Institution: Coventry University		
Unit of Assessment: 17 Business and Management Studies		
Title of case study: Data-driven management strategies and operations: Towards a secure digital transformation of business and society		
Period when the underpinning research was undertaken: 2013 - 2018		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Professor Alexeis Garcia-Perez	Professor in Management Information Systems	2011 - present
Dr Anitha Chinnaswamy	Assistant Professor in Cyber Security Management	2014 - present
Period when the claimed impact occurred: 2013 - 2020		
Is this case study continued from a case study submitted in 2014? No.		

1. Summary of the impact (indicative maximum 100 words)

Digital transformation is core to today's business environment, but it creates risk (OECD). Although digital resilience is of major concern for organisations, many have yet to establish appropriate infrastructure, processes and behaviours. This research has examined these issues across a diverse set of commercial and public sectors, diagnosing and exploring poor practices/operational weaknesses which place organisations, investors and customers at risk. By understanding these issues, this body of research has **developed new models and better data-driven approaches**, creating impact by: (i) **raising organisations' awareness** of their vulnerabilities; (ii) **increasing their digital resilience**; and (iii) **protecting the integrity** of their operations.

2. Underpinning research (indicative maximum 500 words)

The research covers the area of digital transformation, notably data capture and management, and associated resilience, in infrastructure management and the digitisation of operations, initially in the transport and commercial sectors. This work then informed a partnership of local government authorities seeking to improve operational resilience. Lessons from one sector helped to shape investigations and the recommended solutions in other sectors. The 'shared' understanding of failures across these sectors, in the context of their digital transformation, in infrastructure, systems, processes, data management, behaviours and resilience, along with the emerging best practices for mitigation, proved invaluable in creating new models and approaches for managing digital transformation, data capture, data management and digital resilience.

Digital management strategies in the international transport and metals industries

In 2013, with funding (G1, KEEP-SAFE 1) from the Railway Safety and Standards Board, the Coventry team under Garcia-Perez led a consortium from the rail industry including, Network Rail, the Office of Rail and Road, Transport for London, London Underground and Thales. Key outputs were to develop models that showed the interdependencies between railway data, safety (of railway staff, passengers and communities) and infrastructure management costs. These models under-pinned a new data-driven predictive maintenance strategy for railway infrastructure.

Network Rail provided additional funding for KEEP-SAFE 2 (G2) in 2014, with an industry-wide consortium to put into practice and then assess the safety and efficiency learnings (R1) of G1. This consortium, led by Coventry, included Network Rail, Virgin Trains, Serco (IT service provider), Alstom Transport (rail manufacturer), and the University of Oxford. As specified by Garcia-Perez, using sensors and cameras, real-time infrastructure data were collected from a 'fast train' running on the West Coast mainline. Overhead line sagging, track irregularities, embankment concerns, vandalism, flooding and storm impact were revealed in real-time. Based on these data, a prototype solution for rail infrastructure monitoring and management was developed by the Coventry team and its validity demonstrated in an operational environment (in the jargon, to technology readiness level 6). Not only were actual risks identified, but the approach could be rolled out across the rail network, pre-empting system and network failures, reducing service interruptions and mitigating operating risks. This led to a digitally-enabled enhanced infrastructure management strategy for greater efficiency, safety and reduced maintenance costs. Addressing the safeguarding of such data under operational conditions was core to this research project.

Between 2016 and 2019, lessons from G1 and G2 informed the development of the New Business Models for Intelligent Transport Systems (NEWBITS) EU-funded project (G3). Garcia-Perez and Chinnaswamy led Coventry University's contribution to the project's development of principles of Intelligent Transport Systems (ITS) to interconnect people, vehicles and infrastructure (R4). The ITS covered all transport modes, including railway (G1-2, R1), maritime (R3) and automotive (R6), across Europe. Key policy recommendations to the EU Commission (R2, R3) included explaining the value of data for infrastructure management in ITS to interconnect all modes of transport, and what constitutes a successful industry-led approach to the adoption of the latest information technologies.

