BlueCart Cybersecurity Vulnerability Assessment

This vulnerability assessment's purpose is to identify the possible threat sources of our company's cyber attack and present clear data of what each possible threat could mean for our company. I am addressing internal and external security, server security, password security and internal computer security such as the prevention of malware installation. This is not just important for the security team to know but for all 200 staff members as changes to the login process will change for everyone, this could also include our 5 million users also using a secure form of multifactor authentication. These attacks have the potential to cause catastrophic effects on our company and our 5 million users, including money laundering, and identity theft.

Risk Assessment Table

Threat Source	Threat Event	Likelihood	Severity	Justification	Remediation Strategy
Adversarial-Group External Hacker	Brute force login attempts	High	Very High	Likelihood is rated high based on the evidence of over 1,000 failed login attempts from an unknown IP address. According to NIST SP 800-30 Appendix G this indicates an adversary is "highly likely to initiate the threat event." Severity is very high because when we're considering impacts to million user accounts, that constitutes a catastrophic impact on our organization assets and individuals. According to NIST Sp 800-30 Appendix H this represents a severe or catastrophic adverse effect on organizational operations assets or individuals.	**IDENTIFY:** Conduct regular password auditing and implement password complexity requirements. **PROTECT**: Implement multi-factor authentication for all database access to prevent successful brute force attacks. **DETECT**: Implement failed login attempt monitoring with automated alerts for unusual patterns. **RESPOND**: Configure account lockout policies after multiple failed attempts.
Insider threat non malicious Accidental	Mishandling of critical and/or sensitive information by authorized users	Moderate	High	Likelihood is rated moderate because mishandling of critical or sensitive information will happen at least once a year while considering the number of staff and the amount of vulnerable information. Staff also do not have secure credentials which makes it even easier to mishandle said credentials by, say, writing your password on a sticky note. An	**IDENTIFY:** Implement best password practice and privacy screens to limit mishandling sensitive information **PROTECT**: Implement multi-factor authentication for all database access to prevent exposed credentials.

				accident is somewhat likely to occur Severity is ranked high because when considering the staff information of 200 people that could become compromised along with client information would have a huge impact on the organizations assets and individuals.	**DETECT**: Train staff to recognize and report changes or abnormalities on their systems. **RESPOND**: Configure account lockout policies if there are unusual logins or a staff reports an issue or abnormality
Insider Threat Malicious Adversarial - Insider	Conduct internally-based session hijacking	Low	Moderate	Likelihood is rated low because the adversary is unlikely to initiate the threat event. While the company has such weak employee credentials and security, and it would be a prime target for an inside attacker, it is not likely that an insider will be a reason for an attack and the reason for this specific attack. Severity is ranked moderate because of its low chance to occur and it would have negative effects on the company and assets but not to the point of catastrophic like a brute force attacker that has control of an entire system.	**IDENTIFY:** Implement training for recognizing internal threats and a system for reporting that protects all parties **PROTECT**: Implement discrete security programs that protect against malicious activity **DETECT**: The same discrete security program will detect malicious activity and immediately report to the security team for a timely response **RESPOND**: Investigate any other potential insider security issues, and determine how the software detection system did with detecting an issue and reporting it in a timely matter to see if adjustments need to be made
Structural-Software-Operating System	Introduction of vulnerabilities into software products	Low	Low	Likelihood is rated low due to being on updated and secure software, but malware whether through brute force or social engineering is always a possibility. Severity is ranked low because malware would impact only the few people that it can gain access to, such as the user that is logged in to the system with the malware and any data they might enter.	**IDENTIFY:** Implement training for recognizing malware or suspicious emails that could be attempting to install malware through social engineering. **PROTECT**: Implement a security system for incoming emails that will automatically detect malicious emails before

				Malware is also easier to prevent by training and informing staff of best practices while receiving messages or emails.	they reach their recipient. **DETECT**: Identify patterns in the malicious emails so that a specific response can be made to protect the company even further. **RESPOND**: Consistently retrain staff. Test the staff by sending them emails that are meant to look malicious and see what they do with it. Collect data of how the staff respond to learn how to best prepare the staff for unsafe emails.

1. How does NIST make assessments like this more systematic?
    a. There is no longer “guessing” or "inferring" but clearly written documentation that fits most security situations into it so that assessments between departments, companies, or nations can be compared to each other because they were prepared using the same framework.
2. Which specific elements of the NIST frameworks do you think would be most useful in a real-world security audit?
    a. I think that the five core functions, identify, protect, detect, respond and recover would be the most useful in a real-world security audit because it puts action behind the words and the data. If it really is a high severity risk and a high likelihood event then here is the plan to make sure that it doesn’t happen for your company. These five core functions would also be valuable information to share with leadership teams and stakeholders that want to know the plans for improving security. It makes the report full because without it you would just be worried based on how severe or how likely it could be.
3. How might using standardized frameworks improve communication among security professionals, and between technical and executive stakeholders?
    a. Standardized frameworks would improve communication among security professionals and between technical and executive stakeholders drastically. First of all you want to know that at least your company's security team is always preparing audits and reports the same way but if everyone followed the NIST standardized frameworks then companies who contract out together and those who work internationally would all be on the same page about the security issues present and how that information is communicated between companies or nations. Communication between stakeholders would improve because there is a part of the report that hits the "requirement" for everyone. On the technical side

there is the nitty gritty and on the executive side they can see the plan clearly written out about how the company will be protected which is all they care about.

4. Discuss any insights or surprising elements you discovered about the NIST framework approach to security assessment
    a. I was surprised to see how pretty much every possible security event that could happen was covered under the framework. There were several different categories and sections and sub sections that got to an even more specific possible security event. I was also surprised how easy it was to find everything but after the first or second time doing it I learned how it was all formatted and sectioned and was able to find my way through the document a bit faster.