OLIVER WYMAN

MRO SURVEY 2018

TACKLING INDUSTRY DISRUPTION

AUTHORS
Derek Costanza, Partner
Brian Prentice, Partner

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

ABOUT THE SURVEY

In its second decade, the Oliver Wyman annual MRO survey is an industry standard that samples the attitudes and strategies of executives from across aviation as they address key trends and emerging issues in the maintenance, repair, and overhaul (MRO) sector. Nearly 100 aviation professionals responded to the 2018 survey, with a mix across airline operators, captive airline MROs, independent MROs, and original equipment manufacturers (OEMs). Representatives from leasing organizations, financiers, parts distributors, and advisors rounded out the ecosystem of respondents. This year, 52 percent of respondents to the annual survey were senior executives – either in C-suite posts, vice presidents, or above; 78 percent were director level or above. The sample reflects views across major geographic markets, with North America representing 57 percent of inputs, Europe 25 percent, and Asia 11 percent. The balance came from Latin America, the Middle East, and Africa.

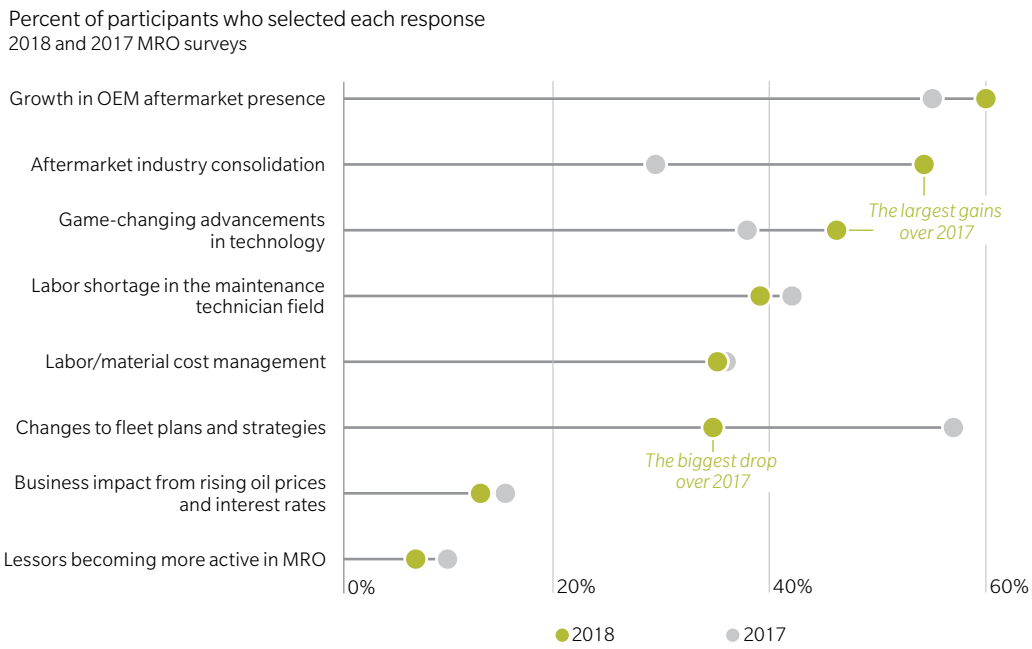
CONTENTS

EXECUTIVE SUMMARY

Another competitive year in the maintenance, repair, and overhaul industry is dawning, and the focus is once again on the quest for market growth by the aircraft, engine, and component manufacturers.

For the second straight year, respondents to Oliver Wyman's 2018 MRO survey ranked the escalating presence of original equipment manufacturers (OEMs) in the aftermarket as a top disruptor for the industry. While last year's survey participants were equally preoccupied by the rapid expansion of the global airline fleet, this year OEMs were seen as the number one disruptor (60%), followed closely by aftermarket industry consolidation (55%) – which in part is a result of heightened competition from OEMs. That category moved up 26 percentage points from last year – the most of any – when it ranked sixth among important disruptors. Another category on the move is the impact of game-changing technology – up nine percentage points; fleet expansion dropped 22 percentage points to sixth place.

Exhibit 1: Top MRO industry disruptors over the next five years



Source: Oliver Wyman analysis

Survey respondents also revealed more apprehension about the control some OEMs – particularly engine and component manufacturers – are exerting over intellectual property (IP) and the expectation that OEMs will leverage it to gain more market share. The marketplace is experiencing a rise in material costs connected in part to IP-ownership concentration, and survey respondents anticipate seeing even higher prices and more IP-propelled OEM market expansion in the near future. Seventy-eight percent of respondents expect OEMs to become the most dominant players in the industry over the next three years, and they also are convinced aircraft manufacturers will meet or approach their aggressive growth targets for aftermarket revenue within the next decade. In 2016, for instance, Boeing set a goal of tripling its aftermarket sales to $50 billion within a decade and created a dedicated global division that combined civil and military MRO services to elevate the activity within the corporate hierarchy.

Managing materials and labor costs in the face of tightening supply also persists as a challenge for all players. As last year's survey revealed, respondents believe the labor shortage among mechanics poses a serious risk to the industry and serves as the primary driver of labor cost pressures – twice as significant as any other factor. The retirement of maintenance technicians and a dearth of newly created ones to take their place are squeezing both ends of the workforce spectrum across the globe.

CYBER THREAT GROWS

Following several high-profile cyberattacks against large transportation and logistics companies, such as Maersk and FedEx, and the transportation infrastructure at major ports in 2017, Oliver Wyman decided to question industry players as part of the 2018 survey about their readiness to fend off hackers. In our Cybersecurity Special Report, we review survey findings that suggest a certain level of complacency, with many respondents unaware of efforts and investments by their companies in cybersecurity. The risk of breaches is real – as we've witnessed for more than a decade in industries from banking, to healthcare, to retail – and the threat is growing for the MRO industry as it strives to digitize. On March 15, the Department of Homeland Security sent out an alert that revealed Russian hackers have been conducting systematic attacks since 2016 on the US electric grid and various infrastructure industries, including aviation, for the purpose of collecting data on network design and control systems.

Any breach in global, interconnected industries like transportation and MRO can spread worldwide in a matter of hours. For this reason, Oliver Wyman believes it is imperative for the MRO industry as a whole to work together to strengthen its cybersecurity and risk management practices around digital operations. With the DHS announcement, cyberattacks on aviation have moved from a possibility to a reality.

