MARSH & McLENNAN ADVANTAGE

GIIA
Global Infrastructure Investor Association

GLOBAL RISKS FOR INFRASTRUCTURE

The technology challenge

CONTENTS

KEY TAKEAWAYS

1. Technology is shaking long-held assumptions about the essential and monopolistic nature of some infrastructure services, giving rise to the potential for stranded assets

2. The risk profile of investments has shifted such that investors and operators require new skills at all levels to navigate the threat of disruption through the strategic adoption of technology

3. Each infrastructure business will need to adopt an appropriate balance of portfolio- and asset-level lenses to help them address their unique technological capability requirements

4. Using technology to optimize existing assets will enable significant gains in cost savings, efficiency, safety, security, and sustainability performance

5. Infrastructure businesses must keep one eye on the horizon so they can anticipate technological innovations that may make for operational discontinuities, spur changes in consumer preferences, or trigger regulatory interventions

INFRASTRUCTURE'S TECHNOLOGICAL REVOLUTION

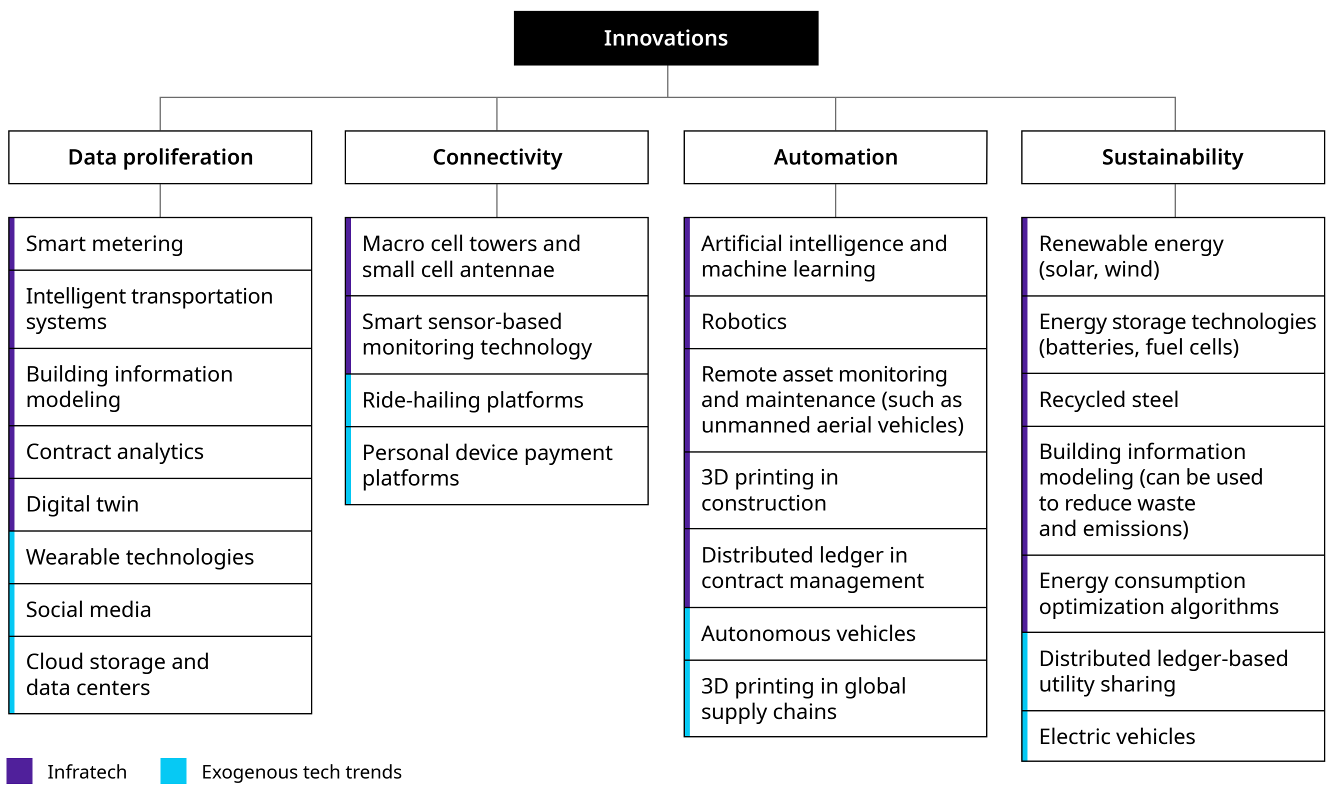
Technological innovation is reimagining the possibilities for the built environment, challenging infrastructure investors and operators alike to pre-empt disruption and actively seek fresh margins.

The infrastructure landscape is becoming more crowded and uncertain, with new technologies creating alternatives and substitutes to previously essential and monopolistic services. As competition heats up over new opportunities, investors and operators may find themselves misallocating capital and mispricing risk. Therefore, any business seeking to maximize return on investment will require a rigorous understanding of the implications of today's disruptive innovations. Unfortunately, by most accounts, the sector still lacks a good grasp of the transformative potential of technology.[1]

Numerous "Infratech" offerings — technologies associated with infrastructure operations — are already generating benefits across all stages of the asset lifecycle. These sit alongside broader exogenous trends that are impacting the sector. Taken together, these developments can be grouped into four categories (see Exhibit 1):

- **Data proliferation:** The widespread creation and collection of data
- **Connectivity:** The greater integration between the built environment and the digital world
- **Automation:** The increased data-driven mechanization of tasks and processes
- **Sustainability:** The growth of technologies supporting the low-carbon transition

Exhibit 1. Key categories of technological innovation in the infrastructure sector (selected examples)



Source: Marsh & McLennan Advantage

At the portfolio level, opportunities for investors with technical expertise are threefold. First, it enables them to evaluate the risk profile of different funds. Second, it lets them identify and pursue technology-rich prospects. And third, it helps them take a more data-intense view of their performance and positioning. For example, investors that fail to track and report on carbon emissions at the portfolio level are not only closing the door on sustainability enhancements but also generating reputation risks for themselves.

