International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

# Organizational Communication System Cybersecurity

Clive Sugama
College of Engineering
Colorado State University
Fort Collins, CO 80523

***Abstract*— Communication systems within military and Government organizations are potential targets from adversaries with malicious intent. Radio Frequency (RF) and network infrastructure would need recurring cybersecurity activities performed on them to prevent cyber threats. Incorporating cybersecurity measures within a communication system and governing personnel to maintain complaint devices is necessary for a secure environment. Planning early and selecting approved RF and network equipment reduces the risk of potential damage occurring from a cyber-attack. Measuring cybersecurity effectiveness of an organization is essential to assess practices being performed.**

***Keywords*— *Cyber security; Communication system; RF; Governance***

## I. INTRODUCTION

Cybersecurity is a necessary practice for military and government organizations using communication systems to transmit and receive information. Neglecting these practices would put the organization at risk for allowing sensitive information being distributed to unauthorized personnel, disrupting critical communication links, and causing damage to its communication infrastructure. Consistently performing cybersecurity measures to counteract potential threats is essential for securing sensitive information.

## II. SECURITY STRATEGY

Intrusion detection / protection of devices and data are necessary for the cybersecurity strategy. Implementing boundary protection and network segregation would also prevent incidents from affecting the whole communication system. Remote access control implementing secure connections to compliant assets is another initiative that was met. Redundancy methods for critical components would be put in place in case of an unexpected system shutdown. Confirming that authentication controls are up to date with respect to user access and password complexity would be part of cybersecurity governance as well.

Ensuring methods are in place within each domain would allow auditors to oversee personnel by ensuring they are meeting cybersecurity expectations. Monitoring these security controls along with acknowledging the classification of data and equipment would allow specific cybersecurity requirements to be adhered to. User awareness and cybersecurity training for personnel would promote knowledge transfer of information assurance responsibilities and cybersecurity governance requirements.

Items for a security policy would include ongoing cybersecurity risk management, auditing, and keeping updated current plans with the latest security countermeasures. Cybersecurity risk management would involve identifying, analyzing, prioritizing, resolving, and monitoring risks. This recurring activity would align with the latest security countermeasures. Regularly checking the DISA's IASE website http://iase.disa.mil/ for the latest security updates would assist with implementing the organizational policy and objectives. Auditing security measures would ensure that network and computer equipment are in compliance with security regulations. Scanning systems on a monthly basis and alerting administrators or system owners of identified vulnerabilities will prompt for actions concerning potential threats.

A governance strategy would include the following procedures mandated by Department of Defense (DoD) directives. These directives include DoDI 8500.01 cybersecurity, DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT), CNSSI 1253 Security Categorization and Control Selection for National Security Systems, NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security, and NIST SP 800-41, Guidelines on Firewalls and Firewall Policy. A budget for cybersecurity implementation and practice would be added to overall program support costs to ensure adequate cybersecurity practices are performed. Resources and funds are critical to the successful governance and implementation of cybersecurity efforts.

The overall security strategy would be based off of the communication system shown in Figure 1. Each domain would have its own security strategies associated with it . The RF domain would have a strategy relating to the transmission devices within that domain while the non-secure domain and secure domain would have more network related security criteria. A Defense in Depth (DiD) strategy would be used in order to safeguard critical assets. Physical barriers such as secured spaces would assist with the perimeter security along with first line intrusion detection and data loss prevention devices. Network security and endpoint security would include segmenting non-secure and secure domains by firewalls, (High Assurance Internet Protocol Encryptors) HAIPE, router access lists, and intrusion detection methods. Application security would involve antivirus software and a Host Intrusion Protection System on every client workstation

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

/ server. Updates would be pushed to clients within each enclave to ensure compliancy. Data security would include classifying data appropriately, encrypting hard drives / data, and controlling access to that particular data. This DiD strategy would safeguard critical assets such as sensitive information, configurations, or other data that could be detrimental if accessed for malicious intent.