SPECIAL REPORT

THE MRO CYBERSECURITY CHALLENGE

MORE DIGITIZATION, MORE TARGETS FOR HACKERS

A chain is only as strong as its weakest link, but in the case of cybersecurity many companies have a hard time identifying where their vulnerabilities lie. As the aviation maintenance, repair, and overhaul industry becomes increasingly digitized, the threat of a breach by hackers grows. While most companies in transportation have become more proactive about securing their own networks, a significant percentage admits to knowing little about the security profile and practices of third-party vendors with access to their systems, data, and components.

That lack of knowledge can lead to disaster as many major corporations have discovered over the past five years. In 2013, hackers used the stolen credentials of a heating, ventilation, and air conditioning vendor to penetrate the network of retail giant Target. They planted Russian-coded malware and stole the personal data of 70 million customers and information on 40 million payment cards. The cost to Target: close to $300 million. In 2014, stolen log-on credentials for a third-party vendor allowed hackers to pilfer data on 56 million credit and debit cards as well as 53 million customer emails at a cost of somewhere north of $180 million. And in 2015, the computer network of the US Office of Personnel Management was breached: 22 million records, including sensitive information on federal employees, contractors, and members of the military – some involved in undercover work – were stolen after hackers got their hands on the credentials of an outsourced background-check provider.

Globally, hacking has become a highly profitable industry, costing economies around the world more than half a trillion US dollars annually – a sum that has been increasing every year. In some countries, hackers work out of regular offices and get paychecks to spend their workday looking for vulnerabilities in organizations' digital networks, lying in wait for holes to develop through which they can penetrate and steal information or worse. Experts place the number of professional hackers at over 300,000 worldwide. In places like Russia, China, Eastern Europe, and North Korea, hacking has become a growth industry. Given the role transportation and aviation play in the global economy, the cyber war against a nation's infrastructure amounts to nothing less than a threat to national security.

On March 15, that danger became all too real with an alert from the United States Computer Emergency Readiness Team, a unit within the Department of Homeland Security (DHS),

warning of Russian state-sponsored hackers who have been systematically targeting the American electricity grid and major infrastructure industries, including energy, nuclear, water, aviation, and critical manufacturing sectors since at least March 2016.

Discovered through analytical work by DHS and the Federal Bureau of Investigation (FBI), the breaches were characterized as part of a "multi-stage intrusion by Russian government cyber actors." The hackers "appear to have deliberately chosen the organizations they targeted, rather than pursuing them as targets of opportunity," and once inside, "sought information on network and organizational design and control system capabilities."

THE SECURITY OF THE AVIATION INDUSTRY IS A MATTER OF NATIONAL SECURITY FOR ALL COUNTRIES

According to the forensic analysis, the initial points of entry were through "trusted third-party suppliers with less secure networks." DHS used the Lockheed-Martin Cyber Kill Chain model to analyze, discuss, and dissect the malicious cyber activity.

TARGETING INFRASTRUCTURE

And this is just the latest brazen assault against infrastructure. While cyber criminals were initially motivated by the money that could be made off stolen data, recent breaches seem more intent on creating organizational chaos. In June 2017, hackers – believed by the CIA and UK intelligence to be Russian military – attacked the Ukraine with software that literally wiped out data and disrupted operations in that country's banking system, government ministries, metro, and at the former Chernobyl nuclear power plant.

From there, the wiper ransomware, named NotPetya, infected computer systems around the world, including those of Danish shipping conglomerate Maersk. This led to serious delays at major ports like Rotterdam, Mumbai, and the Port of New York and New Jersey and the temporary shutdown of the largest terminal at the port of Los Angeles. The episode ended up costing Maersk alone close to $300 million. FedEx's TNT Express suffered a similar loss as another NotPetya victim. It is attacks like these that should prompt transportation companies to reassess their level of cyber preparedness.

Oliver Wyman believes several factors make the MRO industry a prime target, with dire implications equaling or potentially exceeding those witnessed already in other industries. First, industry players have access to the networks of the world's airlines and original equipment manufacturers (OEMs), including major aircraft companies and engine and component-parts makers. While the carriers and OEMs may sometimes be the ultimate targets of the cyber criminals, hackers may decide that access through a vendor in the MRO supply chain may be easier to achieve. That makes all the members potential targets – even and perhaps especially small ones that don't have the cyber preparedness of larger organizations.

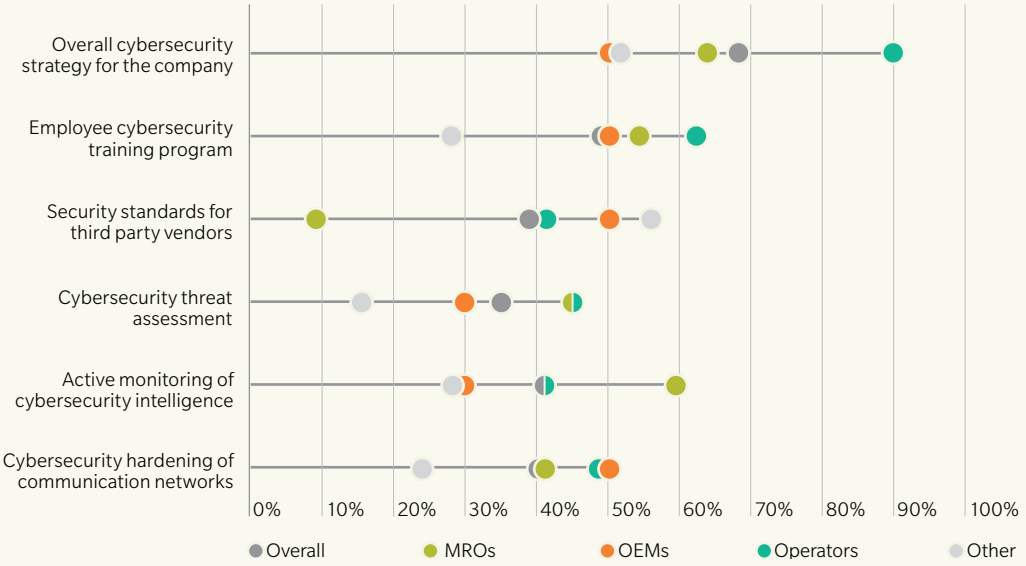
Second, MRO providers operate across the globe, which makes MRO companies more vulnerable to regional disparities in security and ultimately an attractive mark for hackers looking to cause maximum, cross-border disruption. Third, the industry is highly interconnected in its operations, interacting on a daily basis with most segments of the value chain, but maintaining a variety of approaches to cybersecurity. Finally, as the industry becomes increasingly digitized, potentially unsecured access points to systems and data are created and not always protected. This is aggravated by the fact that it becomes difficult to document all the hands that might come in contact with the multitude of components and software moving around the system on a daily basis, meaning the perpetrator may be several steps removed from the ultimate destination.

