

ISRM

AUSTRALIA / NEW ZEALAND

INSTITUTE OF STRATEGIC RISK MANAGEMENT



ISRM ANZ JOURNAL 2022

Autumn Edition

PUBLISHING INFORMATION

First published in Australia in 2022 by ISRM Australia and New Zealand (ANZ)

This work Copyright © ISRM ANZ 2021-2022

Other than brief extracts for research and review, no part of this publication may be produced in any form without the written consent of the Publisher.

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

ISBN 978-1-925821-12-3 PB
ISBN 978-1-925821-39-0 eBook

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 the 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. The ISRM 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.



A WORD FROM



DR GAV SCHNEIDER
REGIONAL CHAIR ANZ

It has been a challenging period of late where risk exposure, leadership, decision-making, and performance have all been impacted in so many ways. The world we live in continues to change rapidly around us, and whilst this change brings new threats, it also brings new opportunities to the fore. The challenge is to effectively manage the downside, while capitalising on the upside – which is far easier said than done. Our goal at the ISRM ANZ Chapter is to provide thought leadership around strategy, risk, and management – to not just survive but to thrive. We are very grateful to our contributing authors for their submissions to this, our second Journal, sharing their thoughts and ideas of what is happening, and what we need to be thinking about. I am sure that you, as a reader, will gain many insights. Even if you take just one idea away, we feel our objectives are being achieved.



DR PAUL JOHNSTON
JOURNAL EDITOR

With this being my first issue as Editor, I would like to thank my predecessor Ron Amram, who has had to step aside due to other obligations, for the way in which he set the tone for the journal. Indeed, the ISRM Australia and New Zealand Chapter Journal provides an ideal opportunity for risk practitioners and academics to share their thoughts, insights, and experiences with fellow “risk types” – which we know are truly multi-disciplinary in nature.

This issue is a collection of opinion pieces on issues relating to strategic risk management in the challenging environment in which we find ourselves. Ranging from SoCI (Security of Critical Infrastructure) and legislation, to leadership and risk-based decisions, this issue provides a snapshot of the contemporary issues being managed. The next issue is scheduled for an August/September release, and I call on industry professionals to consider submitting an article for publication.

I would like to conclude by quoting Ron Amram’s sentiments in thanking “...all of the experts who contributed their time and embodied the spirit of the ISRM by coming together to share knowledge and expertise in a collaborative and supportive format”.



personal benchmarking for
assesses security management
contributions to the security
credibility, better care
nals belong.

EXECUTIVE DIRECTOR, ISRM GLOBAL
WELCOME

When the Australia Chapter of the Institute of Strategic Risk Management was launched in October 2019, little did we know the epoch-defining changes that were just around the corner. Of course, Australia was already suffering from significant challenges, not least a continent-wide drought, bush fires that were threatening the main urban areas, as well as creating a pollution levels that were impacting on both the health of the urban population as well as the ability to maintain basic functions within those urban environments, and the wider geo-political issues of immigration, both legal and illegal, geo-political instability, and the increasing impacts of climate change and global warming on every aspect of our lives.

It is a reflection of the diversity and richness of the ANZ risk and crisis management community that, by the end of the dinner held to launch the Australian Chapter, we had received support to open State Chapters in all of the major cities as well as in New Zealand.

In the two and a half years since then, the ISRM ANZ Chapter has been a leader in developing local and regional relationships with major government agencies and representative organisations, hosting conferences and webinars, as well as establishing programmes that act as a

platform for the regional risk and crisis management community to use to develop their own relationships and activities.

This journal reflects all the qualities that the ISRM embodies. It is open to all, representing a wide range of views on issues that are both critical and time sensitive, and which in some way impact on the lives and well-being of every level of our society, from the national and regional, to the local and personal.

The ISRM was established in order to create a space where practitioners, academics and policy-makers could come to gather to have meaningful dialogue and interaction concerning the most challenging issues of the day. This journal reflects those values in every page, and I am delighted to have the opportunity to write this foreword.

I hope that these articles will be of interest, encourage dialogue, support collaboration and, in ways both great and small, make their own contribution to the continued development of the ANZ strategic risk and crisis management community – and in turn, to contribute to the wider global community that we are all part of.

Kindest regard,

Dr David Rubens
Executive Director, ISRM Global

TABLE OF CONTENTS

- 8** MEET OUR TEAM
- 15** STRATEGY ON A PAGE
- 16** UPDATED SECURITY OF CRITICAL INFRASTRUCTURE LEGISLATION – ARE YOU READY, PERSONNEL-WISE?
DR PAUL JOHNSTON AND GARY SANDERFIELD
- 20** PRESILIENCE AS A UNIFYING PRACTICE TO CHANGE, THRIVE, AND GROW
DR GAVRIEL SCHNEIDER AND LISA YOUNG
- 24** LEADERSHIP SURVIVORS DRIVE ORGANISATIONAL SUCCESS
LEANNE CLOSE
- 28** FATCA ENFORCEMENT – THE NEXT BIG RISK TO AUSTRALIAN BUSINESS?
KRISTINE SEYMOUR
- 30** PATCHING PEOPLE
JOE SAUNDERS
- 34** USING RISK INTELLIGENCE TO MAKE A FAILURE RESILIENT ORGANISATION IN A VOLATILE, UNCERTAIN, COMPLEX AND AMBIGUOUS WORLD
JAMES JORDAN
- 42** RED PILL. BLUE PILL. (PART 1)
DR PAUL JOHNSTON
- 46** STRATEGIC OPERATIONS IN THE NEW NORMAL
RON AMRAM
- 48** CONTEXT FOR THE 21ST CENTURY
JULIAN TALBOT

MEET OUR TEAM



DR DAVID RUBENS

EXECUTIVE DIRECTOR, ISRM GLOBAL

Dr David Rubens established his first consultancy in 1992, is a Chartered Security Professional (CSyP) and has served two terms as a main board director of the UK Security Institute. He holds a doctorate in security and risk management from the University of Portsmouth. His thesis explored non-hierarchical models of strategic management at the extremes of organisational complexity, including issues of capability development, decision making and multi-agency interoperability in hyper-complex situations such as natural disasters, corporate failures and government-level crisis management scenarios. David established ISRM in October 2018. Today it has become recognised as a major institute in the sector, with chapters across SE Asia, the Middle East, USA, Australasia and Eastern Europe, and a vibrant network of academic, research and think-tank institutions.

DR GAV SCHNEIDER

REGIONAL CHAIR

Dr Gav is the Group CEO of Risk 2 Solution and is an acknowledged subject matter expert on human centric and integrated risk management. He has a broad background in safety and security, emergency management and incident response, with extensive senior level management and leadership experience. He has led numerous, high-level consulting and advisory projects and has two decades of Operational Specialised Risk Management, Cultural Change, Security and Safety experience in over 16 countries. Dr Gav has a National Security Clearance NV1 and is a fellow of ARPI, ISRM, GIA, IML as well as a RSecP and CPP. He is considered Australia's leader in the field of Psychology of Risk.



JOE SAUNDERS

REGIONAL VICE-CHAIR

Joe is a dedicated risk management professional with a passion for the study of aggression and violence management. A successful sporting career in the martial arts led Joe into the private security industry where he quickly learned about the challenges in dealing with real aggression, operating within critical legal, ethical and political frameworks. Joe would go on to specialise in aggression management within the healthcare and social service environment.

Joe is a gifted and dynamic presenter, educator and training designer with a knack for communicating a sometimes difficult subject to professionals and laypersons alike. He is an associate of ARPI, ASIS International and the International Law Enforcement Educators and Trainers.

GARY SANDERFIELD

DIRECTOR OF GOVERNANCE AND PARTNERSHIPS

Gary is a highly experienced risk and leadership specialist with over 20 years of experience in operational risk, enterprise risk management and organisational redesign. His focus has been in the Higher Education industry but has included international business, governance, and human centric performance. Gary has held executive level roles in Sales, Operations and Special Projects and has worked in 24 countries. This complex multicultural experience along with a history of business turnaround success based on redesign, cultural change and implementation has given him a unique perspective on risk management. Gary has worked in NASDAQ Traded, private, and government organisations and has carried Secret to Top Secret security clearances in both his military career and in his civilian roles.





ALICIA DOHERTY

DIRECTOR OF EVENTS

Alicia is the Chief Market Development Officer at Risk 2 Solution Group. Prior to joining Risk 2 Solution, Alicia served as the General Manager QLD of the American Chamber of Commerce and has held business relationship and event management positions with the Queensland Department of Premier and Cabinet, Canberra CBD, Events NSW and Austrade. She is a board member of the General Douglas MacArthur Brisbane Memorial Foundation and has held board roles with the American Club and the Australian American Association. Throughout her career, Alicia has consistently worked in close collaboration with business, Government, the US Embassy and the Canberra Diplomatic Corps. Alicia served in the US Army as a UH-1H Helicopter Repairer and Aviation Life Support Equipment Specialist.

JANITA ZHANG

REGIONAL DIGITAL MARKETING MANAGER

Janita is the Group Marketing Manager at Risk 2 Solution. She focuses on delivering attractive and engaging solutions for digital and brand design to drive customer acquisition and retention across B2B and B2C growth segments. Experienced in creating compelling UX designs and concepts, she is responsible for managing and creatively directing the delivery of digital design communications for marketing initiatives across corporate branding, printed publications, EDMs, social media, video, POS materials, website design and events.



NADINE DE LILE

QUEENSLAND CHAIR

Nadine is a risk management professional with broad experience in security and safety risk management, assurance and intelligence within mass passenger transport industries. Nadine began her career in compliance management and investigations with the QLD Department of Justice and Attorney General's Office before transitioning into security risk and intelligence, then safety risk management and assurance within the surface transport industry before finally moving into aviation. Over the course of her career, Nadine has provided leadership to diverse teams of safety and security specialists and has worked closely with and provided support and advice to various government agencies, including state police. Nadine holds tertiary qualifications in Criminology and Criminal Justice as well as Security Risk and Crisis Management and is currently the Queensland Chapter Chair of the Institute of Strategic Risk Management.

RON AMRAM

WESTERN AUSTRALIA CHAIR

Ron is the Managing Director of Safety and Rescue Australia which is the safety division of the Risk 2 Solution Group. He has a 15-year, award-winning track record in management, specializing in project and change management, systems implementation, E-Learning development, and education and training across multiple sectors.

Ron has a powerful academic background having achieved The Faculty of Business & Law's Dean's Award for Excellence in Teaching at Edith Cowan University, as well as a hands-on practical experience having taught civilian, military, law-enforcement and other government personnel martial arts and self-defence in several countries over the last decade.





ANDREW BISSETT

NEW SOUTH WALES CHAIR

Andrew has over 25 years experience in building and embedding enhanced governance practices and educating organisations to improve governance outcomes. Andrew has worked with a variety of organisations at an executive and board level and has extensive experience across a number of industry verticals, including aviation, education, oil and gas, energy, retail, information technology, government, telecommunications and financial services. Andrew led the risk function for Qantas Airways, Tabcorp and Woolworths. Andrew is a sessional post graduate lecturer in Risk Management at the UNSW and facilitates the Australian Institute of Company Directors Course online self paced course.

JULIAN TALBOT

ACT (CANBERRA) CHAIR

Julian Talbot, FRMIA is the Managing Director at SERT Pty Ltd. Julian has over 35 years of international security risk management experience gained on five continents in the resources, commercial, government, and not-for-profit sectors. His credentials include a Master of Risk Management (MRiskMgt), Graduate of the Australian Institute of Company Directors (GAICD), Australian Security Medal (ASM), Certified Protection Professional (CPP), Microsoft Certified Systems Engineer (MCSE), and Fellow of the Risk Management Institution of Australasia (RMIA).

Julian is the author of several books on security and the lead author of the Security Risk Management Body of Knowledge.



