SOCIAL CYBER INSTITUTE

Research Paper 1/23

VALUATION OF REPUTATION DAMAGE FOR TRANSPORT CYBER ATTACK:

METHODS AND FINDINGS

Greg Austin and Glenn Withers

JANUARY 2023

SOCIAL CYBER INSTITUTE

Research Paper #1/23

Valuation of Reputation Damage for Transport Cyber Attack:

Methods and Findings

Greg Austin and Glenn Withers

January 2023

Acknowledgements

The authors would like to acknowledge comments from Dr Peter Abelson of Applied Economics, Caitlin Bennetto of Essential Media, and Dr Virginie Vernin, David Wright and colleagues at Transport NSW, but the paper remains the responsibility of the authors. The analysis was funded by Transport NSW through a contract with UNSW and was subject to Ethics Committee approvals at UNSW. Original focus group data used are obtainable from the authors or from Transport New South Wales.

ABOUT THE SOCIAL CYBER INSTITUTE

Social science research on our emerging cyber world is not keeping pace with the 'gifted technologists' and 'talented tinkerers'. Knowledge transfer from world-class social science researchers to leaders of business and government is slow, haphazard, and undisciplined. The Social Cyber Institute (SCI) creates new modes of thinking specific to individual corporations and non-profits, government agencies and their operating ecosystem. We help you understand the social DNA of your InfoTech and rewire it for the future. SCI is the public research and public analytic arm of the Social Cyber Group.

ABOUT THE AUTHORS

Greg Austin is a co-founder of the Social Cyber Group. He has diverse international experience as Programme Head for Cyber Power and Future Conflict at the International Institute of Strategic Studies; as a Professor of Cyber Security, Strategy and Diplomacy with the University of New South Wales Canberra; and as Vice President with the EastWest Institute in its Brussels office. His academic career, including a Senior Visiting Fellowship in the Department of War Studies at Kings College London, has included eight books on international security, as author or editor, and leadership of several international research projects. His service as a research leader for prominent global NGOs, such as the International Crisis Group and the EastWest Institute, has seen him work from Brussels and London with leading governments at Ministerial level (Russia, China, UK, India, United States, Turkey, Australia), major international organisations at leadership level (United Nations, International Atomic Energy Agency, R20 for Climate Action), and leading corporations (AT&T, BT, Perot Systems). He has consulted for the UK Cabinet Office, the UK Ministry of Defence, the Foreign and Commonwealth Office, the European Commission, and the Australian Department of Foreign Affairs and Trade. He began his career in Australian public service roles, including posts in Canberra and Hong Kong in defence intelligence, parliamentary committees, and ministerial staff. Austin has a Ph D in International Relations and a Master of International Law, both from the Australian National University.

Glenn Withers AO is a Distinguished Honorary Professor at the Australian National University and Visiting Professor at the University of New South Wales Canberra. His Harvard PHD was on conscription. He has held appointments at Harvard University and Cambridge University, and has consulted widely for governments and companies from the OECD and the Australian Broadcasting Corporation to the US Defense Department and the Prime Minister of Malaysia. In Australia, he has been Chair of the National Population Council and Commissioner of the Economic Planning Advisory Commission, and helped to establish the Bureau of Labour Market Research, Bureau of Immigration Research, Productivity Commission, Crawford School of Government , Universities Australia and the Social Cyber Group. He was awarded honours by the Australian government for developing the Australian Immigration Points System. He is immediate past President of the Academy of the Social Sciences in Australia and of the Australian Council of Learned Academies. Currently, he is Chair of the Global Board of the Global Development Learning Network, a World Bank affiliate that operates in 60 countries. He has a wide range of publications in books, academic journals, government reports and consultancy reports, particularly focusing on education, immigration, infrastructure and technology issues.

ABSTRACT

This paper analyses the issue of reputation damage for transport cyber-attacks. Cyber-security attack has become an increasing focus for much business and government planning. Transport infrastructure networks are of special concern. A challenge in responding is to determine the level and allocation of cyber-security budgets. Extensive public sector involvement means that market measures of net benefit may be insufficient for government decision-makers. For example, government reputation effects will also be regarded as important, and so this paper uses focus group methods to demonstrate how project evaluation can incorporate public reputation damage measures.

