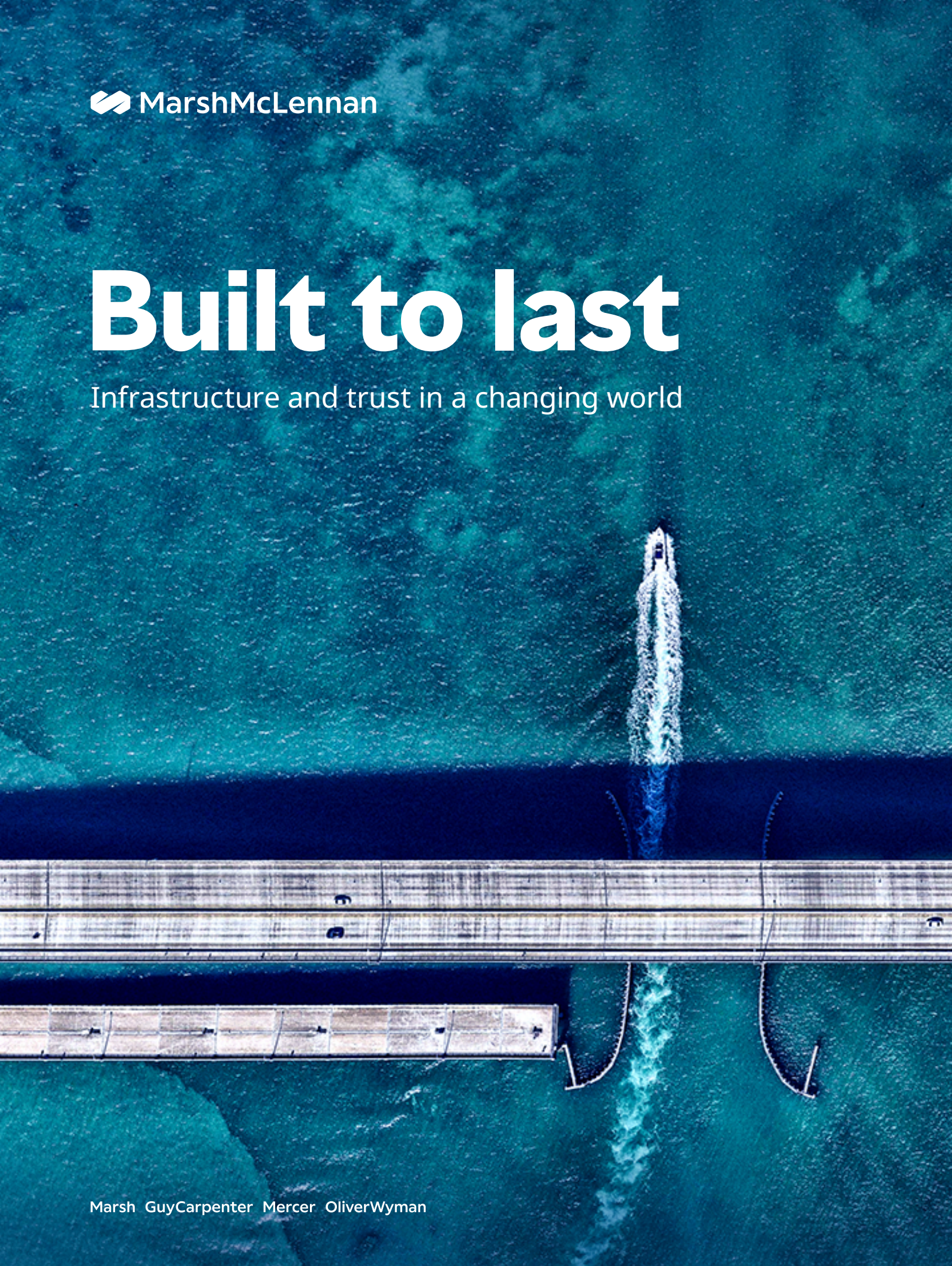
MarshMcLennan

Built to last

Infrastructure and trust in a changing world



Marsh GuyCarpenter Mercer OliverWyman

Contents

KEY TAKEAWAYS

1. Trust plays an important role in the infrastructure ecosystem. As providers of essential services to society and industry, owners and operators of assets must routinely balance expectations of users, investors, governments, and regulators in the face of competing interests and finite resources. Trust is a complex concept, but when the expectations of all stakeholders are consistently met a firm can be confident it has the social license to operate over the lifetime of the asset.

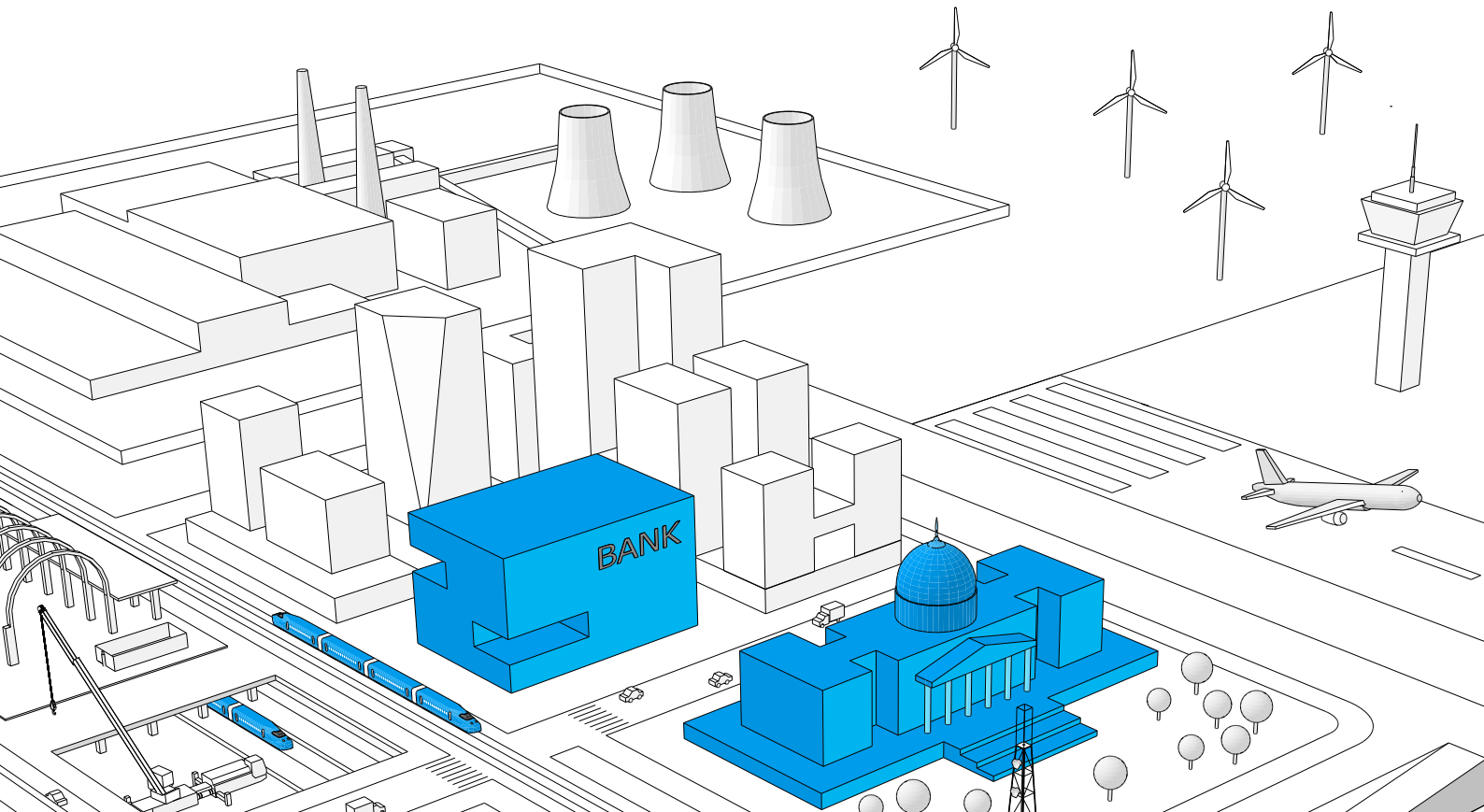
2. The post-pandemic global economic recovery, the intensifying effects of climate change, and the evolving threat of cyber risk are creating new trust-based issues that challenge traditional relationship dynamics. Without appreciating enhanced sensitivities and volatilities that accompany these trends, owners and operators risk being blindsided by fast-moving events.

