Balancing Autonomy and Collective Responsibility

Rethinking the Marine Corps' senior information security officer role

by Dr. Daniel Corbin

>Dr. Corbin is the Chief Technology Advisor for the Deputy Commandant for Information's Information, Command, Control, Communications, and Computers and is the Marine Corps' Senior Information Security Officer. He has worked in DOD information technology acquisitions for over 35 years.

The Charge of the Light Brigade was a military action involving the British light cavalry led by Lord Cardigan against Russian forces in the Battle of Balaclava during the Crimean War. This event is infamously remembered for its clear miscommunication, disregard for evident risks, and the resulting high casualties.

The British light cavalry, the Light Brigade, was ordered to pursue and harass a retreating Russian artillery battery. However, due to miscommunication and possibly a misunderstanding of the orders, the Light Brigade was sent down the wrong valley, heading straight toward a different, well-fortified, heavily armed Russian artillery unit.

The risks were evident and known to some within the command. Enemy guns flanked the valley into which the Light Brigade was charging, and the end of the valley was blocked by the artillery they were ordered to attack. Despite this, the commanders on the ground did not sufficiently question the order, leading to a disastrous frontal assault against a well-prepared enemy.

As they charged down the valley, the Light Brigade came under intense artillery and rifle fire from three sides. The charge displayed remarkable courage and discipline but led to heavy British casualties. Of the roughly 670 cavalrymen who charged, about 110 were killed, and 160 were wounded, a casualty rate of about 40 percent. Nearly 375 horses were also lost.[1]

The Charge of the Light Brigade has become a symbol of heroic failure and futile bravery. The fact that the risks were known but not effectively acted upon makes this episode a poignant example of how soldiers' valor can be squandered through poor decision making and communication. It highlights the importance of clear and sensible orders and the need for commanders to understand and appropriately respond to the risks they face.[2]

It is not an exaggeration to argue that, if not for the diligent efforts of the Marine Corps Forces Cyber Command, units within the Marine Corps could experience the digital analog of Balaclava. This article provides four recommendations to increase the Marine Corps' cyber security posture based on my observation of weaknesses in our cyber security program. Maintaining the situation where the senior information security officer (SISO) alone establishes the level of cyber risk the Marine Corps adopts presents complex challenges. It risks misallocating resources and fragmenting the security posture, potentially fostering an organizational culture that is overly risk-averse or excessively risk-tolerant. This can stifle innovation and operational efficiency and negatively affect inter-departmental trust, ultimately diminishing the effectiveness of our cybersecurity program. We can improve cyber readiness through greater collaboration, communications, and information feedback while increasing the value of our information technology (IT) and command, control, communications and computers (C4) investments. [3]

However ... the process does not consider the risks associated with the cyber security of our digital systems.

The Marine Corps maintains the structures and processes to vet accepted risks within its operations. For example, it maintains a comprehensive method for identifying and financing the necessary capabilities, addressing existing capability gaps, and managing the residual risks within Marine Corps programs. This process, detailed in *MCO 7000.1, Programming, Planning, Budgeting, Execution, and Audit*, is integral in recognizing the risks associated with capability gaps. It is a critical tool Marine Corps leadership uses to make informed decisions to mitigate or accept risks.

However, I argue, generally, the process does not consider the risks associated with the cyber security of our digital systems. The systems are fielded with vulnerabilities identified during cyber security reviews referred to as the Authority to Operate or Risk Management Framework (RMF) process. The SISO determination made from the cyber RMF process likely results in one of two suboptimal outcomes: the Marine Corps spends resources closing vulnerabilities where accepting risks was warranted or the security risks are accepted when they should not have been. Suboptimization occurs because the SISO approves or disapproves the IT and C4 systems based on an *individual* tolerance for risk.[4] The SISO uses technical data the system owner provides to determine the total risks within the system. Based on the assessment, the SISO determines if the value of the system's capabilities warrants accepting the dangers to the mission caused by the new vulnerabilities. The SISO and the project office have insight into the risks of fielding the system. Still, only the SISO has access to the information describing the totality of the risks within the entire IT and C4 portfolio on our networks. That information needs to be shared.