MORE CONCERNED THAN PREPARED

In Oliver Wyman's 2018 MRO Survey, we sought to determine the extent to which cybersecurity is prioritized. While the majority of companies show an appropriately elevated level of concern, the survey also reveals considerable variability in levels of preparedness, which creates the potential for weak links in the supply chain. For instance, a high percentage admitted they had not investigated the vulnerability of third-party vendors: Only nine percent of MROs, 50 percent of airframe, engine, and component manufacturers, and 41 percent of airlines (operators) have established security standards for third-party vendors.

Exhibit 2: Which cybersecurity safeguards has your company implemented?

Percent of total respondents who selected each response for each segment



Source: Oliver Wyman analysis

Other troubling statistics show that less than half of those surveyed – across MROs, OEMs, and operators – have conducted a cybersecurity threat assessment, with only 30 percent of participating OEMs saying they have done one. On a positive note, more than half of the OEM, MRO, and operator categories say they have an overall cybersecurity strategy in place and have conducted employee cybersecurity training. For the airlines, for instance, an impressive 90 percent have developed a strategy, and 62 percent have trained employees.

CYBERSECURITY AUDITS

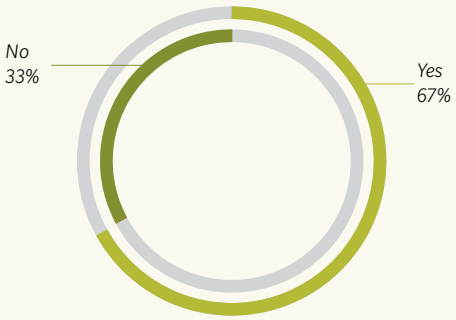
The responses on training are encouraging, given that human error or lack of knowledge about good cyber practices can lead to mistakes like neglecting to install a software patch or responding to so-called phishing emails that can infect a company's network with malware. These small slips are often responsible for a company's cyber woes and can result in massive damage. In 2017, consumer credit agency Equifax suffered a data breach that exposed the personal and financial data of more than 143 million Americans in part because someone simply failed to install a patch developed to fix a software glitch that made Equifax's system vulnerable to attack.

About two-thirds of respondents indicate their companies are prepared for the growing cybersecurity threat. Yet, less than half had conducted a review of cybersecurity risk in operations and maintenance in 2017, with one-fifth saying such an audit was not conducted and one-third saying they didn't know whether or not one had been.

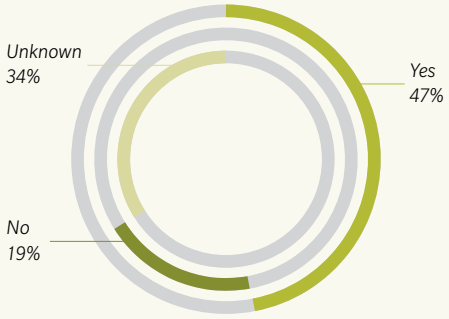
One of the biggest vulnerabilities revealed by the survey shows up in responses from survey-takers in the category labeled Other, which is made up of smaller third-party

Exhibit 3: HOW PREPARED IS THE INDUSTRY?

IS YOUR COMPANY PREPARED TO HANDLE CYBER THREATS?



DID YOUR COMPANY CONDUCT A CYBERSECURITY REVIEW IN 2017?



Source: Oliver Wyman analysis

providers such as finance companies and lessors, parts distributors, professional advisers, and R&D funding agencies. Here, the percentages performing cybersecurity training for employees (28%), cybersecurity threat assessment (16%), hardening of the communication networks (24%), and monitoring of cybersecurity intelligence (28%) were the lowest of all the categories. Yet, these businesses could provide the exact type of backdoor-entry hackers often attempt to get to big organizations. The only activity in which the "other" group outperformed all the other categories was in requiring security standards for third-party vendors (56%).

IN THE CYBER ARMS RACE, THE PERPETRATORS OF CYBERATTACKS ARE NOT STANDING STILL

STEPS TO PREPAREDNESS

To achieve a comprehensive, unified cybersecurity and risk management strategy for the industry, MRO providers should seriously consider taking several actions. First, companies within the industry should conduct independent audits of existing cybersecurity programs. This includes looking at everything from understanding who and what have access to a company's computer network, to whether a real-time detection process and response mechanism have been delineated, to which managers are responsible for each phase of executing cybersecurity protocol, to whether an oversight process exists to ensure procedures are followed and documented.

The industry as a whole also needs to develop a clear framework for mitigating and managing cyber risks. The National Institute of Standards and Technology (NIST) has developed a set of industry-specific standards and best practices intended to be leveraged in designing such a cybersecurity framework. Companies can begin by using the NIST Cybersecurity Framework which views the organization across five phases – Identify, Protect, Detect, Respond, and Recover.

Any cyber risk management system must include certain key elements:

- **Creating infrastructure** that ensures a company has the appropriate detection and monitoring tools;
- **Establishing a process** that guarantees the right procedures are being followed correctly;
- **Developing an organization** that identifies roles and responsibilities and building in oversight; and
- **Documenting all phases** of the strategy to ensure that there are checkpoints to prevent procedures falling through the cracks.

Finally, the industry must work across companies to fortify their information technology systems – both infrastructure and upkeep – and create a security-minded culture. While no solution is guaranteed to avert any and all attacks, developing a holistic approach to the risk management of cybersecurity that's shared across the industry – and updating it regularly – may give companies a leg up. Certainly, cyber criminals aren't standing still.

MRO SURVEY RESULTS

THE FUTURE OF THE AFTERMARKET

THE INDUSTRY'S OEM PREOCCUPATION

For the past several years, aircraft, engine, and component manufacturers have been increasing their role as MRO providers in the aviation aftermarket – a phenomenon that has been identified as a top disruptor by industry respondents in the past two Oliver Wyman MRO surveys.

The OEMs see the MRO sector growing quickly as the global fleet expands. At the 2016 Farnborough Air Show, Airbus projected a doubling of aftermarket spending – pushing it up to $3 trillion by 2035; the MRO portion would top $1.8 trillion, growing annually at a year-over-year 4.6 percent. Around the same time, Boeing set a daunting goal for itself of tripling its MRO revenue within a decade.

Accordingly, more than 75 percent of respondents indicated that the stated ambition of OEMs to aggressively expand in the aftermarket is credible and, in fact, a likely outcome. Most expect the OEMs to gain market share quickly over the next three years, in part because of the leverage they have over intellectual property (IP). This is primarily the case with engine and component manufacturers, but there is a fear that the aircraft OEMs may try to recapture more IP as they push into the aftermarket.

