PhD Research Design - How Can Organisational Learning Be Leveraged to Enable Antifragility of an Organisation?*

Edzo A. Botjes[1,2][0000−0003−0097−7375] and
co-supervisor - Tim Huygh[2][0000−0003−4564−7994]

[1] Xebia Security, Hilversum, the Netherlands, ebotjes@xebia.com
[2] Open University, Heerlen, the Netherlands, tim.huygh@ou.nl

Abstract The current VUCA worlds demands from organisations to be resilient and sometimes even antifragile. The domain focusing on staying relevant is that of risk management.
Information security is a sub-domain of risk management where the threats and response to the threats are very well documented. Within the sub-domain of information security there is an ever going rat-race between the people that want to exploit the threat and the people reacting to the thread by for example mitigating the thread.
In this research we want to look into the role of the learning organisation in the resilient behaviour of the organisation. Why the learning organisation? Since there are scholars that argue that human resilience is the key to organisational resilience.

Keywords: Organisational Learning · Resilience · Antifragility · Information Security

1 The Context

1.1 Unpredictable context threatens business continuity

The increased internal and external hyper-connectivity of organisations lead to more chaotic behaviour of their internal and external context [12,13,30,26,33].

To deal with this unpredictability, organisations aim to become resilient by for example implementing the agile way-of-working and/ or the adoption of a decentralised organisation design [14,15].

1.2 Business Continuity by resilience

Organisations need to adapt since the goal of an organisation is to stay relevant to its stakeholders [32]. Organisational Resilience is incorporated into the definition of Risk Management (ISO 31000), since Risk Management is the business function that aims to optimise the business continuity of an organisation. Business Continuity is achieved when the organisation stays relevant to its stakeholders. [3,4,5,6,7,10,29,8,9].

* Supported by Xebia Security

1.3 Business Continuity by antifragility

Resilience is the behaviour of the value of a system over time in response to a stressor event ($f(time) = value$) [15,31]. Antifragility is the behaviour of the value of a system in response to stress ($f(stress) = value$) [15,36]. Resilient behaviour maximized/ optimized leads to a system with antifragile behaviour. Antifragile is the antithesis of fragile [36]. In the current Body-of-Knowledge on antifragility [14,15] it is theorised that the capability of a learning organisation [34,24,23] is relevant for being resilient as it is relevant to be antifragile.

1.4 Human factor in resilience

In Hoogervorst (2017) [25] it is stated, in the Enterprise Engineering Sigma-theory, that the freedom of human behaviour is the only way to deal with the chaotic world. This is a logical deduction based on the theories on Variety [2,11] and Requisite Variety [11] and organisation behaviour (ref needed). Taleb (2012) [36] stated that the ideal Antifragile organisation is that of a self-employed worker.

1.5 One or more humans?

Organisation are complex-adaptive-systems [28,35]. Organisations can be defined as as "The purpose and function express that enterprises aim to fulfil or address certain (perceived) wants and needs of (certain) societal member of society at large by delivering products and/or services." [25]. Via these two lenses organisations can exists out of one person or out of more than one person. Therefor the attributes of an resilient organisation and an antifragile organisation can be applied to organisations of one or of more humans. This is relevant for the research (application) domain.

1.6 Extended Antifragile Attributes List (EAAL)

Research has shown that to become antifragile, certain types of resilience are relevant [15]. The relevant attributes to become antifragile and resilient are grouped in the EAAL. The ordering in the EAAL makes distinction between attributes relevant to organisation learning as defined by [34] and attributes that are not.

2 Research question

The attributes relevant to organisational learning are applicable to all three types of resilience as for an organisation with antifragile behaviour. This distinguishes the attributes relevant to organisational learning from the other attributes in the EAAL.

2.1 Main Research Question

This leads to the main research question: **How can organisational learning be leveraged to enable antifragility of an organisation?**

This question is relevant since the answer will have impact the design of the organisation. information security as part of risk management.

2.2 Sub-Research Question

This research will firstly limit itself to the application of the research within the domain of information security.

Information Security is a sub-domain of the risk management domain [17,26]. The exposure to incident in the Information security domain is ever increasing [17]. Information security recognizes the importance of the human factor in the response to incidents [1]. Information security recognizes the importance of absorbing change (conformance) as the enablement of creating value (performance) [26,27]. The cost of Information security incidents and the information security investments keep growing [38].

