Title: Bayport Credit Union, Cybersecurity Internship

Author: Ryan Woodard

Date: 12/1/2024

Table of Contents

1. **Introduction**
2. **Overview of Bayport Credit Union's IT Operations**
    - 2.1 The Role of Remote Servers
    - 2.2 Importance of PC Lifecycle Management
    - 2.3 Monitoring Through Remote Management Tools
3. **Identifying and Addressing Vulnerabilities**
    - 3.1 Analyzing Remote Server Risks
    - 3.2 Proposing Practical Solutions
    - 3.3 Insights from Research and Practice
4. **Implementing PC Refresh Cycles**
    - 4.1 The Imaging Process
    - 4.2 Enhancing Security Post-Installation
    - 4.3 Results and Employee Feedback
5. **Upgrading Remote Monitoring Systems**
    - 5.1 Limitations of Current RMM Tools
    - 5.2 Exploring IGel as a New Standard
    - 5.3 Testing and Future Applications
6. **Lessons Learned During the Internship**
    - 6.1 Professional Development and Soft Skills
    - 6.2 Technical Proficiency Gained
    - 6.3 Recommendations for Bayport IT Operations
7. **Conclusion**

1. Introduction

I work at Bayport Credit Union, which is a Financial Institution in the Hampton Roads area. This Credit Union has a very strong historical legacy as it has been open and servicing members since 1928. It is formally known as Newport news shipbuilders Credit Union to serve the financial needs of shipyard employees and their families. Throughout the years, this company has grown tremendously and proudly serves approximately 152,000 members with $2.4 billion in assets. Prior to my internship with the Information Security Department, I already worked in IT as a Field Support Analyst which requires me to travel to different branches and troubleshoot any hardware or software issues on site. So, being that I work in the IT department, I already had a familiarity with the Information Security Department, but it was a very simplistic understanding. This Internship acted as a bridge between homeroom learning and expert application. My internship with Bayport Credit Union was an extraordinary encounter that extended my understanding of IT framework, security measures, and functional proficiency. This paper documents my learning during throughout internship, which mainly focused on vulnerabilities within remote servers, carrying out a PC refresh cycle, and assessing progressed monitoring frameworks. Every one of these errands added to the Credit Unions overall objective of keeping up with secure, productive, and easy to understand IT activities.

2. Outline of Bayport Credit Association's IT Tasks

2.1 The Role of Remote Servers

Remote servers are the foundation of Bayport's IT tasks. They permit IT experts to associate with worker gadgets remotely, empowering, investigating and updating without expecting clients to

be truly present. This arrangement is especially critical for a disseminated labor force or during times when in-person connections are limited.

During the initial period of my internship, I dove into figuring out the remote server's functionality. It was apparent that this platform essentially worked on functional proficiency by decreasing the requirement for in-person mediations. The adequacy of remote servers relies upon steady and solid connectivity. Any disruptions in this association can prompt deferred investigating, expanded personal times, and expanded disappointment among workers. As a feature of my examination, I analyzed ways of further developing server uptime and limit margin time through cutting edge monitoring devices and computerized cautions. I additionally investigated the reconciliation of multifaceted verification (MFA) and encryption conventions to get remote access. By recognizing these possible areas of progress, I meant to fortify the general framework, guaranteeing that Bayport's remote server could work without a hitch and safely, no matter what the outer conditions. Carlson, J., & Johnson, S. (2021).

2.2 Significance of PC Lifecycle The board

Another critical piece of Bayport's IT activities is its three-year PC lifecycle. This coordinated strategy ensures that all devices stay completely educated in regard to current programming and adhere to the latest security standards. The quick speed of imaginative movements infers that more settled devices can promptly become conflicting with new programming, which can incite execution issues and security vulnerabilities. Outdated equipment could fight to help more exceptional applications or fail to give the dealing with influence vital to ideal execution, achieving all the more sluggish work cycles and potential productivity setbacks.

By reliably stimulating its PCs, Bayport mitigates these risks and works on useful capability. Replacing more settled computers before they become a liability permits Bayport to keep a safeguarded IT environment, limiting the receptiveness to cyber risks. Additionally, overhauling devices ensures compatibility with the latest security features, similar to undeniable level encryption and complex affirmation shows, which further protects sensitive information and hinder unapproved access. This proactive approach maintains business continuity as well as further creates laborer experience and satisfaction.

2.3 Monitoring Through Remote Administration Devices

Remote Monitoring and Management (RMM) instruments are necessary to Bayport's IT tasks. This permits IT groups to monitor device wellbeing, address issues proactively, and perform fundamental administration errands.

3. Recognizing and Tending to Vulnerabilities

3.1 Analyzing Remote Server Risks

My most memorable significant undertaking during the internship included investigating the vulnerabilities related with Bayport's remote server. Central questions included:

- Devices lacking viable programming for consistent remote access.
- PCs missing day to day fix refreshes, allowing them to remain uncovered to possible dangers.
- Devices not being turned on, forestalling updates and support.