At the asset level, operators have an ever-widening range of tools for harnessing data and automating processes in pursuit of efficiencies, such as in asset utilization, demand aggregation, and yield management. These potential gains, moreover, often go hand in hand with improved safety and sustainability performance, providing additional incentives by which to attract funding and financing. But operators must navigate a number of risks. For instance, they must ensure that their workforce adopts new tools as intended; that third-party vendors do not expose the asset to cybersecurity risks; and, with respect to critical infrastructure assets, that their chosen solution is truly proven in order to avoid damaging outcomes.

With disruptor firms appearing more quickly than before in response to new technical possibilities and associated changes in consumer demand, technological progress presents as many challenges as opportunities. The following sections explore the changing environment in greater detail and set out key imperatives for infrastructure investors and owners.

With disruptor firms appearing more quickly than before in response to new technical possibilities and associated changes in consumer demand, technological progress presents as many challenges as opportunities

TECHNOLOGY-DRIVEN CHALLENGES

The adoption and implementation of rapidly developing technology by incumbents and disruptors has fundamentally changed the risk profile of both existing infrastructure assets and new investments.

These changes have resulted in new, material challenges for the sector. In particular, investors and operators must account for three key developments:

1. **Evolving nature of competition.** Innovations in **automation, data proliferation, connectivity,** and **sustainability** are transforming the competitive landscape in many subsectors. Where traditional infrastructure investments and business models are predicated on assets providing essential and monopolistic services, technology is often upending one or both of these factors.
2. **Heightened standards of accountability.** Today's innovations allow infrastructure assets to leverage new automation capabilities powered by **data proliferation and collection.** As businesses gain more potent technological capabilities, assets are becoming subject to greater digital oversight from regulatory bodies as well as the general public. This means investors and owners are facing different, and undoubtedly higher, standards of accountability.
3. **Widening cyber risk exposure.** The connection of built infrastructure to the internet and other networks enhances **data proliferation** risks. Greater connectivity also heightens the sector's exposure to cybercrimes such as data fraud, theft, and denial-of-service attacks.

EVOLVING NATURE OF COMPETITION

Technological advances have lowered the traditionally high barriers to entry for infrastructure services previously regarded as monopolistic in nature. These developments are also accelerating a shift in customer demands that may undermine the essential nature of assets and services. For owners and operators of some assets, this has resulted in increased competition, while for others it has reduced or changed demand. These dual forces are generating new risks, the most notable of which being asset stranding, which threatens to erode value or turn assets into liabilities.

This is particularly relevant to the energy sector, with renewable energy and energy storage technologies making large strides in achieving cost and efficiency parity with fossil fuel-based electricity generation. According to the International Renewable Energy Agency, the cost of utility-scale solar photovoltaic energy fell 82 percent between 2010 and 2019, while new solar and wind projects are already cheaper than existing coal-fired power plants in many regions and new coal plants in all major markets.[2] As a result, global coal power capacity has fallen for the first time on record, with more generators being shut down than commissioned in the first half of 2020.[3] The rise of renewables is even threatening to strand assets in other infrastructure subsectors, such as freight rail tracks that exclusively transport coal to power plants.[4]

The competitive pressures being generated by other new or emerging innovations are also impacting assets in the evolving transportation landscape. The growing prevalence of ride-hailing services has depressed public transportation ridership in the US, with an estimated decline of between 1.29 percent and 1.7 percent per year since 2010.[5] Now, amidst the COVID-19 pandemic, commuter rail, toll roads, and international air travel have been rendered less essential by the rapid adoption

Technological advances have lowered the traditionally high barriers to entry for infrastructure services previously regarded as monopolistic in nature

of remote working technologies and shifting work practices.[6] These trends concurrently pose a two-pronged threat to the monopolism and essentiality of many assets in the subsector.

Exhibit 2 below provides an overview of some of the key pressures facing incumbent infrastructure service providers.

Exhibit 2. Technology-driven competitive pressures facing select infrastructure assets

		Is traditional service still:	
Traditional service	**Tech-driven disruptor**	**Essential?**	**A monopoly?**
Fossil fuel-based electricity generation	Renewable energy	Yes	No; genuine alternative available
Centralized electricity distribution via national- or state-level grid	Distributed energy generation	Less essential, especially in the medium term	Yes
Commuter travel (including light rail and toll roads)	Ride-hailing/last mile mobility Remote working technologies	Not essential for all, but still required for many	No; genuine alternatives available
Freight transportation (including airport, seaport, heavy rail)	3D printing (potentially, though limited short-term impact expected)	Yes	Yes

Source: Marsh & McLennan Advantage

HEIGHTENED STANDARDS OF ACCOUNTABILITY

Infrastructure owners and operators have always had to earn their license to operate, either via regulatory approval or by gaining the trust of the communities they serve and the governments they do business with. However, the speed of innovation and the rapid integration of new technologies into infrastructure assets are exposing them to new expectations across two areas of accountability:

- **Data stewardship.** The collection and analysis of personally identifiable information (PII) through connected and networked assets is raising questions over data privacy and security. For instance, data governance concerns have long plagued smart city initiatives.[7]
- **Artificial intelligence (AI) governance.** Automation is escalating fears over "unexplainable" technological "black boxes" that can create structurally faulty assets or deliver unethical (for example, gender- or racially biased) outcomes without disclosing the source inputs and algorithms and methods through which they derive their outputs. There have been fears that algorithmic bias could result in discriminatory service provision from utilities, which could result in energy or water scarcity in developing countries.[8]

The emergence of sophisticated and powerful tools has elevated public awareness of the pitfalls of technology use and invited greater scrutiny of companies and their activities. Investors can expect significant implications for their operations henceforth:

- **A stricter regulatory landscape.** Margin-squeezing or efficiency-hampering regulations as governments move to impose stricter accountability standards.[9]

- **Greater reputational risk.** Exposure to reputational risks as the integration of technology into infrastructure assets increases owners' and operators' responsibility for ethical behavior.

Owners and operators who are not conscientious in their use of technology are at risk of incurring regulatory penalties or reputational damage from potential failures of accountability or public fallouts. These risks are further complicated by the fact that penalties and public concerns vary by country or state, presenting an additional layer of complexity.

For example, pertaining to data stewardship, the rising use of intelligent transportation systems in road infrastructure for regulatory compliance will impose new capex and opex costs on owners and operators of toll roads, while the emergence of data protection laws around commercial data privacy may restrict capabilities and reduce revenue for building information modeling-based construction projects. Beyond such regulatory constraints, investors may also find themselves at risk of reputational damages from data breaches through cyberattacks against their own operations or the technology firms with which they have partnered.

