Valuation of Reputation Damage for Transport Cyber Attack

Greg Austin and Glenn Withers*

2 August 2021

*This report was authored by Professor Greg Austin, Professor of Cyber Security, Strategy and Diplomacy at UNSW Canberra and now Head of the Programme on Cyber, Space and Future Conflict at the International Institute for Strategic Studies; and Professor Glenn Withers, Distinguished Professor of Economics and Public Policy at ANU and Adjunct Professor at UNSW Canberra. The work was reviewed by Dr. Peter Abelson, author of Commonwealth *Handbook of Cost-Benefit Analysis* and Managing Director, Applied Economics Pty Ltd. The project was commissioned by Transport for New South Wales. The views expressed are the responsibility of the authors.

PREFACE FROM TRANSPORT for NSW

The NSW Government promotes the use of data and information to improve its services and to benefit its citizens. This includes the use of data to inform the continuous improvement of cyber security capability against a rapidly evolving threat environment.

The benefit of any investment in cyber security is based on how much it reduces risk. An initiative that has a large impact on reducing risk provides a greater benefit than one that does not have much impact. Therefore, in prioritising cyber security investments, it is important to understand by how much each investment is likely to reduce risk.

Most organisations classify risks on a scale, with values such as very high, high, medium, and low. This is sufficient for most risk management purposes; however, it is less useful for making business decisions to prioritise investments. Decision makers have questions such as 'how much risk do we currently have in this area?' and 'if we implement this solution that costs $x, by how much will we reduce our risk?'

When risks are classified using a subjective scale, it is difficult to answer these questions in a satisfactory way. For example, the answer to the above questions might be 'our risk is currently high, and if we implement the solution that costs $x, our risk will be less.' This does not allow decision makers to evaluate the benefit against the cost of a proposed initiative. For these reasons, many organisations are quantifying risks, in order to provide better answers to these questions.

FAIR (Factor Analysis of Information Risk) is an internationally accepted model and methodology for quantifying cyber and operational risk. In 2019, the cyber security function within Transport for NSW began investigating using FAIR to quantify risks arising from cyber threats, in order to develop more robust business cases for cyber investments and to prioritise cyber investments to achieve the best outcomes in risk reduction.

Using FAIR, a given risk scenario is quantified in terms of how often it is likely to occur (loss event frequency) and the impact it would have if it did occur (loss magnitude). FAIR defines six categories of loss for forecasting impact: productivity loss, response costs, replacement costs, fines and judgements, competitive advantage, and reputation damage.

The first four of these are relatively straightforward to estimate. The fifth form of loss, competitive advantage, does not apply in many public sector risk scenarios.

A pharmaceutical company, for example, would incur loss of competitive advantage if its intellectual property were stolen through a cyber-attack.

The sixth form of loss, reputation damage, is problematic when using FAIR within the public sector. Public trust is extremely important for public sector organisations; therefore, it does not seem appropriate to ignore this form of loss in risk calculations in the same way that competitive advantage can be ignored and therefore we take Public Trust as a proxy for Reputation in the FAIR analysis.

However, how should it be estimated? The commercial sector generally uses profit lost due to losing their customers to project this form of loss. For example, a technology provider with a poor reputation for cyber security would lose many customers and hence damage profits. This method does not seem a good fit for estimating reputation damage losses within the public sector where non-profit arrangements are common.

This missing piece of the risk quantification puzzle prompted the following research paper. In 2020, Transport for NSW commissioned academic research to assist in understanding how to forecast this form of loss for risk scenarios arising from cyber threats. Since other public sector organisations internationally were facing the same question, it was seen that the research would be of interest not only to NSW but to any public sector organisation seeking to quantify risk.

Transport for NSW has established economic parameters used for cost-benefit analysis in many types of business cases. The aim of the research was to provide an evidence base for adding economic parameters to this document that could be used in conjunction with FAIR for cyber investment business cases. Accordingly, the research used methodologies consistent with those used to establish other Transport economic parameters and consistent with methodologies used by NSW Treasury in evaluating business cases.

The content of the report reflects the independent analysis from the researchers and is not official Transport policy.

CONTENTS Page

EXECUTIVE SUMMARY:

1. Cyber-security attack has become an increasing focus for business and government planning. Infrastructure networks are of special concern. However, a less understood dimension of such problems is the effect of cyber-attacks on reputation.

2. This Report reviews this issue of reputation damage for the case of transport cyber-attacks. It does so in the context of transport operations in New South Wales (NSW).

3. The report accordingly first provides analysis of the nature of reputation loss from cyber-attack and the nature of risk management for transport service delivery arrangements in New South Wales. To support this, it examines the general reputation loss literature relevant to cyber damage, and then the publicly documented nature of administrative portfolio arrangements in place for cyber security management, including for business planning for new cyber investments.

4. Reputation issues arising from the literature and portfolio review process are then examined through reporting discussion with key stakeholders, and from a focus group process reflective of wider citizen perspectives on these matters.

5. Given the knowledge obtained, conclusions are offered on how to take forward appropriate evaluation processes for future planning for cyber risk for transport. The core for this is seen to be through enhancing cost-benefit analysis to explicitly incorporate reputation damage. It is proposed that this be done through "contingent valuation" survey methods, which give a monetary measure of such potential reputation loss. Complementary or alternative ways forward on reputation loss matters for transport are also suggested including discrete choice analysis and stock valuation.

INTRODUCTION:

Cyber matters are clearly important for modern transport operations. Transport for NSW's (TfNSW) Transport Cyber Defence (TCD) area continually analyses key cyber security risks across the NSW Transport cluster and seeks to quantify them where possible to develop business cases for targeted initiatives to mitigate/reduce these risks.

However, not all cyber security risks can currently be directly measured in dollar terms for such business case analysis. In particular, the risks associated with reputational damage as a result of a cyber-attack vary with the circumstances and they have been challenging to measure due to their relatively intangible nature.

The objective of the research reported here and commissioned by TfNSW, is to help bridge that valuation gap by producing a more rigorous evidence base around considering the economic cost of reputational damage from a cyber-attack, both to TfNSW and the Government more broadly. One particular focus is to assist in developing a more robust justification for including related cyber-security related economic parameters in the "TfNSW Principles and Guidelines for the TfNSW Cost-Benefit Analysis Guide."

The research plan reported herein had two major elements, around which this Final Report is structured. Thus, following some further introductory discussion, the Report is divided into Part A and Part B.

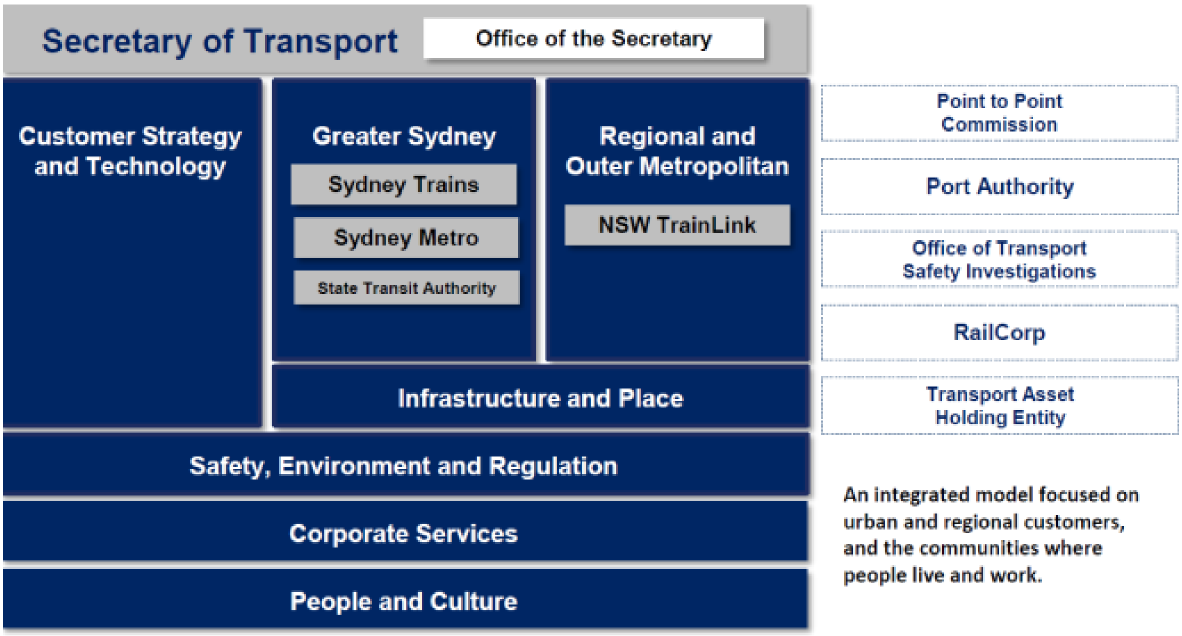
Part A discusses existing information and concepts relating to established knowledge on cyber security and reputational loss, especially for the transport context and in the state of New South Wales. Part B discusses new approaches to quantifying reputation loss for TfNSW itself from major cybersecurity matters and illustrates how to estimate such costs of reputation loss or deficiency in practice.

The Nature of TfNSW Operations.

For the purposes of this project, it was necessary to begin with establishing the scope of TfNSW operations. The project understood TfNSW to be the name of the administrative department of state of the government of New South Wales responsible for all transportation activity within the state's legal jurisdiction (including some aspects of air services and air delivery of health services). Political and legal accountability of TfNSW operates through the state parliament and the Minister for Transport and Roads and the Minister for Regional Transport and Roads. This administrative structure is outlined in Figure 1 below.

The scope and scale of TfNSW embrace a wide range of transport-related activities where issues of cyber-security arise, and its responsibility for automated and computer-linked transport, including drones and driverless vehicles, will create further potentially large-scale cyber vulnerabilities also affecting public safety, public convenience (systems running as scheduled), and stakeholder trust.

Figure 1: 2020 View of the Transport Cluster[1]


Secretary of Transport
Office of the Secretary
Customer Strategy and Technology
Greater Sydney
Sydney Trains
Sydney Metro
State Transit Authority
Regional and Outer Metropolitan
NSW TrainLink
Infrastructure and Place
Safety, Environment and Regulation
Corporate Services
People and Culture
Point to Point Commission
Port Authority
Office of Transport Safety Investigations
RailCorp
Transport Asset Holding Entity
An integrated model focused on urban and regional customers, and the communities where people live and work.

The *Transport Administration Act 1988 No 109*, current as of 1 July 2020[2] establishes TfNSW as a NSW Government agency whose affairs "are to be managed and controlled by the Transport Secretary". TfNSW is legally distinct from the Department of Transport ("functions of TfNSW do not limit the functions of the Transport Secretary as head of the Department of Transport": Clause 3E of the Act). TfNSW legal responsibilities include, but are not limited to the following named entities:

- State Transit Authority (STA)
- Sydney Ferries
- NSW Trains
- Sydney Trains
- Residual Transport Corporation (RTC)
- Sydney Metro.

In 2018-19, TfNSW funded 3966 positions inside its organisation, though more than 26,821 posts were filled across the Transport cluster, serving in 341 locations across the state (2018-19 TfNSW Annual Report). In the 2018–19, the Transport cluster delivered "its largest ever capital works program of more than $13 billion", with TfNSW directly delivering $3 billion of the total cluster capital program". Total Transport revenue for 2018-19 was $19.444 billion

Internal stakeholders in the TfNSW cyber security domain involve relations across different functional areas of the department and between employees and management. The external stakeholders involved in the digital assets of TfNSW involve customers at the core, but also other NSW government departments, state policing authorities, state regulatory agencies,

[1] https://www.transport.nsw.gov.au/system/files/media/documents/2020/transport-cluster-chart-july-2020.pdf.
[2] https://www.legislation.nsw.gov.au/view/html/inforce/current/act-1988-109.

national security agencies, local government authorities, partner corporations involved in large projects, industrial contractors, banks, investment partners, insurance agencies and legal firms.

Initial Conception of Reputation Loss from Cyber-Attack

In approaching reputation loss to such transport operations from cyber-attack, this Report adopted the following main hypothesis and three sub-hypotheses as a starting point:

> ***Main hypothesis*:**
>
> TfNSW's reputation will be significantly impacted by cyber-attack, and this can be usefully assessed for agency management purposes in an economically quantifiable way
>
> ***Sub-hypotheses:***
>
> - The reputation loss will be different for three distinct mission sets: public safety, public convenience, and stakeholder trust
> - The reputation loss will be, in part, shaped by the assumed motivations of the attacker (terrorist versus criminal versus foreign state; external attacker or insider threat)
> - The reputation loss will also be shaped by the perceived levels of preparedness in place in TfNSW at the time of the attack and by the quality of response by TfNSW to the attack.

Figure 2 below captures the initial view taken of the contours of the different types of event and subsequent reputation loss mentioned in the sub-hypotheses. It is purely hypothetical, constructed by the authors for illustration of the structure of the elements involved in reputation quantification.

The hypotheses indicated that cyber-attacks against TfNSW assets, activities and processes would have widely differing impacts according to the stakeholder interest involved, the type and intensity of the cyber-attack, and the mitigation measures put in place by TfNSW.

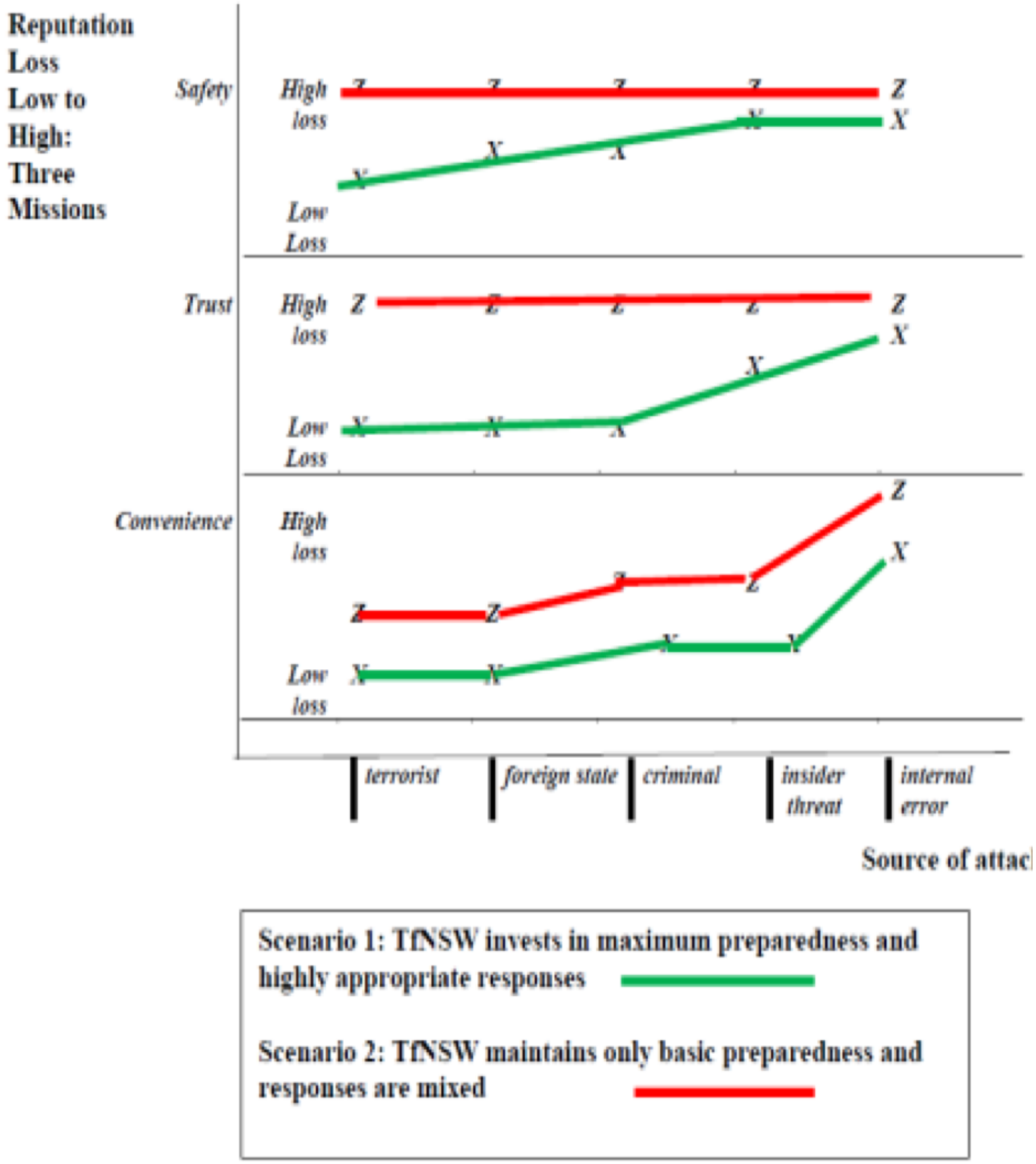
For reputation loss, we can accordingly identify conceptually distinct (though sometimes event overlapping) areas of cyber-attack that TfNSW is likely to experience:

- <u>Attacks on systems that produce customer safety threats</u>: threats to control systems in mass transit systems that may enable or result in physical threats to life and limb, for example in driverless trains
- <u>Non-fatal disruption Operations</u>: threats to control systems and general ICT systems that disrupt the normal operations of TfNSW agencies, either for customers, employees, or external stakeholders
- <u>Financial Crime</u>: threats to the confidentiality of customer data, employee data, or bank data, that lead to fraud
- <u>Privacy breaches</u>: Threats to the confidentiality of customer data that threaten personal interests of clients
- <u>Non-disclosure breaches</u>: theft of commercial-in-confidence data or intellectual property, possibly accompanied by its public release.

This report examines the issues around TfNSW's areas of responsibility and how its reputation would be affected by the possible cyber-attacks identified, and how this could be assessed in dollar terms.

Part A below assesses the relevant literature on reputation and on cyber-harm and reviews the relationship of these issues to the TfNSW portfolio responsibilities. Part B moves from documentation of past and present practice and approaches into exploration of new ways forward for advancing valuation of reputation loss for TfNSW

Figure 2: Provisional Graphic Representation of Reputation Loss under Two Scenarios



PART A. SETTING THE SCENE - PRESENT KNOWLEDGE AND PRACTICE

As indicated above, this Part A assesses the relevant literature on valuation of reputation loss, and reviews the relationship of these issues to the related TfNSW cyber risk portfolio responsibilities. It reports these each in turn. But within these two themes, key sub-themes are presented.

For the literature review, anticipation of cyberattack developments beyond 2020 are the focus, followed by review of the nature of valuation of the consequent reputational harms for these.

For the portfolio review, an overview of cyber security realities inside the department and the cluster is provided, followed by exploration of recent experience of reputation wins and losses, and then a depiction of the application within TfNSW of the cost benefit analysis process within which further consideration of reputation loss could be pursued.

Literature Review on Cyber Attacks and Reputational Harm

The literature review provides essential background on scholarly approaches to analysing the valuation of reputation loss for TfNSW. It is composed against the background of the hypotheses of the research project, as stated above, and here focuses on:

- Cyber-attacks beyond 2020
- Reputational harm from cyber attack
- Measuring and valuing reputational harm.

It is noted first that the relevant iconic literature for the valuation problem is wide. It derives from disciplines ranging from science, technology and engineering to law, economics and political science. Cyber security is a relatively recent problem, and reputational analysis is a relatively recent topic of study. Valuation studies associated with loss of reputation are quite well established for the private sector, through direct market measures. The research for the valuation of reputation loss is less well developed for the public sector, including for the provision of transport services, though they do provide a comparator metric.

This literature review therefore seeks to construct the nature and content of reputation for a body such as a government agency and to characterise and assess the work that has been done in finding methods for valuation of that.

Responding to Cyber Attack beyond 2020

The security environment of cyberspace is becoming more complex, not least through the accelerated development of Artificial Intelligence (AI), the Internet of Things (IoT), and autonomous machines. Cyber-physical systems have become the norm. These are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated through the internet. Just as the internet transformed how humans interact with one another, cyber-physical systems will transform how we interact with the physical world around us (Carruthers 2016). The increase in complexity translates to higher vulnerability to system breaches, or in other words, a greater risk exposure to cyber-attack (Zilberman 2019). This technological acceleration is unprecedented, making forecasts of the cyberspace security environment very difficult albeit fully necessary, including for business case decision-making such as that requiring cost-benefit analysis. We are marching towards the no-visibility era when it comes to the underlying programming of our automated systems. As complexity grows, it will become harder for key decision makers to analyse potential risks and for their technical specialists to prevent, let alone identify cyber-attacks. But investment decisions must still be made.

