Journal of Information and Technology

A Review of the Cybersecurity Programs in the United States Army

Grayson Sawyer & Brayden Emmett

ISSN: 2617-3573

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information and Technology
Volume 5||Issue 1||Page 22 -30 ||October||2021|
Email: info@stratfordjournals.org ISSN: 2617-3573

A Review of the Cybersecurity Programs in the United States Army

Grayson Sawyer, University of Phoenix

Brayden Emmett, University of Phoenix

***How to cite this article*: Sawyer G. & Emmett B. (2021). A Review of the Cybersecurity Programs in the United States Army. *Journal of Information and Technology. Vol* 5(1) pp. 22-30.** https://doi.org/10.53819/81018102t2017

Abstract

Cybersecurity is very complex, and as such, decisions regarding cybersecurity are highly intertwined with the functionality and application of systems. The threat to cybersecurity is, however, ever-evolving and decisions regarding cybersecurity, therefore, need to be made with this in mind. Cybersecurity systems, therefore, need to be tailored to individual systems, be adaptive, have the ability to evolve with the threat as well as be highly integrated with the system designs and the mission these systems support . In the military, it is critical to develop systems that maintain the expected level of confidentiality, non-repudiation, authentication, integrity, and availability that aids towards the collective goal of cybersecurity. In the military there are several stakeholders that play a key part in cybersecurity with the main ones being; the ones commanding or using the military system, the ones involved in the acquisition, life-cycle management and testing, the authorizing officials, the Chief Information Officer (CIO) and the intelligence and the counterintelligence officers. Accountability and control is, therefore spread out throughout the organization. This, however, leads to the blurring of roles and responsibilities. In conclusion, therefore, even though militaries exist for the purpose of combat most of the time, they operate in relatively peaceful conditions. During these peaceful times, they imagine and manufacture wartime conditions to determine their preparedness and the chances of a victory with the current conditions and resources. A communication plan approach will be able to tear down the expected natural resistance since the leaders will support the proposed changes and even devote resources to see that they are successful. The purpose of the communication plan is to, therefore, make the leaders the advocates for change. This is based on the understanding that in this environment, change is not possible without support from the leadership.

Keywords: *Cybersecurity, Intelligence, Communication & United States Army*

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information and Technology
Volume 5||Issue 1||Page 22 -30 ||October||2021|
Email: info@stratfordjournals.org ISSN: 2617-3573

1.1 Introduction

In the military, it is critical to develop systems that maintain the expected level of confidentiality, non-repudiation, authentication, integrity, and availability that aids towards the collective goal of cybersecurity. In the military there are several stakeholders that play a key part in cybersecurity with the main ones being; the ones commanding or using the military system, the ones involved in the acquisition, life-cycle management and testing, the authorizing officials, the Chief Information Officer (CIO) and the intelligence and the counterintelligence officers. Accountability and control is, therefore spread out throughout the organization (Davidson, 2020). This, however, leads to the blurring of roles and responsibilities. For instance, despite the operational command having the authority to assess and accept reasonable risk regarding a mission since he or she is well aware of the full scope of considerations to be made, it is the authorizing officer that is responsible for any action taken under his or her watch even though he or she may not be as familiar with the operating conditions. This is, therefore, an example of overlapping responsibilities and ambiguity that is characteristic of operations in the cybersecurity branch of the military (Snyder et al., 2015). This state of affairs makes it difficult to determine who is responsible for making the final decisions regarding risks to a mission. Furthermore, if an error occurs, it is not easy to determine who is ultimately culpable (Hall & Sobiesk, 2017).

During the acquisition process, signals are sent by the authorizing officials to the acquisition team and the CIO regarding compliance with existing security protocols (Bray, 2020). After carrying out a risk assessment, these officials decide on what controls to apply and goes on to determine whether the program effectively implements these controls. They do not carry out any testing, and as a result, they have limited insight into the effectiveness of these controls (Pajurek, 2017). Feedback on the effectiveness of the systems eventually comes from developmental and operational test evaluations focusing on meeting the requirements and performance of the system in a simulated operational environment. This information is then passed on to the authorizing officials. It is therefore very likely that the feedback gained is not nearly comprehensive enough to discover all areas of vulnerability (Snyder et al., 2015).

