Supply Chain Risk Management

A Framework for Assessing Risk

Introduction: Increased risk to supply chains are due to evolving dependence on globally sourced commercial Information and Communication Technologies (ICT) for mission critical systems and services. Resulting residual risks are passed to end-user enterprises in the form of products and services that may contain defective, counterfeit or otherwise tainted components with malware, exploitable weaknesses and vulnerabilities from sources with unknown trust. This SCRM Framework addresses risk topics relevant to the reliance on others who make risk decisions about matters in which they are not the risk owners. The SCRM Framework also addresses means to identify and counter supply chain attacks that can exploit products and processes throughout the supply chain lifecycle.

In the past, business leaders viewed risk management as a balancing act between **Cost, Schedule and Performance**. When well-executed, managers were rewarded for a job well done. But the risk landscape is constantly changing which demands that the evaluation and management of those risks adjust accordingly. Security is such an instance. With the rapid rise of asymmetric threats and constant attacks to computers and networks worldwide **Security must be added** as a 4th pillar of the risk equation **with equal emphasis to Cost, Schedule, Performance**.

$$\text{RISK} = f(\text{Cost, Schedule, Performance, Security})$$

When calculating risk, program managers understand that influences on any risk pillar impacts the others. For example, pressures on schedule resulting from an advanced delivery date may lead to an increase in cost and decrease in performance or worse, compromised security. Or an increase in performance requirements may delay program implementation and increase costs with an unintended consequence of skimping on security in ways that expose the program or even the enterprise to attack.

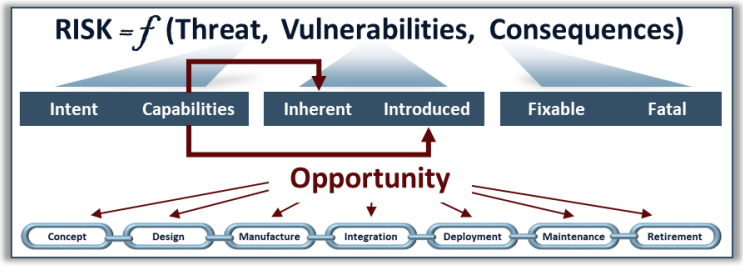
As a result, assessing and mitigating all risk components should be addressed and resolved in a product or service as part of an *integrated risk reduction* program**.** For critical programs, this demands that tradeoffs in performance and specifically security should not be made to the advantage of either cost and/or schedule. If the true lifecycle costs and benefits of managing security risks are fully calculated, it is likely that security can be transformed from a cost drain to a profit center. To more deeply understand and justify performance and security risks as an imperative, it is necessary to consider the **functions of Threat, Vulnerability and Consequence and their calculated risk impact**.

$$\text{RISK} = f(\text{Cost, Schedule, Performance, Security})$$

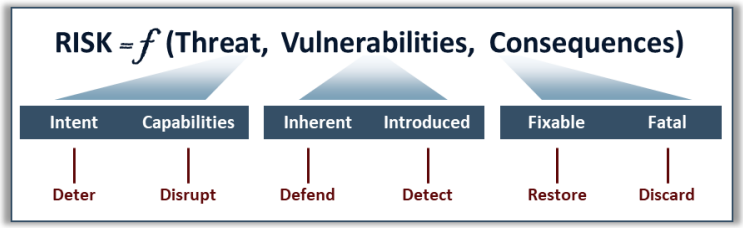
$$\text{RISK} = f(\text{Threat, Vulnerabilities, Consequences})$$

From the **threat** perspective, an understanding of the adversary's intentions and capabilities is vital. Key to this is using the latest threat information to determine if specific and credible evidence suggests an item or service might be targeted by adversaries. But, it must be noted, that while adversaries wish to do harm, they can only be successful if systems, processes, services, etc. are vulnerable to attacks. **Vulnerabilities** are weaknesses which are either *inherent* to the system or have been *introduced* into the system by an outside agent. *Inherent* vulnerabilities are system shortcomings due to design oversights, poor quality control, or faulty processes, and are not normally due to malicious actions. Conversely, vulnerabilities that have been *introduced* (intentionally) are usually a result of nefarious activities from insiders or outsiders that have gained access to compromise some process along the supply chain lifecycle. Lastly, the **consequence** of the risk must be considered. If the threat is realized and the system is attacked and/or compromised, the outcome is either fixable or fatal.

In all cases for attacks to occur, there must be **an opportunity for the adversary's capabilities to be applied**. At any point in the supply chain lifecycle – from concept to design, manufacture, integration, deployment, maintenance and retirement – the *threat may be realized* when an adversary's **capabilities and intentions** align with the inherent or introduced **vulnerabilities** of the system. There is no certainty that an attack will happen, but risk is realized when this alignment occurs. For example, in the manufacturing phase, there may be poor programming processes that permit use of software from an unwitting, non-trusted third-party that has been compromised by a bad actor. Or in the maintenance phases, there may be poor standard operating procedures that permit a maintenance technician to enter and roam a facility, unsupervised, and to replace a broken board with an unchecked counterfeit that has malware installed. Scenarios such as these illustrate that often there is a reliance on others to make risk decisions about matters where they are not the risk owners, thus allowing unknown or misunderstood residual risk to be passed to end-users, programs, systems or even the organization. This demonstrates the need for an *integrated risk reduction* program to be enforced throughout the enterprise.



Once the functions of threat, vulnerability and consequence are measured, recorded, and evaluated, then actual risk can be determined – and a risk management program designed and implemented. In this way a robust set of **options can be developed and comprehensive measures can be executed to manage, mitigate, counter, avoid, or even buy down** risk created by the nexus of threats, vulnerabilities or consequences imposed on the enterprise.



1) Graphics in this presentation originated from the Defense Science Board Report *Resilient Military Systems and the Advanced Cyber Threat,* February 2013
2) Introduction of the concept of Security as the 4th Pillar can be found in the MITRE Report *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*, August 2018