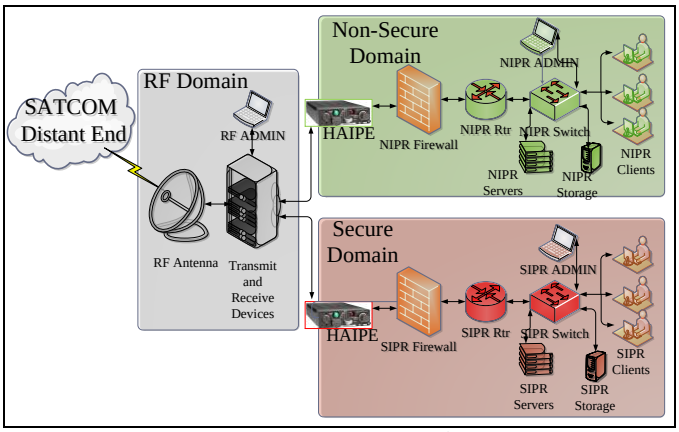


Figure 1. Communication System Infrastructure

Segmented enclaves include the RF, Non-Secure, and Secure domains. The RF domain would require Electronic Key Management System (EKMS) monthly updates to ensure only authorized receivers with EKMS devices on their end are given access to the RF signal being transmitted. The Non-Secure enclave would have a HAIPE to encrypt / decrypt the unclassified IP data being transmitted and received. Similarly the Secure enclave would have a HAIPE to encrypt / decrypt the classified IP data being transmitted and received. A firewall would be located on the Non-Secure and Secure domain to allow limited access control by permitting only authorized IP addresses and denying the rest. Router Access Control Lists (ACL) in the Non-Secure and Secure enclaves would direct and control access in and out of each enclave. Configuration access to devices would be controlled in each enclave by strict password complexity, limited user accounts, and logging capabilities.

The secure design would not only be anchored in policy and planning, endorsed by senior management, but also would be consistent with overall organizational policies, goals and objectives. Some secure design techniques would include Evaluated Product Lists (EPL) and Operating System (OS) security. The devices in the RF, Secure, and Non-Secure domains would have to be verified that they have been Joint Interoperability Certification and Assessment (JITC) approved and have an Authority to Operate (ATO). These devices would be put on the organization's EPL to ensure that the procured system components have been verified so that the protective properties are consistent with the security policy. OS security would apply to client workstations and servers located in the Non-Secure and Secure domains. Multiple levels of OS security would be implemented to ensure there is isolation among the different threads. Supervisory mode and user mode would be implemented within these client workstations and servers to allow privileges to appropriate personnel.

System administrators within particular domains (Secure, Non-Secure, and RF) would be accountable for adhering to the policies within these instructions. Prevention and contingency plans would be developed by these administrators along with information assurance personnel to impede cybersecurity incidents and to reduce impact if an incident does occur. Cybersecurity requirements should be traced to verification and test methods to ensure they are met. Continuous monitoring of RF and IT equipment compliance would be required with the most up-to-date configurations. Ensuring that the devices have an authority to operate (especially new / updated devices) would be essential within the communication system environment. Device vulnerability scanning for compliance would indicate if the communication system devices are up to date. If there are devices that have minor updates needed to meet compliancy, obtaining a Plan of Actions and Milestones (POAM) from the device / system owners would be necessary for remediation. Penetration testing would also reveal potential vulnerabilities to whether in a physical environment or a virtual one. Logs of unauthorized configuration changes, non-compliance findings, and incidents would be maintained for mitigation and trend analysis. Isolation and disconnection of non-compliant workstations / devices would occur for delinquent and severely vulnerable equipment. Physical security checks along with inventory of COMSEC equipment would be required for accountability purposes.

## III. VULNERABILITIES AND THREATS

Potential vulnerabilities include RF signal jamming to shutdown communication capabilities, outdated virus / malware prevention software on client workstations, outdated firmware on devices such as firewalls, switches, routers, HAIPE, workstations, and RF equipment, password complexity, minimal access control, lack of device configuration backups, inadequate redundancy options / plans, and limited encryption on network connected devices. Ensuring Information Assurance (IA) compliance on all network connected devices is essential for cybersecurity efforts. Malicious behaviors include RF jamming within the transmission domain of a communication system, denial of service attacks on the secure / non-secure domains, and insider threats. Shutting down communications services by interfering with RF communications would prevent secure and non-secure data traffic from reaching / being received from the distant end. Anti-jamming measures would have to take place to ensure RF communication services stay operational. Denial of service attacks would occur if an attacker was able to get through to the secure / non-secure domains and unleash a plethora of Internet Protocol (IP) traffic that can overload a server. This abuse case would require swift identification of the source of the attack and blocking from either the firewall or router by an Access Control List (ACL). The insider threat scenario would involve someone within the organization conducting malicious activity to communication system equipment. Personnel working with sensitive communication systems should go through a recurring background check where clearance to work with the equipment would be granted. Insider threats that would either be malicious or inadvertent

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

can affect the communication system in negative ways. A process to identify and counter these threats would reflect the NIST 800-40 instruction [1].