KERRI STEPHENS

SOUTH AUSTRALIA CHAIR

Kerri is motivated by good governance, committed to positive customer outcomes and leverages informed risk taking with leaders to successfully embed innovative solutions and deliver strategic objectives. Kerri's 25 year risk and resilience career spans across various sectors including insurance, agriculture, tourism and now critical service and infrastructure. As SA Water's Risk and Resilience Manager, she works in partnership with leaders and focuses on their most valuable asset - their people. Kerri's CPRA and recent Post Grad in Psychology of Risk underpins the innovative, simple, fit for purpose solutions she creates through her thoughtful combination of positive negotiation, influential communication skills and her passion for culture and well being to create lasting change.

PETE GERVASONI

VICTORIA CHAIR

Pete is a risk and resilience specialist having worked in Government and consulting roles for more than 15 years. Pete is the international project leader for the new International Standards Organization (ISO) for organisational resilience policy formulation and strategy implementation. He was the Convenor of ISO's Organisational Resilience Study Group and an active member of the Standards Australia/ISO working group (MB025/TC292) for Security and Resilience. Currently working with VMIA in Australia, Pete provides risk management and insurance training and facilitation services to Government clients. Pete was also nominated for the 2019 Institute of Public Administration of Australia's Public Sector Leadership Awards for his innovative approach to developing best practice risk management framework. Pete is continually looking at innovative approaches to integrating resilience principles into organisations and providing ongoing leadership in the development of resilience standardisation.





GAVIN PEARCE

NEW ZEALAND CHAIR

Gavin's career in risk management, management consulting and actuarial roles spans 28 years, having worked in New Zealand and Australia for large general insurance companies, government entities and a couple of consulting firms. After living in Sydney for 11 years, Gavin returned to his home country of NZ in September 2019 and joined Tower Insurance as their Chief Risk Officer. At Tower, Gavin is responsible for the risk, compliance and internal audit functions. Gavin has a Master's Degree in Statistics and an MBA from Henley Management College. He is also a qualified actuary and a graduate of the Australian Institute of Company Directors. In late 2018 Gavin was named the RMA Risk Manager of the Year.

STRATEGY ON A PAGE

THE INSTITUTE OF STRATEGIC RISK MANAGEMENT AUSTRALIA AND NEW ZEALAND CHAPTER

OUR PURPOSE

The Institute of Strategic Risk Management (Australia and New Zealand) is the regional chapter of the global Institute of Strategic Risk Management. Our purpose is to increase resilience and enhance risk culture at individual, business, community and national levels. By collaborating with allied organisations, we will encourage thought leadership and contributions to public debate in strategic risk management.

3-YEAR MILESTONES

- 2021**
Brand consolidation and recognition through contributions to public policy debate in strategy and risk, supported by targeted thought leadership events
- 2022**
ISRM professional accreditation will be the benchmark in strategic risk professional standards
- 2023**
Recognised as the pre-eminent professional body in increasing community resilience throughout Australia and New Zealand

STRATEGIC OBJECTIVES



THOUGHT LEADERSHIP
We will initiate and support professional and public discussion on strategic risk management, enhancing understanding and elevating it to a national conversation.



THOUGHT LEADERSHIP
We will contribute to the evolution of a new paradigm of capability standards required by strategy and risk professionals.



INCREASED RESILIENCE
Our thought leadership and constructive influence in public discourse seeks to build resilience in individuals, businesses and communities, and strengthen resilience nationally.

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.



UPDATED SECURITY OF CRITICAL INFRASTRUCTURE LEGISLATION – ARE YOU READY, PERSONNEL-WISE?

By Dr Paul Johnston F.ISRM RPP and Gary Sanderfield M.ISRM

Is your business a part of Australia's critical infrastructure?

In late 2021, the Security Legislation Amendment (Critical Infrastructure) Bill (2021) was passed that sought to amend the 2018 SoCI (Security of Critical Infrastructure) Act. This Act expands the sectors considered as CI from four sectors (electricity, gas, water, and ports) to now also include communications; financial services and markets; data storage or processing; defence industry; higher education and research; energy; food and grocery; health care and medical; space technology; transport; and water and sewerage.

One of the major catalysts for this expansion was the substantial increase in cyber-attacks that have been observed, with the United Nations reporting a 600% increase in cyber-attacks. Perhaps the most sobering aspect of these attacks, however, is that 25% are aimed at CI organisations. Indeed, the Global Risk Report 2022 by the World Economic Forum shows that Australia's number one risk concern is "Failure of Cyber Security Measures":



Sourced from: Global Risk Report 2022 by the World Economic Forum

Updated legislation

Under the new legislation, there are enhanced cyber security obligations whereby organisations will need to establish processes for incident response, regular cyber security test exercises, vulnerability management, and to be able to provide security incident reporting on-demand.

The implementation of this new legislation carries with it some substantial challenges for organisations that now fall under the Act. Some of these include:

- ➔ registration of critical assets: identification, classification, and accountability
- ➔ common understanding or risk-based and protective security
- ➔ effective risk management framework by sector, with common measurements and assessments
- ➔ communication between Home Affairs, state governments, and other stakeholders
- ➔ governance
- ➔ definition and parameters of scope of Ministerial Controls (Cyber)
- ➔ communication in a national security context
- ➔ mandatory reporting of cyber issues
- ➔ transparency requirements for the CI Owners:
 - Reporting requirements
 - Cyber intervention
 - Government intervention in cyber-attack/s

(Sourced from: www.cisc.gov.au)

The new legislation also allows for the government to intervene and assist when there is a concern regarding the cyber control measures currently in place

The new legislation also allows for the government to intervene and assist when there is a concern regarding the cyber control measures currently in place, when the mitigation strategies are deemed to be insufficient, or when the potential level of impact that an ongoing attack will have on critical infrastructure in a cyber emergency is deemed as requiring such action/s. In such instances, the government may step in to:

- ➔ gather information to determine if another power should be exercised
- ➔ direct an organisation to do, or not do, a specified act
- ➔ request an authorised agency provide support.

Other obligations that will be implemented under the legislation include Positive Security Obligations (PSO). This measure will include accountability for the security of critical assets, data security measures, and notification timeframes for cyber incident reporting.

The "Four Pillars" of critical infrastructure security

The new legislation is comprehensive and will focus on four pillars of security, namely:

- 1 Cyber
- 2 Personnel Security
- 3 Physical Security
- 4 Supply Chain and Business Continuity

Whereas many CI organisations will already have in place, or will be quickly working towards establishing, infrastructure and technical capabilities that meet the required standards, from a risk management perspective there an essential element that will arguably take longer to achieve – particularly within organisations that are relatively "new" to being formally designated as critical infrastructure – that of personnel security.

Personnel security involves managing a wide range of issues, and is concerned with assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness. Although policies and procedures can be quickly produced to address such issues, establishing, and maintaining the supporting mindset and culture is not so straight forward.

Are you and your personnel ready?

Indeed, security agencies believe there is an ever-increasing potential for people with malicious intent, having been intentionally embedded within our systems, such as critical infrastructure organisations, and awaiting an opportunity to be activated and strike. Similarly, there is also a substantial growing insider threat posed by persons (that aren't "sleepers", for the lack of a better phrase), be it malicious, negligent, or unethical in nature.

Therefore, there is an increased obligation of taking the necessary measures to not only effectively vet both existing personnel and onboarding new staff who will have access to systems and data, but also to enact an increased sense of security/risk awareness and a positive security/risk mindset and culture.

"Culture eats strategy for breakfast" is a famous quote attributed to Peter Drucker, and defines the situation quite well. An organisation can enact a range of detailed procedures aimed at the four pillars of security, but unless the staff have an appropriate mindset and culture, the resultant management system/s will lack substance and sustainability. Organisations need staff who are not just aware, but who are mindful, of security risk exposures and threat indicators, as well the implications of their own actions and/or inactions.

Are your staff aware of the risk exposures introduced by BYOD (bring your own device) practices, by keeping their system passwords on a notepad in their top drawer, or by

Establishing a culture and mindset that supports these mechanisms, however, is not as straight forward. It is not objective. There are no set performance indicators or thresholds. Evaluation is not absolute.

being "polite" and holding a door open for someone they don't know and who doesn't have a security pass? Whilst establishing a sense of trust is universally recognised as being a foundation stone to establishing a sustainable culture, in this context, such trust cannot be freely given, nor taken for granted. Rather, it needs to form part of a larger equation that results in a positive risk and security culture – one that is based on security awareness and appreciation, informed decisions and engagement, and the provision of regular feedback.



Technical systems and procedures are relatively easy. We reference a set criterion, and we ensure that the deliverables meet or exceed them. It is an objective process, and one that is easily evidenced and assessed. Establishing a culture and mindset that supports these mechanisms, however, is not as straight forward. It is not objective. There are no set performance indicators or thresholds. Evaluation is not absolute.

This is the challenge that organisations will continue to face. Indeed, the primary focus of security risk management in critical infrastructure must evolve as to not only consider the technology that drives it, but also to consider the people who work there. Whilst we have seen this occur with regards to occupational health and safety, we are yet to see the same change in mindset when it comes to security. Now is the time to see that change.

*Reference:
Marsh McLennan, SK Group, & Zurich Insurance Group (2022). The Global Risks Report 2022, 17th Edition. World Economic Forum.*

AUTHOR BIOS



DR PAUL JOHNSTON

Editor of the ISRM ANZ Journal, Dr Paul Johnston is a Lead Risk Consultant with Risk 2 Solution, and is adjunct lecturer with ACU (Australian Catholic University) Executive Education. He holds a PhD in Public Safety Risk Management, a Graduate Certificate in Occupational Hygiene Engineering, and a Bachelor of Behavioural Science. With over 25 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](#)



GARY SANDERFIELD

As the General Manager of Consulting for Risk 2 Solution Group, Gary Sanderfield heads up their efforts to support both Home Affairs and the market sector in preparing for the roll-out of the new SoCI related regulations.

Gary's Career began as a Combat Medic in the U.S. ARMY, and he then spent 6 years working in a Coronary Intensive Care unit and Level 1 Trauma Centre. The lessons learned during these years that make up his business persona include staying calm under pressure, decisive decision making, teamwork, effective communication, discipline, and attention to detail. He is a highly experienced risk and leadership specialist with over 20 years of experience in human centric performance, operational risk, enterprise risk management and organisational redesign. His wealth of knowledge is reflected in his expert training deliveries.

[Connect with Gary on LinkedIn](#)

PRESILIENCE AS A UNIFYING PRACTICE TO CHANGE, THRIVE, AND GROW

By Dr Gavriel (Gav) Schneider and Lisa Young



Whether an organisation is public or private, profit-making or non-profit, government or military, it has a mission to deliver value to stakeholders and customers. The persistent disruptions to our critical infrastructure delivering electricity, water, healthcare, and public safety are intensifying threats to our economic and national security. The ongoing risk and disruption when things go wrong is no longer sustainable nor desirable.

The world has changed around us into a default operating paradigm that is volatile, uncertain, complex, and ambiguous (VUCA)¹. Traditional approaches to problem solving and organisational performance tend to focus on highly structured and linear methodologies which may work well when we have levels of certainty, control, and influence, but seem harder and harder to capitalise on, or even simply perform, when disruption occurs.

The journey to a presilience-based, high-performance model involves new ways of thinking and problem-solving. Presilience is defined as the ability to achieve our mission with people, process, and technology underpinned by situational awareness and risk intelligence. The goal of presilience is to enable an organisation not only to survive continued disruption and chaos but adapt to change, thrive, learn, and grow. It also goes without saying that the

The journey to a presilience-based, high-performance model involves new ways of thinking and problem-solving. Presilience is defined as the ability to achieve our mission with people, process, and technology underpinned by situational awareness and risk intelligence.

best time to be preparing for challenges is not during the challenge but during business as usual (BAU). As such, the concept of presilience centric organisation capitalises on high performance during business as usual too. The promise and practice of presilience is one that equips us to cope with the reality of a digital world, where the intersection of cyber and physical domains converge and cannot be tamed by conventional linear approaches and old-fashioned management theories.

