressing fundamental safety concerns, sometimes placing the burden of managing WVA on staff instead of organisations. As a result, training may only impact discrete elements of WVA and, by itself, prove ineffective in preventing violence, increasing pressure on staff to manage these situations (Tyler et al., 2022).

Organisational interventions, such as the formulation of effective policies and the promotion of incident reporting, can foster an environment that prioritises staff (Beattie et al., 2020, Gadegaard et al., 2018, Mitra et al., 2018). However, the success of these measures hinges on management commitment and may be impeded by resistance to change, resource constraints, or a lack of awareness. Ineffective policies such as zero tolerance may inadvertently normalise violence, leaving staff feeling exposed and unsupported (Tyler et al., 2022).

Morphet et al. (2018) emphasises the importance of well-designed building layouts and security measures in creating safe environments for healthcare workers. Increased visibility and reduced hazards, achieved through proper lighting, clear sightlines, and signage, can help minimise risks. Physical barriers and controlled access points offer additional security and separation between staff and potential aggressors. However, these measures can also create impersonal, restrictive environments, potentially impacting doctor-patient relationships and care quality. The implementation of extensive security measures can be costly and resource-intensive, and balancing safety with privacy and confidentiality remains a challenge (Raveel and Schoenmakers, 2019).

The Trauma-Informed Care approach, encapsulating a holistic viewpoint, emphasises empowerment, collaboration, safety, trust-building, and cultural sensitivity (Beattie et al., 2019). This compassionate approach acknowledges the impact of trauma on individuals and prioritises their well-being. However, implementing trauma-informed care can be resource-intensive, requiring staff training, funding, and time (Gerdtz et al., 2020). Moreover, integration into existing systems can prove challenging, potentially facing resistance or logistical hurdles. A lack of standardisation further complicates matters, possibly leading to inconsistencies in care delivery (Davids et al., 2021).

The risk management approach offers several merits in organisational contexts. Firstly, it enables the identification and assessment of potential risks, promoting a proactive stance towards risk prevention and mitigation (O'Rourke et al., 2018). This approach facilitates informed decision-making by providing a systematic framework for evaluating risks and implementing appropriate mitigation strategies. Additionally, risk management contributes to enhancing overall organisational safety and resilience, as it fosters a culture of risk awareness and response readiness (Morphet et al., 2018, Spelten et al., 2020).

Effective risk management in healthcare services holds the potential to significantly reduce workplace violence and aggression (WVA) incidents. By employing reliable risk assessment tools, staff can proactively identify potential patient risk factors, preventing situations from escalating into violence (Cabilan and Johnston, 2019). This proactive approach has been exemplified by the successful redesign of responses to aggression and violence in emergency departments (Senz et al., 2021).

Davids et al. (2021) and Senz et al. (2021) emphasise the importance of innovating responses and mitigating aggression in emergency settings, while acknowledging the necessity of adequate resources for successful implementation. Cabilan et al. (2023) further underscores the value of effective risk assessment tools and comprehensive staff training. Despite these promising outcomes, the implementation and sustainability of such initiatives may be constrained by resource limitations, particularly in financially challenged healthcare settings (Cabilan, 2023).

The literature of D'Ettorre et al. (2018), Davids et al. (2021), Gerdtz et al. (2020), Hamblin et al. (2017), Karanikas et al. (2022), Somani et al. (2021), Wirth et al. (2021) casts a glaring light on the requirement for system reform through a multifaceted approach to address the daily challenges healthcare staff confront. This revelation necessitates corrective action be undertaken by the key stakeholders, united in a collaborative crusade to eradicate WVA from healthcare settings.

Collaborative Approach and Recommendations for Future Practice

Salmon et al. (2022) demonstrates that WVA in healthcare settings, being a 'wicked problem,' resists linear, one-dimensional solutions. Identified through a systems thinking approach and acknowledging the intricate interplay of various elements across multiple levels in the hospital system. Collaboration lies at the heart of this perspective, fostering the essential connections across these levels, facilitating shared understanding, and driving collective action.

The importance of a collaborative approach in solving wicked problems such as WVA lies in its capacity to bring together diverse perspectives and expertise (Sheppard et al., 2022). Collaboration brings together the vast resources and stakeholders in a multidimensional engagement, consolidating all efforts and approaches into a singular holistic approach (Ford et al., 2010). By pooling knowledge, expertise, and perspectives, collaboration enhances efficiency and enables a preventative approach to WVA. It fosters the development of innovative and comprehensive strategies that harmoniously work in collaboration with each other, amplifying their impact and effectiveness (Hayward et al., 2022).

Salmon et al. (2022) recommends that to address WVA in healthcare, the establishment of collaborative platforms is instrumental. An independent, multi-agency collaboration group can serve as a hub for the consolidation of resources, including physical, financial, and structural, ensuring optimal efficiency in the prevention and management of WVA. This platform fosters better communication and coordination across stakeholders, breaking down silos and contributing to a wider cultural change (Solomon, 2019).

It creates an environment where healthcare organisations, regulatory bodies, law enforcement agencies, and community stakeholders join forces, uniting their efforts to combat WVA. This collective synergy has the potential to generate innovative strategies that effectively address WVA in healthcare, promising a brighter and safer future for all (Parker et al., 2023, Salmon et al., 2022, Solomon, 2019).

Based on the literature and careful analysis, several recommendations can guide future practice in eradicating WVA. Organisational leadership plays a critical role in shaping workplace and organisational culture, safety climate, and reporting culture (Manier et al., 2017b). Prioritising the creation of a safety and reporting culture within healthcare organisations is essential (Campbell et al., 2015, Karanikas et al., 2022). Management and leaders at all levels must foster an environment where workers are confident that their health and safety are paramount. Encouraging the reporting of incidents of WVA and providing information to management leads to positive change and continuous improvement. (Sheppard et al., 2022, Tyler et al., 2022, Campbell et al., 2015).

Innovative responses and the mitigation of aggression can be achieved through the use of risk assessment tools and comprehensive staff training. Instituting a uniform organisational response within healthcare workplaces that recognises patients' and consumers' triggers empowers staff to intervene during the initial stages of escalation,

effectively preventing situations from escalating into violent or aggressive incidents (Senz et al., 2021, Davids et al., 2021, Cabilan et al., 2023, Cabilan, 2023). By embedding a model of care that encapsulates a holistic viewpoint, healthcare organizations emphasise empowerment, collaboration, safety, trust-building, and cultural sensitivity. Such an approach fosters a healing environment where all individuals, including patients, professionals, and support staff, are treated with dignity and respect (Ward-Stockham et al., 2022, Beattie et al., 2019).

Implementing these recommendations holds the potential to revolutionise healthcare practice, creating a more supportive and conducive environment for healthcare professionals, ultimately enhancing the quality of patient care (Davids et al., 2021). Healthier work environments have been linked to improved job satisfaction, reduced turnover rates, and better patient outcomes (Itzhaki et al., 2018). The collaborative approach aligns well with the broader paradigm shift in healthcare towards patient-centred and integrated care (Ward-Stockham et al., 2022). Recognising healthcare as a complex system where the contributions of various stakeholders are intricately linked (Sheppard et al., 2022). Input from frontline healthcare staff, who face the brunt of WVA issues, is imperative for the effective and sustainable implementation of these recommendations. In this way, addressing WVA can serve as a model for tackling other complex problems in healthcare, promoting a culture of collaboration and collective action (Spelten et al., 2022).

However, it is important to note that implementing these recommendations will require a significant shift in mindset and practice (Karanikas et al., 2022). It will necessitate strong leadership, commitment to continuous learning and improvement, and, above all, a willingness to embrace the complexity of the issue. As Salmon et al. (2022) has shown, WVA is a systemic problem, and addressing it effectively will require a systemic solution (Mayhew and Chappell, 2007, Hamblin et al., 2017).

Conclusion

In conclusion, the challenge of eradicating WVA against healthcare workers presents a wicked problem—multifaceted and formidable in its complexity. Nevertheless, it is an imperative that cannot be sidestepped. By employing a collaborative ethos and systems-thinking methodology, healthcare institutions can begin to disentangle the diverse variables contributing to this pernicious issue. The trajectory ahead necessitates a transformational paradigm shift within healthcare systems, centring on a culture imbued with safety, respect, and dignity for all. While this transition is unquestionably arduous, it remains essential to cultivating a safer, more compassionate environment for healthcare providers and patients alike.

Healthcare professionals carry the solemn responsibility of ensuring the well-being of their patients. Yet, this obligation cannot be optimally fulfilled unless the safety and dignity of healthcare providers are likewise assured. Combating WVA is not solely a professional duty; it is a moral exigency. In response, legislators must enact robust protective policies, healthcare organisations put forth comprehensive safety processes, and academic researchers must delve deeper into both the root causes and systemic factors to identify viable solutions. Although the extermination of WVA is improbable, it is a dilemma that can—and must—be confronted. This essay convincingly illustrates that the knowledge, the tools, and the collective will to enact change do exist.

The window of opportunity is now open. A cohesive stance is crucial for fostering a safer and more empathetic healthcare setting for all stakeholders. It is the opportune moment to translate this collective will into tangible, corrective measures that will secure the safety and well-being of colleagues, patients, and healthcare professionals. The time for action is unequivocally now.

References

2016. Occupational Violence Prevention in Queensland Health's Hospital and Health Services. In: HEALTH, Q. (ed.) Taskforce Report. Government, Queensland.

2017. Prevention and management of violence and aggression in health services. In: VICTORIA, W. (ed.) Information for employers. Government, Victoria.

2020. Work Health and Safety Act. In: AUSTRALIA, P. O. W. (ed.). Australia.

2021. Workplace Aggression and Violence Policy. In: HEALTH, D. O. (ed.).

2022. Mutual expectations. For consumers, healthcare staff, students and volunteers. Government, Australian Capital Territory.

ADENIYI, O. V. & PUZI, N. 2021. Management approach of patients with violent and aggressive behaviour in a district hospital setting in South Africa. 2021.

AUSTRALIA, S. 2023. Workplace Violence and Aggression Overview [Online]. Available: https://www.safeworkaustralia.gov.au/safety-topic/hazards/workplace-violence-and-aggression/overview [Accessed].

BEATTIE, J., GRIFFITHS, D., INNES, K. & MORPHET, J. 2019. Workplace violence perpetrated by clients of health care: A need for safety and trauma-informed care. Journal of clinical nursing, 28, 116-124.

BEATTIE, J., INNES, K., GRIFFITHS, D. & MORPHET, J. 2020. Workplace violence: Examination of the tensions between duty of care, worker safety, and zero tolerance. Health Care Management Review, 45, E13-E22.

BOYLE, M. J. & WALLIS, J. 2016. Working towards a definition for workplace violence actions in the health sector. Safety in Health, 2.

CABILAN, C. & JOHNSTON, A. N. 2019. Review article: Identifying occupational violence patient risk factors and risk assessment tools in the emergency department: A scoping review. Emergency Medicine Australasia, 31, 730-740.

CABILAN, C. J. 2023. The development, implementation, and evaluation of a digital occupational violence patient risk assessment tool in the emergency department. Doctor of Philosophy, The University of Queensland.

CABILAN, C. J., ELEY, R., SNOSWELL, C., JONES, A. T. & JOHNSTON, A. N. B. 2023. Inter-rater reliability of the occupational violence risk assessment tool for emergency departments. Australas Emerg Care, 26, 54-58.

CAMPBELL, C. L., BURG, M. A. & GAMMONLEY, D. 2015. Measures for incident reporting of patient violence and aggression towards healthcare providers: A systematic review. Aggression and Violent Behavior, 25, 314-322.

CHOWDHURY, S. R., KABIR, H., DAS, D. C., CHOWDHURY, M. R., CHOWDHURY, M. R. & HOSSAIN, A. 2022. Workplace violence against Bangladeshi registered nurses: A survey following a year of the COVID-19 pandemic. International nursing review.

CRANAGE, K. & FOSTER, K. 2022. Mental health nurses' experience of challenging workplace situations: A qualitative descriptive study. International Journal of Mental Health Nursing, 31, 665-676.

CREDLAND, N. J. & WHITFIELD, C. 2022. Incidence and impact of incivility in paramedicine: a qualitative study. Emergency medicine journal : EMJ, 39, 52-56.

D'ETTORRE, G., PELLICANI, V., MAZZOTTA, M. & VULLO, A. 2018. Preventing and managing workplace violence against healthcare workers in Emergency Departments. Acta Biomed, 89, 28-36.

DAVIDS, J., MURPHY, M., MOORE, N., WAND, T. & BROWN, M. 2021. Exploring staff experiences: A case for redesigning the response to aggression and violence in the emergency department. Int Emerg Nurs, 57, 101017.

FERRI, F., GRIFONI, P. & GUZZO, T. 2020. Online Learning and Emergency Remote Teaching: Opportunities and Challenges in Emergency Situations. Societies, 10, 86.

FORD, K., BYRT, R. & DOOHER, J. 2010. Preventing and reducing aggression and violence in health and social care: a holistic approach, M&K Update Ltd.

GADEGAARD, C. A., ANDERSEN, L. P. & HOGH, A. 2018. Effects of Violence Prevention Behavior on Exposure to Workplace Violence and Threats: A Follow-Up Study. Journal of Interpersonal Violence, 33, 1096-1117.

GERDTZ, M., DANIEL, C., JARDEN, R. & KAPP, S. 2020. Use of the Safewards Model in healthcare services: a mixed-method scoping review protocol. BMJ Open, 10, e039109.

HAMBLIN, L. E., ESSENMACHER, L., LUBORSKY, M., RUSSELL, J., JANISSE, J., UPFAL, M. & ARNETZ, J. 2017. Worksite Walkthrough Intervention. Journal of Occupational & Environmental Medicine, 59, 875-884.

HASSARD, J., TEOH, K. R. H. & COX, T. 2019. Estimating the economic burden posed by work-related violence to society: A systematic review of cost-of-illness studies. Safety Science, 116, 208-221.

HAYWARD, S., VAN LOPIK, K. & WEST, A. 2022. A holistic approach to health and safety monitoring: Framework and technology perspective. Internet of Things, 20.

HERSHCOVIS, M. S. 2011. "Incivility, social undermining, bullying…oh my!": A call to reconcile constructs within workplace aggression research. Journal of Organizational Behavior, 32, 499-519.

HERSHCOVIS, M. S. & BARLING, J. 2010. Towards a multi-foci approach to workplace aggression: A meta-analytic review of outcomes from different perpetrators. Journal of Organizational Behavior, 31, 24-44.

HERSHCOVIS, M. S., TURNER, N., BARLING, J., ARNOLD, K. A., DUPRÉ, K. E., INNESS, M., LEBLANC, M. M. & SIVANATHAN, N. 2007. Predicting workplace aggression: a meta-analysis. Journal of applied Psychology, 92, 228.

ITZHAKI, M., BLUVSTEIN, I., PELES BORTZ, A., KOSTISTKY, H., BAR NOY, D., FILSHTINSKY, V. & THEILLA, M. 2018. Mental Health Nurse's Exposure to Workplace Violence Leads to Job Stress, Which Leads to Reduced Professional Quality of Life. Frontiers in Psychiatry, 9.

KARANIKAS, N., KHAN, S. R., BAKER, P. R. A. & PILBEAM, C. 2022. Designing safety interventions for specific contexts: Results from a literature review. Safety Science, 156, 105906.

KRUG, E. G., MERCY, J. A., DAHLBERG, L. L. & ZWI, A. B. 2002. The world report on violence and health. The Lancet, 360, 1083-1088.

LANCTÔT, N. & GUAY, S. 2014. The aftermath of workplace violence among healthcare workers: A systematic literature review of the consequences. Aggression and violent behavior, 19, 492-501.

MANIER, A. O., KELLOWAY, E. K. & FRANCIS, L. 2017a. Damaging the Workplace: Consequences for People and Organizations. In:

HERSHCOVIS, M. S. & BOWLING, N. A. (eds.) Research and Theory on Workplace Aggression. Cambridge: Cambridge University Press

MANIER, A. O., KELLOWAY, E. K. & FRANCIS, L. 2017b. Damaging the workplace: Consequences for people and organizations.

MAYHEW, C. & CHAPPELL, D. 2007. Workplace violence: An overview of patterns of risk and the emotional/stress consequences on targets. International Journal of Law and Psychiatry, 30, 327-339.

MENTO, C., SILVESTRI, M. C., BRUNO, A., MUSCATELLO, M. R. A., CEDRO, C., PANDOLFO, G. & ZOCCALI, R. A. 2020. Workplace violence against healthcare professionals: A systematic review. Aggression and violent behavior, 51, 1-8.

MITRA, B., NIKATHIL, S., GOCENTAS, R., SYMONS, E., O'REILLY, G. & OLAUSSEN, A. 2018. Security interventions for workplace violence in the emergency department. Emergency Medicine Australasia, 30, 802-807.

MORPHET, J., GRIFFITHS, D., BEATTIE, J., VELASQUEZ REYES, D. & INNES, K. 2018. Prevention and management of occupational violence and aggression in healthcare: A scoping review. Collegian, 25, 621-632.

MUIR-COCHRANE, E., MULLER, A., FU, Y. & OSTER, C. 2020. Role of security guards in Code Black events in medical and surgical settings: A retrospective chart audit. Nursing & Health Sciences, 22, 758-768.

NIELSEN, M. B., MATTHIESEN, S. B. & EINARSEN, S. 2010. The impact of methodological moderators on prevalence rates of workplace bullying. A meta-analysis. Journal of Occupational and Organizational Psychology, 83, 955-979.

NIKATHIL, S., OLAUSSEN, A., SYMONS, E., GOCENTAS, R., O'REILLY, G. & MITRA, B. 2018. Increasing workplace violence in an Australian adult emergency department. Emergency Medicine Australasia, 30, 181-186.

O'LEARY, C. 2019. Nearly 10,000 code blacks reported at Perth hospitals as emergency staff cop thuggery. The West Australian [Online]. Available: https://thewest.com.au/news/health/nearly-10000-code-blacks-reported-at-perth-hospitals-as-emergency-staff-cop-thuggery-ng-b881097074z#:~:text=Nearly%2010%2C000%20code%20blacks%20reported%20at%20Perth%20hospitals%20as%20emergency%20staff%20cop%20thuggery,-Cathy%20O%27Leary&text=Almost%2010%2C000%20code%20blacks%20were,done%20to%20combat%20violent%20behaviour.

O'ROURKE, M., WRIGLEY, C. & HAMMOND, S. 2018. Violence within mental health services: how to enhance risk management. Risk Management and Healthcare Policy, Volume 11, 159-167.

PARKER, S., HARTLEY, J., BEASHEL, J. & VO, Q. 2023. Leading for public value in multi-agency collaboration. Public Policy and Administration, 38, 83-106.

RAMACCIATI, N., CECCAGNOLI, A., ADDEY, B., LUMINI, E. & RASERO, L. 2018. Violence towards emergency nurses: A narrative review of theories and frameworks. Int Emerg Nurs, 39, 2-12.

RAVEEL, A. & SCHOENMAKERS, B. 2019. Interventions to prevent aggression against doctors: a systematic review. BMJ Open, 9, e028465.

RITTEL, H. W. & WEBBER, M. M. 1973. Dilemmas in a general theory of planning. Policy sciences, 4, 155-169.

SALMON, P. M., COVENTON, L. & READ, G. J. M. 2022. A systems analysis of work-related violence in hospitals: Stakeholders, contributory factors, and leverage points. Safety Science, 156.

SCHABLON, A., KERSTEN, J. F., NIENHAUS, A., KOTTKAMP, H. W., SCHNIEDER, W., ULLRICH, G., SCHÄFER, K., RITZENHÖFER, L., PETERS, C. & WIRTH, T. 2022. Risk of Burnout among Emergency Department Staff as a Result of Violence and Aggression from Patients and Their Relatives. International Journal of Environmental Research and Public Health, 19, 4945.

SENZ, A., ILARDA, E., KLIM, S. & KELLY, A. M. 2021. Development, implementation and evaluation of a process to recognise and reduce aggression and violence in an Australian emergency department. Emergency Medicine Australasia, 33, 665-671.

SHEPPARD, D. M., NEWNAM, S., LOUIS, R. M. S. & PERRETT, M. S. 2022. Factors contributing to work-related violence: A systematic review and systems perspective. Safety science, 154, 105859.

SOLOMON, M. 2019. Becoming comfortable with chaos: making collaborative multi-agency working work. Emotional and Behavioural Difficulties, 24, 391-404.

SOMANI, R., MUNTANER, C., HILLAN, E., VELONIS, A. J. & SMITH, P. 2021. A Systematic Review: Effectiveness of Interventions to De-escalate Workplace Violence against Nurses in Healthcare Settings. Safety and Health at Work, 12, 289-295.

SPELTEN, E., THOMAS, B., O'MEARA, P. F., MAGUIRE, B. J., FITZGERALD, D. & BEGG, S. J. 2020. Organisational interventions for preventing and minimising aggression directed towards healthcare workers by patients and patient advocates. Cochrane Database of Systematic Reviews.