As large numbers of devices are connected with each other and essentially to the global network, there is a major risk of security threat, vulnerabilities, data manipulation, stealing, identity, device manipulation, and hacking. Due to the modern ease of automation and digitization, these devices bring an expanded security threat. All devices can provide an entry point for cyber-attacks which may compromise sensitive data, threaten users' privacy and even weaponise the device (Alharbi et al 2020).

Lehto (2020) predicts that for the transport sector, "physical safety—an established practice across transport sectors—and cyber security will become one and the same". He notes that "this critical infrastructure is managed and maintained by a complex set of actors, each of whom tackle cyber security differently". The cyber security threat, he says, is "increasingly becoming cyber-physical, as vehicles, aircrafts, vessels, infrastructure, and control systems become increasingly connected".

We see this already playing out in several areas - e.g in OT where the SFAIRP concept applies, rather than an acceptable level of risk. i.e a different level of proof is required to demonstrate risk is managed. And integrity and availability take priority over confidentiality when safety is under consideration.

Unfortunately, inadequate attention has been paid to transportation cyber risk and resilience (Zhou et al 2020). Efforts are often fragmented, addressing specific segments of the overall system and lacking a coherent framework that captures the overarching complexity of a multifaceted and complex integrated system. Transport policy makers globally are increasingly perplexed by the pace of change. The environment often produces advice that isn't based on clear evidence but, rather, may owe more to organisational developments. In describing this situation, Cohen and Jones (2020) identify four organisational dispositions to be aware of: "business as usual", technological optimism, technological fatalism, and technological ignorance.

Despite the availability of various advanced incident handling techniques and tools, there is still no easy, structured, standardised and trusted way to manage and forecast interrelated cybersecurity incidents (Papastergiou et al 2020). Physical and cyber security should be integrated and reference ideal practice, as laid out in ISO 27001, ISO 27005, IEC 62443, and the US National Institute of Standards and Technology (NIST) cybersecurity framework.

Nowadays, barriers to entry for would-be cyber criminals are falling rapidly because the attackers have a range of (technical) capabilities and substantial resources at their disposal, since malware and malware-as-a service have become more easily and cheaply available through various means and sources (such as Dark Web, Deep Web) (Papastergiou et al 2020).

Unfortunately, cyber-attacks have moved to physical incidents. The first death confirmed from a ransomware attack (in Germany) has created a very dangerous precedent and should be a turning point for government policy makers (Cimpanu 2020).

To prevent and respond better to the effects of minor to severe disruptions, the concept of cyber risk and resilience has emerged as an important policy and management issue . Risk management and resilience is the ability of a system to respond to, absorb, adapt to, and recover from a disaster. Resilience analyses of the transportation infrastructure have the benefit of improving physical operability, system safety, optimising management and investment, with positive socioeconomic impacts. Risk and resilience measures allow decision-makers to collect and utilise data to assess potential impacts of investment and policies for transportation infrastructure (Zhang et al 2015). The highest priority may need to be on intelligent vehicles and the digital infrastructure installed to operate them safely (Trend Micro 2017).

Resilience is a challenging concept for implementation in respect of cyber systems. Foundational work in this area has been carried out by the US Department of Homeland Security (DHS) and Carnegie Mellon University, which is a world leading centre for the study of cyber security. This work is summarised by DHS (2008) in a fact sheet, which identifies ten categories of policy response:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

As observed by Austin (2020c), each element of the resultant DHS Cyber Resilience Review (CRR) assessment facility is backed up by detailed research studies conducted by Carnegie Mellon University (for example CMU 2016). These ten categories, jointly developed by academia and government in the United States, provide the most comprehensive approach to cyber security management for all firms and agencies. The eighth item, external dependency management, is one of the hardest to implement—though all are more difficult than they appear. Thakur (2016) outlines the challenges in that area of external dependencies.

Austin and Withers (2019) have argued for a comprehensive approach to cyber risk management based on their concept of social cyber value, defined there as social and behavioural insights that enhance cybersecurity's value contribution. They argue that all security outcomes in cyberspace are determined by individual people, whose behaviour is shaped by their social setting, either organisational or cultural. There is a sharp imbalance between investments in technology for security in cyberspace as against social aspects at almost every level: national government and business enterprise (as in academia). The result is that the pace of digitization delivers an increased level of systemic risk that can exceed the pace of ability to manage that risk. This shortcoming is compounded by three others of equal or greater importance. First, the further socio-technical threat of unintended system failures, which may be dubbed "cyber incompetence", is also largely unstudied outside the technical realm. Yet it may be even more costly and far more common than the more prominent concern for addressing cyber-attacks. Second, decisions for digital transformation in all organisations can undermine or enhance security and are, in turn, impacted by the competence levels of the decision-makers. Third, the susceptibility of leaders, managers and users to be swayed by disinformation generated by the media or even vendors in fast-moving situations is an equally important threat to business and security.

Austin and Withers (2019) see these four problem-sets as inextricably linked, and argue that we can only analyse any one of them by reference to the idea of the "social cyber ecosystem" in which they all exist. It is their interaction in the shared ecosystem that determines all security and welfare outcomes dependent on cyberspace. The benefit of addressing social cyber system value in this proposed comprehensive fashion (insecurity, incompetence, digital transformation, disinformation threats) is that it creates the conditions for the appropriate reflection on important new ethical questions (especially privacy but also worker values).

Governments around the world have recognised the escalating threats and increasing demands for new types of responses, ranging across civil defence initiatives (Austin ed. 2020a) and education reform (Austin ed. 2020b). Australia may be a leading cyber power, arguably in the world's top ten or twenty, but it too is struggling to keep pace with threats.

Government agencies in NSW face the same situation: escalating threats and inadequate responses. In the most recent NSW Audit of cyber security, agencies were called to "improve cyber security resilience as a matter of urgency" (Hendry 2019). This is on top of the Cyber Security Inquiry announced in August 2020, which was to focus on current lacklustre responses to cyber incidents. Between the period of 1 July 2019 and 30 June 2020, there were 12,689 cybercrime reports in NSW alone (ACSC 2020). The Australian Centre for Cyber Security (ACSC) has observed sophisticated cybercriminals conducting significant victim research on networks they have compromised prior to deploying ransomware (ACSC 2020). These are major challenges that each agency needs to face. An attacker only needs to find one vulnerability, security teams must protect all aspects of the infrastructure.

Reputational Harm from Cyber Attack

The nature of reputation for public organisations can draw on basic propositions well codified early in Van der Hart (1990) and, most recently, their synthesis in Luoma-aho and Canel (2016). Box 1 carries their key findings which demonstrate the complexity of reputation in the public sector.

Box 1: Findings on Public Sector Reputation

- Reputation of public services is a different construct from the reputation of public sector organizations
- Reputation of political and public leaders that lead governments and public administrations is a different construct from public sector or services themselves
- The public services aim ranges from social benefits to individual benefits, and measuring reputation changes accordingly from experts/professional judgment to citizen judgment
- Neutral levels of trust and reputation have been suggested as ideal for public sector organizations' reputation as to best meet existing resources
- Since public sector reputation operates in a political environment, different constraints affecting structures, resources, personnel and goals need to be taken into account for reputation management
- Managing reputation of public sector organizations is an emerging research area with practical implications that deserves deeper explorations of related intangible assets such as legitimacy, engagement, institutional culture, institutional social responsibility, social capital, transparency, relationship building and trust.

Source: Luoma-aho and Canel (2016)

Some reputation literature has focussed especially upon privacy, as is appropriate and important. The early work here was by eminent legal, social and economic scholars such as Noam (1997) and Varian (1997),and is foundational for logical construction and early quantification on privacy. But privacy in this project is one highly significant part of a broader notion of reputation that comes from a range of disciplinary analysis beyond economics and law and also incorporates political science and management approaches. Accordingly, it is sensible to examine the overall dimensions of reputation as follows:

> **Defining Reputation:** For the purposes of this project, we have limited our discussion of TfNSW "reputation" to the organisation and its ministers (their delivery of services, their execution of other legislated obligations, and their probity in doing so). We are not addressing the reputation of the specific services delivered. Where we refer to TfNSW reputation in this report and in this project, we mean reputation, including reputational losses, accruing to the New South Wales government broadly in and around the transportation portfolio.

We would like to put on the table for discussion the proposition raised by the scholars that public sector organisations should aim for a neutral reputation – concentrating exclusively on avoidance of reputational harm and avoiding classic public relations activity intended to promote a positive organisational image independently of normal informational activities.

An alternative view for consideration though is that, at the same time, having a positive reputation for cybersecurity may have benefits including but not limited to: a) increased citizen uptake of digital services b) attraction of scarce cyber talent c) a reduced premium imposed by third parties dealing with TfNSW. A blended view is that this can be accomplished through normal informational activities.

A 2017 survey of Australian companies found that while "three out of four have formally identified risks that could have an adverse impact on their company's reputation", "only a minority of organisations has quantified risks related to reputation" (Lewis 2017: 659-60). The study also found that "less than one third has tested policies' resilience against risk scenarios". On the cyber front, the study found that "CEOs appeared highly concerned with social media, [but] neither they, nor other respondents were as concerned with disruptive innovation (that is, artificial intelligence, Internet of Things, augmented reality)". The survey (660) asked the question: how sensitive is your organisation to reputational risk?

Some of the survey results are in the following four graphics (Figures 3-6) from the 2017 report.

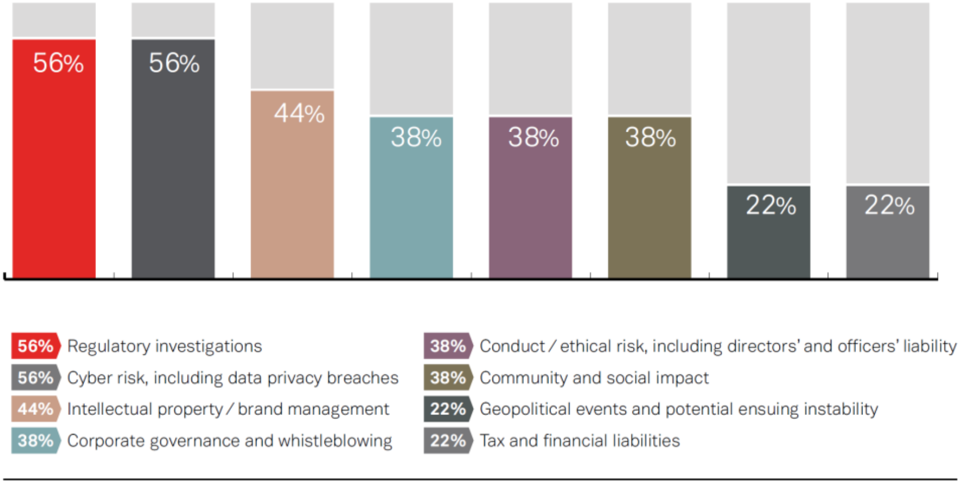
The most extensive and comprehensive approach to reputational harm for cyber-attack itself has been advocated by Agrafiotis et al (2016),working in collaboration with the cyber harm project (formally called Analysing Cyber Value at Risk) at Oxford University.[3] The emphasis there is that reputation loss is best understood as harm "pertaining to the general opinion held about an entity" and not any assessment of the actual damage to broader social and societal

[3] https://www.cs.ox.ac.uk/projects/ACVAR/index.html.

interests. Agrafiotis et al point to the need to understand three dimensions: the progress of reputation loss over time; variations in harm depending on type of asset attacked; and the ability to shape the persistence of reputational damage according to the quality of response and remediation measures.

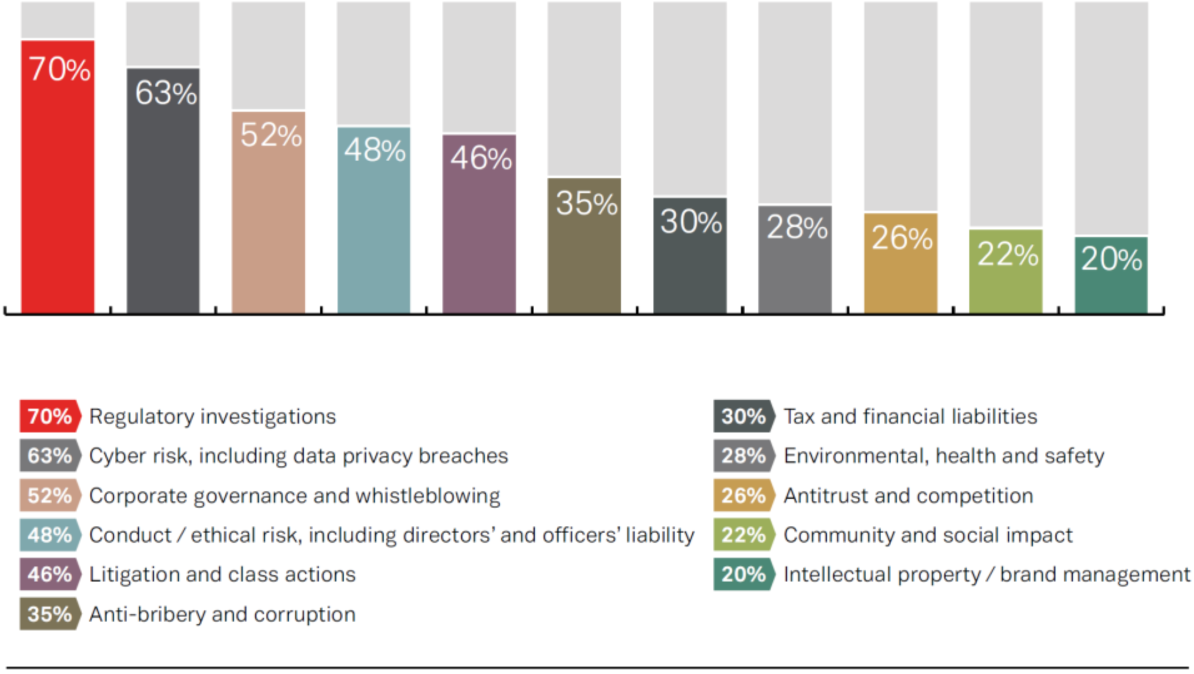
Figure 3: Which risks are most likely to have an impact on a company's reputation?

(56% , 56%, 44% as identified by board members and C-level executives)



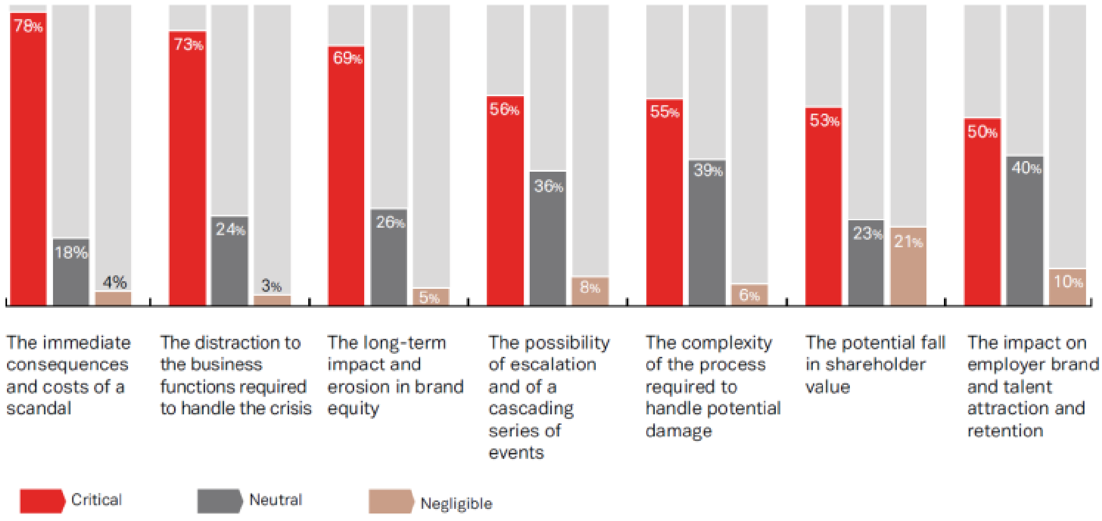
Source: Lewis, 2017

Figure 4: Which risks are most likely to have an impact on a company's reputation? As identified by general counsel and risk professionals



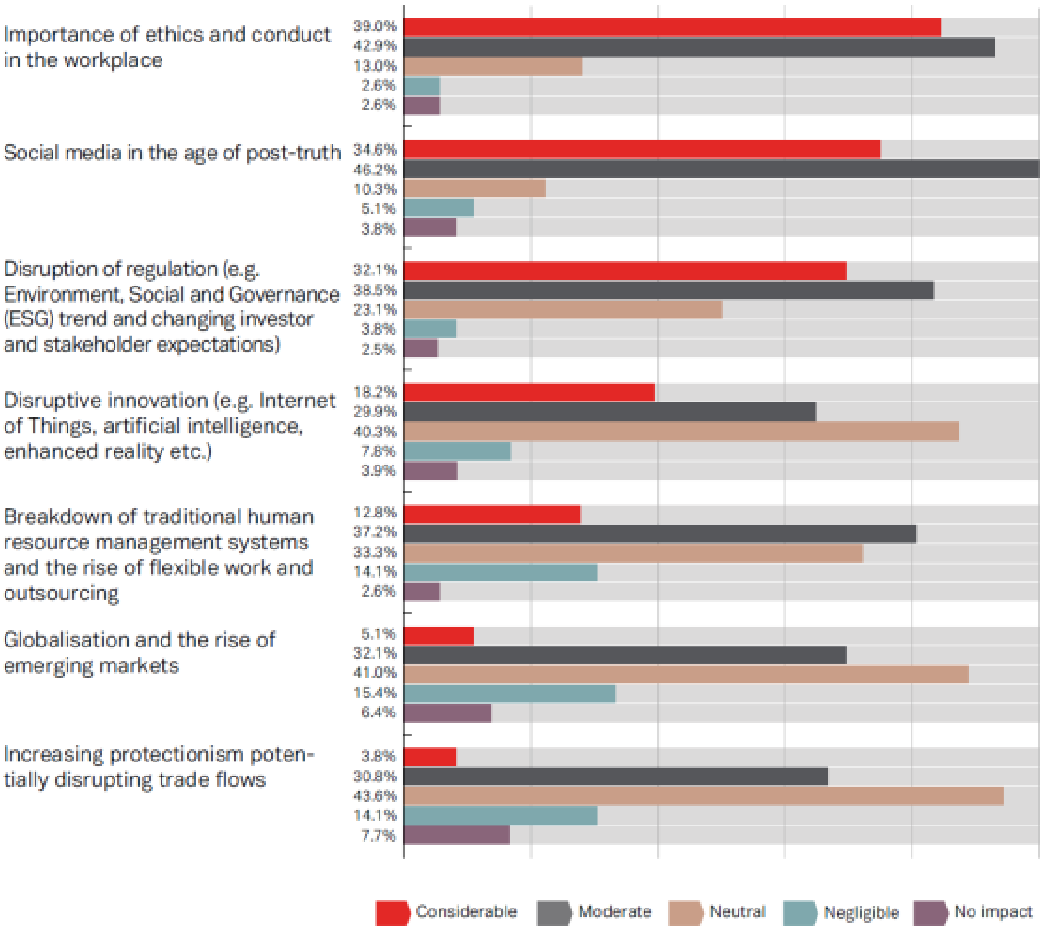
Source: Lewis, 2017

Figure 5: What are the most severe consequences of reputational damage?



Source Figures 4 and 5: Lewis, 2017

Figure 6: Which global trends do you expect will have the longest impact upon your reputational risk profile in the future?



Source: Lewis, 2017

Agrafiotis et al provide a useful list of possible reputational harms, as set out in Table 1. And Agrafiotis et al (2016: 39) identify a method for analysing reputational harm: “identify positive and negative opinions expressed in media (both mainstream and social media) through sentiment analysis, using computer algorithms”. This can provide for both quantitative and qualitative data, especially relevant to understanding the severity of reputational harm and any associated services impact.