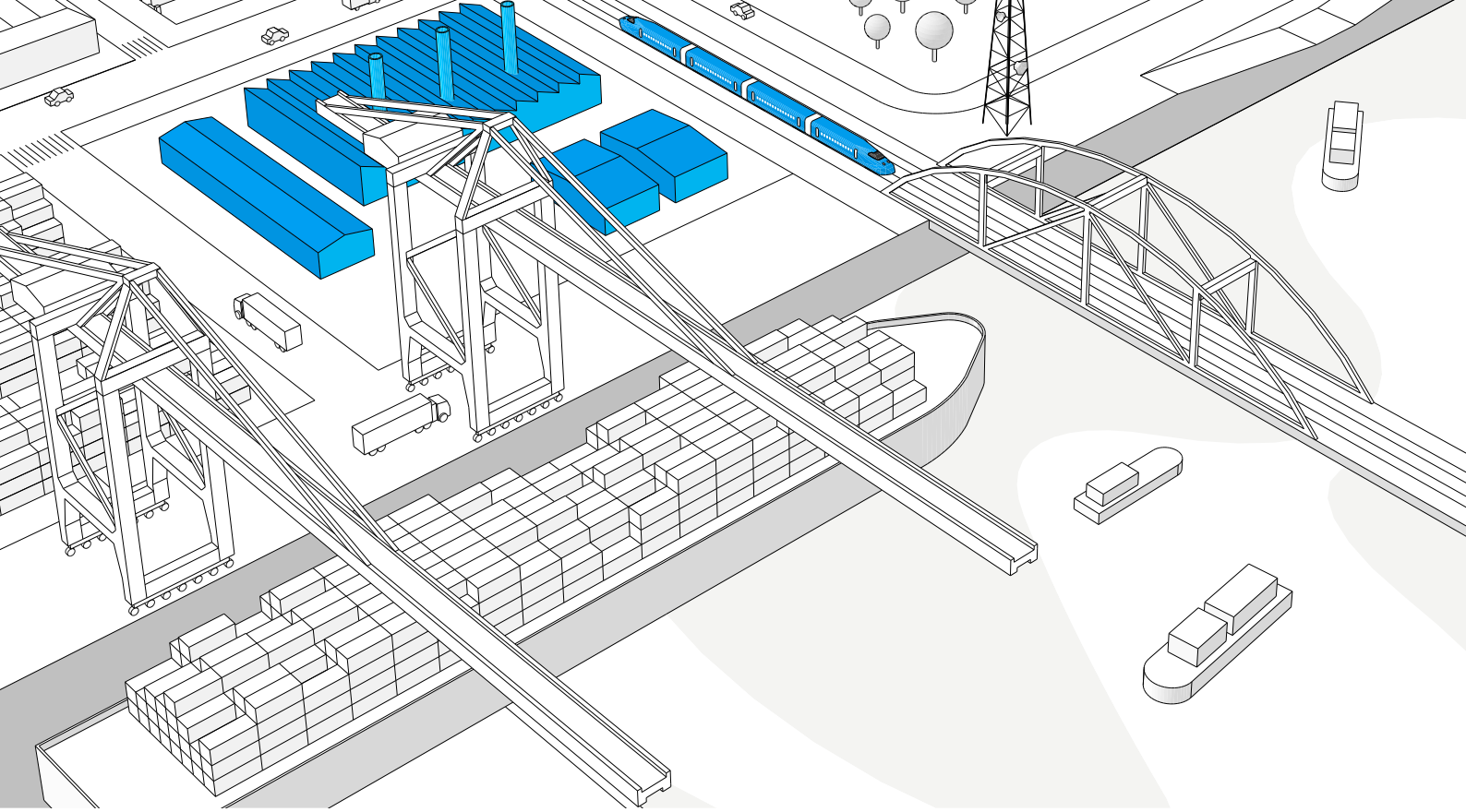
3. Certain transport-focused assets have struggled in the face of the pandemic relative to some energy and digital infrastructure assets. How user demand for transportation services will evolve is still unclear. While some people are clearly willing to return to public transport, health fears continue to hold others back. Demand is only one part of the worry, however, as the pandemic has spurred growing resource nationalism and restrictions on foreign investment that will worry both global investors and foreign owners.

4. Climate change is driving a range of physical and transition risks for infrastructure. An updated view of the acute and chronic physical risks facing an asset is required for mitigation plans to be put in place to ensure service reliability and community safety. Net-zero targets are increasingly being set by countries and companies globally. The likely disorderly path to achieve this state has led to many governments and investors demanding that owners create and disclose credible plans for dealing with the uncertainty. In the face of so many unknowns, scenario planning tools to support decision-making are essential.

5. The ongoing digitization of assets has created an increased surface area for cyberattacks. Ransomware attacks in particular are at an all-time high, with almost 75% of recorded critical infrastructure ransomware attacks since 2013 having occurred in the past two and a half years. Fears about service reliability and the security of personal data are a chief concern for users, governments, and investors. Operators must respond by aligning their policies, employee practices, and supply chains to ensure there are no weak links that can be exploited.

The changing face of stakeholder expectations





Against a backdrop of a world in flux, infrastructure stakeholders have adjusted their expectations of the services they receive and the firms that provide them. Private owners and operators can continue to build and maintain trust by tracking how expectations are evolving and ensuring their strategies and services change accordingly.

As providers of essential services, owners and operators of infrastructure have always had to meet varied expectations of users and local communities, public authorities and, often, regulators. Where an asset is owned and/or operated by a private company, expectations are further altered and complicated by the need to ensure a fair return for investors. Earning the trust of all stakeholders is a challenge, but maintaining it through the lifetime of an asset is even more difficult.

Although this report focuses on trust challenges facing private owners and operators, they also have their own trust-based expectations of key stakeholders in return. These include the stability of laws and regulations set by governments and regulators, as well as fair warning from investors regarding changes in their expectations which might be voiced in public or through shareholder voting. Other expectations include a degree of patience and understanding from users and communities in the face of service disruption arising from essential works. The nature of being a service provider, however, means that a failure to meet stakeholder expectations often receives more attention than the reverse situation.

As an important factor in enabling productive long-term relationships with stakeholders, trust not only confers private infrastructure owners and operators with a social license to operate but also assists in building a solid track record, ensuring industry credibility, and establishing organizational resilience.

However, new issues have exposed the vulnerability of this trust landscape (see Exhibit 1).

