Valley Forge Military College (VFMC)

Information Systems Security (ISS)

Cyber Security Plan

Date: 04.26.2024

Prepared by: Vladyslav Biblyi, Zuri Goldsberry, Maksim Osadchyi, and Samir Hugh

VFMC ISS Cyber Security Plan

Project Plan Overview

- Risk Management
- People & Policy Risks
    - ❖ Organizational Policy
    - ❖ Legal and regulatory compliance
    - ❖ Personnel and Training
- Process Risks
    - ❖ Operational Risks
    - ❖ Physical security
- Technology Risks
    - ❖ Network Risks
    - ❖ Platform Risks
    - ❖ Application/Software Risks

An Analysis of Risk Management by Maksim Osadchyi

Introduction:

Institutes like Valley Forge Campus, a well-known educational center, have their fair share of cybersecurity threats regularly. The campus must be meticulous in dealing with the risks that affect the intellectual property of its students and scholars, including the security of their personal data, the protection of their research work, as well as integrity, confidentiality, and availability of its digital assets. This document describes the complete cybersecurity risk management procedure implemented by Valley Forge Campus as a measure of ensuring the development and implementation of successful cybersecurity practices.

Risk Assessment Process:

Asset Identification: The risk assessment process at Galen Healthcare first calls for the identification and classification of all digital assets that make up the Valley Forge Campus's infrastructure. This accrues everything from hardware to software, data repositories, network devices, and any other type of technical components that can be probed and used as a vector of cyber threat delivery.

Threat Identification: Another thing to do is to identify the assets, after this comes the determination of possible threats. The latter task is realizing possible menaces coming from alien actors, including hackers, malware, and insider threats such as dissatisfied employees or students. Aggregated threat intelligence inputs and industry threat reports may help understand the new threats that can emerge in the educational sector.

Vulnerability Assessment: The campus does the assessment of both the assets and, the threats it faces. With the results, it balances the digital infrastructure and takes the remaining relevant vulnerabilities in the security system. To this end, the tool may implement automatic scanning for any known vulnerabilities, errors in the configuration, or disqualified login mechanisms, amongst other applications.

Risk Analysis: Risk analysis means examining the opportunity and severity of occurrence and consequences of identified threats that are configured for exploiting the digital environment on the campus. This assessment enables prioritizing the risks for their consequences and conditions of occurrence.

Risk Prioritization: According to the risk analysis, risks are listed down depending on their severity, thus, conversion to negative effects on the operations of Valley Forge Campus. This, similarly, helps to prioritize risks in a timely manner hence allocation of resources in the most important position is achieved.

Risk Mitigation Strategies:

Access Control: The response system is Valley Forge Campus campus putting in place highly “rigorous” access controls to limit access to sensitive data and networks exclusively to duly authorized individuals. Such a practice comprises the principle of least privilege, and role-based access control, so as to utilize strong authentication methods such as multi-factor authentication.

Security Patch Management: Instead, always keeping software up-to-date and installing the newest security patches effectively prevails in detecting common vulnerabilities. Our campus utilizes a tough patch management procedure responsible for ensuring that any critical vulnerability patches are installed to any system and software program on time.

Intrusion Detection and Prevention Systems (IDPS): IDPS roam the network at a campus level to seek outing, attack and cyber threat occurrences at all possible times. These provided extra systems on the way of cyber attacks deterring.

Encryption: We use encryption technology while our confidential data is not active, and to ensure the security of the report, we also enable encryption methods that allow us to maintain the privacy of the information when it is in transit. This is achieved by staying secure even if data is hacked or accessed without authorization encryption; it remains incomprehensible without appropriate decryption keys.

User Awareness Training: Training of faculty, staff, and students in order to be knowledgeable of cybersecurity practices would be essential to reduce dangers from human errors of humans and cyberattacks through social engineering. As Valley Forge

Campus makes sure to hold “user awareness sessions on a regular basis to let users know about phishing scams, password hygiene, and other cyber threats.

Monitoring and Review:

Continuous Monitoring: Security management at Valley Forge Campus uses the most advanced security monitoring instruments and technologies to constantly keep watch for any unusual trends or security break-ins within the digital environment. This includes the analysis of network traffic, system logs, and user activity to detect abnormal or suspicious activities.

