Ethan Coyle

Addressing Weak Links and Implementing NIST Framework in Retail Environments

In the advancing digital landscape of the current world, being able to secure sensitive data and information stands as an imperative and critical prerogative, especially for major retail entities such as Amazon that oversee extensive data for their customers. At the very heart of organization security strategies lies proper identification and mitigation of the weakest link inside each organization's security infrastructure. The weakest link vulnerability represents a fundamental and egregious point inside of each infrastructure in which malicious outside exploiters attempt to breach and compromise the overall security and integrity of an organization. It is from these weaknesses that security flaws emanate from a plethora of sources including outdated software, inadequate and improper awareness of the system itself, human error as well as inadequate and ineffective security protocols. For one to fully grasp and comprehend the vastly intricacies of organizations and their flaws in their systems, one must delve fully into the understand of the weakest link inside of a system, as well as how a strategy called SETA(Security Education, Training, and Awareness) can overcome it. In addition to this, one must also delve into how attributes of the NIST Cybersecurity framework can protect the information systems of a retail giant like Amazon. Security within businesses and organizations remain paramount to prevent any outside entity or source from breaching the integrity of the company as well as understanding preventative measures can ensure that propagated issues within a business are effectively managed and mitigate the risks in the overall system.

Before one can understand all the intricacies that lie at the heart of an organization's security, one must ascertain a competent understanding of what some of the core problems are

with a system's weakest links. One of the most important and underlying issues related to the weakest link inside of a system is human error." Employees with access to critical data and resources are typically the single biggest flaw in any security system. " (Team, 2020). Human error constitutes a primary weakness in every system and organization. Systems and computers can catch certain things going on that humans cannot. Due to flaws within human nature, human beings are not able to catch or identify everything that is going on and some things might fall through the crack. This error can lead to sever consequences within any system. Whether by inadvertent or intentional design, employees within an organization possess the potential to compromise the security inside of a system through a plethora of avenues such as : phishing attempts done through company email or other forms, not properly handling data within an organization, weak passwords to sensitive data, and simply not being properly aware of all of the potential risks associated with being inside of and organizational system. "At the core, the struggle to always find a way to prevent people from making the same mistake more than once, and the difficulty in anticipating the next, new mistake, makes people the weakest link in the chain." (Davies, 2023). For an organization, being able to address the issues that arise from human error vulnerabilities remains a pivotal point inside of any structure to fortify security especially within large retailers such as Amazon and other competitive retailers. To efficiently and effectively mitigate the risks that are associated with such vulnerabilities, organizations must be able to mitigate such risks and center their focus as well as efforts on implementing SETA programs within their organization." SETA programs help businesses to educate and inform their employees about basic network security issues and expectations—helping to prevent commonplace cybersecurity mistakes that lead to damaging data breaches."(Dosal,2019). The initiative to implement these programs inside of an

organization plays a pivotal role in the ability of an organization to enhance their cybersecurity posture by the ability to educate employees within their organization about several aspects of security. These trainings in SETA include understanding of potential threats within and outside of a system, the ability for the organization to adeptly train employees over the proper handling of security incidents that might arise, as well as fostering an environment and culture within the organization for situational awareness regarding numerous security concerns and how to manage them.

For one to fully grasp what SETA entails, it is important for one t fully understand of all the various aspects and key elements that go into the core fundamental aspects of a SETA program. The first portion of SETA is Security Education. Security education involves the imparting of knowledge to employees with an in-depth situational knowledge and comprehension of numerous security threats that pertain to a system, organization, or the individual themselves. By and organization being able to provide education over these issues, they can educate their employees over the various risks, threats and best mitigation practices that can be done to help reduce problems that might arise that can compromise a whole organization. For retail giants like Amazon, this education entails the enlightening of various phishing threats, malware , ransomware attacks, social engineering and insider threats that seek to compromise and organizations integrity onto their employees. Moreover, this education also entails the organization being able to disseminate knowledge to their workforce about the best practices inside of the company such as password security and complexity, secure data handling and adherence to the regulatory requirements within an organization to maintain and implement security policies within that organization. When attempting to devise a strategy for this education, a multifaceted approach is needed to ensure that the company can provide workshops,

modules, training exercises, engaging sessions for the organization to impart on their employees is a crucial part of being able to provide organizational awareness. By providing these as well as a plethora of other related training modules, an organization can not only ensure that the workforce inadequately trained and well versed of problems that might arise as well as being able to mitigate risks more easily with proper training and knowledge within the organization.