SPELTEN, E., VAN VUUREN, J., O'MEARA, P., THOMAS, B., GRENIER, M., FERRON, R., HELMER, J. & AGARWAL, G. 2022. Workplace violence against emergency health care workers: What Strategies do Workers use? BMC Emergency Medicine, 22.

STAFFORD, S., AVSAR, P., NUGENT, L., O'CONNOR, T., MOORE, Z., PATTON, D. & WATSON, C. 2022. What is the impact of patient violence in the emergency department on emergency nurses' intention to leave? Journal of nursing management, 30, 1852-1860.

TYLER, V., AGGAR, C., GRACE, S. & DORAN, F. 2022. Nurses and midwives reporting of workplace violence and aggression: an integrative review. Contemporary Nurse, 58, 113-124.

WARD-STOCKHAM, K., KAPP, S., JARDEN, R., GERDTZ, M. & DANIEL, C. 2022. Effect of Safewards on reducing conflict and containment and the experiences of staff and consumers: A mixed-methods systematic review. International Journal of Mental Health Nursing, 31, 199-221.

WIRTH, T., PETERS, C., NIENHAUS, A. & SCHABLON, A. 2021. Interventions for Workplace Violence Prevention in Emergency Departments: A Systematic Review. International Journal of Environmental Research and Public Health, 18, 8459.

WISKOW, C. 2003. Guidelines on workplace violence in the health sector. World Health Organization/International Labour Office, 40.

WONG, A. H., RAY, J. M. & IENNACO, J. D. 2019. Workplace Violence in Health Care and Agitation Management: Safety for Patients and Health Care Professionals Are Two Sides of the Same Coin. The Joint Commission Journal on Quality and Patient Safety, 45, 71-73.

APPENDIX A

Definition of Workplace Violence and Aggression

The development of a unified and comprehensive definition of Workplace Violence and Aggression (WVA) is crucial for understanding and addressing the complex nature of this issue. A clear and consistent definition is essential for the effective development of interventions, targeted prevention strategies, and accurate comparisons across different healthcare settings (Karanikas et al., 2022, Wiskow, 2003). This appendix critically evaluates existing definitions of WVA and aims to propose a comprehensive definition that enhances our understanding of the problem.

A well-researched definition of WVA not only promotes standardisation but also sheds light on the underlying causes and contributing factors of WVA. Factors such as power imbalances, organisational culture, and environmental stressors play significant roles (Salmon et al., 2022). By understanding these root causes, healthcare organisations can develop tailored, evidence-based interventions that lead to more sustainable outcomes for both the organisation and its staff (Wiskow, 2003). This comprehensive understanding forms the foundation for creating a safer and more supportive work environment within Western Australian healthcare.

Furthermore, rigorous academic inquiry into WVA contributes to the development of measurement tools and evaluation processes. These tools enable the assessment of intervention effectiveness in reducing WVA incidence and severity (Gadegaard et al., 2018). By refining the definition of WVA, we can enhance our ability to accurately measure and evaluate the impact of interventions, facilitating evidence-based decision-making and ultimately promoting a safer work environment.

Legislation, Regulation, Code and Standard

The essay focuses on workplaces within Western Australia's health system, including staff members, patients, and visitors. The current legislation, regulations, codes of practice, and standards applicable to this definition include:

The Work Health Safety Act (2020)	**8. Meaning of workplace** 1) A ***workplace*** is a place where work is carried out for a business or undertaking and includes any place where a worker goes, or is likely to be, while at work.
Work Health and Safety (General) Regulations 2022	**55. A. Meaning of psychosocial hazard** A ***psychosocial hazard*** is a hazard that — b) may cause psychological harm (whether or not it may also cause physical harm).
The Health Services Act ("Western Australian Parliament, Health Services Act 2016,")	**6. Terms used** ***employee*** means a person employed in a health service provider and includes — a) the chief executive of the health service provider; b) a health executive employed in the health service provider; c) a person employed in the health service provider under section 140; d) a person seconded to the health service provider under section 136 or 142; ***patient*** means a person who has been, is being, or will or may be provided with health treatment or care; ***staff member***, of a health service provider, means — a) an employee in the health service provider; b) a person engaged under a contract for services by the health service provider; --- **19. Management of the WA health system** 1) The WA health system is comprised of — a) the Department; and b) health service providers; and to the extent that contracted health entities provide health services to the State, the contracted health entities.

The National Safety and Quality Health Service (NSQHS) Standards	**Risk management –** 1.07 – The health service organisation uses a risk management approach to: a) Set out, review, and maintain the currency and effectiveness of policies, procedures and protocols b) Monitor and take action to improve adherence to policies, procedures and protocols c) Review compliance with legislation, regulation and jurisdictional requirements **Predicting, preventing and managing aggression and violence –** 5.33 – The health service organisation has processes to identify and mitigate situations that may precipitate aggression 5.34 – The health service organisation has processes to support collaboration with patients, carers and families to: a) Identify patients at risk of becoming aggressive or violent b) Implement de-escalation strategies c) Safely manage aggression, and minimise harm to patients, carers, families and the workforce
Department of Mines, Industry Regulation and Safety CODE OF PRACTICE: Violence and aggression at work	**Using this code of practice –** All forms of workplace violence and aggression are serious work safety and health issues which can impact on a worker's physical and psychological safety and health. **1.1 What is work-related violence and aggression?** **1.2 Who is responsible for managing violence and aggression at work?** **1.3 Who is at risk?**

Current Policy Framework

The WA Health, Department of Health (DoH) Workplace Aggression and Violence Policy Framework MP 0159/21 defines WVA as;

"workplace aggression and violence is considered to be any incident where a Staff Member is abused, threatened or assaulted in circumstances arising out of, or in the course of, their employment. Examples include, but are not limited to verbal, physical or psychological abuse, threats, spitting, biting or throwing objects." (DOH, 2021).

This definition is unique, deviating from the widely accepted term 'Workplace Violence and Aggression.' This intentional change aims to reflect the escalation sequence of events where aggression precedes violence. However, this modification is not widely recognised in literature and may create confusion when interfacing with other literature on the subject.

Additionally, 'workplace aggression' is commonly associated with workplace bullying in academic literature, potentially leading to conflation of distinct issues of violence and bullying within the workplace. Such conflation could hinder the development of targeted interventions. (Hershcovis, 2011, Hershcovis and Barling, 2010, Hershcovis et al., 2007, Nielsen et al., 2010).

To ensure consistency in communication, research, and intervention development for this essay, it is necessary to revise the policy framework's wording to align with the commonly accepted term 'Workplace Violence and Aggression.' This change will promote a more accurate understanding of the complex dynamics of WVA and facilitate the development of effective interventions.

Acts and Intentions

There are various acts of violence and aggression in healthcare settings encompassing a variety of actions and behaviours, verbal and non-verbal, physical and non-physical, each that pose a real or perceived risk to healthcare staff (Queensland Health, 2016, Government Victoria, 2017, Government, Australian Capital Territory, 2022, Australia, 2023). These actions and behaviours

are defined as bullying, verbal abuse, threat, physical abuse, sexual harassment, and sexual abuse (Boyle and Wallis, 2016).

Importantly, the intention behind an act—whether deliberate or unintentional—due to factors such as confusion or disability, can lead to physical or psychological harm to those who encounter it (either directly or indirectly). The outcomes extend beyond physical injuries, significantly impacting psychological wellbeing. Indeed, even exposure to frequent but low-level aggression can have a detrimental effect on a worker's health (Beattie et al., 2019, Chowdhury et al., 2022, Credland and Whitfield, 2022, Mento et al., 2020, Stafford et al., 2022).

Summary and Definition

From a review of the literature on workplace violence and aggression (WVA) in healthcare, particularly across the Australian Healthcare system, and considering the existing definitions offered by various international bodies, a refined and comprehensive definition can be formulated.

Workplace Violence and Aggression (WVA) is defined as:

"any action, behaviour, or incident occurring within any Western Australian (WA) health system workplace, including all healthcare environments and settings, where a staff member, patient, or any other individual associated with the service provision is subjected to acts of abuse, threats, assault, or harm in circumstances arising out of, or in the course of their work or interaction with the health services.

WVA encompasses a broad range of actions and behaviours, both physical and psychological, that create a real or perceived risk to the safety, health, and wellbeing of individuals within the healthcare setting. These actions or behaviours include but are not limited to verbal and non-verbal abuse, physical assault, sexual harassment, bullying, threat, and other hostility-related actions.

WVA is not limited to intentional acts but also includes incidents that may be unintentional due to factors such as confusion, disability, or other mitigating factors but still have the capacity to cause physical or psychological harm. The key consideration is whether the behaviour creates a risk of harm, with the outcome not limited to physical injuries but also encompassing potential psychological impact and threat to the individual's overall wellbeing."

This definition acknowledges the wide spectrum of behaviours that might represent violence and aggression, the variety of potential aggressors, and the array of settings where such incidents may occur. It underscores the possibility of both physical and psychological harm, emphasising that the implications of such incidents go beyond immediate physical injury and may encompass potential psychological distress and long-term health effects. Moreover, it signifies that the aggressor's intent is not the decisive factor in classifying an incident as an act of violence or aggression; instead, the primary concern is the risk of harm presented to the individual exposed to the behaviour.

AUTHOR BIO

KALLAN GRIFFIN

Embarking on an exciting journey within the realms of Strategic Risk Management, Security, Safety, and Leadership, my career is fuelled by a deep passion for prevention of Workplace Violence & Aggression. My aim is to cultivate work environments where safety and security are not just standards but a culture, enabling everyone to flourish.

My career path has spanned across both government and private sectors, fostering my growth as a strategic planner and an engaging team motivator. This journey has allowed me to develop comprehensive risk control strategies and provide impactful consultancy services to stakeholders. However, I consider these as foundational steps towards a future full of further learning and development.

Guided by the firm belief in the power of prevention and a culture of security, I dedicate my efforts to creating workplaces where safety is embedded into every aspect. It's about proactively managing risks and ensuring a secure atmosphere that doesn't just react to Workplace Violence & Aggression, but rather anticipates and mitigates it.

As I advance in this specialised area of Workplace Violence & Aggression—an underrepresented yet vital domain that demands strategic insight and focused expertise—I am committed to evolving it into a field that commands the respect, value, and efficacy it profoundly deserves. Drawing inspiration from multi-agency collaboration models, I actively seek partnerships with industry experts who are equally committed to developing and evolving this critical field. Together, we can innovate, break down silos, and unite our collective expertise to foster resilient, secure work environments conducive to productivity and well-being.

CONFLICTS OF INTEREST STATEMENT

The author, Kallan, is currently employed by the Western Australian Government's Department of Health service provider South Metropolitan Health Service as the Workplace Violence & Aggression Coordinator. The views and recommendations expressed in this paper are solely those of the author and do not necessarily represent the views of the South Metropolitan Health Service, Department of Health or the Government of Western Australia.

This submission is based on an assignment completed as part of the Graduate Certificate in Health Leadership at the University of Notre Dame. Although the assignment has informed the content of this paper, the research and opinions are independent of this academic program and should not be considered representative of the institution's viewpoints or objectives.

No external funding was received for the research and preparation of this paper, and there are no financial stakes or affiliations with any programs, tools, or companies that would benefit from the findings and recommendations made herein.

THE EMOTIONAL SIDE OF RISK

BY JIM LINDSAY MINSTD MPHIL BSC DIPTEACH

We are all “experts” in risk, and either spend our days making decisions about risks, or advising others how to make decisions about risks. We also have a lot of tools to help us work through what is actually a risk, how likely it is, what the impact is/will be, and what the associated consequence/s could be.

Furthermore, we have a whole range of tools to think about how we can reduce risk. What mitigations and controls can we put in place? Are existing controls working? We then present all of this information with varying degrees of complexity. I have developed complex risk matrices, used templates, and given risks and controls ratings in the form of numbers and colors. Indeed, I have also used latent variables, and regularly mention security culture and human factors as a matter of course.

I think we've all been trying to make risk analysis a “science” – or at least a rigorous process where we can apply logical and analytical thinking to our problem. But behind all of this thinking and doing lies a false assumption.

I think we've all been trying to make risk analysis a “science” – or at least a rigorous process where we can apply logical and analytical thinking to our problem. But behind all of this thinking and doing lies a false assumption.

And that assumption is that we are all the same, and can view a risk objectively. Perhaps like Spock in Star Trek, we have suppressed all of our emotions and are just applying a ruthless and objective intelligence. But clearly, we are not emotionless, and we are not on a sterile spaceship in empty space. Rather, we are made-up of messy emotions, dubious information, and often a lack of measurable facts.

Risk is an essentially emotive issue – and we need to acknowledge it, and bring it to the forefront of our thinking to help us understand our biases and indeed the very lenses through which we look at risks.

When I'm working with a new Board, I often run an exercise looking at risk appetite, and we can do it here with you even though I can't see you.

Can you please draw a line? One end of the line is where you have a low risk tolerance, the other end of the line is when you have a high tolerance to risk.

When you go on holiday, do you have everything planned? Each day with a booked activity, all the travel prebooked, all the accommodation sorted? If that is the case, then you have probably done that so that you can relax and enjoy your holiday. That means, when I ask you to put a cross on the continuum on the line, you would put the cross at the lower end of tolerance.

But if you enjoy having spontaneous holidays with a sense of freedom, then you may have only booked your flight to the country and your first night’s accommodation. Everything else becomes like a Lee Child novel, hopefully without the violence, where you are just traveling and experiencing life. You get relaxed by the open road and freedom, and the cross on your line should be at the higher end.

Now, it is important to know your risk appetite while holidaying, because if you are going on holiday with someone who is at the other end of the risk appetite, things may not go well.

This potential difference in risk appetite also makes a difference at the Board level if you have different emotional reactions to risk. The added complexity is that you don't have one emotional reaction to risk because everything depends on the context and the content. You can have very different responses with your approach to your money compared to your holidays. Do you love investing in the share market, or taking punts on currency exchange rates? Or do you really prefer just to keep your money in a conservative pension fund?

The emotional side of risk gets even more complicated as you age. There is a tendency for your risk appetite and approach to change over time.

If you are 20 and make a decision, it's unlikely that decision is going to cause people to lose their jobs, or have significant financial downsides. But if you've become CEO of a large company, suddenly a decision can have much bigger impacts and consequences. Those consequences can weigh on your emotional ability to take risks. In fact, you might have become the CEO due to your ability to make calculated decisions around risk, and only now are you finding that your former confidence has become undermined.

So, what do we do about the emotional side of risk?

Essentially, emotional responses are not wrong – they just need to be brought out so that you can see them. We don't work in a vacuum, we work with people. Risk controls, mitigations, likelihood, consequences are all words we like. And being scared, nervous or worried are valid emotions associated with risk that need to be acknowledged. Finding the right words to describe our emotional response to risks is something that is very underdeveloped.

We need to find a way to be more articulate about our emotional risk if we are to improve our understanding and conversations about risk management.

AUTHOR BIO

JIM LINDSAY

Jim Lindsay is CEO of Tracecare Limited, who supply specialised protective security advice to the New Zealand Government and other organisations. Jim is a security and governance expert who works across the Pacific. He provides advice and conducts a range of audits and reviews concerning protective security, governance and effectiveness. Jim has also presented training and key note addresses at many events. Jim has degrees from Edinburgh University, Massey University and a diploma from Waikato University. Jim Lindsay has no conflicts of interest.

Connect with Jim on LinkedIn

THE INTERPLAY BETWEEN RISK AND REGULATION IN CRITICAL INFRASTRUCTURE WITH THE INTRODUCTION OF THE SOCI ACT AND CIRMP RULES

BY KONRAD BUCZYNSKI

The SOCI Act 2018 was fully implemented in 2022, alongside its new reforms included in Part 2A of the Act—as any risk practitioner, regardless of the industries they are involved in, would surely already know.

With the regulatory landscape of the Critical Infrastructure (CI) sector changing, it brings a unique set of challenges for organisations in the industry. However, the impact of the SOCI Act and CIRMP (Critical Infrastructure Risk Management Plan) Rules is not uniform across the different CI sectors.

Let's discuss how the SOCI Act of 2018, and its associated CIRMP Rules, have affected CI providers and risk management service providers, and whether the interplay between risk and regulation benefits or hurts CI entities.

The Risk Management Landscape of Australia

There are 3 main levels of risk management in Australia. The enterprise level, the industry level, and the national/government level. Each of these levels tackles risk management in different ways, from standards and best practices at an industry level, to regulation and legislation at the government level.

So, why was the SOCI Act 2018 necessary in this context?

The question that we all have to ask here is whether the CI sector was lacking in the management of risks, affecting this sector to the point where the government had to intervene with regulations to ensure better outcomes.

The most likely answer? The complexity of the threat landscape itself brought about the need for regulation.

In Australia, CI is primarily served by the private sector, and generally speaking, the risk management initiatives within the private sector tend to be more comprehensive than the public sector.

The risk exposure of CI entities, regardless of whether they are public or private, ranges from cyber-attacks, natural disasters, supply chain disruptions, human error, and communication failures among many others.

In addition, vast amounts of individuals and organisations rely on the smooth operation of CI in any country.

The volatile nature of the risk landscape, along with the importance of CI, has prompted regulatory measures to be implemented at a national level.

The Impact of the SOCI Act on CI Providers

The truth is, most operators of an asset that is considered CI, according to the latest Security Legislation Amendment (Critical Infrastructure Protection) Act (SLACIP), are typically at a sufficiently high scale to identify the need for effective CI risk management, and to implement controls.

However, for the operators that are not up to par with the standards, the CIRMP Rules in particular provide a solid foundation to build their risk management efforts on.

One of the main reasons for the positive impact of CIRMP Rules is its focus on material risks and the insistence on analysing them in depth. This serves as an effective control baseline for the level of reduction or mitigation of risk that must be achieved for ideal outcomes.

If principles-based rules were implemented in any other way, it would most likely result in a non-uniform approach to risk management.

The principles-based outcomes of the CIRMP are based on identifying material risks, developing and implementing risk management strategies, maintaining and continuously improving the CIRMP, and reporting on it annually.

These outcomes guide the risk management practices of organisations that are serving critical infrastructure, by requiring them to take a holistic and proactive approach to risk management through the all-hazards approach—ultimately resulting in more effective risk mitigation strategies.

Essentially, the CIRMP Rules encourage organisations to conduct very detailed analyses of threats and vulnerabilities, and articulate risks consequent to these in order to drive a more comprehensive risk management approach.

Additionally, the SOCI Act and the CIRMP Rules have been seen to simplify the process of speaking to the C-Suite and getting their buy-in for implementing vital risk management procedures within CI organisations.

Insights from risk practitioners

In the case of risk management service providers and consultants (including us), there has been a huge surge in demand coinciding with the implementation of the SOCI Act and CIRMP Rules.

One common insight that we have had when working with clients in CI is that it almost came as a surprise that the impact of this legislation would require involvement all the way up to the board level.

Since the board of directors is the team that reports on the profile of the organisation in relation to the legislation, as required by the CIRMP Rules for effective governance—this involvement makes sense.

In addition, the impact and consequences of conducting risk management will most likely improve in the coming years as a result of the guidelines provided by legislation.

Is the SOCI Act a Compliance Burden?

The short answer? No.

The long answer? Let's dive in to see why it's not a compliance burden.

I personally welcome this initiative. It provides some much-needed formality, and throws weight behind the need for security risk management in critical sectors—in much the same way laws and regulations stress the importance of workplace health and safety.

The fact that the regulation has taken the right approach to developing principles-based rules rather than prescriptive ones to address the oversights of poorly designed legislation is highly valuable.

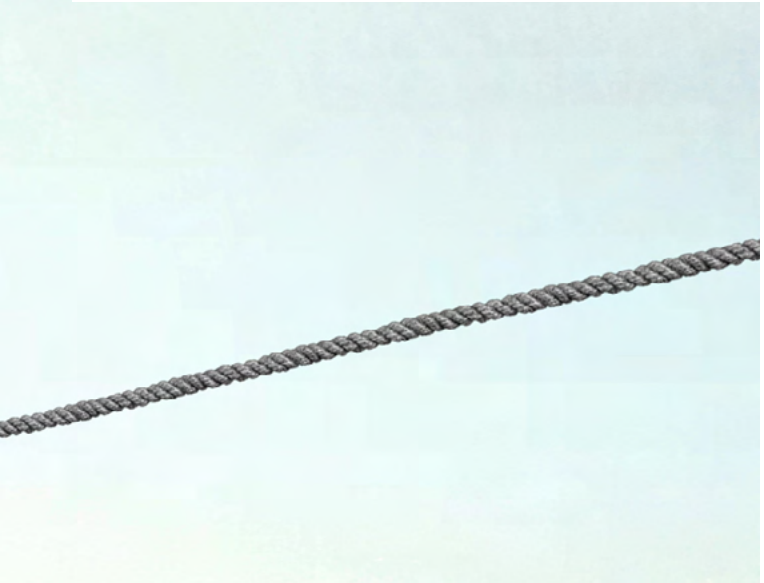
This ensures that the rules encourage growth rather than be a hindrance to businesses, which in turn is beneficial to the entire country.