BRINGING IP IN-HOUSE

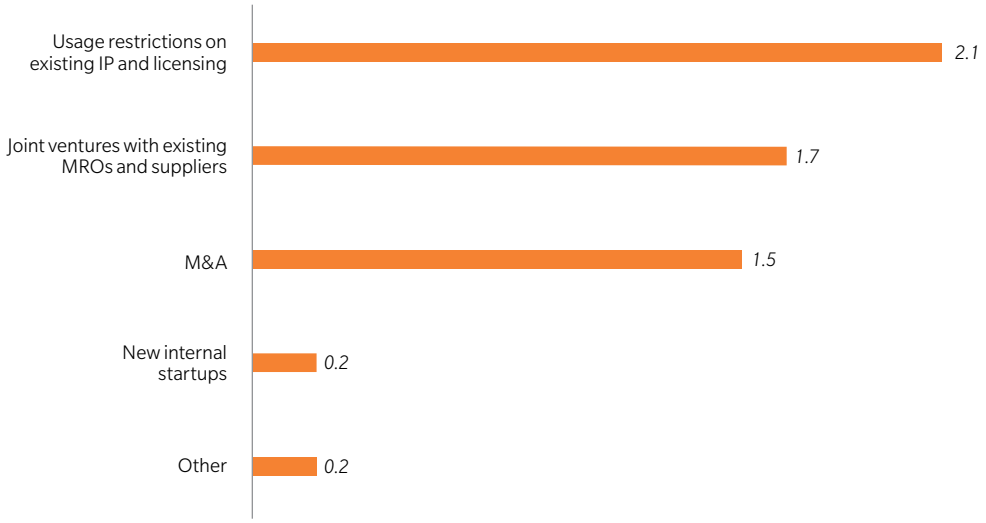
Controlling the IP on components and systems means OEMs can force operators to use their parts and sometimes their MRO operations for repairs and maintenance, providing a competitive advantage in the marketplace. MRO providers, who buy the OEM-designed components, may end up paying more.

In order to continue growing, OEMs are doing what they can to repatriate or buy back IP, so they can own and control more of the materials aftermarket. Materials have historically been a highly lucrative line of business for OEMs, with margins that are easily many times greater than those for labor services. In addition, IP control gives OEMs leverage in a large swath of MRO activities and allows them to drive material usage and prices up, putting MROs and operators at a disadvantage.

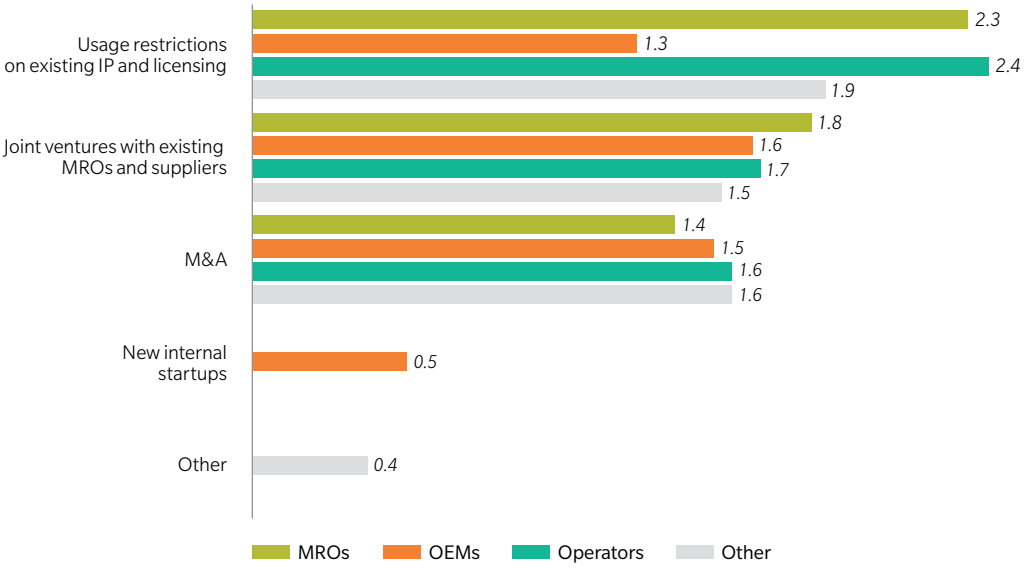
In this year's survey, almost all respondents (97%) report increases in material costs. MROs and operators overwhelmingly attribute this additional operating expense to annual OEM material price increases and restrictions they place on the direct sale of OEM-designed parts because of their IP ownership.

Exhibit 4: How will OEMs grow their presence in aftermarket?

Weighted average of rankings (highest to lowest ranking, scale of 3-1)



Weighted average of rankings for each segment (highest to lowest ranking, scale of 3-1)



Source: Oliver Wyman analysis

Not surprisingly, MROs and operators show the most apprehension over the OEMs' increasing market share and growth in IP. While the rise of OEMs in the aftermarket is nothing new, the push for IP has gained momentum over the last couple of years, along with an increased commitment from aircraft OEMs to expand more heavily into the aftermarket. While both operators (40%) and MROs (50%) tell the survey that they don't control enough IP, the OEMs (89%) seem content with their IP ownership – even as they push for more. Seven out of 10 survey respondents indicate that OEMs control their IP.

MROs and operators are attempting to protect themselves from the rising material costs, but finding the right strategy has proven somewhat challenging. The number one approach has been to partner with OEMs, followed by increased reliance on advanced tech and predictive maintenance and Used Serviceable Materials (USM).

But none of these strategies are foolproof. For instance, a USM strategy depends on having adequate supply. Employing USM essentially involves scraping out-of-service aircraft for the parts and then repurposing them in working planes. Each segment ranks USM as a one of their top strategies for combatting higher materials costs, with more than three-quarters (76%) expecting their USM usage to increase over the next five years.

STRATEGY LIMITATIONS

The more popular the strategy is, the more likely there will be insufficient USM to meet the demand. Even now, operators indicate their inability to increase reliance on USM stems from the lack of a functional material-sourcing strategy. The problem may be that the parts-trading expertise to get the required USM may be too much of a specialized activity for most operators to devote the capital and employ the skill sets necessary. As a next step to manage rising material costs, companies can also trade or broker materials, reinvigorate pooling relationships and LLP consortiums, develop leasing consortiums, and refine maturity to end-of-life program optimization.