Security Training is also another crucial element that needs to be implemented inside of each organization to adequately prepare and train all personnel inside of the organization to be able to identify and manage risks that might compromise the integrity of the organization. If an organization can provide security training to their workforce, this can lead to less compromising issues that come up for several reasons. With the implementation of security training, an organization can equip their employees with practical skills to identify, respond to and mitigate cybersecurity threats. Training exercises such as simulated phishing attacks via company emails with a bogus link can be especially effective in educating employees on potential threats that might arise. Periodically sending out official-looking emails through an organizations IT department that can tempt employees to click on links within them that, once clicked takes the user to a page that says something like " this was a phishing attempt test" or something similar and then providing the employee with training that they must complete is a good practice. Within this type of exercise, the knowledge of how a phishing attempt works, education on how what and why these occur, and mitigation tactics can impart invaluable insight for each employee. This not only helps the employee, but the organizational integrity overall becomes more secure as well. Another training that could be particularly important is for the IT personnel withing the organization to participate in specialized training custom tailored to providing real-life scenario

training to evaluate responses to security, best coding practices to prevent data leaks as well as a multitude of other issues that might come up.

Security Awareness initiatives within each system are also another key component involved in protecting and mitigating risk associated with the weakest link inside of a system. These initiatives aim to instill a company's workforce with a more comprehensive mindset targeting a more security- conscious approach to their business-related work. This awareness also allows the employees to become more proactive participants within the organizations defense abilities to mitigate cyber-related threats. One way that security awareness can be centralized is using reminders, workshops, newsletters, posters, and any other form of intuitive informing to the organization's taskforce. These constant reminders to the employees impart a constant reminder of certain practices that might prove beneficial for the overall security and safety of the company these employees work for. For corporations such as Amazon, this might encompass regularly scheduled and update newsletters informing their employees of current security problems that are strategically placed within offices or sent out periodically through company email to give constant reminders about potential risks. In addition to SETA programs, the ability to leverage cybersecurity frameworks such as NIST Cybersecurity Framework is critical in an organization's ability to fortify their security infrastructure. For one to fully grasp how beneficial NIST Cybersecurity frameworks can be inside of an organization, on must also delve into the fundamental concepts of what NIST Framework is and how it can prove beneficial.

NIST Framework is widely recognized and offers in-depth and comprehensive approach that provides an outline on best practices within an organization on managing and reducing

risks related to cybersecurity threats as well as an overall guideline to mitigation tactics to reduce these risks. “The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.“(FTC,2018).NIST Framework constitutes of five core functions that are paramount to success. These fundamental concepts include Identify, Protect, Detect, Respond and Recover. To gain a comprehensive knowledge of the benefits of NIST Framework, one must be able to fully comprehend and gain competent knowledge over all these core foundations.

The first fundamental core concept in NIST Framework is Identify. This “identify“ function revolves around the insight gained of a deep understanding of an organization’s security risk and vulnerabilities. In a retail environment, this knowledge entails the organization as well as employees to undertake a comprehensive assessment of business processes, data that is being accessed and analyzed, company assets, and the various systems used within the organization. This encompasses a meticulous inventory assessment of all the hardware and software assets used within the organization, the critical business process that are conducted as well as the regulatory and compliance procedures that are pertinent to an evolving retail market. According to a research study conducted by Ethan Bresnahan, it is stated that “ The result is a clearly defined state of an organization’s cybersecurity posture articulated to both technical and business-side stakeholders.”(Bresnahan,2021). By incorporating systematic assessments and vulnerability scans into an organizations operational paradigm, the organization can be aided in areas such as potential weak points in their systems and how they might be able to remediate those to make those less likely to be the sources of issue. In turn, by incorporating these various procedures, prioritized actions can be instantiated easier based on the risks that are identified.

The second fundamental concept related to NIST framework is “Protect.” This function involves a robust implementation of security measures to ensure that the security of the organization and its data is secured and resilient to threats and remains a crucial core foundation for the critical security inside of the organization’s infrastructure. This function can range from user control access and encryption, regulated software that constantly keeps systems up to date and the involvement of firewalls and prevention systems. “With breaches becoming increasingly common, employing proper protocols and policies to reduce a breach’s risk is becoming especially crucial. “(Bresnahan,2021). All these implemented security protection measures aim at the safeguarding of overall security and the restriction of unauthorized access. By implementing a user control access inside of an infrastructure, if there were a breach inside of the organization itself either by human error or any other form of breach, the whole company is not compromised because that person only has access to certain parts of the infrastructure which details a separation of duties and access within the company. Also, by enabling user control access, this ensures that not just anyone can gain access to privileged data that is only meant for specific individuals within the corporation. The introduction of firewalls and security measures like firewalls help to prevent outside and unauthorized access to the company. The firewalls help to secure the infrastructure from exploited attempted hacks that are seeking to gain access especially with malware and viruses. For a company, especially one that manages a vast amount of data related to customers, identity information and access management , (IAM) systems should be a primary focal point in which the organization should focus. These systems help to ensure that the employees have access privileges appropriate to their role and position and to ensure that data that is sensitive is only able to be accessed by authorized personnel only.