The risk with legislation is usually the fact that it could create a compliance environment and culture that may not be healthy, innovative, or agile, and doesn't lend itself to business objectives. In this case, it tends to slow down and constrain, rather than grow and encourage.

However, I don't think this is the case with the SOCI Act and CIRMP Rules.

While risk management and compliance are not mutually exclusive, compliance offers a solid baseline level of controls from a risk management perspective. The rest? It's up to the individual CI providers to build upon.

One thing to kep in mind, compliance does not always ensure security.



AUTHOR BIO

KONRAD BUCZYNSKI

Konrad Buczynski holds a Master's in Risk Management and has contributed to the security risk management landscape in a variety of ways throughout his career. He served as a Director at the Australian Centre for Security Management, and the Chief Security Officer and Crisis/ Business Continuity Program Manager at Thales Australia-New Zealand, the region's largest Defence Prime Contractor at the time.

As a Committee Chair for Security Professionals Australasia (SPA) and Australian Risk Policy Institute (ARPI) Associate, he has also provided a wide range of services associated with risk management to a variety of multinational companies. He is also a member of the Australian Working Group, developing an international/ISO standard for enterprise security management.

He is currently serving as the Managing Director of SECTARA and Industry Risk, both renowned organisations in the realm of SRM in Australia and beyond.

NAVIGATING THE COMPLEXITY OF 'WICKED PROBLEMS': THE SYNERGY OF REALISM AND CONSTRUCTIVISM IN PROBLEM-SOLVING.

BY RONNIE FAULKNER

The term ‘wicked problems’ is widely used in sustainability research and various disciplines today. However, there is no consensus on its theoretical foundations or usefulness in research. The term was initially introduced in 1967 during a seminar at the University of California's Architecture Department by design professor Horst Rittel. He described wicked problems as ill-formulated social system problems characterised by, confusing information, conflicting values among decision-makers and clients, and complex system-wide ramifications. The term 'wicked' signifies the mischievous and often detrimental nature of these problems, where proposed solutions can exacerbate the issues. Six years later, Rittel and Melvin Webber published a seminal paper on wicked problems, leading to a significant increase in research papers using the term and has garnered over 5000 citations, standing as the most highly cited publication on this subject.

The concept of wicked problems is critiqued for its ambiguity and overuse. It has been applied widely and indiscriminately across various disciplines and by researchers from different institutions in North America, Europe, and Australia. This year we celebrate the 50th anniversary of the term Wicked Problems, first introduced by Horst Rittel and Melvin Webber in a 1973 paper titled "Dilemmas in a General Theory of Planning." Primarily used in the context of urban planning and policy-making, this paper described wicked problems as complex, ill-structured, and difficult-to-define problems that often have no single solution. These problems were characterised by being open-ended, involving multiple stakeholders, and having no clear criteria for success or failure.

Over the last 50 years, however, the concept of wicked problems has expanded beyond urban planning and policy, gaining prominence in various disciplines, such as risk management and business strategy. Researchers and practitioners in their respective fields have adapted and applied the concept to describe complex, multifaceted challenges that resist easy solutions. In management and strategy, the term has been utilised to describe complex organisational issues that cannot be solved through conventional problem-solving approaches.

This article explores the concept of "wicked problems," their evolution across various disciplines like risk management and business strategy, and how a balance between realism and constructivism can assist in addressing these complex challenges whilst avoiding overuse or understatement of the organisations problem.

Turnbull and Hoppe (2019) argue that Rittel and Webber's influential paper on wicked problems was more of a political intervention in scholarly discourse than the foundation of an intellectual research program. They suggest that the paper served as an invitation for rationalistic researchers to engage in critical reflection within their paradigm. Historically, their contribution can be seen as just a small component of a broader challenge to the systems view. The statement highlights that Rittel and Webber's work on wicked problems is part of a larger intellectual movement or intellectual challenge to the traditional systems view of problem-solving and management. One that questions and redefines traditional problem-solving paradigms, emphasising the need for more holistic and flexible approaches when dealing with complex, interconnected issues.

Addressing wicked problems, those complex and multifaceted challenges that defy easy resolution, requires a nuanced understanding and a flexible approach. In the quest for solutions, two distinct yet complementary perspectives come to the fore: realism and constructivism. The realist perspective offers practical, adaptive, and collaborative insights, grounded in an acknowledgment of the inherent complexity and uncertainty of wicked problems. Realists aim for feasible and meaningful improvements, steering away from the pursuit of idealised, unattainable solutions.

On the other hand, constructivism - a theory of learning and problem-solving - proposes that our comprehension of the world evolves through experiences, beliefs, and interactions. When applied to wicked problems, constructivism offers valuable insights into how individuals and groups can effectively approach these intricate challenges. In this exploration, we delve into these two conceptual lenses, unravelling their distinctive approaches and assessing their applicability in the ever-evolving landscape of wicked problems.

REALISM

Approaching wicked problems from a realist perspective offers valuable insights into their intricate nature and the formidable challenges they present. This approach is characterised by a practical, pragmatic, adaptive, and collaborative mindset, grounded in an acknowledgment of the complexity and uncertainty inherent in such problems. Realists seek feasible and meaningful improvements rather than idealised or perfect solutions.

A realist viewpoint accepts the inherent complexity and uncertainty of wicked problems. These issues lack straightforward solutions due to numerous variables and interconnected factors. Understanding this complexity, avoiding oversimplification, and embracing the multifaceted nature of these challenges, are key aspects of this perspective. It places significant emphasis on contextual understanding, recognising the importance of comprehending the specific context in which a wicked problem exists. This encompasses factors such as history, culture, and social dynamics that contribute to the problem's complexity.

In the realist approach to addressing wicked problems, a holistic understanding is paramount. This approach aims to gain a comprehensive view of the problem by considering all relevant factors and stakeholders' insights. Realists actively engage diverse perspectives and expertise, making stakeholder engagement and collaboration core principles. Their inclusive approach recognises the importance of involving a wide range of stakeholders, encompassing those directly affected by the problem and those with relevant

expertise. This recognition of the diversity of perspectives as a source of strength can lead to more robust solutions. Additionally, realists acknowledge the inherent conflicts among stakeholders with diverse viewpoints when addressing wicked problems. They understand that finding common ground and navigating conflicting interests, values, and objectives is often an integral part of the process.

Furthermore, realists maintain a long-term focus, understanding that solutions to wicked problems often require sustained efforts and ongoing monitoring. They recognise that many wicked problems cannot be completely "solved" in the traditional sense but require ongoing management. Resource allocation is done judiciously by adopting careful consideration of practical needs, and budget constraints, and prioritising initiatives that promise significant impact. Ethical considerations are seamlessly integrated into the approach, ensuring that solutions consistently respect ethical principles and social values, even when making challenging decisions. This holistic approach of combining long-term commitment, resource allocation, and ethical considerations underscores the commitment to effectively addressing wicked problems while acknowledging their ongoing and complex nature.

Risk management is a critical consideration for those adopting this perspective. They are mindful of potential risks and unintended consequences associated with different potential solutions. Proactively mitigating risks and evaluating trade-offs are integral to their problem-solving process. Relying on evidence-based decision-making, they emphasise the importance of empirical evidence and data in informing their choices. Objective information takes precedence over intuition or ideology.

Adaptability is a cornerstone of the strategy, as practitioners adopt flexible and adaptive approaches, remaining open to adjusting their methods as new information and insights emerge. Recognising that solutions may need to evolve, this adaptability is closely linked to continuous learning and improvement, which are fundamental to this approach. Commitment to ongoing learning and adapting strategies based on feedback and evaluation, employing an iterative approach that proves vital in addressing complex and evolving issues. This iterative approach is commonly used when addressing wicked problems, involving continual assessments of the effectiveness of interventions, refining strategies based on outcomes and feedback, and creating a cycle of actions, assessment, and adjustment.

CONSTRUCTIVISM

Constructivism, a theory of learning and problem-solving, asserts that our understanding of the world is constructed through our experiences, beliefs, and interactions. When applied to wicked problems—complex issues with no clear solutions—it offers valuable insights into how to approach them effectively. Constructivism emphasises understanding diverse perspectives, contending that knowledge is constructed through social interaction and dialogue. This implies that individuals and groups should engage in open, inclusive discussions to comprehend various viewpoints and interpretations held by stakeholders, experts, and the affected community.

Wicked problems often require collective decision-making involving multiple stakeholders. A constructivist approach encourages the participation of all relevant parties in the decision-making process, aiming for more informed and contextually relevant solutions that acknowledge the problem's complexity. Constructivism also highlights problem framing, suggesting that individuals construct their understanding of a problem based on their experiences and beliefs. Therefore, addressing wicked problems necessitates collaboratively framing the issue, including defining boundaries, identifying root causes, and acknowledging inherent uncertainty and complexity.

Iterative problem-solving aligns with constructivist principles, emphasising that problem-solving should be an ongoing, adaptive process. Solutions to wicked problems may need constant testing and adjustment, with an emphasis on feedback and reflection. Continuous learning and adaptation are integral, acknowledging that learning is ongoing, and that the solution landscape itself evolves. Thus, their approach involves continuous learning and adaptation as new information, insights, and perspectives emerge.

The use of dialogue and facilitation are fundamental constructivist methods and prove valuable in addressing wicked problems. They create spaces for open, respectful communication, allowing the integration of diverse perspectives into problem-solving efforts. Advocating a holistic approach to complex issues and when addressing wicked problems, encourages considering not only immediate symptoms but also the underlying systemic factors contributing to the problem's wickedness. Furthermore, constructivism promotes critical reflection, urging individuals and groups working on wicked problems to critically evaluate assumptions, biases, and potential unintended consequences of their solutions.

Risk professionals and rationalistic researchers alike can incorporate elements of both realism and constructivism in their approach to conclude their work activities and studies effectively. Realism's emphasis on empirical evidence, holistic analysis, risk management, and evidence-based decision-making can provide a solid foundation for drawing practical, sustainable conclusions. This approach acknowledges the complex and dynamic nature of wicked problems while striving for tangible progress. Additionally, they can draw on constructivist principles to recognise that definitive solutions may be elusive in certain contexts. By embracing adaptability, inclusivity, and responsiveness, they can propose strategies or interventions that evolve alongside the ever-changing nature of these complex issues. This synthesis of realism and constructivism allows professionals and researchers to strike a balance between evidence-based pragmatism and adaptability, providing comprehensive and nuanced conclusions that better address the intricate challenges posed by wicked problems.

EQUILIBRIUM

Organisations often grapple with finding solutions when addressing wicked problems, and the right equilibrium between realism and constructivism can play a pivotal role in preventing organisations from either overusing the term "wicked problem" or underestimating the complexity of the challenges they encounter. By integrating these two approaches, organisations can find the middle ground. Accurately, identifying and labelling true wicked problems while simultaneously recognising that not all challenges require the same level of complexity. This balance encourages a nuanced understanding of problems and allows for a more accurate assessment of problems, ultimately leading to more effective problem-solving and decision-making within the organisation.

Realism, with its emphasis on empirical evidence, objective analysis, and practical goal-setting, can help organisations avoid the overuse of the term "wicked problem." By adopting a realist perspective, they can ensure that they label a problem as "wicked" only when it genuinely exhibits the characteristics of high complexity, uncertainty, and interconnectedness. This judicious use of the term maintains its credibility and prevents its dilution through overapplication.

On the other hand, constructivism's focus on adaptability, responsiveness, and the recognition of diverse perspectives can assist organisations in understating the problem. By embracing a constructivist approach, they acknowledge that while some issues may not fit the classical definition of wicked problems, they can still be multifaceted and require innovative, context-specific solutions. This prevents the dismissal of complex problems as trivial or easily solvable.

In conclusion, the term 'wicked problems,' introduced by Horst Rittel in 1967 and developed further with Melvin Webber in 1973, describes complex issues that defy easy resolution. Despite its pervasive use across different disciplines, debates persist regarding its theoretical foundations and practical applicability. As we commemorate its 50th anniversary, it is evident that 'wicked problems' have extended beyond their urban planning origins, finding relevance in domains such as risk management and business strategy – demonstrating the conceptual transfer or extension of wicked problems beyond its initial scope. Turnbull and Hoppe suggest that Rittel and Webber's work should be seen as a challenge to traditional problem-solving paradigms rather than a definitive theory. Effectively addressing 'wicked problems' necessitates a balanced approach that combines realism, emphasising evidence-based solutions, and constructivism, promoting adaptability and inclusivity. This synthesis enables organisations to navigate the fine line between overusing the 'wicked problem' label and underestimating the complexity they face. In essence, the term 'wicked problems' continues to evolve and remains relevant across multiple disciplines. The synergy between realism and constructivism provides a robust framework for effective problem-solving and decision-making without over-generalisation or underestimation.

References

Camillus, J. C. (2008). Strategy as a wicked problem. Harvard Business Review, 86(5), 98-106.

Conkin, J. (2006). Dialogue mapping: Building shared understanding of wicked problems. John Wiley & Sons.

Head, B. W. (2008). Wicked Problems in Public Policy. Public Policy, 3(2), 101-118.

Jonassen, D. H. (1991). Evaluating constructivist learning. Educational Technology, 31(9), 28-33.

Lejano, R., Ingram, H., & Ingram, H. (2009). Participatory Environmental Regulation and Local Knowledge: Studying the Complexity-Performance Relationship. Environmental Management 43(6), 1184-1204.

Peters, B. G. (2017). What is so wicked about wicked problems? A conceptual analysis and a research program. Policy and Society, 36 (3), 385-396.

Rittel, H., & Webber, M. (1973). Dilemmas in a General Theory of Planning. Policy Sciences 4(2), 155-169.

Turnbull, N., & Hoppe, R. (2019). Problematizing 'wickedness': a critique of the wicked problems concept, from philosophy to practice. Policy and Society, 38(2), 315-337.

AUTHOR BIO

RONNIE FAULKNER

Ronnie Faulkner has 20 years of experience as a tradesman in the electrical distribution industry, and specialises in construction, maintenance, and operational contracts. He is a strong advocate for health and safety in the construction industry, attributing his safety record to comprehensive risk assessments and making value-based decisions. In addition to his extensive industry experience, Ronnie is a proven leader and continues to develop his leadership skills through involvement in professional institutions, including the Institute of Strategic Risk Management (M.ISRM) and the Australian Risk Policy Institute (AARPI). Ronnie's credentials include an Executive Master of Business Administration and a Graduate Certificate in the Psychology of Risk (Australian Catholic University), Advanced Diploma of Electrical Engineering (TAFE Queensland) and Level 5 Award in Presilience, Leadership & High Performance (Institute of Presilience).

BUILDING EFFECTIVE BUSINESS RESILIENCE PROGRAMS

BY LAURA JURY MBCI M.ISRM

I find that the word "Resilience" means a lot of different things to different people. Is it the ability to bounce back from disruption? Is it about pre-planning, so you have options when a risk is materialized? Is it about understanding if you have enough of a buffer or cushion to soak up the hit?

In terms of Business Resilience, it encapsulates processes designed to understand what is critical to your business and therefore must continue, as well as what is non-essential and can be dropped or stopped, with those resources being redirected elsewhere. While we may all have different terms and definitions. Business Resilience is at its core, all about building solutions that define what the plan is to continue critical work, post-disruption.

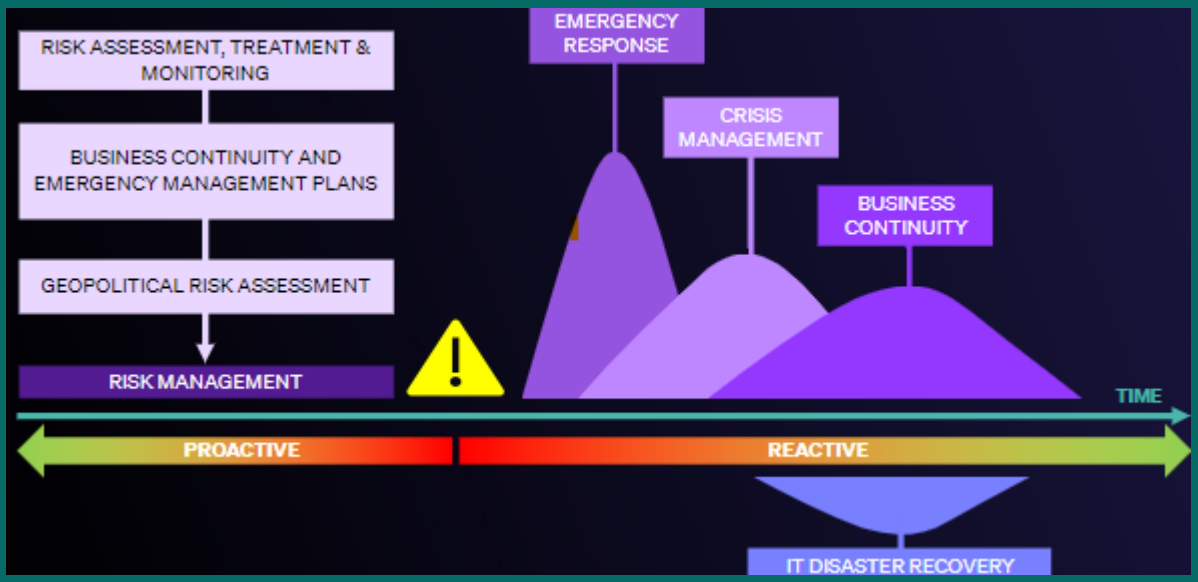
At the proactive end of the spectrum, building and continuously improving Business Resilience is reliant on multiple pieces of work from across the business - things like Risk Assessments to understand the current state is, and enterprise level Board Risk Appetite statements that create a treatment and monitoring framework that measures the tolerance or allowance at an elevated organizational wide view. Externally, this also encompasses the intelligence gathering on geopolitical events and putting plans in place to minimize the risk or impact on the organization.

Close to my heart are those plans created within the Business Continuity and Emergency Management spaces. Driving the process to think, before the event, of what we are capable of and where there is weakness that may break under strain. This extends to also exercising those plans. I think of exercising plans as stretching those muscles, and to thinking through the types of challenges that you may have in a live event, that help you respond in the pressured environment of an incident or crisis.

Then, when the disruption event occurs, several things may kick off, namely the initial on-the-ground **Emergency Response** – what happens immediately to keep people safe, to collate information about the situation, to understand who needs critical information to make effective decisions, and to stay informed about the evolving situation with the intent of minimising the damage.

The **Crisis or Incident Management** is the process of how an Organisation then makes strategic decisions in a disruption, the function of getting the Crisis Team and Leadership teams together to understand the situation, and to make critical tactical and strategic decisions to enable us to start thinking about the ongoing recovery and the continuation of our business.

Business Continuity helps us understand what needs to be recovered, and at what level of urgency - if done well, this is a starting point for identifying what our options are. Creating a common understanding of what would get us to the next step on the road to recovery and where extraordinary measures need to be taken.



All of this is supported by individual risk aligned recovery plans like **IT Disaster Recovery** – moving the digital footprint from a Data Centre that may be disrupted to the alternative Data Centre for the expressed purpose of continuing business.

So, what's is missing? The links to our key suppliers, and a clear understanding of our key suppliers' capability to support us in a disruption? Are we able to use their resources as an alternative? And what happens if the supplier is disrupted independent of us? Do we understand what is the suppliers' Business Continuity capability and plans?

All this feeds into the organisations Business Resilience footprint, which is an eco-system interwoven with diverse information from the organizations digital capability, connections into internal and external stakeholders, relationships with our suppliers and customers. The risk of disruption is not a theoretical problem that Business Resilience is attempting to solve: we have all seen the impacts of not responding well to disruption.

From sustained negative press coverage like what we saw in the Southwest Airline "meltdown" over the past Xmas holiday period last year (with the initial catalyst being a historic, but not unforeseeable, storm which saw nearly 16 thousand flights cancelled and hundreds of thousands of travelers plans disrupted) to an ever-increasing risk of significant Cyber Security events like the Optus privacy breaches (that saw 40% of the Australian populations protected information breached) leading, I suspect, to a sharp uptick in fraud losses.

Then there are IT outages within critical infrastructure that can impact the whole industry, like we have seen across the aviation when the major FAA warning system outage led to closed runways, flight delays and equipment issues across the US.

Finally, we also have labor shortages, industrial and strike action of air traffic controllers in France, or the actions of Scandinavian airlines pilots in the US leading to the airline bringing forward plans to restructure its finances in the face of bankruptcy.

There is no shortage of examples I could provide for this article... and this is before we start to consider the emerging risks that may be just around the corner in this ever-changing world. While the reasons for disruption can be wide and varied, the impact of these events can be planned for.

Attempting to at least get a starting point, and some options pre-planned, goes a long way when you are under the stress and pressure of responding in a disruption. Having a vague plan that your people understand, means they know what their role is and what they need to communicate, resulting in you as a leader being able to use your bandwidth better to make changes on the fly to suit the event.

So, to create an effective Business Resilience framework, think about the interconnected nature of the risk. No doubt you are not starting from scratch. Leverage the existing embedded systems – Risk Management, IT Disaster Recovery, Incident and near miss reporting, Supplier and Vendor information, Crisis Communication. Start somewhere and think deeply about what is critical to your organisation. You will be grateful - if and when that material event occurs.