Table 1: List of Reputational Harms

- Damaged public perceptions
- Inability to recruit required staff
- Reduced corporate will
- Media Scrutiny
- Damaged relations with customers
- Loss of key staff
- Damaged relations with suppliers
- Loss or suspension of certifications
- Reduced business opportunities
- Reduced credit rating

Source: Agrafiotis et al (2016)

The observation by Agrafiotis et al about reputation loss from cyber-attack varying over time is very important and has been supported by other scholars. For example, Brasington and Park (2016) supported that view, noting in particular that loss of intellectual property may be one of the follow-on consequences, “either through theft, loss of exclusivity or loss of commercial confidentiality”. Gao et al (2020: 3) cite the proposition that the direct cost of remediating a cyber security breach can be as low as ten per cent of the total hidden costs. Wang et al (2018: 163) concluded that indirect and hidden costs are usually “not easy to recognize and [are] difficult to measure” even though they may be critical for business survival and competitiveness. The hidden costs of what they call mega data breaches might include lost business, negative impact on business reputation, employee time spent on recovery.

Some international research focusing on these subjects identifies public safety as the most important determinant of reputational gain or loss by a public transportation agency. In this area of concern, the highest priority may need to be on intelligent vehicles and the digital infrastructure installed to operate them safely (Trend Micro 2017). User identity (personal records), important to protect in their own right, will also be a component of the operating system of intelligent vehicles.

Other useful sources include Greenfield & Paoli (2013) who analyse five magnitude levels of reputation harm and remind us of the cascading nature of cyber harm. ISACA (2018) proposes threshold criteria for defining six levels of reputation harm from minor to business-critical. The World Economic Forum (2015: 43) defines cyber-Value-at-Risk (VaR) as a ‘risk measure for a given portfolio and time horizon as a threshold loss value’. It suggests a threshold can be defined in the following dollar terms: ‘a company will lose not more than X amount of money over a period of time, with 95% accuracy'; quantifying the assets under threat, computing the vulnerabilities, creating threat profiles of attackers; harms include future revenue loss, litigation and public relations.

We have also identified a number of additional research findings that can inform our thinking. Wang et al (2019:164) focus on all of the damages (including financial costs) that flow from loss of "trust and credibility with the customers and general public" as the result of data breach. Gwebu et al (2018) link the reputational cost of data breaches to corporate reputation, which they see as an important asset related to corporate financial health (2018). Data breaches can cause an organisation to lose "consumer trust and public confidence" that "may translate into financial or monetary loss" (Krishan 2018).

There has been less scholarly work on public perceptions of cyberattack and the consequences of it, especially for reputation. A ground-breaking study by Kostyuk and Wayne (2019: 26) in the United States found lower levels of concern with the effects of attacks on government agencies compared with data breaches that "personally affected the individual". The respondents did not appear to care as much about the technicalities of how an attack was perpetrated as about the personal implications. Of some note, the authors concluded that their survey (34) demonstrates the "limitations of any potential messaging campaign" about cyber-attacks.

The role of marketing managers in responding to cyber-attacks is a complex one. It is replete with legal implications where public statements of fact may carry legal consequences for the victim organisation. In terms of scholarly research, Whittaker and Farris (2017: 5) found that cyber security "has been an impenetrable domain for marketers, despite the brand, reputational, and consumer damage that data breaches can cause". One reasons for this situation, they observed, was that in addressing preparedness companies focus on "lawyers as the taskmasters".

Some research points to the problem of fungibility or diffusion of organisational responsibility for failure to prevent a cyber-attack. But Skinner (2019: 267) suggests that the mere perception among the public that an organisation has fallen victim to a cyber-attack "may damage [its] reputation with customers and third parties with whom we do business". Vitunskaiet et al (2019: 314) reported a similar finding. Even if the attack or data breach originates from a third party, the "primary organisation" [parent organisation] is responsible and pays the price". Whilst the liability can often be managed contractually, the responsibility and reputational damage will fall on the parent organisation."

One of the most revealing cyberbreaches in respect of the impacts of reputational harm was the attack on Target in 2013 in which "hackers stole credit and debit card information for 40 million Target customers and names, as well as home and email addresses, for another 70 million" (Srinivasan et al, 2019). An independent report recommended that the entire Audit Committee be sacked. The case study report notes that "While Target's board vigorously defended its performance, observers were left wondering about the extent of board accountability for a breach of such large magnitude".

In a filed patent application, Evans (2020) provides a useful taxonomy for measuring value for possible risk. He has three asset classes that are relevant to TfNSW: crown jewels, business critical and business crucial, which are descending degrees of importance. He has a further set of data classes: privacy, personal identification information (PII), credit card information, health care information, financial information, and intellectual property. (For this project, we can easily substitute “safety related data” for “health care”.)

Evans also identified for more complex purposes a suite of considerations for system security that will affect the impact of a cyber breach (not a reputational risk study but still relevant). His patent is for an algorithm for estimating several types of operational cyber risk, including reputational risk, which is useful for differentiating the elements of a cyber breach (Table 2).

Table 2: Impact of a Cyber Breach: System Security Considerations

- Level of **security innovation**: security baked in, bolted on, or end of life
- Level of **system location** where the system lives - on a secure isolated segment, on a cloud service, on vendor network
- Level of **attack cadence** at system level - never attacked, attacked frequently, attacked occasionally, breached
- Level of **asset dependency** at system level: crown jewel, business critical, business crucial
- Level of **regulations** the system must comply with – 1,2,3,4.
- Level of **system recovery** times: 0-4 hours, 4-12 hours, 12-24 hours, over 24 hours
- Level of **restoration costs** at system level – cost to restore the system
- Number of **records at system level** – number of records the system processes
- Level of **reputational impact** – rumour, regional press, international press, for customer facing systems

Source: Evans 2020.

Valuation of Reputational Harm

Having analysed the nature and meaning of reputation, the next task for this project has been that of its valuation. There is to date a limited literature on cyber security and valuation of reputational harm in public sector organisations. For purposes of such valuation of reputational harm, cyber security is a relatively recent problem. Moreover, reputation has not been well-defined operationally and quantitative valuation of non-market concerns is a recent advance in scientific methodology. It is timely to seek to bring these factors together, however, given the salience of the issue. The evolution of relevant ideas renders these problems eminently tractable.

On reputation, as discussed above, the nature of this for public organisations can draw on basic propositions well codified in Van der Hart (1990), Laing (2003), James (2009, 2011), Canel and Sanders (2012) and their synthesis in Luoma-aho (2016). And privacy in particular, in this context, can be well grounded in work such as Noam (1997) and Varian (1997). The result is works surveyed in overviews such as Acquisti, John and Lowenstein (2013), and Moranda, Iemma and Raiteri (2014), though the focus is essentially on private business valuation through so-called “event analysis” where a cyber-attack is known to have occurred.

Particular cases can illustrate the problems well too, as is seen in insights provided into organisational causes and explanations in narrative form through business and government school case studies dealing with cyber metrics and their management e.g. Harvard Business cases such as Herbolzheimer, Sekeris and Chacko 2016, Hogg 2017, McKinty 2017.

But, beyond cases and beyond private sector analyses, the literature is mostly taxonomic. This is important for frameworks and conceptual clarity, to which can now be added innovative quantitative approaches for public agency cyber security valuation issues to be proposed in this report.

The valuation dimension opportunity particularly benefits from the emergence of behavioural and big data and business and public policy scholarship, particularly as a number of strategic bias problems (identified early in Throsby and Withers, 1986) became evident and fostered new methodologies that have now been applied extensively.

This literature addresses aspects of activities not revealed easily in the marketplace through the prices and transactions there. A particular relevant methodology or technique that has emerged is that of stated preference survey models and especially through 'contingent valuation' therein. This approach can distinctively provide household valuations of non-market impacts, especially so that these can be incorporated into cost-benefit analysis (CBA) in a manner commensurate with market-based measures. Such CBA, augmented by non-market valuation, has become termed social cost-benefit analysis (SCBA). This is therefore an approach to the TfNSW project focus.

For purely private firms, reputational impact of a cyber-attack could be quantified for market listed firms by examining the effects on their stock market prices. The distinctive feature of additional measures needed for public organisations' program and project choices is to capture benefits (or costs) not available from the actions of the stock exchange participants who reflect and express market sentiment in dollars. This can include reputational and other damage or indeed gain, where cyber security actions occur.

In the absence of a market integration mechanism such as stock price, alternative measures are needed if quantification is desired. This means that surrogate measures need to be found for such matters - as in the present case of public reputation. Various methods are possible here. Some might be partial indicators such as measurable traffic effects (including revenue measures) for effects of cyber actions. Actions too of partner businesses might provide indicators e.g. if a cyber security improvement reduced risk of partner private information being externally accessed, they may offer lower contract prices.

But these are partial indicators only. There are dimensions of reputation beyond those affecting immediate stakeholders that are pertinent to public agencies in ways not necessarily applicable to firms. This is why our discussion above included stakeholders such as politicians and the wider public. These two groups are bound together here by the fact that the circumstances of public entities also have implications for voters' attitudes to government.

One generic approach to valuation is so-called "revealed preference" estimations of the dollar valuation of some public good style projects. This draws on observed market prices or expenditures. A common example is to use travel costs related to a public facility as a measure of at least the minimum willingness to pay for that entity or facility. However, these methods are too limited to apply usefully to valuing cyber security issues as no clear surrogate measured activities present themselves.

The main alternative is therefore, as indicated, “stated preference” survey methods with “contingent valuation” where relevant parties are asked for their willingness to pay for the good or service or facility. A variant is “willingness to accept” (rather than pay) where a payment to the respondent is considered appropriate for a negative action.

Contingent valuation is a leading form of stated preference methods. Other forms of stated preference that focus on product characteristics rather than more holistic payment are found in “choice modelling” and there are also less dollar focussed satisfaction surveys. For cost-benefit analysis purposes, though, the common approach is stated preference with contingent valuation (Carson 2011).

Although this approach may involve hypothetical questions, it has the advantage of considering projects before implementation, and of embracing as much of the wider community as desired e.g. all voters, even when they are not TfNSW transport users. The contingent valuation survey method can also put a value on so-called “option demand” for a public good. This is the value of a service to infrequent or non-users who desire provision despite that their expected non-use of the service. e.g. Utsunomiya 2018.

The stated preference method is not costly since focus group and survey methods can be used. The difficulty is to make such exercises meaningful and accurate when the circumstance are hypothetical.

With modern computing, survey respondents can also be asked questions regarding the strength of their views on matters, such that a dollar valuation can be deduced. The requirement for validity is to conduct such analysis fully aware of potential biases so that confounding aspects can be allowed for and tested and clarified e.g. definition of reputation, understanding of its relevant dimensions, motivation for answers, form of stating questions etc. Li Liu and Motawalla (2020) provide a recent overview of how this is manageable in such studies.

The stated preference approach is well-established, especially in environmental analysis where matters of valuation ranging from bio-diversity and species preservation through pollution effects of factory emissions to coastal damage from oil spills, have been examined through this lens to inform public decisions. This approach was especially validated, and basic protocols defined, in the report of an eminent panel including two Nobel Laureate economists that followed the Exxon Valdez oil spill off Alaska (Arrow et al 1993). Carson (2012) provides a good summary of the evolution of the field, and Johnston et al (2017) updated the guidelines provided for stated preference analysis to take account of the twenty years of research that followed the Exxon Valdez investigation. A recent volume from MIT Press drawing on European as well as North American practice looks at the extension now in place to research infrastructure using the latest methods and findings (Florio 2019). The Productivity Commission (Baker and Ruting 2014) provides thorough guidance to such non-market valuation for environmental policy.

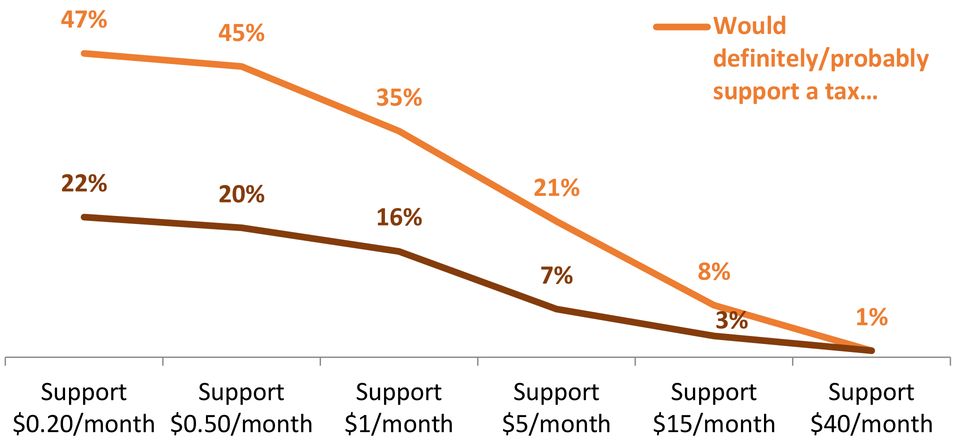
The stated preference method is also common now in areas such as cultural matters. Indeed, Australian studies have been amongst the most influential in this culture field, and the findings there for areas such as arts or public broadcasting, have established ‘community value estimates for use in social rate of return or social cost benefit analysis e.g. Throsby and Withers, 1997.

As an example of findings for dollar valuation of non-market aspects of public activity, a recent study of willingness to pay by Withers (2020) found, as indicated in Figure 7, for the case of public support for enhancing public interest journalism (willingness to pay extra taxes for sustaining and expanding the number of such journalists). The Centre for International Economics (2019) then took these findings to calculate the benefit-cost ratios for a tax incentive scheme for supporting a such journalism.

There are also like evaluations across all areas of public activity at a broad level. One of the most recent for Australia is Centre for Policy Development (2017), and also a more detailed analysis for the Australian Council of Learned Academies (ACOLA, 2016). The latter study, for instance, summarised the willingness to pay for different aspects of government for Australia overall as follows in Figure 8 below.

Transport and communications received 51% support in this ACOLA work for higher funding, this being in the context of a wider willingness to see an expansion of government in Australia if that was devoted to areas supported by the public.

Figure 7: Public Support for Enhancing Public Interest Journalism (willingness to pay extra taxes for sustaining and expanding the number of such journalists)



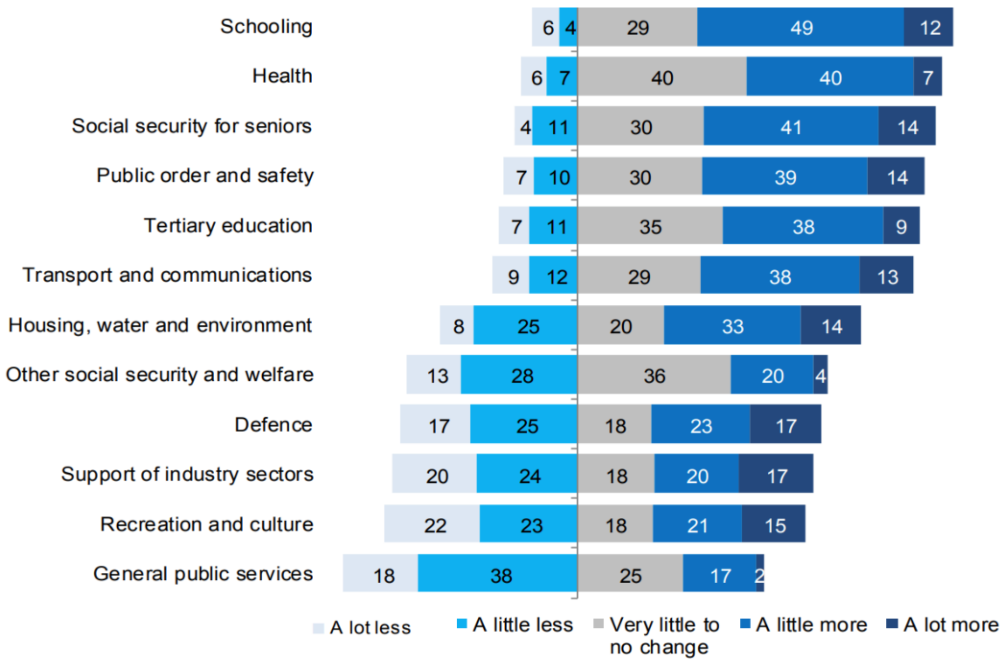
Source: Withers, 2020.

More specifically, stated preference valuation methods are also long-established for transport studies. Revealed preferences, such as through travel cost studies paved the way and there have been numerous stated preference studies too for aspects of transport. But Daniels and Hensher (2000) conclude that, while there has been much progress, there remain key areas where identification of monetary values has not been established and which remain to be researched. This clearly includes the focus of this TfNSW project, the issues of cyber security and reputation value in public transport. No extant studies have been identified that provide such information at this time.

For more well-established aspects of non-market valuation, guidance to methods of valuation are offered in Australia in such sources as various Handbooks or Manuals from key public authorities, both at the general level such as NSW Treasury 2017, and at the portfolio level such as for TfNSW itself (Transport for NSW 2019). There are also Australian textbooks which offer guidance such as Abelson (2019), Boardman et al (2018) and Dobes (2016).

Within the context of this well-established literature on the social cost-benefit application, this project has sought to look further at one, as yet, still open area for application of the methods that have evolved and been accepted in the standard official guides to such analysis viz. valuation for cyber security effects on reputation. The task therefore would be to use a willingness-to-pay survey to demonstrate how this methodology can be applied to the transport reputation issue for public agencies and, specifically, how this would be impacted by the emerging nature of issues in cyber-security.

Figure 8: Willingness to Pay for Government



Source: Centre for Policy Development (2017)

The literature review therefore does suggest that there is more that can constructively be done to obtain dollar valuation for reputation impact of cyber-attack for the purposes of public sector decision-making. It also points out the care that must be present in taking this forward in relation to appropriate specification of the contextual information and whose valuation is being sought.

Portfolio Review of Cyber Risk Management and Project Evaluation

Given this general literature and its guidance on the potential for future valuation for assessing investment to impact on transport cyber-attack, the next task was to undertake a portfolio review on TfNSW and TfNSW cluster agencies to establish:

(a) an overview of cyber security realities inside the department and the cluster
(b) recent experience of reputation wins and losses
(c) an understanding of the application within TfNSW of cost benefit analysis.

The purpose of this analysis is to ensure adequate familiarity with the broad operating environment in which a project on valuing reputation loss will be received. Such a review is essential for another reason. It ensures common understanding of key operating influences. A third purpose in a portfolio review is that is helps expose the sorts of issues that are most likely to be prominent in the minds of stakeholders when judging the reputation of TfNSW, an important complementary source of information for decision-makers in Transport.

The portfolio review feeds into a definition of Research Issues, along with insight from selected findings from the literature review. This definition of Research Issues is seen as a step that provides guidance for ongoing new work in consultation with stakeholders as well as the wider public and is discussed accordingly in Part B below.

The Introduction of this report above provided an overview of the scope of TfNSW as an organisation. Here we focus more on the state of play of cyber security in TfNSW.

The commitment by TfNSW to upgraded cyber security is demonstrated in many initiatives. Its own assessments suggest that the current capability can be described as modest or medium level, but with considerable potential for improvement from foreshadowed investments.

TfNSW is an attractive target to a range of cyber threat actors. It may also be the victim of attacks not targeting TfNSW directly. Cyber incidents or attacks can have unintended consequences and spread throughout systems which were not the intended target. This was the case of the NotPetya and WannaCry ransomware attacks that were intended for specific targets but spread globally, causing billions of dollars of loss and affecting health services in at least the UK.

The risks associated include safety, financial, reputational and disruption to services and customers. This portfolio review looks at the key reporting requirements for TfNSW and how they rate against the current frameworks and policies implemented by the NSW Government with regard to cyber security. The true impact to TfNSW is that it is both a public sector agency with its own internal responsibilities and also a critical infrastructure provider. This creates further complexity to the portfolio in achieving its regulatory requirements as there are both NSW (Cyber Policy) and Federal Government (Critical Infrastructure legislation) contexts to be considered.

