The Role of Humans in Cybersecurity

Jared L. Williams

Marymount University, IT-120-B

Abstract

In the video, ‘The Biggest Issue in Cybersecurity is Humans, Not Machines’ from UK Wired on YouTube, the speaker Rachel Botsman explains how people’s privacy is most compromised by human error, not technology. Botsman explains what us as consumers can expect from companies with our private information. She made it her mission to travel and share her knowledge of online security to cybersecurity professionals, business leaders, influencers, and more. In the video she explains how an Uber driver in Michigan, Jason Dalton, shot six of his passengers in a one day span. This shooting made the public rethink how safe we are when using technology you might not question, such as Uber. People questioned how Uber evaluates who they allow to drive for them. She urges in the presentation to continue trusting these companies because again, the problem was the human component.

Keywords: Uber, cybersecurity, access controls, trust stack

Introduction

Humans serve a vital role in technology because they are tasked with telling the computer what to do. The role humans serve is to continue to learn and create new technology. Without humans technology cannot advance so it's important they keep making progress. Large businesses play a huge role in the advancement of technology by how they treat their employees, or how much creative freedom the company gives them.

Literature Review 1

In an article from Micke Ahola on Usecure he explains the two types of human errors: skill-based error and decision-based errors. Skill-based errors are small mistakes that happen when performing everyday jobs or tasks. Decision-based errors happen when humans make faulty decisions. An example of a skill-based error is a person is sleepy or distracted and makes a simple mistake. A decision-based error is when a person doesn't have the knowledge necessary to complete their task, resulting in an error they might not even know occurred. He then transitions to talking about humans and our passwords, or lack thereof. Ahola says the most used password to this day is, "123456" (Ahola 15). Reasons like that make it so much easier than it should be for those looking to take advantage on the internet.

Literature Review 2

In an article from *The One Brief* titled, "The Key To A Holistic Cyber Security Program: The Human Element" it mentions how not the only threat of cyber breaches comes from outside audities. The author writes that, "43 percent of data loss" comes from employees within the company, whether it be on purpose or not (The Key To A Holistic Cyber Security Program: The Human Element 5). An angry employee could be encouraged to cause financial harm to the company. On the other hand an employee could carelessly open a link exposing the company's systems to malware. It also mentions how employees who bring their own device and connect to the internet cause a security risk. These devices can be hacked into much easier, without having to breach into extra walls. Some things companies can do to prevent or lower the chances of attacks are to prevent personal devices in the workplace and focusing on the individuals you bring in. Once companies have trustworthy employees then their job is to keep them happy. Having happy employees that enjoy their job and how they're treated makes for a more cyber-safe, and effective company as a whole.

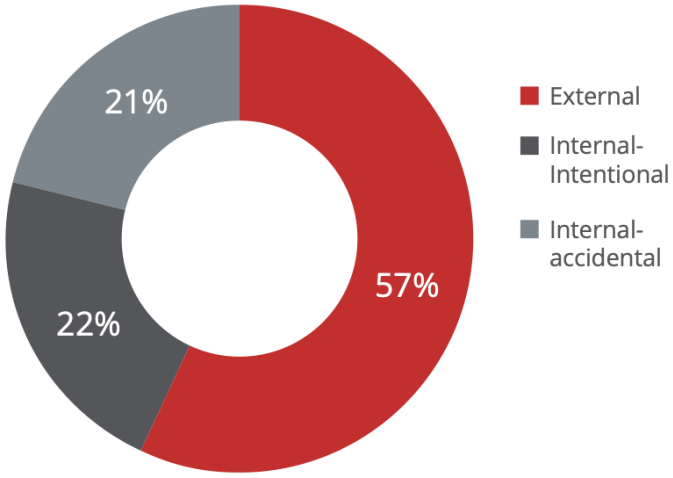

Figure 1. Actors involved in data breaches.

Reflection 1

I thought "The Role of Human Error in Successful Cyber Security Breaches written by Micke Aloha was a very informative article. He went in depth about the different types of errors humans can make in cyber security. Before the article I had not heard of skill-based or

decision-based errors, but he did a good job explaining them. The fact that the most common password in the United States is 123456 was really surprising to me. This shows that Americans are not equipped with the knowledge of how to defend themselves from online attacks. Or that they know what can happen, but are ignorant to the fact that those attacks could very well happen to them.

Reflection 2

The second article from *The One Brief* changes focus to cyber security attacks and how they happen. I found it very interesting and quite frankly surprised that 43 percent of cyber attacks come from the company's employees themselves. Even more surprising was the fact that more attacks from within the company were intentional versus those which were not. I already knew about companies that allow workers to bring their own devices, having a higher chance of unintentionally allowing hackers in their systems because my father works for the military. At his job all non-government phones must be turned off and placed in a locker before entering the workplace.

Conclusion

This module taught me a lot about how important the human aspect is in technology and online security. Hackers find ways to expose the human component because they know that's the area prone to mistakes that can be taken advantage of. I also learned that normal people who use technology just simply aren't aware of the threats that are out there. Another thing I found interesting is how humans can unawarely make errors and not know until months later. These are the errors that get people fired because they can come back and cause real financial conflict for the company involved.

Ahola, M. (n.d.). The role of human error in successful cyber security breaches. Retrieved February 08, 2021, from https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

The key to a holistic cyber security program: The human element. (2018, March 08). Retrieved February 08, 2021, from https://theonebrief.com/people-humans-cyber-greatest-risks/