Nathaniel Crosby

624 Echo Cove Lane

Charlotte, NC 28273

704-890-9040

Tyetechnologies@yahoo.com

March 30, 2020

Mr. Walton

CIO

Walmart Inc

123 Main Street

Charlotte, NC 28273

Dear Mr. Walton:

My name is Nathaniel Crosby. I am a long-time employee and customer of Walmart Inc. and I am writing this to express my concern about a recent discussion and the pending decision to implement a new information system. I understand that the decision is being considered. I think I can provide ways to improve cyber security to protect your company and customers. The first thing is the cyber domain. Cyber domain is a global domain within the information environment that contains the interdependent networks of information. The domain also includes technology infrastructures and data. Examples of this is the internet, telecommunications networks, computer systems, and controllers. The key components of an information system are hardware, software, database, network and people.  These components come together to perform input, process, output, feedback and control. Hardware consists of input/output device, processor, operating system and media devices. There are some similarities between cyber domain and information systems. Cyber domain deals with servers, intranet and channels that are designed for data transfers to stay protected and for those that are allowed. Information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. My suggestion is to introduce a new information system to this company. The best way to introduce this system is to have the following steps put in place. The first step is to appoint a change leader. The change leader role is to make sure everyone is progressing well, be the go-to person for queries and issues from the team and be the link to external support. The next step is to Assign task to each team member. Come up with some tasks everyone should complete to master this new system, starting with the simplest, and progressively getting more advanced. The idea is that once all these items are completed by someone, that person should be an advanced user of new system. Next, have a group session. During this session, it is time to present the system to the team and explain how they will learn how to use it, hold an onboarding session for your team. This is when you address the issues such as What does the new system do? Why are you introducing it? What are the expected outcomes? Make it clear to everyone that they will need to complete the tasks in their own checklist. By the end of this session everyone should be ready to get going. Next have everyone on the team share their progress. This approach of a new system will help with the software development life cycle. The software development life cycle includes Requirements, Design, Implementation, Test, Maintenance. There are four parts to the domain. The physical domain (hardware and software); the information domain (confidentiality, integrity and availability of information); the cognitive domain (how information is perceived and analyzed); and the social domain (attention to ethics, social norms and a broad social. External threats are malicious campaigns and threat actors that attempt to exploit security exposures in your attack surface that exist outside the firewall. Targeted external threats that can compromise your employee or customer data security include: Deep and dark web discussions about your organization. A threat to the company system can cause Walmart to lose customers and employees due to no security protection. Walmart as a company will have to pay millions of dollars on lawsuits. Walmart will also have spend on rebranding their brand and name.

Are these tradeoffs that we really want to make? I am looking forward to your response.

Sincerely,

Nathaniel Crosby