Planning and Governance

TfNSW is currently in the process of implementing a cyber security uplift program being implemented through the NSW government. Each department provides an annual statement to meet the requirements of the NSW government cyber policy. These requirements were introduced in 2019. These statements are provided as a "best of our knowledge" statement. The focus of these statements is to ensure appropriate cyber "buy-in" from each portfolio chief executive.

The five strategic goals of the TfNSW cyber strategy focus on:

- Manage our Risk – Risk reduction through maturity
- Be Response Ready – Battle trained for success
- Manage Cluster Guardrails – Operate in cyber safe environment
- Maintain Strong Foundations – Investment for the future to develop the required building blocks
- Lead the Sector – Lead by example and share lessons learnt

These are many foundational blocks to implementing this framework and many possible frameworks for reporting on successes and failures. The NSW Cyber Security Policy (CSP) is the main framework. One prominent sub-measure used widely is ensuring adherence to the ASD Essential 8. Others include elements of relevant international standards, such as ISO 2701.

Safeguarding Information and Systems

Since 2017, TfNSW has identified key assets within the portfolio. Interestingly, of the 24 business critical systems identified, 17 of them are industrial control systems (ICS) or operational technology systems. Many fundamental cyber security controls for ICS have been enhanced, including controls to identify and prevent data loss, implementing controls to identify cyber security incidents, alerts to inform analysts of cyber security incidents and implementation of email and network control. Table 3 summarises the relevant actors here.

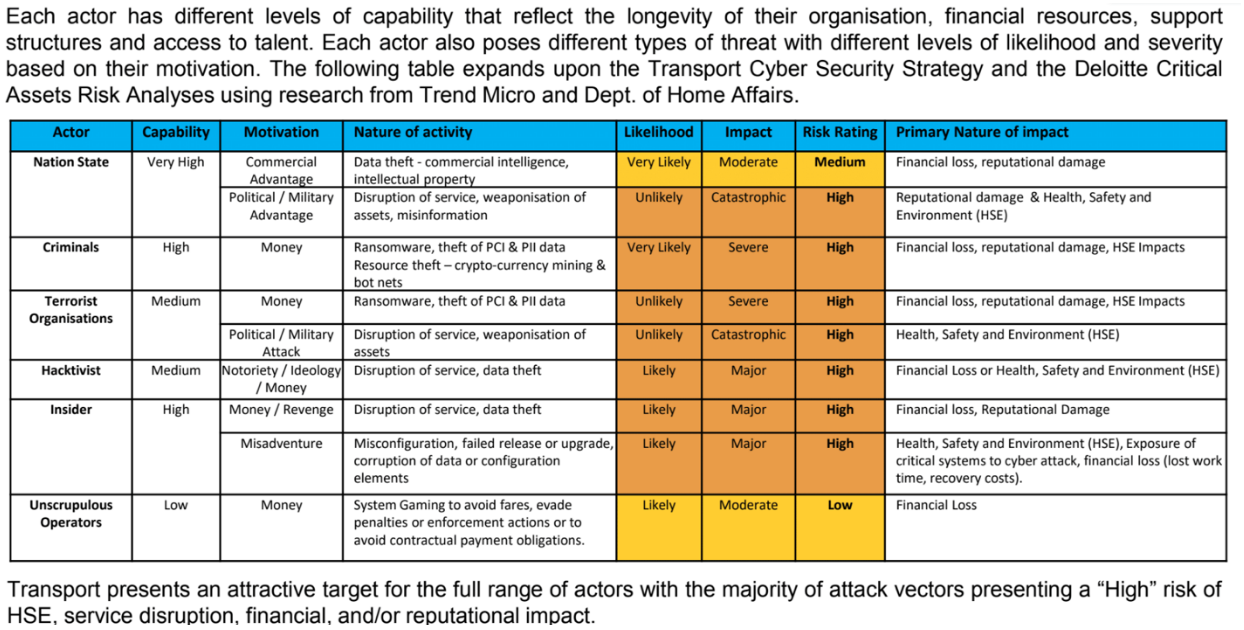
In early 2019 each TfNSW agency undertook a cyber review against both the NSW CSP and the ASD Essential 8 Maturity Model. NSW policy requires TfNSW to report on maturity against the Essential 8 controls for critical assets. The Essential 8 maturity ranges from 0 to 4. Overall, the Essential 8 maturity across all 24 assets is 0.8. Most agencies and divisions have a significant dependency on Group IT and therefore the maturity of the Essential 8 controls under Group IT significantly affects the overall cluster maturity.

TfNSW is also required to report maturity against a series of other controls. This maturity is measured from 1 to 5. Policy states that each control needs to be on level 3 to be compliant.

Risk Maturity

One of the factors that may undermine progress on valuation is multiple understandings of risk and where this risk fits into relevant TfNSW and NSW/Federal government frameworks. It is critical to understand and differentiate between business risk, technical risk and cyber security risks. These are each different but will probably interlink due to the digital environment. These risks must each account into portfolio and over TfNSW risks.

Table 3. Maturity of TfNSW in Threat Analysis



Each actor has different levels of capability that reflect the longevity of their organisation, financial resources, support structures and access to talent. Each actor also poses different types of threat with different levels of likelihood and severity based on their motivation. The following table expands upon the Transport Cyber Security Strategy and the Deloitte Critical Assets Risk Analyses using research from Trend Micro and Dept. of Home Affairs.

Actor	Capability	Motivation	Nature of activity	Likelihood	Impact	Risk Rating	Primary Nature of impact
Nation State	Very High	Commercial Advantage	Data theft - commercial intelligence, intellectual property	Very Likely	Moderate	**Medium**	Financial loss, reputational damage
		Political / Military Advantage	Disruption of service, weaponisation of assets, misinformation	Unlikely	Catastrophic	**High**	Reputational damage & Health, Safety and Environment (HSE)
Criminals	High	Money	Ransomware, theft of PCI & PII data Resource theft – crypto-currency mining & bot nets	Very Likely	Severe	**High**	Financial loss, reputational damage, HSE Impacts
Terrorist Organisations	Medium	Money	Ransomware, theft of PCI & PII data	Unlikely	Severe	**High**	Financial loss, reputational damage, HSE Impacts
		Political / Military Attack	Disruption of service, weaponisation of assets	Unlikely	Catastrophic	**High**	Health, Safety and Environment (HSE)
Hacktivist	Medium	Notoriety / Ideology / Money	Disruption of service, data theft	Likely	Major	**High**	Financial Loss or Health, Safety and Environment (HSE)
Insider	High	Money / Revenge	Disruption of service, data theft	Likely	Major	**High**	Financial loss, Reputational Damage
		Misadventure	Misconfiguration, failed release or upgrade, corruption of data or configuration elements	Likely	Major	**High**	Health, Safety and Environment (HSE), Exposure of critical systems to cyber attack, financial loss (lost work time, recovery costs).
Unscrupulous Operators	Low	Money	System Gaming to avoid fares, evade penalties or enforcement actions or to avoid contractual payment obligations.	Likely	Moderate	**Low**	Financial Loss

Transport presents an attractive target for the full range of actors with the majority of attack vectors presenting a "High" risk of HSE, service disruption, financial, and/or reputational impact.

Source: TfNSW, 2020 (unpublished document)

TfNSW, as a major government agency, and like most other major organisations, has embarked upon a substantial program of work to uplift its cyber capabilities in line with policy and the desired maturity levels.

TfNSW Cyber Culture

TfNSW cyber security policies and practices may well be ahead of those in most other government agencies in Australia. However, the detail of any such assessment may be lost in the public clamour around a major cyber security breach. As with most government agencies around the world, there are enough recorded vulnerabilities and shortcomings in the system to provide fertile ground for any critics determined to attack the reputation of past cyber practices in TfNSW if a major cyber security breach were to occur, especially if it led to loss of life or cascading safety consequences in the community. The critics would say that the breach is the evidence of failure (even if cyber security professionals know that is not always the case). Cyber crisis management in TfNSW and the NSW government as whole would have to be unusually (perhaps miraculously) well practised to achieve early mitigation of the effects of such a cyber emergency without it's having a large negative impact on the reputation of both TfNSW and the NSW government, perhaps equally.

Case studies have shown that for government agencies to meet the requirements of just the "essential eight" may take up to four years, if not longer, from the date they commence. Implementation of such requirements involves 3rd parties and other providers in the ecosystem which may not be currently included or considered within the current strategy.

The "essential eight" strategy was devised by the Australian Signals Directorate (ASD) to help Australian institutions move to a more mature cyber security policy. It is an evolution of the "top four" strategy launched in 2011.[4] The choice of "top four" was made from a list of 35 mitigation strategies advocated by ASD as simple measures which, if implemented, could reduce cyber risks substantially. This program has been emulated in the UK and Canada. In 2017, the program was extended to eight, and renamed the ASD "Essential Eight", and the list of 35 strategies was supplemented to reach 38. Most government departments in Australia, including the Home Affairs Department (responsible for national cyber security) have found it difficult to implement even the top eight mitigation strategies. And after that, there were still more from the list of mitigation strategies left that many government agencies do not implement.

Current cyber security culture within TfNSW appears to be different in different agency areas. Cyber Security is as much a people issue as it is a process or technology issue. The human side of cyber security is critical in meeting the objectives of any uplift program.

Targeted benchmarking, then training of staff at different skill and operational requirements will create a starting point for a holistic development of a TfNSW wide structured approach to developing a cyber security culture policy. Identification of potential staff within TfNSW should also be part of securing the human firewall.

In New South Wales, reputation loss may even be more measurable for the government as a whole, than for one department. This is because of some public failure to distinguish components of government, wide impacts of damage incurred and because, as will be explained, certain estimation biases in examining events separately.

The biggest reputation loss for the NSW government itself involving transport was the Granville rail disaster in 1977 (83 deaths and 210 injured). More recent complaints have related to a range of issues, but few appear to have provoked substantial reputation loss. One was the closing of a speedway at Granville to allow for the construction of a feature to do with WestConnex, the point being that the succession of complaints about TfNSW do not seem to have dented its reputation as seriously as a safety disaster might.

Further analysis of portfolio responsibilities for valuation matters regarding cyber security must also be directed at two major considerations arising from the cyber security dimension: recent experience of reputational gains or damage and how such cyber-attacks stand relative to the department's ambitions to monitor and defeat such events, and the baseline set for this.

[4] For a discussion, see Stilgherrian, "Australia's cyber defence 'pretty ordinary' before ASD's Top Four", 2 June 2015, https://www.zdnet.com/article/australias-cyber-defence-pretty-ordinary-before-asds-top-four/.

These cyber and reputation linkage issues have been discussed above. The other element of the research that remains is the incorporation of such cyber and reputation matters within the Department's approach to the cost-benefit evaluation work that is so important for transport activity operating within the public domain.

Cost-Benefit Analysis

Cost-benefit analysis is widely expected and required for public sector activity for it to be well managed in the public interest. Large project and system investments, as are common for transport provision, are especially seen to require close examination of the magnitude and flow over time of costs and benefits from these. Due attention is to be paid to the special characteristics of such projects so that benefits and costs pertinent to government in the public interest, and beyond the commercial market calculus, can be reflected. Also, suitable reflection of the public sector discount rate for the time distribution of these can be allowed for in such an approach.

Impact on reputation from cyber security activity would be a useful matter for incorporation into such social cost-benefit analysis (SCBA). This project's Literature Review indicated that SCBA practice as yet does not readily allow for reputation impact of cyber security matters. This report therefore seeks to help consider how to fill that gap.

The Portfolio Review process did make clear that TfNSW does make provision for present state-of-the-art SCBA. The portfolio provides a *Transport for NSW Cost-Benefit Analysis Guide*, which is issued by the Evaluation and Insurance area in Group Finance and Investment within the Corporate Services area. It is a comprehensive and up to date (2019 Version 2.0) manual that applies to all agencies within the NSW Transport cluster.

It is helpful that the Guide

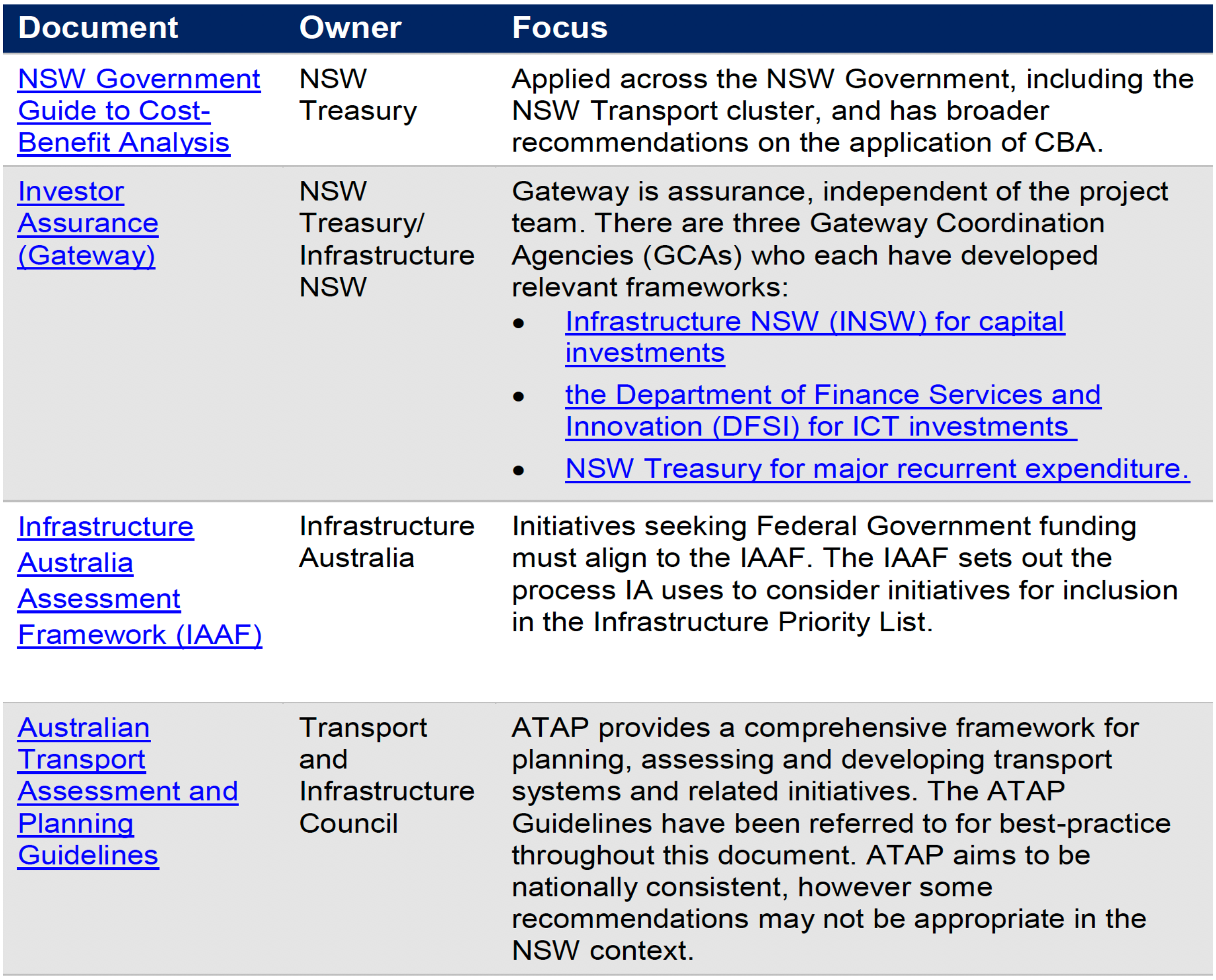
- Provides a consistent, best practice framework for NSW Transport evaluations
- Aims to measure the full impacts of decisions on the NSW community – economic, social and environmental.
- Is aligned with the high-level guidance in NSW Treasury's *NSW Guide to Cost-Benefit Analysis*.
- Co-ordinates with the national guides, the *Australian Transport Assessment and Planning Guidelines (ATAP)*, the *Infrastructure Australia Assessment Framework (IAAF),* and the *Notes on Administration for Land Transport Infrastructure Projects,* where appropriate or required
- Is focussed on the practical application of CBA to decisions in the NSW Transport cluster.

Supporting guidance and frameworks are listed further in Box 2. Some associated guidance products for CBA practice are also provided on the TfNSW website. Responsibility for professional oversight of CBA for TfNSW rests with the TfNSW Evaluation and Economic Advisory Team. This Team co-ordinates especially with the Assurance team and Investment Priorities team in TfNSW ensuring that compliance and assurance requirements for CBA are met when CBA is part of business case consideration.

The TfNSW Guide makes clear the need to examine relevant non-market benefits and costs and to seek to monetise and quantify these where possible to assist the cost-benefit analysis. It acknowledges that these can be difficult to measure but recommends the revealed preference and stated preference methods for consideration for this. Where an estimation of this kind is made and is a principal factor in any decision, it suggests that sensitivity analysis over key aspects of the method be conducted.

The Evaluation and Economic Advisory Team at TfNSW provides resources and advice, including experience from recent CBAs, so that frameworks, tools and information that support CBA based decision-making can be used. However, the Portfolio Review has affirmed that no current resource, direction or case devoted to including the value of reputation impact from cyber-security activity in CBA is available. Nor is there knowledge of this from other overseas jurisdictions eg United Kingdom Department of Transport, 2018.

Box 2. Cost-Benefit Frameworks: NSW and Transport



Document	Owner	Focus
NSW Government Guide to Cost-Benefit Analysis	NSW Treasury	Applied across the NSW Government, including the NSW Transport cluster, and has broader recommendations on the application of CBA.
Investor Assurance (Gateway)	NSW Treasury/ Infrastructure NSW	Gateway is assurance, independent of the project team. There are three Gateway Coordination Agencies (GCAs) who each have developed relevant frameworks: • Infrastructure NSW (INSW) for capital investments • the Department of Finance Services and Innovation (DFSI) for ICT investments • NSW Treasury for major recurrent expenditure.
Infrastructure Australia Assessment Framework (IAAF)	Infrastructure Australia	Initiatives seeking Federal Government funding must align to the IAAF. The IAAF sets out the process IA uses to consider initiatives for inclusion in the Infrastructure Priority List.
Australian Transport Assessment and Planning Guidelines	Transport and Infrastructure Council	ATAP provides a comprehensive framework for planning, assessing and developing transport systems and related initiatives. The ATAP Guidelines have been referred to for best-practice throughout this document. ATAP aims to be nationally consistent, however some recommendations may not be appropriate in the NSW context.

TfNSW Supporting Guidance and Frameworks for CBA.
Source: *Transport for NSW Cost-Benefit Analysis Guide 2019, p.15.*

However, TfNSW has indicated that this may be an important dimension of the business case for cyber-security investment decisions for transport for NSW. Hence the task given for this report. It is appropriate therefore that future work addresses the necessary guidance to underpin augmentation of the TfNSW *Cost Benefit Analysis Guide* and associated analysis products, with reference to the valuation of reputation impact of cyber security attack in the CBA component of the business case for cyber-security investments.

PART B. NEW APPROACHES TO REPUTATION VALUATION

Part A above provided the essence of the relevant literature available for analysis of the valuation of reputation issue for cybersecurity, and it examined the information gathered for this project on the broad operating environment for locating this issue within Transport.

In Part B, this report distils key research issues emerging from Part A that help define the way forward, and then provides guidance on the way forward in the light of evidence gathered for the project and assessment of options.

Research Issues including Stakeholder Insight

As a preliminary matter to defining the way forward, it is noted that the *Risk Management Framework* used by TfNSW (TERM) refers to one set of agencies and obligations for which the Transport portfolio is responsible.[5] For that Framework use, the list is:

- Transport for NSW
- Department of Transport
- Sydney Ferries
- Transport Service of NSW.

However, while these agencies may constitute the bulk of activity and budget they do not represent the totality of the transport portfolio's information and communications activities that may be seriously affected by a cyber-attack that could create reputation loss with the New South Wales community.

Rather each Legal Entity has its own risk management framework, and while the entities shown use TERM, other entities within transport (i.e. Metro, Sydney Trains, NSW Trains) have their own frameworks which are aligned to TERM. There is a hub and spoke model in place whereby the central team provides a set of central controls, including common policies and standards, and assurance, and spokes ensure the implementation of the controls for specific agency systems.

