# Supply Chain Risk Management

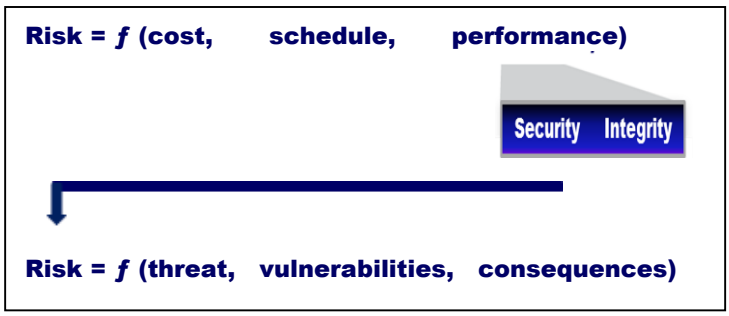
## *A Framework for Assessing Risk*

***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.

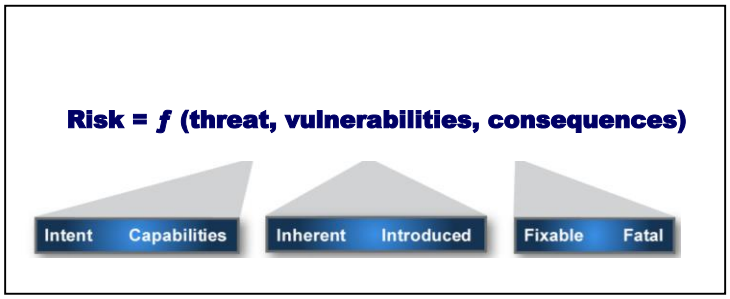
In the business world, many leaders view risk management as balancing the **functions of cost, schedule and performance** and when well-executed, managers provide awards and recognition. Program managers know that influences on any one of the functions impacts the others. For example, pressures on schedule because a delivery date is advanced may lead to increases in cost and decreases in performance. On the other hand, increases in performance requirements may delay the implementation of the program and increase the cost.

**Risk = *ƒ* (cost, schedule, performance)**

For some critical programs, tradeoffs in performance cannot be made for advantages in cost or schedule. Risk related to performance must account for integrity and security in a product or service. To better understand performance risk it is necessary to consider the **functions of threat, vulnerability and consequence**.

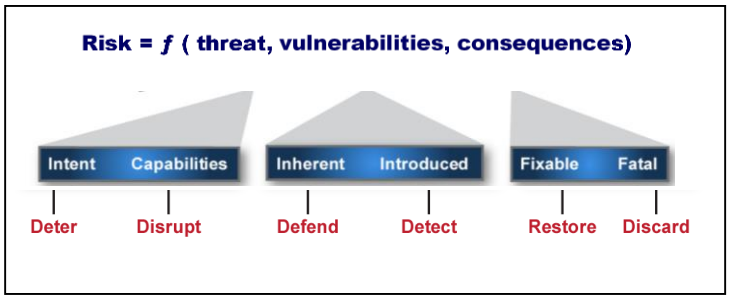


From the **threat** perspective, an understanding of the adversary's intentions and capabilities is vital. Key to this is using the latest available threat information to determine if there is specific and credible evidence that the item or service might be targeted by adversaries. While there may be adversaries that wish to do harm, they can only do harm to systems that are vulnerable to attacks. **Vulnerabilities** are weaknesses which are either *inherent* to the system or have been *introduced* by an outside agent. *Inherent* vulnerabilities are those system shortcomings due to such things as design oversights, poor quality control, or faulty processes, which normally are not due to malicious actions. Conversely, vulnerabilities that have been *introduced* 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 attacked and/or compromised, the outcome is either fixable or fatal.




In all cases 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 the risk is there when this alignment occurs. For example, in the manufacturing phase, there may be poor programming processes that permit the use of software from a non-trusted third-party that has been unwittingly compromised by a bad actor. Or in the maintenance phases, there may be poor standard operating procedures in place whereby a maintenance technician can enter a facility unsupervised and can replace a broken system board with an unchecked counterfeit that has had malware installed. Unfortunately, current processes promote reliance on others to make risk decisions about matters where they are not the risk owners, thus allowing residual risk to be passed to end users and enterprises.


Once the functions of threat, vulnerability and consequence are measured, recorded, and evaluated, risk can be determined – and a risk management program designed and implemented. In this way **mitigation options can be developed and potential countermeasures can be considered to buy down risk** in the area of threat, vulnerability or consequence – or any combination of the three.




Some graphics in this presentation originated from the Defense Science Board Report *Resilient Military Systems and the Advanced Cyber Threat* Feb 2013