Exhibit 1: Examples of how trust is easily lost — showcased via anonymized media content

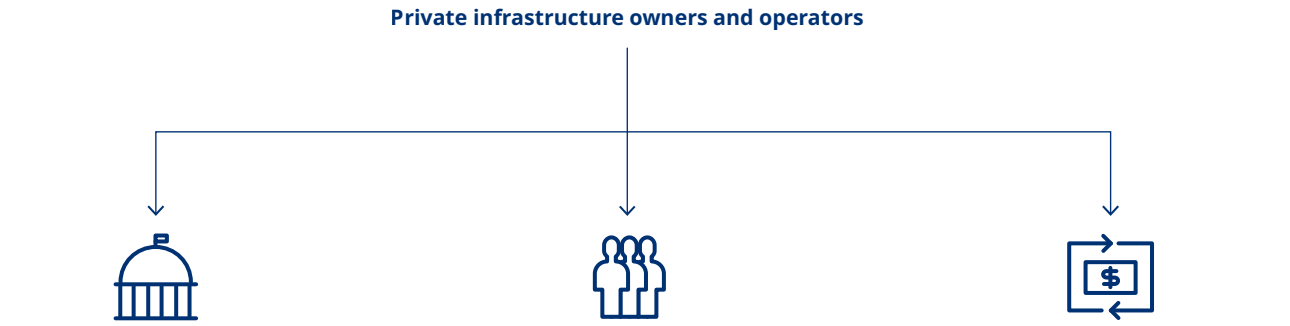
Source: Marsh McLennan Advantage analysis

The potential interplay between different stakeholder expectations also merit consideration. The expectations may at times converge — for instance, both investors and consumers are increasingly concerned about the physical and transition impacts of climate change. But stakeholder expectations may also collide, such as when regulators agree to increase service charges in the face of user opposition for the stated benefit of allowing operators to reinvest those revenues in resilience and climate adaptation measures.

Owners and operators have to carefully navigate the ever-changing landscape of stakeholder expectations. The task is made more challenging by the concurrence of the evolving threats described in the next section.

The first step for private owners and operators in maintaining trust is to identify key stakeholder expectations and track how they are evolving (see Exhibit 2).

Exhibit 2: External stakeholder expectations of private infrastructure owners and operators



Source: Marsh McLennan Advantage

Governments and regulators aim to generate tangible benefits for the public by making their lives more convenient, fostering economic growth and safeguarding national security and resilience. Government and regulator expectations include:

- **Capital and expertise**. The private sector should be able to reduce the pressure on public balance sheets by providing resources for the construction and maintenance of infrastructure assets while minimizing the need for bailouts or subsidies.
- **Value for money**. Private owners and operators should ensure that infrastructure assets generate fair and adequate returns, while meeting defined service levels and protecting consumers.
- **Security and resilience**. Infrastructure is of strategic value to society, and governments demand that infrastructure assets and systems demonstrate resilience in the face of challenging and adverse events.

Users and communities have acquired an even larger voice in recent years as critical actors in the decision-making processes linked to infrastructure development. The usage of social media to organize and campaign around collective grievances, growing awareness of socioeconomic and environmental issues, and the rise of misinformation have all contributed to this phenomenon. User and community expectations include:

- **Quality of service and manageable costs**. Users expect safe, reliable, and economical services. Any form of disruption or adverse change should be quickly dealt with.
- **Transparency in governance and operations**. Owners and operators should share with communities and businesses the rationale behind key decisions.

- **Effective consultation channels**. Both civil society and business stakeholders expect to be engaged in discussions about the potential socioeconomic and environmental implications of projects. Avenues should also be set up for feedback and grievance redressal over the lifetime of an asset.

Investors are increasingly focused on allocating resources to infrastructure indirectly through mechanisms such as funds and listed assets. Investor expectations include:

- **Solid and steady financial performance**. Infrastructure is a highly illiquid asset class, and long-term investments in it are made under the assumption they will deliver expected shareholder returns over time, without radical changes in the underlying business models that may alter the risk-return profile of the original investment.
- **Appropriate governance arrangements**. Reporting should be timely, transparent, and granular enough to support decision-making processes.
- **Comprehensive and consistent ESG disclosure**. The increasing number of global standards and legal requirements in certain countries should lead to corresponding disclosures on the part of owners and operators.
- **Regular and open dialogue**. Shareholders expect to discuss critical societal topics with owner and operators. Recent years have witnessed increasing levels of activism from investors exercising their voting right to influence firms on diverse issues such as climate change, workforce equality, data privacy, and community impact.

As an important factor in enabling productive long-term relationships with stakeholders, trust not only confers private infrastructure owners and operators with a social license to operate but also assists in building a solid track record, ensuring industry credibility, and establishing organizational resilience.

Emerging trust challenges: How can owners and operators respond?

The trust landscape for owners and operators is complicated by three dynamics that affect relationships with key stakeholders. Understanding these ongoing trends is the first step in mitigating their potential impacts. Taking action to address the underlying issues will ultimately protect a business against cascading trust-related concerns.

Pandemic recovery

The global pandemic has led to a significant fall in demand for many infrastructure assets, resulted in a range of workforce challenges, and amplified nationalist sentiment in several countries. Owners and operators must position themselves strategically and operationally to return to full capacity as quickly as demand and regulation allow.

Exhibit 3: Supporting statistics to highlight challenges in pandemic recovery

63% decrease

in overall air traffic volume for 2020 compared to 2019[1]

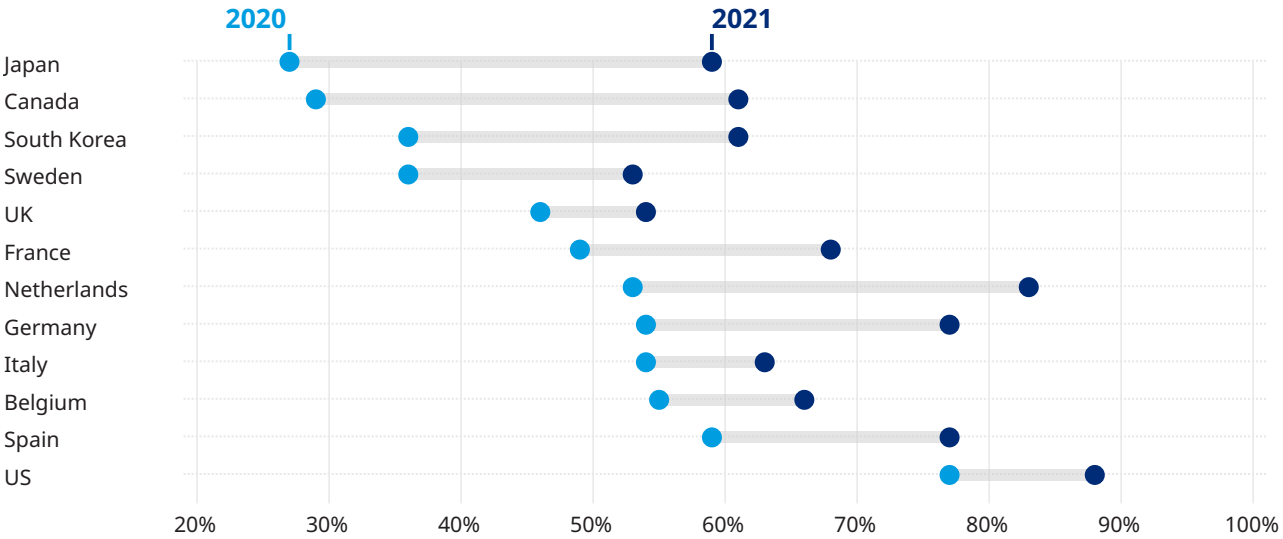
60% decrease

in average maximum monthly toll road traffic in March 2021 compared to January 2020[2]

4% decline

in global energy demand in 2020, **the largest since World War II and the largest ever absolute decline**[3]

% of respondents who believe their country is divided — before versus after the pandemic[4]



1 Airports Council International (ACI). (2021, March 25). *The impact of COVID-19 on the airport business and the path to recovery.* Retrieved August 3, 2021.