When integrating a communication system, certain factors would be considered. If an anti-jamming RF solution is not identified during the selection of a RF device, then there would be a potential to endure complete loss of transmitting / receiving capabilities. Mitigation for this risk would include selecting a RF system capable of utilizing Protected Tactical Waveform (PTW) technology. PTW is designed to provide protected communication services against various interference and jamming threats [2]. Alternate mitigation would be to choose a RF device that is capable of either spread spectrum technology such as frequency hop spread spectrum to prevent jamming of the signal or direct sequence spread spectrum [3]. If a RF device does not have the characteristics of having a Low Probability of Intercept / Low Probability of Detection (LPI / LPD), then interruption of service would likely occur**.** Mitigation would include performing verification tests using RF detection tools and techniques such as wideband radiometer, explicit signature, narrowband scanner, narrowband radiometer, carrier regeneration, code clock extraction, and spurious PN Auto-correlation [4]. If security auditing of the communication system does not take place on a regular basis, then there would be vulnerabilities present**.** Mitigating these vulnerabilities would involve referring to the DoD 8500.2 instruction where system administrators would collect and retain audit data to support technical analysis relating to misuse, penetration reconstruction, or other investigations, and provide this data to the appropriate agencies [5].

Sophisticated access controls and privilege management would occur within various domains of a communication system. This would include the RF domain where admin privileges are granted to operators, specified subject matter experts, and Communication Security (COMSEC) security handlers for Electronic Key Management System (EKMS) equipment. The internal network domain would include access control via firewall and access control lists within routers. Network administrators would have privileges to configure, troubleshoot, and upgrade network equipment.

Secure data communications involving the RF domain and the internal network would be essential for Cybersecurity efforts. EKMS equipment would have to be rekeyed monthly to maintain security posture. HAIPE devices would be placed within the internal network domain to secure information transfer. Data storage would have to include encryption on device drives within storage area networks.

Some applications that provide secure methods include encryption of data storage, network data, and RF communications. Encryption of data storage would include encrypting stored data in Storage Area Network servers as well as individual client computers. Installing encryption applications on client workstations where the hard drive is encrypted and used only by authorized personnel. If a hard drive is lost or stolen, the encrypted hard drive would prevent an unauthorized individual from accessing it. Encrypting network data would include a HAIPE where network data is encrypted and only accessed by a distant end user with a HAIPE utilizing the same set of keys. These HAIPE keys are updated monthly on both ends to provide secure network data transmission.

Adaptive Security Appliance (ASA) firewalls have a capability to deliver IP security (IPSec) tunnels for secure data transfer. These IPSec tunnels would connect one ASA firewall to another ASA firewall or compatible device at the distant end capable of IPSec tunneling. IP data would be transmitted and received through these IPSec tunnels where the data would be encapsulated securely while traveling through various LANs or WANs. A malicious party using sniffing software would only see garbled (encrypted) data being passed through the network.

Encrypting RF communications would include the transmitter having a card or module to encrypt the signal while the receiver would have a decryption component to decipher the signal coming in. This method would assist with preventing an unauthorized party from picking up the signal and observing the data being transmitted or received. An application for RF signal encryption would involve sensitive video broadcasts to multiple parties that have the need to know to view the video being transmitted or other sensitive information being shared. Encryption keys would be updated monthly on both the transmitting and receiving side of the RF domain to prevent malicious individuals from attempting to decipher the keys.

## IV. CYBERSECURITY EFFECTIVENESS METRICS

Metrics and trend analysis of cybersecurity related incidents and efforts would depict needs for a mitigation strategy and potential future outcomes. Incident reports over time are a metric that can be used to assess cybersecurity effectiveness. A scenario would include the number of incidents where the firewall has been breached. As shown in Figure 2, there were a high number of breaches during a particular time period. After applying a critical patch obtained from the manufacturer's website the amount of incidents decreased. Another small spike shown in August was mitigated by applying another patch that was released.

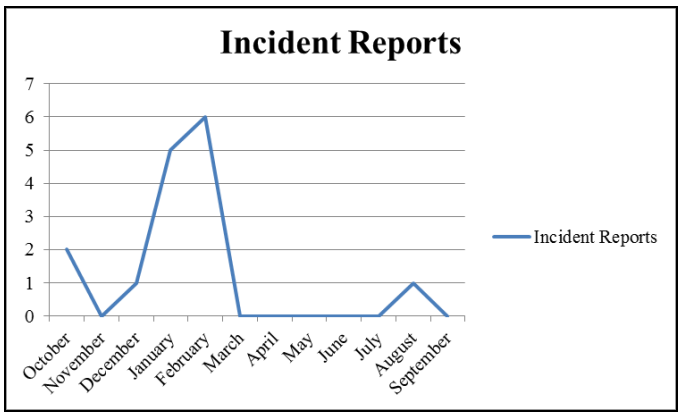


Figure 2. Incident Reports within a Fiscal Year

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 07, July - 2017

Measuring the amount of non-compliant workstations over time is another metric where the cybersecurity effectiveness would be shown. A high number of non-compliant workstations initially would suggest or reveal that system administrators are not performing well or that local users are not accepting updates pushed to their workstations. A significant decrease would indicate where leadership intervention took place and the issue was corrected as shown in Figure 3.