Additionally, legislation and guidance on AI governance may increase costs for assets incorporating AI-powered automation capabilities; the additional measures and processes that these demand may be expensive or difficult to implement.[10] Profit-driven misdemeanors may also draw intense scrutiny: Firms may be tempted to use consumers' PII for purposes beyond those originally proffered or pursue controversial avenues of revenue maximization — such as with energy trading algorithms that redirect electricity production away from impoverished, vulnerable areas.

The emergence of sophisticated and powerful tools has elevated public awareness of the pitfalls of technology use and invited greater scrutiny of companies and their activities

WIDENING CYBER RISK EXPOSURE

Two factors are escalating cyber risk exposure in the infrastructure sector. First, the digitalization of asset design, construction, operation, and maintenance processes has expanded the risk profile of infrastructure assets — beyond information technology (IT) and data security concerns — to include operational technology (OT) risks around device monitoring, management, and control as well.

Second, while individual assets have always been physically connected to larger ecosystems, they are now linked to stakeholders — such as customers, suppliers, peers, partner organizations, and local authorities — through interconnected networks. The interdependencies of digital networks and supply chains further exacerbate assets' cyber vulnerabilities by providing threat actors with multiple avenues of attack.

These two trends are exposing infrastructure assets to a range of cyber threats that often differ drastically in their scope and consequences (see Exhibit 3 on the next page).

Exhibit 3. Overview of cyber threat incident types with hypothetical examples

Data breach: Own data Theft of airport digital twin data containing critical information on security blind spots or infrastructural vulnerabilities that nefarious agents may exploit	Data breach: Customer Unauthorized access to or theft of utility or telco customers' personally identifiable information	Inadvertent disruption of third-party system Transmission of malware to customers' personal devices by infected or compromised airport digital systems
Operational technology malfunction Malicious remote manipulation of smart grid controls, causing power outages and service disruptions	Disruption at external service provider Disruption to cloud digital services preventing ports from accessing customer database and order tracking system	Deletion or corruption of data Malware used to delete or disable access to historical temperature data at power plants, disrupting safety algorithms and potentially causing overheating
Encryption of data Ransomware impedes access to critical data by rail operator until ransom is paid, disrupting passenger services or inhibiting station traffic control systems	Network outage Distributed denial-of-service attacks on telco operator servers, interrupting digital services such as internet or mobile network connectivity	Cyber fraud Theft of telecom services through fraudulent manipulation of financial transactions or illegal access to private networks

Source: Marsh & McLennan Advantage

Cyber risk is amplified for critical infrastructure assets, which are prize targets of hackers: High-profile disruptions not only tend to yield larger ransoms for cybercrime organizations, but may also enhance the hackers' notoriety, granting them leverage for greater gains in future attacks. Approximately 50 percent of IT security professionals worldwide deem their country's critical infrastructure susceptible to cyberattacks, with electric power being the most vulnerable subsector.[11]

Some threat actors focus their activities on localized denial-of-service attacks. A US-based natural gas facility shut down operations for two days in February 2020 following a ransomware attack that infected both its IT and OT networks, although the hacker never gained access to critical operational controls.[12] It is worth noting that the real economic damage in such incidents stems not from ransom payments, but from taking business offline and foregoing the benefits that electronic systems generate.[13]

Malicious attempts to manipulate OT systems can lead to potentially disastrous results for cities or even nations. Iran was linked to a thwarted cyber intrusion aimed at disrupting water supplies in Israel in April 2020. Hackers reportedly sought access to systems that control water flow and wastewater treatment, targeting the programmable logic controllers that operate and regulate water distribution and treatment processes.[14] A month later, Israel in turn was linked to a cyberattack that halted Iran's Shahid Rajaee port for days, creating miles-long traffic jams and backups on connected waterways.[15] State-sponsored cyberattacks that target OT controls can devastate populations or even destabilize societies, presenting a very different risk proposition to infrastructure owners and operators as compared to more financially motivated attacks.

KEY IMPERATIVES FOR INVESTORS

In the face of disruption, investors and operators have to build technological agility by developing new skills, adapting their operations, and adopting a long-term perspective in order to respond to challenges and remain competitive.

Success in this new reality requires infrastructure businesses to mitigate new risks and capitalize on emerging opportunities. These demands in turn generate three key imperatives:

1. **Build core capabilities.** New innovations will test the technological capabilities of organizations. Investors and operators must hence identify the core capabilities they require, determine their organization's needs, and then decide whether to fulfill these needs in-house or via partnerships.
2. **Optimize existing assets.** Investors and operators seeking to maintain a competitive edge and maximize returns on investment must apply technology to their current assets to achieve greater cost savings, efficiency, safety, security, and sustainability.
3. **Keep an eye on the horizon.** Legal rulings and opinions can change quickly, so active monitoring of the social, legal, and physical domains relevant to emerging technologies is crucial for ensuring investment success.

BUILD CORE CAPABILITIES

To be successful in the face of technology-driven challenges, stakeholders must first identify the core technological capabilities that their businesses require. They must then determine the organizational competencies — skillsets, software, or hardware — that they are still lacking. Finally, they must decide upon the appropriate means by which to fill those gaps and complete their digital journey.

Identify Technological Capabilities

The first question for organizations seeking to build technological competency is: What capabilities will be required for the firm to realize its digitalization strategy?

From an investor perspective, infrastructure investments benefit when the firm possesses a level of expertise and the right set of tools. One core capability might be an agile investment strategy capable of responding to new developments in the infrastructure or technological landscape. Another might be a well-balanced portfolio, with robust risk management mechanisms, that is capable of managing disruption from new market entrants or shifting consumer preferences.

Additionally, there has been a drumbeat among stakeholders for greater transparency, particularly in terms of environmental, social, and corporate governance (ESG) metrics. To improve their reporting processes, investors may wish to harness the increased volume, granularity, and speed of data collection being enabled by new software and hardware tools.

Meanwhile, for asset operators, it is critical to overcome implementation challenges when applying new technologies to achieve greater cost savings, efficiency, safety, security, and sustainability (see **Optimize Existing Assets**). A central capability for many firms should moreover be the ability to accurately identify and efficiently procure emerging technologies with the highest likelihood of generating a substantive competitive advantage for early adopters.