2 Fitch Ratings. (2021, March 22). *Global Toll Road Traffic Tracker: 1Q21 Update.* Retrieved August 3, 2021.

3 International Energy Agency. (2021). *Global Energy Review 2021: Economic Impacts of Covid-19.*

4 Pew Research Center. (2021). *People in Advanced Economies Say Their Society Is More Divided Than Before Pandemic.*

The demand for services has fallen significantly in some transportation assets

Trends

Airports, metro rail, and some toll roads have been hit particularly hard by forced remote working and restrictions on international air travel. Moreover, many would-be travelers or commuters are choosing to avoid public transportation for pandemic-related health reasons.

The vast majority of countries globally have not experienced a linear recovery path from COVID to date and there is little to suggest that this will change in the near future. More contagious virus variants have led to a number of countries imposing multiple lockdowns. The stop-start nature of these restrictions causes challenges for owners and operators, particularly in terms of managing workforce utilization.

Longer-term shifts also pose challenges, particularly the uncertainty of what the future of work will look like for many. The coming years will see new norms form and existing ones evolve, and these may differ across industries and geographies. This is a real challenge for operators of assets that have, until now, earned most of their revenue from commuters. Similarly, international air travel will return but IATA predicts that global air passenger numbers will only reach 5.6 billion by 2030 — 7% lower than pre-pandemic estimates.[5]

Trust implications

Any perception of short-term unreliability of services will be frustrating for users. If broader demand challenges lead to a withholding of capital expenditure, which in turn reduces the quality or efficiency of future services, then users will be disappointed and may seek alternative services or scale back demand.

As demand returns, operators will have to progressively build back workforce capacity while ensuring no teething issues impact operations during the resumption of full service. Issues such as delays, breakdowns, or worse still, safety incidents, arising from employee mistakes will create lasting trust issues with users and potentially knock-on revenue and reputation risks for investors.

For investors, the immediate worry is about returns and asset valuations. They will trust that owners and operators will take appropriate measures to manage costs in times when revenues are down, while at the same time remain agile and able to respond quickly to sudden shifts in restrictions and user demand.

Responses

To mitigate these concerns, operators will have to take several steps. To satisfy users with pandemic-related health concerns, investments may be required to adapt physical spaces and user-related processes to support safe-distancing and other health related measures. Building a good working relationship with relevant government departments will support operators in understanding how to adapt operations to new health guidelines and to potentially be made aware of early thinking on future developments and timelines for service resumption. Where transportation asset owners have had the opportunity to take advantage of government support such as furlough schemes, this should be done only as necessary, with the understanding that employees will be brought back onboard as soon as demand permits.

Communication to users about investments and supporting measures taken should be proactive and include broader updates on plans to scale services back up, as well as news of any other improvements which have been made for the user's benefit. Investments in assets should be reviewed strategically, with consideration given to where they can be front-loaded and completed faster and more cost-effectively in a lockdown environment — for example, upgrade works which would otherwise impact capacity at peak times.

---

5 International Civil Aviation Organization. (June 2021). *Economic Development — June 2021 Air Transport Monthly Monitor.*

Asset owners should communicate regularly with investors about the financial impact of the pandemic and the measures being taken to reduce costs and safeguard the future of the business. Where a portfolio of assets is being managed on behalf of investors it should be reviewed to minimize concentration risks. One instance might be transportation assets that derive their primary revenue from cross-border travel as these have been hit harder than those with the ability to serve large domestic markets. For example, in April 2021, passenger volume in Dallas-Fort Worth was 21% below April 2019 levels; however, for Changi Airport in Singapore, the decline was almost 97%.[6,7]

Rising nationalism creates concerns for foreign owners and operators

Trends

The fallout of the pandemic has resulted in an amplification of nationalist sentiment in several countries, leaving foreign firms with local infrastructure interests feeling more exposed to political and geopolitical risks.

Concerns over foreign ownership of critical infrastructure have predated the pandemic in a number of countries. Historically, these worries centered around potential foreign control of key energy and transportation assets. However, more recently these worries have focused on digital infrastructure and the potential for a foreign power to store, access, and manipulate a nation's data. These worries have partly translated into a wide number of OECD and non-OECD countries putting in place measures to more closely scrutinize Foreign Direct Investment (FDI) at a time when opportunistic investors were searching for good deals. In OECD countries, FDI fell by 51% in 2020.[8]

Additionally, in 2020 over 30 countries experienced a significant increase in risk as captured by Verisk Maplecroft's Resource Nationalism Index.[9] The economic impact of the pandemic has been severe, resulting in many job losses and in significant government stimulus programs to support citizens and local companies. Funding must be found for such programs — one increasingly popular way has been to impose direct and indirect measures, such as new taxes, on the extraction of natural resources and delivery of related services.

Trust implications

Foreign owners and operators of infrastructure assets will be watching political developments keenly in the countries they operate in. Governments will be particularly wary of foreign-owned infrastructure businesses that are seen to be earning and exporting outsized returns at a time of national hardship and increasing inequality. They will also likely be setting new criteria for which organizations and investors are eligible to take part in the roll out of future initiatives, such as national 5G programs, to ensure greater control over where and how national data is stored.

From the perspective of institutional investors, any measures that reduce their ability to further invest in a country, or that have the potential to erode their returns from existing investments in a country will be a cause for significant concern.

Responses

Mitigating security-based concerns about foreign ownership of infrastructure assets is challenging. Foreign owners should ensure transparency when disclosing who their investors are and any technology partnerships that they have in place. Certain governments may require operators to provide assurances regarding data ownership

---

6 Changi Airport Group. (2021). *Traffic Statistics — Passenger Movements*. Retrieved August 3, 2021.

7 Civil Aviation Authority of Singapore. (2020). *Civil Aircraft Arrivals, Departures, Passengers And Mail, Changi Airport, Monthly.* Dataset accessed through Data.gov.sg.

8 Kirchner, S. (2021, July 6). *US investors cool on Australia*. The Mandarin. Retrieved August 3, 2021.

9 Blanco, J., & Machado, M. P. (2021, March 4). *Resource nationalism surges in 2020, Covid-19 worsens outlook: Political Risk Outlook 2021.* Verisk Maplecroft.

and storage, particularly for telco assets. If a firm can communicate effectively with government stakeholders about its technical solutions, with an emphasis on data security, they will have a greater likelihood of convincing authorities of their eligibility to own and operate digital infrastructure assets.

Foreign owners and operators need an internal tracking system to identify instances of rising resource nationalism and sources of political and geopolitical risk. A key task will be intelligence gathering and analysis from a variety of sources. To minimize the risk of negative developments, owners and operators must review their approach to managing their interactions with the societies they serve and the communities in which they operate. With societal discontent a key driver of increasing resource nationalism, proactively working with citizens and communities in areas they operate can help lower the level of this concern.

The fallout of the pandemic has resulted in an amplification of nationalist sentiment in several countries, leaving foreign firms with local infrastructure interests feeling more exposed to political and geopolitical risks.

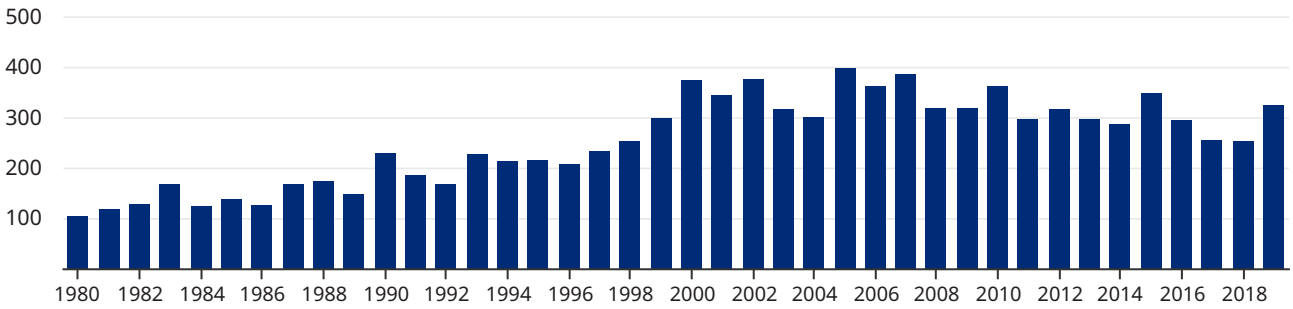
Accelerating impacts of climate change

Climate change is driving a range of physical, transition, and liability risks in infrastructure. Uncertainty surrounding the various paths to decarbonization challenges traditional business models and existing infrastructure investment approaches. Data analytics can guide the use of adaptation measures and the negotiation of innovative risk transfer solutions. Transparent reporting on climate metrics offers new opportunities to strengthen relationships with stakeholders.