"Worldwide spending on information security products and services will reach more than $114 billion in 2018, an increase of 12.4 percent from last year, according to the latest forecast from Gartner, Inc. In 2019, the market is forecast to grow 8.7 percent to $124 billion." - Gartner in 2018 [20].

"The stakes are also getting higher. Gartner estimates by 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from less than 10% today." - Gartner in 2021 [21].

"Worldwide spending on information security and risk management technology and services is forecast to grow 12.4% to reach $150.4 billion in 2021, according to the latest forecast from Gartner, Inc. Security and risk management spending grew 6.4% in 2020." - Gartner in 2021 [22].

The research sub-question that arise are:

1. When is an organisation resilient and why is this relevant to an organisation?
2. What is the role of the learning organisation in the view of an organisation as a complex adaptive system?
3. Can personal behaviour be decoupled from organisational behaviour?
4. Is there a link between organisational behaviour and the learning organisation?
5. What is the best way to influence personal behaviour to influence organisational behaviour in the optimisation of organisational resilience?

3 Work/ Product breakdown structure

The following products are to be envisioned to be part of this research.

1. Research Tool RDS/Graph to improve the literature research method of snowballing and maybe even other types of systematic literature research.

2. Position Paper (Chaos) stating that there is difference between objective and subjective chaos and identifying the role of learning in this context.
3. Research paper on the role of resilience and antifragility in the domain of Risk Management and Information Security Management.
4. Research paper on the link between the Learning Organisation and Organisational Behaviour and Personal Behaviour.
5. Research paper on what defines and influences Personal Behaviour.
6. By somebody else: EAAL Framework replication (in the Organisational domain)
7. By somebody else: EAAL Framework validation in the IT domain

4 Relevant Theories

1. Variety definition by Asbey and Beer [2,11]
2. Viable Systems Theory by Beer [11]
3. Chaos definition by Lorentz [37]
4. Function and Construction by Dietz and Mulder [19]
5. Holistic view on Learning Organisation defined by Senge [34]
6. Risk Management by Hutchins [26]
7. Enterprise Governance of IT by Haes et al. [18]

5 Domain Lenses

1. Complexity Science in contrast to reductionist science
2. Complex Adaptive Systems in the context of Complexity Science
3. Organisation as Complex Adaptive Systems
4. (Organisational) behaviour of organisations
5. Resilience as specific organisational "behaviour"
6. Human behaviour as specific element of resilience
7. Human as a social being
8. Human as an emotional being.

6 Research Lenses

1. Science through the lens of Karl Popper (Verification & Falsification)
2. Science should be open (FAIR, OSF) otherwise verification and falsification is very limited.
3. Work will be done under CC BY-SA 4.0
4. Research will be done in public gitlab repositories.
   The research notes are versioned in a wiki (https://gitlab.com/edzob/complex_adaptive_systems-knowledge_base/-/wikis/home).
   The research project files are versioned in a repository (https://gitlab.com/edzob/complex_adaptive_systems-knowledge_base/-/tree/master/)
   This paper is versioned on gitlab (https://gitlab.com/edzob/complex_adaptive_systems-knowledge_base/-/tree/master/eewc.dc.2021) and
   this paper is versioned on overleaf (https://www.overleaf.com/read/wncjywdqdhpc).

7 Research dogmatic Statements

1. Replication of scientific experiments in the social domain are impossible due to the influence of human beings. This impacts the research design.
2. Enterprise Architecture (EA) and Enterprise Engineering (EE) are part of the social science domain.
3. Organisational Resilience is part of risk management.
4. Risk management aims to "optimise" business continuity.
5. CyberSecurity and Information Security Management are organisational capability in the domain of risk management.
6. The goal of an organisation is to stay relevant for its stakeholders.
7. Business continuity is about staying relevant.
8. Designing and managing the organisation to stay relevant is the shared goal of the expertises of risk management, Enterprise Architecture, Enterprise Engineering and and Enterprise Governance.