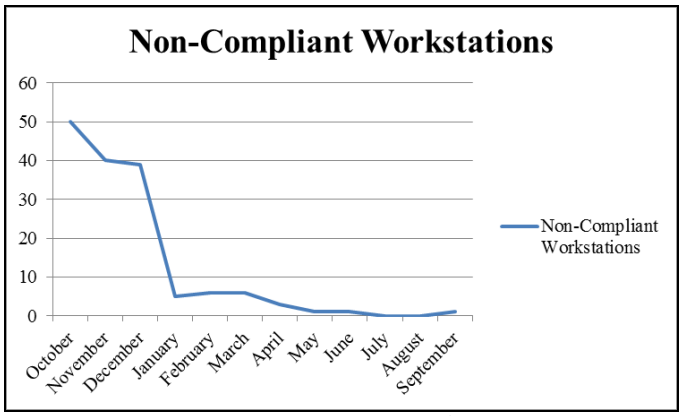


Figure 3. Non-Compliant Workstations Identified in a Fiscal Year

Another metric that can depict the cybersecurity effectiveness is assessing systems with expiring Authority to Operate (ATO) certifications. This metric shown in Figure 4, would specify how many internal systems would have their ATO expiring. Systems within the organization would include systems within the RF domain, non-secure domain, and secure domain. This depiction would show the amount of workload coming up or how proactive system administrators / authorizing personnel are at a given point in time.

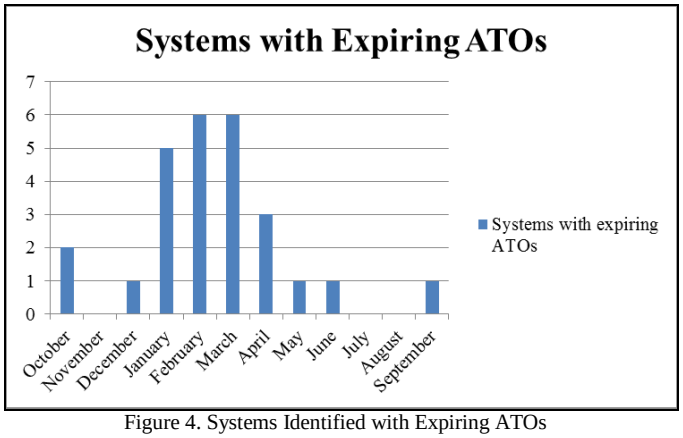


Figure 4. Systems Identified with Expiring ATOs

Logging incidents and discrepancies assist with assessing the overall cybersecurity posture of an organization. Governance of cybersecurity efforts would be displayed within reporting graphs to indicate if intervention is required. Continuous monitoring and logging of issues and discrepancies identified over time would show trends for analytical analysis.

## V. CONCLUSION

Government and military communication systems require personnel to perform recurring cybersecurity practices. Personnel would need to stay current with the latest security threats and prevention methods by referring to DoD instructions and organizational policies. Performing audits with logged incidents would assist with trend analytics. Assessing cybersecurity effectiveness metrics would depict how well the organization is performing cybersecurity practices. Governance and enforcement of cybersecurity efforts would be mandated to reduce communication system risk.

## REFERENCES

[1] P. Mell, T. Bergeron, D. Henning. "*Creating a patch and vulnerability management program*: *recommendations of the National Institute of Standards and Technology (NIST)"*. Washington, D.C.: NIST, 2005.

[2] J. Sullivan, M. Glaser, C. Walsh, W. Dallas, J. Blackman, J. VanderVennet, C. Shunshine, J.C. Chuang, 2013. *"Protected MILSATCOM Design for Affordability Risk Reduction (DFARR),"* MILCOM 2013 - 2013 IEEE Military Communications Conference, San Diego, CA, 2013, pp. 998-1001.

[3] K. Fuchs. 2012. "*Anti Jam Approaches For SATCOM"* http://www.milsatmagazine.com/story.php?number=1273648561 (accessed April 4, 2017)

[4] R. Schoolcraft. 1991. *"Low probability of detection communications-LPD waveform design and detection techniques,"* MILCOM 91 - Conference record, McLean, VA, pp. 832-840 vol.2.

[5] P. Campbell, "Department of Defense Instruction 8500.2 "Information Assurance (IA) Implementation:" A retrospective," *2012 IEEE International Carnahan Conference on Security Technology (ICCST)*, Boston, MA, 2012, pp. 187-194.