The third core fundamental to NIST systems is the concept of "detect." This concept emphasizes primarily the identifying time of the incident in question. By emphasizing the identifying the time of the incident, the impact of the incident can be minimized because of the timely identification of the situation. Situations that occur inside of a business should be able to be properly caught and detected properly to be able to mitigate them as soon as possible. A corporation should employ a robust set of monitoring tolls and systems to have in place to detect events that occur in real time with the timeliness of the detection systems, compromising breaches or issues related to the organization are drastically reduced. Integrating advanced threat detection tolls that utilize machine learning and artificial intelligence(AI) also allow for a significant enhancement to the company's ability to detect and respond to all forms of sophisticated cyber threats that can occur. In line with this is also the organization's ability to respond to threats or problems. This fourth core concept enhanced the detection inside of the organization by instilling a set of appropriate techniques that are targeted towards how to manage those issues if they are detected. This response method necessitates a well-rounded and robust incident response plan that should be instantiated inside of the organization. This response can be conveyed to all individuals of the organization either through incident response drills set forth by the employer or establishing a specific team inside of the company that has a comprehensive training on handling and responding to problems. The integration of these can drastically reduce critical problems that can occur if nobody inside of the company knows how to manage scenarios such as a security breach. Furthermore, to further enhance preparedness and response to incidents, organizations can conduct various cybersecurity scenarios in which the employees must figure out how to respond to the issue and then attend training based on the method that is used in the response to further educate everyone in the company on proper procedures for

mitigating threats. By instilling these drills, this not only gives the organization insight on response effort but also facilitates insightful and invaluable learning for everyone to further improve preparedness in the case of an incident occurring.

Lastly, the recovery process is a paramount foundation that is incorporated in the NIST Framework and remains of paramount importance." Recovery activities implement plans for cyber resilience and ensure business continuity in the event of a cyberattack, security breach, or other cybersecurity event. "(IBM, 2022). This function revolves around the organization's ability to restore and bring their systems back to normal functional operations after an incident has been managed. To benefit from this, the organization must integrate a robust backup and recovery procedure that entails everything that occurred in the incident and how to prevent it in the future. This concept is more like a live and learn concept. If an error occurs and it gets resolved, it needs to be fully documented on what the specific incident was, what happened, how it was resolved, and how to prevent the issue from happening in the future. To ensure that the most is gained out of this, organizations must regularly assess their backup and recovery procedures as well as create all the necessary documentation in case that issue arises later in the future. By documenting and highlighting key aspects of the process, this benefits by providing a more well-rounded resilience inside of the company's system. Recover:

In conclusion, the ability for an organization to safeguard its system and data against cyber threats is a paramount concern for retailers of major corporations like Amazon. The weakest link inside of the system often emanates from human error more so than anywhere else as well as a lack of awareness. Addressing these vulnerabilities calls into question the necessity for a comprehensive approach that entail incorporating systems like SETA programs as well as

leveraging NIST Framework to help establish a more secure and protected environment. By amalgamating these strategies, organizations c can significantly enhance their security by protecting their data, systems, as well as any stakeholders that have interest of ties to the organization which fosters a more secure digital environment in the landscape of technology the is rapidly changing every day.

Work Cited

Bresnahan, E. (n.d.). *NIST Cybersecurity Framework Core Explained*. Www.cybersaint.io. https://www.cybersaint.io/blog/nist-cybersecurity-framework-core -explained#:~:text=Here%2C%20we

Davies, J. (2023, July 5). *Why Humans Are the Weakest Link in Cybersecurity*. Alert Logic. https://www.alertlogic.com/blog/why-humans-weakest-link-cybersecurity/

Dosal, E. (2019, January 22). *Building a Security Education, Training, & Awareness Program*. Www.compuquip.com. https://www.compuquip.com/blog/security-education-training-awareness

FTC. (2018, October 5). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

IBM. (2022, August 21). *What is NIST Cybersecurity Framework? | IBM*. Www.ibm.com. https://www.ibm.com/topics/nist

Malik, K. (2023, January 14). *Are Humans the Weakest Link in Cyber Security? - Astra Security Blog*. Astra. https://www.getastra.com/blog/security-audit/humans-in-cyber-security/

Team, idea BOX. (2020, October 19). *How to Build a Security Education Training and Awareness Program (+FAQs)*. Www.ideabox.com. https://www.ideabox.com/blog/cybersecure-employee-training