

## How to Win the Cyber War

By Sean Price – ISSA member, Northern Virginia, USA chapter



There is a growing consensus that we defenders are losing the cyber war. Some suggest that our failings are strongly related to the relentless increases in system complexity and unknown factors such as new vulnerabilities and attack methods. This article proposes that complexity is a self-fulfilling myth and the unknowns are irrelevant.

Security professionals consider complexity the bane of security. But, is this really accurate for IT systems? In most cases, activities such as data access and network communications are observable and can be understood. Given this point of view, an IT system is not difficult to quantify or analyze. In contrast, a complex system is something comprised of system components that are difficult to analyze or understand. For example, analog circuits within feedback loops are notoriously difficult to analyze from a troubleshooting perspective due to component interactions. We probably consider IT systems complex because we simply do not know how the pieces-parts (software components) work. It is this lack of knowledge that is our doom.

People tend to value user friendly interfaces that simplify system usage. To this extent, we have wandered down the plug-and-play road at our own peril. Our lack of understanding of how things work and interact limits our ability to defend against attacks. Even more incomprehensible, we typically do not have an accurate inventory or understanding of the software components in our systems. This lack of granular information impedes our ability to achieve an appropriate level of maintenance and security for our systems. Consider a government contract for a new fighter aircraft. Every individual nut, screw, panel, wire, and electrical component is

painstakingly identified and noted with its characteristics. The aircraft technical manuals list component attributes such as physical dimensions, torque values, and electrical properties. This level of detail is needed for proper maintenance of the aircraft. This is real systems engineering and management that is sadly lacking in the IT and security professions. How can we ever hope to defend what we do not know? Since we do not do what is necessary from a systems engineering perspective, it becomes increasingly difficult to develop effective countermeasures. Thus, the myth of complexity perpetuates itself due to our poor engineering and management practices.

Presently, we do not know the composition of our systems, attacker capabilities, and emergent vulnerabilities. So we attempt to create defenses by gazing into the abyss of the unknown unknowns using risk-based approaches devoid of adequate system knowledge. Our current paradigm is an operation of futility grounded in the perpetuation of ignorance. It is time to change that. The following principles are proposed as a new security management paradigm:

**Principle 1:** Assurance is the primary security attribute and is proportional to the behaviors of those who derive system components (i.e., developers and integrators) and others (i.e., users) having access to system resources. This suggests that the attitudes and actions of those who develop components, integrate, administer, manage, use, and allocate resources have the biggest impact on security.

**Principle 2:** Knowledge of the composition, functionality, capabilities, and location of system components and data structures drives our ability to select the most appropriate countermeasures.

This is to say that the degree of detailed knowledge of a system influences our ability to defend it.

**Principle 3:** Security risk is a function of our assurance (Principle 1) and knowledge (Principle 2) of a given system. In this regard, unknown threats and vulnerabilities are irrelevant. Greater assurance and knowledge empowers us to detect and repel attackers. This results in lower risk. In cases where there is low assurance or knowledge, it is more difficult to defend the system and risk would be high.

The current security paradigm is reactive because we primarily attempt to defend against the unknowns. However, this new paradigm relies on a basis of knowledge and enables a proactive defensive posture. Proactive security is possible when sufficient understanding of behaviors and knowledge of a system are joined to identify attacks and penetrations. The new paradigm will make attacker activity, such as botnet infections, apparent since they are out of place according to the knowledge we have of our systems. We must turn from the abyss of the unknown unknowns and look to the light of knowledge. This will enable us to strongly defend our systems and begin to win the cyber war.

### About the Author

Sean M. Price, CISA, CISSP, is a security researcher and consulting living in northern Virginia. He specializes in the design and evaluation of security programs and architectures. You can reach him at [sean.price@sentinel-consulting.com](mailto:sean.price@sentinel-consulting.com).