When the risks accepted are within the policy limits described in DOD directives, there is usually no feedback to a mission commander or functional area manager.[5] As in the incident of the Light Brigade, risks are known to a few but not to those who need the information to inform warfighting and business decisions. This article argues for a paradigm shift that involves the broader organization in defining risk acceptance levels and assesses the accumulated cyber risks within a portfolio to understand the risk to the supported mission.

Understanding the Cyber Risk Management Framework

The RMF, defined in the *National Institute of Standards and Technology Special Publication 800-37*, is a process to manage and mitigate information systems risks by focusing on controls that moderate confidentiality, integrity, and availability of the data within the IT systems.[6] Many of these RMF controls are the same ones needed to ensure our processes' integrity in many areas. It will not be until senior leaders understand the relationship between these IT cyber controls and those contemplated in the Marine Corps Managers' Internal Control Program will those leaders see the benefits of the process that validates the IT controls—a value rather than a hindrance to their efforts.[7] Here is an overview of the framework in layperson's terms:

- *Categorize Information Systems:* Identify what types of information the system handles and the impact if this information is compromised. This step is about understanding what's at stake. For example, does public information need more protection, like a website or geolocation data in a tactical system?
- *Select Security Controls:* Choose measures to protect the system. Think of this as setting up defenses based on what you are trying to protect. For example, the geolocation data will require different controls to safeguard our Marines than information on public websites.
- *Implement Security Controls:* Put the chosen measures into action. This step is where the security team and project office begin taking risks. Numerous reasons exist, such as funding or technical limitations, that prevent a project team from implementing controls and result in vulnerabilities within the system. If, for example, there are insufficient funds to modernize our radios, theoretically, there could be a request to leave geolocation data unencrypted. The program manager would commit to correcting this shortfall in the Authority to Operate package.
- *Assess Security Controls:* Checks are conducted to ensure the implemented security measures work effectively.
- *Authorize Information System:* The Marine Corps' SISO reviews the security measures and decides if the risks in the system are acceptable when considering the benefits it provides.
- *Monitor Security Controls*: Finally, the system is continuously monitored to ensure the configuration is secure against the changing threats.

Establishing the Risk Appetite Levels

The purpose of the RMF process is to understand the information system risks or the "state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome"[8] and take steps to reduce those risks to a level acceptable to the organization's leadership. Increased threats, changes to the sensitivity of the data, or changes to configurations can change the required controls.

Risk tolerance refers to the specific amount of risk an organization is willing to accept or retain to pursue its objectives. It is a more detailed and practical aspect of risk management, often quantified regarding potential loss, impact, or other measurable criteria. Risk tolerance is closely related to, but distinct from, risk appetite.[9] While risk appetite is about the broad level of risk an organization is willing to take, risk tolerance defines the boundaries or limits of acceptable risk within that overarching framework.

In practical terms, the SISO attempts to balance the risks associated with IT systems even if no additional guidance is available. Risk adoption is communicated and expressed within the DOD as part of its risk management framework.[10] When the risk levels set by the DOD are exceeded, the Department of the Navy must approve the offending system's use.

Description of Improvement

There have been instances where SISO misalignment with Marine Corps strategy has resulted in either overly cautious or risky positions with suboptimal outcomes. Risk aversion resulted in significant program cost growth and schedule delays in one instance involving our primary data center. This occurrence underscores the necessity for a more integrated approach to risk management, incorporating input from a diverse range of stakeholders.

Input from domain stakeholders generally is not formally available to inform the SISO's risk assessment. More importantly, the risks accepted by the SISO are not hidden but not communicated to stakeholders responsible for mission capability. The determination of these risk levels has mainly been delegated to the discretion of the SISO, who must infer from strategic guidance leadership's intentions. For instance, the updated *Force Design 2030* underscores the Marine Corps' willingness to embrace risks in adopting robotics and autonomous systems to achieve a competitive edge. The SISO's evaluation of the authorization for such innovative systems is viewed through that perspective.