Determine Organizational Needs

Having identified their desired core capabilities, businesses should then determine their organizational needs based upon those capabilities that they still lack. Investors may want to consider their needs through a predominantly portfolio-based lens, while operators may prefer an asset-specific lens. Exhibit 4 explores a selection of technology-related organizational needs as viewed through the two lenses.

Exhibit 4. Selected technology-related organizational needs viewed through different lenses

Organizational need		Portfolio lens	Asset lens
People	Leadership	Leaders with the ability to navigate tech-driven short- to medium-term investment and divestment decisions; fund managers who can convince investees to support technology strategy	Leaders with the ability to convince the relevant public sector authorities of end user value-add from adopting technology, particularly for critical infrastructure assets
	Talent	Investment teams bolstering existing acquisition and industry capabilities with specialist knowledge and understanding of technology	Employees capable of operationalizing technology in, for example, maintenance activities
Intelligence	Knowledge	Readily available intelligence on latest developments in technology and infrastructure, including changes in global and regional regulations or customer needs and wants	Specialists to oversee the execution and maintenance of technical systems; legal and compliance experts familiar with local requirements
	Data analytics	Big data and advanced analytics to support efficient data capture, information sharing across portfolio companies, portfolio management, and reporting processes (such as for ESG metrics)	Analytics staff to drive asset efficiency improvements by harnessing asset and customer statistics; modern and potentially automated databases, systems, customer experience, and reporting tools
Risk	Enterprise risk management	Top-down, macro-level portfolio risk analytics, including concentration risks, with tools for rebalancing and hedging	Bottom-up risk identification processes for technology-driven issues, with associated granular plans for mitigation at asset level
	Cybersecurity	Robust measures to safeguard information technology systems and sensitive data, including response protocols; strong data governance policies with trained workforce	Strong operational technology defenses, with sufficient protections against intrusions of critical systems and controls, alongside solid incident response plans

Source: Marsh & McLennan Advantage

Select Fulfillment Strategy

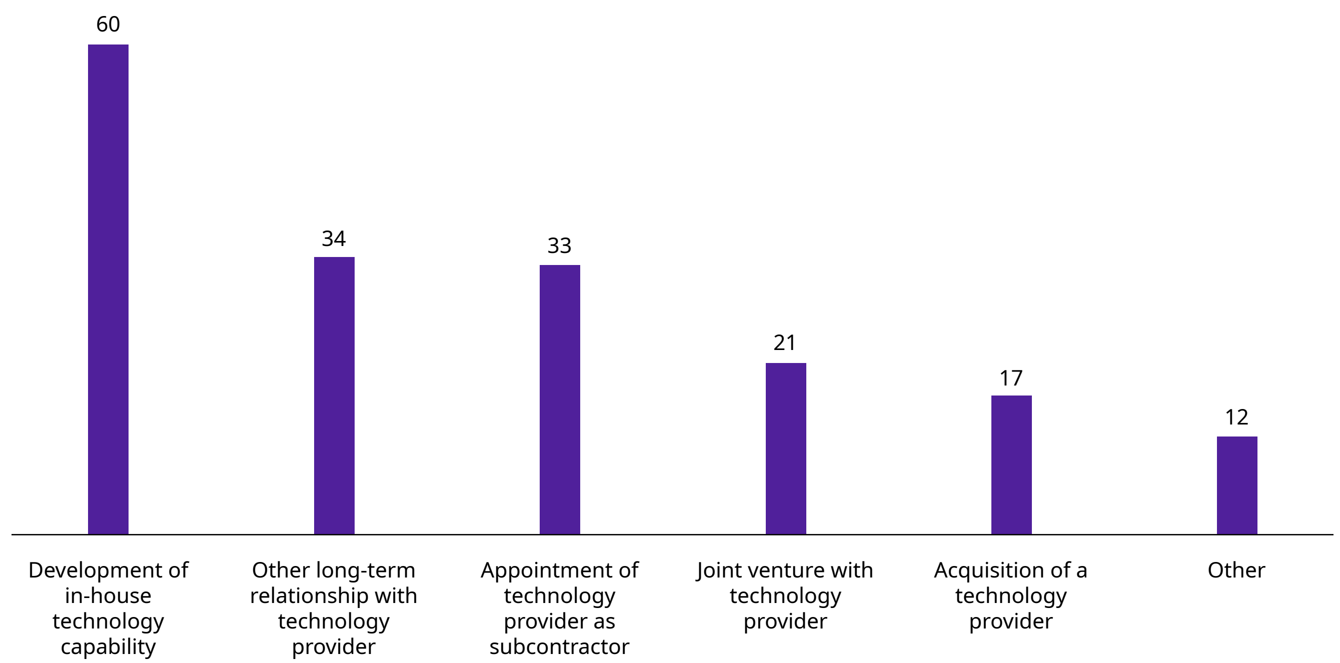
Investors and operators should conduct systematic cost-benefit analyses of the available choices before committing to a given strategy or suite of strategies.

Leading infrastructure companies have been exploring a range of options, from fully in-house to entirely external solutions, for executing their digital transformation (see Exhibit 5). A majority favor developing in-house capabilities so as to drive growth, increase productivity, and attract talent, while a smaller group expects to subcontract their technology needs to an outside provider or enter into some other long-term relationship with external vendors.[16]

Exhibit 5. Range of options for building technological capabilities

How (if at all) is your company expecting to engage with technology providers to deliver the digital transformation of infrastructure over the next five years?

Percent of respondents



Source: Pinsent Masons 2020 Global Infrastructure Survey

Investors and operators should conduct systematic cost-benefit analyses of the available choices before committing to a given strategy or suite of strategies

Exhibit 6 provides an overview of some of the key factors that infrastructure players should take into account in determining the trajectory of their digital transformation. Investment firms might first and foremost want to consider operating size, budget, and assets under management in making their technology decision: It may be more prudent for smaller firms to engage external vendors and consultants, whereas larger ones may be able to assemble an in-house digital team to drive the digital agenda across their entire portfolio.

Operators should similarly evaluate if their budget will permit them to hire in-house programmers and develop proprietary systems and platforms or if they would be better off contracting vendor-managed solutions.