As a result of R1-6 and networking by the Coventry team, Garcia-Perez and Chinnaswamy engaged with the Future Aluminium Forum (FAF) and AlCircle to inform the cybersecurity and digital transformation strategies of the international metals industry. The team has explored with aluminium producers good and poor practices, exchanging knowledge about the dynamic cybersecurity landscape in the sector. A key output from this is an increased commitment by Forum members and progression towards a comprehensive approach to digital resilience for infrastructure management.

Digital resilience in local government

Based upon the outcomes of research with the transport and manufacturing industries, the research team worked with a UK local authority in 2018 (G4) to improve operational practices and digital resilience. The aim of G4 was to achieve the operational change required to overcome some of the key barriers to eGovernance and ICT adoption, particularly those related to data security and operational resilience (R2, R5, R6). The project involved testing the responses of staff to three types of simulated cyber-problems (phishing emails, malicious software and identity theft), to examine vulnerabilities and responses of the organisation. The research highlighted the digital vulnerabilities of local authorities; the need for better digital and ICT training for staff; and the importance of leadership, governance and incident management skills at senior management level.

3. References to the research (indicative maximum of six references)

R1. Garcia-Perez, A., Shaikh, S.A., Kalutarage, H.K. and Jahantab, M. (2015) 'Towards a knowledge-based approach for effective decision-making in railway safety'. *Journal of Knowledge Management* 19 (3), pp.641-659. DOI: https://doi.org/10.1108/JKM-02-2015-0078.

R2. Sallos, M.P., Garcia-Perez, A., Bedford, D. and Orlando, B. (2019) 'Strategy and organisational cybersecurity: a knowledge-problem perspective'. *Journal of Intellectual Capital* 20 (4), 581-597. DOI: https://doi.org/10.1108/JIC-03-2019-0041.

R3. Garcia-Perez, A., Thurlbeck, M. and How, E. (2017) 'Towards Cyber Security readiness in the Maritime Industry: A knowledge-based approach'. in *Proceedings of the International Naval Engineering* Conference. held 17-18 May 2017, Singapore.

R4. NEWBITS (2016) *Policy Recommendations: New Business Models for ITS* [online] available from http://newbits-project.eu/wp-content/uploads/2016/12/NEWBITS_PReB_final.pdf [23 February 2021].

R5. Cegarra-Navarro, J.G., Garcia-Perez, A. and Moreno-Cegarra, J.L. (2014) 'Technology knowledge and governance: Empowering citizen engagement and participation'. *Government Information* Quarterly 31 (4), 660-668. DOI: https://doi.org/10.1016/j.giq.2014.07.001.

R6. Morris, D., Madzudzo, G. and Garcia-Perez, A. (2020) 'Cybersecurity threats in the auto industry: Tensions in the knowledge environment'. *Technological Forecasting and Social Change*, 157 (120102). DOI: https://doi.org/10.1016/j.techfore.2020.120102.

Grants

G1. Garcia-Perez, A. (PI) (2013) *KEEP-SAFE 1*. Railway Safety and Standards Board (RSSB). Total grant amount: £33,000.00.

G2. Garcia-Perez, A. (PI) (2014) *KEEP-SAFE 2*. Network Rail. Total grant amount: £55,000.00.

G3. Garcia-Perez, A. (Work Packaged Leader) (2016 to 2019) *New Business Models for Intelligent Transport Systems (NEWBITS)*. European Commission: Horizon 2020 research and innovation programme, grant number: 723974. Total grant amount: €1,976,000.00 (£1,725,403.68), funding to Coventry University: €269,750.00 (£235,540.31). Available from https://cordis.europa.eu/project/id/723974 [24 February 2021].

G4. Garcia-Perez, A. (PI) (2018) *Cyber security monitoring and risk assessment in local government authorities: a social engineering exercise.* UK Local Government Authority. Total grant amount: £10,000.00.