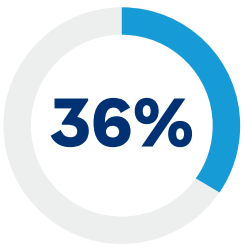
Exhibit 4: Supporting statistics to highlight challenges due to climate change

79% increase

in climate-related disasters in the period 2000-2019 vs. 1980-1999[10]



of global greenhouse gas emissions are caused by infrastructure construction and operations[11]



of investor capital was aligned with net-zero targets in June 2021, a fourfold increase from December 2020[12]

+231%

growth in the number of companies disclosing their environmental impact with CDP in 2020 compared to 2010[13]

36%

of institutional investors prioritize ESG in infrastructure, double than reported in 2016[14]

10 Ritchie, H., & Roser, M. (2019). *Natural Disasters*. OurWorldInData.org. Data from EM-DAT: OFDA/CRED International Disaster Database, Université catholique de Louvain. Retrieved August 3, 2021.

11 Saha D. (2018). *Low-carbon infrastructure: An essential solution to climate change?* The World Bank. Retrieved August 3, 2021.

12 Net Zero Asset Managers Initiative, Marsh McLennan Analysis.

13 CDP. (2020). *The A List 2020.* Retrieved August 3, 2021.

14 EDHEC Infrastructure Institute. (2019). *2019 Global Infrastructure Investor Survey.*

Infrastructure assets are threatened by the physical impacts of climate change

Trends

Infrastructure is often not designed to withstand future — and at times current — climate conditions. With scientists expecting an increase globally in events such as heatwaves, droughts, wildfires, floods, and tropical cyclones, the threat to infrastructure assets is clear. The 2021 Western North America heatwave delivered extreme temperatures which caused road pavements to buckle, brought public transport to a standstill, and resulted in rolling blackouts in various areas of the Pacific Northwest.[15,16] Hurricane Harvey in 2017 caused extensive damage to Texas' roads, bridges, and energy system, resulting in over $10 billion in infrastructure damage.[17]

Chronic trends driven by climate change will also increasingly damage assets. For example, with a mean temperature increase of 2°C, the corresponding rise in sea level could submerge about 100 airports globally.[18] Water is essential for thermal and hydroelectric power generation, and water stress induced by climate change will put at risk 47% of thermal power plant capacity and 11% of hydroelectric capacity globally.[19]

Trust implications

Physical damage can trigger cascading failures and affect a broad range of stakeholders. Service disruption may lead to loss of trust from users and communities, and may also complicate relationships with public sector authorities. Investors are wary of how damage to assets may affect returns on investment through asset devaluation and the impact on financial performance caused by revenue shortfalls.

A catastrophic climate event will not necessarily lead to a loss of trust from governments, users, and communities, but it might do so if owners and operators are not seen to have been adequately prepared to respond effectively and in a timely manner.

Long-term impacts on ecosystems (such as the depletion of water resources and deforestation) and harm to people and the environment caused by infrastructure failures (for example, through spills of toxic substances) may lead to legal and reputational risks with steep financial liabilities.

Responses

Private infrastructure owners and operators should prepare to invest in hazard and vulnerability modeling to quantify present-day and future impacts of natural catastrophes under multiple climate change scenarios. These models can inform the design of adaptation measures and resilience investment programs, and support first-response and crisis management. Results from such tools can be incorporated in project planning, thus increasing the confidence governments, lenders, and investors have in the long-term financial sustainability and resilience of assets. The output of hazard models can also offer reliable information to be used in reporting on physical risks whenever this is required, for example in generating data for crisis and scenario stress-testing that can be shared with regulators. In the wake of a catastrophe, climate-resilient infrastructure can help contain damage and disruption, thus helping manage reputational and liability risks.

---

15 Prociv, K. (2021, June 28). *Pacific Northwest is in one of the most intense heat waves ever, with the worst still to come*. NBC News. Retrieved August 3, 2021.

16 Fischels, J. (2021, June 29). *The Record-Breaking Heat Wave That's Scorching the Pacific Northwest*. NPR. Retrieved August 3, 2021.

17 Eaton, C. (2017, September 1). *Hurricane Harvey's Damage to Texas Infrastructure Estimated at $10 Billion*. Government Technology. Retrieved August 3, 2021.

18 Yesudian, A. N., & Dawson, R. J. (2021). Global analysis of sea level rise risk to airports. *Climate Risk Management, 31*, 100266. https://doi.org/10.1016/j.crm.2020.100266

19 Kressig, A., Byers, L., Friedrich, J., Luo, T., & McCormick, C. (2018, April 11). *Water Stress Threatens Nearly Half the World's Thermal Power Plant Capacity*. World Resources Institute. Retrieved August 3, 2021.

It is also critical for owners and operators to invest in innovative risk transfer solutions, and the results of hazard and vulnerability models can provide insights that can be leveraged when negotiating risk transfer arrangements. Products such as parametric insurance can provide faster payouts compared to indemnity insurance and can minimize the time needed for recovery, thus increasing confidence among governments and investors in the ability of owners and operators to manage risk.

Decarbonization and climate disclosure are challenging traditional business models

Trends

A growing number of governments, regulatory bodies, and businesses are committing to the principles of climate change mitigation and adaptation by reducing emissions and investing in resilience and preparedness. Uncertainty regarding the path to net-zero, however, continues to manifest in various forms. Particular concerns include demand risk, technological obsolescence, and legal and regulatory developments, especially regarding emissions and reporting. Continued uncertainty over the direction and stability of government policies in various countries can add to the confusion. As the urgency to decarbonize grows, target-based reporting on environmental performance and greenhouse gas emissions is becoming a new standard across industries and geographies. Although disclosure is increasingly becoming a mandated requirement by a variety of public authorities, this is not just about formal requirements. Voluntary initiatives such as the Financial Stability Board's Task Force on Climate-related Financial Disclosures (TCFD)[20] are also gaining momentum.

Trust implications

For some infrastructure businesses the uncertainty surrounding the pace and direction of decarbonization can translate into an unwillingness to invest in climate adaptation measures. This can exacerbate preexisting concerns among stakeholders around the ability of firms to adjust to the transformations brought about by climate change. For governments and investors, an abrupt or disorderly transition may result in concerns about the ability of infrastructure businesses to adapt to new market trends and regulatory requirements. Difficulties owners and operators face in adjusting to the transition may also have consequences for socioeconomic resilience and national security, creating concerns among both public authorities and users. Likewise, businesses that are viewed to be slow in pursuing a path to decarbonization may experience reputational and liability risks based on societal and public sector perceptions. A sluggish decarbonization journey could also result in missed business opportunities: government-led stimulus programs approved in the wake of the pandemic, for example, have often included allocations for green infrastructure and climate adaptation measures.

