RESEARCH SUMMARY

Cybersecurity and Supply Chain Risk Management Are Not Simply Additive

Implications for Directions in Risk Assessment, Risk Mitigation, and Research to Secure the Supply of Defense Industrial Products

VICTORIA A. GREENFIELD, JONATHAN W. WELBURN, KAREN SCHWINDT, DANIEL ISH, ANDREW J. LOHN, GAVIN S. HARTNETT

To access the full report, visit www.rand.org/t/RRA532-1

ISSUE

Our analysis in this report and such events as a 2017 cyberattack that impaired commercial distribution globally and the 2020 SolarWinds breach lend credence to the view that costly cyberattacks have become an eventuality for many organizations. Against that backdrop, the Air Force Research Laboratory (AFRL) asked RAND Project AIR FORCE (PAF) for assistance understanding how cyber-related risks compare with other risks to its defense-industrial supply chains—a scope that included supply chains for hardware, not supply chains for software—and exploring implications for directions in risk assessment and mitigation and for research. AFRL was interested in how attackers might use supply chains to wage attacks, such as through malicious code, and how supply chains might, themselves, be targets of attack, such as through disruption.

APPROACH

Over an 18-month period, beginning in mid-2019, PAF sought to answer two research questions, "How do cyber-related risks differ from or compound other concerns about supply chain risk management (SCRM)?" and "What do, or could, these differences mean for risk assessment, risk mitigation, and research?" To conduct the analysis, PAF drew insights from the literatures on cybersecurity, SCRM, game theory, and network analysis and worked with sets of stylized supply chains and fundamental principles of risk management. The report uses the phrase *cyber SCRM* broadly, to refer to the cybersecurity of supply chains, including attacks *through* supply chains to reach a target and attacks on supply chains in which the target of the attack is the supply chain itself.

continued

KEY INSIGHTS

The first insight pertains directly to the first research question, and the subsequent insights pertain largely to the second research question, but with some overlap:

- **Cyber-related risks could be substantially worse than and different from others.** Cyber events can present the worst of all the characteristics of conventional hazards, judged in terms of their onset, duration, visibility, and reach, and can pose even greater challenges than nondigital threats, given the potential for strategic adversaries to inflict harm at low cost and without punishment of repeated attempts.
- **Preventative measures are not enough.** Preventative measures cannot stand alone or be pursued at the expense of taking steps to facilitate response and recovery or build resilience. Creating impenetrable defenses is infeasible, and attempting to create them would entail further risks and costs.
- **Cyber SCRM requires more than an amalgam of *cyber* and *SCRM*.** The risks of cyberattacks might be unhindered or even elevated by some conventional means of addressing cyber and SCRM concerns—such as those for exploitation and disruption—separately, suggesting the potential for trade-offs among risk-reduction objectives. Absent any trade-offs, a fusion of cyber- and SCRM-based measures could be inadequate if conventional SCRM underestimates the potency of cyberattacks relative to other sources of risk.
- **Private-sector efforts to manage risk may not meet national security needs.** Strategic interactions between suppliers and attackers could lead to underinvestment in security, especially without coordination among suppliers, but compounding factors, involving risk assessment, incentives, and supply chain visibility, could make matters worse. A supplier that cannot see how far its supply chain reaches or the dependencies within it cannot be expected to mitigate risk to its own satisfaction, let alone to that of the Department of the Air Force (DAF).
- **Research can do more to support cyber SCRM.** This could include delving into the details of some long-standing issues, such as those regarding risk assessment, possibly with new or different analytical methods, and by exploring other issues that came to the fore in this research, such as those concerning private-sector engagement.

RECOMMENDATIONS

We suggest taking a comprehensive approach to cyber SCRM that would address cybersecurity and SCRM together by

- framing the potential consequences of cyberattacks in terms of the availability, quality, and cost of defense industrial products that serve mission-critical roles, not just or primarily in terms of information security
- establishing priorities among those cyber and SCRM consequences based on what they could mean for mission attainment
- setting out terms for cyber SCRM strategies, with due attention to response, recovery, and resilience, that account for concerns about
  - information security and supply chain functionality
  - differences in DAF and private-sector interests that could affect whether and how industry contributes to risk reduction
  - trade-offs among risk-reduction objectives, relating, for example, to supply chain disruption, on the one hand, and information vulnerability, on the other.

continued

We also discourage dwelling too much on efforts to fine-tune risk assessments and build impenetrable defenses, which are unlikely to succeed and could distract from other risk reducing activities. Finally, we highlight opportunities for research in four areas that could strengthen the foundation for risk management:

- approaching risk assessment with realistic expectations and with greater emphasis on supply chain functionality
- establishing needs and priorities for responding to, recovering from, and increasing the resilience of supply chains to cyberattacks, especially in relation to supply chain functionality and mission attainment
- examining the utility and limits of private-sector risk reduction
- crafting a comprehensive strategy for cyber SCRM.

RAND PROJECT AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, 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 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.