Like most organizations, the Marine Corps has a different risk acceptance profile than any individual.[11] The Marine Corps' leadership should shape a cyber risk profile using a vetting process to assess risks to other mission areas rather than relying on the SISO, who may not have the same global view as a group of senior Marine Corps leaders.

While one could argue the current situation enables rapid decision making about accepting cyber security risks, it can lead to a disconnect between the accepted risks and the organization's collective understanding of the aggregated risks. This is critical as we modernize using innovation. For example, develop, security, operations benefits are improved with a mature risk appetite program.[12]

We can improve communication of the cyber risks across our portfolios. While there are several cases where stakeholders have insight into previous risk acceptance decisions, it is limited. For example, the ongoing financial audit within the Marine Corps has exposed many instances in which IT control requirements that existed for years were not fully met for our audit-relevant systems. Still, the program manager and the SISO accepted the risk and allowed the system to be deployed without the proper controls. While no evidence suggests the accepted weaknesses have harmed the Marine Corps, the chance of exploitation existed, nonetheless. Based on the recent positive audit findings, the Marine Corps has a de facto risk appetite statement, which could read: *The Marine Corps will have a low-risk appetite for systems that feed our balance sheet.* This risk appetite for audit-relevant systems is having a positive effect. We need to institutionalize the process that elevated this enterprise risk and do it without dependence on external auditors.

The implications of continuing the approach in which the SISO establishes the risk appetite levels for the Marine Corps are multifaceted. In the short term, it leads to potential misallocations of resources and a fragmented security posture. In the long term, it risks creating an organizational culture that is either too risk-averse or too risk-tolerant, hindering innovation and operational efficiency. This disconnect also impacts inter-departmental trust and the overall effectiveness of our cybersecurity program.

The current situation can be addressed using an integrated model combining four lines of effort. This approach properly balances the SISO's autonomy with the collective responsibility of our senior leaders, ensuring that risk management strategies reflect the Marine Corps' diverse operational realities. Theoretical and practical arguments underscore the necessity for broader organizational involvement in risk management. The following four recommendations use an inclusive approach that aligns with systems thinking and best practices in risk management, enhancing the organization's ability to manage risks comprehensively and dynamically.

> ***By embracing a balanced approach ... we can enhance our cybersecurity resilience ...***

- *Stakeholder-Defined Risk Tolerances and Appetites*: Each functional area manager should define risk tolerances for each area. The SISO's role is to ensure that controls are implemented to achieve the risk levels established in the appetite statements. The SISO will require the aggregation and cumulation of all cyber risks to the mission to fall within the functional area manager-defined tolerances using Hubbard and Van den Hooven systematic methodologies.[13] Two examples of IT-related risk appetite statements are provided for consideration that the SISO could use to inform the risk assessments for all functional area IT systems.
- The Marine Corps has zero tolerance for *sharing data with unauthorized persons*. The Marine Corps has zero tolerance for sharing data with unauthorized persons which puts individuals at risk of personal injury or death, financial injury, or contact with classified data. This statement will drive the SISO to ensure controls are in place to minimize system data breaches.
- The Marine Corps has a MEDIUM risk appetite concerning adopting *new technologies or platforms*. The Marine Corps explores the potential of new technologies to improve efficiency and productivity while recognizing the potential for change management challenges and time or cost overruns with the need to harmonize digital innovation with operational and programmatic policy. The SISO will use this statement to be more accepting of the system even if it has a less mature change management system.
- *Revise Policy for Broader Stakeholder Consultation:* Policies and processes should be updated to formalize stakeholder involvement to ensure the SISO decisions align with organizational objectives.
- *Implement Checks and Balances:* Regular audits and peer reviews would ensure accountability and continuous improvement in RMF decision-making at the mission level.
- *Assess Gaps in System Controls:* The accumulated risks of unmet controls must be tracked to assess the risk across the portfolio to understand the potential of a cyber incident to have a material impact on a Marine Corps mission.