Exhibit 6. Selected decision-making considerations around building technological capabilities

	Size and budget	Risk appetite	Existing skills and resources	Nature of underlying asset
Portfolio lens	• Opportunity to flexibly and fluidly leverage skills across the portfolio may make it more cost-effective to bring capabilities in-house • When and how best to integrate technology specialists into teams of investment and industry specialists	• Competitive value of being a first adopter of new technology, as opposed to waiting for it to be tried and tested and potentially cheaper • Value of investing in or acquiring technology startups to bolster internal processes, based on projected returns on investment	• Skillset and technical knowledge of fund managers, analysts, and support staff • Receptiveness of infrastructure management teams to external experts versus in-house specialist colleagues • Potential for external talent to complement in-house skillsets	• Extent to which the capability is aligned to core business objectives; firms may prefer to outsource noncore capabilities
Asset lens	• Operating budget, revenue growth, and customer base will determine the feasibility of directly hiring technology specialists, such as analysts and programmers, over engaging an external vendor	• Suitability of a given technology to existing workflows; firms must determine utility and feasibility of implementation, particularly where a systemic overhaul may be necessary to properly digitalize operations • Additional cyber risk inherent to technology partnerships • Potential reputational risk when engaging third-party providers, particularly for critical infrastructure	• Adaptability of existing staff and personnel to new digital tools and systems • Limitations of existing in-house skillsets • Legal, cultural, and social implications of outsourcing work or adopting automated solutions that displace jobs	• Permissions or allowances within service contracts to bring external parties into operations and processes, especially for critical infrastructure

Source: Marsh & McLennan Advantage

OPTIMIZE EXISTING ASSETS

Investors and operators must consider all avenues for optimizing their existing assets. At the asset level, there are many ways in which new and emerging innovations can be applied to activities including core operations, maintenance, and customer engagement. New investments can be costly, however, and also come with a degree of risk: either in selecting the wrong option entirely or from implementation obstacles within a workforce. Therefore, it is essential to understand the range of relevant technologies, their use cases and benefits, and their substitutes and costs when making investment decisions.

There are other considerations for investors with a portfolio-wide perspective. They should identify potential synergies, either in the form of economies of scale or from sharing experience across management teams and ensuring that future investment decisions are made on a well-informed and risk-adjusted basis.

Exhibit 7 showcases a range of technologies being utilized across infrastructure subsectors and highlights their key benefits. A selection of notable use cases follows the exhibit, although it is important to understand that a single asset can utilize many different technologies at the same time.

Exhibit 7. Benefits of integrating technology into selected infrastructure assets

	Artificial intelligence and machine learning	Digital twin	Distributed ledger	Intelligent transportation systems	Remote asset monitoring and maintenance	Robotics	Sensor-based monitoring technology
Cost savings	Minor or indirect benefit(s)	Minor or indirect benefit(s)	Minor or indirect benefit(s)	Not applicable	Minor or indirect benefit(s)	Minor or indirect benefit(s)	Minor or indirect benefit(s)
Efficiency	Most significant benefit	Most significant benefit	Minor or indirect benefit(s)	Most significant benefit	Most significant benefit	Most significant benefit	Most significant benefit
Safety	Secondary benefit(s)	Secondary benefit(s)	Not applicable	Minor or indirect benefit(s)	Minor or indirect benefit(s)	Minor or indirect benefit(s)	Minor or indirect benefit(s)
Security	Minor or indirect benefit(s)	Minor or indirect benefit(s)	Most significant benefit	Not applicable	Minor or indirect benefit(s)	Not applicable	Secondary benefit(s)
Sustainability	Secondary benefit(s)	Minor or indirect benefit(s)	Secondary benefit(s)	Secondary benefit(s)	Secondary benefit(s)	Secondary benefit(s)	Secondary benefit(s)

Not applicable · Secondary benefit(s) · Minor or indirect benefit(s) · Most significant benefit

Source: Marsh & McLennan Advantage

Artificial intelligence and machine learning

Infrastructure firms are adopting AI and machine learning (ML) solutions to generate benefits across a range of business processes. The Vermont Weather Analytics Center is one example. Established by the Vermont Electric Power Company to address intermittency and congestion at their wind farms, it uses an ML-driven forecasting system that tracks clouds and wind gusts to generate energy demand forecasts.[17] The system has reduced energy forecasting errors by 6 percent for solar and nine percent for wind.

Elsewhere, AI-powered analytics promises to revolutionize data volume management in telecommunications: Chinese firms are developing an AI- and ML-powered platform that uses user tags and usage record information to predict network utilization in real time. The platform reduced the strain on telco operator support systems by 63 percent in initial trials.[18]

Digital twin technology

Digital twin technology is helping infrastructure firms optimize their operations, particularly through reducing costs and bolstering efficiency. Alstom is using a digital twin model to enable predictive maintenance for the West Coast Main Line in the United Kingdom,[19] allowing the company to amass complex and up-to-date data on the positioning of its railroad fleet and then use that information to optimize the scheduling of fleet maintenance. The system has reduced expenses, optimized maintenance processes, and enabled the firm to run scenario simulations anticipating possible damage or loss events.

Meanwhile, among utilities, General Electric Renewable Energy's digital twin wind farm integrates models that measure and predict asset health, wear, and performance, allowing operators to optimize assets for efficiency and reliability. The twin was originally expected to boost energy production by up to 20 percent and create US 100 million in extra value over the lifetime of a 100-megawatt farm;[20] in 2019, the company reported that the model has increased megawatt-hour output by five to seven percent.[21] Although the technology is nascent, it has the potential to support the overall condition of assets and bolster their longevity.