Furthermore, there are insufficient authorities that exist to explore the robustness and resilience of these systems (Pearson, 2021). This is because an annual report by the Director of Operational Tests and Evaluation is the only time the feedback is given to Congress on the performance of military systems, including cybersecurity. This feedback is, however, limited to defense acquisition programs and other programs that are chosen at the director's discretion. Testing usually happens early in the life cycle of a program, and no additional testing is done unless a program is undergoing modification (Snyder et al., 2015). Feedback from intelligence and counterintelligence communities who are responsible for the collection, analyzing and dissemination of information regarding possible threats and actual incidents, on the other hand, does not always find its way back to key stakeholders in acquisition and authorizing due to weak linkages. As a result of these shortcomings in feedback streams:

- There is insufficient scope in feedback and monitoring mechanisms
- No probing is done to determine the operational ramification of cybersecurity shortfalls
- Critical gaps exist in the feedback mechanisms, and thus information from independent sources cannot be compiled to produce any useful intelligence.
- Deficiencies in feedback also serve to inhibit individual accountability

2.1 Planning the Change

Cybersecurity is very complex, and as such decisions regarding cybersecurity are highly intertwined with the functionality and application of systems. The threat to cybersecurity is, however, ever-evolving and decisions regarding cybersecurity, therefore, need to be made with this in mind. Cybersecurity systems, therefore, need to be tailored to individual systems, be adaptive, have the ability to evolve with the threat as well as be highly integrated with the system designs and the mission these systems support (Eisenberg et al., 2014).

Cybersecurity extends beyond denying access; it also encompasses the intrinsic attributes of robustness and resilience that are characteristic of military systems. Robustness and resilience, however, call for diversity and consistency to maintain functionality in the occasion where subsystems collapse. Changes to key performance parameters would, therefore, be welcome if they served towards elevating cybersecurity so that systems can be able to compete with comparable concerns regarding acquisition and programming. The designs would, however, need to adaptable so that they can deal with evolving threats not just static requirements such as the denial of access (Eisenberg et al., 2014). The principles of robustness and resilience could be incorporated into the survivability of key performance measures. The goal is to, therefore, ensures that cybersecurity systems are modifiable enough to deal with evolving threats not to have concrete solutions that could deal with all foreseeable electronic warfare threats; To achieve this objective there is the need to carry out the following tasks:

2.2.1 Realign the role and responsibilities pertaining to cybersecurity risk management.

There is the need to balance systems' vulnerability, threat, and operational impact as well as empower the authorizing officials to be able to integrate and adjudicate among stakeholders in cybersecurity

The current cybersecurity management systems do not and balance the three elements of risk (vulnerabilities, threats, and impact on missions). There exist no formal mechanisms which relay data to all the relevant stakeholders, especially the authorizing officials. Furthermore, no formal mechanisms exist to take care of competing solutions between programming and operations. It is possible that solutions might exist within the organizational context, and input from both sides can help improve these systems (Karaman, Çatalkaya & Aybar, 2016). To address this, there is the need to follow a framework where the program manager would be responsible for assessing the vulnerabilities of systems; the intelligence and counterintelligence community, on the other hand, would take care of the threats and the mission head would be responsible for operational mission assurance. Through this framework, it is possible to balance the three components of risk. The authorizing official would then bring all the components together and therefore make well-informed decisions. Through this model, there is a clear separation of roles and responsibilities,

and a single individual in the form of the authorizing official is empowered to integrated and adjudicate issues across the three components.