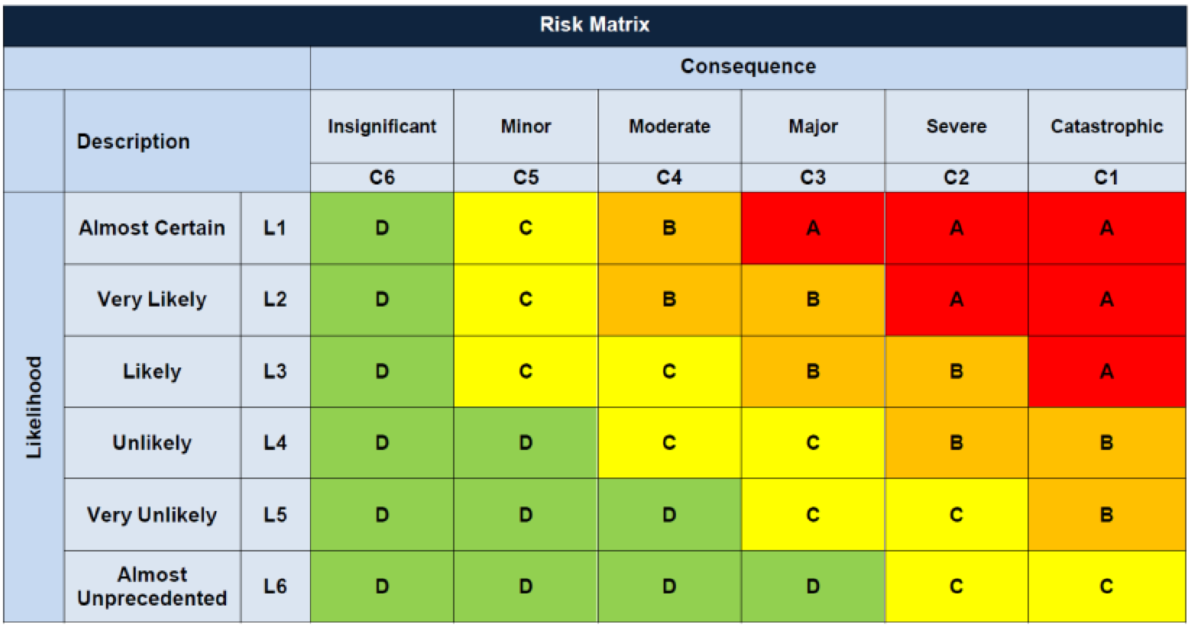
It may not impact this project directly, but it would be useful to establish whether the dependencies between systems inside the portfolio, or between the portfolio and the outside world, have been mapped and managed in line with the standards proposed by the Carnegie Mellon University and the US Department of Homeland Security.[6] Affirmation of the fully architected nature of the hub and spoke model is an important related research issue.

[5] TfNSW, "TfNSW Enterprise Risk Management Standard", 1 July 2020.

[6] See Ross Gaiser and John Haller, "Methods and Tools for External Dependencies Management", Department of Homeland Security and Carnegie Mellon University, 2015, https://resources.sei.cmu.edu/asset_files/Podcast/2015_016_001_435533.pdf. We note the references to managing external dependencies in the documentation provided by TfNSW. They are not included here because of classification of that information.

More broadly, the threats to the portfolio that might arise in cyberspace can be considered to align with the six levels of risk outlined in the TfNSW *Risk Management Framework* in Table 5 below. This research therefore understands reputation in the same way that the Framework does: "Establishing and maintaining the trust and confidence of our stakeholders and the public". This project is not assessing risk. It is not addressing reputation loss relating only to the efficient delivery of some particular individual services and is indeed broader than just reputation accordingly.

Table 5: TfNSW Risk Matrix



Risk Matrix

			Consequence					
	Description		Insignificant	Minor	Moderate	Major	Severe	Catastrophic
			C6	C5	C4	C3	C2	C1
Likelihood	Almost Certain	L1	D	C	B	A	A	A
	Very Likely	L2	D	C	B	B	A	A
	Likely	L3	D	C	C	B	B	A
	Unlikely	L4	D	D	C	C	B	B
	Very Unlikely	L5	D	D	D	C	C	B
	Almost Unprecedented	L6	D	D	D	D	C	C

Source: *TfNSW Risk Management Framework*, 2020

Drawing on this approach, the questions/hypotheses addressed in this research for reputation can be defined as:

1. How might cyber-attacks affect the reputation of Transport?
2. How might a monetary valuation be placed on the effect of cyber-attacks on Transport?
3. How should such monetary valuations be incorporated in transport project cost-benefit analysis procedures for judging cyber-security investments and projects?

The Literature Review and the Portfolio Analysis reported in Part A provide the existing approaches to this. However, this can be augmented usefully by interrogation of key stakeholders for the TfNSW group.

Extensive interviews/meetings were therefore held with Transport managers and related agency officers to ensure mutual understanding for the pursuit of these questions. Interviews were also held with key stakeholders outside of official Transport structures, in other agencies and in private business. The discussions were in confidence to guide the researchers through informal exchange.

However, this work when combined with the Literature and Portfolio Review insights produced a clear set of issues to be directly considered in defining the way forward to obtain new insight. These issues are in two parts: the Nature of Cyber Issues and the Nature of Valuation Issues, and can be summarized as follows:

The first set of issues relate to the framing of cyber issues (including attack and data breach) for this field work. In particular, in the Literature and Portfolio Review work it was found important to ensure clarity and understanding by participants of the following elements of cyber issues affecting reputation loss:

- Type of damage arising:
  - Safety
  - trust (protecting personal data)
  - convenience

- Scale of damage arising:
  - Safety: casualty levels
  - trust (protecting personal data): number of people affected (records revealed)
  - convenience: what services disrupted, for how long

- Intensity of public sentiment

- Time factor:
  - from Day Zero to Day 30, Day 31 to Day 180, beyond day 180

- Source of the attack:[7]
  Terrorist, hacker (criminal or hactivist), foreign government, incompetence

- Quality of prevention measures in place prior to the cyber incident:
  - an overall judgement of competence rather than a forensic, granular and specialist analysis on how well Transport acted to prevent this type of incident

- Quality of response to the cyber incident:
  - an overall judgement of competence rather than a forensic, granular and specialist analysis on how well Transport acted to terminate the incident and repair systems
  - were cascading effects allowed to generate when they could have been prevented?
  - remedial or compensatory actions for affected citizens.

The second set of issues relate to appropriately eliciting Valuation of Reputation Loss for Transport from Cyber Attack (including data breach) through the field work. The analysis and consultation undertaken indicated that the following variables need to be understood, and reflected in any field work phase for valuation:

[7] We note that TfNSW identified seven sources of cyber threat: Nation State, Criminals, Terrorist Organisations, Hacktivist, Insider, Unscrupulous Operators.

- Elements of Cyber Attack damage that are able to be measured from standard operational data and attributed monetary values without new public valuation research

- Public understanding of key components of reputation affected by Cyber Attack (as per Type and Scale of Damage, Time Factor, Source and Quality of Prevention and Response) including through cases in Focus Group discussion

- Stakeholder understandings across various business, professional, local government and consumer groups, of cyberattack possibilities, and consequences for them, to be gained from interviews with key representatives.

- Public understanding of the nature of the Transport portfolio and its component agencies and operations and their relationship to Government and to business partners and private transport providers.

- Potential differences in valuation according to ownership and operation eg public vs private, actions pre-, during- and post- cyber matters, and attribution of responsibility

- Sources of information for the public about issues arising from the various types of Cyber Attack covering types of interpersonal advice, mainstream media, social media.

- Public understanding of the magnitudes of the dollar estimates being expressed and their context including over time.

- Major demographics in relation to all answers in the population survey, including age, gender, education, occupation, income, household composition, residence location, political identification plus transport use.

It was concluded that with these issues so identified it could be productive to pursue new research using field data gathering - both qualitative and quantitative. Further, one main path for such consideration is to operate via focus group analysis and by a population survey using a stated preference contingent valuation approach.

As indicated above in the Literature Review, contingent valuation refers to use of hypothetical questions in context through a survey to elicit attitudes to the problem and their monetary expression through “willingness to pay”.

The use of a prior focus group was seen as advisable because of the complexities of risk analysis and cyber security and of the transport system. Prior examination of survey questions, words, concepts, information, contexts etc to be provided to full survey respondents would not only be productive, but essential for a truly meaningful product regarding actual valuation of potential cyber-attack damage to reputation in transport. The idea was to ensure that the potential survey questions are attested as accessible and properly targeted.

The general stated preference, contingent valuation, methodology based on survey was suggested as appropriate to answer the research issues questions and to meet the research aims for improved cyber-security investment policy and decision because it has been widely tested and used previously, though not applied to this specific topic. Contingent valuation is fully recognised in official benefit-cost guidelines and practice, in Australia and overseas.

The data collection process can be administered economically and conveniently by on-line standing commercial omnibus survey. The focus group phase is best seen as producing guidance to precise wordings for the survey, for which precedent questions have been successfully applied by the researchers in other fields such as government outlays and taxes or public interest journalism. That said, focus groups can also supply interactive information that can be useful for analysis in a way that is hard to deduce from large scale surveys and can generate related attitudinal information that may be of value for agency management quite apart from the reputation valuation matter.

For a contingent valuaton (CV) survey, the data can be collected from a stratified random sample for the NSW population, with no individual identification, and with data on personal characteristics being those already collected for the standard omnibus survey without addition for specific project applications.

A distinctive feature of a full population (CV) survey would be the inclusion of both users and non-users in relation to the transport services. The analysis can be used for both a customer and voter focus accordingly, depending on the concerns of the decision-makers using the data.

The data can be analysed using both descriptive data presentation (graphs, charts, tables) based on Excel spreadsheets, and using standard software such as SPSS for more complex quantification analysis such as regression

This analysis can thus assist the valuation objective that was the concern to investigate in this research by demonstrating how a suitable quantification of reputation loss from cyber-attack can be constructed. Specific applications can pursue this general methodology and approach for particular project proposals or across a well-specified array of alternative projects as needed.

In sum, it is felt therefore that the necessary data collection can draw on clear concepts of cybersecurity and organisational reputation, to then a) use the focus group approach to affirm the capacity to understand such concepts accurately and intelligibly, and b) to use a following population survey to apply the well-established stated preference, contingent valuation, methods to these concepts, so as to deduce monetary valuation for transport of the problems of cyber-attack. This can enable cyber investment decisions to be more fully informed overall, but specifically in this way by being guided by rigorous cost-benefit guidance through this path. This can take full account of the research issues revealed by this Project's investigation of literature, portfolio review and informal stakeholder discussion.

Focus Group Analysis

Focus Group analysis was pursued for the project to begin to demonstrate the analytic path being proposed and its utility and conduct. For this purpose, Focus Group review was conducted for the project, given the research issues specified, by Essential Research in February 2021, so as to provide new insight into the context and process for obtaining valuation of reputation for Transport as regards cyber-attack. The Focus Group implemented for this was an on-line and broadly representative sample for NSW, with the discussion guide for the group structured to reveal understanding of both the Cyber Issues and the Valuation issues outlined above. The Focus Group Discussion Guide is attached as Attachment 1 to this report.

The Focus Group discussion delivered qualitative information that provided insight from the interaction and interrogation of a small but broadly representative group of the general NSW public. Some reflection of the qualitative discussion is given as an Appendix to this Report.

This in itself can be helpful for decisionmakers in the Transport system, particularly when combined with extensive parallel work already in place for stakeholders, eg Newgate Research, *Transport for NSW Stakeholder Reputation Study*, August 2018).

Moreover, the focus group qualitative findings can be tested, or generalized, by extension of the analysis to a full-scale population survey if desired. This extra step would allow the move from qualitative findings to quantification of valuation for reputation, which is our present desired outcome.

Specifically, after the extensive discussion of cyber and transport issues in qualitative terms, as seen in this Appendix to this Report, respondents were then asked specifically how much they would be willing to pay to obtain a 50% improvement in transport cybersecurity. This was a deliberate direct test of the feasibility of seeking stated preference contingent valuation of cyber -attack impact on Transport reputation in NSW.

In this experiment, conducted with the Focus Group, two indicative payment numbers were nominated for the respondents' consideration. This is called a "closed ended" or "dichotomous choice" format, in such contingent valuation analysis.

Within this Focus Group:

- 23% of the group affirmed they would "definitely" or "probably" be supportive of a $30 a year increased payment for the improved cyber security.
- 15% of the group affirmed they would "definitely" or "probably" be supportive of a $40 a year increased payment for the improved cyber security,

The full Discussion Guide and the specific willingness to pay questions used for the Focus Group are given in Attachment 1 for this Report.

These questions were intended to induce familiarity with quantification but asked only several options for a single fixed improvement and allowed qualitative answers such as "definitely would support" etc. Therefore, to go further, the quantification question to monetise the benefits from cybersecurity enhancements comprising safety, privacy and efficiency (the elements of reputation here) was then advanced to a wider array of payment options and to several levels of resultant improvement.

The question further sought a specific number as a maximum willingness to pay in increased annual taxation. This is called an "open-ended" format in stated preference contingent valuation. A maximum was sought under this open-ended approach for two resultant improvements: 50% and of 10%.

The nature of the precise form of that improvement was left to the respondent's expectation, though their preferences for priorities in cyber improvement were interrogated, so that there was an implicit assumption of improvement to meet such preferences. Deeper analysis, such as in any follow-up population survey, would constructively interrogate the composition of such improvements explicitly.

In expressing their concerns in discussion in this present Focus Group experiment, the participants themselves focussed on benefit being delivered principally through enhanced software and computer improvements and protections through more resources, and the participants expected the funds raised from this tax increase to be spent specifically on improving safety, convenience and privacy.

It was explicitly recognised by the Focus Group participants that compromise to safety, privacy and convenience would produce reputational damage from cyber-attacks. The priority ordering amongst the group as to their level of concern across the different types of cyber-attack was as follows for the "very concerned" option:

- **Reduce safety of transport users and the public including by causing accidents: 61% very concerned.**
- **Reduce convenience including through delays, cancellations and congestion: 38% very concerned.**
- **Violate privacy of customers: 30% very concerned.**

And in terms of actions which would increase reputation post-attack, the following three were seen as the most important:

- **A formal Government apology.**
- **Speedy restoration of normal service.**
- **Evidence of improved cybersecurity**.

It is worth noting however that the Focus Group participants in this project exercise:

- **felt that the overall NSW Government actual performance in managing public transport was seen as strong already in these dimensions, with 70% endorsing performance as either "very good" or "fairly good"**
- **had great difficulty recalling cyber security problems or incidents that had occurred or affected them in NSW Transport service provision**
- **were confused over the actual responsibility and relevant agency involvement which meant that where financial gains would be deployed was not fully clear. Nevertheless, around 50% did express familiarity with TfNSW.**

As knowledge of cyber security problems in general rises in the modern era, this attitude could change and should therefore be monitored carefully. Greater information on the nature of cyber threats could also alter attitudes of respondents.

These observations are useful findings illustrating the joint knowledge potential needed to result in the metrics required for cost-benefit analysis, but also being beneficial for wider management knowledge. Thus, for TfNSW itself, insights from the stated preference contingent valuation process can carry across into wider TfNSW management strategy, including linkage to:

- frameworks such as Carnegie Mellon's Factor Analysis of Information Risk (FAIR) and the Australian Defence Materiel Organisation's Schedule Compliance Risk Assessment Methodology (SCRAM),
- opinion metrics such as Unisys Trust and Newgate Research Reputation Study, and
- case insights for understanding, such as the 2020 State Transit Authority (STA) ransomware incident or the Services NSW Breach (Parliamentary Inquiry) and others.

This is a two-way learning process.

That said, the quantitative willingness to pay valuation results found from the Focus Group deliberation for this research, are as given in Table 6.

Table 6. Willingness to Pay for Improvement in Transport Cyber Security

MAXIMUM PAYMENT ($ pa)	0	5	10	20	30	40	50
10% Cyber gain (% of focus group)	69	15	8	0	0	0	8
50% Cyber gain (% of focus group)	30	15	8	24	0	8	15

Source: Essential Research, unpublished report, February 2021.

It is observed that a distinct majority (55%) of this group would support an increase of $10 or more per annum per annum for a significant cyber security improvement of 50%. But majority support was not present for a tax increase for a modest 10% improvement in cyber security, presumably because it was felt that such improvement could be expected through efficiencies in current expenditure allocations - though this presumption could itself be directly tested in further research. It should also be recalled that, as indicated above, there was quite strong support for the government's performance in managing public transport in NSW in this Focus Group.

By this preliminary estimate, the average willingness to pay for a 50% improvement in Transport cyber-security was $17 per person per annum. This would represent an increased cyber budget for TfNSW of around $115 million over the present allocation.

This is an initial indicative estimate only of the type of figure that could be incorporated into cost-benefit analysis, with appropriate field work using a large population sample, to calculate the reputation benefit per NSW resident for an improvement in cyber-security for NSW Transport.

It is here a very indicative estimation illustrating the methodology, and more specific analysis would be pursued for cost-benefit purposes for concrete project proposals. Benefits could then be compared with project costs to help order investment proposals. Due attention would need to be paid to avoiding double-counting where reputation issues might be reflected in other elements of the project e.g. supplier costs affected by Transport reputation in managing cyber and the risk factors accordingly embodied in supply contracting. Such exposition would form the basis for a *Cost-Benefit Handbook* entry for standard process.

In early academic discussion over contingent valuation itself, the question was asked by critics whether "some number is better than no number?" (Diamond and Hausman 1994). This criticism led to major improvement in these methods such that they are now in standard use in government. Of course, the methods still require skill in application to ensure that the estimates obtained are accurate. Where any reservations remain, or quick analysis is deployed, "sensitivity analysis" is an immediate mechanism for any remaining "abundance of caution". This means the evaluators can see what difference alternative benefit estimates across a range make to project validation. Where sensitivity in results to reasonable alternative assumptions is found to be strong, then further deeper research to resolve the matter is wise.

Ways Forward

If it were desired to properly validate or affirm the order of magnitude of the results obtained here from this small Focus Group analysis, a representative sample NSW population survey should be undertaken. A sample questionnaire for such an exercise was in fact designed, which incorporated findings from the Focus Group on the wording of questions to be asked. Such a survey can provide, from the willingness to pay questions, a dollar estimate of valuation of Transport reputation damage that could be incorporated in business case evaluation for investments in cyber projects for Transport, as illustrated from preliminary Focus Group research.

A sample of the form the questionnaire could take for such a Population Survey is given in Attachment 2 to this report. This embodies much of the insights from this project's early work as well as the more general body of such work. But more research could still be useful, before such a large field implementation is undertaken, to refine this instrument further. This is because cybersecurity is such a complex area, as are matters of "reputation". **A useful further process before proceeding with any full surveys could use small field tests, and especially cover such information issues for the questionnaire shown by the Focus Group work to heavily influence answers.** These are especially:

- the precise sectoral and governmental information to be provided to respondents
- the form and magnitude and impact of cyber-attacks being considered
- the nature and focus of the improvements for cyber-security

The resultant final Transport Cyber Attack Valuation questionnaire would then provide a basic answer on reputation valuation for cyber-attack, and its application could be customised as desired for specific project proposals via conduct of project specific stated preference contingent valuations.

Such surveys are not expensive relative to major Infrastructure projects, but care in their conduct is required since

- Public surveys on hypothetical projects can become politically controversial, more so where options are being reviewed but without advance commitment.
- Stated Preference methods based on willingness to pay can involve specification of payment methods and amounts and, where used, these can be used to politically sensationalise a valuation exercise.

Concern over political sensitivity may sometimes be exaggerated, however, since such stated preference methods of valuation are a standard and much used methodology for many projects in Australia and elsewhere especially in the environmental, health and cultural domains. Those conducting such work, including in other NSW government project evaluation, have developed survey instruments that understand such concerns.

Alternatively, **benchmarks can be estimated from wider exercises, eg across government, which reduce the concern over particular projects or service by embedding specific area matters within a multi-service context.** Indeed, this may be an excellent way forward for not only does it diffuse sensitivity over particular projects or fields, but it controls for the embedding problem that occurs where questions are asked about specific areas in isolation from alternatives and the bigger picture of government activity. In Australian cost-benefit analysis this has been called the "koala problem": if willingness to pay to save the koalas is asked in isolation rather than as part of wider wildlife and environmental deliberation, exaggerated valuations may be obtained. Overall, this can establish relativities in priorities.