The ability to achieve robust and consistent high performance as individuals, teams, and organisations, to support and maintain our collective societal ecosystem, is no simple thing. Billions of dollars and countless hours have been spent on innumerable secrets to success. After many bouts of trial and error, failures and successes, and practical application of risk management, resilience, working with humans and being human ourselves, the idea for a way to bring these concepts and theories together materialised as the 'presilience journey'. The journey itself consist of the following three unifying critical success factors, as primary drivers to positive outcomes:

- 1 Compliance** – conformance to a set of criteria that we are obligated to perform or choose to perform because it is the right thing to do, or we are legally bound to do so.
- 2 Resilience** – preparing and implementing the things we need to survive a disruption or crisis and continue to operate either in a degraded, business-as-usual, or optimal state. The idea of resilience is centred on toughness and the ability to overcome disruption as quickly as possible and return to a BAU state as quickly as possible.
- 3 Presilience** – the capability to adapt, proactively prevent bad outcomes, and opportunistically use what we learn to grow and thrive even as the landscape in which we attempt to manage or control continues to test our human, technological and operational limits.

¹The term VUCA was first used in the late 1980s by the US war college and since has become very popular to explain our current operating context.

In the landscape in which an organisation operates, there are many things that may impede an enterprise from accomplishing its objectives, achieving its financial, strategic, or operational targets, or meeting its mission.

In the landscape in which an organisation operates, there are many things that may impede an enterprise from accomplishing its objectives, achieving its financial, strategic, or operational targets, or meeting its mission. A presilience-based mindset is best paired with a strategic view to move beyond traditional approaches to risk management and resilience, to an evolved unified model that requires the following aspects:

- ➔ **An integrated perspective that fully utilizes people, process, and technology tied to purpose, strategy, or mission that is anchored by principled governance.**
- ➔ **Multi-level thinking and multi-disciplinary leadership anchored by consideration of self, others, organisation, and society.**
- ➔ **Silo busting that converges vertical, horizontal, and circular viewpoints to achieve a nimble structure that enables scale, flexibility, and reliability and leverages diversity across the organisation.**
- ➔ **Fostering skills in leadership, followership, and the ability to understand the dynamics of how people function in groups, teams, and units.**
- ➔ **Situational awareness and risk intelligence to make informed decisions with what we know now and as the intelligence data changes over time.**
- ➔ **A non-binary mindset that leverages the best of people, process, and technology without being burdened by negative bias.**



The journey aims to provide a scaffolding that integrates the best of compliance, resilience and presilience to achieve sustained high performance to meet desired outcomes.

So, what is the Presilience journey

Presilience means we are able to build on the expertise we have in compliance and resilience while incorporating the aspects of proactive prevention and the idea of bouncing back better or in a different direction after a seminal event. The applications of a presilience mindset are intended to be continuous and adaptive. The journey aims to provide a scaffolding that integrates the best of compliance, resilience and presilience to achieve sustained high performance to meet desired outcomes. In essence, it is about turning any threat, disruption, or risk into something the individual, team, or organisation can capitalise on to adapt, grow, thrive, and navigate the complexities of a dynamic world.

From our perspective a unifying presilience practice should include the following principles:

- ➔ Meets people where they are now
- ➔ Creates and/or serves as a reference framework
- ➔ Toolbox approach (should enable the subtraction and addition of tools without degradation of the model)
- ➔ Is multidisciplinary and not tied to only one school of thought
- ➔ Integrates key aspects for success across the cyber-physical-digital domain
- ➔ Enables linkages between aspects that on face value may seem unrelated
- ➔ Most useful theories or models can be aligned without significant stretching
- ➔ It can be applied on the 4 levels described (individual, team, organisation, and society)

With these criteria in mind, it becomes clear that the idea of a continuous journey to build on compliance, integrate resilience, and foster a spirit of presilience does enable a mental model to both manage business as usual but also to thrive during disruption. Over time this approach will morph and adjust but, in the meantime, where there is dynamic and rapid change happening it is useful to have a suite of tools, techniques, and methods that not only help us make sense of our current world but enable us to position ourselves, our teams, our organisations, and ultimately our societies for the world of the future. We hope you will join us on this journey.

AUTHOR BIOS



DR GAVRIEL SCHNEIDER

Dr Gavriel (Gav) Schneider is the creator of the concept of Presilience® and an acknowledged leader in the fields of security and risk management. He is a well-known leader in human based risk management and the psychology of risk and is a serial entrepreneur and has been running his own businesses since 2001. He is one of the very few to make the IFSEC Global Influencers in Security Thought Leadership - top twenty list for 3 consecutive years 2019, 2020 & 2021 as well as being awarded the risk consultant of the year 2019 (RMIA).

He has conducted business in over 17 countries and provided a wide range of services for a very diverse client base ranging from heads of state to school teachers. He is a leading academic and subject matter expert in his field and is a much-sought after International speaker. He has trained thousands of people in his own right and to date, his companies have trained in excess of 150,000 people in numerous countries.

He has also authored two books including the highly acclaimed "Can I See your Hands - A Guide To Situational Awareness, Personal Risk Management, Resilience and Security" and is a lifelong martial artist with master grades in several systems. Dr Gav serves as the Group CEO for the Risk 2 Solution Group and is the ISRM ANZ regional Chair.

[Connect with Gav on LinkedIn](#)



LISA YOUNG

Lisa Young, CISA, CISM, CISSP, is an operational risk and security metrics professional with a passion for solving problems with data. She is a prominent cybersecurity veteran, having worked in government, military, industry, and academia. Lisa is currently on sabbatical from her role Vice President of Cyber Risk Engineering at Axio Global, Inc., an integrated risk management software company. Since 2021 she has been part of a multi-disciplinary team as a senior risk advisor on the COVID task force at DHS CISA.

She holds a Master of Public Policy with a cybersecurity concentration from the University of Maryland and a B.A. in Business Administration from University of South Florida.

Her superpower is preparing security teams to protect and defend their organizations from cyber criminals, respond to crises, and recover when something bad happens.

Connect with Lisa on [LinkedIn](#) or via [RSA Conference](#)

LEADERSHIP SURVIVORS DRIVE ORGANISATIONAL SUCCESS

BY LEANNE CLOSE

***“We are shaping the world faster than we can change ourselves, and we are applying to the present the habits of the past”
Winston Churchill” (1945)***

For leaders, these words of Winston Churchill remain as applicable today as they were in 1945. It is estimated that 60% of Australian small businesses fail in their first three years of operation, but the larger the enterprise, the greater their chance for survival (ASBFEO, 2019). Understanding what influences these outcomes will assist managers improve the longevity of their businesses. Knowledge of market forces, ongoing research, managing opportunities and risks, and strong financial acumen all impact business success (Lee-Schneider, online). Leaders must also appreciate the value of effective leadership and management in attracting and retaining the right staff, and to motivate, develop and guide employees to achieve high-performance outcomes. These essential focus areas form a key part of the CEO’s role, as well as those of Boards and managers, if their organisation is to be successful and sustainable for the long term.

Leadership expectations about management and organisational design continue to evolve. The latter half of the 20th century focused heavily on transactional versus transformational leadership. However, there are major weaknesses in this binary choice, including the ambiguity of the transformational or charismatic leadership style influencing work outcomes (Yuki, 1999).

In assessing the human dimension of leadership, one simplistic, and potentially controversial, way is to assess the abilities of people

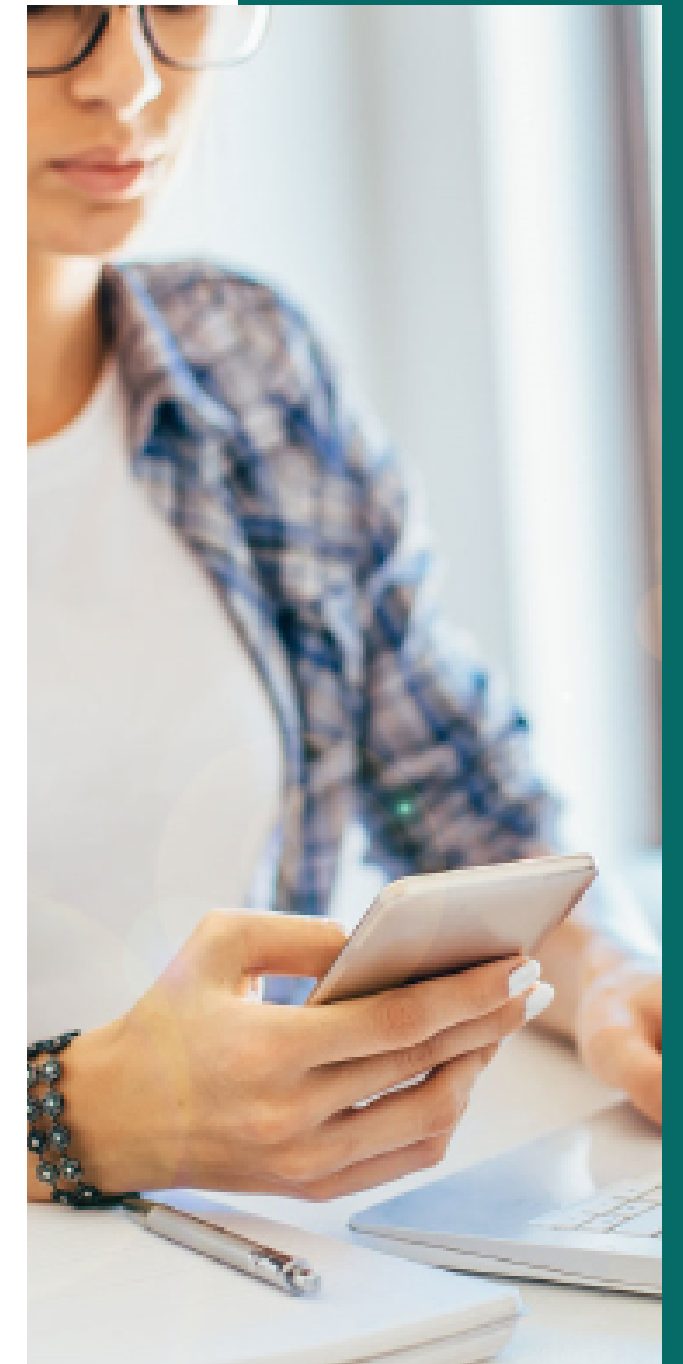
during a crisis, using the 10-80-10 principle (SRMC, online). During a crisis, about 10% of people, the “Survivors”, are leaders who have a plan and take decisive action. Another 80% are dazed, panicky or disoriented, called the “Confused”. They may struggle to make sense of the situation, seek direction, and/or wait for others to take the lead and advise them what to do. Ten percent, the “Doomed”, behave in counter-productive ways, intentionally ignoring authoritative sources and who potentially do the wrong thing (ibid).

Creating more “Survivors” becomes important as organisations navigate increasingly volatile, uncertain, complex, and ambiguous (VUCA) operating environments (Bennett & Lemoine, 2014). Investing in pre-planning, leadership development, and staff preparedness during BAU times makes sense for the inevitable times of crisis and VUCA environments.

Ensuring that leaders focus on eight essential organisational processes is another key to organisational success and longevity (Yuki, 1999). These are:

- 1 **Organising work to fully utilise personnel and resources,**
- 2 **Coordination of inter-related group activities,**
- 3 **Obtaining member agreement about objectives and priorities,**
- 4 **Establishing mutual trust and cooperation among members,**
- 5 **Improving group identification,**
- 6 **Improving member confidence in the capacity of the group to attain its objectives,**
- 7 **Improving procurement and efficient use of resources; and**
- 8 **Improving coordination within the organisation and outsiders.**

Importantly, these objectives should not only be articulated, but pursued and measured. Schneider and Sofianos (2021) advocate “Presilience”, a risk intelligence approach to achieving high-performance, long-term business outcomes (Schneider & Sofianos, 2021). In their model, measurement of these organisational processes allows leaders, staff, and external stakeholders to assess an organisations’ ability to manage uncertainty to achieve business objectives. They contend the model provides a basis for ideas generation, improved processes, analysis of emerging situations and



According to the International Disaster Database, 2020 recorded more natural disasters than the average of the last 20 years (Moonen, 2021). Anecdotally, more time, money and focus are spent recovering from business crises and major disruptions, than preparation and pre-planning.