2.2.2 The need to close the gap in the feedback mechanism through regular reports on cybersecurity programs

These gaps can be closed by increasing the number of assessments that reflect the real state of cybersecurity and ensuring that this information reaches all the relevant stakeholders, especially the authorizing officials. The flow of feedback in its current state is incomplete, and no formal mechanism exists that passes on information to the authorizing officials. These reports should not only be in quantifiable metrics but also in qualitative measures as well (Karaman, Çatalkaya & Aybar, 2016).

2.2.3 Individuals should be held accountable for violating cybersecurity policies in place

With the implementation of the above recommendation, it would be possible to have a better system of monitoring and evaluation. As such, individuals can be held accountable when they violate policies. In these instances, there should be consequences attached to prohibited actions (Snyder et al., 2015).

3.1 The Changing Role of Stakeholders in Cybersecurity

Under the proposed system, the responsibilities of stakeholders do not necessarily change. The proposed framework only shifts and specifies roles and responsibilities to ensure that there are no loopholes in the monitoring and feedback mechanisms. The role of the stakeholders will be as follows:

- The role of the CIO will remain unchanged since the CIO will remain at the helm of cybersecurity
- The acquisition and life-cycle management team will be required to carry out more assessments to determine the true state of cybersecurity in the military.
- The operational component (program operators and managers) will focus on identifying vulnerabilities within the system. This is probably a responsibility that was under their belt only that it was not specified.
- The intelligence and counterintelligence community, on the other hand, will assess threats that threaten cybersecurity
- A mission head will be added to give accurate information about missions and therefore facilitate much more accuracy in assessing risk.
- The authorizing official will serve the function of integrating these functions and adjudicating among the stakeholders.

4.1 Reflection

The military is a very mature organization, and as actual change is incredibly hard to implement. It has stood the test of time surviving the cold war era and the post-cold war era, which were perhaps the time it was really tested. As such, there is no incentive for this organization to change its core practices. Even though proposed changes hold merit, the organization may be opposed to

these changes due to the fact that it clings to its past since it's a great source of pride and esteem. The military is essentially a bureaucracy, and as such, this organization relies on consistency while addressing familiar problems. Any form of change, therefore, threatens to subvert the standardization and consistency that is the norm. Militaries are societies deeply embedded in their own values, beliefs, sociology, and history. The culture of this institution is built on shared values and history. The governing principles and procedures in the military are hence deeply intertwined with social status and individual identity. Change, therefore, threatens to disrupt the military social order by altering the dynamics that guide operations. The guiding theme in the military is "don't fix with what is not broken." Therefore, despite having pragmatic solutions to a problem that threatens the very survival of the country, the proposed changes may not occur due to the rigid and immovable foundation that the military is built on.

The opposition to change is likely to emanate from the human instinct of elf-preservation. Disturbing the eco-system of cybersecurity will definitely affect the position of various individuals within the organization to a certain degree. Stakeholders may hence fear that this will affect their relevance and respectability within this society. Disciplined organizations, therefore, rarely focus on new, untried ideas, concepts, or innovation since they are likely to disturb the peace.

Furthermore, the military is constantly reinforcing ideas that tie them to the past through various ceremonies and traditions. This has the effect of emphasizing the distinction of the military community and increasing the collective identity among the members. Even though cultivating a culture deeply embedded in the values of collectivism, obedience, self-sacrifice, devotion to tradition, and a knowledge of history is useful in preparing for combat; it makes embracing change very difficult. For instance, the military encourages the good of the group over that of the individual, and this, therefore, discourages individuals from departing from the norm

In the military, therefore, changes that are likely to subvert the core practices have little likelihood of being successful. As such it is necessary to employ the strategies that have worked in the past by working with leaders who understand the culture of the organization and can, therefore, be to generate the right kind of organizational response to change. The senior leaders have most likely struggled with changes before, and they, therefore, understand what works and what doesn't.

