**CYB-250**

**Milestone**

**Candace Ralston**

**2/3/2023**

People are always excited about the newest technology that comes out, especially when the company that they work for tries it out. Bringing new technology in the work can help with productivity, sales, and even make life easier for the employees. The technology that we will be talking about is a new headset. This headset has the ability to project documents on an optical screen for the technicians to use. The headset will have communication with the main server at the central office. Then it goes through the persons cell phone with a Bluetooth connection. This headset will increase the company’s accessibility, workflow, and help in many other ways as well. Unfortunately, new technology also brings new risks to the company as well.

Of course, the biggest risk that the company has when introducing new technologies into a company would be the human factor. What companies have done in the past was reprimand people and even written them up if they allow a breach to happen willingly or not (Kaspersky.com). This of course just got people to not report any type of breach or attack. They then try to handle it themselves, like with ransom ware attacks they just pay the ransom instead of reporting it. There was several instances of that happening and even after they paid the ransom there were times that the attacker came back and did it again but instead of one computer they did it to every computer on the network. People don’t need to be written up, reprimanded, or even fired if this happens, they need to be told what not to do. The company needs to have meetings and workshops that help people deal with breaches and attacks. This would cut down on them trying to handle it themselves and them not reporting them. For instance, with these headsets if the company tells people that they would be fired if they lost them or they got stolen they would not report them lost or stolen. They just need to tell people how important the device is and what would be lost if something happens to it.

As said in the last paragraph, the best data protection strategy would be training. It is said that data protection should not fall on the IT staff but on everyone (mulibriefs.com). Even though it means more training for everyone it would be good knowing what to do and what not to do. What needs to be done is just training people for what can happen. If more companies do this instead of punishing people, they will more likely do what is best for the company. Like with this headset, as soon as people receive the device they should be told and shown what to do if they lose it or it gets stolen.

One of the System protection trends that I will talk about is an endpoint/server protection technology. One of these technologies is a next-generation antivirus (NGAV). This is a solution that applies an advanced endpoint that protects any form of technology (cynet.com). This employs machine learning and artificial intelligence (AI) to identify new types of malwares. This will tell the machine that there is malware and that it needs to take care of it.

**References**

[The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within | Kaspersky official blog](https://www.kaspersky.com/blog/the-human-factor-in-it-security/)

Conn, R./Oct. 21, 2020/[MultiBrief: 5 data protection trends of 2020 that will define security next year (multibriefs.com)](https://exclusive.multibriefs.com/content/5-data-protection-trends-of-2020-that-will-define-security-next-year/science-technology#:~:text=5%20data%20protection%20trends%20of%202020%20that%20will,Shifts%20in%20Responsibility%20...%205%205.%20Training%20)

[Endpoint Protection: The Basics and 4 Key Technologies (cynet.com)](https://www.cynet.com/endpoint-protection/endpoint-protection-the-basics-and-4-key-technologies/)