What gets measured gets done. Security engineering as a discipline is still in its infancy. The field is hampered by its lack of adequate measures of goodness. Without such a measure, it is difficult to judge progress and it is particularly difficult to make engineering trade-off decisions when designing systems.

The qualities of a good metric include that it: (1) measures the right thing, (2) is quantitatively measurable, (3) can be measured accurately, (4) can be validated against ground truth, and (5) be repeatable.

By “measures the right thing”, we mean that it measures some set of attributes that directly correlates to closeness to meeting some stated goal. For system security, we see the right goal as “freedom from the possibility of suffering damage or loss from malicious attack.” Damage or loss applies to the mission effectiveness of the information infrastructure of a system. The mission can be maximizing profits while making quality cars or it could be defending an entire nation against foreign incursion.

We therefore propose risk as a good metric for system security. The phrase “freedom from the possibility of suffering or loss” is indeed the English language definition of risk. More formally, the risk of some event happening is defined as the probability of that event happening multiplied by the consequences (damage or loss) from that event. The overall risk to a system therefore can be defined as the sum of the risk of all the bad events (failures) that can be induced by a malicious attacker on an information system. Of course, one must properly account for consequences so as not to count the same consequence more than once. In other words, if one bad event suffices to cause the loss of confidentiality of all data in a system, then you can not add that consequence in the sum for any other event that happens to cause full or partial loss of data confidentiality.

By the discussion above, risk appears to be a direct measure of the qualities that are sought in systems. Thus risk appears to meet the first criteria of a good metric by measuring the right thing.

The second criterion calls for quantifiable measurability. In principle, one can enumerate the complete list of bad things that happen to a system by malicious action. One can use hazard analysis techniques and attack trees to create such enumerations. Getting a complete list is hard, but it is doable at some level of abstraction.

Next, using the more formal definition of risk, one must find the probability of all the enumerated events and the consequences of such an event to mission effectiveness. Within mature disciplines such data can come from statistics on a long history of empirical events. Such are the techniques used by insurance companies. Unfortunately, the realm of information security has a very short history with little good objective data sets collected on attacks and with few (if any) rare catastrophic events yielding widespread critical damage (though some might say that some worms of the recent past did serious damage).

In principle, as more data is collected, probabilities can be established through empirical data. Until then, subject matter expert opinion based on difficulty, cost, and other such factors related to the bad event, can be used as an approximation. For events that end up having a profound effect on the final calculation of system risk, one can perform experimentation to try to form a better basis for those probabilities. The consequence part of the equation can be established through failure analysis linked back to mission effectiveness. It is most straightforward to do such an analysis if mission can be reduced to cost, but other measures can be established for more challenging missions such as national defense. So, we see that measurability is at least possible in principle, that it is practical today to some degree of accuracy, and that there is a path by which that accuracy can be improved.

The criteria of accuracy and validation are closely tied together. Without ground truth, neither can be established. This appears to be the most difficult criteria for security metrics. The ground truth of probabilities and consequences is hard to establish without a long history of empirical data, and even there it is hard to establish for rare events. To-
day, best effort is expert opinion back by rationale, including experimentation, modeling and other evidence that can be mustered to back the opinion. Eventually, such approximations can be replaced by the growing body of empirical data. So, even though validation today is problematic, it is possible to approximate validation and it will eventually be possible to do it with increasing accuracy.

How this relates to trustworthiness? A system is trustworthy if it is worthy of reliance on the character, integrity and ability of system to meet its goals. Without a metric to gauge progress toward its goal, it is likely to continue to be difficult to make efficient progress toward trustworthiness as a system property.

Mr. O. Sami Saydjari is the founder and Chief Executive Officer of the Cyber Defense Agency, where he provides vision, leadership and expertise for building a Research and Consulting concern that creates effective systematic defenses for high-value systems against aggressive cyber-attack. Before founding the Cyber Defense Agency, Mr. Saydjari was a Senior Staff Scientist in SRI International’s Computer Science Laboratory, where he was the program leader of the Cyber Defense Research Center (CDRC). While at SRI, Mr. Saydjari led the survivability assessment of the DARPA UltraLog program, whose goal to improve the survivability of software agent architectures to solve large scale distributed applications.

Mr. Saydjari has 18 years of experience performing and directing information assurance research, including 13 years at the National Security Agency and 3 years as a DARPA Program Manager of Information Assurance. Prior to SRI, Mr. Saydjari was the Information Assurance Program Manager for DARPA’s Information Systems Office. He created and drove the security architecture and technology for a common reference architecture for DARPA and DISA’s advanced programs. His focus areas include high-assurance operating systems, network security, public-key infrastructures, and security architecture.

Before his assignment at DARPA, Mr. Saydjari was the technical director of the Office of Network Security Infrastructure for the National Security Agency (NSA). In this role, Mr. Saydjari performed an advanced survivability architecture analysis of the MISSI system, including attack trees and fundamental review of required system architecture properties. At NSA, Mr. Saydjari was also the leader of several information assurance research teams in A1 INFOSEC systems design (LOCK), highly assured distributed operating systems design, and trustworthy network systems design.

Mr. Saydjari earned his M.S. in Computer Science from Purdue University. The Director of NSA named Mr. Saydjari an NSA fellow in 1993 and 1994. He has published more than a dozen technical papers in the field of information security and has presented the results of his research at both such as the National Cryptologic Quarterly, the National Computer Security Conference, IEEE Security and Privacy Conference, and the ACM New Security Paradigms Workshop. He is based in Wisconsin Rapids, Wisconsin.