The quality of the research is conveyed through its publication in top-ranking journals in field, its use by other researchers, and through the award of grants from international and national funders.

4. Details of the impact (indicative maximum 750 words)

The research (R1-6, G1-4) has informed the digital transformation of organisations in the UK and internationally by improving infrastructure and operational management strategies leading to the following impacts: i) influencing the digital transformation strategy of the railway industry in the UK; ii) new EU policies to influence the development of data-driven interconnected ITS; iii) raising awareness of the challenges of digital transformation and cybersecurity in manufacturing; and iv) changing digital management policies and practice of local authorities in the UK.

Improving digital transformation in transport in the UK and Europe

The development of a prototype solution for data-driven infrastructure management (R1, G1, G2) enabled changes in infrastructure management policies and practices at Network Rail (S1). The research informed investments in a new data-driven predictive maintenance strategy. The outcomes have helped Network Rail improve safety and efficiency, reducing maintenance costs, failures and repairs, while improving quality of service and safety for passengers and staff. Assuming a 10% effectiveness, the prototype is estimated to have had a financial impact of £8 million over its first 12 months. The NW&C Region Systems Review Panel Chair from Network Rail described the research in the following way (S1):

> *"This demonstrator has shown the potential of implementing a data-driven approach to predictive maintenance in our efforts to improve safety and efficiency and to reduce maintenance costs, failures and repairs on the overhead line equipment and to improve quality and safety for passengers and staff. … The work… gave us an insight and informed our thinking"* NW&C Region Systems Review Panel Chair, Network Rail (S1).

As a result of R1, G1, G2, Network Rail has developed a technical specification for the rail industry supply chain to fit a permanent intelligent instrumented pantograph to passenger trains and Network Rail's monitoring fleet. Network Rail has also used the research (R1, G1, G2) to inform its digital transformation strategy*, "particularly its data driven strategy for improved safety and efficiency"* (S1).

The outcomes from R1, G1 and G2 informed the development of new policies and business models for the EU NEWBITS project (R2-4, G3). These policies were presented to the European Directorate-General for Mobility and Transport (DG-MOVE) at the European Parliament on the 21st March 2019. The policies were seen as central in moving from a fragmented and unconnected transport system, to an interconnected multimodal data-driven Intelligent Transport System (ITS). The ITS design was implemented to guide research and developments across Europe.

> "[*The research] became... key … in the success of the NEWBITS project in the delivery of policy recommendations to the European Commission (DG MOVE), the European Parliament (European Conservatives and Reformists Group), as well as representatives of stakeholders (both industry and members of ITS community)"* Senior Advisor, IRF Global (S2).

Influencing digital transformation in international manufacturing

The principles of data management and resilience developed in (R1-R6, G1-4) have been adopted by the international aluminium manufacturing sector within a project at the sector level. Since 2018, our team has spoken regularly at the annual conference of the Future Aluminium Forum and other events (S4). The research and collaborations have helped to raise awareness at an international level of the challenges associated with delivering successful digital transformation strategies, through specialised outputs (S7), including webinars, podcasts, interviews, articles and workshops. As a result of R1-6 and G1-4 and research within the aluminium manufacturing sector, Garcia-Perez was invited to become a member of the International Advisory Board for the Future Aluminium Forum Digital (S6), to work in collaboration with the industry to further enhance digital transformation while mitigating the associated data risks. The research (R1-R6, G1-G4) and industry engagement have changed policy and practices of leading aluminium industry manufacturers to effectively deal with the cybersecurity challenges. Overcoming these challenges is essential to the infrastructural and operational change required for the digitisation of the factory and its entire supply chain (S5).