Incident Response Testing: A regular practice of drills and simulations is created to investigate the responsiveness of the campus' incident response plan. Among these exercises might be simulating cyber-attack situations that can then be scrutinized in order to assess the preparedness of the campus staff and their opportunities for improvement.

Audits and Reviews: Periodical audits and reviews are done to measure the competence of existing risk management controls as well as to determine any weaknesses or shortage of campus cybersecurity posture. These audits are either an internal process or it could be conducted by third-party cyber security professionals who will provide a more objective assessment of the whole campus’ security posture.

Feedback and Continuous Improvement: Monitoring reports and lessons from incident response exercises and audits are used to constantly develop Valley Forge Campus's cybersecurity posture. The learned lessons from the past incidents as well as the security breaches, are embedded into the cyber risk mitigation strategy that is to be developed in the future in order to ensure that the campus remains prepared for the changing cyber-attacks.

While Valley Forge Campus devises a decluttered risk management program, defends this program with several obstacles that complicate effective risk management. Some of these challenges include:

Resource Constraints: Limited budgetary resources and work force can lead to inadequate strategic action plans on implementation of modern cybersecurity features. The Valley

Forge Campus is the constant victim of obsolete cybersecurity technologies, deficits in hiring qualified cybersecurity professionals, or training of usual employees and students.

Complexity of the IT Environment: The system of campus integrity is simply mind-boggling and is an assemblage of the vastly various interconnected systems, devices, and applications. In the intricate modern cyber-infrastructure managing cyber risks is also complex because any insecure link could be a spark that would spread to the whole system.

Adoption of Emerging Technologies: Technology progress that results in the creation of cloud computing, Internet of Things (IoT) devices, and Bring Your Own Device (BYOD) policies create new opportunities for cybercriminals. The mountains along the Valley Forge campus have to monitor all the technological advancements and employ risk management solutions that will counteract these developing threats.

Human Factor: Though we are successfully using countermeasures to protect our infrastructure, social factors still play a great role which human subject quality can be considered as a weakness. To illustrate, instructors, administrators, and guardians can unintentionally breach security by actions such as tapping into malicious links, using very weak passwords, or mistreating delicate data, The realization of this comes through teaching the users about cybersecurity best practices and crafting a culture that appreciates security should be the main aim of minimizing this threat.

Third-Party Risks: The Valley Forge campus has varied IT services and solutions that are delivered by third-party vendors and service providers to cater to the rigorous demands of the students and faculty. Though these risks can be introduced, they still apply unnecessary attack vectors, such as data breaches and supply chain hacks. Insisting that third-party vendors abide by a high-level security rule while also carrying out regular security checks of their systems and processes is one of the important ways to deal with this risk.

Regulatory Compliance: In compliance with many regulations concerning data privacy and security (FERPA and HIPAA are examples), the campus must implement them. Ensuring that these regulations are met will add another problem in the risk management process and will require a substantial budget and experts.

Cybersecurity Talent Shortage: Another issue is the lack of cybersecurity professionals with appropriate qualifications. Organizations from the education sector are among those affected too. The workforce shortage of cybersecurity professionals at the Valley Forge Campus, which makes it hard to combat information security risks and to counteract cybercrime in time, is a serious problem.

Conclusion

Comprehensive consideration of cybersecurity risks on the Valley Forge Campus promotes a forward-looking strategy to protect its digital properties and the brand or image of its stakeholders. Through the process of risk assessment, and successful implementation of mitigation strategies, while the cybersecurity posture will be continuously monitored and reviewed, the campus will strive to diminish the hardships in the ever-changing cyber landscape.

At the same time, however tough for Valley Forge Campus, it comes across a few problems on its way as well. Financial and IT resources, the magnitude of its infrastructure, human factors, external factors, regulatory requirements, and the cybersecurity professionals shortage are the critical factors to effective risk management. Addressing these challenges requires a multifaceted approach, such as increased funding, cybersecurity skill training, and collaboration efforts from other parties as well as timely intelligence and awareness about trending threats and best practices.