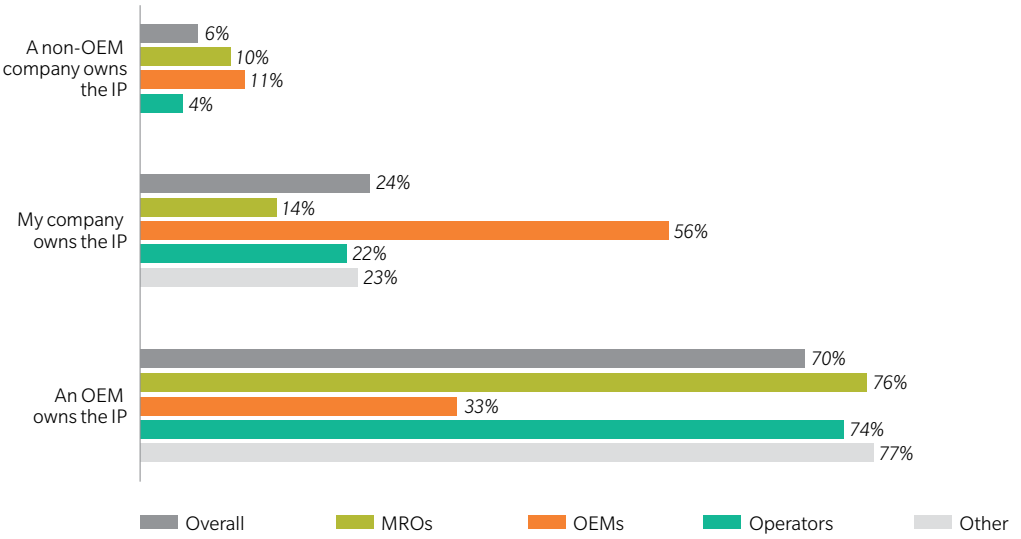
Without further concerted efforts by MROs and operators to address rising material costs, an expansion in OEM IP ownership is expected to challenge the industry's ability to acquire materials and manage their cost for the foreseeable future.

Meanwhile, with an anticipated increase in OEM IP ownership and their strengthening aftermarket positon, aircraft manufacturers and third-party specialists are perceived as the most likely to innovate over the next five years. The survey says they also are the ones most likely to drive improvements in asset productivity and aircraft reliability in the future. Respondents appear least optimistic about the ability of the airlines and MRO providers to improve either asset productivity or aircraft reliability down the road.

SURVEY RESULTS REVEAL TRENDS AND STRATEGIES IN IP, MATERIAL COSTS AND USM

Exhibit 5: Who owns the IP your aftermarket service depends on?

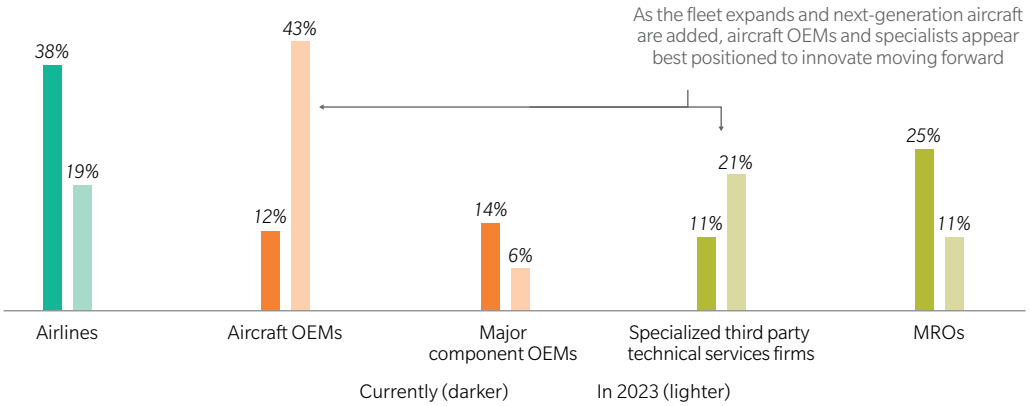
Distribution of responses by segment



Source: Oliver Wyman analysis

Exhibit 6: Who is best positioned to create innovative solutions and improve asset productivity and aircraft reliability?

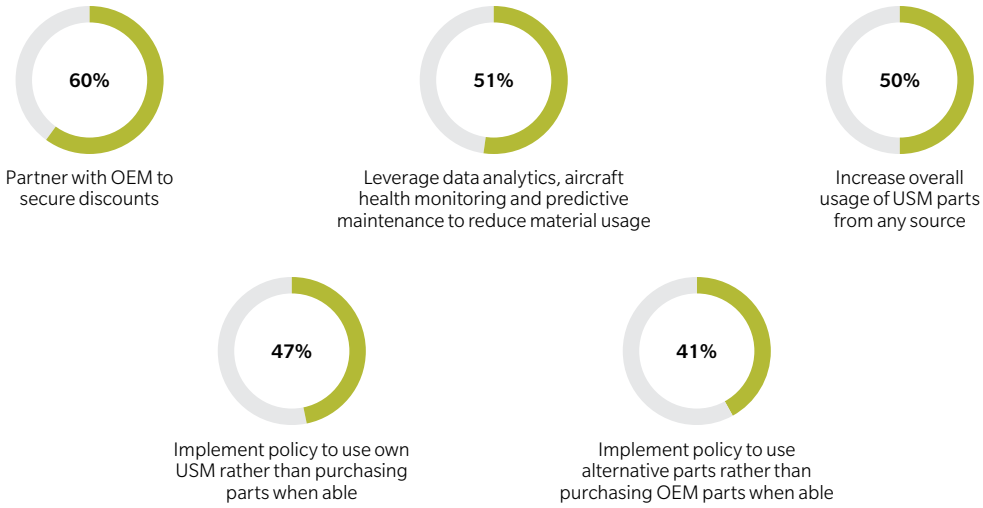
Distribution of total responses by year



Source Oliver Wyman analysis

Exhibit 7: Top 5 strategies adopted or being considered to combat rising material costs

Percent of respondents who selected each response



Source: Oliver Wyman analysis

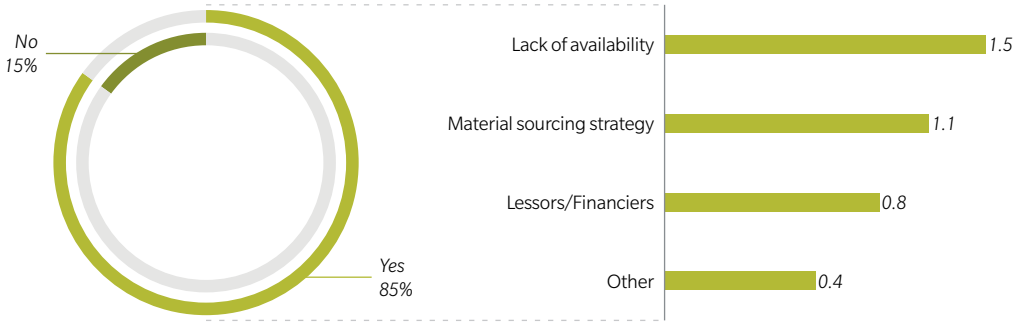
Exhibit 8: The limits on a used serviceable materials strategy

IS YOUR USE OF USM INHIBITED?

