Problem Statement
Valuing TfNSW Reputation Damage from Cyber Risk

VWB 2019-01

Valuing Wider Benefits

Problem Description

Question	Response
Description of the problem and purpose of the proposed research	Transport for NSW's (TfNSW) Group Cyber Defence (GCD) has begun analysing and quantifying key cyber security risks across the Transport cluster to develop business cases for targeted initiatives to mitigate/reduce these risks. However, not all cyber security risks can currently be measured in dollar value terms. In particular, the risks associated with reputational damage as a result of a cyber-attack, have been challenging to measure. Two examples are prominent in the industry. In 2017, the Swedish Transport Agency admitted to a huge breach of confidential data held in its driver's license and vehicle registration database, through an outsourcing arrangement with IBM. Due to a lack of adequate safeguards, unauthorised personnel at IBM subsidiaries in Eastern Europe had access to large numbers of confidential records. Besides the entire national driver's licence database, the records included information on intelligence agents, military and police transport and personnel, people with criminal records and those in witness protection programs. In the political fallout, two ministers stepped down, and the agency director was dismissed and fined.[8] Another example took place in March 2018 with the city of Atlanta in the United States which was subjected from a ransomware attack. Municipal employees who attempted to log on to affected systems were greeted with an anonymous demand for a six-bitcoin payment — equal to about US$51,000 at the time — in exchange for a key that would remove the virus and allow city workers back into their files. Many city services and programs were affected by the attack, including utility, parking, and court services. City officials and residents were forced to complete paper forms by hand and up to a third of software programs used by the city remained offline or partially disabled.[9] Both examples showcase how such breach cause major disruption to operational functions, affect individuals and can impact the reputation of Government. The objective of the research is to produce a rigorous evidence base around the economic cost of reputational damage from a cyber-attack, both to TfNSW and the Government more broadly, as well as understanding the economic value of a personal record to TfNSW. This will assist in developing a more robust justification for including cyber-security related economic parameters in the "TfNSW Principles and Guidelines for the TfNSW Cost-Benefit Analysis Guide." The research project will focus on the below hypothesis: *"TfNSW's reputation will be significantly impacted by cyber-attack, in an economically quantifiable way."* The NSW Government relies on digital technology to deliver services, organise and store information, manage business processes, and control critical infrastructure[10]. The increasing global interconnectivity between computer networks has dramatically increased the risk of cyber security incidents. Such incidents can harm government service delivery and impact the public, and may include the theft of

[8] https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html and https://www.theguardian.com/technology/2017/aug/01/sweden-scrambles-to-tighten-data-security-as-scandal-claims-two-ministers

[9] https://en.wikipedia.org/wiki/2018_Atlanta_cyberattack, and https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/

[10] https://www.audit.nsw.gov.au/our-work/reports/detecting-and-responding-to-cyber-security-incidents-

Transport for NSW T 8202 2200 | F 8208 2209
18 Lee Street, Chippendale NSW 2008 | PO Box K659, Haymarket NSW 1240

Question	Response
	information, denial of access to critical technology, or even the hijacking of systems for profit or malicious intent. Today more than ever, the NSW Government promotes the use of data and information to improve its services and to benefit its citizens[11] [12]. Whilst protection against malware, hacking and data theft is growing in importance and methodologies, process, policies and procedures are put in place to mitigate such risks[13] the NSW Government is under scrutiny to demonstrate improved Cyber protection. Examples of risks include: a) theft of a large holding of personal information – customer or employee data, b) a ransomware attack that renders data and IT systems inaccessible, resulting in the inability to provide customer-facing services for an extended period of time, and/or permanent loss of data c) An attack affecting the availability or integrity of a safety-critical system. TfNSW's GCD is using FAIR – Factor Analysis of Information Risk – as a trusted modelling framework to analyse these risks and gain a better understanding of their economic magnitude. FAIR identifies six forms of loss that can result from a loss event: 7) Productivity loss 8) Response costs 9) Replacement costs 10) Competitive advantage loss 11) Fines and judgements 12) Reputation damage Loss types 1, 2, 3, and 5 can be calculated in a fairly straightforward way. Loss type 4, competitive advantage is more applicable to the commercial sector. Loss type 6, Reputation Damage, has been challenging to quantify and often represents the largest cost of a cyber incident in profit-driven companies, as it includes uncaptured revenue due to lost customers. The loss events from a cyber-attack would definitely result in the loss of public trust impacting the reputation of TfNSW and more broadly the NSW Government. However, there appears to be no clear methodology or framework for quantifying these losses in Australia or NSW for public sector and government entities. Rather, it has been noted that: *"Approaching reputation in the public sector entails complexities in terms of goals, needs, audiences, definitions and resources that are different from that of the private sector*".[14] The ultimate aim of this research project is to quantify reputational damage, focussing on the following two areas within the current TfNSW economic guidelines: 3) An economic valuation framework for reputational damage to TfNSW arising from a cyber-attack. This question will require foundation level analyses into the question of how reputation damage is assessed for public sector organisations.

[11] https://www.digital.nsw.gov.au/policy/data-information
[12] https://www.digital.nsw.gov.au/policy/cyber-security-policy/useful-links
[13] https://www.ipc.nsw.gov.au/data-breach-guidance

[14] Public Sector, Trust and Reputation in the Public Sector, 2016 SAGE Publications

Transport for NSW T 8202 2200 | F 8208 2209
18 Lee Street, Chippendale NSW 2008 | PO Box K659, Haymarket NSW 1240

Question	Response
	4) An economic value of a record of personal (customer) information. This would provide an approach to quantify the cost to Transport and the NSW Government of a major breach of personal information. There is existing research on the cost of a data record and the aim of this research is to confirm or challenge these costs. It is anticipated that the research will also provide a foundation for identifying and evaluating the success factors in implementing cyber initiatives and could be used in benefits realisation cases.