AUTHOR BIO

LAURA JURY MBCI M.ISRM

Laura Jury is a seasoned Resilience Consultant within Aviation, with a distinguished career in crisis and resilience management. She excels in designing and implementing crisis response structures, significantly elevating enterprise resilience. Currently, Laura is leading the development of an advanced Business Continuity Framework at Air New Zealand, showcasing her commitment to mitigating risks in the high-stakes aviation sector. Previously, as a Crisis & Resilience Manager within Financial Services, Laura directed responses to major incidents, leveraging her strategic communication and emergency response skills. Her collaborative approach ensures robust, evolving crisis preparedness and response capabilities, driving organisational resilience across various sectors.

NAVIGATING FINANCIAL RISKS – A CASE STUDY OF NEW YORK SIGNATURE BANK

BY DR PRITI BAKHSHI ET AL

PART I: BACKGROUND

US BANKING INDUSTRY

American banks are complicated financial entities that are crucial to the economy. Commercial, savings, credit, and investment banks are included. Commercial Banks are the most common banks that offer savings and checking accounts, loans, mortgages, and investments to people and corporations. Savings Institutions are thrift institutions that offer savings accounts and mortgages, helping people become homeowners. Credit Unions are member-owned cooperatives that offer inexpensive savings, checking, lending, and credit card terms and fees. Investment banks provide securities underwriting, mergers and acquisitions advice, securities trading, and investment banking to corporate and government clients.

Multiple regulatory agencies ensure system safety and stability:

- The Federal Reserve System (The Fed) manages monetary policy to regulate inflation, interest rates, and economic stability.
- The OCC: It oversees national banks and federal savings associations for safety, soundness, and fairness as an independent bureau of the Treasury Department.
- The Federal Deposit Insurance Corporation (FDIC) protects depositor funds up to $250,000 per depositor per institution, boosting bank confidence.

FDIC – FEDERAL DEPOSIT INSURANCE CORPORATION

US bank customers are protected by the FDIC if a bank or savings company fails. It was formed in 1933 to shield depositors against Great Depression-era bank failures by guaranteeing deposits up to $250,000 per account category at every FDIC-insured bank.

The FDIC relies on premiums from insured institutions. It also has a Treasury Department credit line to boost its finances. As seen by New York's Signature Bank failure, the FDIC's financial resiliency helps sustain banking stability. In such cases, the FDIC quickly reimburses insured deposits, minimizing financial instability.

The FDIC's resources and monitoring assist depositors and banks. The FDIC offers a digital platform for depositors to check if their bank is FDIC-insured and understand their deposit coverage. This transparency reassures them about their deposits.

Banks can learn about FDIC membership, compliance, and risk management through the FDIC's web platform. This information helps banks navigate the complicated regulatory landscape and achieve client protection and financial stability standards.

The FDIC is a vital part of American banking. It safeguards depositors' funds and the financial system's stability. The FDIC strengthens banking sector trust and ensures its continued role in the U.S. economy through proactive involvement and strong financial resources.

NEW YORK SIGNATURE BANK (SBNY)

Popular New York City commercial bank New York Signature Bank (SBNY) had 40 financial centres in numerous states. SBNY was founded in 2001 as a publicly traded company with diversified ownership and no big stockholders. The bank lent to CRE and C&I clients using uninsured deposits from medium-sized commercial firms. SBNY diversified businesses in 2018 to change strategy. A private equity division, digital assets banking group, and client-specific blockchain-based payment system Signet were introduced as part of this diversification.

The bank received more large, uninsured deposits in 2020 and 2021. This doubled the bank's assets, mostly due to

digital asset deposits. In 2022, when interest rates rose and the digital asset industry became unstable, the bank reduced its digital asset deposits. This decision led to a $17.6 billion withdrawal that year, with 62% of it coming from digital asset deposits, especially in the fourth quarter.

WHAT HAPPENED?

New York-based Signature Bank experienced significant expansion in a brief period, which, although impressive, indicated potential strategic vulnerabilities. From December 2018 to December 2022, the total assets of Signature Bank skyrocketed from $47 billion to $110 billion, indicating a remarkable 134% growth between 2019 and 2021. This growth rate was distinctly greater than the average 33% increase seen among a set of 19 comparable banks over the same timeframe.

A notable aspect of Signature Bank's growth strategy was its reliance on uninsured deposits, a funding source often deemed unstable due to its susceptibility to large withdrawals during financial uncertainties. By the close of 2021, a significant 82% of Signature Bank's total assets were tied to uninsured deposits, a proportion roughly twice as high as that of its peer group.

This pronounced dependence on uninsured deposits suggests a potential concentration of risk within the bank's operational framework. Furthermore, Signature Bank's foray into the digital assets industry exposed it to added liquidity risks.

I. Managerial and Liquidity risk

Between December 2018 and December 2021, Signature Bank received a "satisfactory" assessment from the Federal Deposit Insurance Corporation (FDIC). Additionally, the FDIC granted the bank the penultimate CAMELS score regarding its management. Yet, past management inefficiencies were instrumental in the bank's subsequent downfall. Even with the "satisfactory" label during this time frame, the FDIC took multiple actions to address concerns about the bank's financial fluidity and management. Notably, in 2019, the FDIC lowered Signature Bank's liquidity grade from 2 to 3.

This shift implied a need to refine the bank's methods of managing liquidity. Examining records from the FDIC revealed a mismatch between the bank's operations, risk factors, and complexity—most notably due to gaps in their emergency liquidity plans and internal oversight. Such gaps limited the bank's ability to foresee and handle potential financial crises.

As the bank neared its closure, the FDIC implemented guidelines that called for board-level decisions and offered advice on management, financial fluidity, and governance. In the years 2018 and 2019, concerns emerged about how the bank's leadership managed growing financial and operational risks, especially regarding their commitment to risk guidelines and emergency liquidity plans. Many of these concerns lingered over the following years as they remained unaddressed. By the time of its shutdown, the FDIC hadn't finished reviewing the 2022 reports on Signature Bank. Early insights from the FDIC's 2022 financial fluidity assessment revealed plans to echo its 2019 board-focused guidelines and to introduce new concerns about the bank's financial audit processes.

On March 11, 2023, just a day ahead of the bank's shutdown, the FDIC announced an interim downgrade of the bank's CAMELS score, citing the bank's failure to address its financial and managerial issues promptly. This statement highlighted the management's struggle to oversee and control the bank's financial health, thereby endangering its longevity due to severe mismanagement. The bank's leadership displayed a lack of foresight, particularly in preparing for financial emergencies. While the FDIC indicated its plan to impose stricter actions on the bank, the bank ceased operations the next day.

Throughout its existence, Signature Bank's leadership struggled to address ongoing financial and managerial issues. The FDIC's intensified oversight in 2019 and 2020 was not enough, given the bank's deep-rooted problems. The FDIC's prolonged and insufficient actions, in the face of the bank's ongoing challenges, only made matters worse. The ultimate enforcement steps and rating downgrade, given just before the bank's 2023 demise, highlight the importance of timely and decisive interventions to prevent such failures in the financial sector.

II. Un-Insured Deposit risk

Signature Bank New York (SBNY) had uninsured deposits ranging from 63% to 82% of its total assets. In contrast, an April 2023 GAO report highlighted that SBNY's peers typically maintained a ratio between 31% and 41%. SBNY's heavy reliance on these deposits significantly amplified its liquidity risks. Although the bank's strategy focused on large commercial deposits, it lacked comprehensive policies to manage this risk. Furthermore, while bank management was confident in the stability of its deposit base due to its client-centric model, it did not establish robust liquidity stress tests or strategies to manage potential deposit runoffs.

SBNY experienced substantial growth in 2020 and 2021, largely attributed to its association with emerging sectors like cryptocurrency and the broader economic response to the pandemic. By 2021, deposits related to digital assets made up 27% of the total, with significant concentration among a few high-value depositors. Despite these indicators and the FDIC's reservations regarding the deposit concentration, SBNY's management remained steadfast in their confidence, emphasizing the strength of their client relationships. They failed to fully recognize the inherent risks associated with their large uninsured deposit base, especially when juxtaposed with the financial crises faced by banks in 2008. The bank's strategy lacked a comprehensive contingency plan for potential financial market disruptions.

III. Other risks

Credit Risk: Signature Bank possessed a notable amount of loans directed towards the cryptocurrency sector, which was undergoing a decline during the period of the bank's downfall. This implies that a significant chunk of the bank's lending portfolio was vulnerable if cryptocurrency-based borrowers couldn't meet their loan obligations. Given the nascent and unpredictable nature of the cryptocurrency industry, there's an increased likelihood of borrowers failing to repay. Such cryptocurrency ventures are more prone to economic struggles, unemployment, or outright business shutdown compared to those in older, more stable industries. When a borrower can't pay back a loan, the bank faces a loss on that amount. This situation can result in substantial financial setbacks for the bank, especially if it is heavily invested in a specific industry or market segment.

Market risk: Signature Bank's investments in the cryptocurrency market were particularly risky, as the cryptocurrency market is volatile and unpredictable. The value of cryptocurrencies can fluctuate wildly, which means that the value of Signature Bank's investments could also fluctuate wildly. If the value of Signature Bank's cryptocurrency investments declined significantly, the bank would lose money. This could lead to a decrease in the bank's net worth and an increase in its risk of failure.

Contingency risk: Signature Bank's involvement with cryptocurrency deposits also introduced a contingency risk. Given the evolving regulatory landscape surrounding cryptocurrencies, there could be unforeseen legal or regulatory challenges that the bank might face. Cryptocurrencies, still finding their footing in the mainstream financial sector, come with uncertainties tied to regulatory crackdowns, technological disruptions, or macroeconomic

factors. The bank's engagement with cryptocurrency could have triggered unforeseen consequences, especially if sudden regulatory shifts or global events were affecting the cryptocurrency market. This contingency risk emphasizes the unpredictable nature of emerging markets and the potential repercussions of being associated with them.

PART II: STRATEGIES TO MITIGATE, HEDGE AND REDUCE RISKS

1. Buy Options such as Puttable Bonds or Swaptions

The primary goal of purchasing options like puttable bonds or swaptions is to protect against the potential increase in interest rates. These financial instruments provide the bank with the flexibility to sell back the security at a pre-set rate. If interest rates do go up, this option allows the bank to modify its existing debt or swap agreements to more advantageous conditions. While this strategy doesn't directly pertain to uninsured deposits, it does enable the bank to better manage its overall exposure to interest rate fluctuations, which may, in turn, influence how appealing its deposit rates are to customers.

2. Raise Additional Capital

The primary aim of securing additional funding is to bolster the bank's capital reserves. Doing so not only enhances the bank's resilience against potential losses but also helps it comply with regulatory mandates concerning capital adequacy. While this move doesn't directly impact uninsured deposits, it could instil greater confidence among depositors. This heightened sense of security may make them more inclined to keep uninsured deposits with the bank.

3. Invest in Risk Management Systems

The goal of implementing advanced risk management systems is to recognize and effectively manage various kinds of risks, such as those related to liquidity and interest rates. While these systems don't specifically target uninsured deposits, they do offer indirect benefits. A well-designed risk management framework allows the bank to better assess the risks tied to uninsured deposits, enabling it to take suitable measures to mitigate those risks. This, in turn, could contribute to a more secure environment for holding such deposits.

4. Diversification in Deposits and Investments

The overarching objective of diversification, both in deposits and investments, is to create a more stable and resilient financial environment for Signature Bank. On the deposit side, the aim is to reduce vulnerability to sudden withdrawals or market changes by diversifying across different types of depositors, such as retail, institutional, and governmental, as well as various deposit products like checking accounts and term deposits. This strategy serves as a cushion against liquidity crises and market volatility.

5. Stress Testing

The goal of stress testing at Signature Bank is to gauge its ability to weather adverse but plausible scenarios. Through simulations, the bank evaluates how its balance sheet would react to events like sharp interest rate hikes, loan defaults, or sudden withdrawals of uninsured deposits. The findings help identify weak points, enabling the bank to take pre-emptive actions such as boosting capital or revising risk strategies. This practice enhances the bank's resilience and can also increase depositor confidence.

6. Credit Default Insurance for Loans

The objective here is to shield Signature Bank from the default risks associated with loans extended to cryptocurrency firms. The bank can achieve this by acquiring credit default insurance, which would compensate the bank if such a company fails to repay its loan. Considering the volatile nature and regulatory ambiguity of the cryptocurrency sector, this insurance adds an extra layer of protection, helping to minimize the associated risks.

7. Training the Management and Risk Management Team

The goal is to bolster Signature Bank's in-house capabilities for recognizing, evaluating, and managing risks. To accomplish this, the bank could invest in specialized training for its managerial and risk management staff. Topics covered could range from advanced risk modelling and regulatory compliance to understanding emerging risks, such as those in the cryptocurrency sector, and best practices in risk governance. With better training, the teams are more apt to spot early indicators of different types of risks, whether they be credit, market, or operational. This enhanced skill set allows for a more proactive and efficient approach to risk management, better preparing the bank for various financial complexities and regulatory changes.

PART III: RISK MANAGEMENT TECHNIQUES AND MODELS

Credit Risk: (Basel II and Basel III)

Basel II: Basel II developed more sophisticated methods for determining credit risk. The probability of default (PD), loss-given default (LGD), and exposure at default (EAD) for a bank's assets must all be estimated using internal models. These models need to have been used by Signature Bank when making loans to the bitcoin sector. These models would have allowed the bank to allocate the proper capital reserves based on the risk profile of these loans and would have offered a more accurate evaluation of the credit risk related to each borrower.

The probability that a borrower would stop making loan payments is known as the probability of default (PD). PD is often calculated based on several variables, including the borrower's financial statements, industry forecast, and credit history.

The sum of money that a lender anticipates losing if a borrower fails on a loan is known as the loss-given default (LGD). The value of the loan's collateral and the borrower's capacity to repay the loan even if the collateral is sold are often taken into account when estimating LGD.

The amount that a lender is in danger of losing if a borrower defaults on their loan is known as exposure at default (EAD). The outstanding sum of the loan plus any accrued interest and fees is often used to calculate EAD.

The expected loss can be calculated by

EL=PD x LGD x EAD

If a borrower with a PD of 10%, LGD of 50%, and EAD of $1 million. In this case, the lender would anticipate losing $50,000 on the loan.

To determine whether their capital is adequate, banks employ EL. Regulations known as "capital adequacy requirements" call on banks to keep a specific level of capital on hand to cover any potential loan losses.

In the case of Signature Bank, the bank suffered huge losses when the cryptocurrency market crashed because it had not properly evaluated the PD, LGD, and EAD of its Bitcoin loans.

Basel III: Basel III tightened up the capital regulations. To protect against potential losses from credit risk in its cryptocurrency-related loans, Signature Bank should have kept stronger capital buffers.

The danger of default on Bitcoin loans is considerable due to the erratic and volatile nature of the cryptocurrency market. Due to the concentration of the loans Signature Bank made to holders of cryptocurrencies, the bank was more vulnerable to losses in the event of a fall in the cryptocurrency market.

Banks are mandated by Basel III to maintain capital reserves to cover potential loan loss exposure. However, following the 2022 bitcoin market meltdown, Signature Bank's capital buffers were insufficient to cover the losses the bank incurred on its cryptocurrency loans.

One of the key causes of Signature Bank's demise was its failure to keep proper capital buffers. The value of Signature Bank's Bitcoin loans had to be written off when the cryptocurrency market fell in 2022. The bank suffered huge losses as a result, of exceeding its capital reserves. Due to this, the bank was unable to fulfil its obligations to its creditors and depositors and was consequently forced to liquidate.

Market Risk (Basel II and Basel III):

Basel II: Basel II addresses market risk as well, requiring banks to calculate possible losses from market fluctuations using Value risk models. Value at risk could have been used by Signature Bank to estimate probable losses on its bitcoin assets.

Basel III: Basel III introduces new capital costs for trading book activities, substantially enhancing market risk restrictions. By doing this, banks will be deterred from assuming excessive risks in their trading books. Given the volatility of the cryptocurrency market, Signature Bank ought to have made sure that its market risk capital was sufficient.

The stressed value-at-risk **(VaR)** criterion is another Basel III addition. To ensure that their capital buffers are sufficient to sustain even unexpected losses, banks must perform VaR calculations under more demanding market conditions. Under more unfavourable market circumstances, Signature Bank may have used stressed **VaR** to estimate the probable losses on its cryptocurrency investments.

Banks must comply with Basel II requirements and calculate potential losses from market fluctuations using value-at-risk **(VaR)** models. **VaR** models are statistical models that calculate the most money a bank could lose on its trading book over a specific period, assuming normal market circumstances. **VaR** might have been used by Signature Bank to determine the possible losses associated with its Bitcoin investments and to allocate money appropriately.

The failure of Signature Bank to effectively manage its exposure to market risk was not the sole issue that led to its demise. The bank also had a sizable amount of exposure to the real estate sector, which was severely impacted by the 2022 economic slump. However, a significant contributing cause was the bank's poor management of its market risk in the bitcoin sector.

Contingency Risk (Basel III):

Basel III: Basel III highlights the significance of managing liquidity risk. To determine how unexpected occurrences or regulatory changes in the cryptocurrency market could affect its liquidity position, Signature Bank should have carried out stress testing, including liquidity stress tests. This would have made it easier to create backup plans.

Basel III liquidity stress testing might have been utilized by Signature Bank to evaluate the effects of various scenarios on its liquidity position. The bank could have, for instance, assessed how a sudden withdrawal of bitcoin deposits or a change in regulations that made it more challenging for the bank to get capital would affect its liquidity position.

The possible effects of various situations may have been understood by Signature Bank, who could have created backup plans to lessen the risk of unforeseen events. The bank could have, for instance, planned to sell assets to generate liquidity or to raise more capital.

The Basel III liquidity coverage ratio (LCR) and net stable funding ratio (NSFR) standards might have been employed by Signature Bank to make sure that it has enough liquid assets to meet its short-term liabilities. Requirements for the LCR and NSFR are made to help banks withstand shocks to the liquidity situation.

Uninsured Deposit Risk (Basel III):

The Liquidity Coverage Ratio (LCR), which Basel III introduced, aims to ensure that banks have enough high-quality liquid assets to cover their short-term liquidity demands. To reduce the risk brought on by its significant reliance on uninsured deposits, Signature Bank should have maintained a high LCR.

A crucial part of Basel III's liquidity structure is the LCR. A 30-day stress scenario requires banks to keep a reserve of high-quality liquid assets (HQLA) to fulfil their short-term liquidity requirements. It should be simple to convert these HQLA into cash without suffering a major loss in value.

Because it relied on uninsured deposits, Signature Bank was vulnerable to unforeseen withdrawals, particularly during difficult financial or economic circumstances. The bank's liquidity position might be put under pressure if a sizable number of depositors decide to withdraw their money all at once.

Signature Bank needs to have kept a high LCR to reduce the risk of liquidity gaps brought on by withdrawals of uninsured deposits. To fulfil its immediate obligations, this entails keeping a sufficient quantity of HQLA that can be swiftly liquidated.

Government securities, reserve funds from the central bank, and high-quality corporate bonds are examples of HQLA assets. These assets are very liquid and have a low-value loss when sold or pledged in the market.

Banks must adhere to strict LCR standards set down by Basel III, and regulators rigorously monitor compliance. Regulation-related penalties and reputational harm may occur from failure to comply with LCR rules.

Regular stress tests simulating different liquidity stress scenarios, such as major deposit withdrawals, should have been performed by Signature Bank. These evaluations would aid in identifying any potential gaps in the bank's liquidity position and provide information for emergency preparation.

ADVANTAGES

Greater decision-making: By giving companies a greater awareness of the risks they face and the possible outcomes of various courses of action, risk management techniques and models can assist them in making more informed decisions.

Reduced losses: By helping firms detect and mitigate risks before they cause damage, risk management techniques and models can help those organizations decrease their losses.

Improved compliance: Risk management models and procedures can assist firms in adhering to industry standards and legal obligations.

Enhanced reputation: Organizations can improve their reputation and draw in investors and consumers by implementing a solid risk management system.

DISADVANTAGES

Cost: Implementing and maintaining risk management strategies and models can be expensive.

Complexity: Risk management strategies and models may be intricate and complicated to comprehend, making it difficult to put them into practice successfully.

False sense of security: If risk management strategies and models are not properly implemented, they may cause firms to feel insecure.

Data Restrictions: The accuracy of risk management strategies and models depends on the data upon which they are built. The risk assessment's conclusions might not be accurate or full if the data is unreliable.