So called "contingent valuation" methodology is applied for this purpose in the paper, generating illustrative "willingness to pay" estimates for public reputation. The measures are obtained for the case of transport cyber-attack in the Australian state of New South Wales. 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 in this way, but complementary or alternative ways forward on reputation loss matters for transport are also discussed, including discrete choice analysis and stock valuation.

Contents

Introduction

Cyber matters are clearly important for modern transport operations. Managers continually analyse key cyber security risks and seek 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, where government is involved, reputational damage for government itself as a result of a cyber-attack is crucial for official decision-makers and is challenging to measure due to its relatively intangible nature.

The objective of the research reported here, 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 transport authorities and the Government more broadly, beyond market measures such as costs of prevention and remediation and beyond stock market impacts for listed companies. The focus is to assist in developing a more robust justification for including such wider cyber-security related measures in Cost-Benefit Analysis so that improved quantitative guidance on cyber security investment can still be provided. The measures proposed will be based upon contingent valuation methodology, using willingness to pay stated preference techniques.

The scope and scale of activity embraced here, in principle covers all government-linked transport-related activities where issues of cyber-security arise. It potentially extends even to new automated and computer-linked transport, including drones and driverless vehicles, which will create further potentially large-scale cyber vulnerabilities also affecting public safety, public convenience (systems running as scheduled), and stakeholder trust. However, the application chosen focuses on land and ferry transport that involves major government regulation or provision and is conducted for the state of New South Wales in Australia.

Literature Review on Cyber Attacks and Reputational Harm

It is noted first that the relevant 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 nevertheless 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.

This literature review 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.

Cyber and Transport

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 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, Alharbi et al 2020,

Cimpanu 2020). As complexity grows, it will become harder for key decision makers to analyse potential risks and for their technical specialists to prevent, let alone even identify cyber-attacks. But investment decisions must still be made.

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".

Unfortunately, inadequate attention has been paid to such transportation cyber risk and resilience (Zhou et al 2020). The environment often produces advice that isn't based on clear evidence but, rather, may owe more to organisational developments. Lehto, above, indicated that organisational segmentation is a major problem. 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, but these are the basics only.

Resilience analyses of the transportation infrastructure have the benefit of further improving physical operability, system safety, optimising management and investment, with positive socioeconomic impacts eg US Department of Homeland Security 2008. 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).

Austin and Withers (2019) have argued for an even more 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. It is the interaction with technology and engineering and management in the shared ecosystem that then determines all security and welfare outcomes dependent on cyberspace.

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), but the struggle to keep pace with escalating threats requires ongoing and enhanced attention (ASSC 2020).

Reputational Harm from Cyber Attack

A comprehensive approach to reputational harm for cyber attack itself has been advocated by Agrafiotis et al (2016). The emphasis there is that reputation loss is best understood as harm "pertaining to the general opinion held about an entity". To justify such a comprehensive approach, Gao et al (2020: 3) following Wang et al (2018) cite the calculation that the direct cost of remediating a cyber security breach can be as low as ten per cent of the total hidden costs.

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 levels of reputation harm as does the World Economic Forum (2015) in its notion of cyber-Value-at-Risk (VaR). A number of additional research findings can further 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. Data breaches can cause an organisation to lose "consumer trust and public confidence" that "may translate into financial or monetary loss" (Krishan 2018).

Early work in Whittaker and Farris (2017), Kostyuk and Wayne (2019), Skinner (2019), Vitunskaiet et al (2019) and Evans (2020) also did provide analysis of the nature and meaning of reputation for public organisations drawing on the 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. These analyses look at estimating direct market costs and revenue or seek summative evaluation though corporation purchase or stock market valuations.

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, but public reputation analyses for government transport responsibilities remain to be provided.

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 in other domains or even to benefits in the environmental sphere from transport investment, but for reputation as a whole.

The relevant general literature for this, 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 'contingent valuation' approaches and especially 'stated preference' such as 'willingness to pay' survey models therein. This approach can distinctively provide household, voter or general public valuations of non-market impacts, especially so that these can be incorporated into cost-benefit analysis (CBA) in a manner complementary to any market-based measures. Such CBA, augmented by non-market valuation, has therefore become termed 'social cost-benefit analysis' (SCBA).

Stated Preference Valuation

For purely private firms, reputational impact of a cyber-attack can be quantified for market listed firms by examining the effects on their stock market prices. The distinctive differentiating 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 includes 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.

