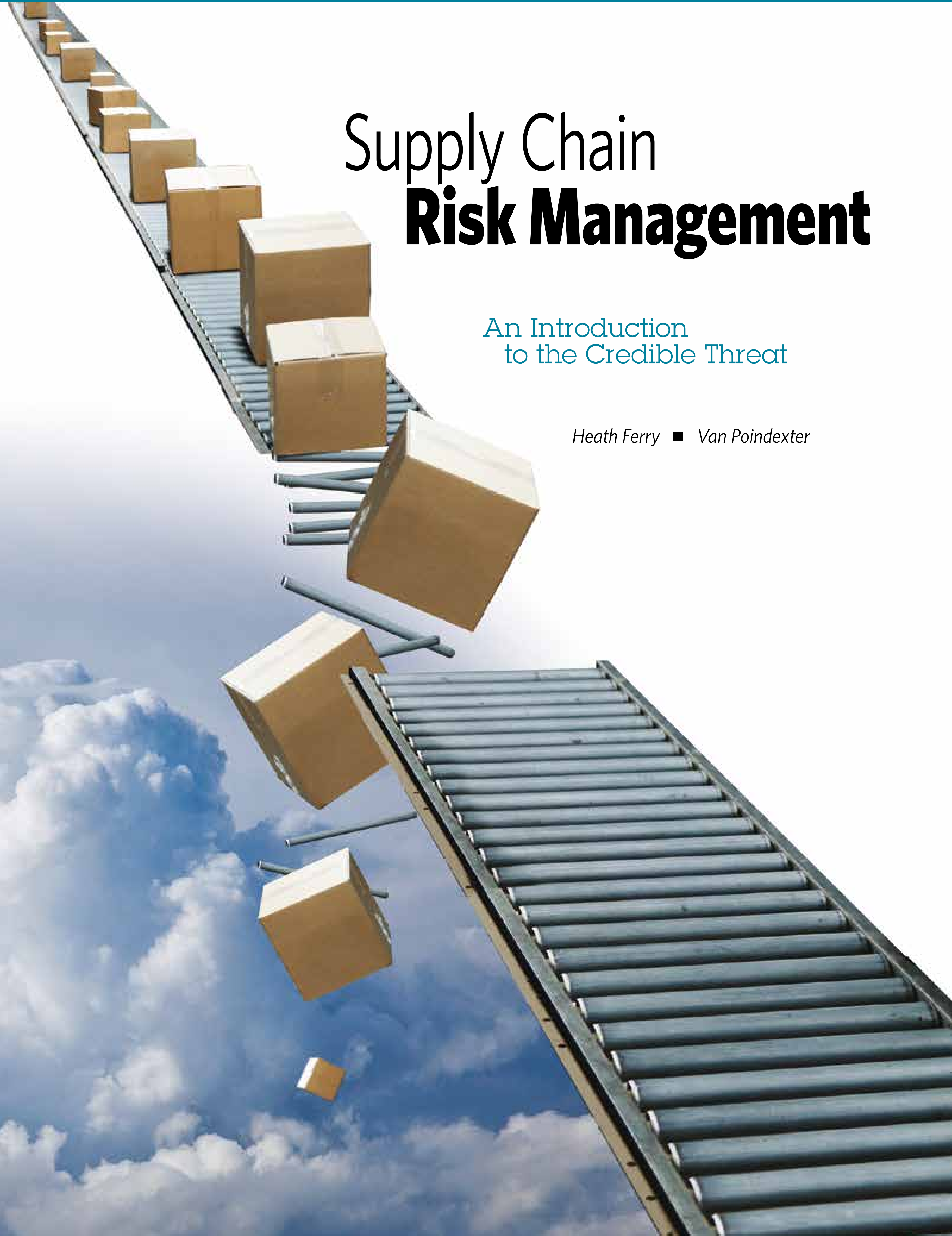
Supply Chain
Risk Management

An Introduction to the Credible Threat

Heath Ferry ■ Van Poindexter



We live in a wonderful world of instant information, and everything is connected. All we have to do is pull out our phones, tablets, laptops or any other similar device and get the information we need virtually instantaneously.

While all this advanced communications technology constitutes one of the greatest things about living in a technologically advanced world, it also exposes us to one of the biggest threats. How can we be sure that any and all of these devices were made to strict manufacturing standards and weren't designed with the flaws built in or downloaded? Some of the same tools that make our lives easier also could leave us wide open to a cybersecurity breach. This article examines the elements of supply chain risk management, the national security risks associated with exploitation, and the concerns for the Department of Defense (DoD).

