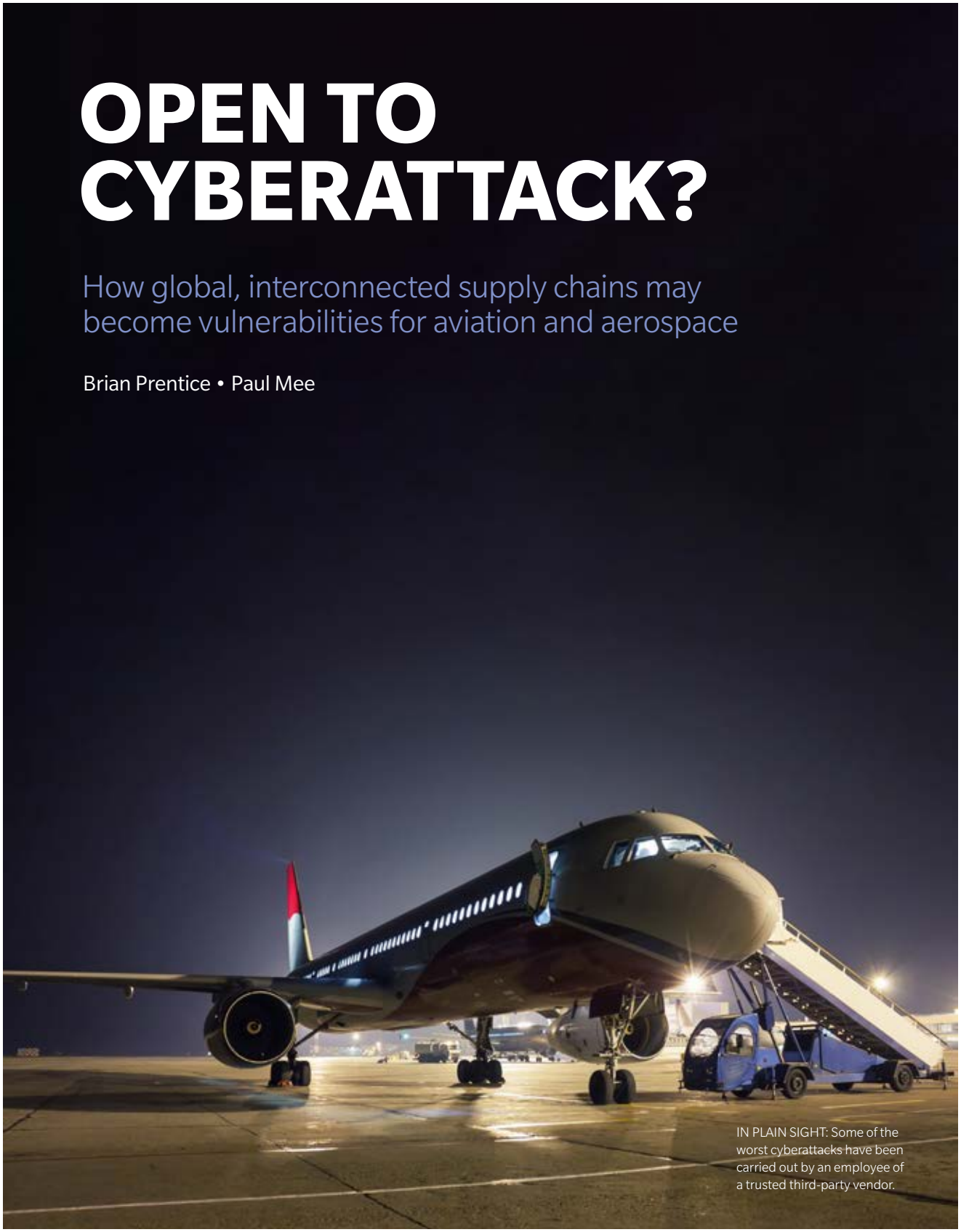
OPEN TO CYBERATTACK?

How global, interconnected supply chains may become vulnerabilities for aviation and aerospace

Brian Prentice • Paul Mee



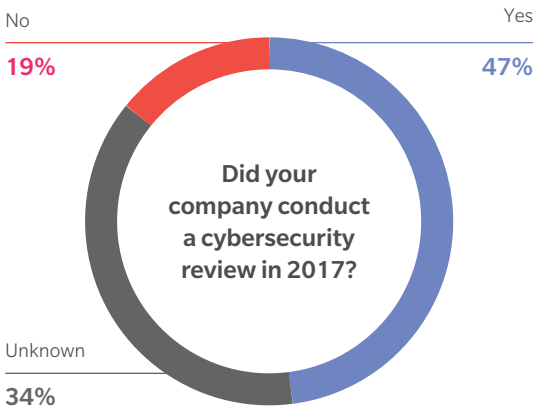
IN PLAIN SIGHT: Some of the worst cyberattacks have been carried out by an employee of a trusted third-party vendor.

IN MARCH, THE US DEPARTMENT of Homeland Security and the Federal Bureau of Investigation issued a troubling alert: Since the same month two years before, Russian state-sponsored hackers had been infiltrating the nation's electricity grid and various infrastructure industries, including aviation, collecting information on how the networks were organized and what systems' controls they had in place. While no sabotage appears to have been perpetrated, the unsettling question remains – what are the Russians going to do with the data they collected?

While all these industries, especially their biggest players, tend to have extensive cybersecurity in place, it may not be as comprehensive as the nation would hope. In this case, instead of gaining access through the front door, where the alarm system was more robust, these hackers simply went around back and entered through the more vulnerable networks of third-party and supplier operations, relying on myriad techniques including phishing emails infected with malware and the theft of credentials.

Needless to say, the scenario should send chills throughout the aviation and aerospace industries. While major aircraft manufacturers and airlines make obvious targets because of the potential to conspicuously disrupt international commerce, they also rank high on hackers' to-do lists because they maintain global, highly interconnected supply chains that over the past few years have been aggressively digitizing operations. More digitization means more attack surface for hackers. The many links on aviation's and aerospace's supply chains – some big, many small to midsize – all become potential vulnerabilities, given the daunting task of ensuring that vendors with access are capable of providing the same level of rigor in both their cybersecurity and their employee training.

HOW PREPARED IS THE INDUSTRY?



Source: MRO Survey 2018; Oliver Wyman analysis

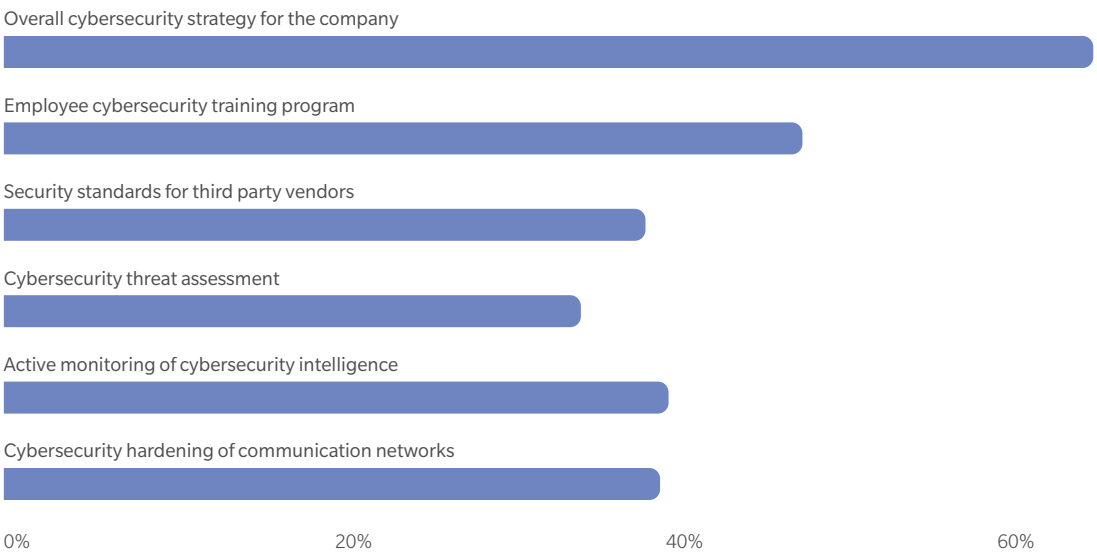
Vulnerable links

While the biggest organizations within the industry's fold may have advanced cybersecurity, the same cannot always be said about the vast network of service providers and suppliers. Many of these are considered members of the maintenance, repair, and overhaul (MRO) industry that services the nation's aircraft.

In a 2018 Oliver Wyman survey of the MRO industry, responses revealed potential holes in the bulwark. For instance, while 67 percent of respondents said their company was prepared for a cyberattack, fewer than half were able to say whether they had conducted a cybersecurity review in 2017. Only nine percent of independent MRO providers, 50 percent of airframe, engine, and component manufacturers, and 41 percent of airlines confirmed that they have established security standards for third-party vendors. That leaves potentially many companies without a clear view into the digital security of vendors – almost all of which maintain credentials to log onto their systems.

And that lack of knowledge can lead to disaster, as many major corporations have discovered over the past five years. In 2013, for instance, hackers used the stolen credentials of a heating, ventilation, and air conditioning vendor to penetrate the network of retail giant Target to steal the data of 70 million customers and information on 40 million payment cards. The cost to Target: close to $300 million.

WHICH CYBERSECURITY SAFEGUARDS HAS YOUR COMPANY IMPLEMENTED?
PERCENT OF TOTAL RESPONDENTS WHO SELECTED EACH RESPONSE FOR EACH SEGMENT



Source: MRO Survey 2018; Oliver Wyman analysis

While cyber criminals in earlier decades seemed 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 Ukraine with software that literally wiped out data and disrupted operations in that country's banking system, government ministries, and metro, and at the former Chernobyl nuclear power plant.

A global emergency

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. It is attacks like this one that should prompt transportation companies to reassess their level of cyber preparedness.

Globally, hacking has become a growth 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 is on the rise.

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 a response system have been delineated, to which managers are responsible for each phase of the cybersecurity protocol, to whether oversight exists to ensure procedures are followed and documented.

Industry standard

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 has developed a set of industry-specific standards and best practices intended to be leveraged in designing such a cybersecurity framework.

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.

Brian Prentice
is a Dallas-based partner in Oliver Wyman's transportation practice.

Paul Mee
is a New York-based partner in Oliver Wyman's digital practice.

This article originally appeared in Forbes on April 11, 2018.

For more information on this subject, please contact:
Brian.Prentice@oliverwyman.com or Paul.Mee@oliverwyman.com