Hypothesis & Variables

Question	Response
For explanatory research, please describe a clear hypothesis with variables for testing **For exploratory research,** please describe how the proposed research will contribute to future explanatory research	TfNSW's Group Cyber Defence is interested in understanding how to quantify reputation damage as a result of a cyber-attack. This has two components: 1. Assessing reputation damage and quantifying the damage such that it can be used in Cost Benefit Analyses. 2. Assessing the value of a record of personal (customer) information. This would provide an approach to quantify the cost to Transport of a major personal information data breach. The research project will focus on the below hypothesis: *"TfNSW's reputation will be significantly impacted by cyber-attack, in an economically quantifiable way."*

Strategic Criteria & Alignment

Question	Response
Alignment with strategic theme	This Problem Statement is aligned with the research theme 'Valuing Wider Benefits. The research focuses on producing a rigorous evidence based justification for quantifying the benefits of transport investments and programs. It is also aligned with the 'Safety and Security' theme to improve the security of employees and contractors in delivering the future transport network for NSW, and the security of its customers. The Problem Statement aligns with the Future Transport Technology Roadmap and the Future Transport 2056 Strategy.
External driver of change analysis **Outline how the research will better position TfNSW to respond proactively to macro drivers of change**	Macro drivers of change that affect the state of NSW addressed in the research: **Social:** Digital crime and digital terrorism are increasingly becoming the norm and have a direct impact on society and citizens level of trust in government organisations. This has heightened risk for government particularly as agencies implement digital transformation, collect valuable personal data, and open up data sources to the community. **Political:** Government reputational loss is directly linked to political leadership and its environment. Cyber risk and threats to public service agencies can impact political leadership. **Economic:** The cost of Cyber-attacks and that of Cyber protection is growing for government organisations. Cyber-attacks have direct impacts on our state and national economy, threatening the stability of our nation as a trading partner.

Transport for NSW T 8202 2200 | F 8208 2209
18 Lee Street, Chippendale NSW 2008 | PO Box K659, Haymarket NSW 1240

Question	Response
Potential research impact	The research project output will enable Transport to develop rigorous business cases for well-targeted investment to reduce cyber risk. Outputs will also be applicable more broadly in modelling cyber risk across the whole of the NSW Government and other types of enterprise risk across Transport and the NSW Government, where reputation damage is a factor. The research project will form the foundation for future work in evaluating the cyber initiatives that were implemented post-business case, and identifying the success factors.

Technical Criteria

Question	Response
Innovation **Outline how the proposed research will result in new knowledge**	This research would generate new knowledge for new approaches relating to modelling cyber risk across the whole of the NSW Government. Literature and research has been driven from the US. More research is needed to reflect the impact of cyber-attacks on NSW government reputation and trust.
Basis in completed research and/or observed practice	In the USA, the Online Trust Alliance (OTA) report [15] states that an estimated two million cyber-attacks in 2018 resulted in more than $45 billion in losses worldwide as local governments struggled to cope with ransomware and other malicious incidents. Analysis also suggest a rise in reported ransomware attacks against state and local governments in the US. Australia 2020 Cyber Security Strategy[16] references the Joint Cyber Security Centres (JCSCs) established across Australia to assist in developing evidence to further research in this area. There is little research evidence available that applies to the NSW and Australian public sector.
Feasible data requirements	The research project will aim to capture international data sources as well as new datasets for both commercial and government cyber incidence of cyber-attacks and/or data breaches. This must be accounted for in the research proposal. The researcher may have to undertake field measurements to obtain the majority of data required for the research. Datasets will in the first instance be limited to publicly available data sources. As the research progress through each milestones, TfNSW will then assist on as needs basis.

[15] Online Trust Alliance (OTA), https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/
[16] https://www.homeaffairs.gov.au › reports-and-pubs › files › cyber-security.

Transport for NSW T 8202 2200 | F 8208 2209
18 Lee Street, Chippendale NSW 2008 | PO Box K659, Haymarket NSW 1240

Level of Collaboration & Resource Requirements

Question	Response
Level of collaboration **Please select the level of collaboration required to complete the proposed research**	**1. 'Quick-Fire' Research** ☐ Intense bursts of research activity (e.g. under 8 weeks). Intended to make use of 'hackathon'-type environments, where students/researchers work collaboratively and intensely on particular problems involving data interrogation and visualisation.
	2. Undergraduate Final-Year Research ☐ Suitable for final-year undergraduate students (e.g. capstone, Honours) as part of the research requirements for their undergraduate degree (i.e. 1 to 2 semesters).
	3. Higher Degree Research ☐ Project may form whole or part of a postgraduate research degree (i.e. Masters, PhD), and contribute to new knowledge (i.e. 1 to 3 years).
	4. Major Collaborations and Funded Research ☐ Project may form the basis for a significant collaboration agreement between TfNSW and the relevant research institution, including major competitive grant funding (e.g. Australian Research Council funding with TfNSW as an industry partner).
Comments	We anticipate that the research project will be part of a broader postgraduate research program. Research may propose an extensive literature review prior to engaging and developing cost evaluation frameworks for TfNSW lost reputation and impact. Timeframe for the delivery of this project is important. It is anticipated that first results will be shared before June 2020
Supporting TfNSW resources	The TfNSW Group IT and Group Cyber Defence will assist the researchers in using real use case and data available.

Transport for NSW T 8202 2200 | F 8208 2209
18 Lee Street, Chippendale NSW 2008 | PO Box K659, Haymarket NSW 1240