How the “short arm” of predictive knowledge could be a problem within the field of cybersecurity

By: Shacara Pitre

December 7, 2021

Introduction

(1) I believe that the “short arm” of predictive knowledge could create more problems than solutions. Technology in itself is predictable and can be unreliable at times. To clarify, our computers can shut down and we can lose files, data, etc. if they are not backed on a hard drive or cloud. The use of technology alone can come with many pros and cons. One of the pros of technology is that it allows for more opportunities for people as well as security. However, the use of technology can come with cyber criminals who want to hack our servers, cyberbullying, scammers, etc. Overall, technology is a tricky area to navigate because there are so many possibilities that allow for people to do good and bad things. Throughout this paper, I will analyze and explain my opinion in more detail of why the “short arm” of predictive knowledge could be a problem within cybersecurity.

The “short arm” of predictive knowledge

When it comes to developing a cyber-policy and infrastructure, we need to be aware of the challenges that are out there. Also, we need to understand the risks involved with using technology. I think we need to be creative, but also practical when it comes to these strategies because security is important in preventing hackers from accessing our information. (2) We

should not rely on predictive knowledge when it comes to figuring out ways to advance our cybersecurity. This is because we can never really know which obstacle a hacker might use to either get into our system along with when they would attack. Furthermore, the information with predictive knowledge is not proven to work, so it should not be relied heavily on or taken too seriously without any factual information supporting it. Overall, it should be taken into consideration as a resource because technology is steadily growing it just should not be the end all be all.

What we know is beneficial for protecting infrastructure

Having some form of security in an organization or business is vital, especially with the aging of technology. The effects of not having any form of cyber security can be detrimental to a company. For instance, "it can harm an organization's ability to innovate and to gain and maintain customers" (NIST Improving Cybersecurity). One thing that we do know is beneficial to a company is the NIST Cybersecurity Framework. There are many benefits, but one of them is that it protects an organization's private information and keeps it confidential.

Also, the Framework is adaptable, in a sense, that it can be altered to fit the needs of an organization and is able to manage the various risks in the organization. Likewise, the Framework allows for organizations to keep their existing forms of cybersecurity risks protection. However, it is more to support them to make their company stronger against any kind of cyber threat. Another benefit of the NIST Cybersecurity Framework is when it comes to the Framework profiles. They are beneficial in the sense that they are able to "describe the current state of or the desired target state of specific cybersecurity activities" (NIST Improving Cybersecurity).

A benefit of the Framework is that it provides an opportunity for communication, specifically between stakeholders in organizations. This is important when it comes to a successfully run organization. Furthermore, it is important for stakeholders to communicate their vision for the company along with strategies to eliminate the cybersecurity risks. Overall, the NIST Framework can be used in the future at my workplace or at any workplace setting because going into any job, you want to make sure that the company's information is secure and ensure that it does not undergo any cybersecurity risks. The Framework would be used for identifying measurements, specifically as it relates to managing the risks of cybersecurity. Lastly, the NIST Framework is one of the many tools out there that we know of to ensure our information is secure.

What companies can do to keep themselves safe from cyber criminals

A good CISO at a company would follow strict guidelines to ensure their employees and company are secure and safe from any kind of technological threat. They would not rely solely on the "short arm" of predictive knowledge, but resources and tools that are out there that they know can decrease the chances of being hit with a cyber-attack. For instance, making sure that company databases, computers, applications, and websites are secure and protected from any kind of threat. Some good protections that I would implement and that I think are beneficial to a company are the CIA Triad. This involves Confidentiality, Integrity, and Availability. These are the three core principles that will guide a company in the right direction to success instead of being vulnerable.

The idea of availability involves making sure that people can access the information from anywhere at any time. A few ways to ensure that systems are available is "...keeping hardware

up-to-date, monitoring bandwidth usage, and providing failover and disaster recovery capacity if systems go down" (Fruglinger, 2020). Also, it is important to have backups to store data in case it is lost or systems are hacked because they are not always reliable on their own. Another protection that would be beneficial for the companies' system is erasure coding. This "...combines data with parity information and then splits or "shards" it and distributes it across the storage environment" (Cloudian). Furthermore, erasure coding is a way to restore data that is lost.

With all that being said, it is important to note that availability of files in systems does not mean that everyone can access it. Also, it cannot be altered in any sort of way because that would go against the integrity and confidentiality concepts in the CIA Triad. Lastly, I feel as though every company should be incorporating all three components of the CIA Triad as a safe and secure way to protect their data.

Conclusion

Given the tools and resources out there to help with keeping a company secure, I do not think that we should change that until we can prove that the new knowledge is useful. We should always be open to learning new things because in the cybersecurity world, things are constantly changing and we need to be adaptable. However, if something works, then it should be continued. I will say that even though predictive knowledge might be useful for us in the future, it should not be relied on. It could create overall problems within the workplace and conflict between coworkers because some might have a different view of it than others. Overall, predictive knowledge helps us to think critically and realize that there is more out there for us to

know. However, predictive knowledge is unreliable in businesses because it is not a risk that some businesses are willing to take.