**CYB-250**

**Cyber Defense and Emerging Trends**

**Candace Ralston**

**2/14/2023**

There are always factors in cybersecurity that need to be thinking of when putting out a new type of technology. The biggest factor that the people need to think of when thinking of the security in new technology would be the human factor. The human factor is actions or events that a person would do that would lead to a successful data breach. There are many reasons to trust employees but this is one reason not to completely trust them. After all they are not just putting themselves at risk but the company and everyone in it at risk. All it takes is one person opening up the wrong email, not updating the security on a device, or going on the wrong website to have a breach. Hackers are always finding ways of using the human factor to hack into a company. In fact, it is said that 53% of viruses and malware come from careless and uninformed employees (Kaspersky.com).

With the new head set that allows you to see important documents anywhere having the right security is the way to go. After all the headset is in constant communication with the server that resides in the central office through the persons phone. Once people start noticing what these headsets do they will want to steal it or hack into it. Hacking into these headsets or even stealing them to get into them would allow hackers to access the central office server and all the data there. Knowing the risks and the punishments and the rewords to keeping the headset from being hacked into is the way to go.

There are strategies to protect companies from a security breach from these headsets because of a human factor. One of these ways is to inform employees that it could happen and even giving them information on attacks that have happen. Having a meeting or a training video with information on security before giving them the headset would be the first thing to do. Also, these meetings or training videos would be mandatory. Another way would be to put restrictions that would be mandatory for all the devices. One of these restrictions for a company device would be to remotely create, access, and delete data in your work profile (support.google.com). This would make sure that you aren’t doing what you are not suppose to be doing and are doing what you are supposed to be doing. They would need to do this if the headset was stolen or lost. So, the company would be able to remotely delete all the files on it and make sure that it is no longer connected with the server.

There are many risks that these strategies can prevent. One of these risks would come from phishing emails. This is when attackers send malicious emails designed to trick people into falling for a scam (proofpoint.com). A phishing attack simulation tool has showed a failure to see it range between 4-20% depending on the attack (proofpoint.com). Another type of risk would be ransomware, which is malicious software (malware) that threatens to publish information or block access to data (proof point.com). Unless that person or company comes up with a ransom of let us say $1million dollars they will publish information or continue to block access. Of course, the main way of preventing these attacks and others would be to reward the person or people that report the attacks or prevent them. When someone prevents an attack from happening, they get something like a cash bonus or in a retail setting a gift card. If they report an attack they would get the same thing, most likely less because they didn’t prevent an attack. By doing this you make sure that you are showing the employees that it is a good idea to report or prevent an attack.

One of the emerging trends in cybersecurity because of human factors are remote jobs. Since covid more people are going with remote jobs because of the convenience of not leaving their home. However, because of this hacking has become more common. Companies still need to be aware of who is on the server and what are they doing. The people on the remote jobs need to make sure that their security is up to date and that they are aware of any phishing email or ransomware. Another human factor trend would be people wanting to bring their own devices (BYOD). This would mean that the company would need a BYOD security plan or update an existing one. Many companies do have a BYOD policy but it is not up to date with todays technology. So, they would have to make sure that all policies are up to date with today’s technologies. With the new headset I would also looking into another trend were people are wanting to bring a company device home. The company would have to make sure that they have a policy for that or to update one. You would need to make sure that all of these trends are under a plan that can help with an attack. With the headset you would want to make sure that you can remotely disable or delete the information on it if it is stolen. The company has to work with the employees but also has to protect itself.

Having a data protection strategy in case of a breach would be a good idea as well. This would allow for any protection against an attack. With the smart headsets as an example, I would go with a data back up and recovery. This will back up all the data, unless it’s no longer needed, to a secure and protected location. When this data is needed, like after an attack and they lost the data, a recovery process releases it from its secure storage and verifies it (techtarget.com). This would be a good strategy to have in case of one of those headsets getting lost or stolen because the company would more then likely wipe the information on it clean. The risks would be that if you needed to wipe the headset clean you would not be able to retrieve any of the information on it. The rewards would be that you would be able to retrieve the lost information.

When using cryptographic techniques with the headset you would want to use asymmetric encryption for securing the documents (educba.com). This helps to resolve a key exchange problem of symmetric encryption by exchanging the secret keys. Since the documents on the headset need to be moved around and sent to different people this would be needed to make sure they get to the right person. The disadvantage of this would be that someone could steal the key then they could read all of the documents. Also, steganography would be good as well (educba.com). This is a technique that facilitates the hiring of a message that is to be kept secret inside other messages. So, again when the person with the headset needs to send a document to another person, they would be able to know that the right person has it. One of disadvantages of this would be the other person unable to read it because they don’t know what to look for. The only way to see the document is to have the keys or know the message inside the other message. There are advantages and disadvantages to everything but having one or more of these would help the company.

For the system protection I would go with endpoint/server protection. This is the ability to protect the assets that are last touch point of the network it is connected to (cybersecurity.att.com). These endpoints are any remote device that is sending and receiving communications within an organization’s network. These include desktops, laptops, tablets, smartphones, servers, POS systems, and BYOD devices (cybersecurity.att.com). This would be perfect for the smart headset since it already works with other devices like it. The risk at not having endpoint would be that the device would be more vulnerable to attacks. Attackers can use your company’s assets to execute code or exploit vulnerabilities through an endpoint. With the endpoint protection you would be able to protect the vulnerability that a device like the smart headset.

Another type of security technology that I would like to talk about would be the intrusion detection system (IDS). This is technology which monitors all the traffic that enters the organization to ensure that those are not malicious (educba.com). An IDS is really becoming popular right now because people are still trying to get into companies. They are either trying to steal or trying to damage and sabotage the company. Even though there are people that will try to get at the company through the network there are still those that will do it the old fashion way. There are even people that hear that the company is coming up with new technologies that they want for theirs. So, they try to get into the company to steal the idea or sabotage it. Back to the example with the headset, if people hear about this before the company starts using it people will want to try and steal it or sabotage it. There are existing policies on intrusion detection but they do need to be updated because there are ways that people can sneak in. In one place I heard that a person stole a vest of the workers and just walked in the back and walked out with a new TV. So, an IDS system would still be good for companies to have and not just go with security on their network.

Having the right security, it the way to go with any size company. Even if you have just a web only company you have to have all kinds of security just to be sure nothing gets stolen. Of course, there are security policies and plans that you don’t think of when doing a small business. So, you would have to look into all kinds of policies and have a plan as to how to work with them.

**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/)

[What policies is my organization enforcing on my device? - Android Enterprise Help (google.com)](https://support.google.com/work/android/answer/7502354?hl=en#zippy=%2Cmy-organization-owns-my-device)

[The Human Factor of Cybersecurity - Key Findings Hub | Proofpoint US](https://www.proofpoint.com/us/human-factor)

Kirvan, P./Jan. 6, 2021/[20 keys to a successful enterprise data protection strategy | TechTarget](https://www.techtarget.com/searchdatabackup/tip/20-keys-to-a-successful-enterprise-data-protection-strategy)

Tawde, S./[Cryptography Techniques | Learn Main Types of Cryptography Technique (educba.com)](https://www.educba.com/cryptography-techniques/)

Stone, M./Aug. 12, 2020/[What is Endpoint Protection? Benefits, Solutions Explained | AT&T Cybersecurity (att.com)](https://cybersecurity.att.com/blogs/security-essentials/endpoint-protection-explained)

Pedamker, P./[Security Technologies | Top 7 Key Security Technologies (educba.com)](https://www.educba.com/security-technologies/)