Of course, if direct willingness to pay methodology remains an issue, **other alternative methods can be adopted to assist valuation**. **Or these methods can complement WTP,** if it is felt to be insufficient. Examples are:

- *"planning balance sheets"* where all elements in a project choice are made clear, systematic and transparent, but components that are beyond dollar metrics can still be listed and left for the decision-makers' own valuation after all other components' metrics and risks and probabilities are incorporated.
- *"ordinal survey analysis"* where relative preferences are obtained rather than absolute values, but in such a way that absolute values can be imputed from imposed distributions assumed or taken from other analyses. Categories can be converted to continuous distributions using advanced statistical methods (Turnbull 1976).
- *"discrete choice analysis (DCE)"* where focus group and survey methods are sued and emphasis is given in multiple choice questions to attributes of the activity or object of interest so that the analysis captures what matters in the assessment of value.

A further promising way forward is to bring across analysis from private market measurement for the purely business elements of the decision-making. The focus in the stated preference contingent valuation exercise has been to elicit full public or community valuation. Within that, transport users can be distinguished from non-users, and this may also be an important source of management information. But it has been assumed that, from the perspective of elected governments, whole of community preference testing can be important in ways that do not apply for purely business calculations. This is especially pertinent where **social cost-benefit analysis** is required, as opposed to purely business project evaluation such as in discounted cash flow analysis.

That said, where more specific information on purely business calculation is desired, reputation effects there can be confined to users (and, in the stakeholder analysis, to partners). Those insights from the Stated Preference contingent valuation and from the Stakeholder Analysis (which can be formalized beyond that used in this project), can be complemented by Event Analysis based on stock market valuations.

Event Analysis uses financial market data to measure the impact of a specific event on the value of a firm (Mackinlay 1997). In recent years it has been much used to look especially at the stock market impact of security breaches and vulnerability announcements. Originally focused on impacts in a relatively short time period, the research has expanded to look to longer-term effects (Chang et al 2020) and to differentiate the nature and magnitude of the event (Campbell et al 2003).

The stockmarket measures reflect the views of all market participants regarding the standing of the firm and how it may be affected by its management of cyber matters, including cyber-attack. Changes in stock valuation are interpreted in the financial literature as summarizing firm reputation (Tosun 2020). For the business component of TfNSW decision-making, the conclusion is that a parallel examination of the implications of cyber-attack for firms can be used to assess the business component of tfNSW projects too for cyber security investments for that purpose. This is a complementary or parallel direction for informing Transport decision-making on cyber investment, especially where that is most business-oriented.

This project more generally used the recent emergence of growing incidence of cyber-attack in contemporary society as its focus, for showing the applicability of appropriate public valuation to assist with business case decisions in government services areas. The growing importance and awareness of this issue indicates that ongoing work for this purpose should be incorporated into public management procedures.

To conclude, this study outlines an accessible framework through focus group and population survey methods for help in managing these issues in organisations, even where they are technically specialised and complex. The idea is to:

1. **help integrate the qualitative knowledge generated into more general transport management learning and knowledge**
2. **provide direct quantifications via stated preference surveys for more technical decision-making tools such as in social benefit-cost analysis in transport**
3. **develop and use complementary methods such as event analysis as a cross-check or "triangulation" in this field**
4. **use this systematic and analytic approach to knowledge to be further located relative to global best practice in transport evaluation**
5. **demonstrate how these method scan benefit from working across government service activity in other agencies.**

ATTACHMENT:

FOCUS GROUP QUALITATIVE DISCUSSION ON TRANSPORT REPUTATION AND CYBER ATTACKS

On the Cyber Issues, it was generally felt that Governments cannot prevent true emergencies – part of classifying these situations is that they are largely unavoidable, and the governments' role was seen as being to minimise the effects. However, the criteria to judge a successful government response to any emergency were understood and it was further acknowledged that they depend on the type of emergency. Across the Group these criteria for success were seen to broadly involve:

- Existing risk management processes/policies
- Consequences (e.g. societal, economic, physical/mental health, political)
- Availability and reliability of information
- Transparency
- Timely initial response(s) which then build to a finalised approach
- Consistency of approach within and across levels of government
- Responses based on evidence and expert opinions
- Learning from previous experiences/examples

Who Constitutes Government?

However, the participants did find it difficult initially to understand the idea of "the government's reputation" as a separate issue and to distinguish, without further guidance, between the government and the Premier's reputation, for example. The Premier is defined as the leader of the government, which means that rating the two separately is very difficult in participant's minds.

Reputation and Nature of Emergency Response

Similarly, to determining the quality of an emergency response, there were many elements which were seen to help determine the government's reputation. These included:

- Awareness and connection to public sentiment and issues
- Working for the good of the public, not a limited few
- Balancing conflicting needs when responding to emergencies
- Transparency/honesty
- Empathetic connection
- Adaptability to emergencies or new information
- Ability to follow through on promises/implement changes
- Policies educated by experts (not politics)

NSW Government Reputation especially Privacy

At the time of the Focus Group, a majority of participants felt that the NSW government generally has a positive reputation, and this was primarily due to good management of the Covid-19 pandemic.

It was valuable to learn that most participants did not recall examples of cyber-security breaches – those who could tend to be more politically engaged than the others. Those that could recall cyber-breaches or attacks tended to recall fairly large-scale and less recent situations. Few recalled recent Services or Transport NSW breaches, and no one in the groups claimed to be personally impacted by them.

That being said, most respondents recognised the large amount and types of data produced by governments – and the value of these data to other actors. Their spontaneous concerns were primarily connected to the financial value of their personal information and the consequences for them if this information is accessed. While participants agreed that this situation would reflect poorly on the government impacted, they generally did not realise the broader impacts (such as safety and convenience) in the population.

Cyber Attack Impacts: Privacy and Beyond

When looking at the two other possible impacts of a cyber-attack beyond privacy that were presented, participants express less concern than for a privacy violation. The discussion in the Focus Group revealed here that:

1. *Violating privacy of customers* was generally understood by participants, generally voted most concerning, and recognised as having many personal and sometimes severe implications eg
   - "Violate privacy of customers. Would have a ripple effect, theft of identity, protected custody etc"
   - "Violation of privacy can in turn lead to financial and security issues for an individual, in this case possibly me. Any private information can be used to steel, blackmail, antagonise, influence discriminate and intimidate to name just a few".
2. *Reducing safety of transport users and the public including by causing accidents was* generally understood by participants, the second most concerning and overtakes privacy when the participant is concerned by possible deaths, though some participants felt that this impact is more unlikely than the first and therefore less of a concern eg
   - "This is concerning, but it takes a great deal of skill to implement, and most systems have security in place, so while it would have a great impact, it's an unlikely event".
   - "I think the second is most concerning which would have a flow on effect on the 3rd. I don't believe it's as much of an issue on its own. Would it be an inconvenience, yes; is it as bad as the media makes out to be, I don't think so."
3. *Reducing convenience including through delays, cancellations and congestion* was generally understood by participants, and seen more as inconvenient than as anything worrying.

Cyber Attack Location and Motivation

When prompted with some examples of recent cyber-attacks, there was a diversity of views between those who said Services NSW versus NSW Health Service (NHS) examples given were most concerning. Some found both worrying:

> "I think anything to do with personal information and security is the most concerning though the idea that companies and trains can be hijacked & derailed without physical presence is scary"

Others saw Services NSW as more concerning as participants felt it was most likely to impact them directly e.g.

> "Personally, I would be most concerned about the Service NSW breach. Reason being is that it is closest to home and more inclined to affect me directly".

While others were concerned by the possibility of deaths in the NHS example:

> "The situation that concerns me most is the NHS breach because it has the greatest impact on human life if patient surgeries have to be cancelled due to a ransomware attack - that is so awful".

Also, there was some polarisation with roughly the same proportion of participants being surprised by any of the examples, as those who were not surprised:

- "None of them really surprised me…I guess I've gotten cynical over the years and don't get surprised at how low people can get".
- "Prior to today, I had not heard of any of these situations however none of them surprise me because in this day and age, especially with the internet, anything is possible, and nothing is off-limits for those who are looking to do wrong."
- "The Services NSW example surprises me the most as it is closest to home for us as I am also a user of Services NSW so it feels like I could have been at risk of this too".

Focussing on Transport Cyber Attack

However, once the examples prompted participants, they were more able to describe or outline the possible impacts of an attack on TfNSW, affirming that opinion research here for contingent valuation would require well-constructed information provision if informed answers and deliberation are desired:

- "If a Cyber- Attack were to happen on the NSW Transport, I think that NSW would grind to a stop. Depending on how bad it is, it could affect so many people, from the transport workers to the general public and also the transport of goods and services. It could stop ppl getting to and from work which would disrupt everything and working life to personal life. Children getting to and from school. And the transport of good and service would affect the productive of the state in so many ways".

- "If the cyber-attack was just, say, for example, access to my Opal card and my travel history I would not be too concerned so long as my credit card details were not at risk. If, however, the rail coordination and signal points etc could be hacked and cause a collision between trains that would be a horrific outcome. A situation whereby the coordination of traffic lights was hacked would be somewhere in between with regards to severity"

- "Something as minor as hacking the Opal system making trips free, that wouldn't be good at all (Insert sarcasm emoji here), through to freezing the entire rail network stranding people till alternatives can be found to hacking the signals potentially causing a collision".

At the same time, respondents did struggle to articulate what the NSW government, in particular, could do prevent these attacks – often falling back on listening to expert opinions, running test attacks with 'white hat hackers' and investments. Participants often claimed they didn't know enough about the topic to say what the government should do – it's beyond their scope to answer, indicating the importance of education in this area if a more informed public is desired. Once again, the importance of correctly specified information provision for population survey follow-up arises from this focus group insight.

Participants did support the hypothesis arising from earlier literature research that the severity, length of crisis and number of victims are understood as the primary drivers of the perceived seriousness of a cyber-attack. The perpetrator or motivation is a secondary element mentioned by some participants. A few participants felt that all cyber-attacks should be treated equally seriously as they could have unpredictable impacts eg

- "I don't think we can take any cyber-attack as less serious, I think that small and big would affect the state in some way."
- "All cyber-attacks should be considered serious as they may just be a test".

Political/terrorist groups and foreign governments/departments were seen as the most concerning perpetrators of cyber-attacks by far, with employees of the agency being less concerning

- "Political/terrorist groups - these are the most concerning for me. They have an agenda that's about disabling and maiming, with intent to cause as much harm as possible, including taking life, and with a longer-term intent of demoralising the general populace".
- "Employees are also really concerning as they have so much intel into the company and documents and files/programs, they could be collating this information for years before attacking"

Less clear was recognition of cyber failure i.e. swapping from cyber-attacks to cyber-breaches was confusing for participants as they attempted to think of situations where the attacks could be accidental or unplanned. Indeed, they struggled to think of situations where a breach could have occurred, despite a few listing breaches during some early topic discussion. That said, and acknowledging the need to recognise the different understanding of attacks versus breaches, there's some indication that the characteristics which make a cyber-attack more or less serious, also apply to a potential breach

- "I suppose if it affects people and their lives and livelihoods then I think it's more serious to me".
- "Whether it was intentional or unintentional, it should still be treated and dealt with the exact same".

Transport Cyber Preparation and Response's Impact on Respondent Behaviour

In terms of anticipating and responding to gaps in knowledge or attitude, participants also struggled with big 'what if' questions about the reputational impact of a cyber-attack or breach, as there are so many aspects of this that they felt that they needed to consider.

Participants who solely (or mostly) rely on public transport to get around, had a denial or limited response answer often in their response to what would change with a cyber-attack:

- "I do not think a cyber-attack would impact me that much in terms of using transport services as I still need to get to where I am going as I do not have a car at the moment".
- "I don't think it would impact my use of transportation services, as it is an essential service for me to get anywhere and live my life. Even if it occurred over a number of years my answer wouldn't change".

At most, they may stop using the auto top-up function on their Opal care and at most they may vote differently at the next election

> "If this was an ongoing problem I would no longer register my Opal card and attach an auto top up".

Equally, participants who were less reliant on public transport say the issue would concern them, but wouldn't lead to a behavioural change. However, if the attacks occurred over a long period of time without being fixed by the government this would erode the government's reputation

- "One successful cyber-attack is unfortunate. Two is careless. Any more than that, over a number of years, would cause me to demand some staff to find another occupation because they clearly are not up to it".
- "If the government was very slow at responding to the attack or showed little incentive in fixing these issues, I would also consider other modes of transport".

- "I would be more suspicious and wary about the transport options. If the government wasn't doing there upmost in protecting transport systems from cyber-attacks over years it would definitely reduce the amount of time I would spend on transport services".

The Key Role of Information and Message

Most critical for participants was that the government's next steps should be appropriate to the emergency that it faces – many participants perceived at that time that the Victorian government mishandled their Covid-19 response by over-reacting and pushing lockdown for too long. That said, information was emphasised as crucial. For cyber-security, this covered immediate information needs:

- Initial response from government
- Impact for the system or public
- Plan for further interventions

And it covered later information needs as regards:

- Perpetrator(s) and motives

Sources of information also were a focus, and it was felt that those individually impacted should be informed directly via text or email as soon as it's known their data has been accessed.

Further, risk of injury or death from a cyber-attack, needed to be communicated on those transport lines themselves as well as through email/text/press conference

> "If Opal was hacked and banking information was taken then a mass text to all of the customers would do it... If signals went down from a cyber-attack causing delays, then social media and the other mediums they use to let us know about transport delays would do it. I use a real time transport tracker mornings before I commute to work…That would work too".

Government websites and press conferences were seen as most important, followed by public announcement - recordings on their websites and apps. TV, radio and other formal news sources were less favoured, with some acknowledgement that the media could sensationalise the facts, so this and social media would be a secondary option eg

- "I would watch the news about it, but more online as that can be updated as it happens, than print, radio or TV as they're dependent on deliveries or specific news breaks".
- "Most public media puts a 'spin' on their view of 'media releases' so a personal agency representative on TV would be my expectation".
- "Social media accounts would be more real time than most traditional main-stream news services".

As to the messenger, this was said to depend on the size of the breach/attack and targets – generally the Transport Minister as a core expectation for major issues. But as severity increased, the Premier should be conveying the issue to the public.

And the regularity of updates was emphasised and was discussed by reference to the 2019-20 bushfires and Covid-19 pandemic – ongoing, daily (if necessary), updates and clarification as new information is available, were seen as now expected.

The need for micro-targeting was also recognised even within a Focus Group that was not itself fully representative of all communities, because of its small size. Thus multicultural, disability, and aged communities, and key groups impacted for work and essential service were identified – and the need for well-planned communication based in good part on having consulted those communities (often through representative organisations) as a component of a preparatory strategy involving partnerships in place, and not just as an after-the-event add-on, was stressed.

REFERENCES:

Abelson P. 2019. *Public Economics: Principles and Practice.*, Sydney: Applied Economics,

Acquisti A, LK John and LK and G Lowenstein. (2013)," What is Privacy Worth? ", *The Journal of Legal Studies*, 42(2). June, 249-274.

Acquisti, A, A Friedman and R.Telang, 2006. Is There a Cost to Privacy Breaches? 27th International Conference on Information Systems, Milwaukee.

ACSC. 2020. ACSC Annual Cyber Threat Report July 2019 to June 2020. https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Agrafiotis I, JR Nurse, M Goldsmith, S Creese and D Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity.* 4(1)

Alharbi HB, N Abdulrazak Baghanim and A Munshi. 2020. Cyber Risk in Internet of Things World. *3rd International Conference on Computer Applications & Information Security (ICCAIS).* Riyadh, Saudi Arabia. pp. 1-5, https://ieeexplore.ieee.org/abstract/document/9096720

Arrow K, R Solow, PR Portney, EE Leamer, R Radner and H Shuman. 1993. Report of the NOAA Panel on Contingent Valuation. *Federal Register* 58, pp 4601-4614

Austin G ed. 2020a. *National Cyber Emergencies. The Return to Civil Defence*. London: Routledge

Austin G ed. 2020b. *Cyber Security Education: Principles and Policies*. London: Routledge

Austin G. 2020c. U.S. Policy: Cyber Incidents and National Emergencies. In Austin (ed) *National Cyber Emergencies. The Return to Civil Defence*. London: Routledge, 2020, pp. 31-59

Austin G and G Withers. 2019. Creating Social Cyber Value. Social Cyber Institute Working Paper No. 1. https://www.researchgate.net/publication/342863286_Creating_social_cyber_value_as_the_broader_goal

Australian Government. 2006. *Handbook of Cost-Benefit Analysis*. Department of Finance and Administration, Canberra

Baker R. and B. Ruting. 2014., *Environmental Policy Analysis: A Guide to Non-Market Valuation.,* Staff Working Paper, Canberra; Productivity Commission, January

Benoliel, M., Manso,M., Ferreira, P.Silva, C., and C.Cruz. 2021 ""Greening" and comfort conditions in transport infrastructure systems: Understanding users' preferences" , *Building and Environment*, 195, 1-12

Boardman, A. et al, 2018, *Cost-Benefit Analysis, Concepts and Practice*, Cambridge University Press, fifth edition.

Brasington H and M Park. 2016. Cybersecurity and ports: Vulnerabilities, consequences and preparation. *Ausmarine*, 38(4), p. 23

Campbell,K, L.Gordon, M.Loeb, and L.Zhou 2003, "The Economic Cost of Publicly Announced Information Security Breaches", *Journal of Computer Security*, 11, 431-448

Canel M and K Sanders. 2012. Government Communication: An emerging field in political communication research. in H Semetko and M Scammel eds. *Handbook of Political Communication* Thousand Oaks CA: Sage 85-96

Carruthers B. 2016. Internet of Things and Beyond: Cyber-Physical Systems. IEEE Internet of Things, Newsletter, Internet of Things and Beyond: Cyber-Physical Systems. https://iot.ieee.org/newsletter/may-2016/internet-of-things-and-beyond-cyber-physical-systems

Carson, RT. 2011, *Contingent Valuation: A Comprehensive Bibliography and History,* Cheltenham UK, Edward Elgar.

Carson RT. 2012. Contingent Valuation: A Practical Alternative When Prices Aren't Available. *Journal of Economic Perspectives* 26(4), 27-42

Centre for International Economics, *Tax Concessions for Public Interest Journalism,* Canberra, November. https://piji.com.au/wp-content/uploads/2019/11/piji-tax-concessions-for-public-interest-journalism.pdf

Centre for Policy Development. 2017. What Do Australians Want? Melbourne: CPD. December, https://cpd.org.au/2017/12/what-do-australians-want-discussion-paper-december-2017/

Chang,KC, YK Gao and SC Lee, 2020, "The Effect of Data Theft ona Firm's Short-Term and Long-Term Market Value,", *Mathematics,* 8, 1-21

Cimpanu C. 2020. First death reported following a ransomware attack on a German hospital. ZDNet. https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/

CMU. 2016. External Dependencies Management. Carnegie Mellon University, in cooperation with U.S. CERT. https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-EDM.pdf

Daniels R. and D Hensher. 2000. Valuation of Environmental Impacts of Transport Projects: The Challenge of Self-Interest Proximity. *Journal of Transport Economics and Policy*, 34(2), May, 189-214

DHS. 2008. *Fact Sheet: Cyber Resilience Review. Department of Homeland Security. 5 September 2008,* https://us-cert.cisa.gov/resources/assessments#ten-domains

Diamond, PA and JA Hausman. 1994 "Contingent Valuation: Is Some Number Better Than No Number?", *Journal of Economic Perspectives*, 8(4), 45-64.