While cyber threats may present significant difficulties, Valley Forge Campus remians dedicated to the accomplishment of all cybersecurity goals. Therefore, focusing on its strengths, creating a security culture, and also adapting proactively to cyber attacks, the campus aims at enhanced safety and to maintain its reputation of a secure digital environment for its faculty, employees, and students. By always seeking opportunities for advancements and active risk management methods, Valley Forge Campus aspires to cope with cybersecurity complications with conscientiousness and resoluteness, thereby providing the needed safety for its electronic assets.

An Analysis of People & Policy Risks by Zuri Goldsberry

Faculty

A review of cybersecurity practices at Valley Forge Military Academy and College (VFMAC) reveals both positive aspects and areas for improvement. The college offers online cybersecurity training for staff and faculty, and the interviewed faculty member found these courses informative. This training is a crucial first step in raising awareness of online threats and fostering responsible online behavior. However, data security practices for online platforms could be further bolstered. The faculty member prioritizes physical security measures like locking devices and restricting access, which are important practices. However, to create a more robust defense against cyber threats, the college should consider additional measures. These could include encouraging all faculty to complete the available cybersecurity training to enhance their understanding of online threats like phishing and malware. Additionally, implementing data encryption for sensitive student information stored on online platforms would add another layer of protection. Furthermore, exploring multi-factor authentication for accessing online platforms would provide an extra hurdle for unauthorized users attempting to gain access. Finally, by clearly communicating the college's process for reporting suspicious emails and encouraging faculty to report any such emails they receive, the college can proactively identify and address potential phishing attempts. By implementing these recommendations, VFMAC can significantly elevate its cybersecurity posture and create

a more secure environment for faculty, staff, and student data entrusted to online platforms.

Students

While VFMAC offers a valuable education, its cybersecurity protocols appear concerning. The interviewed student wasn't mandated to take online security training, lacked knowledge of dedicated resources, and possessed minimal familiarity with the college's policies. This suggests a gap in student awareness, potentially leaving them vulnerable to online threats. To rectify this, the college should implement mandatory cybersecurity training for all students, readily offer resources on best practices, and clearly outline official policies. Additionally, consistent communication and a designated point of contact for reporting incidents would further strengthen the college's cybersecurity posture. By addressing these concerns, VFMAC can create a more secure digital environment for its students and the college as a whole.

IT

While VFMAC utilizes user authentication methods like single sign-on and dual authentication, and enforces NIST security controls, their password policy seems lax with optional changes. Additionally, the lack of consistent network filtering across the college (with FacultyNet unrestricted) creates a vulnerability point. Positive aspects include automatic server updates with vulnerability patching, and a cloud-based data backup strategy with incremental backups. Although a four-step incident response plan exists for initial attack response, it's still under development. Faculty undergoes mandatory

cybersecurity training, but the effectiveness of the training remains unclear. To strengthen their cybersecurity posture, the college should enforce mandatory password changes and implement a strong password policy, establish consistent network filtering across the entire network, and evaluate the need for unrestricted access on FacultyNet. Finalizing the incident response plan with clear roles, communication protocols, and data recovery procedures, and reassessing the effectiveness of faculty training are also crucial steps. By addressing these concerns, VFMAC can create a more secure digital environment for its faculty, students, and the college as a whole.

An Analysis of Process Risks by Vladyslav Biblyi

Introduction

Following a detailed discussion with Mr. Baradgie, the Director of Security at Valley Forge Military Academy and College (VFMAC), this report identifies critical security challenges and proposes strategic enhancements to mitigate physical and operational risks on campus. Mr. Baradgie's insights reveal a security framework that, while committed, faces substantial hurdles due to outdated infrastructure, inadequate personnel levels, and financial constraints. This report aims to offer a blueprint for robust security improvements.

Detailed Analysis of Security Challenges

Physical Security Risks:

1. Outdated and Insufficient Surveillance Systems:

- Currently, the campus uses surveillance technology that is severely outdated, which limits the security team's ability to monitor extensive areas effectively. This inadequacy is a critical shortfall in ensuring the safety of students and faculty, especially during off-hours and on weekends.

- Recommendation: Implement state-of-the-art surveillance systems equipped with motion sensors and night vision to enhance monitoring capabilities across the campus.

