Interdisciplinary Term Paper

Thomas Roeseler

IDS 300W

Dr. Peter Baker

1 April 2024

How does the implementation of effective cybersecurity policies and advanced cybersecurity technologies influence individuals' online privacy actions and behaviors on the Internet when these policies and technologies are designed to prevent and mitigate certain threats?

Cybersecurity has rapidly become a very popular and very important issue in today's world. It has become increasingly important as technology has rapidly advanced in the world. There are many areas and many industries in the world that have been affected by cybersecurity and those industries have had to invest majorly in cybersecurity to make sure they can protect their data the best they can. Because cybersecurity is still for the most part a new issue to the world and governments around the world, there aren't very many policies or laws that surround it. A good amount of the people who engage in cybercrime are people who believe they will not get caught because it is harder to be caught when committing a crime online because they aren't leaving a trace behind and they could be committing a crime in one country, but administering it in another one.

Cybersecurity is seen everywhere in today's world. It is needed in almost anything you can think of in the world because of how fast technology has advanced in recent years. Implementing cybersecurity policies and practices can be a tough task. In the government, you have to deal with the process of passing laws and approvals and everything around that. In an organization or company, they may not have all the resources or finances they need to implement a certain policy that could benefit them. Implementing policies or practices can benefit everyone involved because it can help reduce their risk of being a victim of a cyber-attack and can involve training and awareness for employees or anyone who is a part of that policy. A reason that policies are important for companies is so employees are aware of certain techniques that an attacker may use, so they can recognize what the attacker is doing and not let it happen. Another good reason is that if an attack does occur, there can be policies that deal with reaction and recovery to attacks, so employees know what to do in certain situations.

A good example of a government policy in place is Europe's General Data Protection Regulation(GDPR). This can be used as a baseline for what governments of other countries can/should do in order to help ensure data protection of consumers. This also shouldn't be the only policy in place because there should be some that are directed more towards individuals and ones that can deal with the cyber criminals. What some people don't realize is how much damage cyber-attacks can cause, whether it is financially or physically. There have been school systems, hospitals, water treatment facilities, and other critical infrastructure that have been victims of cyber-attacks. This shows how much damage attacks can cause. For these attacks, the attackers may use ransomware which means they won't give access to their computer/data back to the victim until they have paid a certain amount requested by the attacker.

Some people don't like the idea of implementing cybersecurity policies because they don't know much at all about cybersecurity and aren't sure how it can benefit them. People who have had experience with cyber-attacks and have been exposed to them are more likely to like the idea of implementing cybersecurity policies. Because cybersecurity is still very new to today's world, not everyone is familiar with it and how important it is which is why they may not like the idea of implementing a policy as such. A good goal to make is to find out how we can improve cybersecurity policies and technologies and how they can make a positive impact on actions around digital privacy. Digital privacy is a very important thing to people because everyone deserves a right to privacy and there are some cybersecurity concerns that can negatively affect that right and at times will violate that right.

Cybersecurity is an important topic in the world today because of how far it can go. One example of showing how damaging cyber attacks can be on the well-being of people is when a water treatment facility was poisoned by a hacker. If this wasn't caught right away, this could have affected many people. It was an attack on one in Miami, Florida around the time the Super Bowl was being played there. So not only does Miami have a big population, but there were also a lot of visitors in the city at that time because of the Super Bowl. The reason cybersecurity has

rapidly become an important issue in today's world is because of the rapid digitalization of pretty much everything. Tons of industries rely on technology and the Internet for data storage and basic duties that they have to do for them to operate. Because these industries are relying on technology and the Internet, they have to face the problems that cybersecurity brings. Cybersecurity has created the need for more jobs and for companies to have to work around those problems by finding ways to increase security and limit vulnerabilities.