References

Acharya, V. V., Richardson, M., Schoenholtz, K. L., Tuckman, B., Berner, R., Cecchetti, S. G., Kim, S., Kim, S., Philippon, T., Ryan, S. G., Savov, A., Schnabl, P., & White, L. J. (2023). SVB and Beyond: The Banking Stress of 2023. Social Science Research Network. https://doi.org/10.2139/ssrn.4513276

Aibangbee, Y. (2023b). Improving The Government's Lender of Last Resort Function: Lessons From SVB and Signature Bank. Bank Policy Institute. https://bpi.com/improving-the-governments-lender-of-last-resort-function-lessons-from-svb-and-signature-bank/

Azahar, A. H. M. (2018). The Evaluating Banking Operation Management on Signature Bank. Social Science Research Network. https://doi.org/10.2139/ssrn.3301931

Bank Regulation: Preliminary review of agency actions related to March 2023 bank failures. (2023, April 28). U.S. GAO. https://www.gao.gov/products/gao-23-106736

Blackboard. (n.d.). Blackboard Learn. © 1997-2023 Blackboard Inc. All Rights Reserved. U.S. Patent No. 7,493,396 and 7,558,853. Additional Patents Pending. https://web-p-ebscohost-com.spjain.idm.oclc.org/ehost/detail/detail?vid=0&sid=c02dbfea-ec58-43e2-b588-37dcfd229067%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=bth&AN=164699278

Drechsler, I., Savov, A., Schnabl, P., & Wang, O. (2023). Banking on uninsured deposits. Social Science Research Network. https://doi.org/10.2139/ssrn.4411127

EBSCOHost | 164699278 | BANK FAILURE RISK: A STUDY ON SILICON VALLEY BANK, SIGNATURE BANK & SILVERGATE CAPITAL CORPORATION. (n.d.).

FDIC releases report detailing supervision of the former signature Bank, New York, New York. (n.d.). https://www.fdic.gov/news/press-releases/2023/pr23033.html

INSTANT EXPERT: What's next after the failure of - ProQuest? (n.d.). https://www.proquest.com/docview/2789784481/51B049EB3464519PQ/9?accountid=162730

Spanburg, D. (n.d.). FDIC: Options for deposit insurance reform. https://www.fdic.gov/analysis/options-deposit-insurance-reforms/index.html

AUTHOR BIO

DR. PRITI BAKHSHI

Dr. Priti Bakhshi, Associate Professor at S P Jain School of Global Management in the area of Financial Risk Management. She is a Ph.D., MBA (Finance), M. Com, MA, and NET qualified along with many International and National Certifications. She has over 26 years of experience in Industry, Academics, Research, Supervising DBA Scholars, Consultancy, and Mentoring Start-Ups. She has completed many Consultancy projects for DRDO-Inmas, Narcotics department of India, PMKVY, UMS India, World Bank and Aide-at-action, etc. She has Mentored Women Entrepreneurs under a Goldman Sachs Women Entrepreneurship program by ISB in association with London Business School. Her papers and cases are published in ABDC, Thomson Clarivate and Scopus Indexed Journals. She is editor/reviewer for INFOMS, Taylor & Francis, Emerald, Inderscience and many more. She has written a book titled: Indo-European Union Trade Dynamics.

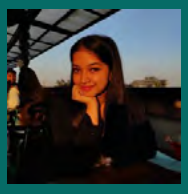
She has also participated in many national and international Conferences. She is recipient of

- Associate of the Quarter award by S P Jain School of Global Management in Jun'22
- Gold Award - ICAI International Research Awards 2021 for the Best Research Paper in the Finance category.
- Best paper award and First Prize at International Conference on Sustainable and Renewable Energy Challenges and Opportunities organized by PIET in association with CSIR-NEERI in December, 2020.
- Best Paper Award in RDA's 20th International Conference.
- "Best Professor – Finance & Banking" by IDMBA-AMP at Hyderabad
- "Teaching Award: The Demystifying Award" by Jaipuria Institute
- "Teaching Award: Problem Solver of the Year Award" in 2017 by JIM, Indore
- "Women Achiever's Award" by Idreamz Production, 2019 hosted by Mandira Bedi

CO-AUTHORS

ANSHAJ GUPTA
MBA Student at S P Jain School of Global Management

SHIVAM SETHI
Student at S P Jain School of Global Management

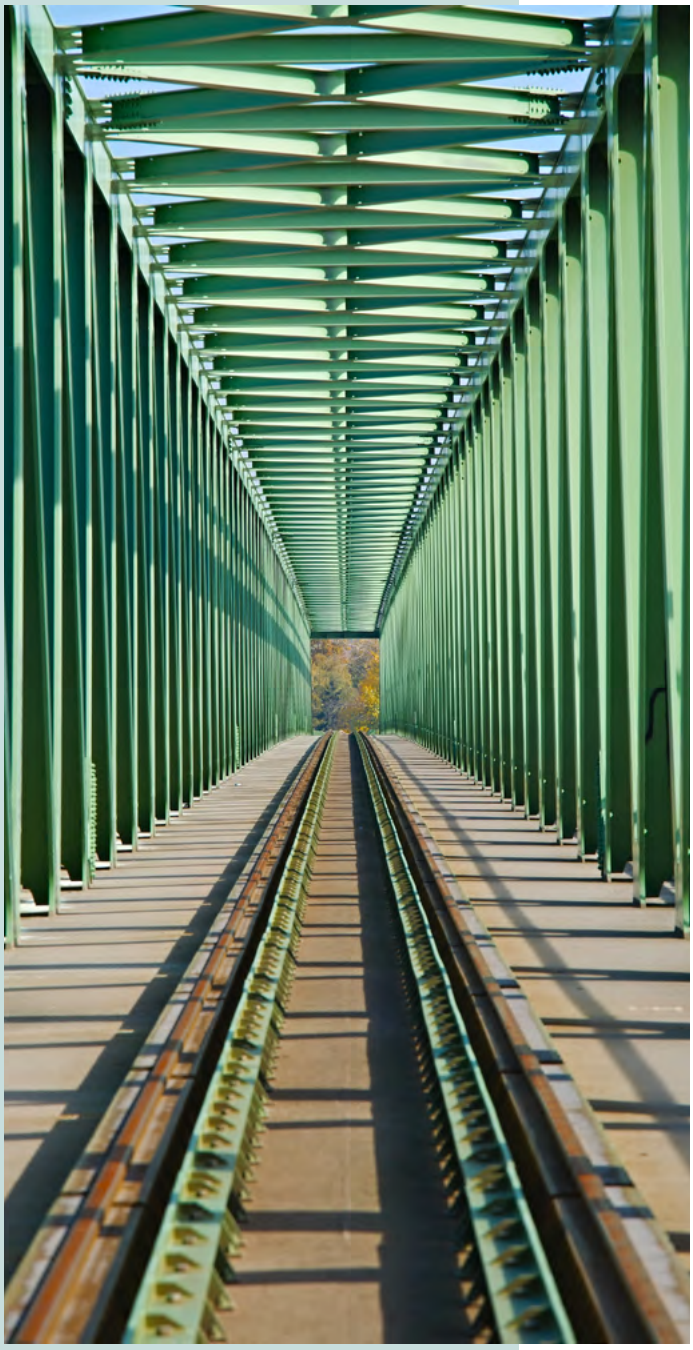


ANJUSHA NATH
GMBA Student at S P Jain School of Global Management

DEVANSH HINGAD
GMBA Student at S P Jain School of Global Management

MANAGING ORGANISATIONAL RISK THROUGH EDUCATION

BY MARK COSTELLO



ABSTRACT

In an era where organisational risks are increasingly complex and multifaceted, the role of education in managing these risks becomes paramount.

This article delves into the criticality of educational initiatives as a strategic tool in mitigating various forms of organisational risks, ranging from cyber security threats to compliance issues. It argues that well-structured educational programs, tailored to specific organisational needs, can not only equip employees with the necessary skills to identify and manage risks but also foster a culture of awareness and resilience.

Through a blend of theoretical insights and practical examples, the article showcases the effectiveness of educational strategies in risk mitigation. It also discusses the broader benefits of these programs, such as enhanced employee morale and organisational reputation.

Moreover, the article offers practical guidance on implementing educational programs, addressing budgeting, scheduling, and content customisation. By emphasising the real-world implications and benefits for business practitioners, this article contributes significantly to the discourse on risk and resilience management, highlighting education as a key component in the proactive management of organisational risks.

INTRODUCTION

In the dynamic landscape of contemporary business, organisations are continually exposed to a spectrum of risks that can threaten their stability, reputation, and long-term success. Organisational risk encompasses a broad range of challenges, from cyber threats and technological disruptions to regulatory compliance and workforce management. These risks, if not adequately managed, can have profound implications, potentially leading to financial losses, legal complications, and diminished public trust.

Amidst this backdrop, education emerges as a vital tool in the arsenal of risk management. By equipping employees with knowledge and skills, organisations can enhance their ability to identify, assess, and mitigate risks effectively. Educational programs tailored to address specific risks can foster a culture of risk awareness and resilience, empowering employees to become proactive agents in risk management.

The objective of this article is to explore the integral role of education in managing organisational risk. It seeks to provide insights into how educational strategies can be effectively implemented to mitigate various forms of organisational risks. By presenting a blend of theoretical frameworks and guidelines for practical application, the article aims to contribute valuable perspectives to business practitioners, enabling them to understand the criticality of education in risk management. This exploration is not only relevant but essential for modern businesses seeking to navigate the complexities of risk in an ever-evolving global market. The article underscores the significance of education in transforming the approach to organisational risk management, shifting from reactive measures to proactive strategies that safeguard the organisation's interests and ensure its sustained growth and success.

THE CURRENT LANDSCAPE OF ORGANISATIONAL RISK

The contemporary business environment is characterised by a rapidly evolving risk landscape, where organisations are confronted with an array of challenges that are increasingly complex and interconnected. This section provides an overview of the predominant organisational risks in the current business climate, highlighting their dynamic nature and the need for adaptive risk management strategies.

Cyber Threats: In the digital age, cyber threats have emerged as a prominent concern for businesses worldwide. These include risks associated with data breaches, cyber-attacks, and information security. The sophistication of cyber criminals, coupled with the growing reliance on digital infrastructure, has elevated the severity of these threats. Businesses are now tasked with safeguarding sensitive data and ensuring robust cyber security measures are in place, a challenge compounded by the rapid pace of technological change.

Compliance Issues: Regulatory compliance is another critical area of risk for organisations. With an ever-increasing array of regulations across different industries and regions, staying compliant is both vital and challenging. Non-compliance can result in hefty fines, legal repercussions, and reputational damage. This is particularly pertinent in sectors such as finance, healthcare, and technology, where regulations are stringent and frequently updated.

Market Volatility: Economic fluctuations and market volatility present significant risks to organisational stability. Factors such as global economic shifts, political changes, and trade disputes can swiftly impact market conditions, affecting business operations and profitability.

Supply Chain Vulnerabilities: The global nature of supply chains exposes organisations to a variety of risks, including logistical disruptions, geopolitical tensions, and natural disasters. The COVID-19 pandemic has underscored the fragility of global supply chains and the need for robust contingency planning.

Workforce Management: The evolving nature of work, accelerated by trends like remote work and the gig economy, presents new challenges in workforce management. Issues such as employee engagement, mental health, and adapting to new work models are increasingly pertinent.

Environmental and Social Governance (ESG) Risks: There is a growing emphasis on sustainability and social responsibility in business operations. ESG risks, related to environmental impact, social responsibility, and corporate governance, are now critical considerations for businesses, driven by both regulatory requirements and consumer expectations.

These diverse risks reflect the complexity of the modern business environment. They demand a multifaceted approach to risk management, where education plays a crucial role. By staying informed and adapting to these evolving risks, organisations can not only mitigate potential threats, but also seize opportunities for innovation and growth. The next sections will explore how education serves as a cornerstone in this adaptive approach to managing organisational risk.

THE ROLE OF EDUCATION IN RISK MANAGEMENT

In the context of the ever-evolving landscape of organisational risk, education stands as a powerful tool for empowerment and resilience.

The strategic implementation of educational programs plays a pivotal role in equipping individuals within an organisation to not only identify, understand, mitigate, and manage the risks they face but also to effectively capitalise on diversification and growth opportunities that arise from those challenges.

Empowering Through Knowledge: Education in risk management transcends the mere dissemination of information; it involves cultivating a deep understanding of the nature of risks and their implications. By educating employees, organisations enable them to recognise potential threats, understand their origins, and grasp the consequences of these risks on the business. This knowledge is fundamental in fostering a proactive approach to risk management, where risks are anticipated and addressed before they escalate into crises.

Types of Educational Programs:

1. **Cyber Security Training:** Given the prominence of cyber threats, cyber security training is essential. Such programs should cover topics like recognising phishing attempts, securing personal and company data, and understanding the company's IT security policies. Regular updates and refresher courses are crucial, given the rapidly changing nature of cyber threats.

2. **Legal Compliance Workshops:** To navigate the complex web of regulations and compliance requirements, legal compliance workshops are indispensable. These workshops should address specific regulations relevant to the industry, such as GDPR for data protection or HIPAA for healthcare. They also need to focus on the implications of non-compliance and the practices necessary to ensure adherence to legal standards.

3. **Crisis Management Training:** Preparing for potential crises through simulation exercises and scenario planning can significantly enhance an organisation's readiness. This training involves developing strategies to handle various crisis scenarios, from natural disasters to public relations crises, ensuring a swift and effective response.

4. **Financial Risk Management Courses:** Understanding financial risks, such as market volatility and credit risks, is crucial for certain sectors. Courses on financial risk management can help employees in finance-related roles to better navigate these challenges.

5. **Health and Safety Training:** In industries where physical safety is a concern, health and safety training is vital. This includes not only compliance with safety regulations but also training in safe practices and emergency response.

6. **Environmental and Social Governance (ESG) Education:** As businesses increasingly focus on sustainability, ESG-related education becomes crucial. This involves understanding the environmental impact of business activities, social responsibility practices, and effective corporate governance.

7. **Soft Skills Development:** Education in soft skills, such as communication, problem-solving, and leadership, is also essential in risk management. These skills enable employees to collaborate effectively, make informed decisions, and lead initiatives in risk mitigation.

Integrating Education into Organisational Culture: The most effective educational programs are those that are integrated into the fabric of the organisation. This integration involves regular training sessions, continuous updates, and a culture that values ongoing learning and awareness. Moreover, tailoring these educational programs to the specific needs and risks of the organisation ensures their relevance and efficacy.

Education in risk management is not a one-time event but a continuous process. It is a strategic investment that empowers employees, fosters a culture of risk awareness, and equips organisations to navigate the complexities of modern business risks effectively.

PRACTICAL STRATEGIES FOR IMPLEMENTING EDUCATIONAL PROGRAMS

Implementing educational programs to manage organisational risks involves a strategic approach that aligns with the unique needs and resources of the organisation.

This section provides guidance on developing and integrating such programs, with a focus on budgeting, scheduling, and content tailoring.

Developing the Program: The success of an educational program in risk management hinges on its relevance to the specific risks and operational context of the organisation. Initiating with a thorough training needs analysis, this approach involves identifying key risk areas and assessing the current knowledge and skills at both the individual and collective levels within the organisation. This assessment not only highlights existing gaps but also leverages the workforce's collective capabilities, setting precise objectives for the program.

Customisation of content is essential. The program should integrate real-life examples and case studies pertinent to the employees' daily experiences, thereby bridging the gap between theory and practice. Interactive methods such as simulations and group exercises, which replicate actual workplace challenges, are critical. These methods not only foster practical application of knowledge but also encourage collaboration and knowledge sharing, reinforcing the collective capacity for risk management and promoting a culture of continuous learning and improvement.

Budget Considerations with ROI Focus: In developing educational programs for risk management, budget considerations are fundamental. A realistic estimation of costs – including materials, technology, trainers, and administrative support – is essential. Utilising cost-effective strategies like online training or in-house trainers can maximise budget impact. Additionally, securing funding may involve internal resources or external grants and partnerships.

A crucial aspect of budgeting is the focus on Return on Investment (ROI). Demonstrating a clear ROI is key in justifying the expenditure and influences future budget allocations. This involves evaluating the program's effectiveness in reducing risks, improving compliance, and enhancing employee efficiency. ROI can be assessed by tracking metrics such as incident reduction rates, compliance improvements, and employee performance post-training. By strategically allocating resources to areas with the highest risk impact and investing in scalable solutions, like digital platforms, organisations can optimise long-term ROI. This approach not only validates current spending, but also supports sustained investment in educational initiatives, essential for ongoing risk management and organisational development.

Scheduling and Implementation: The implementation of the program should consider the operational schedule of the organisation to minimise disruption. Offering flexible scheduling options or multiple sessions can ensure wider participation. Implementing a pilot program initially can provide valuable insights for adjustments before a full rollout. Post-implementation, gathering feedback and evaluating the program's impact are essential for measuring effectiveness and guiding continual improvement.

Integrating with Organisational Culture: For educational programs to be successful, they must be integrated into the organisational culture. This involves securing strong support from management and clearly communicating the program's benefits to all employees. Incorporating risk management education into the onboarding process for new employees can also reinforce its importance across the organisation.

Leveraging Technology: In today's digital age, leveraging technology in educational programs offers both flexibility and efficiency. Online learning platforms enable organisations to reach a wider audience, transcending geographical limitations. Additionally, these platforms have evolved beyond mere content delivery; modern education techniques designed by professional educators now incorporate a variety of interactive and engaging learning activities, such as virtual simulations, interactive quizzes, and collaborative online projects. These dynamic methods enhance the learning experience, making it more immersive and effective. Furthermore, technology provides valuable tracking tools that help monitor participation and assess outcomes, ensuring the effectiveness of the educational programs and facilitating continuous improvement.

The successful implementation of educational programs for risk management requires a holistic approach that encompasses thorough planning, strategic budgeting, customised content, flexible scheduling, and continuous evaluation. By aligning educational strategies with the organisation's specific needs and culture, businesses can effectively enhance their capacity to manage risks and foster a culture of continuous learning and improvement.

THE BENEFITS BEYOND RISK MITIGATION

While the primary goal of educational programs in risk management is to mitigate organisational risks, these initiatives often yield additional, far-reaching benefits that can significantly enhance the overall health and competitiveness of an organisation.

Improved Employee Morale and Engagement: Educational programs contribute to a more informed and skilled workforce. When employees are equipped with the knowledge and tools to effectively manage risks, it fosters a sense of empowerment and confidence. This empowerment can lead to higher levels of job satisfaction and engagement, as employees feel more valued and capable in their roles.

Enhanced Reputation: Organisations that invest in risk management education demonstrate a commitment to best practices and continuous improvement. This commitment can enhance the organisation's reputation among stakeholders, including customers, investors, and regulatory bodies. A strong reputation for risk management can also be a competitive advantage, positioning the organisation as a leader in its industry.

Cultivation of a Learning Culture: Educational programs in risk management can be a catalyst for developing a culture of continuous learning and improvement within the organisation. This culture encourages employees to seek knowledge, stay updated with industry trends, and be proactive in identifying and addressing risks, leading to a more agile and adaptive organisation.

Increased Innovation and Performance: An informed and engaged workforce is more likely to contribute to innovation and high performance. Employees who understand the broader context of their work and the associated risks are better equipped to propose innovative solutions and improvements, driving the organisation forward.

CHALLENGES AND CONSIDERATIONS

Implementing educational programs for risk management is not without its challenges. However, understanding these challenges and proactively addressing them can lead to more effective program outcomes.

Resource Constraints: One of the primary challenges is the allocation of resources, including time, money, and personnel. Solution: Prioritising risk management education as a strategic investment and exploring cost-effective methods such as online training can help mitigate this challenge.

Employee Resistance: Resistance to change or scepticism about the value of such programs can be a hurdle. Solution: Engaging employees in the development process and clearly communicating the benefits and relevance of the training can increase buy-in and participation.

Keeping Content Relevant and Up-to-Date: The rapidly changing nature of risks, especially in areas like technology and compliance, can make it challenging to keep educational content current. Solution: Regularly updating training materials and involving experts in the field can ensure that the content remains relevant and effective.

Measuring Effectiveness: Assessing the impact of educational programs on risk management can be complex. Solution: Establishing clear metrics for success and conducting regular evaluations can help in quantifying the effectiveness of these programs.

Cultural Alignment: Ensuring that the educational program aligns with the organisation's culture and values is crucial for its success. Solution: Customising programs to reflect the unique aspects of the organisation’s culture and integrating them into regular business practices can enhance alignment and effectiveness.

While there are challenges in implementing educational programs for risk management, these can be addressed with strategic planning and proactive solutions. The benefits of these programs extend beyond risk mitigation, contributing to a more engaged workforce, a stronger organisational reputation, a culture of continuous learning, and enhanced overall performance.

CONCLUSION

The exploration of education as a tool in managing organisational risk reveals its multifaceted importance in today's complex business environment. This article has highlighted the critical role that educational programs play in empowering employees to identify, understand, and effectively mitigate various organisational risks. From cyber security threats to compliance issues, the landscape of organisational risk is diverse and ever-evolving, necessitating a proactive and informed approach.

The implementation of educational programs, while challenging, offers a strategic pathway to not only address these risks but also to accrue additional benefits. These benefits extend beyond risk mitigation, fostering improved employee morale, a stronger organisational reputation, and a culture of continuous learning and improvement. The integration of such programs into the fabric of an organisation requires careful planning, budgeting, customisation, and evaluation, but the payoff is a more resilient and agile organisation.