AUTHOR BIO

Leanne Close APM is the Chief Executive Government and Strategic Engagement for Risk 2 Solution. She also sits on several government and not for profit boards. Leanne was a police officer with the Australian Federal Police for over 33 years, culminating in her role as Deputy Commissioner. Leanne worked for the Business Council of Australia in 2021, managing the community rebuilding charitable trust called 'BizRebuild'. She has also written for the Australian Strategic Policy Institute on terrorism and national security related topics, and co-edited the ASPI 2020 Counter-Terrorism Yearbook.

[Connect with Leanne on LinkedIn](#)



enhanced decision making, leading to improved productivity and performance, which can be measured and improved over time (ibid).

According to the International Disaster Database, 2020 recorded more natural disasters than the average of the last 20 years (Moonen, 2021). Anecdotally, more time, money and focus are spent recovering from business crises and major disruptions, than preparation and pre-planning. Organisations that invest in a human-centred approach, coupled with new digital solutions in a rapidly evolving technological environment, will provide significant opportunities for businesses to thrive and survive. In other words, managing and investing time, energy and focus on those eight key organisational processes results in high-performing teams, improved management of risks, and allows organisations to continually grow and learn. The aim should be to not repeat the bad habits of the past.

In building strong leadership capabilities, it is essential that leaders recognise their role and the impact they have on workplace culture and behaviours, which directly impact the reputation of an organisation. Prioritising and investing time, money and resources on leadership development and collaborative strategic planning will equip leaders

with the tools to engage, motivate and manage staff and business processes effectively. This in turn will lead to improved organisational outcomes, productivity, staff engagement and trust - therefore improving the longevity and survivability of the organisation in highly competitive marketplaces.

Changing organisational dynamics, coupled with significant technological advances of the past 25 years, requires a mature model of leadership incorporating a focus on managerial compliance (transactional) with values-based and people-centric (transformational) approaches. The requirements on C-suites and Boards to navigate increasingly complex legal, regulatory, and competitive environments demands a mature approach in building leadership capabilities and investing in their teams – creating more “Survivors”. It also ensures leaders are provided with the skills to manage those eight essential organisational processes to secure business success, and to build and maintain a high-performance culture. The resulting organisations are more sustainable and better equipped to not just manage well during BAU, but to thrive and survive during VUCA periods over the long-term.

References

- Australian Small Business and Family Enterprise Ombudsman (ASBFEO) (2019), Small Business Counts: Small Business in the Australian Economy, July 2019, Australian Government www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-small-business-counts2019.pdf
- Bennett, N and Lemoine J What VUCA really means for you Harvard Business Review, Vol. 92, No. 1/2, 2014 www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2389563 accessed 22/12/21
- Churchill, W (1945) in Lee, M. (2021) Leading Virtual Project Teams: Adapting Leadership Theories and Communications Theories to 21st Century Organizations, 2nd Edition, CRC Press, 2 Park Square, Abingdon UK, p.2
- Lee-Schneider, D online: www.davidleeschneider.com/7-reasons-why-your-business-is-going-to-fail-within-your-first-year/ accessed 20/12/21

Moonen, G, Editorial: Solidarity in the face of a clear and present danger. Disasters and Crisis Management, Journal No. 3 2021, European Court of Auditors p5

Schneider, G and Sofianos, N (2021) Moving to Presilience in a VUCA World: The new norm needs a new way, accessed 22/12/21, www.r2s.academy/courses/take/presilience-leadership-and-high-performance/pdfs/25362319-presilience-monograph-draft-version-june-2021

Security Risk Management Consultants (SRMC), Ohio USA www.srmcllc.com/news-home/2020/4/6/pandemic-and-the-10-80-10-principle accessed 22/12/21

Yukl, G. (1999) An Evaluation of the Conceptual Weaknesses in Transformational and Charismatic Leadership Theories. Leadership Quarterly. 10(2), 285–305 in ODUMERU, J. A. and IFEANYI G.O. Transformational vs. Transactional Leadership Theories: Evidence in Literature, International Review of Management and Business Research June 2013, Vol 2 Issue 2

FATCA ENFORCEMENT – THE NEXT BIG RISK TO AUSTRALIAN BUSINESS?

BY KRISTINE SEYMOUR

Accounts receivable have never been more important than they are right now. Supply chain shortages, a tight labor market, and rising fuel prices all contribute to the soaring costs of business. Companies need to run as efficiently as possible. Governments are no different, with multiple stimulus packages, inflation, and mounting deficits, they rely on tax and penalty collection to fund operation. One of the biggest risks to business is the United States government enforcing their Finance and Taxation Compliance Act (FATCA) in Australia.

FATCA enforcement is not just for banks reporting on US citizens' accounts. FATCA is much broader, and few understand the risks and need for additional controls to be implemented. Indeed, the unintended consequences of FATCA regulation and non-compliance may be the next unforeseen disruption to Australian business in the short term.

FATCA is an annual reporting requirement that tracks assets and accounts of American citizens and green card holders to reduce tax evasion and money laundering, among other offences. Non-compliance is a criminal offence, regardless of ignorance. Financial accounts that are subject to the reporting requirement are any account with a positive balance that is under ownership or control of an American citizen or green card holder, with few exceptions. Control is defined by signatory authority, e.g. the right to wire company funds or use a company debit card. Company accounts may be subject to Foreign Bank Account Report (FBAR) filings

due to being under the control of an American, even though the employee does not own the money in the company's bank account. A minimum penalty for non-compliance is USD\$10,000 per account and a maximum of 50% of the balance of each non-compliant account, and a possible (7) seven years jail that would be the company representative's responsibility, not the employee in control of the company's funds.

The ATO's agreement to assist in FATCA enforcement states the agency will serve notices of non-compliance on behalf of FINCEN (Financial Crimes Enforcement Network). However, it will not collect penalties on any Australian citizen or entity. Company funds would be protected from automatic collection, but the debt would remain, and the company's credit rating may be at risk. This unexpected expense would be an unwelcome surprise. Consulting a cross-border specialist to identify any applicable accounts for a FBAR filing is a simple solution.

Although US tax and FBAR compliance filing is the responsibility of the individual, employing a criminal may interrupt operations and cause reputational damage. Authorised representatives, AFSL holders, lawyers, accountants, and occupations who are held to professional standards would be ineligible to practice. Working with children, bonded employees, security personnel would all suffer the same fate. Employment contracts could be voided and directors could lose their positions. Disruption to the workforce would be inevitable.

FATCA enforcement is a viable and likely threat. Investment and continuing developments in technology, combined with intergovernmental agreements, is bringing enforcement on a mass scale closer to fruition. In 2010, FINCEN received a USD\$12.7million modernisation budget to improve IT and big data solutions, specifically aimed at receiving account information from foreign financial institutions (FFIs) and data scraping to locate US citizens worldwide to reconcile to the FFI reports. An intergovernmental agreement in 2015 between Australia and the US was signed, whereby

The ATO's agreement to assist in FATCA enforcement states the agency will serve notices of non-compliance on behalf of FINCEN (Financial Crimes Enforcement Network). However, it will not collect penalties on any Australian citizen or entity.

Australia agreed to share taxation information for relevant parties, collect penalties and outstanding taxes from non-Australian citizens, and serve notices for non-compliance to relevant Australian or dual citizens. In 2018, the United States passed the Clarifying Lawful Overseas Use of Data Act and in 2021, Australia entered into a CLOUD Act agreement that will allow for expedited data sharing once the agreement receives full Parliamentary and Congressional approval. This agreement is focused on sharing data efficiently for the purposes of serious crimes, such as terrorist financing, money laundering, tax evasion and individual fraud. In November 2021, when the USD\$1.2T Bi-Partisan Infrastructure bill passed into law in the United States, President Joe Biden went on record stating that enhanced tax collections is one way he planned to reduce the deficit. Also in 2021, over 1600 treasury agents were hired to process the backlog of tax returns and FBARs in the IRS and FINCEN. With the need for the government to run more efficiently, the United States looks to be prepared to commence FATCA enforcement soon. Is your business prepared?

FATCA enforcement can wreak havoc across an organisation unless controls and measures are put into place. Understanding and effectively using the data your company holds could be the difference between a simple filing and chaos. Through proper data risk management, keeping track of relevant parties is possible. Perhaps like a KYC check, adding a FATCA check at onboarding, or a FATCA check when an employee is given permissions for the company accounts. As ignorance is not an excuse,

knowledge is key, but identifying impacted parties may be trickier than first thought. US citizens can be dual citizens and employed using their Australian passport; green card holders might be under the false assumption they are no longer required to file US tax compliance because the card is expired and is no longer valid for residing in the States; or Accidental Americans who may be unaware of their status. In many cases, US citizens living in Australia are unaware of their filing obligations, so starting the conversation and providing information is important to both the employee and the company. An important part of the conversation is to highlight the amnesty program for those who have not been filing their US tax compliance.

Expat tax compliance is not an easy filing, and should be completed by a cross-border specialist. Many expat specialists will provide information to employers for their staff. Find a firm with multiple enrolled agents (EA) to ensure capacity, check for good reviews or request references. The ability to leverage the tax treaty effectively for the maximum benefit means, for many, no taxes are payable to the US.

Time, like receivables, is valuable. Spend it wisely and prepare your company now for FATCA enforcement.

AUTHOR BIO



Kristine Seymour is the Head of Strategic Partnerships and Growth at US Global Tax and a Master of Fraud and Financial Crime candidate at Charles Sturt University. US Global Tax is the largest US Expat tax specialist firm in Australasia. Kristine works with organisations who need advice on how the US tax system impacts their business.

Contact Kristine at kristine@usglobaltax.com

PATCHING PEOPLE

JOE SAUNDERS F.ISM RPP



I recently had the opportunity to interview Rick Shaw, a Las Vegas-based threat assessment professional, on my Managing Violence Podcast. Among many other pearls of wisdom, Rick said something that really struck a chord with me.

“We patch our systems, but we don’t seem to patch our people.”

While Rick said this in the context of updating and upskilling staff in emerging criminal trends, the simplicity and ubiquity of the idea resonated with me across a broader risk context. In an era when business of all sizes are paying absurd amounts of money for software solutions with mandatory update and patch schedules, how often are we updating and patching our people? If we are entrusting our people to drive these expensive systems, are our people not our biggest strength and our biggest vulnerability?

To explore this further, we should first define what a “patch” actually is. Typically, a patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This sometimes includes fixing security vulnerabilities and performance issues. Patches are often written to improve the functionality, usability, or performance of a program.

Let’s unpack this and see how it might apply to our human systems, not just our tech systems.

In the software world, fixing something that is not working as expected is fairly urgent and important. After all, your paying customers aren’t going to keep schilling out their monthly subscription for a service that is buggy or inconsistent. Fixes are expected.

Update Patches

A “people patch” may be something as simple as updating trends, expectations, or information relevant to that person’s role. If you are managing a risk management team, it should not be taken for granted that “risk people” are all passionately digesting the latest news on their industry just because that would be good practice. Allocating a set amount of time each week to provide a general update is a good practice to ensure that everyone is across the latest developments relevant to their role. This might be in the form of academic research, news reports, case studies, or even just internal changes such as budgets or focus areas. Providing a regular update patch ensures that everyone is working from the same base information, and not downloading unvetted update patches from the water cooler or employee WhatsApp group.

