"Beyond the CIA Triad: The 9 Point Core Security Principles Star Versus The CIA Triad For Better Risk Evaluation and Mitigation Strategies."

By Jim West

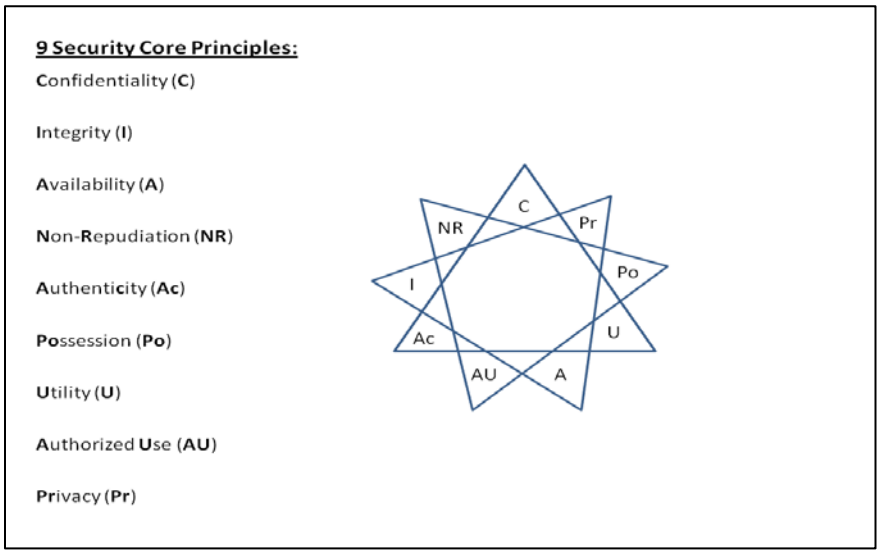
Helps senior leadership with a visual representation of how their mission goals align with their organizations security projects and efforts.

Helps auditors and assessors provide better understanding on how to mitigate via defense in depth and more precisely accommodate for weaknesses.

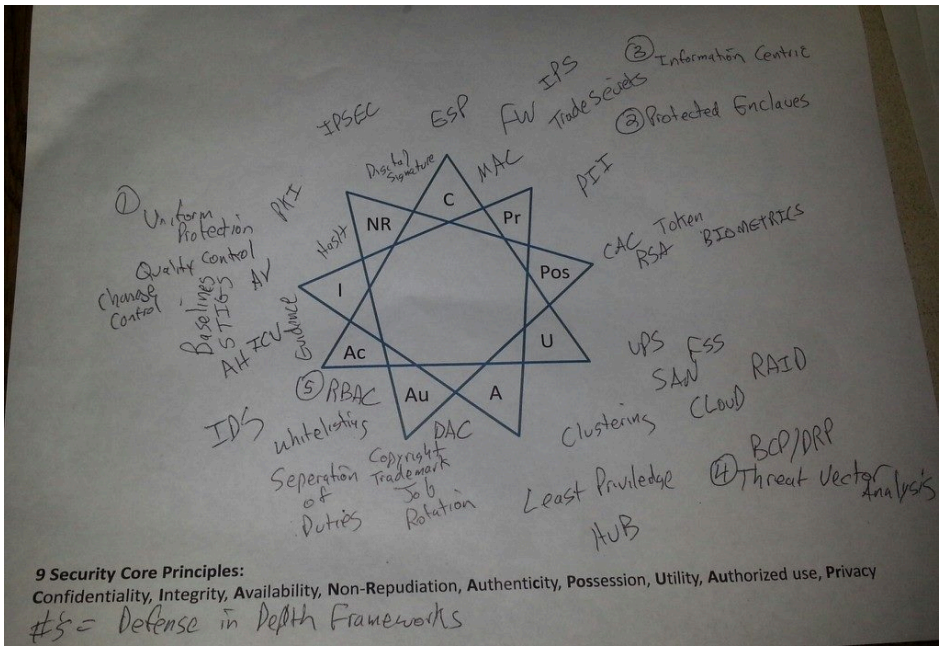
Helps organizations develop their strategy to align security plans and projects with their current mission as well as their vision.

Everyday risk is identified, mitigated, transferred, accepted, or (in a worst case scenario) ignored. What is apparent in today's ever changing world of cyber security is that risk is not something to be taken lightly. Getting senior leadership's understanding of risk, the security professional's valuation of risk, and the mitigation actions completed is all part of the never ending risk negotiation. Currently many security professionals speak of how the CIA triad plays a part in the management of risk, but lacks the details of considering all aspects of risk. This triad only takes into consideration the factors of confidentiality, integrity, and availability. This does not consider the other 6 core security principles of Utility, Authentication, Authorized Use, Privacy, Possession, and Non-Repudiation. The nine (total) core security principles are needed to fully address risk in more detail than this triad allows.

According to *The Official (ISC)2® Guide to the ISSMP® CBK®:* "The traditional information security triad consists of confidentiality, integrity, and availability. *Confidentiality* is the protection against the risk of unauthorized disclosure; *integrity* is the protection against unauthorized modification; and *availability* is the protection against the risk of denial of service. Don Parker then added possession, utility, and authenticity. *Possession* is the protection against the risk of loss of theft; *utility* is the protection against the loss of the ability to use for the intended purpose; and *authenticity* is the protection against the risk of not conforming to reality. Nonrepudiation, authorized use, and privacy round out the nine core principles. *Nonrepudiation* is the protection against the risk of deniability; *authorized use* is the protection against the risk of unauthorized use of cost incurring services; and *privacy* is the protection against the risk of disclosing personal information." (Tipton, Litchko, Hennell, Lang 136).