According to the November 2012 DoD Instruction (DoDI) 5200.44, Supply Chain Risk Management (SCRM) is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the product and its subcomponents or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation and disposal).

So what does all of this mean to the government and the overall acquisition life cycle? SCRM is a credible inside threat every bit as much as a malicious insider, counterfeiters, terrorists or industrial espionage agents. Is SCRM just a cyber issue? An intelligence issue? An acquisition issue? Honestly, it is all the same and should be treated as such. A concerted effort should be made, across all levels and domains, to address it at every step of the acquisition life cycle.

The DoD, military, business and intelligence operations—including communications and command and control—rely heavily on trusted networked systems, devices and platforms. All of these components support the ever-increasing number of capabilities that support the DoD's missions. Every component is designed, manufactured, packaged and delivered to end users, and global supply chains provide multiple attack vectors that increase a program's cybersecurity risk. The supply chain is a globally distributed and interconnected web of people, processes, technology, information and resources that creates and delivers a product or service. Global supply chains are dynamic, multilayered and complex. Lack of visibility and traceability through all of the diverse layers of the supply chain create security challenges because each component has its own supply chain that provides multiple opportunities for an adversary to sabotage the raw materials, manufacturing processes, packaging and even shipping. All of these can collect information on DoD systems and lead to either industrial or traditional espionage.

Ferry *is one of the newest cybersecurity professors at the Defense Acquisition University (DAU) South Region in Huntsville, Alabama. He currently provides Mission Assistance, curriculum development, and support to all segments of the Defense Acquisition Workforce. He holds a master's degree in cybersecurity and has multiple cybersecurity certifications.* **Poindexter** *is a professor at DAU South Region. He currently is involved in enhancing the awareness and proactive involvement of support managers and logisticians in identifying and mitigating risks in the Department of Defense supply chain. He is working on his doctorate in education.*

Figure 1. The Four Aspects of Supply Chain Risk Management

- **Security** provides the confidentiality, integrity and availability of information.
- **Integrity** focuses on ensuring that the products or services in the supply chain are genuine and contain no unwanted functionality.
- **Resilience** focuses on ensuring that the supply chain provides required products and services under stress.
- **Quality** focuses on reducing unintentional vulnerabilities that may provide opportunities for exploitation.

Integrity
Security
Resilience
Quality

Source: National Institute of Standards and Technology (NIST) Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015, Page 4.

Supply chain risk, by definition, is any risk that an adversary may use in order to sabotage, exfiltrate information, maliciously introduce unwanted function or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of a system so as to surveil, deny, disrupt or otherwise degrade the function, use, or operation of that system. Other risks include the insertion of counterfeits, unauthorized production, tampering, insertion of malicious software, loss of confidential government information, and poor manufacturing and development practices in the supply chain. Counterfeit components have the potential to degrade performance, but they often are introduced into the supply chain for financial rather than malicious purposes. Counterfeits can contain intentional modifications for the purpose of sabotage or exfiltration of information. SCRM focuses more on identifying the potential impacts of threats from malicious actors, rather than counterfeits. Supply chain weaknesses and vulnerabilities offer adversaries attack vectors for cyber exploitation and manipulation.

The Need to Manage the Supply Chain

Everything is interconnected today, and one component in a system or network can have an impact on one system or on multiple systems at the same time. Therefore, risk must be considered for each component before it is purchased or integrated into a system. The more critical the mission, the system and the component, the more diligent we must be in managing risk. Risk management decisions require that the decision maker consider three factors (cost, schedule and performance) and consider the impact of his or her decision about the desired or needed level of performance (in this case, cybersecurity) in the context of the impact of performance criteria on cost and schedule.

A May 2012, Senate Armed Services Committee inquiry report stated that China was found to be the dominant source country for counterfeit electronic parts, a major vulnerability in the supply chain. The Chinese government has failed to take steps to stop counterfeiting operations, which means DoD must step up its efforts to manage and mitigate the counterfeit threat. Unfortunately, DoD lacks knowledge of the sheer scope and impact of counterfeit parts on critical defense systems. This lack of knowledge can compromise performance, reliability of defense systems and can even risk the safety of military personnel. The defense industry's reliance on unvetted independent distributors and the weaknesses in their testing regime for electronic parts creates unacceptable risks and vulnerabilities. The defense industry routinely failed to report cases of suspect counterfeit parts. This has to stop.

