What are the risks and benefits ~~that~~ associated with implementing a Zero Trust Security Model?

Jaalen Cooper

Interdisciplinary Theory and Concepts 300W

Dr. Kat LeFever

jcoop042@odu.edu

December 3, 2022

Abstract

As technology continues to grow and evolve at seemingly light speed, the threats that come along with it continue to grow as well. Hackers and other threats have today become more sophisticated and continue to wreak havoc on users and companies all around the globe. They do nothing but try and destroy people's livelihoods, make businesses lose substantial amounts of money and gain unauthorized access to sensitive information that should be kept out of the public eye. That is why the cybersecurity industry has surged and why there are now many new security measures that have been created to prevent any ~~of~~ threat from reaching their goal of chaos and to mitigate the damage that said threats could do. One of the security measures that exist is the Zero Trust Security Model. The implementation of security measures, such as this security model may not only help lead new innovative security systems in cybersecurity~~,~~ but also helps to deal with the issues that the business industry goes through as well as the securing information systems in different fields, such as the healthcare field. However, it with any new security system~~s~~, there are still some issues that some may feel are too much to ignore and blindly implement. Here the disciplines of cybersecurity, healthcare, and business will use to show benefits that come with implementing such a security model as well as discussing the risks and issues associated with it as well.

Keywords: Zero Trust Security Model, cybersecurity, healthcare, business, benefits, risks

Introduction:

Cyberattacks have risen by a substantial amount in recent years. It has been reported by Forbes that as early as June, cyberattacks increased as much as 15.1% compared to the previous year. This is more than likely due to out-of-date and unequipped security systems. These security systems struggle to keep up with the increased sophistication ~~in~~ that new cyberattacks continue to have. This is proven as cybercriminals can penetrate 93% of company's networks, allowing them to gain unauthorized access to all kinds of sensitive information that can do whatever with. The weak security systems that many of these businesses and companies are going to lead to even more attacks occurring and even more sensitive information getting accessed. However, there are ways to try and deal with these attacks, even with their increased sophistication. One way is by implementing a zero-trust security model. These types of security model make it harder for attackers to get through due to a major increase in the number of zones the attackers must go to. However, you cannot simply implement a security model without understanding that it may have some risks that must be assessed. This is the reason why there is a need to evaluate both the benefits and risks equally to help provide and better and clearer ~~and~~ understanding of the security model and how it fit into the different sectors & industries that exist, such as business and healthcare.

Zero Trust Security:

As society continues to create new, innovative technology, the number of threats that lurk out there continues and grow and they at a rapid pace. Cyberattacks have not only increased in frequency, but also in sophistication. This has made it harder to prevent attacks and ~~to~~ mitigate the damage that the attacks can do. This has led to cybersecurity having many different security models and systems that were created to combat cyberattacks. However, there is one that seems to be very promising and that is the zero-trust security model. A zero-trust security model is essentially a security model that's requires all users to be constantly authenticated and authorized. It doesn't matter if the user works in the company or organization or not, they are going to be checked to ensure that they are who they say they are and that they have authorization to whatever is trying to be accessed. Zero-trust does through "the creation of zones and segments", which require constant authentication to go through. It works by terminating the connection to the network when any unusual or malicious activity is detected, which stops attackers from gaining access. By cutting the connection, you are cutting off all attack paths that the cybercriminal is using to gain unauthorized access and create chaos. A security model like this may be an important stepping stone in the cybersecurity industry that could be the beginning of an era of security models and systems that can deal with the increased sophistication of ~~the~~ today's cyberattacks. It already is being used to protect Critical National Infrastructure, or CNIs, which are essential sectors of the infrastructure, such as food and energy. This was because, "14 out of the 16…CNI sectors were targeted last year by sophisticated cyberattacks" and the utilization of the zero-trust security model was seen as a viable option to deal with the attacks. It even led to the pentagon creating an "Zero Trust office," to use the security model to deal with

this issue. This type of security model is the future of cybersecurity and is a new challenger in the cybersecurity discipline that is ready to protect the data of all types of industries, such as business and healthcare.

Healthcare:

Healthcare is a vital discipline society as it is the one that keeps the people of society in good health, extends the people's quality of life, and tries to restore people back to good health when their health has declined. It is also an industry that has seen the rapid growth and evolution of technology in it, just like cybersecurity. This technology has been used to help increase the quality of care needed to do all the things previously listed that make the discipline what it is. The discipline is also one that has the responsibility to get information and data from people and keep that info and data safe and secure. This responsibility is where you see cybersecurity and healthcare intersect as the implementation of different tools within cybersecurity is how the healthcare industry is going to secure said sensitive data & information. Furthermore, with implementing tools and different forms of security in healthcare, there must be a major focus on ensuring that the information that needs to be secure cannot be accessed by anyone that does not have authorization, which would not only include cyberattackers, but workers in healthcare as well who have not been given clearance to access certain information and/or data. This is where the thought of using zero-trust security comes in as greatly strengthens security by dealing with these new-age attacks and ensuring the information not easily accessible to attackers. However, even with the bulk in security, there are still issues that hold organizations back from utilizing the security model. The biggest are the financial burden that comes with implementing such a large security system and, "the inability to change due to the limitations of legacy systems and the medical devices" that are being used. Many of these systems and devices are out of date and

cannot be switched over to the security model. Issues like these keep complete integration of the model from occurring.