So what does this all mean? The practical implications for business practitioners are clear. In a world where risks are an inherent part of the business landscape, the ability to manage these risks effectively is a crucial competitive advantage.

> *Education in risk management is not merely a compliance exercise; it's an investment in the organisation's most valuable asset—its people.*

By equipping employees with the knowledge and skills to manage risks, organisations not only safeguard their operations but also position themselves for sustained growth and success.

Education in managing organisational risk is an essential component of a comprehensive risk management strategy, contributing to the resilience, adaptability, and overall health of the organisation. As businesses continue to navigate an increasingly complex world, the role of education in risk management will undoubtedly become more pronounced, underscoring the need for continuous learning and adaptation in the face of emerging challenges.

AUTHOR BIO

MARK COSTELLO

Security Training Thought Leader and Industry Innovator

Mark Costello, owner and Managing Director of Asset College, is a recognised leader in the security training landscape. His extensive career includes roles within the Australian Defence Force and the private security sector, and over 18 years in the Vocational Education and Training (VET) sector. Since founding Asset College in 2006, Mark has been pivotal in elevating training standards across Australia's security industry.

Asset College has grown under his leadership to become one of the nation's premier training providers, offering over 40 nationally-recognised qualifications in security, safety, and leadership. The college has been consistently acknowledged for excellence, securing the Large Training Provider of the Year at the Queensland Training Awards in 2020 and maintaining finalist status in subsequent years through 2023. Mark's commitment to quality is evidenced by high student completion rates and strong endorsements from industry and graduates alike. In his earlier career, Mark held key roles in operations and business development in the security sector, complemented by his military experience. He has significantly contributed to the field through his involvement in numerous advisory committees, including the Department of Home Affairs' Screener Reform Project and the Queensland Police Ministers Firearms Advisory Committee. His work extends to consulting on regulatory optimisations and workforce capacity-building initiatives.

Mark is currently developing new accredited qualifications targeting Operational Safety and a Graduate Certificate in Security, Risk and Intelligence aimed at enhancing C-suite security strategies.

His academic credentials include a Master of Business Administration, various postgraduate and vocational qualifications in related fields, and he holds several professional designations, including Certified Protection Professional (CPP) and Fellow of both the Institute of Strategic Risk Management and the Australian Security Industry Association Limited.

Mark's deep understanding of security industry challenges and his strategic insights make him an invaluable asset, particularly at influential forums like the Protective Security in Government Conference.

WHEN RISK MANAGEMENT GOES ROGUE: ELECTRICAL SAFETY AND THE 2009 HOME INSULATION PROGRAM

BY TONY LEVERTON, M.ISRM

BACKGROUND

The "Energy Efficient Homes Package" was announced by (then) Prime Minister Hon. Kevin Rudd on 3 February 2009. A component of that Package was the "Homeowner Insulation Program", replaced on 1 July 2009 by the "Home Insulation Program (HIP)".

The HIP was administered by the Department of the Environment, Water, Heritage and the Arts (DEWHA). The Package and Program were established in the context of the Rudd Government's use of expansionary fiscal policies at their discretion to counter the effects of the financial crisis of 2007–2008. The Energy Efficient Homes Package was a part of a A$42 billion Nation Building – Economic Stimulus Plan. Hon. Peter Garrett was the DEWHA Minister and responsible for the Package up until late February 2010, when it was transferred to Hon Greg Combet and Hon Penny Wong.

The insulation program covered 1.2 million homes and it was estimated that by 2015 it would have produced savings of approximately 20 x 109 kilowatt-hours (72 petajoules) of electricity and 25 petajoules (6.9×109 kWh) of natural gas savings. All installations were conducted by private contractors, as selected by home owners.

The HIP was beset by controversy when the deaths of four workers (Matthew Fuller, Reuben Barnes, Mitchell Sweeney and Marcus Wilson) in separate incidents - three of those in Queensland - were linked to the program, and electricians warned that poor installation of metallic foil insulation could lead to further deaths or injury through electrocution.

The cost of the Home Insulation program was estimated at around $1 billion and another $1 to $1.5 billion was needed to rectify the problems associated with the program.

The Royal Commission into the Home Insulation Program was established on 12 December 2013. Mr Ian Hanger AM QC, a barrister, was appointed as the Royal Commissioner to inquire into the Australian Government's Home Insulation Program. Mr Hanger reported his findings to the Government on 29 August 2014.

DEATHS ASSOCIATED WITH INSTALLING ROOF CAVITY INSULATION

Three of the four insulation installer deaths were from electrocution.

- 14 October 2009: Matthew Fuller, aged 25 – a metal staple used to lay foil insulation at a house in Meadowbrook, Logan City, had pierced an electric cable laying in the roof cavity livening the foil and escaping to earth through contact with the metal roof. His girlfriend, Monique Pridmore, who was working with Matthew, tried to rescue him and was seriously injured as a result.

- 21 November 2009: Marcus Wilson, aged 19 – Marcus was installing top-up cellulose insulation, on a very hot day, in the roof cavity of a house in St Clair (NSW) and suffered extreme hypothermia complications.

- 18 November 2009: Reuben Barnes, aged 16 – a metal screw used to fix the plasterboard ceiling to metal ceiling battens had pierced a 6mm2 twin thermoplastic sheathed cable in the channel of one of the metal ceiling battens. Reuben was laying fibreglass batts insulation in the roof cavity of a house in Stanwell, near Rockhampton.

- 4 February 2010: Mitchell Sweeney, aged 22 – a metal staple used to lay foil insulation in the roof cavity of a house in Milla Milla, South Atherton Tablelands, had pierced a lighting cable and livened the foil insulation. Mitchell's contact with the metal roof had created a path to earth.

A further severe electric shock as a result of foil insulation through the HIP was also claimed:

> *"Colin Brierley, 63, of Windaroo in the Gold Coast hinterland, says he suffered a massive electrical shock just a week after he had foil insulation installed in his home. He says the jolt of power went through his knee and exited his head, and he wound up in an induced coma in a Brisbane hospital."*

MAJOR FINDINGS OF THE ROYAL COMMISSION[2]

Seven significant failings in design and Implementation ***(Extracts 1.1.34)***

1. "Planning was sacrificed to speed. A practically unachievable commencement date for the Program, if it was to be properly and carefully designed, was unrealistically adhered to;"

2. "The allocation of the HIP to the Department of the Environment, Water, Heritage and the Arts (DEWHA), which was ill-equipped to deal with a program of its size and complexity;"

3. "A failure, until very late in the HIP, on the part of the Australian Government to identify and manage the risk to installers of injury and death;"

4. "Permitting a product to be used under the HIP that was manifestly unsuitable and dangerous;"

5. "A decision to relax training and competency requirements so as to substitute 'supervision' for insulation specific training, but without the nature of it ever being specified or clarified;"

6. "Permitting the HIP to commence in Phase 2 without there being in place a robust audit and compliance regime;"

7. "The Australian Government's reliance upon others (the States and Territories and employers) to regulate, monitor, police and enforce such occupational health and safety arrangements as might have been appropriate. Despite professing such reliance, the Australian Government never made clear to the States and Territories what its expectations were of them, nor did it enquire whether they had the resources necessary to act as the Australian Government expected."

> *"1.1.35 As with most serious failures of public administration, it is not possible to isolate one error or failure that caused all of the problems that emerged with the HIP. The causes of failure of the HIP were multifactorial. Overall, it was poorly planned and poorly implemented."*

Training / Supervision

"8.14.1.1 the effect of the change to the competencies … was to replace the requirement of training for persons inexperienced in the installation of insulation with a requirement they be 'supervised'. It was sought to be justified on the basis that all States, with the exception of South Australia, had as at that date no requisite training or registration for installers. This does not make it right, given that once industry experts were assembled to advise on the need for training their advice was ignored;

8.14.1.2 the unanimous view of industry was that training was required. That was also the view of DEWHA;

8.14.1.3 The nature of supervision required was not specified in any of the formal documentation for the HIP, such as the Guidelines, the Installer Advices or the Terms and Conditions for registration;

8.14.1.4 the Project Control Group's decision to remove the need for installers to achieve the minimum competencies was imprudent where there could be no assurance (and none was sought to be imposed) that the supervisors would in fact supervise as they ought, especially in cases in which the installer was particularly young and inexperienced;"

Reliance placed on State Safety Agencies

"11.5.6.1 the Australian Government failed to take proper responsibility for the regulation of its own program, by its almost complete reliance upon State and Territory regulatory regimes;

11.5.6.2 at no stage did the Australian Government ascertain that State and Territory regulatory regimes would be adequate to deal with the risks to personal safety and property given the nature and extent of the demands likely to be placed upon those regimes by the HIP. … ;

11.5.6.3 the Australian Government, wrongly, regarded itself as justified in leaving to the States and Territories almost entirely responsibility for OH&S under the HIP. … This reliance upon the States and Territories, and the lack of communications with them, resulted in there being inadequate regulatory arrangements for installations under the HIP."

MEDIA COMMENT[3]

"*In my view each death would, and should, not have occurred had the HIP been properly designed and implemented*," Hanger said.

"*The decision to permit the use of reflective foil sheeting as ceiling insulation was, in my view, fundamentally flawed. It contributed directly to the deaths of Mr Fuller and Mr Sweeney.*"

Despite knowing that installers were installing reflective foil sheeting across ceiling joists, and attaching it with metal staples, well before October 14, 2009, nothing was done to stop the practice, the commissioner said.

He particularly referred "*to what occurred (and, perhaps more importantly, what did not occur) in the weeks following Mr Fuller's death*". "*Deficiencies in the supervision of employees, which contributed to the death of Mr Marcus Wilson … were also known to be an issue well prior to 14 October 2009 but, again, nothing meaningful was done.*"

"*Finally, despite electrical safety issues being raised squarely as an issue after the death of Mr Fuller, insufficient action was taken to prevent further tragedies – had it been, I am satisfied that Reuben Barnes' death could have been avoided.*"

AFTERMATH - 'LEARNING FROM FAILURE'

In December 2014, the Australian Government set up an independent review of its processes for the development and implementation of large public programs and projects, having regard for the Royal Commission report into the HIP and an audit report into the National Broadband Network program.

The 'Learning from Failure' report , authored by Prof. Peter Shergold, was published in August 2015. It included the following recommendations:

> *"A.2 Whilst acknowledging the value of frank and fearless oral discussions, the Australian Public Service Commissioner should issue a Direction that significant advice also be provided to ministers in writing. Ministers should insist on receiving frank written advice from the APS, noting that it is generally their decision whether to accept or reject all or part of the advice."*
>
> *"A.4 An APS-wide policy on record keeping should provide practical guidance about when and how records must be created, including that records of deliberative discussions in all forms, including digital, should be retained." and*
>
> *"F.23 The default position that new policies proceed straight to large-scale roll-out should be reversed and instead new policy proposals should include a trial or demonstration stage, allowing new approaches to be developed fast and evaluated early."*

In February 2016, Hon. Greg Hunt, Minister for the Environment, announced the final update on the Australian Government's response to the Royal Commission report.

> *"Secretaries of Departments, through the Secretaries Board, will consider Professor Shergold's report and his conclusions, with a view to ensuring the Australian Public Service has the necessary capability to design and deliver major policy initiatives effectively, efficiently and safely."*
>
> *The Australian Public Service Commissioner "concluded that there was not a sufficient basis for formal investigations of individual public servants to proceed".*

Whether any threatened lawsuits (e.g. Colin Brierley) were seen through to their conclusion is unknown.

OBSERVATIONS

At the Royal Commission, I was asked by counsel for the Australian Government whether there were actions I would have taken differently. I replied (RC Report, page 237):

> *"Just speaking from a personal point of view, I guess in hindsight there were probably two periods where—perhaps three but certainly two periods where I look back and see that I and we could—could and should have done more."*

These two actions were:

1. A faster response to the Electrical Safety Office's first awareness of foil insulation laid across electrical cables in August 2009: The ESO's procedures included a full investigation of serious electrical incidents so that any safety concerns arising might be addressed in changes to legislation, codes, industry practice or the ESO's compliance checking priorities.

   Prof. Shergold, in assessing the Australian Public Service, referred to the need for adaptation and agility. Adaptation and agility – the ability to change in response to significant risk and to be swift to recognise and deal with it - in the ESO were lacking in the period from first knowledge of the dangers of foil insulation (August 2009) to the first reported electrocution (October 2009). To its credit, however - with one exception (see 2 below) – after this, the ESO gave the matter urgent and full attention, developing and implementing practical solutions.

2. Pursue an earlier ban on the use of foil insulation: There were disparate and strong forces involved. These dynamics included:

   a. the early acceptance of foil in the HIP by DEWHA - inexperienced in running a centralised program of the sort demanded by the Prime Minister's Office, and in an extraordinarily short timeframe - because of strong lobbyist voices in support of that product, which continued right up to early 2010, as foil installers had invested heavily in stock;

   b. an apparent equal-constituency approach to (round-table) consultation after the first foil insulation fatality i.e. the views of the Queensland ESO seemed to carry the same weight with DEWHA as other stakeholders whose primary focus may have been on insulation product and installer registration, supervision, payment, audit and fraud;

   c. inability to obtain from DEWHA details of HIP registered foil installers operating in Queensland, until after the first fatality;

   d. no unity of action across State electrical safety agencies, because insulation safety issues varied - foil insulation being primarily installed in Queensland;

   e. a reluctance by DEWHA (and ESO initially) to work with electrical industry representatives, such as the Master Electricians and the National Electrical Contractors Association, who were both pushing a ban on foil insulation; and

   f. the apparent political viscosity presented by a State Labor Government needing traction to dramatically alter a Federal Labor Government program. If the political hues of the two levels of government had been different, there would very likely have been a swifter and more focused response.

These, together, aligned to promote alternative arrangements to a foil insulation ban - banning metal staples, reintroducing and adapting training and installer information, installing RCD's and advising on safe practices such as isolating the power before entering a roof space. All important, but leaving in place the primary cause.

A further issue, referenced in the report and relating to my reply:

3. Pursue the concerns raised with the Queensland Building Services Authority (QBSA) about the dangers of ceiling fires, and follow-up the referral of my concerns to the Department of Prime Minister and Cabinet by the QBSA. I wrote to Ian Jennings, CEO of QBSA in February 2009 expressing concern about the known fire-risks of loose-fill insulation and downlights as heat sources. I asked him to consider being party to a joint media release on this matter. After repeated reminders (email and phone messages), and an approach in March to Chris Boyle, Policy Director at QBSA without a reply, I assumed QBSA had no interest in taking the matter further.

   In April I drafted a media release for Ministerial consideration. This wasn't sent out by the Minister's Office (despite frequent reminders to the departmental Public Affairs liaison officer) until early October 2009, just before the first fatality.

   A year or two later, I happened to attend a meeting with Chris and asked him what QBSA had done about my representations, he told me he had passed on my concerns in an email to the First Assistant Secretary at the Prime Minister's Department, and that she told him she had passed the email to the relevant person. Chris then sent me a copy of his April 2009 email correspondence.

   The Royal Commissioner's Report refers to Chris Boyle's email, although it mistakenly attributes Chris as being an ESO staff member. The Report also mentions that the DEWHA senior officer acknowledged he was aware of the email and its concerns.

Three other issues arise from this tragedy with respect to effective program and crisis management:

1. Record-keeping: The Royal Commissioner was scathing about Australian Government witnesses often stating "I can't recall" (or similar) when questioned at the hearings. He also criticised the Australian Government for its inability to access, or its delay in accessing and presenting relevant records to the Commission. This was a matter subsequently addressed in principle by Prof. Shergold. Queensland's ESO narrowly escaped a similar scolding. I left the ESO in March 2012. I was contacted by Crown Law in January 2014 (when overseas) who wanted to interview me as a possible witness. I was told, to my surprise, a former ESO colleague had advised the Royal Commission there were no ESO records on the HIP interactions available to access.

I was also told that another former colleague (from WHSQ) had said he had passed on to me an approach he had received from DEWHA seeking input from a health and safety perspective. Neither he nor I had any documented record of this – although he believed he had a brief conversation with me. His name was unfamiliar to me and my record-keeping practice (see para below) would have shown such an important initiative, if it had been made to me, and I would have responded to DEWHA enthusiastically, given my strong interest and earlier actions.

On my return to Brisbane, I contacted the ESO and asked to have access to my old (electronic) emails, but was advised they had all been disposed of and could not be retrieved. I told them there were hard-copy files in the system that I had created with copies of all significant documents, including emails. I cited the official file numbers (they had all been archived, thankfully) and was able to go through the files and tag all relevant documents – many of which were contemporaneous handwritten notes. These were submitted in evidence as attachments to my Affidavit. There were many documents and these seemed to be of great value to the Royal Commission.

LEARNING 1: KEEP IMMACULATE RECORDS WHEREVER POSSIBLE. THIS WILL PROTECT REPUTATIONS - YOUR EMPLOYER'S AND YOURS.

2. **Consultation – a double-edged sword:** Unless one understands the full range of risks, heroic efforts to consult may be doomed to failure. DEWHA consulted with a wide range of interest groups, including State agencies, and even worked with the newly-formed Commonwealth and State Controllers-General group. Unfortunately, with risk focus being on registration and fraud, electrical and workplace health and safety were overlooked by almost all. Should consultation with States have remedied this omission? One would have thought so but, apart from advice from an ACT representative – and the dismissed early warnings of NECA - no-one thought to step back and review the risks. Sadly, the DEWHA risk identification process became a self-defeating exercise where those ignorant of electrical safety were asked for their opinions of the risks the HIP faced.

LEARNING 2: CONSULTATION REQUIRES MORE THAN ASKING QUESTIONS AND RECORDING ANSWERS. IT MUST INVOLVE TESTING THE BOUNDARIES BETWEEN THE KNOWN AND THE UNKNOWN. INDEPENDENT PEER REVIEW NEEDS TO BE BUILT IN. LATERAL THINKING IS A VALUABLE TOOL - WHEN TAKEN SERIOUSLY.

3. **Crisis-management and functional integration:** When an organisation, be it DEWHA or the ESO, finds itself on a difficult path, approaching a crisis, there are often indicators or warnings that emerge before the crisis hits. Effective leadership involves assessing indicators and reviewing "just in case" plans, as well as formulating tentative solutions and knowing their complexities. Organisational structures are usually built around functional capabilities, and these can be ungainly when confronted with a crisis. Streamline these, temporarily, for the crisis.

One of the first functions to be affected is cross-organisational communication. This is because leaders can involve themselves in the immediate, detailed responses at the cost of a wider focus. Effective crisis-control will include operational and policy responsibilities as well as stakeholder management - people directly affected, other organisations, the media and the Minister. But in the midst of the storm one can forget what is most important in moving forward – an integrated approach to solutions that builds on the best from all functions within the organisation.

Learning 3: As the ancient parable of the blind men and the elephant tells us, each will have their own perspective of the "beast". Leadership involves vision, seeing the whole picture as it changes, and constantly communicating that to those whose scope is limited.

CONCLUSION

In its publication "Ministerial Careers and Accountability in the Australian Commonwealth Government" , the Australian National University states ("A Recent Scandal: The Home Insulation Program" by Chris Lewis):

> *"In the end, while the Rudd Government implemented the HIP in order to offset predicted lower private-sector economic activity caused by the GFC, the failure of the program was derived from its determination to implement the HIP speedily; the lack of consultation with industry players over safety, quality and rorts; and poor judgment about likely industry and consumer behaviour."*

To this I add - organisations, such as the ESO, drawn into the unintended consequences of the decisions of others must constantly scan for trouble ahead, adapt and be agile in preparation for a crisis and communicate their assessment internally and externally. The crisis may actually not arrive, but the exercise will have been worthwhile for the next one – and, sadly, there is usually a next one.

AUTHOR BIO

TONY LEVERTON

Tony Leverton was the Director (Policy) for Queensland's Electrical Safety Office from October 2005 to March 2012. In this role he was responsible for managing electrical safety policy and legislation, community engagement and Board services. He appeared as a witness before the Royal Commission in 2014. He is currently a Tutor at a Queensland RTO.

MODERNISING RISK ASSESSMENTS AND BUILDING COMMUNITY RESILIENCE

BY ZOE MILES

The growing demand for risk assessments and the evolving terrorism threat landscape both require a transformation to the risk management industry. The adoption of technology-driven risk assessments enables greater objectivity and scalability in assessments of venues against terrorism risks. These assessments diminish restrictions in time and allow for greater accessibility by a wider population. The democratisation of the risk assessment process permits greater risk awareness and, when established collectively, fosters greater community resilience. This article examines the value of technology in creating a more security conscious society that is resilient to the effects of terrorist threats.

In a period of rapid technological progression, the way risk assessments are conducted requires a change – one that offers the potential for greater scalability as well as enhanced situational awareness and resilience. Within a matter of months, Martyn's law is expected to be enacted in the United Kingdom, mandating annual terrorism risk assessments of venues with a capacity of or greater than 800 people. The enactment of this pioneering counter-terrorism standard epitomises a change in security standards, standards that will require an estimated 650,000 risk assessments to be completed within the United Kingdom each year.