Dobes L. 2016. Social cost-benefit analysis in Australia and New Zealand: the state of current practice and what needs to be done. Canberra: ANU Press for ANZSOG, (with Joanne Leung, George Argyrous)

Evans M. Cyber Innovative Technologies. 2020. Digital asset based cyber risk algorithmic engine, integrated cyber risk methodology and automated cyber risk management system. U.S. Patent Application 16/585,202

Florio M. 2019. *Investing in Science. Social Cost Benefit Analysis for Research Infrastructure.*, Cambridge Mass. MIT Press

Gao L, TG Calderon and F Tang. 2020. Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, p.100468

Gwebu KL, J Wang and L Wang. 2018. The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems,* 35(2), 683–714

Hendry. 2019. NSW govt cyber office to hire 75 new staff as remit expands. itnews. https://www.itnews.com.au/news/nsw-govt-cyber-office-to-hire-75-new-staff-as-remit-expands-552408

Herbolzheimer C, E Sekeris and L Chacko. 2016. *Can You Put a Dollar Value on Your Company's Cyber Risk?* HBS Case H036LI-PDF-ENG, 5 October

Hogg JJ. 2017. Why the Entire C-Suite Needs to Use the Same Metrics for Cyber Risk., HBS Case H04OUR-PDF-ENG, 17 November

James O. 2009. Evaluating the expectations disconfirmation and expectations anchoring approaches to citizen satisfaction with local public services. *Journal of Public Administration Research and Theory*, 19(1), 399-418

James O. 2011. Performance measures and democracy: Information effects on citizens in field and laboratory experiments. *Journal of Public Administration Research and Theory,* 21(3), 399-418

Johnston RJ, KJ Boyle, W Adamowicz, J Bennett, R Brouwer, TA Cameron, WM Hanemann, N Hanley, M Ryan, R Scarpa, and R Tourangeau. 2017. Contemporary Guidance for Stated Preference Studies. *Journal of the Association of Environment and Resource Economics*, 4(2), 319-405

Kostyuk N. and C Wayne. 2019. Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats. http://www-personal.umich.edu/~nadiya/communicatingcybersecurity.pdf

Krishan R. 2018. Corporate solutions to minimize expenses from cyber security attacks in the United States. *Journal of Internet Law* 21(11), pp.16-19

Laing A. 2003. Marketing in the public sector: towards a typology of public services. *Marketing Theory* 3, 427-445

Lehto M. 2020. Cyber Security in Aviation, Maritime and Automotive. In: P Diez, P Neittaanmäki, J Periaux, T Tuovinen and J Pons-Prats eds. *Computation and Big Data for Transport. Computational Methods in Applied Sciences*, vol 54. Springer Cham. https://link.springer.com/chapter/10.1007/978-3-030-37752-6_2

Lewis R. Reputational risk and Australia's top organisations. *Governance Directions*, Vol. 69, No. 11, Dec 2017: 659-664, https://search.informit.com.au/fullText;dn=282934426591229;res=IELBUS

Li X-B, X Liu and L. Motiwalla. 2020. Valuing Personal Data with Privacy Considerations. *Decision Sciences*, May

Luoma-aho V and M-J Canel. 2016. Public Sector Reputation. In CE Carroll ed. *SAGE Encyclopedia of Corporate Reputation.* (pp. 597-600). SAGE Publications. pp. 597-600

McKinlay, A.C, 1997, "Event Studies in Economics and Finance", *Journal of Economic Literature*, XXXV, March, 13-39.

McKinty C. 2017). The C-Suite and IT Need to Get on the Same page on Cybersecurity., HBS Case H03MQV-PDF-ENG, 26 April

Morando F, R Iemma and E. Raiteri. 2014. Privacy Evaluation: what empirical research on users' valuation of personal data tells us. *Internet Policy Review*, 3(2), May, 1-12

Noam E. 1997. Privacy and Self-Regulation: Markets for Electronic Privacy. In US Department of Commerce, *Privacy and the Self-Regulation in the Information Age*, Washington DC, NTIA, chapter 1B

NSW Treasury. 2017. *NSW Government Guide to Cost-Benefit Analysis,* Policy and Guidelines Paper, TPP 17-13, Sydney: The Treasury

Papastergiou S, H Mourartidis and H Kalogarki. 2020. Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. Evolving Systems. Springer. https://link.springer.com/content/pdf/10.1007/s12530-020-09335-4.pdf

Skinner C and P Skinner. 2019. Bank Disclosures of Cyber Exposure. *Iowa Law Review* 105, no. 1 (November): 239-282

Škorput P, S Mandžuka, S Bermanec and H Vojvodić. 2020. Cybersecurity of Autonomous and Connected Vehicles. In I Karabegović ed. *New Technologies, Development and Application III.* NT 2020. Lecture Notes in Networks and Systems, vol 128. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-46817-0_63

Srinivasan S, L Paine and N Goyal. 2019. Cyber breach at Target. *Harvard Business School Case Studies*

Thakur, M. 2016. Cyber Dependency at a Domestic and International Level: Literature Review. University of New South Wales Canberra, https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/pdf/Cyber-Dependency-Lit-Review-FINAL_0.pdf.

Throsby, CD and GA Withers. 1986. Strategic Bias and Demand for Public Goods. *Journal of Public Economics,* 31(3), December

Throsby, CD and GAWithers. 1997. What Price Culture? In R Towse (ed), *Cultural Economics: The Arts, the Heritage and the Media.* International Library of Critical Writings in Economics, Cheltenham, Edward Elgar

Tosun, OK, 2020, "Cyber Attacks and Stock Market Activity", manuscript, Cardiff Busines School

Transport for NSW. 2019 *Transport for NSW Cost-Benefit Analysis Guide*, Version 2.0, Sydney: NSW Government

Turnbull, B.W. 1976. The empirical distribution function with arbitrarily grouped, censored and truncated data. *The Journal of the Royal Statistical Society: Series B (Methodological)*, 38(3), 290-295

Urbanek, A. 2021, "Potential of modal shift from private cars to public transport: A survey on commuters'attitudes and willingness to switch – a case study of Silesia Province, Poland", *Research in Transportation Economics*, 85, 1-17.

Utsunomiya K. 2018. The value of local railways: An approach using the contingent valuation method. *Research in Transportation Economics.,* 69(C), 554-559

van der Hart H. 1990. Government organisations and their customers in the Netherlands: Strategy, tactics and operations. *European Journal of Marketing*, 24(7), 31-42

Varian H. 1997. Economic Aspects of Personal Privacy. In US Department of Commerce, *Privacy and the Self-Regulation in the Information Age.*, Washington DC, NTIA, chapter 1C

Vitunskaite, M, Y He, T Brandstetter and H Janicke. 2019. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, 83, pp.313-331

Wang P, H d'Cruze and D Wood. 2019. Economic costs and impacts of business data breaches. *Issues in Information Systems* 20(2). pp. 162-171

Wathieu, L and A Friedman. 2007. An Empirical Approach to Understanding Privacy Evaluation. Working Paper 07-075, Harvard Business School

Whitler, KA and PW Farris. 2017. The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research,* 57(1), pp.3-9

Withers, G. 2019. *Community Value of Public Interest Journalism, November 2019*, Melbourne: PIJI

Withers, G. 2020. *Community Value of Public Interest Journalism, April 2020*, Melbourne: PIJI

Zilberman, B. 2019. How Cyberattacks Directly Impact Your Brand: New Radware Report. [online] Radware Blog. Available at: <https://blog.radware.com/security/applicationsecurity/2019/01/how-cyberattacks-directly-impact-your-brand-new-radware-report/#:~:text=Repercussions%20can%20vary%3A%2043%25%20report,by%2054%25%20of%20survey%20respondents

APPENDIX A:

On-Line Focus Group Discussion Guide and Focus Group Valuation Questions

A.1 On-Line Focus Group Discussion Guide

About Online Overtime Focus Group Discussion Guides

An overtime online focus group schedule covers about 7-9 different topics/discussion points foreach of the three days.

It is important to break each day into themes that link. The first day we usually start more broadlywith the topic to get people used to 'talking' in the group and with each other and to give them topics they will be comfortable and knowledgeable answering – often about them!

Response setting: [STANDARD] means that participants will see comments from anyone thathas posted before them.

Response setting: [RESPONSE] means that participants will see nothing until they comment.They answer this 'blind' and cannot be influenced by other people's comments.

Response setting: [PRIVATE] means that participants will not be able to see comments from anyone else.

Response setting: [OPTIONAL] means that participants can choose to comment or to skip through.

Response setting: [SINGLE / MULTIPLE CHOICE + EXPLANATION] means that participantswill see a randomised list of options to select from, and will have to provide a comment

DAY ONE: Based on general knowledge (a) *Reputation Focus* (views on government reputation in delivery of services) (b) *Cyber Focus* (implications for citizens of cyber threats)

0.0 Welcome

Response setting: [OPTIONAL]

Hi, my name is xxxxxx and I will be moderating this group :)

Thank you for agreeing to participate and contributing your time!

To participate in this research, you need to log in for at least 30 minutes a day over the next threedays.

You can log in from wherever you are, as long as you have internet access and choose any timeconvenient to you.

For those of you who haven't done this before, here are some basic things about how an onlinediscussion group works:

- I will post a number of questions each day and you all answer them and discuss your answers amongst yourselves.
- You won't all be logged on at the same time, so we encourage you to return back to the discussion later in the day to see what others have said.
- Participating in this research is confidential and we don't use any of your personal information in the results of the research.

You can find a copy of our privacy policy here.

To start: Just click on the next topic 'Introduction' in the left-hand column.

If you run into any troubles, please email caitlin.bennetto@essentialmedia.com.au and I will assistyou.

1.1 Introduction

Response setting: [STANDARD]

To start off with, do introduce yourself to the group.You
can share as much or as little as you like.

1.2 Last year

Response setting: [STANDARD]

The Covid-19 pandemic has had big impacts on all of us. We all experienced disruptions to daily routines. There were major changes to how we accessed the internet and office systems for bothwork and recreation.

How has the pandemic impacted you over the last year – positively or negatively?

How has your community been impacted?

MODERATOR PROMPT: Has the way you use technology (for work or recreation) changed during the pandemic?

1.3 Government responsibilities

Response setting: [STANDARD]

Thinking about government generally (not just the political party in power currently or present parliament), its role is to help deliver security services (such as the police), safety (road rules), public health, education and community welfare. Each element can be provided by federal, stateand local governments in different ways.

Most people expect governments to oversee or deliver these services reliably, consistently and with appropriate safety and security. They expect them to regulate the behaviour of private companies; contract companies for providing services for the public; and raise and spend publicmoney directly themselves.

Managing emergencies and crises is also a responsibility for all three levels of government.

Is it important that governments (at all levels) prevent emergencies from occurring? Why?Is their reaction to emergencies important? Why?

What criteria would you use to judge the performance of federal, state and local governmentsduring the Covid-19 pandemic?

1.4 Government reputation 1

Response setting: [STANDARD]

If governments don't manage their responsibilities and crises well, their reputation can suffer.What criteria would you include to define a government's reputation?

What examples can you give me of a 'good reputation'?

What examples can you think of which show how a 'bad reputation' could develop?

1.5 Government reputation 2

Response setting: [STANDARD]

How would you describe the NSW government's reputation?

What events or crises would you use as examples that have influenced the NSW government's reputation?

1.6 Cyber-risks 1

Response setting: [STANDARD]

As part of the range of services that governments conduct and offer – they create, access and distribute huge amounts of information every day. This information can be about the weather, local sewerage, traffic conditions, people's personal information and much more. All of this information isstored on computers and much of it is transferred via the internet using secure systems.

Can you recall any examples of government information being accessed or distributedinappropriately or accidentally?

Regardless of your knowledge in this area, if information was made available to people outside thegovernment, or people who shouldn't have access to it – what impact do you think this could have?

How is this risk to governments different than for the risk to individuals, communities and businesses?

1.7 Cyber-risks 2

Response setting: [STANDARD]

Here are some examples of how a cyber-attack could impact users:

- Violate privacy of customers
- Reduce safety of transport users and the public including by causing accidents
- Reduce convenience including through delays, cancellations and congestion

Which (if any) of these are most concerning to you? Why?

1.8 End of day one

Response setting: [OPTIONAL]

Thanks for contributing your time and participating today!

It would be great if you could log back on for a second time today, review what other people havesaid and make comments to show when you agree with someone's viewpoint or when you have adifferent view.

Looking forward to hearing from you tomorrow.

DAY TWO: Based on a specialist inject at the start of Day 2 (a) Cyber Focus (implications for citizens of cyber threats to transport in New South Wales (b) Reputation Focus (views on government reputation for cyber security in oversight and delivery of transport services)

2.0 Welcome to day two

Response setting: [OPTIONAL]

Thanks for logging in again and welcome back to the discussion. Today we'll be talking more aboutthe possible impact and effect of cyber-attacks.

2.1 Risks to governments 1

Response setting: [MULTIPLE CHOICE + EXPLANATION]

At the end of yesterday, we asked you what sort of cyber-attack would concern you most: one causing inconvenience, one causing data breaches or one causing safety issues. Here are somereal-world examples of cyber-attacks and errors:

- Service NSW – NSW Government contacts 186,000 Australians to let them know their personal information has been compromised in a cyber-attack: https://www.service.nsw.gov.au/cyber-incident
- Toll Group Australia – Systems offline for months and corporate data stolen in two successive ransomware attacks: https://www.itnews.com.au/news/toll-group-unveils-year-long-accelerated-cyber-resilience-program-551025
- BHP – A train shuttling iron ore in the Pilbara was intentionally derailed as it was travelling without a driver. This train wasn't intended to be driverless and was intentionally derailed by train controllers. An unintended result of derailing this train, was another two trains being derailed and destroyed. This mistake cost around $200 million in losses: https://thewest.com.au/business/mining/bhp-derails-268-car-pilbara-train-which-travelled-92km-without-driver-ng-b881012020z
- National Health Service (United Kingdom) – In 2017 a global ransomware attack impacted 100 countries and 45 NSH hospitals across the United Kingdom. The attack blocked access to any files on computers which didn't have the most recent security updates, until aransom was paid. Patient records weren't compromised but surgeries were cancelled as a result of not being able to access patient details: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

Which of these situations would concern you the most? Why?Had

you heard of any of these situations before today?

Which (if any) of these situations surprised you?

2.2 Risks to governments 2

Response setting: [STANDARD]

What impact do you think a cyber-attack could have on NSW transport agencies?Would

this impact the broader community or individuals?

Please provide as much details as you can – give us examples if you can at all think of any actual cases or hypothetical ones that you can imagine.

2.3 Cyber-attacks 3

Response setting: [STANDARD]

In June 2020, the Prime Minister acknowledged that public and private organisations at all levelswere dealing with large-scale cyber-attacks from external groups. The Federal government is notresponsible for protecting NSW government agencies, all of which have their own cyber security departments or arrangements.

Do you recall hearing about this situation at the time?

What (if anything) do you think the **NSW** government could do you prevent these threats impactingthem?

Based on what you've read or heard, how effective do you believe the NSW government's cybersecurity is?

2.4 Seriousness of cyber-attacks

Response setting: [STANDARD]

If a cyber-attack occurred, are there any factors which would make it **more** serious or concerning?In

comparison, are there any factors which would make it **less** serious?

2.5 Perpetrators

Response setting: [MULTIPLE CHOICE + EXPLANATION]

There are a number of people, organisations or groups that could intentionally (or otherwise) posea risk to the NSW transport system's cybersecurity.

Which (if any) of the following possible perpetrators would be most concerning to you?Why is

that / are those groups most concerning?

Are there any other groups or people we haven't listed, you think could be a risk to cybersecurity?

- Employees of the organisation or the agency
- Individual criminals
- Traditional organised criminal groups

- Political/terrorist groups
- Foreign governments/departments
- Other person/group (please specify in your explanation)

2.6 Other sources of cyber threat

Response setting: [STANDARD]

Not all situations will be intentional cyber-attacks – it's possible that some risks will be the result ofoutdated systems, lack of training or other factors. These factors may allow an attack to occur more easily or permit someone to access information they aren't supposed to.

Are there any such situations that have you heard of, in terms of serious failures in computersystems or data, that aren't intentional cyber-attacks?

What characteristics of a security breach would make them **more** or **less** serious to you?

2.7 End of day two

Response setting: [OPTIONAL]

Thanks for contributing your time and participating today!

It would be great if you could log back on for a second time today, review what other people havesaid and make comments to show when you agree with someone's viewpoint or when you have adifferent view.

Looking forward to hearing from you tomorrow.

DAY THREE: (a) Impact Focus: what are the economic and social costs for government orfor the community if a government agency has a bad reputation for cyber security. b) Value Focus (how a dollar valuation of reputation impact of cyber security investments for government transport activities can be obtained)

3.0 Welcome to day three

Response setting: [OPTIONAL]

Thanks for logging in again and welcome back to the discussion. Today we'll be talking more aboutcyber-attacks and what happens after a successful breach.

3.1 NSW public agency cybersecurity

Response setting: [STANDARD]

If a private company like Yahoo can be hacked in a way that exposed the personal information of 500 million customers, the loss of reputation could sees many consumers refuse to purchase fromthem again.

If you felt the NSW government's reputation was negatively impacted by a cyber-attack, would thisimpact how you use transport services?

How would your answer change if the cyber-attacks occurred over a number of years? Would the

types of people or organisations involved in the attack change your answer?

And would the speed and form of a government response to the attack also alter your answer? Inwhat ways?

MODERATOR PROMPT: Criminal, terrorist, foreign government, disgruntled employee.

3.2 Next steps

Response setting: [RESPONSE]

If there was a cyber-attack or cybersecurity breach at any of the public transport agency, wherewould you expect to see or hear information relating to it?

If you were impacted by the breach, how closely would you follow the story in the media?How would

you expect the agency to respond and why?

How would you keep up to date with developments in this situation?

3.3 Informing their customers

Response setting: [STANDARD]

When and how would you expect a public transport agency experiencing a cyber-attack to informtheir customers?

What (if any) factors make it **more** important for a transport organisation to inform their customersabout a security breach?

3.4 Cognitive test

Response setting: [STANDARD]

The question for this topic is hosted on another platform and should take 10 minutes to complete –please follow this link to complete the topic. These questions are examples of how some population survey questions could be set up on this topic.

When instructed please return to this page and respond below with “DONE” to continue.

3.5 Final Thoughts

Response setting: [OPTIONAL]

Thanks for contributing your time and participating over the last three days. This research hasconducted for Transport for NSW and the University of New South Wales.

Just before we finish up, do you have any other thoughts around this research?

A.2 Focus Group Valuation Questions: Linked Survey

Intro Thanks for clicking on the survey link. Please provide your email address below so we can verify everyone has completed this section.

○ Email: (1) ____

Q30 Your answers to these questions will assist with academic research into transport in NSW and advise government based on that research.

For the following three categories of damage, please indicate the reputation loss that would follow from these three types of cyber-attack on government transport activities in NSW.

	Loss of convenience (e.g. trains don't run for a few days) (1)	Loss of trust over privacy (e.g. personal banking data is accessed) (9)	Major safety incident (e.g. severe accident with 50-200 deaths) (11)
Not much reputation loss (little community concern, news dies off quickly, low cost of remediation ($100,000)) (1)	○	○	○
Moderate reputation loss (some citizens complaining, news headlines continue for a week or two, moderate cost of remediation ($1 million)) (8)	○	○	○
Quite serious reputation loss (headlines continue for months, remediation costs start to reach tens of millions of dollars) (9)	○	○	○
Severe reputation loss (calls for a Royal Commission, government Minister resigns, remediation costs or compensation costs approach $100 million) (10)	○	○	○

Q1B Looking at the question above, was the scale of reputation loss easy to understand?
Did the values sound right for the topic?
Do you have any further feedback about this question?

____

____

____

____

____

Q1A

How frequently do you currently use the following forms of transport?

	Five or more times per week (1)	One to four times per week (2)	Once a fortnight (3)	A few times a month (4)	Once a month (5)	Once every few months (6)	Less often than once every few months (7)	I don't use this form of transport (8)
Train (1)	○	○	○	○	○	○	○	○
Private car (2)	○	○	○	○	○	○	○	○
Taxi or Rideshare (3)	○	○	○	○	○	○	○	○
Ferry (4)	○	○	○	○	○	○	○	○
Tram or Light-rail (5)	○	○	○	○	○	○	○	○
Bus (6)	○	○	○	○	○	○	○	○
Bicycle, Motorcycle or Other small vehicle (7)	○	○	○	○	○	○	○	○

Q31 Looking at the question above, did we miss any forms of transport you use?
Was the range of frequency useful for you?
Do you have any further feedback about this question?