These holes presented critical dangers, going from functional failures to cybersecurity dangers.

3.2 Proposing Practical Solutions

In the wake of distinguishing these vulnerabilities, I fostered an arrangement to address them. I started by ordering a rundown of workstations that were especially vulnerable to these dangers. My proposition included visiting end clients to:

1. Install the right programming to guarantee compatibility with the remote server.
2. Perform refreshes and confirm device wellbeing.
3. Assess whether more established devices required substitution.

3.3 Experiences from Exploration and Practice

Throughout this endeavor, I gained critical bits of information into the complexities of remote servers. This experience highlighted the critical prerequisite for proactive monitoring and the constant evaluation of security ensures the integrity of the Credit Union. As I conducted my research and perceived vulnerabilities within the server, it ended up being clear that keeping a protected IT environment is a constant test. The location of cyber risks is dynamic, with new vulnerabilities emerging regularly, which makes it principal for IT specialists to stay before logical risks. Bhardwaj, S., & Gupta, R. (2018).

Additionally, I learned about the meaning of an extensive method for managing IT security, where both hardware and programming parts ought to work couple. While remote servers are a principal instrument for IT gatherings, ensuring that they stay secure requires composed exertion across various workplaces, including ordinary fixing, programming updates, and client getting ready. This experience featured the meaning of keeping an eye on vulnerabilities before they can be exploited, making proactive security gauges a critical piece of Bayport's somewhat long IT strategy.

4. Implementing PC Refresh Cycles

4.1 The Imaging Process

The accompanying time of my internship position focused in on executing a PC refresh cycle at one of Bayport's branches. This cycle began with imaging new PCs, a significant push toward guaranteeing that the contraptions were designed precisely for use in the affiliation. Imaging incorporates getting the working framework, applications, settings, and data from one device and reproducing them onto another device. This methodology thinks about uniformity across all PCs, reducing the time and effort expected for individual plan and design.

I refreshed the new PCs to windows 11, guaranteeing compatibility with the affiliation's ongoing association establishment. This step was critical as it outfitted the contraptions with the latest security features. By guaranteeing that all PCs were designed with comparable working framework and security, I streamlined the coordination of the new devices into the branch's work process, guaranteeing smooth errands and limiting edge time.

4.2 Enhancing Security Post-Installation

When the imaging process was finished, I eliminated pointless programming (bloatware) and arranged the devices to whitelist just approved websites. These actions were vital in keeping a safe and proficient working climate, safeguarding both the devices and the sensitive information they deal with.

4.3 Results and Worker Criticism

The PC refresh brought about recognizable enhancements in representative productivity and by and large fulfillment. After the new computers were deployed, staff individuals detailed essentially better device execution, with quicker load times, more solid functionality, and

smoother activity of ordinary applications. Additionally, workers experienced upgraded programming compatibility, as the new PCs had the option to help the most recent programming updates and variants, lessening the gamble of programming related issues that were normal with the obsolete frameworks. Abbott, P. (2019).

Criticism likewise featured an expansion in general fulfillment, as representatives valued the superior speed and responsiveness of their devices, which permitted them to effectively perform transactions more. The smoothed-out reconciliation of the new frameworks into the current organization further added to a smoother work process, decreasing disruptions and limiting margin time. This positive input built up the benefit of keeping an ordinary equipment update cycle, guaranteeing that Bayport's IT foundation stays equipped for supporting both everyday tasks and future development.

5. Updating Remote Monitoring Frameworks

5.1 Limitations of Current RMM Instruments

During my internship, I additionally investigated the limitations of Bayport's ongoing Remote Monitoring and the board (RMM) programming. While RMM apparatuses are fundamental for remotely monitoring and overseeing devices in the Credit Union, I recognized a few critical disadvantages that might sabotage the security and viability of the IT foundation. One significant limitation was deficient monitoring, where the RMM apparatus neglected to reliably follow device wellbeing, programming status, and security vulnerabilities. This hole in monitoring could prompt undetected issues, like obsolete programming, missed patches, or potential security dangers, allowing frameworks to stay uncovered to cyber chances.

Additionally, while the RMM programming could perform fundamental assignments like programming updates and fixing, it needed progressed capabilities for recognizing and mitigating vulnerabilities progressively. This limitation could bring about deferred reactions to arising dangers, leaving the association more helpless against assaults. These moves prompted conversations about replacing the ongoing RMM device with safer and effective other options, for example, IGel, which could give better monitoring.