Fixer Patches

Another purpose of a patch can be to fix previously unknown errors. Maybe you’ve just found out that the new intern has never operated a commercial copier before and has been tasked to send something called a “fax” to that one client who insists on pretending it’s still 1997. Will you scrap the entire project (fire the intern) or patch in the required knowledge? These fixes, or knowledge patches, should be consistently applied across all team members. If someone doesn’t know how to do something, or they don’t know the way your team does something, create an environment where it is safe to ask for a patch. Even better, create a culture where your leadership are constantly looking for opportunities to provide patches and fill gaps as they appear.

Improvement Patches

In the software world, fixing something that is not working as expected is fairly urgent and important. After all, your paying customers aren’t going to keep schilling out their monthly subscription for a service that is buggy or inconsistent. Fixes are expected. Therefore, it is improvements that tend to win customer loyalty. When a software manufacturer voluntarily improves a system you were already happy with, at no additional cost, it triggers positive feelings towards the whole enterprise. The same can be said for our human patches. Improvement patches might be things like free professional development, upskilling, accreditations, or secondments to learn additional skills. Remember that risk management is about threats and opportunities. Are you seizing every opportunity to improve your staff? It is seldom a bad investment.

Vulnerability Patches

Perhaps the most immediately relevant patch for risk managers is to address security vulnerabilities. The vulnerability patch is a more urgent and more critical fixer patch. The vulnerability patches may not necessarily be security related, but there are some obvious examples in the security risk management realm. Perhaps you have an employee that keeps a notepad with all of the system passwords sitting on their desk, conveniently labelled “PASSWORDS” in bright pink marker. Or maybe it’s the well-meaning, but naive, new employee who holds the door open for everyone, regardless of whether they have an access card or not. It could, however, just as easily be someone developing a gambling problem, being too “free and easy” on their personal social media accounts, or engaging in office banter that verges on bullying. Whatever the vulnerability, it needs to be urgently patched.

These are just some easy examples of people patches. The most important thing is that you have a deliberate and effective strategy for rolling out your patches. It should include a balance between continuous improvement and update patches, prioritised fixer patches, and the urgent vulnerability patches. At a minimum, whenever another part of the system changes, the humans operating the system must be patched to ensure they understand how to interact with the changes. This is a frequently missed opportunity, and undermines the effectiveness of the (sometimes quite expensive and impressive) changes that are being made.

Patch wisely, strategically and resiliently.

Finally, a word of caution. Although meant to fix problems, poorly designed patches can sometimes introduce new problems and vulnerabilities. Patch management is a part of lifecycle management, and when we're talking about our people, that can be a very long time indeed. Just as a rushed software patch can corrupt an entire system and destroy confidence in the manufacturer, a rushed people patch (see: sweeping policy changes) can disenfranchise hundreds of people and cripple morale in a single keystroke.

AUTHOR BIO

Joe Saunders is State Manager (VIC/TAS) and National Practice Lead - Violence Prevention at Risk 2 Solution.

Joe is a recognised thought leader in the field of occupational violence and is regularly called upon to present at local and international events. He is the co-author of the ASRC's Occupational Violence, Aggression and Duty of Care research paper, and has contributed articles for numerous journals and publications, including LexisNexis Risk Management Today, Security Insider, Aviation Security International, and The Circuit Magazine. He combines 15 years of experience in frontline conflict management with post-graduate research into psychology, workplace safety and security risk management.

Joe is a gifted and dynamic presenter, educator and training designer with a knack for communicating a sometimes-difficult subject to professionals and laypersons alike. He is a Fellow of the Institute of Strategic Risk Management (ISRM), an Associate of the Australian Risk Policy Institute (AARPI) and a Member of the International Law Enforcement Educators and Trainers Association (ILEETA).

[Connect with Joe LinkedIn](#)



USING RISK INTELLIGENCE TO MAKE A FAILURE RESILIENT ORGANISATION IN A VOLATILE, UNCERTAIN, COMPLEX AND AMBIGUOUS WORLD

James Jordan BSc (Security); MEmergMgt; DipGov (Security); GCertPsychRisk

Summary

The concept of a Failure Resilient Organisation is one that has been gathering strength within a world that is facing increasing levels of Volatility, Uncertainty, Complexity and Ambiguity (VUCA).

The question arises as to what is a Failure Resilient Organisation? Often, focus is on the failure aspect, and its definition of 'the lack of success'. This definition in itself is very limited, and this paper seeks to expand the discussion into the influences of how and what is interpreted, as the definition offered is too simplistic to capture the broader meaning of 'failure' in a few words.

This requires the concepts of Sense Making, Risk Intelligence, and their value to informing the concept of the Failure Resilient Organisation, to be expanded upon. In particular, the aspects of Risk Intelligence and the need to place greater emphasis on intelligence capability building, rather than risk identification, as you need the former to build the latter.

To demonstrate the need for intelligence to inform risk, we also need to expand on the conceptual tools of Situational Awareness, Critical Thought Processing and Adaptive Planning, with an emphasis on avoiding the pitfalls of cognitive biases.

Finally, it looks to the application of Risk Intelligence to build Risk Libraries as a tool which can be used to develop an understanding of the information needs of the current environment, and those of the potential environments in the future. This can then be used against the organisation's understanding of 'failure', and how it can become a more resilient

Introduction

When considering the value of the concept of a Failure Resilient Organisation within the context of an environment that is subject to increasing Volatility, Uncertainty, Complexity and Ambiguity (VUCA), to understand the importance of the application of Risk intelligence is crucial to success.

To do this, we first need to consider what is a Failure Resilient Organisation, and secondly, how is Risk Intelligence applied in this context.

What is a Failure Resilient Organisation?

The question of what a Failure Resilient Organisations does not have a simple answer. It is not, as some might suggest, just a matter of putting in measure to toughen it up.

This is because the definition of what constitutes a failure, and what does it mean to be resilient to that failure, is a matter for interpretation by each organisation individually. This makes the identification and evaluation for each organisation a complex situation.

A 'failure', to compare against the dictionary definition "the lack of success" (Dictionary.com, 2021), is difficult to define within the context of an organisation as what is 'successful' is in itself a subjective scale, depending on strategic priorities. The reality is that things not occurring as expected is a common everyday occurrence, and organisations regularly adapt and change course in response. This in itself does not constitute a failure, but it can be seen as part of its ability to resist failure.






What can be identified is the elements of how an organisation can determine what it needs to know when making the decision of what is a failure in their terms, against what it sees as a success, and what that failure means to the organisation in terms of harm.



While there are many ways to identify, and then go on to assess and contextualise this process, the one that provides an association with the application of Risk Intelligence (a connection that will be made later in the essay) is that of the High Reliability Organisation, as defined in the book by Weick and Sutcliffe 'Managing the Unexpected' (Weick & Sutcliffe, 2015). In this book, the authors noted that organisations that sought information from a collaborative approach that sought out a wider perspective on complex decisions were better able to make sense of their situation, and were more likely to have positive outcomes.

Sense-Making, as a concept, was first expressed by Katz and Kahn in their research on 'The social Psychology of Organisations' (Katz & Kahn, 1978), which introduced the concept of using the undertakings and beliefs of the groups within an entity to understand the reasons behind their creation. It is the properties of Sense-Making that provide the input that creates the foundation of an organisation that is mindful of its environment, and was able to adapt to changes as they were occurring. Weick and Sutcliffe (2015) felt that this mindfulness was the essential part of a High Reliability Organisation.

The authors of this book also developed a set of principles that represented a High Reliability Organisation, based upon the concept of Sense-Making, that represented how these organisations make themselves Failure Resilient:

-  **They have a Preoccupation with Failure by putting in place monitoring processes that monitor when things do not go 'as planned', what responses were put in place, and that take the time to assess to determine the root cause.**
-  **There is a Reluctance to Simplify Interpretations to ensure that they understand the environment in its entirety, so that all factors that have the potential to influence an outcome are explored.**
-  **By being Sensitive to Operations, they ensure that they have a level of situational awareness that provides them with early indications of changes to their external and internal environments that may affect the ability to achieve outcomes.**
-  **A Commitment to Resilience by ensuring that potential changes are assessed and mitigations, if necessary, are put in place so that impacts to objectives do not lead to failure.**
-  **They are organisations that have a Deference to Expertise that acknowledges that not all capability rests within the organisation, and will seek out knowledge from external sources.**

It is the application of these principles, in a mindful way, that allows an organisation to make sense of its environment so that it can deliver on its objectives in a manner that is reliable, regardless of impact.

As a result, in its efforts to become a High Reliable Organisation, it has become resilient to failure in both its ability to avoid and reduce the potential, but also be able to respond quickly by being well prepared.

Risk Intelligence

There is no single definition regarding Risk Intelligence. There are those who propose definitions such as the "capacity to learn about risk from experience" in an effort to mitigate threats (Apgar, 2006), and there are others that look at the "identification, analysis, assessment, control and avoidance, minimisation or elimination of unacceptable risks" (Businessdictionary.com, 2020).

These definitions, and various other similar versions, all place too much focus on the definition of the word 'Risk', and as such focus on the aftermath of the realisation of risk, and less on the prevention of said risk. What is forgotten is that the purpose of intelligence is to inform an organisation so that it can appropriately prepare, by giving it the opportunity to understand the cause of the risk – as noted in this definition of intelligence, "global capacity of the individual to act purposefully, to think rationally, and to deal effectively with his environment" (Wechslet, 1944).

This latter definition is more in alignment with the context of the application of mindfulness and sense-making in a form more aligned to emotional intelligence, rather than the traditional risk concepts as discussed in the paper titled 'What is Risk Intelligence' by Dr Schneider, Dr Johnston and Ms Down from Risk2Solution (Schneider, Johnston, & Down, 2017). As noted in this article, much of what defines a High Reliability Organisation in its endeavour to make itself Failure Resilient is similar to that of this concept of Risk Intelligence.

This can be expanded on by considering those principles that define the High Reliability Organisation, where there is a focus on putting in place the resources to monitor its internal and external environments, so that it can effectively and efficiently collate the data required to make informed analysis that can be used to identify risk.

As a result, in its efforts to become a High Reliable Organisation, it has become resilient to failure in both its ability to avoid and reduce the potential, but also be able to respond quickly by being well prepared.



As a result of the application of these principles, High Reliability Organisations can be often seen to be implementing a common set of conceptual tools that assist in the development their Risk Intelligence:

- **The establishment of monitoring and data collection capabilities to established Situational Awareness from the environmental inputs in order to identify potential failures, and to ensure that changes to the organisation can be identified as early as possible.**
- **The capability to apply Critical Thought Processing to collected data in a manner that acknowledges potential sources of cognitive bias, so as to ensure that analysis of data is not simplified, and that suitable expertise is available to make educated judgements.**
- **Has introduced and developed Adaptive Planning skills to allow it to rapidly adjust organisational responses to environmental inputs, which demonstrates a sensitivity to those influences and a commitment to ensuring that they have minimal negative impact on objectives.**

The application of these principles relies on two elements for the success use of Risk Intelligence. Firstly, is the empowerment of social leadership in individuals that have expertise. As a capability, this does not come naturally as the ability to manage stress, and the corresponding adrenal response, often triggers an emotional response to a problem rather than one based upon logic.

As noted by Kelly Coker (2020), to manage this capability requires individuals to understand how the Antecedent Behavior Consequence Model, and the Reticular Activating System within the human mind manages the 'neural seesaw' between the Type 1 (Emotional) and Type 2 (Logical) manner in which the brain perceives, and places cognitive biases against the information presented to it when the Reticular Activating System is placed under stress – which then leads to emotionally influenced Type 1 based decision making (Kelly Coker, 2020).