As flagged above, one generic approach to valuation is so-called 'contingent valuation' through 'revealed preference' estimations of the dollar valuation of some public good style projects. 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, revealed preference operating instead via "stated preference" survey methods where relevant parties are asked for their willingness to pay for the good or service or facility, including through government. A variant is "willingness to accept" (rather than pay) where a payment to the respondent is considered appropriate for a negative action.

Other forms of contingent valuation 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 through willingness to pay (Carson 2011).

Although this approach may involve hypothetical questions, it has the advantage of considering projects before or after implementation, and of embracing as much of the wider community as desired e.g. all voters, even when they are not transport users. The 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.

Accordingly, this paper reports on a focus group conducted to ascertain willingness to pay and to allow quantification of the non-market valuation of reputation. With modern computing, survey respondents can 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.

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

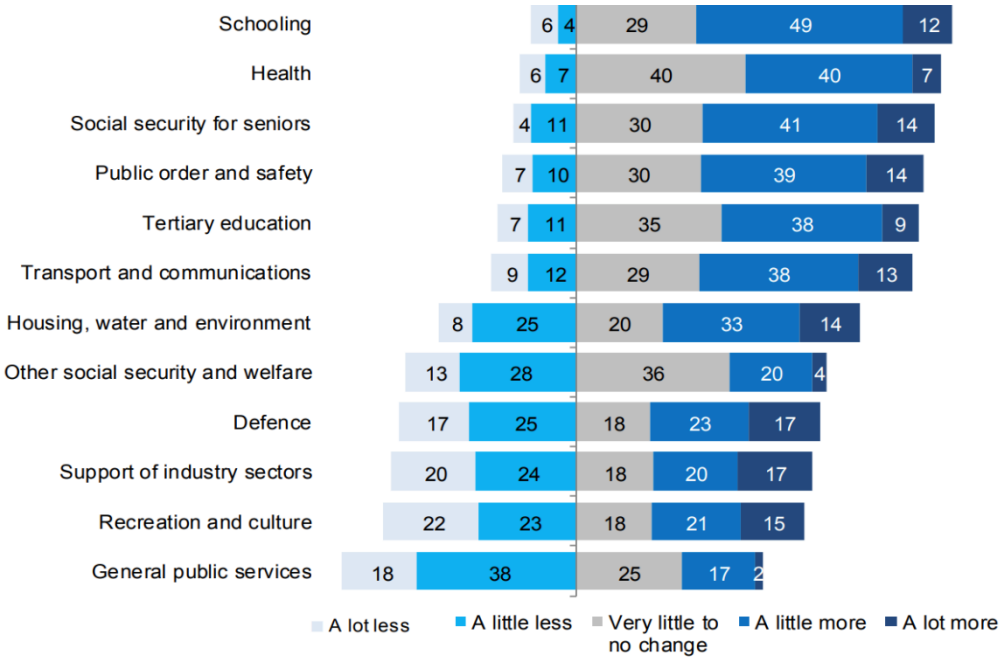
the Exxon Valdez investigation. A recent volume drawing on European as well as North American practice looks at the methods now in place to research such valuations using the latest methods and findings (Florio 2019).

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 paper, the issues of cyber security and reputation value in public transport. No extant studies have been identified that provide such information at this time.

There are however some broader evaluations across all areas of public activity, which include total transport outlays by government. One of the most recent for Australia is Centre for Policy Development (2017). This study, for instance, summarised the willingness to pay for different aspects of government for Australia overall as given in Figure 1 below.

Transport and communications received 51% support in this CPD 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 1: 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 in transport.

A Focus Group Analysis

The literature review insights above produced a clear set of issues to be directly considered in defining the way forward for appropriately eliciting valuation of reputation loss for transport from cyber attack using field work. The analysis and consultation undertaken indicated that the following variables need to be understood, and reflected in focus group analysis for valuation:

- 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

- Public understanding of the nature of the government's 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 such new research using field data gathering - both qualitative and quantitative via focus group analysis. The use of a focus group approach was seen as advisable because of the complexities of risk analysis and cyber security and of the transport system. Testing of questions, words, concepts, information, contexts etc to be would not only be productive, but essential for a truly meaningful product regarding actual valuation of potential cyber-attack damage to reputation in transport. Focus groups can 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.

The data for this was collected from a focus group of twenty selected as a stratified random sample for the NSW population as to region, gender and education, with no individual identification, and with data on personal characteristics being those already collected for their involvement in a standard omnibus survey without addition for specific project applications.