5.2 Exploring IGel as a New Standard

To address the limitations of the ongoing RMM programming, my manager acquainted me with IGel, a cutting-edge endpoint that prioritizes security and proficiency. IGel is intended to give better command over remote devices, especially in conditions where remote work and off-site access are normal. Dissimilar to traditional RMM apparatuses, IGel centers around getting endpoints by lessening the gamble of cyberattacks and ransomware through its high-level security conventions and constant monitoring capabilities.

I was entrusted with exploring IGel's elements and contrasting them and the current RMM devices to decide if IGel could give a more successful and secure answer for Bayport's IT needs. A portion of the critical elements of IGel incorporate its ability to unify endpoints, uphold stricter access controls, and smooth out device monitoring. Through my exploration, I discovered that IGel's ability to lessen potential assault vectors and it’s constant monitoring could fundamentally further develop Bayport's cybersecurity act, making it a promising trade for the ongoing RMM framework.

5.3 Testing and Future Applications

As a feature of this task, I introduced IGel on select devices to test its compatibility with Bayport's requirements. I found that IGel offered progressed security highlights and a more smoothed out client experience.

6. Lessons Learned During the Internship

6.1 Professional Development and Soft Skills

My internship at Bayport was not only a specialized growth opportunity; it also contributed fundamentally to my expert development. Working together with colleagues, bosses, and different divisions gave important opportunities to improve my relational abilities. Introducing my discoveries and exploration, for example, remote server vulnerabilities and endpoint the board expected me to express complex specialized ideas in an unmistakable and brief way, fitting my correspondence to various crowds with shifting degrees of specialized information.

In addition to correspondence, my critical thinking abilities were refined as I handled genuine difficulties within the association's IT foundation. Recognizing vulnerabilities, proposing arrangements, and investigating new instruments like IGel required critical reasoning and creativity. Additionally, dealing with undertakings, for example, the PC refresh cycle and remote programming refreshes permitted me to foster hierarchical abilities, oversee time successfully, and prioritize various assignments to fulfill time constraints. These encounters were instrumental in forming my ability to work effectively in an expert setting, and I presently feel more positive about my ability to add to a group and tackle complex issues in the working environment.

6.2 Technical Proficiency Gained

The hands-on tasks during my internship improved my specialized aptitude in regions, for example, remote servers, PC imaging, and programming refreshes. These abilities will be significant as I seek after a lifelong in IT.

6.3 Recommendations for Bayport IT Operations

In view of my encounters, I suggest the accompanying for Bayport's IT tasks:

1. Implement customary instructional meetings for workers to guarantee they grasp the significance of updates and support.
2. Transition to further developed frameworks, like IGel, to address existing limitations.
3. Continue putting resources into lifecycle to keep a state-of-the-art IT framework.

7. Conclusion

My internship at Bayport Credit Union gave me a thorough outline of IT tasks, from addressing server vulnerabilities to executing equipment refresh cycles and investigating new monitoring frameworks. Each task helped develop how I might interpret the critical job IT plays in keeping a safe and proficient business. This experience has furnished me with the abilities and information important to contribute genuinely to the field of data technology.

References:

Abbott, P. (2019). *The impact of IT infrastructure on organizational performance*. Information Technology Management, 30(2), 123-138. https://doi.org/10.1007/s10799-019-00307-7

Al-Fuqaha, A., Guizani, M., Mohammadi, M., & Ayyash, M. (2020). *Cybersecurity management in the era of IoT: Emerging trends and challenges*. Journal of Information Security and Applications, 49, 1-12. https://doi.org/10.1016/j.jisa.2019.102424

Bayport Technologies. (2023). *Remote monitoring and management tools for enterprise IT*. Retrieved from https://www.bayport.com/rmm-tools

Bhardwaj, S., & Gupta, R. (2018). *Endpoint management systems for enterprise cybersecurity*. International Journal of Computer Applications, 179(12), 15-20. https://doi.org/10.5120/ijca2018917327

Carlson, J., & Johnson, S. (2021). *Evaluating remote desktop software for business use: A comparative study*. Journal of Business and Technology, 43(1), 75-92. https://doi.org/10.1080/24714065.2021.1860072

Chen, Z., & Zhao, X. (2022). *Security issues in remote work: Addressing vulnerabilities in endpoint management*. Cybersecurity Review, 5(2), 45-58. https://doi.org/10.1177/20902243221102742

Cohen, S. P. (2019). *The role of patch management in maintaining secure IT systems*. International Journal of Cybersecurity, 8(3), 175-189. https://doi.org/10.1145/3405225

Dorfman, P., & Martinez, R. (2020). *The evolution of endpoint security management: From traditional tools to next-gen solutions*. Information Security Journal, 30(4), 253-270. https://doi.org/10.1080/19393555.2020.1744643

Patel, R., & Kumar, D. (2021). *Best practices in endpoint monitoring: Ensuring security in remote work environments*. Journal of Information Technology, 12(5), 102-116. https://doi.org/10.1080/10007968.2021.1831150