8 Produced Work

1. Botjes 2020 - MSc Thesis “Defining Antifragility and the application on Organisation Design” - peer reviewed by 4 in exam commission, 7 practitioners and 30 subject matter experts. [14]
2. Botjes 2021a - IEEE Paper “Attributes relevant to antifragile organizations” - peer reviewed by 4 experts. [15]
3. Botjes 2021b - Whitepaper on objective & subjective chaos “Design for chaos” - not-peer reviewed [16]

9 Changelog

version 2021-12-09

1. section 9 "changelog" added
2. typo’s fixed
3. added CC BY-SA 4.0 to running author
4. final sentence added to section 1.2 "Business Continuity by resilience"
5. made more clear difference between resilience and antfragility at the beginning of section 1.3 "Business Continuity by antifragility"
6. rewrite of 1.5 section "One or more humans?"
7. replaced "to optimise the resilience" by "to enable antifragility" in section 2.1 "main research question"
8. added reference to the relevance of Information Security in section 2.2 "Sub-Research Question"
9. extended the description at the beginning of section 3 "Work/ Product breakdown structure"

version 2021-12-07

1. added section 1.6 "Extended Antifragile Attributes List (EAAL)"
2. added paragraf at the beginning of section 2 "Research question"
3. added links to wiki, paper and research repositoru in section 6 "Research lenses"

version 2021-12-02 version submitted to EEWC-DC.

version 2021-10-11 created draft version.

References

1. Ali, R.F., Dominic, P.D.D., Ali, S.E.A., Rehman, M., Sohail, A.: Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences **11**(8) (2021), https://doi.org/10.3390/app11083383
2. Ashby, W.R.: An Introduction to Cybernetics. Chapman & Hall and University Paperbacks, London, UK (1956)
3. Aven, T.: On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Analysis: An International Journal **31**(4), 515–522 (2011), https://dx.doi.org/10.1111/j.1539-6924.2010.01528.x
4. Aven, T.: Foundational issues in risk assessment and risk management. Risk Analysis: An International Journal **32**(10), 1647–1656 (2012)
5. Aven, T.: The risk concept — historical and recent development trends. Reliability Engineering & System Safety **99**, 33–44 (2012), https://dx.doi.org/10.1016/j.ress.2011.11.006
6. Aven, T.: The concept of antifragility and its implications for the practice of risk analysis. Risk Analysis **35**(3), 476–483 (2015), https://dx.doi.org/10.1111/risa.12279
7. Aven, T.: Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research **253**(1), 1–13 (2016)
8. Aven, T.: Fundamental principles of risk management and governance: Review of recent advances. Japanese Journal of Risk Analysis **29**(1), 3–10 (2019)
9. Aven, T., Thekdi, S.: Enterprise Risk Management: Advances on Its Foundation and Practice. Routledge (2019)
10. Aven, T., Zio, E.: Knowledge in risk assessment and management. John Wiley & Sons (2018)
11. Beer, S.: The heart of enterprise: the managerial cybernetics of organization, Managerial cybernetics of organization, vol. 2. John Wiley & Sons, Chichester, West Sussex, UK (1979)
12. Bennett, N., Lemoine, G.J.: What a difference a word makes: Understanding threats to performance in a vuca world. Business Horizons **57**(3), 311 – 317 (may 2014), https://dx.doi.org/10.2139/ssrn.2406676
13. Bennett, N., Lemoine, G.J.: What vuca really means for you. Harvard Business Review **92**(1/2) (feb 2014)