Secondly, is the element of timeliness which comprises of two aspects, sufficiency, and intuition. Sufficiency considers the processes that collect, analysis and deliver the Risk Intelligence need to be developed well enough in advance to ensure that bias and simplification, both of which are hallmarks of a brain in a Type 1 thinking state (Kahneman, 2011), are not influencing factors. Intuition is the acknowledgment of giving those responsible for the outcomes the ability to make decisions. By providing a means to utilise the Risk Intelligence, to support informed intuitive judgements, when the requirements do not provide the luxury of time to consolidate and collect all the required data.

With the understanding that a Failure Resilient Organisation is about building an assessment of the internal and external environments, we can see that the application of Risk Intelligence is the corner stone.

With the understanding that a Failure Resilient Organisation is about building an assessment of the internal and external environments, we can see that the application of Risk Intelligence is the corner stone.

Application of Risk Intelligence

One of the best examples of the practical use of Risk Intelligence is the construction of an Organisational Risk Catalogue. The Risk Catalogue for an organisation is derived from an understanding of its objectives at the strategic level, and their application at the operational level, and is an essential building block in the building of Resilience (Presilience, 2021). The concept of Resilience as defined by its creator Dr Gav Schneider in his book 'Can I See Your Hands' (Schneider, 2017).

Noting that a Risk Catalogue and a Risk Register are very different concepts, with very different purposes, the Register is a summary of risk analysis within the context of an individual risk assessment, whereas a Catalogue is based upon a process of discovery prior to the assessment being undertaken.

The benefits derived from a Risk Catalogue are best demonstrated by understanding the process by which one is constructed. This will also demonstrate the connection with Risk Intelligence, and its central importance to the delivery of successful outcomes.

With the value established from the Enterprise Risk Assessment for the operational functions and assets, we now have a situation where the process to identify Risk Events and Hazards (as defined by the ISO 31000:2019 standard) can be catalogued into a series of libraries that relate to each function and asset. Further, we can look to establish libraries for specific contexts that are reoccurring. To establish each of these libraries, we need to utilise our knowledge of the environment to determine what the range of potential 'occurrences or change of a particular set of circumstances' (ISO, 2018) that can occur to a function and asset.

In many ways the process can be described by the famous speech by Secretary of Defence Donald Rumsfeld to the Pentagon in which he said "because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we do not know we do not know. And if one looks throughout the history of our country and other free countries, it is the latter category that tends to be the difficult ones" (Rumsfeld, 2021).

Using Risk Intelligence to provides us with the opportunity to identify and develop the information sources that will allow us to take an 'unknown unknown' environment and Risk Events, and then develop a library of 'known unknowns'. Noting that the process is not to evaluate them

The benefits derived from a Risk Catalogue are best demonstrated by understanding the process by which one is constructed. This will also demonstrate the connection with Risk Intelligence, and its central importance to the delivery of successful outcomes.

to determine their likelihood/consequence, but just that the Risk Event is relevant for latter consideration. The next step is to identify the various Hazards that reflect the potential "element which alone or in combination has the potential to give rise to risk" (ISO, 2018). This allows us to identify what sources of information are required to feed information into the development of the Risk Events.

This development of information sources is critical to the effectiveness of the Catalogue as it provides a basis for the determination of what information is required, so that the assessments of likelihood/consequences can be undertaken in the context of future Risk Management Plans.

The Catalogue is often, but not always, a development from the Enterprise Risk Assessment, which defines the organisational objectives that in turn provides the bases by which the functions and assets that support operations can be valued. The benefits from this are that the organisation has the ability to develop the analysis processes that allow it to determine the information sources needed to collate an understanding of its threat and vulnerability sources. More importantly, it does so in a more timely manner so that the analyse can be provided with ample opportunity to put mitigations into practice in a preventative rather than a reactionary manner.

There are two further benefits that can be gained from the construction of the Risk Catalogue for an organisation. Firstly, the process of information identification, analysis and the development of Risk Events and Hazards can be incorporated into the review and monitoring process of the Risk Management Plan. This assists in ensuring that the process has the ability to identify new and emerging threats and vulnerability sources.

Secondly, the hardest part of any Risk Assessment is starting the Risk Event identification process. The questions around what information do I need, and what Risk Events and Hazards should I include, are key hurdles that can intimidate less experienced practitioners. A central tenant of Risk Intelligence is to provide an opportunity to learn from the historical analysis of risk, and the catalogue provides newer practitioners with a foundation of analysis to begin their assessment.

What makes a Failure Resilient Organisation?

So, to answer the question as to what makes an Organisation Failure Resilient? We could use the obvious answer that it's about ensuring that we have the 5 P's in place (Proper Planning Prevents Poor Performance) to ensure that it has the opportunity to consider risks in a timely manner, but that would not tell the whole story.

What this fails to acknowledge is that in a VUCA world we are now being presented with ever increasing 'Wicked Problems', as defined by Horst Rittel and Melvin Webber (Cooper, 2021), and we need to acknowledge that Prior Planning is not in itself enough to present solutions.

These problems are defined by their ever-changing nature, and the lack of ongoing solutions and complexity shows that we need to be able to move our thinking toward adding another 'P' (Prior) to the methodology by the application of Risk Intelligence. By using tools like Risk Catalogues, we are acknowledging that we need to ensure we have the right means by which we can make sense of our environment and our mitigations, and to ensure that when those situations where the risk is realised do occur, we are prepared to respond to failures in a timely manner, and most importantly to learn from them.

References

Apgar, D. (2006). Risk Intelligence: Learning to Manage What We Don't Know. Harvard: Harvard Business Review Press.

Bennis, W. (1989). Managing the dream: leadership in the 21st century. Journal of Organizational Change Management.

Bennis, W. G., & Nanus, B. (1997). Leaders: The Strategies for Taking Charge. New York: Harper Collins.

Blume, L. E. (2008). The New Palgrave Dictionary of Economics. Cornell University.

Buinessdictionary.com. (2020, June 22). Buinessdictionary.com. Retrieved from Business Dictionary: <https://www.dictionary.com/noresult?term=risk%20intelligence>

Cannon, W. B. (1915). Bodily changes in pain, hunger, fear, and rage. New York: Appleton-Century-Crofts.

Capowski, G. (1994). Anatomy of a leader: where is the leader of tomorrow? Management Review.

Collins, C. B. (2012). The Psychology Book (Big Ideas Simply Explained). New York: DK Publishers.

Cooper, K. (2021, June 28). "Wicked" problems: What are they, and why are they of interest to NNSI researchers? Retrieved from Network for Nonprofit and Social Impact: <https://nnsi.northwestern.edu/wicked-problems-what-are-they-and-why-are-they-of-interest-to-nnsi-researchers/>

Deal, T. a. (2000). Corporate Cultures: The Rites and Rituals of Corporate Life. Harmondsworth: Penguin Books.

Dervin, B. (1997). Semantic Scholar. Retrieved October 20, 2020, from <https://www.semanticscholar.org/paper/Given-a-context-by-any-other-name%3A-methodological-Dervin/1f5bd8835e28d968ace9cfb9d4c9639c306463f9>

Dictionary.com. (2021, June 21). Dictionary.com. Retrieved from <https://www.dictionary.com/browse/failure>

Douglas, M. (1991). Purity and Danger. Journal of Cross-Cultural Psychology.

Drinko, C. (2020, July 27). How to Avoid Binary Thinking and Think More Clearly. Retrieved November 2020, 7, from Lifehack: <https://www.lifehack.org/881768/binary-thinking>

Epstein, S. (2003). Handbook of Psychology: Personality and Social Psychology. Hoboken: John Wiley & Sons Inc.

Grossman, D. (. (2008). On Combat, 3rd Edition. Warrior Science Publications.

House, R. (1977). Leadership: The cutting edge. Carbondale, Edwardsville, Southern Illinois: University Press.

ISO: International Standards Organisation (2018). ISO 31000:2018 Risk Management - Guidelines. 2018. ISO.

Jaques, E. (1951). The changing culture of a factory. Tavistock Institute of Human Relations. London: Tavistock Publications.

K. Weick, K. S. (2015). Managing the Unexpected. Sustained Performance in a Complex World. Hoboken,

New Jersey: John Wiley & Sons.

Kahneman, D., & Frederick, S. (2002). Representativeness Revisited: Attribute Substitution in Intuitive Judgment. Heuristics and Biases: The Psychology of Intuitive Judgment, 51-52. Retrieved 10 30, 2020, from https://www.researchgate.net/publication/275859463_Heuristics_and_Biases_The_Psychology_of_Intuitive_Judgment

Kahneman. (2011). Thinking, Fast and Slow. Machmillan.

Kahneman, D. (2003). Maps of Bounded Rationality: Psychology for Behavioral Economics. The American Economic Review.

Kappa, P. T. (1991). Creating then communicating your vision. In Phi Theta Kappa Leadership Development Program. Jackson, MS: Phi Theta Kappa.

Katz, D., & Kahn, R. (1978). The Social Psychology of Organizations 2nd Edition. New York: Wiley.

Katz, R. I. (1955). Skills of an effective administrator. Harvard Business Review.

Kelly Coker, M. P. (2020, March 3). Understanding The Antecedent Behavior Consequence Model. Retrieved October 29, 2020, from Betterhelp: <https://www.betterhelp.com/advice/behavior/understanding-the-antecedent-behavior-consequence-model/>

Kotter, J. (1990). A force for change: How leadership differs from management. New York: Free Press.

Kotter, J. (2001). What leaders really do? Harvard Business Review, 79(11).

Kotterman, J. (2006). Leadership vs Management: whats the difference. Journal for Quality and Participation, 29(2).

Logan, D., King, J., & Fischer-Write, H. (2009). Tribal Leadership: Leveraging Natural Groups to Build a Thriving Organization. HarperCollins.

Presilience. (2021, October 18). Retrieved from Presilience: <https://presilience.info/>

Ross, L. (1977). Advances in experimental social psychology. New York: Academic Press.

Rumsfeld, D. (2021, Jun 12). Defense.gov. Retrieved from United States Department of Defence: <http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636>

Schein, E. H. (1990). Organisaitonal Culture. American Psychologist.

Schneider, B. B. (2014). The Oxford Handbook of Organizational Climate and Culture. Oxford: Oxford University Press.

Schneider, D. G. (2017). Can I see your hands. Irvine, CA: Universal Publishers.

Schneider, D. G., Johnston, D. P., & Down, K. (2017). What is risk intelligence. Risk Management Today, 43-46.

Senior, B. &. (2010). Organisational Change 4th Ed. Essex: Prentice Hall.

Taylor, J. (2019). Perception Is Not Reality. Psychology Today.

The Association for Qualitative Research. (2020, Oct 18). The Association for Qualitative Research. Retrieved from The Association for Qualitative Research the Hub of Qualitative Thinking: <https://www.aqr.org.uk/glossary/system-1-and-2>.

van der Eyden, T. (2002). Social Kingdom. Public Management of Society, 487.

Watson, C. M. (1983, March-April). Leadership, Management and the Seven Keys. Business Horizons.

Wechslet, D. (1944). The measurement of adult intelligence. Baltimore: Williams and & Wilkins.

AUTHOR BIO



James Jordan has a strong belief in his responsibility to educate and mentor the future workforce, he has ongoing interest in his responsibilities as an educator that began for his time as the Senior Instructor for the Protective Security Training College (Attorney Generals Department). Now in the newly created role of National Security Manager for Babcock Australasia, James is enjoying the opportunity to bring his experience to one of Australia growing Defence and Critical Infrastructure Service organisations.

[Connect with James on LinkedIn](#)

RED PILL. BLUE PILL. (PART 1)

BY DR PAUL JOHNSTON F.ISRM RPP

The launch of the recent Matrix: Resurrections movie provides an ideal opportunity for risk professionals to either revisit, or perhaps ask themselves for the first time, the question “have I been red-pilled or blue-pilled?”