Distribution of total responses

MAIN FACTORS INHIBITING USE OF USM

Weighted average of rankings (highest to lowest ranking, scale of 3-1) (among yes responses)



Source: Oliver Wyman analysis

MORE RESULTS

MRO SURVEY ON LABOR

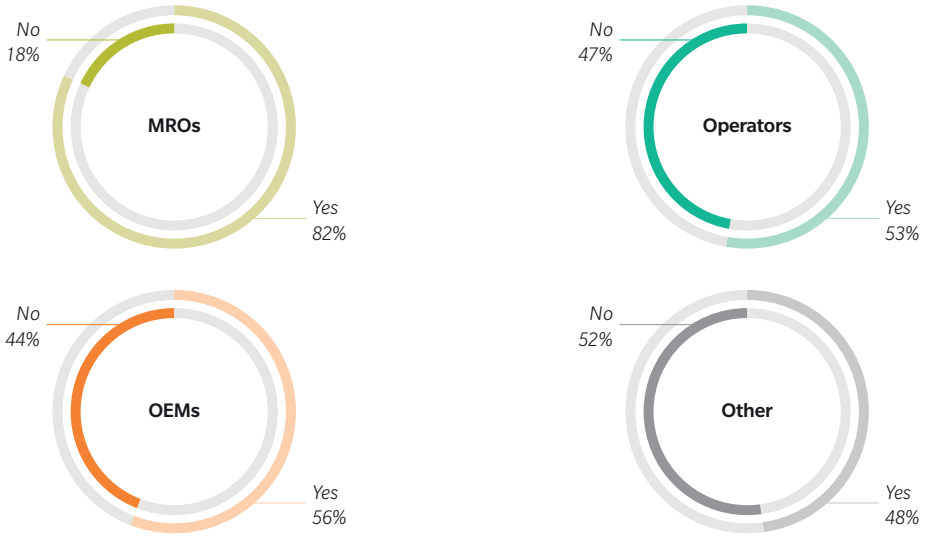
THE LABOR SHORTAGE IS EVERYONE'S HEADACHE

Across the industry, there is a strong belief among respondents (60%) that OEMs will want to expand into labor-intensive segments of the business. In particular, MROs feel most threatened by the prospect of OEMs investing in "wrench-turning" services (82%).

Oliver Wyman does not expect OEMs to push too far, too fast for a strategy to grow touch-labor services. Labor-intensive lines of business have unique challenges and lower margins, especially in the airframe MRO side of the business. Moreover, given the increasingly strong growth of OEMs in the aftermarket for higher-margin materials – several times the margin for labor – they would be better off doubling down on investments in materials as opposed to expanding into touch labor. If OEMs do decide to pursue investment in labor services, it would be more advantageous for them to offer component-related and more material-based services over airframe-related services.

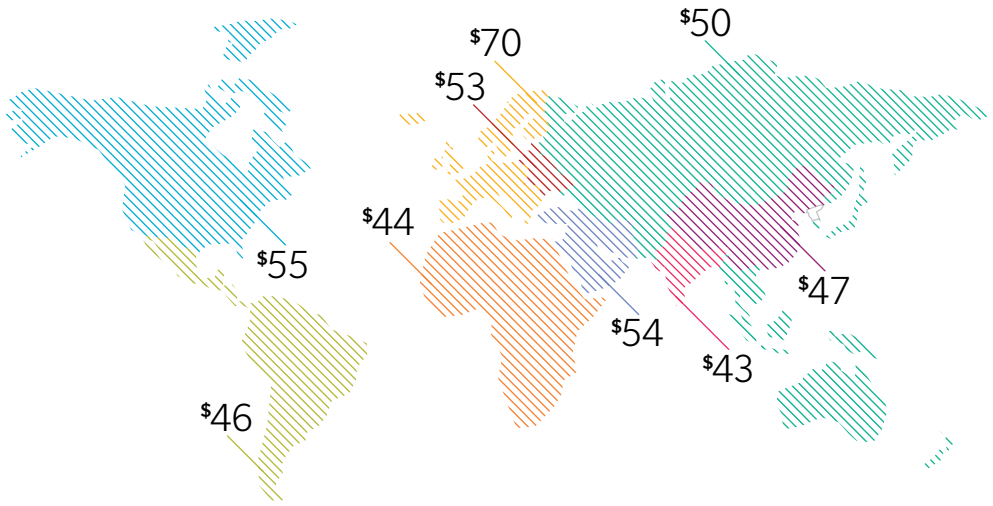
Exhibit 9: Do you believe OEMs will make large investments in "wrench-turning" services?

Distribution of responses for each segment



Source: Oliver Wyman analysis

Exhibit 10: Current prevailing technician billed rates for heavy airframe maintenance



Source: Oliver Wyman analsyis

OEMs may also be deterred by the looming labor shortage, which will be a challenge to all segments of the MRO industry and aftermarket – whether or not OEMs make a move into labor. For this reason, pressure on technician wages is a top concern for respondents in this year's survey. Respondents overwhelmingly are reporting pressure to increase technician wages (97%).

For 2018, respondents indicate average billed airframe labor rates ranged from a high of $70 in Western Europe to a low of $43 in South Asia. The US is on-par with Eastern Europe in the mid to low $50s, and Latin America and China mirror each other's rates in the mid $40s. These levels make intuitive sense given underlying skilled pay rates, but also indicate a very competitive, global marketplace, especially when the costs of ferrying aircraft – crew, fuel, and additional out-of-service time – are factored in.

WAGES ON THE RISE

As this year's survey affirms, technician labor supply is viewed as the primary global challenge, by a factor of two, to keeping labor costs down and is largely responsible for the number two concern – global wage inflation. As reported in last year's survey, technician retirements and a lack of new technician creation continue to squeeze the labor supply – a trend that is unlikely to be resolved in the near term.

In an effort to mitigate rising labor costs, MROs and operators identified several strategies they have adopted or are considering adopting. For operators, a major lever that can be pulled is resorting to outsourcing or right-shoring – that is, continuing to offer the service but locating it in places with both the best costs and efficiencies (56%). This is a less viable option for OEMs (33%) or MRO providers (29%) as they have for the most part already taken advantage of outsourcing manufacturing and right-shoring.