14. Botjes, E.: Defining Antifragility and the application on Organisation Design. Master's thesis, Antwerp Management School (may 2020), https://dx.doi.org/10.5281/zenodo.3719389
15. Botjes, E., van den Berg, M., van Gils, Bart Mulder, H.: Attributes relevant to antifragile organizations. In: 2021 IEEE 23nd Conference on Business Informatics (CBI) (2021), https://dx.doi.org/10.1109/CBI52690.2021.00017
16. Botjes, E.A., Eusterbrock, T., Nouwens, H., van Steenbergen, M.: Design for chaos - a dya white paper by sogeti. https://labs.sogeti.com/wp-content/uploads/2021/11/Design-for-Chaos-a-DYA-white-paper-by-Sogeti-version-20211008-v1.pdf (11 2021), (Accessed on 12/02/2021)
17. Culot, G., Nassimbeni, G., Podrecca, M., Sartor, M.: The iso/iec 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal (2021), https://doi.org/10.1108/TQM-09-2020-0202
18. De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T.: Enterprise Governance of IT, Alignment, and Value. Springer International Publishing, Cham (01 2020), https://doi.org/10.1007/978-3-030-25918-1_1
19. Dietz, J.L., Mulder, H.B.: Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation. The Enterprise Engineering Series, Springer International Publishing (2020), https://www.springer.com/de/book/9783030388539
20. Gartner: Information security spending to exceed $124b 2019 | gartner. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 (aug 2018), (Accessed on 12/08/2021)
21. Gartner: Cybersecurity presentation guide for security and risk leaders. https://www.gartner.com/en/articles/the-15-minute-7-slide-security-presentation-for-your-board-of-directors (dec 2021), (Accessed on 12/08/2021)
22. Gartner: Gartner forecasts worldwide security and risk management spending to exceed $150 billion in 2021. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem (may 2021), (Accessed on 12/08/2021)
23. Garvin, D.A.: Building a learning organization. Harvard business review **71**(4), 78–91 (jul 1993)
24. Garvin, D.A., Edmondson, A.C., Gino, F.: Is yours a learning organization? Harvard business review **86**(3), 109–116 (apr 2008)
25. Hoogervorst, J.A.: Foundations of Enterprise Governance and Enterprise Engineering. Presenting the Employee-Centric Theory of organisation. Springer (2017), https://doi.org/10.1007/978-3-319-72107-1
26. Hutchins, G.: ISO 31000: 2018 Enterprise Risk Management. CERM Academy Series on Enterprise Risk Management, Certified Enterprise Risk Manager(R) Academy (nov 2018)
27. Huygh, T., Steuperaert, D., Haes, S., Joshi, A.: The role of compliance requirements in it governance implementation: An empirical study based on cobit 2019. In: Proceedings of Hawaii International Conference on System Sciences (HICSS 55) (01 2022), https://www.researchgate.net/publication/354718657
28. Jackson, M.C.: Critical Systems Thinking and the Management of Complexity. Wiley, 1 edn. (2019)
29. Jensen, A., Aven, T.: A new definition of complexity in a risk analysis setting. Reliability Engineering & System Safety **171**, 169–173 (2018)

30. Mack, O., Khare, A., Krämer, A., Burgartz, T.: Managing in a VUCA World. Springer, Cham, Switzerland (jul 2015), https://dx.doi.org/10.1007/978-3-319-16889-0
31. Martin-Breen, P., Anderies, J.M.: The bellagio initiative, background paper, resilience: A literature review. In: Resilience: A Literature Review. Brighton:IDS (11 2011), http://opendocs.ids.ac.uk/opendocs/handle/123456789/3692
32. Op't Land, M., Proper, E., Waage, M., Cloo, J., Steghuis, C.: Enterprise Architecture: creating value by informed governance. The Enterprise Engineering Series, Springer Science & Business Media, Berlin, Germany (oct 2008), https://doi.org/10.1007/978-3-540-85232-2
33. O'Reilly, B.M.: No more snake oil: Architecting agility through antifragility. Procedia Computer Science **151**, 884–890 (2019), https://dx.doi.org/10.1016/j.procs.2019.04.122
34. Senge, P.M.: The Fifth Discipline: The Art and Practice of the Learning organisation. A Currency book, Doubleday/Currency, New York, NY, USA (mar 1990)
35. Stacey, R.D.: Strategic management and organisational dynamics: The challenge of complexity to ways of thinking about organisations. Pearson education (2007)
36. Taleb, N.N.: Antifragile: Things That Gain from Disorder. Random House, New York, NY, USA (nov 2012)
37. Wikipedia contributors: Chaos theory — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Chaos_theory&oldid=944540733 (2020), (Online; accessed 12-March-2020)
38. Yaqoob, T., Arshad, A., Abbas, H., Amjad, M.F., Shafqat, N.: Framework for calculating return on security investment (rosi) for security-oriented organizations. Future Generation Computer Systems **95**, 754–763 (2019), https://doi.org/10.1016/j.future.2018.12.033