A distinctive feature of the focus group was the inclusion of both users and non-users in relation to the transport services. The analysis constructed in this way 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 use the focus group approach to affirm the capacity to understand such concepts accurately, and intelligibly deduce a preliminary estimate of monetary valuation for public

transport investment of the problems of cyber-attack. This can then demonstrate how to 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.

Focus Group Results

Focus Group analysis was pursued for the project to demonstrate the viability of 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, given Covid limitations, an on-line and representative sample for the State of New South Wales (NSW) in Australia, 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 an Appendix to this article.

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 A.1 to this paper.

After the extensive discussion of cyber and transport issues in qualitative terms, as seen in Appendix A.1, 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 then nominated for the respondents' consideration, in a "closed ended" or "dichotomous choice" format, common in stated preference analysis, seen in Appendix A.2.

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 prior qualitative 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 was a move to an "open-ended" format in stated preference contingent valuation. A maximum was sought under this open-ended approach for two resultant cyber 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 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:

- felt that the overall State 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; and
- 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 the portfolio co-ordinating agency.

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. In Australia, subsequent major national cyberattacks involving Medibank Private and Optus companies may have increased focus on such issues since the focus group conduct.

These observations illustrate the knowledge needed to result in the metrics required for cost-benefit analysis, but are also 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), both used by the agency;
- opinion metrics such as Unisys Trust and Newgate Research Reputation Study, cpmmissioned by the agency; and
- case insights for understanding such as the 2020 State Transit Authority (STA) ransomware incident or the Services NSW Breach (Parliamentary Inquiry) and others.

That said, the quantitative willingness to pay valuation results found from the Focus Group deliberation for this research, are as given in Table 1.

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 existing support within this Focus Group for the government's performance in managing public transport in NSW.

By this preliminary estimate, the average willingness to pay for a 50% improvement in Transport cyber-security was $17 per person per annum. This represented an increased cyber budget for TfNSW of around $115 million ($A2021) over the actual allocation.

Table 1. 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.

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.

Ways Forward

The quantitative finding 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.

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 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.

If it were desired to properly validate or affirm the order of magnitude of the results obtained here from this Focus Group analysis, a full representative sample NSW population survey should be undertaken to 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 stated preference 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 government project evaluation, have developed survey instruments that understand such concerns.

Alternatively, benchmarks can be estimated from wider exercises, eg across all 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 still sued but 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 partners. 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 active 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 state agency 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 agency 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.

Conclusion

To conclude, this study outlines an accessible framework through focus group/ survey methods for help in managing cybersecurity issues in public-linked organisations, even where those issues are technically specialised and complex. The idea is to use such research 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. encourage development and use of 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 better located relative to global best practice in transport evaluation and
5. demonstrate how these methods can benefit from also working across government service activity in other agencies on like problems.

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 P ons-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 GA Withers. 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, O.K., 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

The online focus group schedule covers about 7-9 different topics/discussion points for each of the sessions on each of three days.

It is important to break each day into themes that link. The first day we start more broadly with 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 in answering – often about them!

We use the following response settings:

- **[STANDARD]** means that participants will see comments from anyone that has posted before them.
- **[RESPONSE]** means that participants will see nothing until they comment.They answer this 'blind' and cannot be influenced by other people's comments.
- **[PRIVATE]** means that participants will not be able to see comments fromanyone else.
- **[OPTIONAL]** means that participants can choose to comment or to skipthrough.
- **[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)

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.

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 duringthe pandemic?

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?

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?

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'sreputation?

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?

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

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)

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.

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?

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 actualcases or hypothetical ones that you can imagine.

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?

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?

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)

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?

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)

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.

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? In what ways? (*MODERATOR PROMPT: Criminal, terrorist, foreign government, disgruntled employee.)*

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?

Informing their customers

Response setting: [STANDARD]

When and how would you expect a public transport agency experiencing a cyber-attack to inform their

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

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.

Final Thoughts

Response setting: [OPTIONAL]

Thanks for contributing your time and participating over the last three days. This research has been conducted 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?

APPENDIX B: 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) _____

Q 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)	○	○	○

Q1A 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?

_____

Q1B 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)	○	○	○	○	○	○	○	○

Q1C 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?

_____

Q 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)

Q 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)