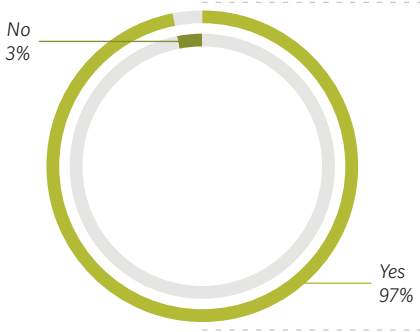
Operators appear bullish (74%) about the power of data analytics, aircraft health monitoring, and predictive maintenance to improve labor productivity and potentially reduce labor demand – although MROs (43%) and OEMs (44%) don't share their enthusiasm. They switch positions when it comes to job sharing and the adoption of process improvements to increase productivity and efficiency: MRO providers (76%) and OEMs (67%) overwhelmingly support the strategies and operators (48%) are less confident.

Any attempt to increase worker productivity must include a robust and comprehensive training program. While 47 percent of respondents agree, they are not always happy with the outcomes of those programs. Among a set of eight training-program components, respondents consistently say they are dissatisfied with their outcome and effectiveness, while still underscoring their importance. The discrepancy is most notable when it comes to reducing maintenance costs and communicating insights from one location to another. Most respondents expressed considerable frustration with the cost and benefit of training, and they are looking for more flexibility and better design and execution.

Exhibit 11: There's no fighting supply and demand

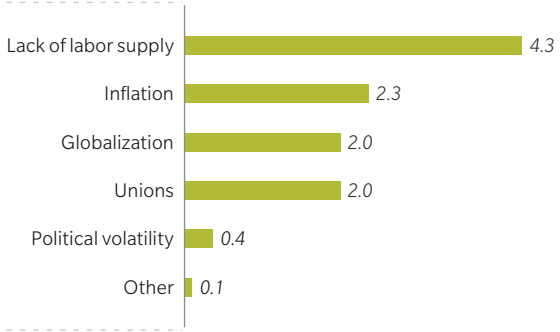
HAVE YOU EXPERIENCED ANY UPWARD TECHNICIAN WAGE PRESSURE?

Distribution of total responses



MAIN DRIVERS OF TECHNICIAN WAGE PRESSURE (ONLY REFLECTS RESPONDENTS REPLYING YES)

Weighted average of rankings
(highest to lowest ranking, scale of 5-1)

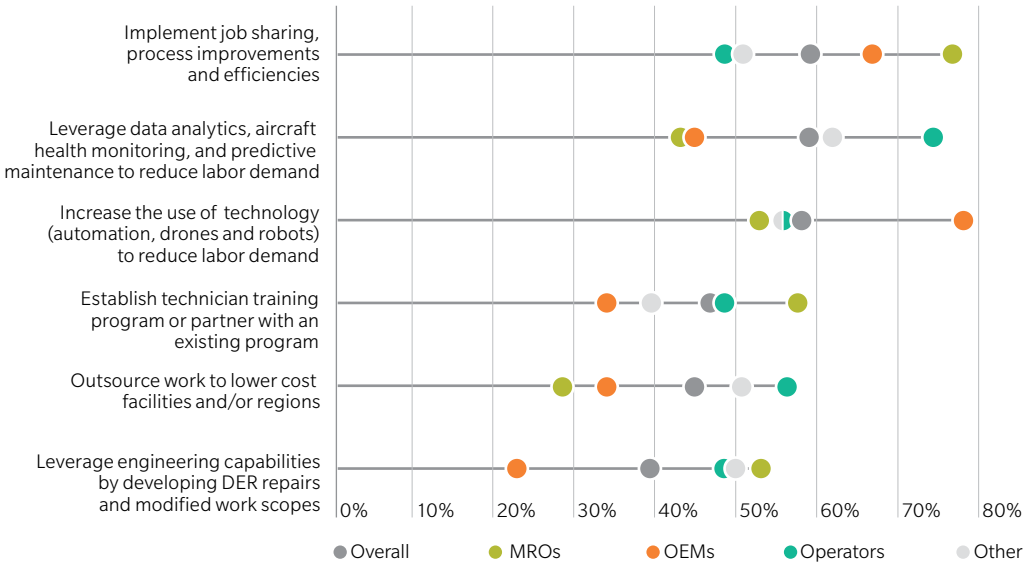


Source: Oliver Wyman analysis

Exhibit 12: Strategies to combat rising labor costs

WHAT STRATEGY OR STRATEGIES HAVE YOU ADOPTED OR ARE YOU CONSIDERING TO COMBAT RISING LABOR COSTS?

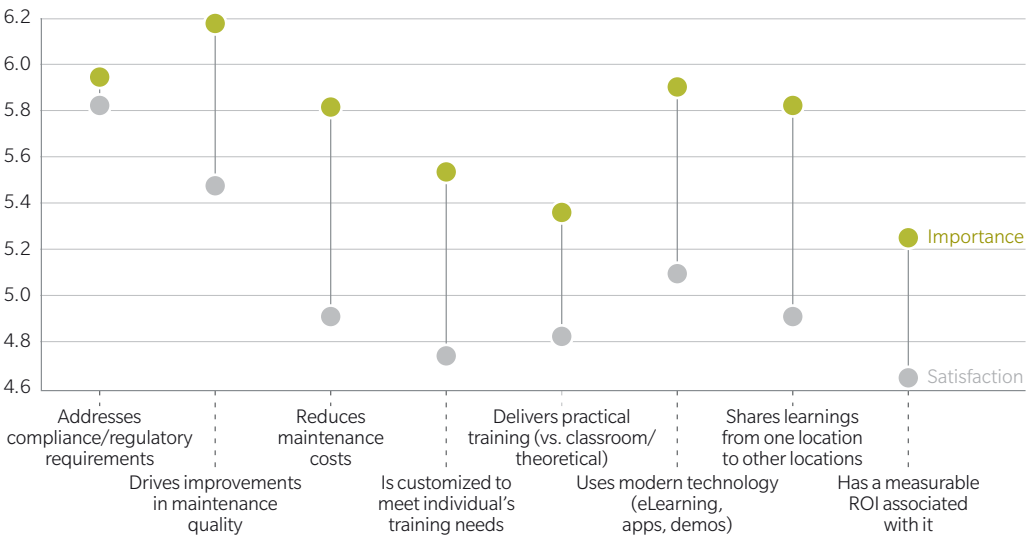
Percent of total respondents who selected each response for each segment



Source: Oliver Wyman analysis

Exhibit 13: The difference between average importance ranking vs. average satisfaction ranking

Rankings on a scale of 0 to 10; rankings of importance and satisfaction made separately



Source: Oliver Wyman analysis

CONCLUSION

It was another interesting year for the industry. On one hand, the competition has never been more intense, with many aircraft, engine, and component manufacturers looking to expand their aftermarket businesses.