SCRM traditionally refers to managing risks in the manufacturing and delivery supply chains. Globalization requires that SCRM include the process of identifying critical components and functions; identifying supply chain threats, vulnerabilities, and risks; determining likelihood (susceptibility) and the impact of those risks; and developing strategies in response. All of these supply chain exploitation risks should be assessed at each stage of the life cycle.

How to Manage It

One solution might be to buy only U.S.-made products, but this usually is difficult and could carry a higher cost, with the exception of certain very critical components. Trusted Suppliers (including Trusted Foundries) have been accredited by the Defense Microelectronics Activity to provide secure design, manufacturing, packaging and testing services. These suppliers also provide foundry capability, prototyping, testing and packaging services. Producing chips or other microelectronics through a Trusted Supplier can be more expensive than purchasing chips from commercial sources.

The Trusted Foundry program was started in 2004 to ensure that mission-critical national defense systems had access to microelectronics from secure, domestic sources. This program identifies Trusted Foundries for contract semiconductor manufacturing at features sizes down to 22 nanometers. Although most SCRM focuses on the tactical end—protecting

> **There is growing concern that counterfeit parts—generally the misrepresentation of a part's identity or pedigree—can seriously disrupt the DoD supply chain, harm weapon systems integrity, and endanger troops' lives. Additionally, with many manufacturing steps being performed offshore, sophisticated adversaries have the opportunity to inject vulnerabilities that introduce kill switches, back doors or Trojan viruses to render systems ineffective upon command or to leak sensitive information.**
>
> Source: "Trusted State-of-the-Art Microelectronics Strategy Study," July 2015, Potomac Institute for Policy Studies report.

components from sabotage or espionage—the trusted process is a response to a strategic SCRM issue: that companies are increasingly moving their semiconductor fabrication facilities overseas. As with the other Trusted Suppliers, purchasing components from entities with accredited trusted processes can be more expensive than purchasing them from commercial suppliers, which limits the use of this option for reducing risk. Even when components are purchased from trusted sources, continuous configuration control and parts management remains necessary.

Component Testing

Testing can provide an effective method to help detect counterfeit parts and identify unintentional design flaws rather than find that potential malicious alterations, particularly latent functionality that could be triggered well after a component or software code is already installed in a system. Normal test protocols operate under the assumption that the test process will expose all of a component's possible behaviors. Testing can help verify whether a component works according to the design specifications, but testing has its limitations. Malicious functionality can remain hidden or dormant during normal testing and is difficult to discover. Investigating the supply chain of each critical component begins with determining its source and possible attack vectors along the supply chain.