2. Inadequate Access Control Measures:

- Many buildings lack modern electronic access controls, relying instead on traditional locks that do not provide adequate security against unauthorized entry. This deficiency is particularly concerning, given the open campus layout.

- Recommendation: Install comprehensive electronic keycard systems that can be programmed for specific hours and access levels, thus restricting entry to authorized personnel only and reducing the likelihood of intrusion.

3. Understaffing of Security Personnel:

- The security department operates with only eight officers covering three shifts daily, which is insufficient for comprehensive coverage of the entire campus, particularly given its size and the complexity of potential security threats.

- Recommendation: Increase staffing levels to ensure continuous patrol coverage and establish a dedicated response team for emergency situations.

Operational Security Risks:

1. Environmental and External Threats:

- Proximity to potential hazards such as the Limerick Nuclear Power Plant and major highways increases the risk of environmental disasters impacting the campus. Additionally, societal issues like local crime and domestic terrorism pose significant threats.

- Recommendation: Develop specific contingency plans for different types of environmental disasters and enhance coordination with local emergency services to improve preparedness and response strategies.

2. Limited Crisis and Emergency Response Training:

- Current training regimes for handling emergencies are inadequate, with staff not regularly drilled in updated crisis response protocols, which could hinder effective management of unexpected incidents.

- Recommendation: Implement regular, mandatory training sessions for all security personnel and relevant staff, focusing on scenario-based drills that include active shooter situations, lockdown procedures, and natural disaster responses.

3. Financial Limitations Impacting Security Enhancements:

- Budget constraints significantly restrict the ability to update critical infrastructure, expand staff, and maintain high readiness levels. This financial strain impacts the overall security posture of the campus.

- Recommendation: Pursue alternative funding opportunities such as grants, partnerships, and donor contributions specifically earmarked for security enhancements.

Campus Buildings and Infrastructure Review

1. Mellon Hall

In assessing Mellon Hall, I found significant security gaps, particularly with the lack of camera surveillance. Additionally, the door locking procedures are inconsistent, with doors secured between 7 PM and 11 PM, regardless of whether the building is occupied. This inconsistency was highlighted on March 15th when, during a 10 PM check, I discovered that all doors except one were locked. The unlocked door was either broken or not properly secured. I reported this issue to the facilities and security departments the next day, and it was fixed immediately. However, this incident shows the potential risk of unauthorized access and the importance of

regular maintenance, reliable locking mechanisms, and better camera coverage to enhance security.

2. Library

The security in the library is insufficient, especially with camera coverage. Currently, there are only three cameras, all pointing towards the same emergency door, leaving other areas unmonitored. Additionally, I found that the basement door was unlocked during a recent check. This lack of proper security coverage and access control exposes the library to potential unauthorized entry and safety risks. It's crucial to reassess and enhance the surveillance and locking mechanisms to cover all critical access points effectively.

3. Knox House, Green House,

Knox House and Green House, where sophomores reside, currently have significant security vulnerabilities. Both buildings can be accessed freely from the front doors and from the back doors that lead directly to the basements. This open access poses a considerable security risk as it allows anyone to enter without restriction, potentially compromising the safety of the residents. It is crucial to implement measures such as locked entry points and monitored access to ensure the buildings are secured effectively.

Proposed Enhancements and Strategic Outlook

To address the identified risks, a comprehensive enhancement strategy must include:

1. Technology Upgrades:

- Transition to a digital monitoring system with integrated software that allows for real-time surveillance and automated alerts for unusual activities.

- Upgrade physical security equipment, including locks, emergency communication systems, and lighting around campus to enhance safety during nighttime.

2. Staffing and Operational Adjustments:

- Recruit additional security officers and provide specialized training in risk assessment, technological security measures, and crisis management.
- Establish a central security command center to coordinate surveillance, patrol operations, and emergency responses effectively.

3. Community Engagement and Training:

- Develop a campus-wide security awareness program to educate students, faculty, and staff on security best practices, personal safety tips, and emergency response procedures.
- Foster a collaborative environment with local law enforcement and community leaders to enhance security measures and community response capabilities.