5.1 Plan for Implementation

The plan for the implementation revolves around convincing senior leadership to accept the proposed transformation in the cybersecurity department. Without a military culture that is receptive to change, the proposed plan will most likely be ineffective; as a result, it is necessary to seek leadership support so as to facilitate a change in culture. It will, therefore, be my prerogative to make the leadership aware of the brutal truth in the field of cybersecurity to ensure that they keen enough to treat the issues facing cybersecurity with the warranted attention (Long, 2019).

To enact this change into cybersecurity I will, first of all, ensure that the proposed changes are all in alignment with existing structures; this will make the transition smoother and cost-effective. Failure to do this may doom the plan since there will be great opposition to proposed changes. A communication plan will be the means through which I will communicate with the senior leadership. By laying out the very real concerns, I have the leadership will most likely give me a

meeting, and I will then prepare a presentation that will convince them of the efficacy of proposed changes (Roldan & Reith, 2018).

The communication plan will reiterate the dangers posed by cybersecurity threats. It will label cyber warfare as the new frontier, and as such, the military needs to perceive it as big a threat as weapons of mass destruction. The truth is that the military has remained dangerously unprepared to respond to the threat of cyber-attacks. This has left the military extremely vulnerable, and the leaders do not seem fazed by the magnitude of the challenge ahead of them. There is laxity, and complacency in the military towards the importance of cybersecurity, and this condition emanates from ignorance about this threat. The communication plan will, therefore, highlight the ways in which cyber-warfare threatens the survival of the military itself. The plan will emphasize the need for the military to move towards an information-centric mode to ensure that it is prepared to deal with the impending threat. The truth is there are very many weaknesses in the IT structure, and the military could benefit from benchmarking and adopting best practices that are followed by private sector organizations that have very strong IT governance (Eisenberg et al., 2014). The military needs to recognize that threat posed by cyber-attacks is real and while they are devoting resources to developing weapons and training soldiers there is a need for resources to be also allocated to strengthen the military's readiness for protecting the computer systems.

In recent years there has been increased integration between the physical and the cyber domain. By compromising electronic systems, it is possible to discover vulnerabilities in the real world which an enemy can attack. Cyber-attacks can also compromise other physical resources and human resources and use them against one's own military. In the world, we live an enemy does not need to leave their desks in order to carry out an attack. There exist viruses that can be used to take down an entire transportation or military system, hackers can also hijack various services denying services or even obtain critical data which they can be exploited to help an enemy's war efforts. In 2016, Russian intelligence was able to hijack various election centers, after which it changed and deleted election data (Karaman, Çatalkaya & Aybar, 2016). Mueller has also indicted various Russian nationals that broke into the Democratic National Committee servers and stole critical data and leaked it on WikiLeaks. Presently there are concerns that Russia will interfere with the 2020 elections. US cyber defense is therefore very vulnerable, and by making the military heads aware of this while presenting real facts in the communication plan, I will be able to convince them to follow through with my plan since there are feasible and applicable ideas that are likely to streamline operation as well as increase security (Roldan & Reith, 2018).

Cyber-attacks can very easily destabilize a nation; by attacking the power grid or the banking systems, a country can descend into chaos. They can also be used to support conventional war efforts; they can, for instance, be used to stop government officials from communicating, or tracking secret information, and exposing troops position, strategy and information (Hill, 2015). Without properly securing cyberspace, the country can easily lose a war despite having advanced machinery and the best-trained men in combat. In the communication plan, I will strive to use a language they understand. Even though military men may not understand complicated technological jargon, they will understand the danger that exists when they learn of what hackers can achieve through hacking into a military system.