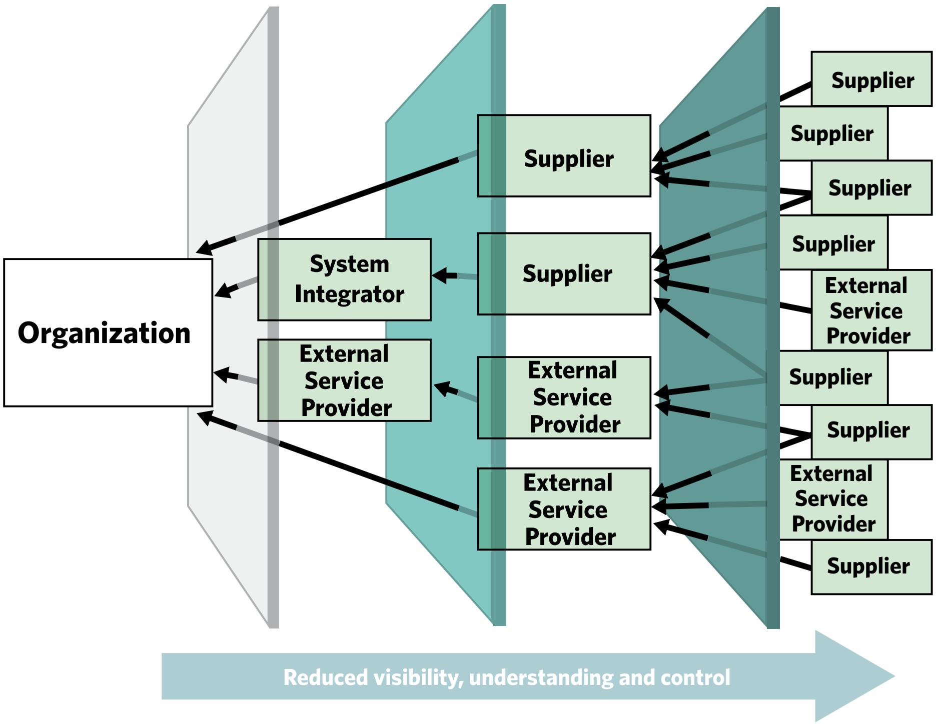
Responses to Risk

It is impossible to eliminate all risks associated with the supply chain, especially when it comes to the use of electronics, computers and other computerized components. The attempt to remove or mitigate risks can be extremely expensive and time consuming. Applying countermeasures and mitigations will lessen the consequence of a compromised component or system by incorporating risk management strategies throughout a component's or system's life cycle. There are four basic ways to address identified risk:

- **Treat it**: Employ protective measures (countermeasures and mitigations) that may either reduce the consequence or likelihood of a threat exploiting or triggering a vulnerability, or remove the threat or vulnerability that generates the risk.
- **Transfer it**: Allocate some or all of the responsibility for risk mitigation to another organization and/or phase of life cycle by passing the risk along.
- **Tolerate it**: Make a conscious decision to continue with the activity (or acquisition) despite the identified risk.
- **Terminate it**: Eliminate the likelihood of a threat, susceptibility to a vulnerability or impact of exploitation by not continuing with the activity or acquisition.

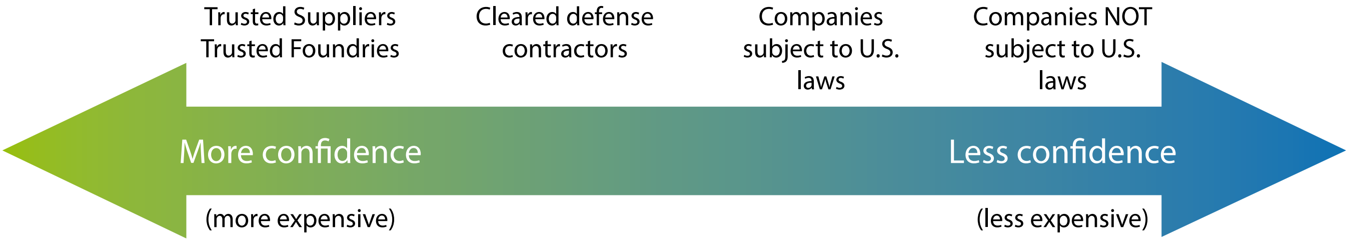
The options to consider in response to identified risks associated with a component range from doing nothing (usually not

Figure 2. An Organization's Visibility, Understanding and Control of Its Information Technology Supply Chain


Organization
System Integrator
External Service Provider
Supplier
Supplier
External Service Provider
External Service Provider
Supplier
Supplier
Supplier
Supplier
External Service Provider
Supplier
Supplier
External Service Provider
Supplier
Reduced visibility, understanding and control

Source: N*IST Special Publication 800-161, SCRM,* April 2015, Page 8.

Figure 3. Trusted Suppliers



Source: "Managing Information Communications Technology Global Supply Chain Risk Awareness Module 2014," Institute for Defense Analyses (IDA), Page 33.

an option) to redesigning a system to avoid using a component that does not have acceptable risk mitigation options. Risk mitigation requires significant effort and could have a significant effect on cost and schedule.

Choosing an option that requires less effort will save upfront costs but often will result in greater costs later in the system's life cycle. Vulnerabilities identified early in a system's design often can be significantly lessened or eliminated with simple design changes or procurement constraints at relatively low cost. It is much less expensive to design in cybersecurity from the very inception of the project rather than to implement cybersecurity fixes throughout a system's life cycle.

Conclusion

Supply chain risk management is not a simple one-time, one-solution scenario. All of those in the acquisition field need to understand the need and implications of poor practices that can easily lead to cost overruns and, even worse, a security incident where DoD information is stolen. The acquisition workforce needs to institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions, address cybersecurity in relevant and meaningful training, include a requirement to purchase from original equipment manufacturers, their authorized resellers or other trusted sources whenever available and increase government accountability for cyber risk management. The Defense Acquisition University is working closely with Supply Chain Risk experts from the Aviation and Missile Research, Development, and Engineering Center (AMRDEC) Cyber Campus to present the most up-to-date information and integrate it into the curriculum. Later articles will discuss further the threats, vulnerabilities and policy associated with the supply chain and the DoD path forward.

The authors can be reached at **heath.ferry@dau.mil** *and at* **van.poindexter@dau.mil**.