Business:

The business discipline is a complex one, but on the surface, is one where a good or service is provided, and consumers come all around to get said good or service. However, there is one aspect of the discipline that has been previously stated and that is securing important data and information. That has been hard to do in recent years, however, as businesses all around the world have been the target of many cyberattacks. The reason for this is because of years of underestimating and overlooking when it comes to the possibility of these types of attacks. However, recently the rise in cyberattacks on businesses has led to cybersecurity being an important and mandatory part of businesses and companies. Companies like IBM have created a zero-trust security model and they have even unveiled a "version of ~~[their]~~ Cloud Pak for Security that aims to help customers looking to deploy zero-trust security facilities for enterprise resource protection." Many businesses have seen the benefits that come with implementing zero-trust security and are beginning to use it more and more to protect their assets and protect the information of their users and consumers. Unfortunately, the security model can't be utilized by everyone due to reasons, such as cost and has caused many small businesses and become the main targets of cyberattacks. The Wall Street Journal reported that after an assessment by a company known as RiskRecon, it was found that "data breaches at small businesses globally jumped 152%, compared with the two prior years." This is due to these companies believing that won't get attacked because of the fact that bigger businesses exist. There's also the issue of these smaller businesses not being insured for cyber attacks, which inevitably cost them more money when an attack occurs. This is made even worse because the "pricing for small-business cyber

insurance has gone up between 10% and 15% annually since [COVID]" which means that they can't fix that vulnerability. This means that these smaller businesses need better security and luckily zero-trust security is a viable option for many companies because of the many ways it can be implemented.

Common Ground:

Conducting ~~the~~ interdisciplinary research on this topic led to a couple major findings. First, one benefit that stood out and the security model filled in each discipline was that it didn't just improve security, but it did it in a specific way. The security model filled the void that many organizations and businesses had when it came to their inside security. For instance, many healthcare organizations tend to, "focus [their] security at the perimeter [which] leaves themselves vulnerable to attacks from the inside," which causes a gaping vulnerability to inside attacks. This vulnerability led to attacks such as the infamous WannaCry ransomware attack, which was an attack on the National Healthcare System (NHS). This attacked happened, "due to the outdated Windows operating system." Since there wasn't any form of protection like zero-trust security, the worm was able to spread to the devices and cause significant damage. This can also apply to the business discipline as since many businesses, especially small businesses, do not believe that they will be attacked then they don't invest in security systems and models like zero-trust and that ends up costing them in the end. However, my research also found that the biggest risks are caused by years of underestimating the need for cybersecurity combined with rapid grow of technology, which has led many disciplines, but especially healthcare and business with outdated systems and devices that are extremely vulnerable. This has caused incompatibility from switching over from their previous devices to a zero-trust model and leads to an entire system overhaul which is expensive and not possible for all in both sectors.

Conclusion:

The zero-trust security model is a relatively new model that seems to be a promising tool to combat the ever-growing cyber attacks that occur. The enhanced security it provides is just what many in the business and healthcare sectors need to deal with this new level of sophisticated attacks due to its ability to completely shut down any access that an unauthorized attacker may gain. However, it is not perfect and there are still things, such as cost and user compatibility to consider as issues that must be dealt with. All in all, the zero-trust security model is a new and innovative part of cybersecurity that can intersects smoothly with other disciplines, such as healthcare and business and seems to be new form of defense that won't go away anytime soon.

References

Cooney, M. (2021, May 5). *IBM embraces zero trust with upgraded Cloud Pak Service*. Network World. Retrieved November 21, 2022, from https://www.networkworld.com/article/3617929/ibm-embraces-zero-trust-with-upgraded-cloud-pak-service.html

Haber, M. J. (2020). Zero Trust. In *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations* (2nd ed.). essay, Apress. Retrieved 2022, from https://learning.oreilly.com/library/view/privileged-attack-vectors/9781484259146/html/453451_2_En_22_Chapter.xhtml.

Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020, October 7). *Towards developing a secure medical image sharing system based on Zero trust principles and Blockchain technology - BMC Medical Informatics and decision making*. BioMed Central. Retrieved November 21, 2022, from https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01275-y

Notice of data security incident. Shields Health. (2022, July 25). Retrieved November 21, 2022, from https://shields.com/notice-of-data-security-incident/

Tyler, D., & Viana, T. (2021, August 16). *Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture*. MDPI. Retrieved November 21, 2022, from https://www.mdpi.com/2076-3417/11/16/7499

Patrick O'Connor, C. I. S. S. P. (2022, November 8). *The biggest cyber attacks of 2022*. BCS. Retrieved November 21, 2022, from https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/

Spinski, T. (2022, June 9). *Small businesses struggle with an increase in cyberattacks*. The Wall Street Journal. Retrieved November 21, 2022, from https://www.wsj.com/articles/small-business-cyberattacks-increase-11654540786

Brooks, C. (2022, October 12). *Alarming cyber statistics for mid-year 2022 that you need to know*. Forbes. Retrieved November 21, 2022, from https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=12327e607864

Glazemakers, K. (2022, July 7). *How zero trust can stop the catastrophic outcomes of cyberattacks on critical infrastructure*. TechNative. Retrieved November 21, 2022, from https://technative.io/how-zero-trust-can-stop-the-catastrophic-outcomes-of-cyberattacks-on-critical-infrastructure/