Stratford Peer Reviewed Journals and Book Publishing
Journal of Information and Technology
Volume 5||Issue 1||Page 22 -30 ||October||2021|
Email: info@stratfordjournals.org ISSN: 2617-3573

6.1 Conclusion

In conclusion, therefore, even though militaries exist for the purpose of combat most of the time, they operate in relatively peaceful conditions. During these peaceful times, they imagine and manufacture wartime conditions to determine their preparedness and the chances of a victory with the current conditions and resources (Hill, 2015). The purpose of the communication plan will be to identify the gaps that can be exploited and hence present the plan I propose as the solution. This approach will be able to tear down the expected natural resistance since the leaders will support the proposed changes and even devote resources to see that they are successful. The purpose of the communication plan is to, therefore, make the leaders the advocates for change. This is based on the understanding that in this environment, change is not possible without support from the leadership. Without the intimate involvement of senior leadership, changes will not be treated with the urgency and the seriousness that is required. Before changing the rest of the organization, it is necessary for a dramatic shift to occur in the leadership attitudes towards cyber-security and since the military is designed in a manner in which the members will follow the direction of their leaders, resistance will be minimal.

References

Bray, T. (2020). *Military Information Technology Certification Training Addressing Implementation Procedures against Cyber-Attacks: An Exploratory Case Study*. University of Phoenix.

Caulkins, B. D. Enhancements to Cybersecurity Curricula to Support Behavioral Aspects of Cyber.

Davidson, L. (2020). Defining the Workforce and Training Array for the Cyber Risk Management and Cyber Resilience Methodology of an Army. In *ECCWS 2020 20th European Conference on Cyber Warfare and Security* (p. 466). Academic Conferences and publishing limited.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in psychology*, *9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

Eisenberg, D. A., Linkov, I., Park, J., Bates, M. E., Fox-Lent, C., & Seager, T. P. (2014). Resilience metrics: lessons from military doctrines. Solutions, 5(5), 76-87.

Grimshaw, M. D. (2017). *Operational cybersecurity risks and their effect on adoption of additive manufacturing in the naval domain*. Naval Postgraduate School Monterey United States.

Hall, A., & Sobiesk, E. (2017). Integration of the cyber domain at the United States Military Academy. In *Proceedings of International Workshops: Realigning Cybersecurity Education, Melbourne, Australia. doi* (Vol. 10, No. 3293881.3295778).

Hill, A. (2015). Military innovation and military culture. Parameters, 45(1), 85. https://doi.org/10.3389/fpsyg.2018.00744

Karaman, M., Çatalkaya, H., & Aybar, C. (2016). Institutional Cybersecurity from MilitaryPerspective. International Journal of Information Security Science, 5(1), 1-7.

Long, M. C., Bush, J., Briggs, S., Patel, T., Westervelt, E., Shepard, D., & Schwenk, D. (2019). *An Army Guide to Navigating the Cyber Security Process for Facility Related Control Systems: Cybersecurity and Risk Management Framework Explanations for the Real World*. ERDC Construction Engineering Research Laboratory Champaign United States. https://doi.org/10.21079/11681/35294

Pajurek, M. (2017). Cybersecurity military entities of the United States of America. *Facta Simonidis*, *10*(1), 163-178.

Pearson, J. R. (2021). *Addressing Cybersecurity and Safety Disconnects in Army Aviation: An Exploratory Qualitative Case Study*. Capella University.

Poe, L. R. (2018). The Development of Information Assurance and Cybersecurity Competency Lists.

Roldan, H., & Reith, M. (2018). A Strategic Framework for Cyber Attacks in the Military. In *International Conference on Cyber Warfare and Security* (pp. 622-XV). Academic Conferences International Limited.

Santiago, G. (2019). *Cybersecurity Risk Management Process For Unmanned Aerial Systems (Uas) At The Strategic Level*. Naval Postgraduate School Monterey United States.

Snyder, D., Powers, J. D., Bodine-Baron, E., Fox, B., Kendrick, L., & Powell, M. H. (2015). Improving the cybersecurity of us air force military systems throughout their life cycles. Rand Project Air Force Santa Monica Ca.

Tikk, E., & Kerttunen, M. (Eds.). (2020). *Routledge Handbook of International Cybersecurity*. Routledge. https://doi.org/10.4324/9781351038904