Remote asset monitoring and maintenance

Remote asset monitoring and maintenance tools are producing outsized gains in efficiency, cost savings, and safety. Some solutions provide newfound back-end analytical capabilities that directly enhance existing monitoring systems. In 2018, Severn Trent created an AI model that identifies, locates, and manages water pipeline leaks, cutting the time it takes to find leaks by more than 50 percent and reducing leak incidence rates by over 16 percent in pilot tests.[22]

Other devices, such as unmanned aerial vehicles, are expected to completely transform frontline asset maintenance operations while cutting costs and improving employee safety. AT&T has used drones to test and improve distributed antenna system networks at football stadiums.[23] Typically, a connectivity analysis and testing operation can take 10-15 employees up to five days to complete; by using drones, AT&T shortened the process to four hours while improving worker safety and saving on tower climb costs, which average between $2,000 to $5,000 per inspection. In the utilities sector, wind turbine inspections cost around $1,500 per tower; using a drone cuts the cost in half.[24] Additionally, utilities can improve energy production based on more granular data from drone inspections; one solar generator estimated $42,000 in additional revenue resulting from repairs that manual inspections typically miss.[25]

Exhibit 8 on the next page illustrates the many benefits of extensive yet strategic technology integration through the example of the airport industry, which has dramatically transformed numerous areas of operation over the last decade.

Digital twin technology is helping infrastructure firms optimize their operations, particularly through reducing costs and bolstering efficiency

Exhibit 8. Notable technological transformations in the airport sector circa 2010-2020

Operation	~2010
Air traffic control	• Standard operations conducted in ATC tower with direct view of airport runways • Cameras used to track airplane and ground vehicle movement under the supervision of an operational management team
Baggage delivery	• Baggage transferred using standard conveyor belts and a tug and trolley system • Manual baggage collection by passenger at terminal building
Baggage processing	• Manned check-in desks; bag drop services only available within terminal building • Bags tagged using barcodes, which are prone to damage and "no-read" issues
Biometrics	• Agents manually process passports and boarding passes at check-in desk
Terminal maintenance	• Inspections involve direct, in-person assessments of facilities and assets
Travel retail	• Retail concessions are the primary source of nonaeronautical revenue • Customers can only shop in person at retail outlets within terminal buildings
Security	• Backscatter X-ray devices for both baggage and passengers, which are subject to human error and health concerns over exposure to ionizing radiation

Operation	~2020	Cost saving	Efficiency	Safety	Security	Sustainability
Air traffic control	**Sensor-based remote controller operations** conducted from a distant location		✓	✓		
	Digital twin technology used to manage daily operations and monitor vehicle flows	✓	✓	✓	✓	✓
Baggage delivery	**Autonomous robots or vehicles** can deliver baggage		✓	✓	✓	✓
	Baggage delivery can be **outsourced**, with service to homes, hotels, and more		✓			
Baggage processing	**Automated bag drop facilities** with multiple drop locations	✓	✓			✓
	Bags tagged using **radio-frequency identification technology**			✓	✓	
Biometrics	**Automated facial and fingerprint recognition** systems		✓	✓	✓	✓
	Self-operated curb-to-gate **biometric screening terminals**		✓			
Terminal maintenance	**Unmanned aerial vehicles**, such as drones, support maintenance inspections and operations	✓	✓	✓	✓	✓
Travel retail	Growing use of **digital travel retail platforms**, like AOE's Omnichannel Multi-Merchant Marketplace (OM3), to improve customer conversion rate through reduced waiting times, personalized real-time information via apps, and flexible transaction options	✓	✓			
Security	**AI- and ML-powered millimeter wave scanners** used to speed up security check processes as well as reduce errors and potentially harmful health effects		✓	✓	✓	

Source: Marsh & McLennan Advantage and Oliver Wyman analysis, press

KEEP AN EYE ON THE HORIZON

It can be challenging for investors and operators to initiate long-term plans around emerging technologies given that the technological landscape is in constant flux, shaped by rapid and unexpected shifts in technical possibilities, consumer preferences, and regulatory frameworks. The environment for new solutions can vary dramatically, and the success of their implementation will rely on social, legal, and physical conditions often not within the control of businesses.

Amidst this uncertainty, firms cannot afford to become paralyzed by indecision. It is important to keep an eye on the horizon, monitoring emerging innovations, identifying areas of risk, and taking action after having considered opportunities on a risk-adjusted basis.

The following case studies illustrate some uncertainties that organizations need to consider when assessing new technologies (see Exhibit 9).

Exhibit 9. Selected examples of technology-driven uncertainties in the infrastructure sector

Technology	Smart city infrastructure	Autonomous vehicles (AVs)	5G
Reputational risks	**Data governance** concerns	Consumer confidence in **safety and reliability**	**Health risk** of EM field exposure, **public cost** of rollout, **environmental impact** of infrastructure
Regulatory uncertainty	**Consumer protection, labor contracts, fair competition**	**Safety, accident liability, privacy, security**	**Spectrum auctions, infrastructure deployment, network sharing**
Geographical limitations	**Technical** and **financial suitability** for low- to middle-income countries	**Reliability** outside test environments, **replicability** in adverse weather or road conditions	**Scalability** in sparsely populated rural areas

Source: Marsh & McLennan Advantage

Smart city infrastructure

Smart cities collect and utilize large amounts of data to optimize processes. This, however, lends itself to public dissent and in certain cases outright opposition over privacy issues. Quayside, a proposed sustainable smart city project on Waterfront Toronto, was abandoned in 2019 after community leaders, activists, and academics launched a campaign over data governance and antidemocratic concerns.[26]

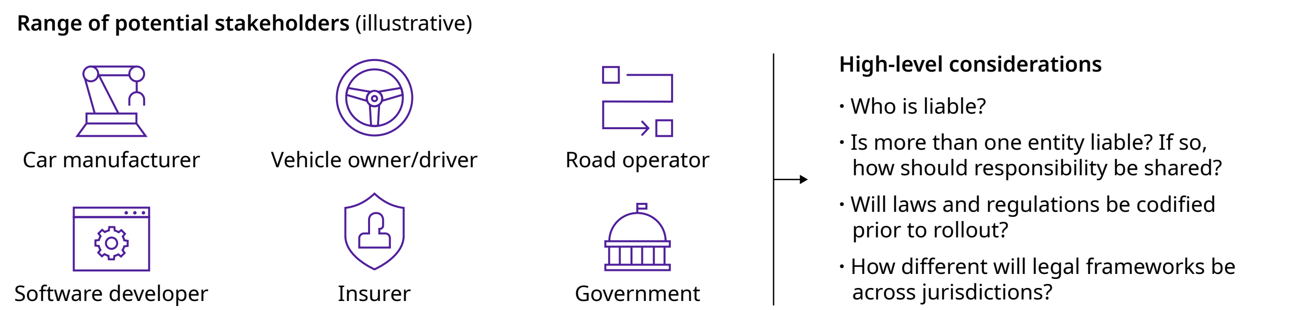
While there have been successful cases of smart city projects in recent years, such as the Fullerton FiberCity,[27] the OECD's 2020 review of smart city initiatives found member states to be lacking in regulatory frameworks that properly legislate for affordability, consumer protection, taxation, labor contracts, and fair competition.[28] Moreover, since smart city concepts are not standardized, infrastructure designs and plans have to account for local needs, introducing new costs and risks.[29]