Responses

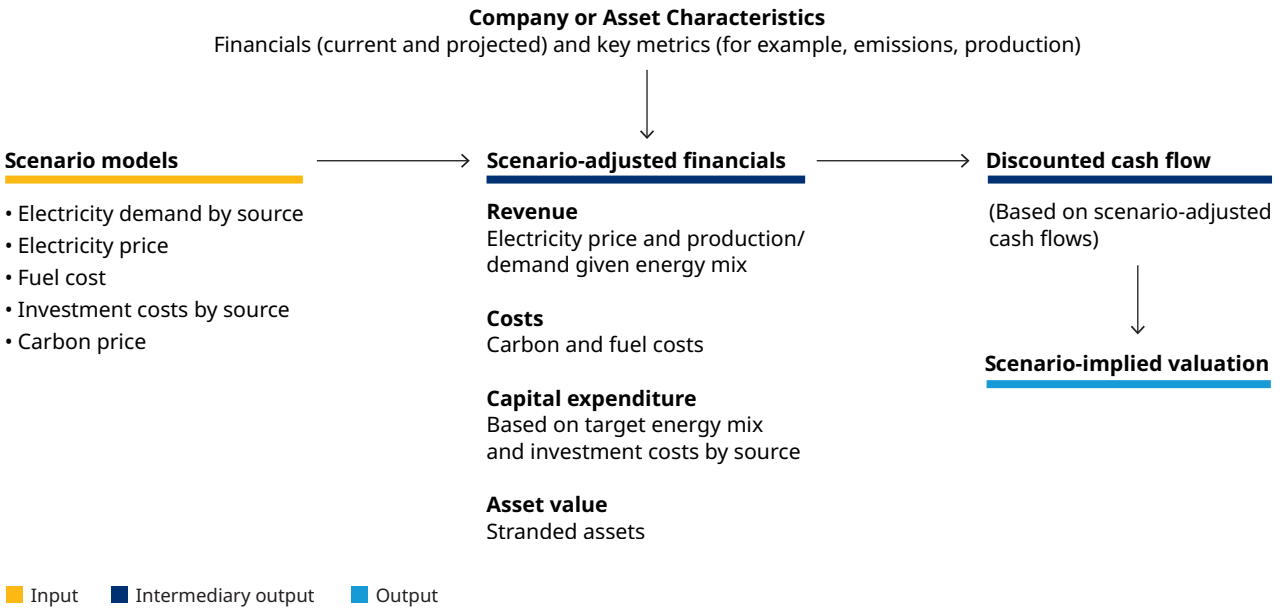
A foundational step in being able to build trust through disclosure is effective climate scenario planning. Scenario planning allows businesses to consider multiple different possible futures and understand the ways in which they will be impacted by each, rather than trying to accurately forecast a singular outcome. Scenario planning is essential in creating strong and credible transition strategies, and in effectively communicating these programs to stakeholders. Methodologies such as the one commissioned by the United Nations' Environment Program Finance Initiative (UNEP FI) and delivered by Oliver Wyman and Mercer[21] allow for the impact of transition climate risks to be considered across infrastructure sub-sectors. If an unregulated power utility, for example, was to use this tool, then relevant variables for future scenarios would include regional carbon prices, electricity demand, fuel costs, and investment costs (see Exhibit 5).

---

20 To learn more about the Task Force on Climate-related Financial Disclosures (TCFD), please see *Task Force on Climate-related Financial Disclosures*. fsb-tcfd.org. Retrieved on 26 July 2021.

21 United Nations Environment Programme Finance Initiative, Oliver Wyman, & Marsh. (2018). Extending our horizons: Guiding banks through climate-related impacts.

Exhibit 5: Framework for an unregulated power generation utilities asset using climate scenario variables



Source: Marsh McLennan Advantage analysis

Outputs from scenario planning exercises can also be used by private owners and operators in annual reports and other means of disclosure to build the confidence of investors and regulators. Infrastructure businesses should gain a thorough understanding of the reporting requirements they are legally bound to align with, as well as of those promoted by institutional investors and financial institutions. Reporting on environmental performance can increase the confidence investors have in the long-term sustainability of the firm's business model, and strengthen relationships with governments and regulators concerned about mitigating climate change in line with national or regional emissions targets.

Businesses that are viewed to be slow in pursuing a path to decarbonization may experience reputational and liability risks based on societal and public sector perceptions.

Heightened cyber threats

The digitization of infrastructure has brought operators many benefits, but also leaves them with multiple vulnerabilities at a time when cyberattacks on assets are at an all-time high. Protecting operations and customer data is a paramount concern for all stakeholders and involves a coordinated response from leaders, employees, and risk transfer specialists, as well as throughout a firm's supply chain and broader infrastructure ecosystem.

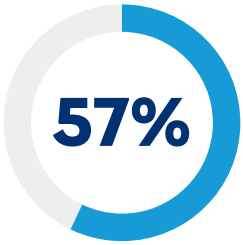
Exhibit 6: Supporting statistics to highlight cyber threat challenges

50%

of IT security professionals worldwide believe their country's critical infrastructure is susceptible to cyberattacks[22]

56%

of gas, wind, water, and solar utilities around the world experienced at least one shutdown or operation data loss incident in 2019[23]

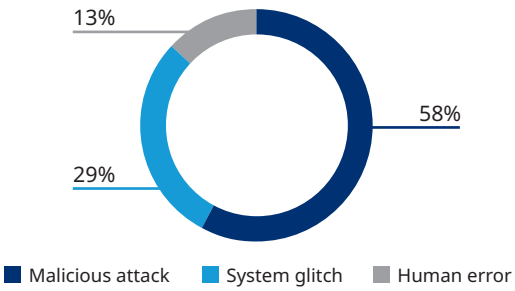


of US-based respondents were not confident that companies follow their own privacy policies regarding user data[24]

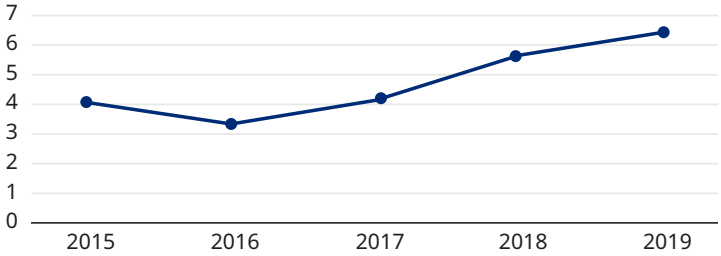
102% increase

in the number of organizations affected by ransomware from Jan-Apr 2021 compared to the same period in 2020[25]

Root causes of data breaches in the transportation industry[26]



Average total cost of a data breach in the energy industry[27]



22 Claroty. (2020). The global state of industrial cybersecurity.

23 Siemens & Ponemon Institute. (2019). *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?.*

24 Pew Research Center. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.*

25 Check Point Software Technologies. (2021). *The New Ransomware Threat: Triple Extortion.*

26 IBM Security. (2020). *Cost of a Data Breach Report.*

27 Ibid.

Trends

Growing digital connectivity due to innovations in technology, such as automation and artificial intelligence, has enabled infrastructure owners and operators to make significant gains in efficiency and costs savings for their assets. However, this increased digitization within an asset's operations, throughout an asset's supply chain and between multiple assets, has meant that there are now numerous points of attack for threat actors — a cyberattack surface that only widens when one also considers the broader vendor ecosystem, such as the cyber risks faced by managed service providers (MSPs). Researchers have estimated that two-thirds of data breaches occur due to third-party vulnerabilities.[28]

A rise in ransomware attacks has highlighted the urgency of preparing for cyber incidents and the importance of minimizing the potential loss from cascading failures. Close to 75% of recorded critical infrastructure ransomware attacks since 2013 have occurred in the past two and a half years.[29] Recently, a cyberattack forced Colonial Pipeline, a leading oil company in the US, to pause supply, disable systems, and ultimately pay $4.4 million worth of Bitcoin in ransom.[30] As the operator of the largest petroleum pipeline in the country, Colonial Pipeline's data breach pushed gas prices up and led state governments to implement tax policy changes and price gouging laws.[31]