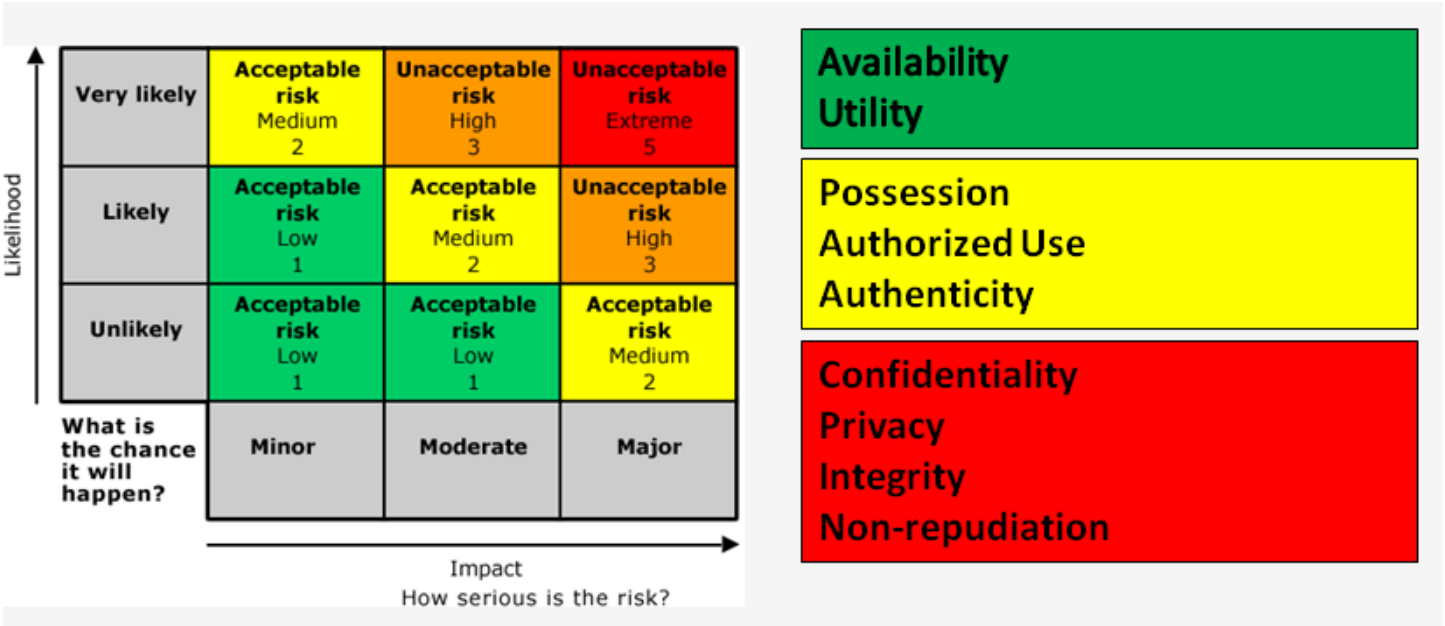
When all 9 core security principles are brought into the picture it provides a more detailed understanding of how technologies align to the principles protecting the organization's goals. This visual representation allows security professionals to understand what technologies are available and how they can be used to mitigate risks in regards to the identified core security principle.



There is correlation between opposite points on the star. This does not show direct opposites in security, but rather to display how certain technologies are not directly involved in mitigation of certain core principles. Example: Your organization is in the defense sector and confidentiality is at the top of its mission's goals. As certain confidential information gets leaked to the public (more available) then confidentiality is compromised. Another example is that Denial of Service (or DoS) attacks would target the Availability and Utility sections of the star. This does not directly mean a compromise in Integrity or Confidentiality. So again the example of Confidentiality and Availability are just one example of how a weakness in one area could undermine another, but this is not always the case where there is still room for risk negotiation to occur.

From an auditors perspective, measuring risk should account for factors such as current security measures/countermeasures employed, the configuration of security enabled devices, risk response, security plans, procedures, and user awareness. When an auditor identifies a weakness they can easily align it to the core principle and provide a more detailed recommendation to leadership on the options available to mitigate the weakness(es). If the auditor's rationale was a lower risk, it is better to align such a rationale with the core principle and related technologies to better explain the rationale than simply stating 'defense in depth'. Defense in depth now can be visually applied to risk assessments.

Once leadership begins to employ the 9 point star in their risk management process(es), they can assign values from a typical risk appetite chart to the star. An organization can then list out in detail which core security principles they are willing to accept risk on, and those related technologies associated with the principle. Example: A company has a requirement for high data availability (non-sensitive data), so they would seek out technologies around Availability & Utility. After a quick cost benefit analysis the company determines that they simply cannot afford their own SAN, but with the newer technology of cloud computing they could possibly leverage a third party contract that provides them with the Availability required and the solution was driven by the relation of the core principle.



Now the trick question; how do all of these core principles come together? They appear in user awareness, technical training, security plans, policies, and procedures. Granted, new turn key technologies alleviate a great deal of the workload, but without proper training on how to deploy, configure, utilize, and maintain these technologies their effectiveness is only as good as the level of user's training. With all of the technical tools in place, users still pose a risk through insider threats, and data leaks. This is where reviewing Authorized Use and Availability of data in regards to the organization's Confidentiality goals are key. These are further broken down by common security concepts like the separation of duties, least privileged, and job rotation methodologies. These are aligned to the 9 point star, and help address threats once they have been identified.

The 9 point core security principles star will help many organizations seek out possible solutions to risks, while auditors detail what is lacking in an organization's ability to achieve its security goals, and finally provide senior leadership a more detailed visualization of what principles are acceptable risk and which ones are not. The goal is to provide a new perspective to support risk management and it's never ending negotiation.