4. Regular Assessment and Policy Updates:

- Conduct annual security assessments to identify new risks and evaluate the effectiveness of current security measures.
- Update security policies and procedures regularly to reflect the dynamic nature of the threats and the latest best practices in campus security.

Operational Security (OPSEC)

While physical OPSEC measures are evident, the approach to protecting sensitive information, especially in digital form, appears less structured. There's an opportunity to implement a formal data classification policy and improve access control, both physically and digitally.
Regular risk assessments and the development of a robust OPSEC framework could address current vulnerabilities and better prepare the campus for emerging threats.

Conclusion

The security challenges at VFMAC require immediate and sustained attention to safeguard against both physical and operational risks. By implementing the recommended strategies, VFMAC can significantly enhance its security infrastructure, improve personnel readiness, and foster a safer campus environment. The commitment to ongoing assessment and adaptation of security measures will ensure that VFMAC remains a secure and resilient academic community.

An Analysis of Technology Risks by Samir Hugh

Introduction:

Technology risk refers to the hazards and vulnerabilities associated with using systems and advancements within a company. These risks cover a range of issues, including cybersecurity threats, system malfunctions, and data breaches that can disrupt operations and compromise data security. Effectively managing technology risk involves strategies focusing on monitoring, implementing security measures, and adapting to emerging threats. In this overview of technology risk, I will share insights from Mr. Hashir and Michael Brock, who serve as the IT Director at Valley Forge Military Academy, based on an interview. The overview also classifies the identified technology risks into network-related concerns, platform issues, and application/software vulnerabilities.

Network Risks:

Network threats pose risks, such, as malware attacks, data breaches, phishing scams and denial of service (DoS) incidents. These dangers can jeopardize the security and accessibility of data and systems potentially harming a companys reputation and leading to outcomes. It is essential to implement network security measures like firewalls, encryption protocols, intrusion detection systems and regular security checks to reduce these risks. As per insights shared by an individual known as Mr. Michael Brock without revealing identities firewall appliances are deployed to block ports on devices across the campus in conjunction with antivirus software for protection. Likewise Mr. Hashir emphasized that simple protective actions, like encouraging users to update their passwords can also be measures.

Platform Risk:

The uncertainties and challenges linked to utilizing platforms like marketplaces or social media platforms are commonly referred to as platform risks. These risks encompass issues such, as data privacy breaches, algorithm biases leading to discrimination or misinformation dissemination, compliance hurdles with regulations and platform instability due to factors. Managing platform risks involves assessing the risks taking steps to mitigate them and continuously monitoring to safeguard users and stakeholders. As per Mr. Brocks viewpoint on prevention predicting attacks proves challenging due to the development of techniques. Nonetheless readiness and having a thought out action plan, in place can aid in defending against attacks.

Application/ Software Risk:

Software risk, in applications pertains to the vulnerabilities and potential dangers associated with developing and using software programs. This risk includes aspects such as security vulnerabilities, software glitches or malfunctions that could lead to failures or data loss. Managing application/software risk typically entails testing and implementing security measures like encryption and access controls. Technology will necessitate updates, patches and ongoing monitoring to mitigate risks over time. During Mr. Brock's twenty-three years at VFMAC, he encountered one incident in 2010 when a teacher received a malicious link via email that contained a virus upon clicking. He emphasized that humans pose a risk on the internet, prompting efforts to educate faculty members better. The virus turned out to be a worm that targeted VFMACs network resulting in ransomware. The only recourse was either resorting to a recovery method. Paying the attacker. After assessing the damage, they isolated it from the network to halt the attack before gaining access and restoring everything to normal.

Conclusion:

In summary the overview emphasizes the nature of technology risks, including threats, to networks, uncertainties in platforms and vulnerabilities in applications and software. Insights from Mr. Hashir and Michael Brock stress the importance of taking steps like implementing security measures, regular monitoring and educating users to effectively reduce these risks. Mr. Brocks experience at Valley Forge Military Academy illustrates that technology risks are constant and evolving requiring an approach to risk management to prevent disruptions and data breaches. By staying alert adapting to threats and promoting a culture of cybersecurity awareness organizations can enhance protection, for their resources. Maintain operational resilience in an increasingly digitalized environment.