Autonomous vehicles (AVs)

Although some major technology firms have confidently demonstrated the feasibility of AVs in recent years, test run fatalities have reignited doubts over the safety of fully driverless AVs, raising liability risks and potentially affecting revenue projections for owners and operators of assets such as toll roads.[30] Indeed, as of 2019, 71 percent of Americans were afraid of riding in fully autonomous vehicles.[31] Given the technology's nascence, AV regulatory frameworks are still weak. While jurisdictions recognize the need for strong legislation on autonomous driving at the international level,[32] regulations around safety, liability, privacy, and security are still in their infancy.[33] It is also likely that different entities will preside over regulations in different domains — local authorities might govern urban and suburban roads, whereas state- or federal-level authorities would manage highways and interstates — creating further legislative complexity.

The reliability of AVs on California and Nevada highways, where most tests are being conducted in the US, also may not translate to roads elsewhere;[34] moreover, adverse weather conditions or unsuitable road conditions could inhibit vehicle sensors. These uncertainties leave road operators and owners with questions over potential legal liabilities for accidents involving AVs — for example, if a road sensor malfunction were to cause a crash (see Exhibit 10).[35] Broader questions around the extent to which AV systems will rely on riskier vehicle-to-infrastructure interfaces with potentially larger impact scopes are also casting doubt on the investment value of AV-related infrastructure.

Exhibit 10. Present uncertainty over legal liability for AV accidents



*According to SAE International's Six Levels of Autonomy, only Level 5 vehicles require zero human input. Human control is legally mandatory up to Level 4; commercial AVs presently reach up to Level 3.[36]

Source: Marsh & McLennan Advantage

5G

The rollout of 5G hardware has been plagued by public concerns in some regions, with scientists expressing concern over the potential hazard that it poses to human health through increased exposure to wireless radiation: 5G requires new-generation small cell smart antennae every 60 meters to achieve its coverage and connectivity goals.[37] Notably, more than 50 percent of US consumers are uneasy about 5G's health, environmental, and financial impacts.[38] Such concerns will be important to the infrastructure sector moving forward as investors and operators scrutinize the investment potential of 5G and its underlying assets.

Regulatory uncertainty is also a growing concern with 5G rollouts already underway in many countries. The Global System for Mobile Communications Association (GSMA) argues that governments are not advancing 5G-specific regulatory changes quickly enough, particularly with regard to spectrum auctions, infrastructure deployment, access to site locations, network sharing, and power density.[39] Moreover, given that 5G utilizes high-frequency bands that trade off range for capacity such that more base stations will be required in a given area than in the 4G era, the technology could potentially wind up less scalable in sparsely populated rural areas such as certain parts of Africa or Southeast Asia.[40]

CONCLUSION

Continued innovations in data proliferation, connectivity, automation, and sustainability are transforming the infrastructure sector and subverting longstanding assumptions about traditional assets. It is therefore critical that infrastructure businesses recognize technology for the double-edged sword it is. On one hand, it is introducing new challenges in the form of an evolving competitive landscape, heightened standards of accountability, and widening exposure to cyber risk. On the other, it presents new opportunities that enterprising businesses would do well to capture.

While the sector's technological revolution has precipitated an era of ever-increasing demand and supply uncertainty, the need for new infrastructure across the globe continues to rise beyond the capacity of governments to fulfill alone. To bridge the infrastructure gap and answer the world's call for long-term, capital-intensive assets and services, the private and public sectors must work together to deliver infrastructure that is safe, affordable, and sustainable.

To play their part, private infrastructure businesses must keep pace with the latest technological developments. They must therefore strive to address three key imperatives moving forward: build core capabilities, optimize existing assets, and keep an eye on the horizon. These imperatives should serve as a starting point wherefrom firms can develop a comprehensive and coherent digital transformation strategy to navigate the technologically driven future.

ENDNOTES

1 Pinsent Masons. (2020, January 28). Changes needed to drive infrastructure's technology revolution. Retrieved January 8, 2021.

2 IRENA. (2020). Renewable power generation costs in 2019.

3 Shearer, C. (2020, August 3). Analysis: The global coal fleet shrank for first time on record in 2020. CarbonBrief. Retrieved January 8, 2021.

4 Gagan, O. (2019, March 21). Should investors be wary of stranded assets? Raconteur. Retrieved January 8, 2021.

5 Rapier, G. (2019, February 5). Uber and Lyft are having a terrible effect on public transportation, new research shows. Business Insider. Retrieved January 8, 2021.

6 The National Academies. (2020, September 8). COVID-19 Trends impacting the future of transportation planning and research. Retrieved January 8, 2021.

7 Barth, B. J. (2020, August 12). Death of a smart city. OneZero. Retrieved January 8, 2021.

8 Seoane, C. G. (2019, October 11). Why utilities adopting AI should put ethics first. Atos. Retrieved January 8, 2021.

9 Global Infrastructure Investor Association. (2020, November). The future of regulation.

10 Marsh & McLennan Advantage. (2020, November). Governing artificial intelligence: managing business risks in a digital world.

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

12 Cybersecurity and Infrastructure Security Agency. (2020, October 24). Alert (AA20-049A): Ransomware impacting pipeline operations. Retrieved January 8, 2021.

13 The Maritime Executive. (2017, June 28). Maersk's cargo operations hit hard by cyberattack. Retrieved January 8, 2021.

14 Warrick, J. & Nakashima, E. (2020, May 8). Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran. The Washington Post. Retrieved January 8, 2021.

15 Warrick, J. & Nakashima, E. (2020, May 19). Officials: Israel linked to a disruptive cyberattack on Iranian port facility. The Washington Post. Retrieved January 8, 2021.