> *"[The research] played a pivotal role in introducing this sector to the risks associated with a breach and the need to have a response plan. As with any heavy industry, the risks are huge if a plant is breached and worker safety is of the highest importance.*
>
> *[Garcia-Perez] continued to support the Future Aluminium Forum events as a member of the Advisory Board and also held a dedicated 'Cyber Resilience' Workshop for delegates in 2019, which recreated a cyber-attack and highlighted how different areas of the company should approach the situation and react effectively"* Conference Director, Future Aluminium Forum Digital (S4).
>
> *"I found the Cyber Security Workshop very informative … I have already communicated the main takeaway message for me which was that we should be putting a Cyber Security Strategy in place and assessing our digital resilience to the possibility of an attack on our company"* Global Industry Manager (Metals), AMETEK (S5).

As a result, industry representatives have been able to collaborate in outlining the strategy to prepare for, respond to and recover from a cyber-attack. Such attacks have occurred for real in this sector, with the most significant one in 2019 having a €50 million cost for the organisation affected.

Improving digital resilience in local government

This work (G4, R2, R5, R6) led to raised awareness and changes in policies and practice of the senior management board and staff at a UK local authority in 2018 (G4, R2, R5, R6). The board redesigned the ICT and digital transformation strategy, to focus upon improving cybersecurity and eGovernance in the organisation (S3). These elements are now seen as a pre-requisite for successful operation and data compliance in this sector. As a result of this research and its conclusions:

> *"We got our staff talking about the issue, and what to look out for. We have seen an upturn in the reports of phishing that we are receiving to our service desk, which proves that there is a greater understanding and a heightened vigilance around the organisation.*
>
> *We have also made changes to the way in which we actually deal with cybersecurity incidents, by implementing a process to log and deal with phishing reports in a timely fashion, meaning that we are taking a proactive approach to the cyber threats. Thanks to our collaboration… the council now have a clear insight into staff attitudes towards cyberattacks, which challenged some of the beliefs we held regarding their awareness levels"* Services Manager, UK Local Government Authority (S3).

5. Sources to corroborate the impact (indicative maximum of 10 references)

S1. NW&C Region Systems Review Panel Chair, Network Rail (2020). *Impact of the case study on the Railway Systems Industry testimonial letter* to Coventry University.

S2. Senior Advisor, IRF Global (2019). *NEWBITS success – Impact of the case study of the British Railway (Dr Alexeis Garcia-Perez) testimonial letter* to Coventry University.

S3. Services Manager, UK Local Government Authority (2020). *Testimonial letter* to Coventry University.

S4. Conference Director, Future Aluminium Forum Digital (2020). *Testimonial Email* [email] [14 July 2020].

S5. Centre for Business in Society (CBiS), Coventry University (2020). 'CBiS Supports Effort of the Aluminium Sector to Improve its Digital Resilience – Feedback from Cybersecurity Workshop'. *Centre for Business in Society Spring Newsletter* April 2020 (9), p. 8. Available from: https://www.coventry.ac.uk/globalassets/media/global/08-new-research-section/cbis/newsletters/issue-9----v2-spring-newsletter-2020.pdf [24 February 2021].

S6. Future Aluminium Forum Digital *Advisory Board* [online]. Available from: https://futurealuminiumforum.com/advisory-board [24 February 2021].

S7. Outputs influencing digital transformation in international aluminium manufacturing:

- Hingley, P. (2020). *Building cyber resilience in Aluminium manufacturing* [online webinar]. Available from: https://vimeo.com/430643962 [24 February 2021].
- Garcia-Perez, A. (2020). 'Are you cyber aware?' [Podcast with Bloxsome, N.] [online]. Available from: https://anchor.fm/nadine-bloxsome/episodes/Aluminium-ON-AIR-Are-you-cyber-aware-eda7uk [24 February 2021].
- Garcia-Perez, A. (2020). 'The cyber security challenge for advanced manufacturing', *Aluminium International Today: The Journal of Aluminium Processing and Production* 31 (4), 41-42. Available from: https://issuu.com/quartzbusinessmedia/docs/aluminium_international_today_july_?e=31308538/63248280 [24 February 2021].