The increased use of new digitally connected devices (smart meters in homes, microgrids at industrial sites, and others) has resulted in a significant surge in the amount of user data being collected. The rise of a black market for data has also meant that many cybercriminal groups have targeted infrastructure solely with the purpose of acquiring and selling of selling large amounts of user and employee data as a commodity to other threat actors. For instance, the data theft of the entire customer database of People's Energy, a UK based sustainable energy firm, had minimal direct financial risk to customers but raised the possibility of customers being targeted through suspicious phishing emails and calls in the future.[32]

Trust implications

Collectively, cyber risks can upend trust dynamics between owners and operators, and key stakeholders. Cyber incidents spread across interconnected assets can especially challenge the credibility of owners and operators in the eyes of governments that expect reliable and quality service. Data theft and ransomware attacks, particularly with geopolitical motivations, can have a knock-on impact on a government's public image, hamper national economic resilience, and complicate international relations. Cyber events may also result in property damage or bodily injury that may be subject to exclusion in traditional insurance policies, raising concerns among investors and public authorities on the ability of infrastructure businesses to deal with the financial consequences of an attack.

From an investor perspective, the reputational and financial consequences that accompany cyber risks are very concerning. Cyberattacks can threaten investor income and the valuation of an asset, and possibly result in regulatory inquiries and lawsuits. This increased attention from regulators and policymakers is influenced by the fact that users are increasingly wary and vocal about the ways in which companies utilize their data, and the rise of digital surveillance. Large data breaches will only entrench this sentiment of distrust.

---

28 Carter, S. D. (2020, July 2). *Hackers Putting Global Supply Chain at Risk*. National Defence Magazine. Retrieved August 3, 2021.

29 Rege, A. (2021). *Critical Infrastructure Ransomware Incident Dataset*. Version 11.2. Temple University. Retrieved August 3, 2021.

30 Eaton, C., & Volz, D. (2021, May 19). *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*. The Wall Street Journal. Retrieved August 3, 2021.

31 Holzberg, M. (2021, May 12). *Colonial Pipeline Company Begins To Restore Service As Gas Prices Reach $3 A Gallon*. Forbes. Retrieved August 3, 2021.

32 People's Energy Company. (2020, December 23). Information and FAQs on the 16 December data security incident. People's Energy Company. Retrieved on 26 July 2021.

Key stakeholders may also have different expectations regarding cyber risks. For instance, investors may expect a level of data collection to drive strategic decisions and improve profitability, but this may come into conflict with users who are skeptical of and opposed to an increase in the amount of data captured.

Responses

Instill best practices to assure stakeholders that all measures have been taken to prevent attacks

Owners and operators should adopt a risk management strategy that includes regular reviews of security practices such as firewalls and update patches. Ensuring software is up to date and that single points of failure in IT infrastructure are identified and removed, also helps prevent cyber incidents from cascading. Concurrently, special emphasis should be placed on ensuring that employees not only understand the significant impacts posed by cyber threats but are also trained in cybersecurity practices themselves.

Regularly reviewing risks across the supply chain can help prevent any unfortunate incidents arising from interactions with third parties. Firms must also review their own role in the supply chain. Research suggests that larger organizations are more likely to focus on risks they face from their supply chains than the risks they themselves pose to their supply chain (see Exhibit 7).[33]

Respond to cyber incidents in a timely and transparent manner whilst also showing stakeholders the way forward

In addition to putting comprehensive preventive cybersecurity practices in place, owners and operators should prepare for worst-case scenario cyber risk events by developing response strategies to mitigate disruptions in operations.

Adopting a timely and transparent approach in responding to cyber incidents is crucial, especially in light of rising stakeholder pessimism. A 2019 survey in the US found that almost 80% of respondents believed companies would not publicly admit to data misuse.[34] Regulators like the US Securities and Exchange Commission have outlined requirements for companies to disclose cybersecurity risks and incidents to investors.[35] Recently announced privacy-focused legislation (for example the California Consumer Privacy Act) and the frequency of data breaches across industries has only furthered scrutiny on owners and operators to be transparent about their cyber risk track record.

Stakeholders will also expect owners and operators to bounce back from a cyber incident in a timely manner. Appropriate insurance to provide coverage in the event of incidents can help with quickly undertaking redressal measures for affected users. Participating in national industry forums and sharing data on cyberattacks with the infrastructure sector (for example through the United States' National Cybersecurity and Communications Integration Center) can also help build industry resilience. Organizations can identify common cyber threat actors and their respective methods, discuss industry vulnerabilities, share cyber risk strategies and promote better coordinated responses. Through these actions, owners and operators can learn from the experiences of other actors in the industry, prepare internally and maintain stakeholder confidence.

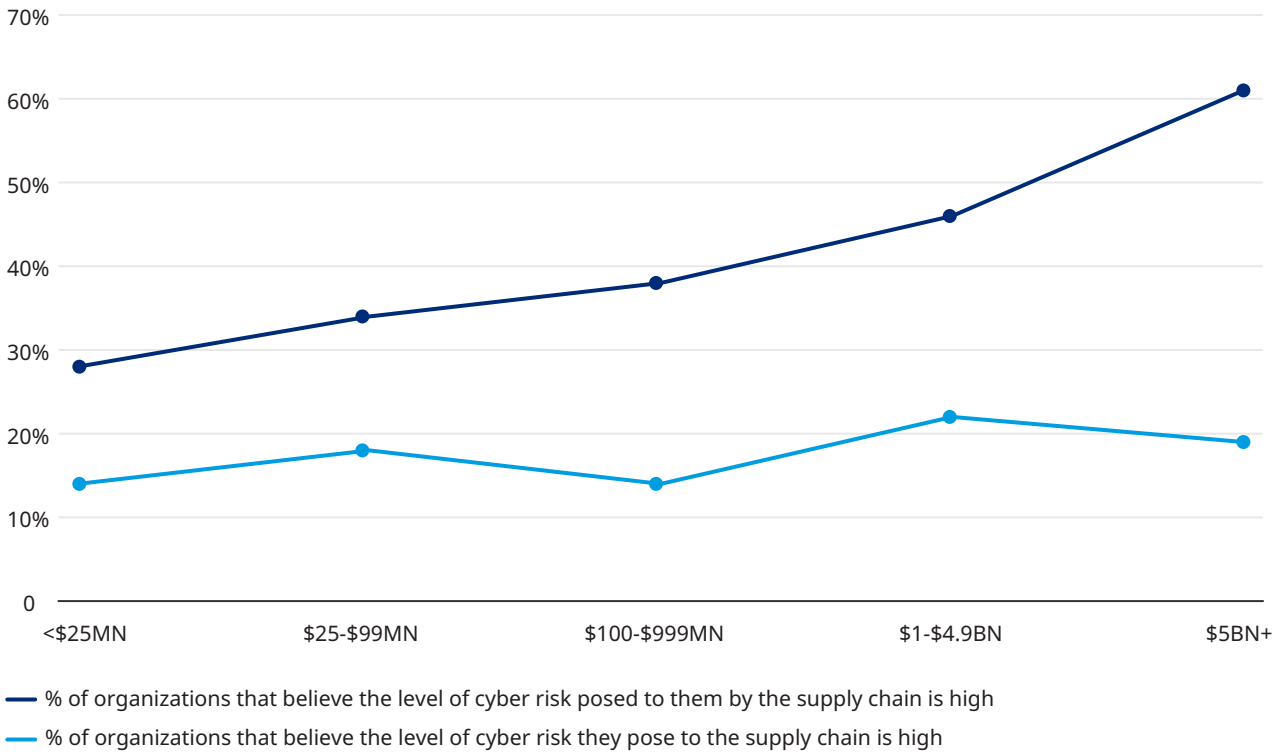
---

33 Marsh & Microsoft. (2019). *Global Cyber Risk Perception Survey Report 2019.*

34 Pew Research Center. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.*

35 etner, C. (2019, March 25). *Ignore the SEC's Strengthened Stance on Cybersecurity At Your Own Peril.*

Exhibit 7: The supply chain cyber risk perception gap



Note: The questions asked to the respondents were — "What level of cyber risk is posed to your organization by its supply chain/ third parties?" And the reverse: "What level of cyber risk does your organization pose to its supply chain/third parties?" The graph represents those respondents who believe the cyber risk level is "somewhat" or "very" high for both questions.