On the other, it's a year when participants should be thinking about working more closely together to develop strategies and mutual defenses to ward off the growing ranks of ever more sophisticated and determined cyber criminals. As the industry's digitization has increased, so too has the risk of hacker penetration mounted, and that danger will only further escalate as transportation incorporates into operations more artificial intelligence solutions and autonomous functions. Cybersecurity strategies aimed at protecting a single organization alone may not end up being comprehensive enough, making it important for transportation and aftermarket players to consider collaboration to fill in gaps in cybersecurity coverage and risk management.

Besides building joint defenses against the worldwide cyber threat, there is also perhaps room for some united efforts to address the industry's looming labor shortage, which will only become more pressing after 2020 with the growth in the global fleet and the increasing demand for air travel around the world, particularly in Asia. Would it make sense, for instance, for major MRO providers to work together with key universities and technical schools to ensure that training encompasses all the skills 21st century aerospace mechanics need? What can national and state/provincial governments and companies do to attract more students to the profession in time to avoid the worst impacts of the anticipated mechanic shortfall?

Or perhaps the answer lies in accelerating development of programs in predictive maintenance and other advanced analytics strategies. While the intensity of the competition and increasing scarcity of labor may make it difficult to set aside rivalries long enough to pursue such lofty mutual goals, immediate intervention and a degree of coordinated action would seem to be required to create enough new technicians on a schedule that will make a difference or push technology fast enough to help mitigate the shortfall.

As it is for most industries, disruption that challenges the status quo also opens the door for vast improvements in efficiency and operational excellence with the right strategies.

RECENT PUBLICATIONS
FROM OLIVER WYMAN

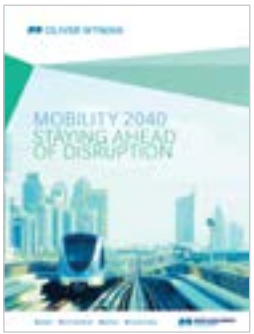
For these publications and other inquiries, please visit www.oliverwyman.com and our Oliver Wyman Ideas app: http://apple.co/1UBhSPE.

MRO SURVEY 2017

A deep dive into innovation, technology adoption and the impending talent shortage facing the maintenance, repair, and overhaul sector.

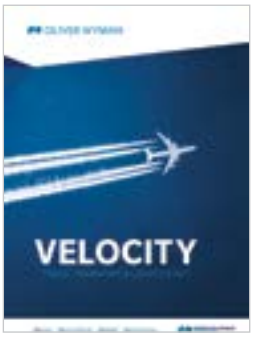
2018-2028 GLOBAL FLEET & MRO MARKET FORECAST COMMENTARY

A 10-year outlook for the commercial airline transport fleet and the associated maintenance, repair, and overhaul (MRO) market.



MOBILITY 2040 STAYING AHEAD OF DISRUPTION

Our new research study of emerging trends and the future of passenger transport.



VELOCITY 2017

Perspectives on the issues facing the global travel, transport, and logistics industries.

THE OLIVER WYMAN AUTOMOTIVE MANAGER

Perspectives on the latest trends and issues in the automotive industry.

PERSPECTIVES ON MANUFACTURING INDUSTRIES, VOL 12

A collection of viewpoints on industrial companies' challenges and trends, as well as their opportunities and potential courses of action.

FORBES CONTRIBUTORSHIP

Oliver Wyman's transportation team regularly explores transformative ideas and technologies across travel and transport for Forbes.com.

NOW ARRIVING

Oliver Wyman's PlaneStats.com publishes an in-depth data chart each day. Subscribe to daily email delivery at www.planestats.com/arrival_subscribe.

TEN DIGITAL IDEAS FROM OLIVER WYMAN

In this collection of articles, we showcase ten digital ideas from across our firm for how business leaders can digitally innovate their businesses.

THE OLIVER WYMAN HEALTH INNOVATION JOURNAL, VOL. 1

Insights into how the health industry is changing because of new technology and new attitudes.

INCUMBENTS IN THE DIGITAL WORLD

How incumbent organizations can ultimately win in a marketplace transformed by digital disruptors.

THE OLIVER WYMAN ENERGY JOURNAL, VOL. 3

The latest thinking from across Oliver Wyman's energy practice on how shifts underway will create new risks and opportunities not just for the energy sector, but also for every company and person that depends on it.

THE OLIVER WYMAN RETAIL JOURNAL, VOL. 5

The new retail and consumer landscape will throw up threats and opportunities in almost every corner of the business – and much faster than in past upheavals.

THE OLIVER WYMAN RISK JOURNAL, VOL. 7

Collection of perspectives which represent the latest thinking on the topic of risk from across Oliver Wyman.

THE OLIVER WYMAN CMT JOURNAL, VOL. 3

Our latest thinking on the opportunities and challenges in communications, media, and telecommunications.

OW IDEAS APP

Oliver Wyman Ideas offers our most recent insights on issues of importance to senior business leaders.

ABOUT OLIVER WYMAN

Oliver Wyman is a global leader in management consulting with offices in 50+ cities across 26 countries.

Our aviation, aerospace and defense experts advise global, regional and cargo carriers, aerospace and defense OEMs and suppliers, airports, MROs, and other service providers in the transport and travel sector to grow shareholder and stakeholder value, optimize operations, and maximize commercial and organizational effectiveness.

The team's capabilities also include: CAVOK, technical consulting on safety and compliance, maintenance programs, and certification (www.cavokgroup.com); PlaneStats.com analytical data tools; and strategies and modeling for market share, network, and fleet planning analyses via our Network Simulation Center.

This deep industry expertise and our specialized capabilities make us a leader in serving the needs of the sector.

Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC].
For more information, visit www.oliverwyman.com. Follow us on Twitter @OliverWyman.

For more information on this report, please contact:

ROGER LEHMAN
Transportation Practice Leader
roger.lehman@oliverwyman.com

DEREK COSTANZA
Aviation Partner & Lead Author
derek.costanza@oliverwyman.com

BRIAN PRENTICE
Aviation Partner and Co-Author
brian.prentice@oliverwyman.com

Cyber risk expert contributors: Paul Mee, Partner, and Jim Cummings, Senior Advisor

Alan Eberstein, Marine Ladner, Cyril Straughn-Turner, and Pat Wechsler also contributed to this report.

Designed by Melissa Ureksoy, Mike Tveskov, Jocelyn Arnaud, and Luis Hurtado de Mendoza.

www.oliverwyman.com

OLIVER WYMAN