16 See note 1.

17 Engerati. (2017, July 24). How is data supporting renewable integration? VELCO demonstrates. Retrieved January 8, 2021.

18 Wray, S. (2019, November). AI and edge computing trialled to reduce telco bill strain. TM Forum. Retrieved January 8, 2021.

19 Alstom. (2020). Alstom develops a rail network digital twin for railway yard design and predictive fleet maintenance. Retrieved January 8, 2021.

20 GE Reports. (2015, May 19). Wind in the cloud? How the digital wind farm will make wind power 20 percent more efficient. General Electric Power Conversion. Retrieved January 8, 2021.

21 Rook, B. (2019, April 22). How digital twins are transforming wind operations. Windpower Engineering & Development. Retrieved January 8, 2021.

22 Severn Trent. (2018, December 4). Severn Trent creates machine learning to help tackle leakage by filtering five billion data points. Retrieved January 8, 2021.

23 Culler, D. (2019, December 4). Telecom reaches new heights, cuts costs with drones. AGL Media Group. Retrieved January 8, 2021.

24 PowerTechnology. (2018, June 29). Technical innovations in wind power O&M. Retrieved January 8, 2021.

25 Wall, R. (2019, May 6). 8 Ways drones are lowering the cost of infrastructure inspection. Power Engineering. Retrieved January 8, 2021.

26 See note 7.

27 GIIA. (n.d.). Fullerton FiberCity. Retrieved January 8, 2021.

28 OECD. (2020). Smart cities and inclusive growth.

29 United Nations Economic and Social Council. (2016, February 26). Smart cities and infrastructure: Report of the Secretary-General [Item 3(a) of the provisional agenda]. Commission on Science and Technology for Development, Nineteenth session, Geneva.

30 Schmelzer, R. (2019, September 26). What happens when self-driving cars kill people? Forbes. Retrieved January 8, 2021.

31 American Automobile Association. (2019, March 14). Three in four Americans remain afraid of fully self-driving vehicles. Retrieved January 8, 2021.

32 Baker McKenzie. (2018). Global driverless vehicle survey 2018.

33 The Japan Times. (2020, June 26). Countries agree regulations for automated driving. Retrieved January 8, 2021.

34 Hancock, P. A., Nourbakhsh, I., & Stewart, J. (2019). On the future of transportation in an era of automated and autonomous vehicles. Proceedings of the National Academy of Sciences, 116(16), 7684-7691.

35 Topham, G. (2020, October 23). UK insurers warn against go-ahead for self-driving cars on motorways. The Guardian. Retrieved January 8, 2021.

36 Shuttleworth, J. (2019, January 7). SAE standards news: J3016 automated-driving graphic update. SAE International. Retrieved January 8, 2021.

37 The 5G Appeal. (2017). Scientists warn of potential serious health effects of 5G. Retrieved January 8, 2021.

38 Sykes. (2020, February). Survey report: Americans' perceptions of 5G technology. Retrieved January 8, 2021.

39 GSMA. (2020, March). Realising 5G's full potential: Setting policies for success.

40 Sbeglia, C. (2020, January 27). GSMA: "South Africa will lead the increase in 5G activity expected in sub-Saharan Africa." RCR Wireless News. Retrieved January 8, 2021.

AUTHORS

Blair Chalmers

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

Darrel Chang

Research Analyst
Marsh & McLennan Advantage
darrel.chang@oliverwyman.com

With special thanks to contributors from the Global Infrastructure Investor Association, including Lawrence Slade (Chief Executive Officer), Jon Phillips (Director, Corporate Affairs), and John Kavanagh (Head of Policy and Public Affairs).

Design by Daniela Romo

MARSH & MCLENNAN CONTRIBUTORS

Oliver Wyman: Saahil Malik, David Bornstein, Meghna Basu, Nicholas Tonkes

Marsh: Adrian Pellen, Andrew Birt, Martin Bennett

Marsh & McLennan Advantage: Richard Smith-Bingham, Leslie Chacko, Ben Hoster, James Sutherland, Chen Qi Hang, Samuel Koh

ABOUT MARSH & MCLENNAN COMPANIES (MMC)

Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's 76,000 colleagues advise clients in over 130 countries. With annual revenue of $17 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. Marsh advises individual and commercial clients of all sizes on insurance broking and innovative risk management solutions. 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 wellbeing 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 @mmc_global or subscribe to BRINK.

ABOUT THE GLOBAL INFRASTRUCTURE INVESTOR ASSOCIATION (GIIA)

GIIA is the membership body for the world's leading institutional investors. Since 2016 we have grown to around 75 members, including many of the leading fund managers, pensions funds, sovereign wealth funds and insurance providers, together with the leading professional advisors to the sector. We work with governments and other stakeholders to promote the role of private investment in providing infrastructure that improves national, regional and local economies and helps to tackle global challenges. GIIA members have investments in 1,500 assets, across 49 countries, totaling $780 billion of infrastructure assets under management.

This report and any recommendations, analysis or advice provided herein (i) are based on our experience as insurance and reinsurance brokers or as consultants, as applicable, (ii) are not intended to be taken as advice or recommendations regarding any individual situation, (iii) should not be relied upon as investment, tax, accounting, actuarial, regulatory or legal advice regarding any individual situation or as a substitute for consultation with professional consultants or accountants or with professional tax, legal, actuarial or financial advisors, and (iv) do not provide an opinion regarding the fairness of any transaction to any party. The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. We are not responsible for the consequences of any unauthorized use of this report. Its content may not be modified or incorporated into or used in other material, or sold or otherwise provided, in whole or in part, to any other person or entity, without our written permission. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Information furnished by others, as well as public information and industry and statistical data, upon which all or portions of this report may be based, are believed to be reliable but have not been verified. Any modeling, analytics or projections are subject to inherent uncertainty, and any opinions, recommendations, analysis or advice provided herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. We have used what we believe are reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied, and we disclaim any responsibility for such information or analysis or to update the information or analysis in this report.

We accept no liability for any loss arising from any action taken or refrained from, or any decision made, as a result of or reliance upon anything contained in this report or any reports or sources of information referred to herein, or for actual results or future events or any damages of any kind, including without limitation direct, indirect, consequential, exemplary, special or other damages, even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. No responsibility is taken for changes in market conditions or laws or regulations which occur subsequent to the date hereof.