The reason this cybersecurity research question can be studied interdisciplinarily is because it deals with cybersecurity policies and the public. Because they're cybersecurity policies and deal with the public, you can use multiple disciplinary views with this topic. Political science, sociology, and economics are three perfect examples of disciplines that can be used to study this research question. Creating effective policies for a cybersecurity concern can be very time-costly, but in the long run, it could be very beneficial to many people and organizations. Spending money and investing in cybersecurity as a business is a smart thing to do and should be done by everyone because if money is not spent on it, it could end up costing you so much more because recovery from an attack can cost so much financially and even more than you realize because you could lose business because of it as a result if trust is lost. Cybersecurity if not cared for can cause lots of damage including potential damage to the economy if attacks similar to a cyber-attack on the Colonial Pipeline which provides gas for almost all of the East Coast of the United States. Not only does the government and organizations need to care about cybersecurity, but individuals as well. There are many cases of individuals falling victim to cyber-attacks and those individuals could have either lost their data or lost money or had to deal with lots of things because of the potential for stolen credit card information and maybe even identity theft.

From an economics perspective, it is best to invest money into cybersecurity before you end up having to spend more dealing with the repercussions of a cyber-attack. It is looked at as similar to an insurance policy because you are insuring yourself to have a better chance of

survival and recovery if someone were to try to attack your systems. The economics and political science perspectives share the idea that policies are important, but economics really stresses the financial side to a policy and political science cares strictly about getting a policy done. “We argue that public support for governmental cybersecurity measures rises as a result of exposure to different forms of cyberattacks,” (Snider et al., 2021). Political science and sociology perspectives both care about what the public thinks and tries to benefit the public the most they can when trying to create policies. This quote shows again why some people may not be for creating policies surrounding cybersecurity because they haven’t been exposed to cyber-attacks and people who have are more likely to support the government with creating cyber policies.

Ransomware is something that there should be certain policies that give the victim a plan or assistance because most victims won’t be able to pay and even if they do, there's no promise that they get their information back and no promise that their information isn’t be used by other people already. “Ransomware is malicious software that prevents a user from accessing the device—usually through unbreakable encryption—until a ransom is paid to the attacker,” (Paquet-Clouston et al., 2019). Ransomware can be seen through an interdisciplinary perspective as a headache because it involves paying a ransom and is not what anyone wants to do and is an extremely difficult issue to solve without paying a ransom. Ransomware is something that can affect anyone because a victim can be a company that stores data and your data could be stolen by them. Another way it can affect anyone is because anyone can be the victim, it isn’t only companies, it happens to individuals as well. A lot of people don’t worry about their cybersecurity practices because they don’t think they’ll ever be a victim of an attack, but when it happens, they realize they should have used better cybersecurity practices and then begin worrying about cybersecurity.

Companies that do contracting work for the government are required to follow the NIST framework which is a cybersecurity framework that is used to help better manage and reduce

cybersecurity risks. The NIST framework has five important components. Those components are identify, protect, detect, respond, and recover. Each of these components have plans for whatever happens and what to do in any given situation. “NIST clearly recommends that organizations should maximize the impact of the dollars spent on their cybersecurity investments based on cost–benefit analysis,” (Gordon et al., 2020). The NIST framework also tells organizations how to prepare and reduce risks before anything happens, so there is a smaller chance that something happens. “When President Trump issued EO 13800, the NIST Cybersecurity Framework became the law of the land for US federal government agencies and firms wishing to do business with these agencies,” (Gordon et al., 2020). This shows that the government will implement cybersecurity policies, but this policy doesn’t benefit everyone and is more directed towards companies that work with the government. Either this policy or another policy should be directed at every company in general, so there is an accessible resource to many companies, so they can reduce their cybersecurity risks and manage cybersecurity better as it becomes increasingly important for their company. The NIST framework or something new should also include what happens to the attackers if they get caught because then that could potentially turn away potential attackers.

The sociology disciplinary perspective firmly believes that if the consequences are stated before a potential attacker does an attack, then it could turn them away from pulling through with the attack. “The public has grown increasingly sensitive to the importance of online privacy, and is keenly aware of the ethical, political, legal, and rights-based dilemmas that revolve around government monitoring of online activity and communications,” (Snider et al., 2021). With more and more people learning about cybersecurity and becoming interested in the issue at hand, the more likely there will be more support for government involvement with the issue. There will likely be more policies created and other things done about cybersecurity from the government. Using an interdisciplinary perspective and because cybersecurity is becoming increasingly important in the world, it is likely that more people will support the government

implementing new policies to help manage cybersecurity because if nothing is done about it, there can be major consequences because of it. With all of the things that are already being affected by cyber-attacks, if nothing is done, there will only be more attacks and they won't get any better. From a political science and economics perspective, the government may use cybersecurity as an opportunity to try to benefit the economy and the government itself. General Strain Theory (GST) is a sociological theory that can be linked to online behavior because people who are treated negatively are more likely to act negatively because of their emotions and a perfect way for people to do that is to go online and do it behind a screen instead of to someone's face.