Whilst this may sound somewhat dramatic, let’s explore the implications of what has become a popular culture metaphor that represents the choice between embracing the truth of reality (red pill) or the ignorance of illusion (blue pill). Before we start, however, I am not suggesting that we are plugged into the matrix. What I am asking is whether we are mindful of the processes and influences that can, and do, directly impact our risk-based decisions. Indeed, I am asking you to reflect on whether we make informed decisions or influenced decisions.

Whilst many will know the answer to this question based on the psychology of decisions alone, it is not the answer per se that I am interested in, but rather a reflection on the issues that underlie it.

In addressing these issues, the current world in which we find ourselves provides more than an ample range of matters to reflect on. Ranging from the COVID-19 virus and vaccination programs, to whether the world is flat or a globe, each issue is arguably associated with a relative truth.....and I ask those readers who just rolled their eyes to bear with me for a moment. I am not seeking to offer an opinion on any of these issues, but rather to ask the reader to unpack their own opinion – on these, and any other “fact” that we hold to be “true”. I am seeking to make the reader comfortably uncomfortable in considering and evaluating their own reality...their own truths.

What is truth?

This question has troubled mankind for millennia. Why is this so challenging? Surely, we can just refer to the common or collective knowledge of the world in which we live, and be comfortable in the truth that such represents. But is that sufficient? In most instances, it is probably safe to say “yes”, but in others, we find a range of opinions and vastly different conclusions apparently drawn from the same data.

In this sense, personal truths can be found where an individual’s beliefs and knowledge intersect. When it comes to fundamental quantitative matters such as $2 + 2 = 4$, I daresay we can reach an agreement. But, when it comes to more complex qualitative issues, such as defining the relationship between mankind and the environment, the sense of an absolute truth may be more challenging to define. This is where we particularly need to ask ourselves whether we are being informed or influenced? The answer may be the same in either case. But if we don’t interrogate the process, how can we be so sure of the integrity of the outcome?

Informed or influenced?

Data interrogation is something we do not do as frequently or as thoroughly as we should. The quality of our decision will not only depend on the quality of the data, but also the filters and lenses that we then apply to the same. The consideration of the issues associated with this is where we can find the answer to whether we are being informed or influenced.

To differentiate between “being informed” and “being influenced”, I offer the following definitions:

Being informed refers to explicit or overt delivery of information, in which clear language and communication is employed. This relates to the principles of cognitive psychology, and people overtly understand that they have been informed. In general terms, they regard the information received with objective credibility.

Being influenced, however, refers to a far more subtle process in which people may not be overtly aware of the relationship, point of reference, and value that they may have developed towards an idea of concept. This relates more to the principles of social psychology, and the credibility attributed to information in this sense is more subjective in nature.

The question of which is more “powerful” is where the challenge lies, and where we start seeing a divergence in individuals’ relative truths – even on issues that may be regarded as being absolute in nature.



Relative truths

Hence we return to the question as to what a “truth” really is. Personal values and the very delivery of information impact heavily on this. Regardless of what we like to tell ourselves, “who” told us and “how” they did it are both crucial considerations on what information is actively received, how it is regarded, and how we then employ the same in our subsequent decisions and actions. It is a simple fact that we are all biased one way or another – the key is to be mindful of this, and to be aware of how the underlying dynamics work.

Unfortunately, I do not have the space to address this fully in this context, but I do want to raise some key factors for your reflection, and to promote an increased awareness of those dynamics involved (issues which I will seek to address further in Part 2), as opposed to providing definitive answers...to which the reader will undoubtedly apply their own personal lenses in any case.

When we speak of data interrogation, the issues of data reliability, validity and comparability come readily to mind. After all, this is the means by which we initially assess the quality of the data that we are presented with. What I am referring to are the psychological processes that then kick-in and contribute to not only our assessment of the former, but also to how we interpret the same on a personal level.

In short, I am referring our own biases and heuristics – those cognitive shortcuts and rules-of-thumb that we apply when choosing which data source to listen to, and the credence that we attribute to them. I am also referring to the cognitive process and structures that essentially direct our attention, with these ranging from the Reticular Activating System (which directs our attention to those issues which are of interest to us, or that could do us harm) and Broadbent’s Filter Model of Attention (which is concerned with the issue of selective attention, given that we process information with limited capacity, with the selected information being processed early and with priority), to the principles of persuasion as defined by Dr Robert Cialdini (practices that can be used to significantly increase the chances that someone will be persuaded by you – namely those of reciprocity, scarcity, authority, consistency, liking, social proof and unity) and emotional intelligence as defined by Daniel Goleman (practices to recognise one’s own emotions and those of others, and how to employ the same to guide thinking and behaviour – namely self-awareness, self-regulation, motivation, empathy and social skills).

These, and similar, mechanisms have long been used by those seeking to influence others, with both positive (i.e. public safety officials) and less than desirable intent (i.e. criminals and cult leaders). I will let the reader allocate politicians to which category they think best. The principles remain the same – the difference between facilitating an exchange of information and manipulation is that of intent, which in itself can be difficult to determine due the very nature of how our cognition and personal risk related senses. That is why our sense of reality and our relative truths both vary on both a micro and macro scale.

We return to the question as to what a “truth” really is. Personal values and the very delivery of information impact heavily on this. Regardless of what we like to tell ourselves, “who” told us and “how” they did it are both crucial considerations on what information is actively received, how it is regarded, and how we then employ the same in our subsequent decisions and actions.

Reality

If this makes the ability to determine truth from falsehoods, and risks from opportunities, sound difficult, that is my point. Be mindful that our reality is essentially our perception of reality – particularly when we speak of complex issues or wicked problems. The manner in which we receive, process, store, and retrieve information relating to such things is a highly complex, and (unfortunately) relatively unreliable process – and that can be employed to influence our decisions significantly.

We need to enhance and maintain our awareness of these complexities, and to apply critical thinking and analysis to key issues, even to those that seem apparent. Indeed, we need to regularly reflect on, and review, our world view – our sense of reality and what we regard to be “normal”. Easier said than done, the result may surprise you in terms of the clarity this provides.

What’s next?

When we ask ourselves whether we have been “red-pilled” or “blue-pilled”, we give ourselves the opportunity to pause and reflect on the narratives and messaging that we are exposed to on a personal, organisational, and societal level. I am not suggesting that you become a “conspiracy theorist”, and that is an easy rabbit-hole to go down. Rather, I am encouraging you to become a truly critical thinker – and to ask of yourself “have I been informed, or have I been influenced?” ...“have I been red-pilled, or have I been blue-pilled?”



AUTHOR BIO

Editor of the ISRM ANZ Journal, Dr Paul Johnston is a Lead Risk Consultant with Risk 2 Solution, and is adjunct lecturer with ACU (Australian Catholic University) Executive Education. He holds a PhD in Public Safety Risk Management, a Graduate Certificate in Occupational Hygiene Engineering, and a Bachelor of Behavioural Science. With over 25 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](#)



STRATEGIC OPERATIONS IN THE NEW NORMAL

By Ron Amram

The modern operating environment is unlike any experienced in history, and is described as VUCA (volatile, uncertain, complex, and ambiguous). A VUCA environment has continuous, rapid, and unpredictable changes, complex and global networks, and a lack of clear cause and effect relationships to inform organisational decisions, at both strategic and operational levels (McCaughey, Beckmann, Schneider, & Down, 2017). As Weick and Sutcliffe explain, “we have to act in situations we can’t possibly understand. And the reason we can’t understand them is because all of us must apply limited conceptions to unlimited interdependencies.” (Weick & Sutcliffe, 2015, p. 3) – characteristics that have resulted in a fundamental shift towards strategic partnerships, supplier integration, agility, flatter organisational structures, and effective and rapid integration as essential organisational strategies (Bayraktar, Jothishankar, Tatoglu, & Wu, 2007).

In such a complex, fast-paced, increasingly competitive and networked global economy, strategic operations management is crucial to sustainable, competitive advantage, and can be seen as a uniting function of multiple organisational functions and spans outside of the organisation into its supply chain and stakeholders (Brown, Bessant, & Jia, 2018).

This observation demonstrates the critical importance of the connection between operations and strategy. Strategy refers to the long-term goals of the organisation. Operations relate to the short-term and ongoing supportive functions that enable the implementation and achievement of strategic goals. An operations strategy therefore “aims to ensure that key operational management activities are performed better than rivals so as to provide support for the overall strategy of the firm as well as serving as the firm’s distinctive competence” (Lowson, 2002, p. 38).

It is noted that the achievement of operational performance goals is strongly influenced by culture and the way strategies are interpreted and aligned with competitive priorities (McCradle, Rousseau, & Krumwiede, 2019). Both operational and overall strategies must therefore be clearly communicated and understood within the firm (Schneider, Sinclair, Najem, & Beckmann, 2018). Despite this important connection, however, over 66% of senior managers and

executives, and roughly 84% of frontline employees, do not understand the important of the link between strategy and operations (Sull, Homkes, & Sull, 2015).

The Hayes and Wheelwright Four Stage model is an excellent tool to identify the effectiveness, efficiency, aspirations and focus of the connection between operations and strategy at an individual, team, and organisational level. Although several decades old, and developed with manufacturing in mind, the model holds true in a modern context and across service industries just as well. The model is illustrated in Figure 1 below:

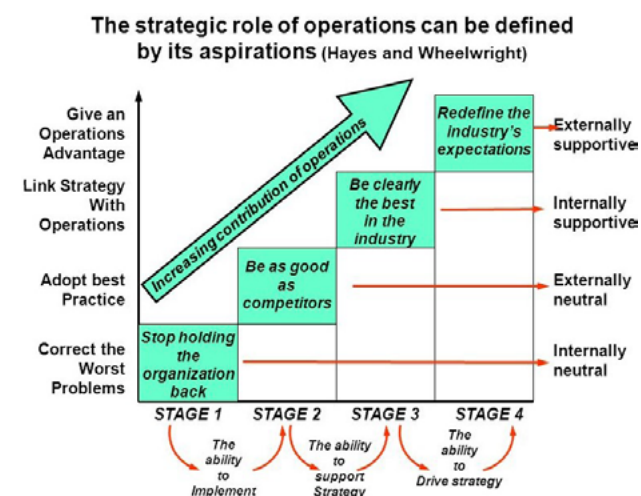


Figure 1: Hayes and Wheelwright Four-Stage Model¹

The four stages of the model are as follows:

- 1 Stage 1 (Internally neutral) – at this stage the organisation is underperforming operationally, compared to market and/or regulatory benchmarks, and tends to be reactive to market changes. There can be a myriad of reasons as to why operations are underperforming. However, the result is the same, and is that the organisation cannot maintain a competitive advantage or achieve strategic objectives. The aim at stage 1 is to achieve internal neutrality – in other words, to arrive at a state where operations don’t have a negative impact, don’t hold the organisation back, and are performing consistently.**

¹Retrieved from <https://slideplayer.com/slide/9873728/>

- 2 Stage 2 (externally neutral) – at this stage the organisation is aiming to maintain performance on par with competitors, and industry or market best practice. While at this level operations don’t hold strategy back, operations do not provide a competitive advantage, but allow for the implementation of strategy.**
- 3 Stage 3 (Internally supportive) – at this stage operations and strategy become positively linked. In other words, operations performance is aligned with overall strategy. At this stage the organisation can start using its operational efficiency to create and capitalise opportunities.**
- 4 Stage 4 (Externally supportive) – at this stage the operational ability of the organisation is leading the industry. Operations provide a strong competitive advantage, to the point where strategy can be developed around it. This is often where market innovators and disruptors sit.**

In a VUCA environment, the link between operations and strategy is more critical than ever. The environment in which organisations operate has changed dramatically as a result of COVID-19, technological leaps, artificial intelligence, and more. These have all had a significant impact on global supply chains, work culture, consumer behaviour, and more.

Organisations that seek to not only survive, but to thrive, in such an environment must examine the link between operations and strategy. But more so, they need to examine the culture of both, and to remember that the link between operations and strategy is, more often than not, people.