____

____

____

____

____

Q2A How often do you rely upon each of the following information sources to learn about any transport issues or operations in NSW?

	Always (1)	Most of the time (2)	Rarely (3)	Never (4)
Discussion with friends and family – in-person or telephone (1)	○	○	○	○
Newspapers and Magazines- hard copy or online (15)	○	○	○	○
Commercial Television (16)	○	○	○	○
Public Television (17)	○	○	○	○
Social Media such as Twitter, Facebook (18)	○	○	○	○
Websites specifically for that form of transport (e.g. Sydney Trains) (7)	○	○	○	○
A government website (6)	○	○	○	○

Q2B Did we miss any other sources of information you would use? How comfortable did you feel using the frequency scale in this question? Do you have any further feedback about this question?

____

____

____

____

____

Q3A How would you rate the NSW government's performance in managing public transport?

○ Very good (1)

○ Fairly good (15)

○ Neutral (19)

○ Fairly poor (16)

○ Very poor (17)

Q3B Do you have any feedback about this question?

____

____

____

____

____

Q4 Before today, had you heard of an agency called 'Transport for New South Wales'?

○ Yes (1)

○ No (15)

Q5A Transport for New South Wales (TfNSW) is now responsible for managing transport systems across NSW (including ride-share and private vehicles). They work with Sydney Trains, NSW Trains, State Transit, Sydney Metro, as well as private companies, to improve transport for everyone.

One emerging role of TfNSW is to assist all transport, but especially public transport, deal with any cyber-attacks on the operation of the transport system. To what extent are you concerned or not concerned that any of the following issues could impact you?

	Very concerned (9)	Somewhat concerned (11)	Neither concerned nor unconcerned (12)	Somewhat unconcerned (13)	Very concerned (14)
Violate privacy of customers (1)	○	○	○	○	○
Reduce safety of transport users and the public including by causing accidents (23)	○	○	○	○	○
Reduce convenience including through delays, cancellations and congestion (24)	○	○	○	○	○

Q5B Are the examples listed above clear any easy to understand?
Are there other issues which could impact you?
Do you have any further feedback about this question?

____

____

____

____

____

Q6A Please rank the following from 1 (most responsible) to 5 (least responsible) if a successful cyber-attack occurred?

______ The NSW Premier (1)
______ The Minister for Transport (28)
______ A TfNSW Official (29)
______ Other NSW Government Officers (30)
______ Transport Operators (31)

Q6B Did we miss any other people you think should be held responsible for a successful cyber-attack?

Do you have any further feedback about this question?

____

____

____

____

____

Q7A To what extent would the following actions increase the reputation of the NSW government, after a successful cyber-attack that affected people's safety or privacy

	Very much (9)	Somewhat (11)	A little (12)	Not at all (13)	Unsure (15)
A formal Government apology (1)	○	○	○	○	○
Speedy restoration of normal service (28)	○	○	○	○	○
Evidence of improved cybersecurity (29)	○	○	○	○	○
Monetary compensation (30)	○	○	○	○	○
A Government inquiry (27)	○	○	○	○	○

Q7B Are we missing any other actions the Government could take?
Was the scale appropriate for how you wanted to answer the question?
Do you have any further feedback about this question?

____

____

____

____

____

Q8A To what extent would the following features make you feel more or less concerned about a cyber-attack on public transport that affected the public's safety and privacy?

	Very much (11)	Somewhat (16)	A litte (15)	Not at all (13)	Unsure (12)
The impact was felt for a long time (1)	○	○	○	○	○
The impact was felt for a short time (30)	○	○	○	○	○
The impact was on a large scale (25)	○	○	○	○	○
The impact was on a small scale (31)	○	○	○	○	○
An internal error caused the situation (26)	○	○	○	○	○
An external attack caused the situation (24)	○	○	○	○	○
A government agency was targeted (27)	○	○	○	○	○
A private company was targeted (29)	○	○	○	○	○

Q8B Do you have any feedback about this question?

____

____

____

____

____

Q9A There are a number of policies, procedures and resources that a NSW public transport agency could implement in order to strengthen their cybersecurity against attacks and breaches. If new new actions and policies could reduce the likelihood of cybersecurity threats by **half**, to what extent would you support or oppose paying **$30 per year** in increased taxes to the state government for increased cybersecurity?

○ Definitely would support (4)

○ Probably would support (21)

○ Probably would not support (22)

○ Definitely would not support (23)

○ Unsure (24)

Q10 And to what extent would you support or oppose paying more for increased cybersecurity, if the amount of tax you would have to pay was **$40 per year?**

○ Definitely would support (4)

○ Probably would support (21)

○ Probably would not support (22)

○ Definitely would not support (23)

○ Unsure (24)

Q9B The initial question we asked was, *"There are a number of policies, procedures and resources that a NSW public transport agency could implement in order to strengthen their cybersecurity against attacks and breaches. If these new new actions and policies could reduce the likelihood of cybersecurity threats by **half**, to what extent would you support or oppose paying **$30 per year** in increased taxes to the state government for increased cybersecurity?"*

To what extent do you agree or disagree with the following statements about this question?

	Strongly agree (11)	Somewhat agree (12)	Neither agree nor disagree (13)	Somewhat disagree (14)	Strongly disagree (15)
The language used was clear and easy to understand (1)	○	○	○	○	○
The answers provided accurately reflected my view (2)	○	○	○	○	○
It was straightforward to understand the yearly tax increase (3)	○	○	○	○	○

Q9C How confident did you feel when answering that question?

○ Very confident (6)

○ Somewhat confident (7)

○ Neither confident nor unconfident (8)

○ Somewhat confident (9)

○ Very unconfident (10)

Q10 What did you think it means to *"...strengthen their cybersecurity against attacks and breaches."*?

____

____

____

____

____

Q11 What would you expect the funds raised by the proposed tax increase should be spent on?

____

____

____

Q32 What is the **MAXIMUM** amount you would be willing to pay in annual taxes for **halving** the risks of cybersecurity attacks and damages for transport provision in NSW?

○ $0 (6)

○ $5 (7)

○ $10 (8)

○ $20 (9)

○ $30 (10)

○ $40 (13)

○ $50 (14)

○ More than $50 (15)

Q33 What is the **MAXIMUM** amount you would be willing to pay in annual taxes for reducing the risks and damages of cybersecurity attacks by **10%**?

○ $0 (6)

○ $5 (7)

○ $10 (8)

○ $20 (9)

○ $30 (10)

○ $40 (13)

○ $50 (14)

○ More than $50 (15)

APPENDIX B:

Sample Transport and Cybersecurity On-Line Population Survey Questionnaire

Quotas

Gender/Age/ Location	Male			Female			TOTAL
	18-34	35-54	55+	18-34	35-54	55+	
Sydney	74	79	67	75	81	77	**453**
Regional NSW	30	38	120	105	121	134	**548**
TOTAL	**104**	**117**	**187**	**180**	**202**	**211**	**1000**

Monthly X Values	Percentages		TOTAL
	10%	50%	
$24	125	125	**250**
$60	125	125	**250**
$120	125	125	**250**
$240	125	125	**250**
TOTAL	**500**	**500**	**1000**

Screener

D1. What is your age?

SINGLE RESPONSE

1. Under 18 **[TERMINATE]**
2. 18-19
3. 20-24
4. 25-29
5. 30-34
6. 35-39
7. 40-44

8. 45-49
9. 50-54
10. 55-59
11. 60-64
12. 65-69
13. 70-74
14. 75 and over
15. Prefer not to say **[TERMINATE]**

D2. How do you identify?

SINGLE RESPONSE

1. Man
2. Woman
3. Other (please specify)
4. Prefer not to say

D3. What is your residential postcode?

4-DIGIT OPEN-BOX.

PROGRAMMER NOTE: HIDDEN QUESTION, AUTOCODE BASED ON POSTCODE.

D4. Location

SINGLE RESPONSE.

1. Sydney
2. NSW other than Sydney
3. Outside of NSW **[TERMINATE]**

Engagement with Transport

Q1. How frequently do you **currently** use the following forms of transport?

a. At least once a week
b. At least once a fortnight
c. At least once a month
d. Every few months
e. Almost never
f. **I don't use this form of transport**

SINGLE RESPONSE PER ROW. RANDOMISE STATEMENTS.

1. Train
2. Private car
3. Taxi or Rideshare

4. Ferry
5. Tram or light-rail
6. Bus
7. Bicycle, motorcycle or other small vehicle

Q2. Prior to the Covid-19 pandemic, did you use these forms of transport more, less or at the same level of frequency?

a. **More frequently prior to the pandemic**
b. **Same frequency prior to the pandemic**
c. **Less frequently prior to the pandemic**
d. **Unsure**
e. **I didn’t use this form of transport prior to the pandemic**

SINGLE RESPONSE PER ROW. RANDOMISE STATEMENTS.

1. Train
2. Private car
3. Taxi or Rideshare
4. Ferry
5. Tram or light-rail
6. Bus
7. Bicycle, motorcycle or other small vehicle

Q3. Which of the following sources do you use to obtain the transport information you want in NSW?

MULTIPLE RESPONSE. RANDOMISE EXCEPT ‘NONE OF THESE’ WHICH IS ALSO EXCLUSIVE.

1. Discussion with friends and family
2. Newspapers and Magazines – hard copy or online
3. Commercial Television or Radio i.e. Channel 7 etc.
4. Public Television or Radio i.e. ABC, SBS etc
5. Social Media such as Twitter, Facebook
6. Websites specifically for that form of transport (e.g. Transport.Info)
7. Real time transport apps e.g. Google Maps, AnyTrip or Citymapper
8. None of these

Q4. Before today, had you heard of an agency called 'Transport for New South Wales', also called TfNSW?

SINGLE RESPONSE.

1. Yes
2. No

TfNSW performance

Q5. Transport for New South Wales (TfNSW) is responsible for managing transport systems across NSW (including ride-share and private vehicles regulation). They work with Sydney Trains, NSW Trains, State Transit, Sydney Metro, as well as private companies, to improve transport operations for everyone.

How would you personally rate the overall performance of Transport for NSW (TfNSW) based on the interactions you've had with the organisation and anything else you have seen, heard or read about it?

SINGLE RESPONSE.

1. Very good
2. Fairly good
3. Neutral
4. Fairly poor
5. Very poor

Q6. One emerging role of TfNSW is to assist all transport, but especially public transport, deal with any cyber-attacks on the transport system. How would you personally rate the overall performance of Transport for NSW (TfNSW) for cybersecurity based on anything that you have seen, heard or read about in the past 12 months?

SINGLE RESPONSE.

6. Very good
7. Fairly good
8. Neutral
9. Fairly poor
10. Very poor

Public Attitudes

Q7. TfNSW responsibilities include managing transport emergencies .. While such emergencies can't be prevented entirely, governments should do as much as possible to minimise the risk of them occurring and take appropriate action to overcome their possible impacts.

Below are some examples of potential transport responses by government to an emergency or incident. In your opinion, how would you feel if TfNSW decided that it needed to take the following action to overcome the effects of a public emergency?

For each of the actions, please select one of the following to indicate your likely attitude toward the emergency or incident that generated the action by government?

1. **Not concerned/do not have a view**
2. **A little concerned**
3. **Moderately concerned**
4. **Concerned**
5. **Very concerned**

SINGLE RESPONSE PER ROW. RANDOMISE STATEMENTS.

1. Government pays up to $1 million compensation to those affected by the transport emergency or incident
2. Government pays more than $100 million compensation to those affected by the transport emergency or incident
3. Fewer than 1,000 people are inconvenienced for up to one week by the transport emergency or incident
4. More than 100,000 people are inconvenienced for up to one week by the transport emergency or incident
5. Fewer than 10 people are injured due to the transport emergency or incident
6. More than 100 people are injured due to the transport emergency or incident

Q8. Which of the following possible perpetrators of a cyber-attack would most concern you?

Please rank all the options below by dragging and dropping them in order of highest concern (1) to lowest concern (5).

PROGRAMMER NOTE: INCLUDE CYBER ATTACK DEFINITION FROM Q7 AS A POP-UP FOR THIS QUESTION. RANK ALL (DRAG & DROP). RANDOMISE ALL

1. Government employees
2. Individual hackers
3. An organised criminal group
4. Political/terrorist groups
5. Foreign governments

Q9. To what extent would the following further actions restore trust in the performance of TfNSW, if a successful cyber-attack had occurred and resulted in some accidents, severe traffic congestion, and more crowding on bus and trains?

PROGRAMMER NOTE: INCLUDE CYBER ATTACK DEFINITION FROM Q7 AS A POP-UP FOR THIS QUESTION.

a. **Very much**
b. **Somewhat**
c. **A little**
d. **Not at all**
e. **Unsure**

SINGLE RESPONSE PER ROW. RANDOMISE STATEMENTS.

1. A formal Government apology
2. Speedy restoration of normal service
3. Immediate briefing and regular updates
4. A state parliamentary enquiry
5. Evidence of improved cybersecurity
6. Financial compensation for victims of the attack

7. Government pays up to $1 million compensation to those affected by the transport emergency or incident
8. Government pays more than $100 million compensation to those affected by the transport emergency or incident
9. Fewer than 1,000 people are inconvenienced for up to one week by the transport emergency or incident
10. More than 100,000 people are inconvenienced for up to one week by the transport emergency or incident
11. Fewer than 10 people are injured due to the transport emergency or incident
12. More than 100 people are injured due to the transport emergency or incident

Q8. Which of the following possible perpetrators of a cyber-attack would most concern you?

Please rank all the options below by dragging and dropping them in order of highest concern (1) to lowest concern (5).

PROGRAMMER NOTE: INCLUDE CYBER ATTACK DEFINITION FROM Q7 AS A POP-UP FOR THIS QUESTION. RANK ALL (DRAG & DROP). RANDOMISE ALL

6. Government employees
7. Individual hackers
8. An organised criminal group
9. Political/terrorist groups
10. Foreign governments

Q9. To what extent would the following further actions restore trust in the performance of TfNSW, if a successful cyber-attack had occurred and resulted in some accidents, severe traffic congestion, and more crowding on bus and trains?

PROGRAMMER NOTE: INCLUDE CYBER ATTACK DEFINITION FROM Q7 AS A POP-UP FOR THIS QUESTION.

a. **Very much**
b. **Somewhat**
c. **A little**
d. **Not at all**
e. **Unsure**

SINGLE RESPONSE PER ROW. RANDOMISE STATEMENTS.

7. A formal Government apology
8. Speedy restoration of normal service
9. Immediate briefing and regular updates
10. A state parliamentary enquiry
11. Evidence of improved cybersecurity
12. Financial compensation for victims of the attack

Willingness to pay

PROGRAMMER NOTE: HIDDEN QUESTION. ALLOCATE BASED ON LEAST FILLED QUOTA. USE THIS VALUE FOR Q10 TO Q13 BELOW.

Option	Percentage
1	10%
2	50%

Q.10 There are a number of policies, procedures and activities that TfNSW could pursue to enhance its ability to protect against cyber-attacks and cyber breaches in the public and private transport systems.

If new actions and policies could reduce the likelihood of these types of threats by **<PERCENTAGE>**, and these were funded through extra taxes for this, to what extent would you support or oppose paying **<$X1> per year (or <$X1> per month)** in increased taxes?

RANDOMLY SELECT $X FROM OPTIONS 2-4:

Option	X Monthly Value	X Annual Value
1	$0	$0
2	$2	$24
3	$5	$60
4	$10	$120
5	$20	$240
6	$30	$360

SINGLE RESPONSE.

1. Definitely would support
2. Probably would support
3. Probably would not support
4. Definitely would not support
5. Unsure

Q11 And, again recalling these actions that could be pursued by TfNSW to enhance protection against cyberattacks and cyber breaches, to what extent would you be willing to pay more for this same **<PERCENTAGE>** improvement in the TfNSW's cybersecurity – if that increased the amount of tax you pay by **<$Y1> per year (or <$Y1> per month)**?

IF Q10=1, SET $Y1 TO Q5 OPTION + 1
IF Q10=2 TO 5, SET $Y1 TO Q5 OPTION – 1

Option	Y Monthly Value	Y Annual Value
1	$0	$0
2	$2	$24
3	$5	$60
4	$10	$120
5	$20	$240
6	$30	$360

1. Definitely would pay more
2. Probably would pay more
3. Probably would not pay more
4. Definitely would not pay more
5. Unsure

Q12 What is the **MAXIMUM** amount you would be willing to pay in **taxes** for a **<PERCENTAGE>** improvement in the reputation of TfNSW for dealing well with the cybersecurity risks to NSW transport ?

PROGRAMMER NOTE: DO NOT DISPLAY RESPONSE OPTIONS LOWER THAN $Y VALUE (E.G. IS Y=4 [$120] DO NOT DISPLAY CODES 1 TO 3)

1. $0
2. $24 annually / $2 monthly
3. $60 annually / $5 monthly
4. $120 annually / $10 monthly
5. $240 annually / $20 monthly
6. $360 annually / $30 monthly
7. $600 annually / $50 monthly

Q13 Previously, you said you [DTS IF Q10=1 “definitely would” / Q10=2 “probably would” / Q10=3 “probably would not” / Q10=4 “definitely would” / Q10=5 “are unsure if you would”] pay a **<$X1> per year (or <$X1> per month)** increase in taxes, to improve TfNSW’s performance (trust in TfNSW) for ensuring cyber security by **<PERCENTAGE>**.

Rather than increasing taxes, would you be willing to pay more in transport fares and charges to improve cyber security by **<PERCENTAGE>**?

1. Definitely would pay more
2. Probably would pay more
3. Probably would not pay more
4. Definitely would not pay more
5. Unsure/Not applicable

Q14. If you had to pay more in taxes to ensure that TfNSW had better cybersecurity to properly support and protect transport in the state, rank in order of priority how important these three factors below would be to you

Please rank these options from 1 to 3, with 1 being your highest priority

RANK ORDER NUMERIC RESPONSE. RANDOMISE OPTIONS

1. Transport safety for customers and employees
2. Improved convenience for customers (e.g. reliability of services, comfort etc)
3. Enhanced privacy for customers and employees

Q15. Are there any other factors you would consider important to ensure that TfNSW could have improved performance (increase the trust you have in TfNSW) from delivering enhanced cyber security for transport in the state?

Feel free to write them in here or press the arrow (-> icon) below to continue.

OPTIONAL. OPEN-END RESPONSE

Demographics

Thank you for your time so far, we only have a few more questions.

D5. Have you ever experienced a situation where your personal or financial details were accessed or released as part of any cyber-attack or breach?

SINGLE RESPONSE.

1. Yes, in the last 6 months
2. Yes, in the last 7-12 months
3. Yes, in the last 1-5 years
4. Yes, more than 5 years ago
5. No, never
6. Prefer not to say

D6. What is the total of all wages/salaries, government benefits, pensions, allowances, and other income that your household usually receives (GROSS – before tax and superannuation deductions)?

SINGLE RESPONSE

1. $3,500 or more per week ($182,000 or more per year)

2. $3,000-$3,499 per week ($156,000-$181,999 per year)

3. $2,500-$2,999 per week ($130,000-$155,999 per year)

4. $2,000-$2,499 per week ($104,000-$129,999 per year)

5. $1,500-$1,999 per week ($78,000-$103,999 per year)

6. $1,250-$1,499 per week ($65,000-$77,999 per year)

7. $1,000-$1,249 per week ($52,000-$64,999 per year)

8. $800-$999 per week ($41,600-$51,999 per year)

9. $600-$799 per week ($31,200-$41,599 per year)

10. $400-$599 per week ($20,800-$31,199 per year)

11. $300-$399 per week ($15,600-$20,799 per year)

12. $200-$299 per week ($10,400-$15,599 per year)

13. $1-$199 per week ($1-$10,399 per year)

14. No income

15. Negative income

16. Prefer not to say

D7. What is the highest level of education you have attained?

SINGLE RESPONSE

1. Year 9 and below
2. Year 10 and above
3. Certificate levels I-IV
4. Diploma or advanced diploma
5. Graduate diploma or certificate
6. Bachelor or honours degree
7. Post-graduate degree
8. Other (please specify)
9. Prefer not to say