One important cybersecurity practice for companies and organizations is to train your employees on cybersecurity because it is important they know how to deal with certain situations and they know what good cybersecurity hygiene is, so they can do it. "Even organizations well versed in cybersecurity could not easily predict how likely their employees would carry out the expected cybersecurity behaviors. Even more challenging would have been having a clear view of the personal challenges that employees might have encountered when attempting to carry out effective cybersecurity practices while simultaneously dealing with a highly stressful event," (Whitty et al., 2024). This piece from Monica Whitty is very true, organizations won't know how their employees are going to react in every situation, even when they're supposed to do something specific because when they're under pressure and in the moment, they might not act the correct way they're supposed to. This justifies why users are considered the weakest link to a system. Users are always considered the weakest link of a system because you never know for sure how a user is going to react while everything else in your system is set to do something specific and doesn't change unless told to by a user. Users are also considered the weakest link because they are the most vulnerable because they have to deal with outside people and are most likely to mess up because they can get tricked into

doing something wrong or give information out to the wrong people if they were to be the target of a social engineering attempt.

Financial institutions can be major targets for cybercriminals because not only do they sometimes use ransomware to potentially get a ransom paid, but they can also steal important financial and personal information from all customers because their data is stored by the financial institution and then those attackers can use that information to their advantage to potentially gain even more money. “The digital assets of financial institutions are also attacked by cybercriminals who attempt to infiltrate their computer systems and steal valuable information,” (Dupont, 2019). Integrating all of the disciplines together for this issue brings in the insights of using greed to try to get more money for themselves by potentially harming other people and making those people have to work hard to recover from that attack if they were greatly affected by it. There have been numerous attacks where victims had to deal with the consequences of the attack for years after because they had the worry and stress about potentially getting their identity stolen and lines of credit put in their name.

Cost-benefit analysis is one of the economics disciplinary perspectives major insights. The economics discipline stresses it so much because companies should be spending money on cybersecurity because if money is not spent, there could be major consequences that end up costing lots of business and even more money than the cost of paying to protect from these attacks. The NIST framework also stresses the importance of using cost-benefit analysis for cybersecurity issues. The political science disciplinary perspective agrees with implementing a cost-benefit analysis for companies because it is beneficial to spend money on cybersecurity rather than spending lots of time and money on recovery from a cybersecurity related problem. The sociological perspective for this topic isn’t as involved as the other two disciplinary perspectives because the sociological perspective focuses on people themselves more than frameworks and money, but the sociological perspective believes it is a good idea to try to

benefit the people as much as possible and if this will benefit them, then they believe its a good idea.

Because cybersecurity has become such an important and critical issue in the world today, there needs to be actions taken to ensure that we are limiting cybersecurity risks and doing our best to protect important information from people who do not need access to it. Actions that can be taken are to increase spending on cybersecurity infrastructure and to create policies and plans that benefit everyone, whether it is the government, a company or organization, or an individual. All three disciplines included in this interdisciplinary research process were able to share insights to help solve the question. Political Science, Economics, and Sociology all came together to answer the question. Implementing policies can be very beneficial to everyone because it could potentially turn away some potential cybercriminals if they know what their consequences could be and everyone would have better access to plans and resources if they were to be a victim of a cyber-attack.

References

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. Journal of Cybersecurity, 5(1). https://doi.org/10.1093/cybsec/tyz013

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. Journal of Cybersecurity, 6(1). https://doi.org/10.1093/cybsec/tyaa005

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. Journal of Cybersecurity, 5(1). https://doi.org/10.1093/cybsec/tyz003

Snider, K. L., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. Journal of Cybersecurity, 7(1). https://doi.org/10.1093/cybsec/tyab019

Whitty, M. T., Moustafa, N., & Grobler, M. (2024). Cybersecurity when working from home during COVID-19: Considering the human factors. Journal of Cybersecurity, 10(1). https://doi.org/10.1093/cybsec/tyae001