Source: Marsh & Microsoft. (2019). *Global Cyber Risk Perception Survey Report 2019*.

Research suggests that larger organizations are more likely to focus on risks they face from their supply chains than the risks they themselves pose to their supply chain.

Conclusion

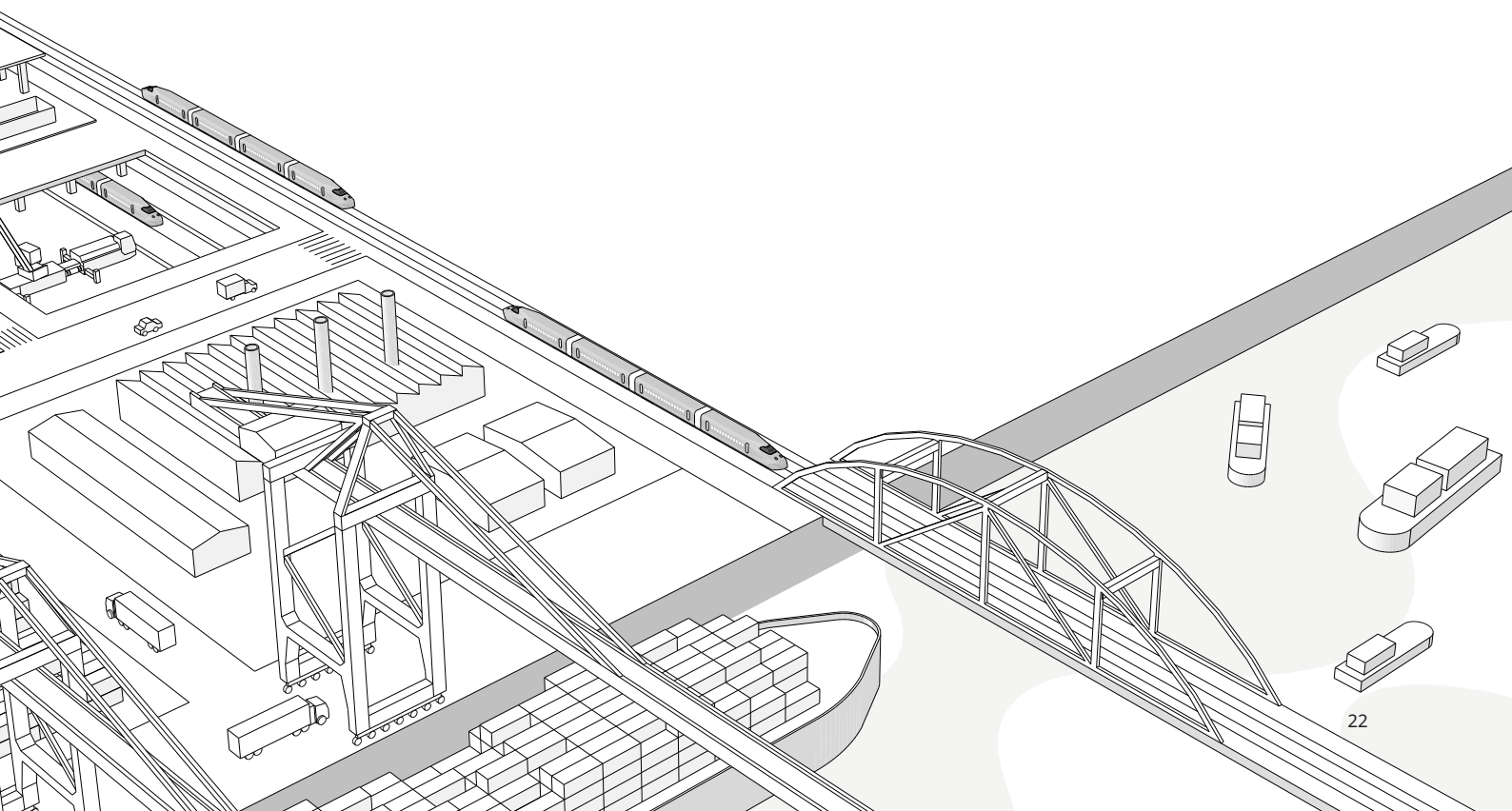
The concept of trust is vital for infrastructure asset owners and operators because they provide essential, often monopolistic, services to societies and industries. Although trust is a common thread in how owners and operators manage relationships with key stakeholders, it is rarely discussed explicitly by an involved party. Instead, the existence of trust is best determined when the collective expectations of users and communities, governments and regulators, and investors is examined in light of the performance of infrastructure businesses. When these expectations are collectively met, owners and operators can be assured of their important, but intangible "social license to operate" status.

Stakeholder expectations will continue to evolve. It is imperative owners and operators build capability to recognize changing expectations and respond accordingly. Equally, the factors that drive and complicate stakeholder expectations will, in turn, shift. While the main drivers currently are the recovery from the pandemic, climate change and cyber risk, new challenges will emerge and bring their own complications.

Leading owners and operators will be able to stay in control of their current operations while making sense of dynamics that will impact areas such as future demand, resilience, staffing, and their competitive landscape.

Trust will remain an essential by-product of delivering on stakeholder expectations. Changes in individual stakeholder expectations cannot be easily predicted and will continue to require targeted and situation-specific responses. However, there are common organizational behaviors that owners and operators can seek to foster internally to equip themselves best for the inevitable trust-related challenges that will arise.

Transparent, proactive communication on performance and challenges builds goodwill with all stakeholders. Ensuring appropriate channels for two-way dialogue with each stakeholder group makes them feel they have a voice. And balancing fair financial returns with a clear commitment to invest in resilience measures showcases levels of stewardship that support long-term success.



Acknowledgements

Authors

Blair Chalmers

Director, Marsh McLennan Advantage
blair.chalmers@mmc.com

Claudio Saffioti

Research Manager, Marsh McLennan Advantage
claudio.saffioti@oliverwyman.com

Sumer Drall

Research Analyst, Marsh McLennan Advantage
sumer.drall@oliverwyman.com

Contributors

Marsh McLennan

Richard Smith-Bingham, Martin Bennett, Adrian Pellen, Amarik Ubhi, Andrew Perry, Alexis Bradshaw, Viet Hoang Phan

Design

Ramona Pillai, Cheryl Lai

Web Design

Weronika Talaj, Hoh Wai Leong, Lydia Woo

Scan the QR code to visit website.

Marsh McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's 78,000 colleagues advise clients in 130 countries. With annual revenue over $18 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. Marsh provides data-driven risk advisory services and insurance solutions to commercial and consumer clients. Guy Carpenter develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. Mercer delivers advice and technology-driven solutions that help organizations redefine the world of work, reshape retirement and investment outcomes, and unlock health and well being for a changing workforce. Oliver Wyman serves as a critical strategic, economic and brand advisor to private sector and governmental clients.

For more information, visit mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK.