RESEARCH SUMMARY

Exploring Options to Improve Supply Chain Operations

A Review of Current Approaches and New Opportunities in Demand Forecasting, Robotic Process Automation, and Cyber Integrity

JAMES A. LEFTWICH, DAHLIA ANNE GOLDFELD, BRADLEY DEBLOIS, CHAD HEITZENRATER, LUKE MUGGY, SHANNON PRIER, JOSHUA STEIER, CHRISTOPHER E. MAERZLUFT, SYDNE J. NEWBERRY

To access the full report, visit www.rand.org/t/RRA1734-1

ISSUE

The U.S. Air Force (USAF) has had long-standing concerns about its supply chains and their potential for degradation. Given the varied types of resources for which USAF manages the supply chains and opportunities for degradation, the RAND Project AIR FORCE research team identified technology and investment options to mitigate supply chain degradation, focusing specifically on forecasting the demand for legacy aircraft spare parts, applying robotic process automation (RPA), and mitigating risks associated with cyber integrity.

APPROACH

We conducted extensive literature reviews, held discussions with subject-matter experts, and employed various analytical methods. For demand forecasting, these methods included analysis of recent forecast accuracy data to identify drivers of forecast error and an assessment of ongoing efforts to address known issues. For RPA, our analyses included a characterization of bot development and identification of potential application areas in the logistics, engineering, and force protection (A4) community. For cyber integrity, the analysis involved applying a mission assurance approach to identify potential risks and mitigations.

CONCLUSIONS

- Demand Forecasting
  - Primary drivers of demand forecast errors, such as propulsion systems and low demand for expensive parts, are well known to personnel who study the problem.
  - Decades of research on demand forecasting suggest there are a variety of methods to forecast spare parts demand, although there is not a one-size-fits-all best approach.
  - USAF's migration to a commercial enterprise resource planning system for demand forecasting is already showing promise.
  - It is unclear whether demand forecast accuracy is resulting in aircraft downtime.
- Application of Robotic Process Automation to Improve Supply Chain

continued

  - The USAF A4 community's current approach to bot implementation does not allow it to fully leverage the potential of bots.
  - Questions remain about whether USAF personnel possess the technical expertise to fully leverage bot technology, and the data suggest this concern is warranted.
  - Unified direction and guidance could help USAF maximize the potential of bots.
- Cyber Tampering
  - Potential vectors for integrity attacks within the supply chain include the software supply chain, software vulnerabilities, and credential-based attacks.
  - Risks related to both development and operation of bots underscore the need to consider cyber risk across the bot life cycle and incorporate training and best practices.
  - In addition to existing processes, risk-based analysis can drive cybersecurity, engineering, and mission-execution decisionmaking for technology under consideration.
  - Current Headquarters U.S. Air Force Deputy Chief of Staff for Logistics, Engineering and Force Protection (HAF/A4) risk management framework (RMF) controls are primarily focused on detection and are unlikely to sufficiently mitigate focused, tampering-based mischief.

RECOMMENDATIONS

- Demand Forecasting
  - USAF should maximize the potential benefits offered by the investment already made in ESCAPE. However, USAF should analyze the value of demand forecast improvements to supply chain performance prior to making additional investments.
  - If additional investment in forecast accuracy improvement is warranted, the 448th Supply Chain Management Wing should target specific areas of improvement, such as expanded causal analysis for parts with intermittent, infrequent, and highly variable demand.
- Application of Robotic Process Automation to Improve Supply Chain
  - USAF should expand the application of bots within the A4 community, including processes and data integration not currently accomplished. We provide a suggestion with our bot example.
  - USAF should work with the USAF lead for RPA to establish standards for centralized development and management of bots and should advocate for funding for increased security measures.
- Cyber Tampering
  - USAF should consider mitigation approaches for integrity attacks identified by this analysis, especially in bot implementation, as a complement to existing cybersecurity controls.
  - USAF should continue to evaluate cyber risks in context by implementing a process for considering how threats, vulnerabilities, and consequences to missions change as new systems, technologies, and information-handling methods are considered and implemented.

RAND PROJECT AIR FORCE

RAND Project AIR FORCE (PAF), a division of RAND, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. For more information, visit PAF's website at www.rand.org/paf.