The Hayes and Wheelwright model can help identify where an individual, team, or organisation sits in terms of its operational capability, and draw the link to strategy from there. If nothing else, it provides an excellent starting point for analysis that can be used, over time, to truly transform an organisation.

References

Bayraktar, E., Jothishankar, M., Tatoglu, E., & Wu, T. (2007). Evolution of Operations Management: Past, Present and Future. *Management Research New*, 30(11), 843-871.

Brown, S., Bessant, J., & Jia, F. (2018). *Strategic Operations Management*. Routledge.

Lowson, R. H. (2002). Strategic Operations Management - The New Competitive Advantage? *Journal of General Management*, 36-56.

McCaughey, G., Beckmann, J., Schneider, G., & Down, K. (2017). Old vs New Embracing a New Risk Paradigm. Australian Catholic University.

McCradle, J. G., Rousseau, M. B., & Krumwiede, D. (2019). The effects of Strategic Alignment and Competitive Priorities on Operational Performance: The Tole of Cultural Context. *Operations Management Research*, 4-18.

Schneider, G., Sinclair, R., Najem, M., & Beckmann, J. (2018). *Risk Culture: Getting it Right*. Brisbane: Australian Catholic University.

Sull, D., Homkes, R., & Sull, C. (2015, March). Why Strategy Execution Unravels - and What to Do About It. *Harvard Business Review*, pp. 1-10.

Weick, K. E., & Sutcliffe, K. M. (2015). *Manging the Unexpected: Sustained Performance in a Complex World*. Hoboken, New Jersey: Wiley & Sons, Inc.

AUTHOR BIO



Ron Amram is the General Manager – Education, and WA/SA State Manager for Risk 2 Solution, and Director of Combat Arts Institute of Australia. A multi-award-winning university lecturer in several fields, Ron holds qualifications in Finance, Leadership, Risk Management, Psychology of Risk, Security, Music, Fitness, and Education. This diverse background has enabled Ron to work as a consultant in education, project management and risk management in multiple sectors for a decade before joining the R2S team. Ron has a passion for security and personal safety and is a world-recognised authority on personal protection. Ron has delivered training to thousands of people and organisations including government, law enforcement, security, military, close protection, and civilians all around the world.

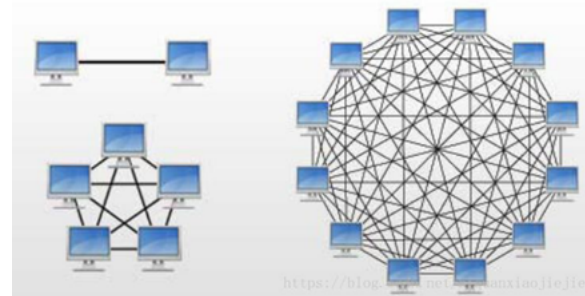
[Connect with Ron on LinkedIn](#)



Objects connected via IoT will include not only everyday electronic devices, but vehicles, equipment, and things not ordinarily thought of as electronic at all. Coffee mugs, shoes, food, clothing, shelter, tools, materials, parts, and subassemblies; commodities and luxury items, landmarks, and monuments; all the various items of commerce and culture will form the IoT. Against this backdrop, multiple networks, AI systems, AGIs, and ASIs will have access to or control over elements of IoT, such as cars, household appliances, machinery, and power generation.

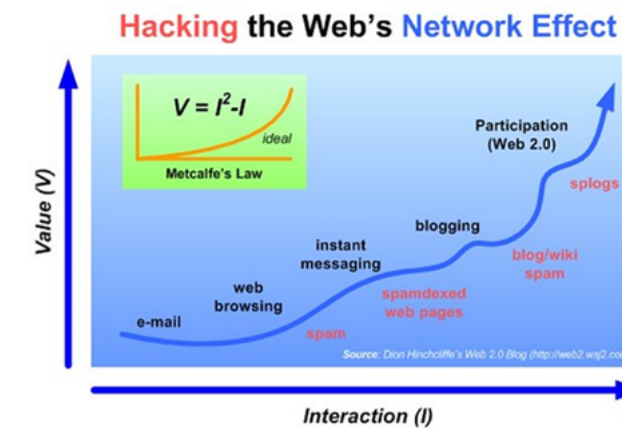
The addition of brain implants as man-machine interfaces, such as Elon Musk's Neuralink, means that humans will also form part of this IoT. The benefits will be amazing. But there is a lot to be legitimately concerned about. This interdependent mesh will leave not a single aspect of human society, culture, or environment untouched.

No discussion of this would be complete without a nod to perhaps the strongest effect within all this, Metcalfe's law. Metcalfe's Law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2), or $n(n-1)/2$, where n equals to number of nodes. Essentially, the more entities in a network, the more valuable the network becomes. Exponential growth is intrinsic to this law. And equally, so is complexity.



This Photo by Unknown Author is licensed under CC BY-SA

In a system where the utility of the network is a direct function of the entities already in the system, there is a powerful dynamic that tips towards complexity, and potentially winner takes all outcomes. Our risk universe will expand in the foreseeable future. And yet, because we are all parts of a system that already functions at a level well above us, the outline of this emerging enormous thing remains invisible to us.



This Photo by Unknown Author is licensed under CC BY

All we know is that from its very beginning, it will upset the status quo. Fierce pushback, disruption, and unintended consequences are all to be expected. What do we even call this very large masterpiece? A new life form? At its core, billions of humans are already joining an always-on layer of connectivity that comes close to directly linking brains to each other. Do not mistake this for a Black Swan event or events. There are already obvious interdependent risks. Risk management is not the only tool we have. But, applied correctly, it is perhaps one of our best tools.

The risks we are managing today pale compared to what is coming. Now, more than ever, the world needs competent risk management professionals who can advise our leaders and businesses. For the good of society, our organisations, our environment, and our families. William Gibson said, "The future is already here—it's just not evenly distributed". Similarly, the context for the 21st century is here—it's just not obvious yet.

References

[1] Kelly, Kevin. The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future. New York, New York: Viking, 2016.

[2] Kahneman, Daniel. Thinking, Fast and Slow. London: Penguin Books, 2012.

[3] Cialdini, Robert. Pre-Suasion: A Revolutionary Way to Influence and Persuade. New York: Simon & Schuster, 2018.

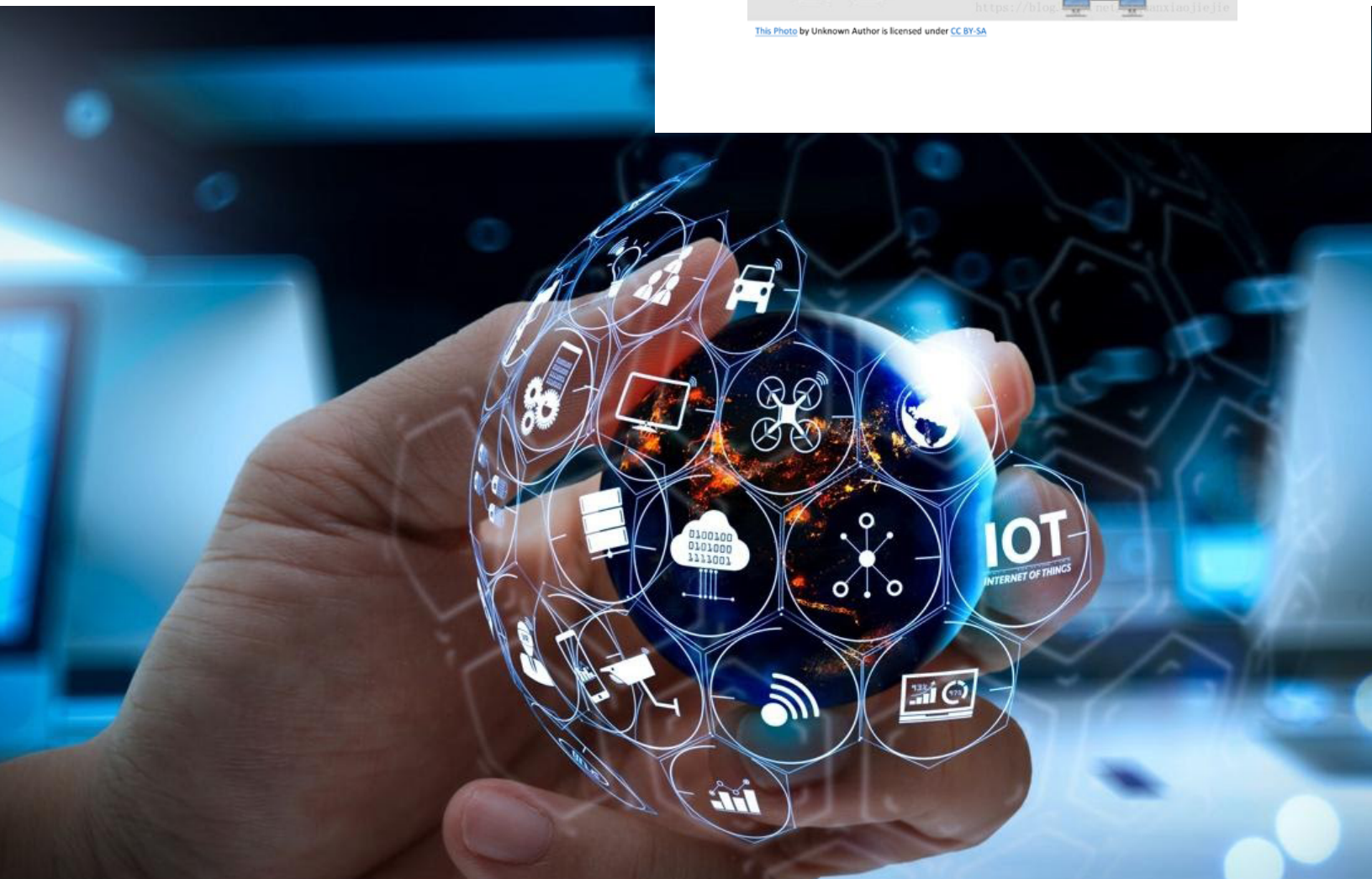


AUTHOR BIO

Julian Talbot F.ISRM holds a Master of Risk Management and has 30 of years risk management experience in the commercial, government, and not-for-profit sectors in Australia and internationally. His background includes roles as Senior Risk Adviser for the Department of Health and Ageing, Paramedic, and WHS consultant. Julian was also the co-founder, Chairman, and Divisional Manager of a \$350 million ASX listed entity.

He has served as Director of the Risk Management Institution of Australasia, Manager of Property & Security for the Australian government's most extensive international network, Security Manager for Australia's largest natural resources project, Operations Manager for geological exploration operation in East Africa, and Head of Risk for an international mining operation in Indonesia.

[Connect with Julian on LinkedIn](#)





ABOUT THE INSTITUTE OF STRATEGIC RISK MANAGEMENT

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 ANZ – KEY PERSONNEL

Dr Gav Schneider, Regional Chair
gav.schneider@isrm.org.au

Joe Saunders, Regional Vice-Chair
joe.saunders@isrm.org.au

Gary Sanderfield, Director of Governance and Partnerships
gary.sanderfield@isrm.org.au

Alicia Doherty, Director of Events
alicia.doherty@isrm.org.au

Janita Zhang, Regional Digital Marketing Manager
janita.zhang@isrm.org.au

Nadine De Lile, QLD Chair
qldchair@isrm.org.au

Ron Amram, WA Chair
wachair@isrm.org.au

Andrew Bissett, NSW Chair
nswchair@isrm.org.au

Julian Talbot, ACT Chair
actchair@isrm.org.au

Kerri Stephens, SA Chair
sachair@isrm.org.au

Pete Gervasoni, VIC Chair
vicchair@isrm.org.au

Gavin Pearce, New Zealand Chair
nzchair@isrm.org.au

ISRM
AUSTRALIA / NEW ZEALAND

INSTITUTE OF STRATEGIC RISK MANAGEMENT