Implementation will require careful planning, collaboration, and continuous evaluation to adapt to evolving risks and functional changes.

Conclusion

Implementing these recommendations starts the journey toward a more inclusive and effective risk management process within the Marine Corps that is both a challenge and an opportunity.

By embracing a balanced approach that combines the SISO's expertise with the collective organizational wisdom of senior leaders, we can enhance our cybersecurity resilience and align our risk management strategy with the Marine Corps' broader mission and values. This shift is not merely procedural but a fundamental rethinking of how we perceive, manage, and communicate cyber risk, setting a new standard in cybersecurity risk management within the Marine Corps. To do less than these activities puts our mission leaders in the same situation as Lord Cardigan: unaware of the dangers he faces even though the information is available to mitigate them.

Notes

1. Rachel Bates, "Negotiating a 'Tangled Web of Pride and Shame': A Crimean Case-Study," *Museum and Society* 13, No. 4 (2015).

2. Erynn Kim, "The Charge of the Light Brigade: Giving Meaning to A Meaningless War," Concord Review 21, No. 4 (2011).

3. Martina Neri, Federico Niccolini, and Luigi Martino, "Organizational Cybersecurity Readiness in the ICT Sector: A Quanti-Qualitative Assessment," *Information & Computer Security* 32, No. 1 (2023). Cyber readiness refers to an organization's ability to identify, prevent, and respond to cyber threats. It involves taking proactive actions to protect the security of digital assets, stay current on the latest security strategies, and continuously assess and improve cybersecurity measures. This readiness encompasses human behavior, policies, and technical expertise, and it is an ongoing effort that requires continuous monitoring and education. Achieving cyber readiness involves making decisions based on real data and evidence of security outcomes, as well as implementing cybersecurity frameworks, maturity models, and training programs. Organizations need to be fully prepared to defend against cyberattacks and mitigate potential risks.

4. Generally, within the DOD it is the authorizing official that has the responsibility to determine if a system is authorized to be used within the network with SISO oversight. The SISO and authorizing official are the same individual in the Marine Corps.

5. Department of Defense, *DoDI 8510.01 Risk Management Framework For DOD Systems*, (Washington, DC: 2022). Office of the DOD Chief Information Officer. Functional area managers generally have responsibility for the system and the missions it supports.

6. National Institute of Standards and Technology, NIST *SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View*, (Washington, DC: 2018).

7. Commandant of the Marine Corps, *Marine Corps Managers' Internal Control Program,* (Washington, DC: 2018).

8. Douglas W. Hubbard and Richard Seiersen, *How to Measure Anything in Cybersecurity Risk* (Hoboken: John Wiley & Sons, 2016).

9. Terje Aven, "On the Meaning and Use of the Risk Appetite Concept," *Risk Analysis* 33, No. 3 (2013); and Festus M. Epetimehin, "Impact of Risk Appetite on the Value of a Firm," *European Scientific Journal* 9, 22 (2013).

10. *DoDI 8510.01.*

11. "Impact of Risk Appetite on the Value of a Firm."

12. Olivia H. Plant, Jos van Hillegersberg, and Adina Aldea, "Rethinking IT Governance: Designing a Framework for Mitigating Risk and Fostering Internal Control in a DevOps Environment," *International Journal of Accounting Information Systems* 45, (2022).

13. Chris van den Hooven, "Quantitative Risk Calculation in Cybersecurity: The Value of Quantifying Risk," *ISSA Journal* 18, No. 10 (2020); and *How to Measure Anything in Cybersecurity Risk* (Hoboken: John Wiley & Sons, 2016). Hubbard describes the application of quantitative techniques to assess and measure uncertainty in cybersecurity by applying statistical methods.