The integration of technology into risk assessments has the potential to enable risks to be assessed anywhere and at any time, transcending traditional risk management methodologies.

Although convenient, the real impact of technology-based risk assessments lies in its scalability; the ability to be accessed readily by many. As a result of this democratisation, a greater sense of security consciousness is enabled, applicable to not only crowded venues, but also the broader community. Its adoption retains the ability to increase the resilience of society, ensuring a greater degree of safety regardless of evolving threats. In depiction, this opinion piece will examine the value of technology-based risk assessments and its ability to create greater accessibility, scalability and, in turn, a more security conscious and resilient society.

The tragic attack at Manchester Arena in England on May 22, 2017, highlights the devastating impacts of terrorism as an unpredictable, security risk. An inquiry into the attack and security of the targeted venue found that not only did the responsible company have an inadequate general written risk assessment, but that the risk assessment failed to identify terrorism as a potential hazard and to adopt necessary security measures to reduce those vulnerabilities (Manchester Arena Inquiry 2021). The deficiencies of security measures in venues capable of hosting large crowds and the global nature of terrorism, along with growing numbers of individuals being indoctrinated to extreme right and left-wing ideologies, and radical religious beliefs, exemplifies the necessity of strengthening security measures and guidelines, both within the public and private sphere.

Conventionally, risk assessments are conducted using qualitative or semi-qualitative methods. When conducted thoroughly, this produces a solid background to raise risk concerns and prioritise risks for mitigation, and for defences to be developed and implemented. This method relies on the subjective and heuristic judgement of risk managers, and the accuracy of the assessments is guided by the knowledge, process and reasoning of the assessor. The lack of enforcement of the industry has resulted in a similar lack of standardisation and consistency.

The nature of qualitative risk assessments is limited to the capabilities of the assessor - that is, the process is timely and therefore costly, extensive, and subjective. It is because of these subjective judgements that such flaws as bias, gaps in knowledge, and time constraints may occur, which impacts upon the accuracy and scalability of the risk assessment, and, in turn, the effectiveness of adopted security measures. Moreover, the reliance upon the knowledge of the human assessor results in the assessed risk being a perceived risk rather than an actual risk, and the assessment of the likelihood and consequence of an attack on a venue or location becomes one that is subjectively determined rather than objectively identified. This results in an oversimplification of the risk environment, despite its complex nature.

Quantitative risk assessments, which adopt technology into their processes and formats, provide a progressive solution.

These risk assessments are founded on quantitative data obtained from online sources. The Global Terrorism Database provides a comprehensive source from which data relating to terrorist incidents from 1970 can be accessed and used in the assessment of terrorism risk. This historical data, used in conjunction with real-time information, allows for the development of quantifiable and accurate risk assessments to be produced without the presence of subjectivity and bias.

A site's location, online presence, distance to previous terrorist attacks, similarity to previous target types, national or international status, location to high-risk assets, and existing security measures all become analysed on a far greater and more accurate scale. However, the adoption of technology into the risk assessment process goes beyond merely the type of data accessed and applied to assessments, as algorithms are used to calculate the threat terrorism poses, along with the vulnerability and resilience of a location to an attack. The risk that is assessed represents the risk itself, providing stakeholders true actionable insights and the ability to adopt effective security measures.

The ability to meet the growing demand for risk assessments is reliant upon its scalability. Where traditional assessments are limited to human schedules, assessments are, at most, conducted annually or irregularly. Comparatively, due to the automation of the assessment process of quantitative risk assessments, limitations based on time are diminished. Because of this, a greater number of risk assessments are able to be completed more regularly, and as needed rather than once per year. There is the possibility for each publicly accessible event to be assessed against possible terrorist threats and for security procedures and policies to be modified to suit the threat at that time.

Likewise, the ability to access risk assessments online increases their accessibility to a wider range of individuals. The opportunity to conduct terrorism risk assessments anywhere, at any time, and produce an accurate assessment of the risk is revolutionary. Its accessibility is further enhanced with the opportunity for any individual to conduct a qualitative risk assessment with the assistance of technology. The requirement to conduct a risk assessment becomes possible with the internet, transcending traditional expertise requirements. This increase in scalability and the democratisation of the process is one of the most significant advantages of qualitative risk assessments. It is through this scalability and democratisation that a sense of security awareness arises, and with greater security awareness among a growing population, security consciousness within the community is heightened.

To be risk aware is to understand the risks that exist, what impacts those risk can have, what security measures can minimise or prevent those risk from occurring, and enables looking for new risks which may arise. Quantitative risk assessments provide any person the ability to become risk aware. This is vital as it is not only within crowded venues that terrorist attacks occur, and the knowledge acquired by users of quantitative risk assessments can be implemented in not only professional environments, but also social.

The greater the amount of people who are risk aware means a greater community-oriented security consciousness. A terrorist is a risk that has the capacity to be more security conscious than its target, and will identify and act on vulnerabilities in security measures of a site to conduct as devastating an attack as possible. A terrorist's ability to be security conscious, paired with a lack of necessary security measures to detect and prevent a terrorist attack, transforms a risk to a reality.

The positive impact of quantitative risk assessments is felt further than the heightened individual security awareness. With greater accessibility, security consciousness within the collective community becomes possible, and resilience within the community to terrorism occurs. Quantitative assessments provide a tool that can be accessed as required by venue owners and operators, allowing for greater and more accurate designation of resources to effective risk mitigation measures.

By embracing technology into the risk management process, everyone can play a role in safeguarding the community from the threat of terrorism.

Traditional risk assessments produce uncertainty through the possibility of subjectivity, bias, gaps in knowledge and assumptions. Adopting technology into the risk management process eliminates the need for humans as assessors, which allows for risk assessments to be conducted on a greater scale than ever before. By taking away the need to have risk management knowledge to conduct a risk assessment, and by increasing the capacity of the risk management industry to conduct risk assessments more often, a greater amount of people can learn and identify what risks exist, how best to respond to those risks, and how to identify new risks. This heightened awareness is important in a society where terrorists are a conscious risk that maintains the ability to target vulnerable targets with gaps in security. By employing technology in the risk management process, a more security conscious society is created, resilient to evolving terrorism threats.

References

Manchester Arena Inquiry (2021) – Manchester Arena Inquiry. Available at: https://manchesterarenainquiry.org.uk/report-volume-one/part-6-smg-and-showsec-terrorism-threat-mitigation-measures/risk-assessment/ (Accessed: 06 October 2023).

Statement of Conflict of Interest

I authored an article on quantitative risk assessments and find it important to note that I am employed at Assess Threat, a provider who developed a quantitative terrorism risk assessment. Whilst I aimed for impartiality, I want to make aware to readers of this conflict of interest when reading the article and considering its message.

AUTHOR BIO

ZOE MILES

Zoe Miles is dedicated to topics of national security with a focus on terrorism and counterterrorism. Zoe works as the lead researcher for Assess Threat, an innovative counterterrorism software addressing ethical and broad-scale community resilience via automated data science. Zoe has contributed to research works including anti-vehicle ramming devices and shrapnel trajectory data from ballistic tests, and more recently, Martyn's Law. Her most recent work has been driven by terrorism-related incidents. Zoe holds a Bachelor of Arts majoring in Sociology and Security, Terrorism and Counterterrorism at Murdoch University and a Graduate Certificate in Intelligence Analysis at Charles Sturt University.

WICKED PROBLEMS - EMERGING AND STRATEGIC RISKS

BY DR PAUL JOHNSTON

The world has seen dramatic changes over the last 2 to 3 years, and I feel on safe ground to say that we will continue to see the same in years to come – after all, we live in a VUCA world. Indeed, VUCA has become the catch-cry for many a risk management professional in trying to manage and communicate the many issues that continue to arise.

But, is VUCA enough? We have recently seen a number of revisions to VUCA. It's no longer just **VUCA** – volatility, uncertainty, complexity, ambiguity. We have seen **VUCAD** – volatility, uncertainty, complexity, ambiguity, digitised. Then, we have also seen another version of **VUCAD** – volatility, uncertainty, complexity, ambiguity, disruption. Now, we have **D-VUCAD** – disruption, volatility, uncertainty, complexity, ambiguity, diversity.

I am not attempting to choose a favourite, but to highlight the fact that, as our long-favoured term of reference continues to change, the same is reflected in the issues at hand…issues that continue to appear, evolve, and shape shift – and it is these issues that I wish to focus on…the emerging and strategic risks.

So, what are the key emerging and strategic risks that we need to have on our risk radar?

A review of literature would indicate that the key risks in question encompass such diverse areas as:

- **Environment**
- **Technology**
- **Socio-political**
- **Public health**

These are the top emerging risk areas identified by publications such as the 2019 AXA & Eurasia Group "Future Risks Report", and the 2023 "The Global Risks Report" by the World Economic Forum, Marsh McLennan & Zurich Insurance Group.

In identifying these emerging risks, particular note was made of two characteristics, namely:

[1] the pace of emergence, awareness, and preparedness for risks; and

[2] the extent of risk interconnections and ripple effects of the same.

[1] PACE OF EMERGENCE, AWARENESS, AND PREPAREDNESS FOR RISKS

The very nature of emerging risks makes it especially challenging to predict the timing of their impact. Even if a risk has been identified and thoroughly assessed, there is still uncertainty as to its risk velocity (ie. how quickly it may develop), which may in turn then hinder timely risk mitigations and management.

The risks on which there is the most consensus—those which I have cited – are often thought to be more immediate in nature, meaning that their impact is likely to be felt in less than five years. This illustrates the importance of time horizon when evaluating a risk.

Further to this commentary, it is interesting to note the manner in which these risks have been seen to manifest in recent years, with recent publications by organisations such as the World Economic Forum, government agencies, and research institutions all identifying the same in their forecast reports as continuing to constitute emerging risks – particularly with regards to their ongoing evolution and expansion, for lack of a better term.

[2] RISK INTERCONNECTIONS AND RIPPLE EFFECTS

One of the major trends that was apparent is the increasing interconnection observed between risks and the extent of their ensuing ripple effects.

Indeed, as we all are aware, risks also influence each other, sometimes creating vicious circles – risks and a resulting relationship that we have become accustomed to call "wicked problems". The last decade has been marked by examples of new and evolving risks that have and continue to emerge from complex systems – systems such as the global financial system, biodiversity and ecosystems, and the international trade supply chain.

Commentary that *"interconnected risks can trigger unexpected large-scale changes to complex systems, or imply uncontrollable large-scale threats to them"*, remains valid as a statement today as we look forward to the next 5 years.

I would like to now briefly explore each one of these 4 areas.

ENVIRONMENT

Risk #1: Climate change

Climate change is consistently identified as the top emerging global risk, with natural resource management and pollution also being within the top 10. Many environmental risks, such as climate change and biodiversity loss, are caused or worsened by human activities, and in turn these interconnected risks have far-reaching consequences for society. Such risks are often considered to be more immediate than others, with tangible effects already being identified by researchers and members of industry.

Particular attention is given to the physical risks stemming from a changing climate, namely the increased exposure to and changing patterns of extreme weather events and natural disasters – each of which are perceived as having more tangible effects than financial risks or liability risks related to climate change.

Risk #5: Natural resources management

That said, significant attention is also being given to those risks presented by natural resource management – with it being observed that the same is already having measurable impacts – in particular with regards to (i) the loss of biodiversity, unsustainable land use, deforestation, and desertification, and (ii) the over-consumption of natural resources.

Similarly, concerns are also continuing to be voiced about the relationship between population growth and unsustainable use of natural resources. Even though global population growth is slowing down, it is unlikely to stabilize by the end of the century, and the concern is that this will amplify environmental risks and heighten the pressure on natural resources management.

Risk #7: Pollution

Pollution also continues to warrant concern and discussion, and has the most consensus about the timing of its impact, with the largest number of risk leaders considering it already present. Air, water, and soil pollution remains the main concerns, but plastic pollution and waste management is rapidly gaining momentum.

TECHNOLOGY

Risk #2: Cybersecurity risks

Cybersecurity risks continue to be the second-most important emerging issue highlighted by risk leaders, which comes as no surprise given the recent rise in cyber-attacks, with this being paired with the potential economic impact of a successful large-scale cyberattack – albeit on industry, critical infrastructure, or the wider community. In this sense, the main concerns appear to relate to the potential shutdown of essential services and critical infrastructure by malicious actors, cyber extorsions and ransomware, as well as identity theft. However, most specialists agree that the full-scale implications of cyber threats are yet to be experienced, especially as technology continues to rapidly evolve.

Risk #6: AI and big data

Looking beyond the traditional technologies, however, we can see that a larger set of risks at the intersection of technology and society are rapidly emerging – those associated with AI (artificial intelligence). The disruptive potential of associated new technologies, which could play a role in the transformation of existing economic and social structures, continues to be discussed with increasing frequency and concern with regards to the expected significant ripple effects from the technological sphere to the socio-political sphere.

SOCIO-POLITICAL

Risk #3: Geopolitical instability

Geopolitical instability continues to increase in prominence, with the rise of nationalism and populism, and tensions between nation states being the main sources of concern.

Risk #4: Social discontent and local conflicts

Similarly, the concerns associated with the risk of social discontent remains high, with income gap and wealth disparities to be the amongst the most worrisome concerns, as were migration and territorial concerns.

Risk #9: New threats to security

New threats to security has seen a levelling out, if you like, with this being attributed to the downward trend in terrorist attacks in most regions. That said, risk leaders are equally worried about evolving terrorist attacks by smaller groups and lone wolves, and of cyber warfare triggered by nation state-sponsored cyberattacks.

Risk #10: Macroeconomic risks

Although at the lower end of the top 10, macroeconomic risks are impacted by the other risks highlighted prior to this – namely, climate change, geopolitical instability, and social discontent.

PUBLIC HEALTH

Risk #8: Pandemics and infectious diseases

It is interesting to note that only 5% of risk leaders regarded a medical/public health risk as being a top emerging risk in as recently as 2019. This, however, has now changed with regards to pandemics and infectious diseases in particular – with this change being attributed specifically to the COVID-19 pandemic.

Indeed, this also has seen a heightened level of risk awareness and appreciation in relation to pandemics and infectious diseases, with the main areas of concern relating to three main areas:

- new strains of infectious diseases—for example, COVID, Ebola and Zika
- antimicrobial resistance and “super bugs”
- changing patterns of infectious diseases caused by the impact of climate change and global travel.

ONTOLOGY BASED APPROACH

As we can all appreciate, each of these areas represent a potential rabbit hole that we can willingly or unwillingly do down. But, in order to "manage" these risks, let us pause and ask ourselves a few simple questions. What do they have in common? What is a trait that each one undoubtedly shares?

Each is a wicked problem, intertwined with at least one other risk area.

My students and colleagues will know that I love to use the word "ontology", and that I have cheekily asked them to call themselves "risk ontologists" on many occasions. But this is not as light-hearted a request, as it have may sounded in the past.

Ontology is a formal system for identifying and modelling concepts, and their relationships or dynamics. It refers to a system of logic whereby we develop and attribute meaning to elements around us and how they interact.

As risk professionals, and indeed as risk leaders, we need to be ontologists – we need to not just understand, but to truly appreciate and communicate, the inter-relatedness of these issues…the fact that they are indeed wicked problems.

We also need to be mindful of our approach to managing issues, such as wicked problems, in the VUCA world in which we find ourselves. That is, we need to change our mindset of attempting to control the flow of what may be a raging torrent, to acknowledging the reality of the situation, and look to ways by which to work with, or around, the same flow. We need to adopt the mindset of "control what you can; manage and influence that which you can't". This is my mantra.

Wicked problems are typically defined as problems that are difficult or impossible to solve because of their complex and interconnected nature. Furthermore, they lack clarity in both their aims and solutions, and are subject to real-world interpretation and constraints which hinder risk-free attempts to find a solution.

So, with this understanding, why do we continue to deploy significant resources on aspects we cannot control? Let's turn our focus to controlling what we can, and managing and influencing that which we can't. Rather than accepting defeat, preparing for a prolonged engagement, and/or actually creating more problems, let's change strategy and tactics.

To illustrate my point, let's examine one of the four risk areas again, namely that of Environment, but with more specificity.

ENVIRONMENT

Of the environmental risks, I am casting a lens on natural disasters, bush fires in particular, to provide an appropriate example.

When we discuss bushfires, or wildfires, we can see the very nature of wicked problems at play, with there not just being one causal factor, nor a one-size fits all solution.

Indeed, some of the factors that contribute to bushfire risk levels and behaviour include:

- Climate change and weather patterns
- Fuel load management
- Urban rural interface expansion
- Design standards and maintenance
- Emergency services delivery model and community awareness
- Human factor

Climate change and weather patterns: The first topic that gets raised when discussing bushfires is inevitably climate change and weather patterns. Indeed, we are seeing changes in climactic conditions and patterns, with both contributing to the ideal conditions for increased bushfire risk levels and intensity.

That is, we have seen increases in, not only temperatures, but also the frequency and duration of these higher temperature weather events; similarly, we have also seen changes in relative humidity levels, with both factors contributing directly to conditions where a bushfire is more prone to ignite, as well as to rapidly increase in intensity, as the actual fuel itself is typically drier and hotter, both of which combine to increase the likelihood of fire ignition and spread.

Then we factor in the increased rainfall that has the real potential to increase fuel loads (ie. grass, trees etc) growing in bushfire prone areas. Rain is an interesting element in the equation, as we really can't win. If we receive excessive rain in the off-fire season, more fuel will accumulate. If we don't, the existing fuel will dry out and become more flammable. It's all a matter of timing and is something that we have no control over.

Fuel load management: Turning our attention to fuel load management, the key is to reduce the density and/or the distribution of fuel loads. This can be done via prescribed fire programs, which involves the periodic, intentional, and controlled burning of fuel in select areas. We know this has a number of benefits, ranging from fuel management to actually assisting a wide range of flora to maintain themselves and rejuvenate. The Australian environment is literally designed to burn, and fire is part of the natural ecosystem.

The key is intensity and frequency. Most flora and fauna will survive high frequency-low intensity fires, as opposed to low frequency-high intensity fires. Hence the need for prescribed fire programs. Called mosaic burn programs, selected areas are burnt at differing time frames, as different species have different rejuvenation periods. Intense fires can change the entire ecology and biodiversity of a given area via both changing the profile of flora present, as well as by potentially changing the chemical profile of soil.

Indeed, suitable fire breaks can be established around houses and other infrastructure via the strategic use of prescribed fire programs, as opposed to simply reverting to creating mineral fire breaks – which themselves can lead to soil erosion.

Urban rural interface expansion: What is the difference between a bushfire being a hazard or a risk? Realistically speaking, a bushfire is a hazard that arguably only becomes a risk when we interact with it. As mentioned earlier, bushfire is a natural part of the Australian ecology – it can be argued that it only becomes problematic when it interacts with communities.

This introduces the issue of the urban-rural interface – that is the area where communities interact with the environment, typically in rural or semi-rural areas. It is where we see communities and developments expanding into what were traditionally bushland or otherwise natural environments.

It is where we are placing properties into areas where bushfires transition in their status from hazard to risk. In this sense, it is a matter of balancing the desired lifestyle with effective bushfire risk management. It could be said this is a wicked problem within a larger wicked problem with the main issues being fuel load management, infrastructure design, and community-based emergency management – the latter of which remain to be discussed. But we can start to see the manner in which each element is inter-related with another.

Design standards and maintenance: The standard AS 3959 specifies the construction requirements for buildings built in bushfire-prone areas in order to improve the buildings resistance to bushfire attack including from burning embers, radiant heat and flame contact or a combination of these. It encompasses physical design, construction materials, and the establishment of asset protection zones (forms of firebreaks) as determined by the relative Bushfire Attack Levels (BALs). It is considered best practice and is a requirement when constructing any building or structure in a bushfire prone area – forming an element of the National Construction Code.

Its strength is the level of detail and guidance it provides. Its limitation, as with any building code, is the degree to which the "approval" standards are maintained after occupants actually move in, both commercial and domestic. Indeed, a common observation is that asset protection zones and gutters are not maintained, with this being attributed to complacency, a lack of risk awareness, or the perception by some that such practices are not needed as they undertook a "tree change" because they wanted a "bush" lifestyle as opposed to a "suburban" style existence.

Emergency services delivery model and community awareness: The service delivery model for fire services in rural areas is a mixture of rural fire service volunteers and/or part-time auxiliary fire fighters – depending on factors such as population, risk levels and available support services. However, regardless of whether the volunteer of auxiliary service provision model is in place, there seems to be fairly consistent observation being reported. Although the numbers of people living in rural-interface areas is indeed increasing, we have not seen the same growth in residents joining their local fire brigade. Hence we have a deficit in response capabilities that is arguably increasing.

Similarly, with the influx of people seeking a "tree-change", there has been observed a significant increase in the percentage of residents in urban-rural interface areas that do not have a developed sense of bushfire awareness, nor appreciation. Indeed, many have never experienced a bushfire in real-time, nor have they learnt the indicators or factors involved in determining relative bushfire risk levels.

Therefore, whilst we are promoting families to move out to rural areas, as a means by which to relieve the demands on big city infrastructure and to financially support rural communities – both of which are indeed beneficial – the same actions are arguably increasing the bushfire risk profiles of the very same communities.

Human factor: Risk management, and the risk perception/s it is based on, is highly subjective in nature. It calls on the human element to obtain, interpret, analyse, and act on, available data. Not to be judgemental, but it is here that we most often see wicked problems manifest themselves.

We attribute value to certain elements or factors, and as these values are subjective in nature and arguably inconsistent across individual persons and groups, we arrive at the very core of wicked problems – namely the lack of clarity and being subject to differing interpretation/s and priorities.

So, let's revisit the previous elements discussed, doing so through though the "human factor lens", and by discussing how they manifest themselves in real world terms.

Climate change and weather patterns: Climate change and weather patterns are not things we can manage, but are subject to. So, in the context of this discussion, it will be considered in that manner – namely as an influencing factor that we don't fully understand, cannot predict with absolute certainty, and cannot control. It is in itself a wicked problem that impacts directly on all aspects of bushfire risk management, particularly that of fuel load management.

Urban rural interface expansion: We continue to see people seeking a "tree change", moving away from urban areas to more rural or semi-rural areas – the urban rural interface – with this being actively promoted and encouraged by different levels of government, as well as by private sector developers.

This has seen an increasing population being potentially placed in harm's way. Without being too melodramatic, we now have larger populations moving to areas which have a higher bushfire risk profile than suburban areas, and in doing so, we are placing communities in locations where there has traditionally been undeveloped land. We are placing communities in locations where a bushfire was formerly a hazard, but now (by their very presence) the same potential fire now represents a risk.

The question then beckons as to the increased bushfire risk that is often attributed to climate change. Is climate change playing as large a part as some suggest? Or, is it because we are placing communities in locations that had previously been undeveloped land? Where fire was once considered a hazard that could be monitored, as opposed to now being a risk that that has to be more directly managed. Are we attributing this to climate large disproportionally, due to a casual relationship rather than a causal relationship? On a side note, should the same type of question be asked of another natural disaster – that of floods?

I am not offering an answer perse. What I am offering is my mantra "control what you can, and manage and influence that which you can't:. In this sense, we cannot control climate change, not in terms of immediate changes of note. But we can control the expansion of the urban rural interface. In doing so, can we address two aspects of this wicked problem, by also managing/influencing the potential impacts of climate change on bushfire risk?

Design standards and maintenance: Directly linked to the expansion of the urban rural interface, is the implementation and maintenance of standards defined by the AS 3959 standard after buildings are completed and commissioned. This is something that we can control, and indeed can continue to influence post construction.

The central issues here relate to maintenance – of fire breaks, roof gutters, the general condition of the structure, and the placement of compromising items in proximity to the structure itself.

Sounds simple enough? Maybe. But, the conflicting mindsets and perceptions or expectations are where the real wicked problem emerges. People move to rural areas

as part the “tree change”, opting for the “bush” lifestyle over the traditional urban existence, and herein lies the challenge, and I will call on a consulting experience I had some years ago to illustrate.

In a previous role, I was involved with providing bushfire risk management advice to a Victorian government agency in the aftermath of the devastating bushfires they experienced in 2007. As part of this, the project team visited a number of regional areas devastated by the fire event. During one such visit, only 6 months after the worst bushfire – what many called a fire storm – that local residents had ever experienced, we encountered what you would have expected – a very risk aware and risk averse community where the houses followed the AS 3959 standard to the letter.

However, 6 months after that, only 12 months after the firestorm event, we returned to the same areas. What did we find? A number of residents (in one town that stands out) had reverted to pre-fire behaviour. In many instances, the fire breaks were no way near as well maintained, items were stored near houses, flammable trees were noticed as having been planted near houses.

When I asked a number of residents as to why, I received a number of responses, but this one stayed with me...."If I wanted to do all that, I would have stayed in Melbourne..... we moved to the bush to enjoy a bush lifestyle, and to live in the bush.....what’s the chance of it happening again?”

And, there we have the conflicting mindsets and perceptions/expectations that underpin the wicked problem. What we want vs what we need to do to mitigate our risk exposures. Opposing goals and objectives.

Local authorities find themselves, in instances such as this, struggling to enforce/encourage feasible solutions due to the opposing mindsets and interpretations of given scenarios. One decision/solution is in direct opposition to the other. One is promoting bush lifestyle, and the other, bush safety – concepts which appear to be oppositional in their views and requirements. Dammed if you do, dammed if you don’t.

Interestingly, however, we have observed quite the opposite in other parts of the country, where in a number of instances, houseowners have been fined by their local council for cutting down established trees to form an appropriate asset protection zone/firebreak. Here, we have the homeowner wanting to ensure they can safely enjoy the bush lifestyle. Whereas the council appears to be preventing it, saying that such trees cannot be removed, in direct contradiction to the AS3959 standard.

Which one is correct? In each of these cases, the solution for one creates a problem for the other. Indeed, we can even see the roles reversed in these simple examples. Sound like a wicked problem?

Fuel load management: The science at the centre of these example relates to fuel load management. Rather than repeating myself, however, let’s turn our focus to yet another area where we find a demonstrable wicked problem – national parks, and nature reserves.

There has been, and continues to be, a source of some conflict between bushfire services and some national park agencies – that of prescribed fires as a means of fuel load management. Indeed, we have seen the same occurring overseas in other jurisdictions.

So, some statements of facts:

- Most flora and fauna will survive high frequency-low intensity fires, as opposed to low frequency-high intensity fires.
- Bushfire services want to conduct prescribed fire programs to reduce fuel load accumulation.
- National park agencies don’t want prescribed fires, in order to maintain the totality of biodiversity.

Both can refer to science in support of their case. Both have precedence that they can cite. Which one is absolutely right? Which one is absolutely wrong? In this dilemma, we find a wicked problem.

Emergency services delivery model and community awareness: We close off this example by revisiting the emergency services delivery model and community awareness in uran-rural interface areas.

The wicked problem is this – we are promoting families to move out to rural areas, as a means by which to relieve the demands on big city infrastructure and to financially support rural communities – both of which are indeed beneficial. However, the same actions are arguably increasing both the bushfire risk profiles of the very same communities, and the need for resources that will be required to conduct effective bushfire risk management. In each instance, it could be said we are reducing one at the expense of the other.

WHAT CAN WE TAKE FROM THIS?

I chose bushfires as the example for wicked problems as it is a concept we can all appreciate the significance of, whilst also possessing a range of dynamics that exist just below the surface.

Indeed, in many aspects there are things we simply cannot control, but feel the need to exert effort to try. We can see the frustration of trying to control the things that we cannot, and the potentially devastating impacts if we sit idly by. And that is the real challenge of wicked problems – the urge to control what we cannot, whereas perhaps we are better to manage and influence those impacts that we can.

I commenced this paper by discussing emerging and strategic risks – and quickly equated them to being typical of wicked problems due to the VUCA world in which we live. Indeed, their complexity and inter-relatedness made it a logical leap. Similarly, as with wicked problems, emerging and strategic risks are both relative terms. Each may be defined a certain way, but mean something different to each person and organisation in real terms – and that defines the true nature of the emerging and strategic risks (or wicked problems) that we are, and will continue to, be confronted with.

If we don't truly understand and appreciate the inter-relatedness of issues, such as those cited…if we don't adopt a more ontology-based approach that acknowledges the potentially wicked nature of these (and other) issues… we will not be able to address such issues, let alone understand and identify the trends that may be on the horizon.

Bibliography

AXA & Eurasia Group (2019). Future Risks Report October 2019.

IRGC (International Risk Governance Council) (2015). IRGC Guidelines for Emerging Risk Governance: Guidance for the Governance of Unfamiliar Risks.

PWC (PricewaterhouseCoopers International Limited) (2022). 2022 Global Risk Survey: Embracing Risk in the Face of Disruption.

World Economic Forum, Marsh McLennan, SK Group & Zurich Insurance Group (2021). The Global Risks Report 2021, 16th Edition: Insight Report.

World Economic Forum, Marsh McLennan & Zurich Insurance Group (2023). The Global Risks Report 2023, 18th Edition: Insight Report.

AUTHOR BIO

DR PAUL JOHNSTON

Editor of the ISRM Journal, Dr Paul Johnston is a Lead Risk Consultant and Behavioural Scientist with Risk 2 Solution, and is the Academic Lead at the Institute of Presilience, as well as being the ISRM ANZ Research Lead. He holds a PhD in Public Safety Risk Management, a Graduate Certificate in Occupational Hygiene Engineering, and a Bachelor of Behavioural Science. With 30 years of HSES (Health, Safety, Environment & Security) Risk Management experience in both the public and private sectors, Paul has provided operational, management system consulting, research & analysis, and training services to a wide range of industry groups throughout Australia and internationally.

Connect with Paul on LinkedIn

NAVIGATING RISK LIKE A PRO: LEADERSHIP AND LEARNING

BY KERRI STEPHENS

Finding the delicate equilibrium between proactive preparation and real-world adaptability is a challenge that seasoned professionals understand intimately. Being a risk leader is not just about writing reports and recommendations from afar; it's about embracing the uncertainty and partnering as one of the change-makers in your organisation.

Having empathy, genuine curiosity (I often think other people's roles are so much more interesting than my own) and a continuous improvement mind-set has served me well. You're welcome to take and adapt these insights I've curated below, to suit your own unique situation. All I ask in return is that we, as risk professionals keep it real, by sharing what works and what we'd do differently next time.

THE EXECUTIVE TIME-CRUNCH

- *Understand their world:* Executives operate in a time-poor realm, juggling a myriad of responsibilities. Recognising their priorities, challenges, and drivers is paramount. Speak their language – tailor your messages to resonate with their priorities, and align risk with their strategic goals.

- *Cut through the noise:* Crafting reports for the board and executives requires a surgical approach. Cut to the chase—highlight the headline elements. Connect strategy and risk, focus on potential impacts and recommended actions. Present a snapshot that guides decision-making without overwhelming them with unnecessary details.

PAY HOMAGE TO DETAIL LOVERS

- *Respect the detail enthusiasts:* Within every executive team, there are those who thrive on details. Acknowledge and respect their inclination towards thoroughness. They are the gatekeepers of precision and provide invaluable insights.

- *Balance the negativity bias:* Detail-oriented individuals often have a heightened negativity bias. When addressing risks, it's crucial to balance caution with optimism. Effective risk management enables the organisation to navigate the threats and vulnerabilities with confidence.

TWO SIDES OF THE SAME COIN: RISK AND STRATEGY

- *Customised understanding:* Different audiences perceive risk differently. For the board and executives, highlight how risk and strategy are not adversaries, but the yin and yang of organisational success. A seamless integration of both is essential for effective decision-making.

- *Strategic decision-making:* Your role as a risk manager transcends reporting risks; it's about delivering the right data at the right time. Tailor your approach to present concise, impactful data in a digestible format to guide strategic decision-making.

FUTURE-STATE VISION, COMPLETE WITH STEPPING STONES

- *Clear vision:* An unwavering focus on the future state of embedded risk management is crucial. What does success look like for your organisation, and how will you get there? Communicate this vision clearly (and often) to inspire commitment and engagement.

- *Define stepping stones:* Embedding risk management is a meticulous, step-by-step process. Pay attention to the details and clearly outline the practical stepping stones from the current state to the future. To do this well, you must understand your organisation's unique DNA and culture.

- *Balance the sprint and the marathon:* Despite the urgency, keep an eye on the end game. Establish the necessary training, resourcing, and support team around you. Embedding sustainable solutions is not a sprint; it's a marathon requiring endurance and a strategic mindset. Your vision and attitude are contagious and sets the tone for the entire organisation.

LEAD BY EXAMPLE

- *Acknowledge imperfections:* Set the stage by acknowledging when you could have done better. Embrace vulnerability and demonstrate that learning is a continual process.

- *Challenge your own perspectives:* Don't shy away from admitting when you've had to re-assess your own perspectives. Adapting to new information is not weakness; it's a strength. Recall tough decisions and be willing to pivot strategically.

- *Model behaviours:* Embrace diversity, challenge the norm and be the driving force behind a culture that learns from both successes and failures.

PARTNERSHIP POWER MOVES

- *Risk management partnerships:* Work in tandem with leadership. Dare to be their ride-or-die, or partner in crime. Then you're not seen as the bearer of bad news; you're just as invested, right there in the ring, navigating through uncertainty together.

- *Strategic positioning:* Find that sweet spot where you're a part of the decision-making process, not just an outsider dictating from afar. This is where leadership and learning truly shine.

THE FENCE IS UNCOMFORTABLE ANYWAY

- *Importance of taking a position:* Most of us have been there, straddling the fence isn't sustainable. Be flexible, but know when you need to hold your ground. Taking a stance is part of leadership.

- *Change is the only constant:* Agility is key. Change is constant and being willing to adapt is the cornerstone of successful risk management leadership.

TWO KEY TAKEAWAYS FOR THE RISK LEADERS OF TOMORROW:

1. ***Embrace vulnerability:*** Be vulnerable enough to acknowledge those areas that require improvement. Be honest in your appraisal of risk maturity and chart a clear course.Your leadership team will respect you more for it.

2. ***Take a stand, adapt as needed:*** Don't fear taking a position. It's part of the leadership gig. Just remember, adapting to new information is not a U-turn; it's a strategic pivot that will serve your organisation well in the future.

Running the risk management marathon requires sustained performance - understanding your audience, acknowledging diverse perspectives, and customising information for maximum relevance. It's about balancing the tactical with the strategic, the headline with the details, and the present with the future.

AUTHOR BIO

KERRI STEPHENS

Kerri Stephens is an accomplished Risk and Resilience professional with more than two decades of experience. A life-long learner, Kerri is a graduate of the Australian Institute of Company Directors (GAICD) and holds a Graduate Certificate in Psychology of Risk, highlighting her steadfast commitment to understanding the human element in risk management.

She is an active contributor to the advancement of risk management practices and was recognised as a finalist for Risk Manager of the Year by the Risk Management Institute of Australasia (RMIA), reflecting her dedication and achievements in the field.

Her career has spanned diverse sectors in London and Australia, including insurance (Marsh - Adelaide and London), agriculture (Elders Rural Services Aust Ltd), tourism (Journey Beyond), government critical infrastructure (SA Water), and for-purpose healthcare (RFDS). Kerri serves as the Principal Advisor – Risk and Assurance for Royal Flying Doctor Service SA/NT and is the ISRM South Australian State Chair.

CALL FOR PAPERS

ISRM GLOBAL JOURNAL

We are calling for papers from risk and resilience management professionals who would like to share their experience and insights with their colleagues. Papers will be chosen based on the grounds of relevance, quality and significance. Articles may also be chosen, at the editor's discretion, for inclusion in future journal issues.

TYPES OF PAPERS

OPINION PIECE

- To be original in content, and to provide appropriate references where other content is indeed included. The responsibility for originality and plagiarism issues remains with the author, not the Institute of Strategic Risk Management (ISRM).
- Make a contribution to business practice, and have not been previously published elsewhere.
- Provide opinions and insights, as well as practical information on how to deal with contemporary risk and resilience management issues.
- Not be commercial in nature (i.e. advertising or publicising a service or product)
- Author/s to include a statement regarding conflicts of interest.
- Papers should be submitted in Word and double spaced.
- Harvard referencing should be utilised as appropriate.
- Suggested paper length: 800 to 1500 words

PEER-REVIEWED ARTICLE

All of the guidelines above, plus:

- Answer the “so what” question.
- Address the implications/impacts for business practitioners, supported by appropriate practical examples (where applicable).
- Suggested article length/s:
  - Empirical article <5,000 words excluding title page, abstract & references
  - Review <4,000 words excluding title page, abstract & references o Meta-analysis <4,000 words excluding title page, abstract & references
  - Case history <3,000 words excluding title page, abstract & references

BEFORE SUBMITTING

Please ensure you have the following before submitting:

- A suitable high-definition professional headshot;
- A brief biography (approx. 100 words); and
- 2 or 3 quotes/extracts from the paper that best captures its key points.

HOW TO SUBMIT

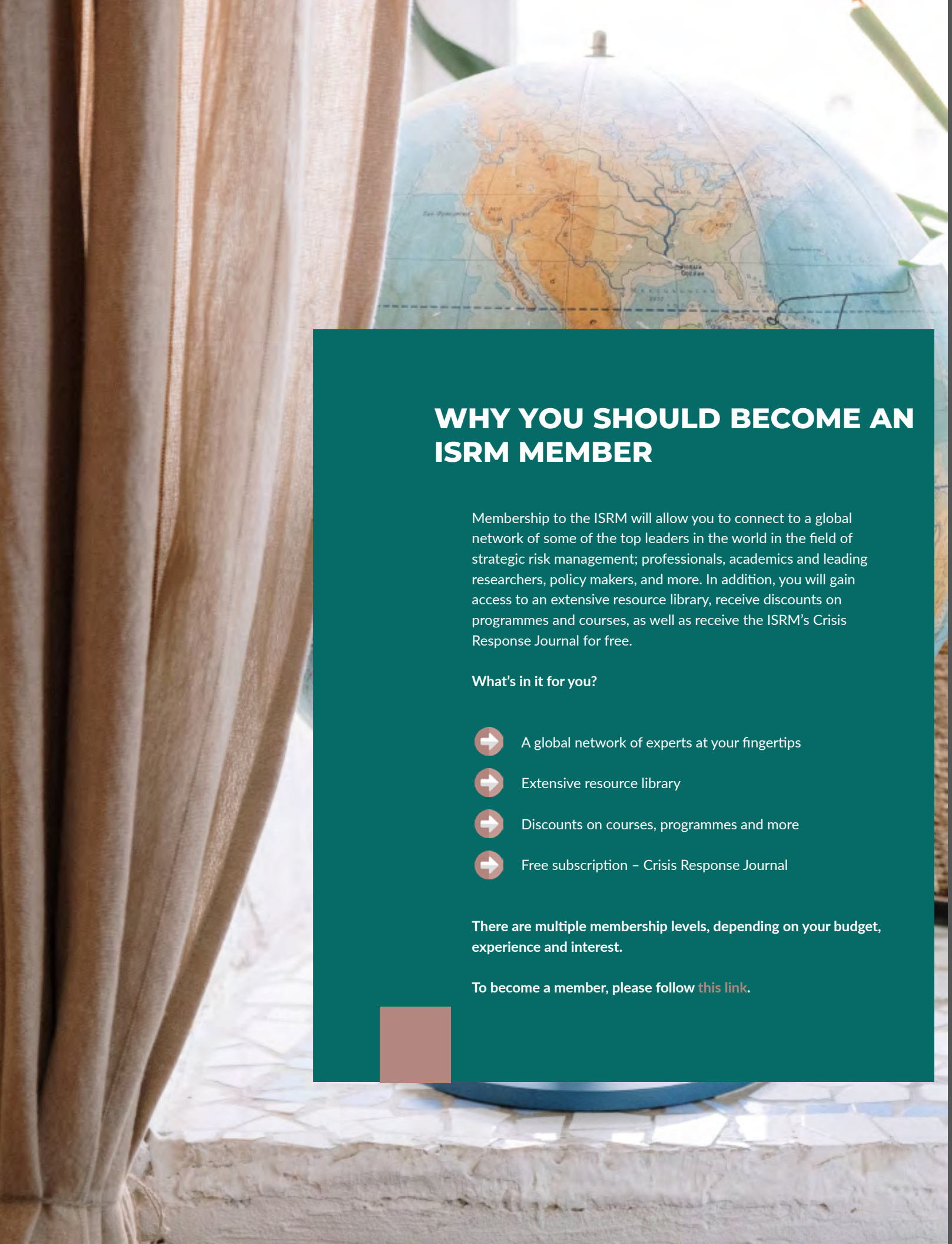
Complete the submission form at www.isrm.org.au/call-for-papers

SCAN ME

ABOUT THE ISRM

The Institute of Strategic Risk Management (ISRM) has been established in order to create a global centre where practitioners, academics and policy makers can come together to share information, help progress and promote the underlying understanding and capabilities associated with strategic risk and crisis management, and develop their own personal and professional networks.

The ISRM has experienced tremendous growth since 2020 due to its global network of experts, excellent educational output and opportunities, and its unique and collaborative environment.



WHY YOU SHOULD BECOME AN ISRM MEMBER

Membership to the ISRM will allow you to connect to a global network of some of the top leaders in the world in the field of strategic risk management; professionals, academics and leading researchers, policy makers, and more. In addition, you will gain access to an extensive resource library, receive discounts on programmes and courses, as well as receive the ISRM's Crisis Response Journal for free.

What's in it for you?

- A global network of experts at your fingertips
- Extensive resource library
- Discounts on courses, programmes and more
- Free subscription – Crisis Response Journal

There are multiple membership levels, depending on your budget, experience and interest.

To become a member, please follow this link.

ISRM

INSTITUTE OF STRATEGIC RISK MANAGEMENT

For more information on the Institute of Strategic Risk Management (ISRM), please visit www.theisrm.org or contact info@theisrm.org.