Group ID: **10-07**

Future Trends Report

Based on Analysis of the Team's Chosen Community / Organisation in Mid-Term and Final Evaluation

Community / Organisation Studied: **Grocery Delivery / Sheng Siong**

STEP 1. Identify Challenges

Challenge #1

Based on our survey of 65 working adults, respondents showed concern over the privacy of their data, with 15% of them being worried about the prevalent threat of data mining, where grocery delivery services make use of data mining to suggest items for users to purchase. These respondents shared that while using a grocery delivery service, they have been suggested items to purchase based on what they have already purchased. For grocery delivery consumers, the increasing prevalence of data mining used to suggest products is more than just annoying. (Observation)

This could be problematic in 2030 as it can cause a significant percentage of potential consumers of such services to be discouraged from purchasing suggested products, or from using the service altogether. In the near future, when the number of grocery delivery consumers significantly increases, (Problem) suggesting products through data mining may lead to a significant decrease in product sales for the grocery company, reducing their net profits. (Greater Consequence)

According to Lisa Barnard, assistant professor of integrated marketing communications at Ithaca College, individually targeted advertisements "account for a 5 percent reduction in intent to purchase an advertised product." Essentially, when a consumer is suggested a product to purchase, he/she is 5% less likely to purchase that particular product. Similarly, according to a September 2013 study from data privacy management company Truste, "1 of 3 Internet users say they have stopped using a company's website or have stopped doing business with a company altogether because of privacy concerns." This highlights that when consumers are aware that their data is being used by the company, they may choose to not purchase the product or not use the service at all. Though the research is not specifically targeted at grocery delivery websites, the research is still applicable as the data mining is carried out in a similar fashion. (Research)

Challenge #2

Based on our survey of 65 working adults, 60% of survey respondents indicated that it may be unnecessary for human staff to be present in the future as the advancement of technology in grocery delivery services eliminates the need for cashiers and supermarket staff. There has been an increasing trend in the use of automation in the grocery industry which can directly affect that of the grocery delivery industry. (Observation)

This could be problematic in 2030 as it can lead to a significant portion of workers in the grocery industry becoming replaced by automated machines. This can be in the form of robots used to stock factories, pack groceries, deliver groceries, and many more. (Problem)

As a result, this could, in the long run, significantly decrease the need for human workers in the industry and cause a rising trend in unemployment. (Larger Consequence)

According to Forbes' Bernard Marr, between 35 and 50 percent of the jobs that exist today are at risk of being lost to automation. "Repetitive, blue collar type jobs might be first, but even professionals — including paralegals, diagnosticians, and customer service representatives — will be at risk." Similarly, according to "The Future of Jobs", an insight report by the World Economic Forum in January 2016, who surveyed chief human resources officers and senior talent executives of employers who represent 15 of the world's largest economies, accounting for 65 percent of the global workforce, it is likely that we will see "massive labour substitution and displacement of jobs" in the next few years due to the emergence of advancements in technology. These findings do support our respondents' opinions that automation is likely to replace a significant number of jobs in the grocery delivery industry. (Research)

Challenge #3

Based on our survey of 65 working adults, 60% of our survey respondents indicated that data leaks are an issue of concern with the use of grocery delivery applications . Current apps and websites require users to input their personal information such as their home address, contact number, email, and even credit card number. Though such information is not intentionally disclosed to anyone but the company, there is a possibility that the information may be compromised unknowingly. (Observation)

This could become problematic in 2030 because if a history of data leaks accumulates, there may be a decline in public trust towards such delivery services, causing consumers to be skeptical of the safety of such services. (Problem)

As a result, total usage of such grocery delivery services and its frequency may drop, reducing individual company profits, which may cause the industry to become unsustainable. (Greater Consequence)

The International Data Corporation believes that by 2020, more than 1.5 billion people, or roughly 1/4 of the world's population, will be affected by data breaches. "While we have already felt the effect of massive breaches that have exposed the credentials for hundreds of millions of people, the IT impact will be felt more keenly in the coming years." Even in Singapore, the number of data breaches has increased. According to the Cyber Security Agency of Singapore, "378 business email impersonation scams were recorded in 2018, an increase from 332 in 2017. This led to businesses in Singapore suffering close to S$58 million (US$42 million) in losses, an increase of about 31 per cent from the previous year." This evidently shows that the rise in the number of data leaks and breaches in Singapore is a legitimate concern for grocery delivery consumers in Singapore as there is a reasonable chance that it could happen to them while they are using such services. There is thus a possibility that consumers will be turned away from using such services due to skepticism over their data security. (Research)

Challenge #4

Based on our survey of 65 working adults, more than 50% of survey respondents indicated food safety as a potential problem of grocery delivery services. This is likely to be due to the fact that during the process of grocery delivery, groceries are transported from place to place before reaching their final destination, which increases the risk of groceries being contaminated. This is of great concern for food products delivered through grocery delivery services. (Observation)

This problem would be more widespread with the increase in grocery companies having grocery delivery services by the year 2030, as people will be deterred from using grocery delivery services with the worry that the food they consume is not safe. If proper measures are not put into place, companies like Sheng Siong that own such services may face problems with the law, as the safety of consumers should be of utmost priority.(Problem)

As a result, this will decrease the number of users of such services, possibly leading to the industry being unsustainable. (Greater Consequence)

According to a Rutgers University study, “Researchers interviewed more than 1,000 meal service customers and ordered 169 meal kit packages themselves. They reported that 47 percent of the food items arrived with surface temperatures above 40 degrees (fahrenheit), which falls in the USDA's "danger zone"-food that reaches a temperature between 40 and 140 degrees. Bacteria grows most rapidly in that range.” The study showed that food delivery services, specifically those in New Jersey, may deliver food that is dangerous for consumers to consume. Though these numbers are likely to be less severe in Singapore due to stricter laws, there is still every possibility that grocery delivery service consumers in Singapore will face similar problems. Also, according to Susan Bell of the Singapore Business Review, “Most consumers don’t know the temperatures at which their foods should be maintained for safe consumption and aren’t testing proteins delivered to their houses. And as there are no temperature regulations for food deliveries, this challenge lies with the individual players in the industry, knowing that a wrong step not only puts consumers at risk of illness, but it also poses a risk to the reputation of the brand and potentially contributes to the larger issue of food waste.” From the research above, consumers of grocery delivery services in Singapore should be more concerned about the safety of food delivered to their homes as it is easily overlooked but can put the consumer in significant danger. (Research)

Challenge #5

Based on our survey of 65 working adults, 40 of 65 survey respondents indicated that the lack of interaction through the use of online grocery delivery services could be a potential problem as an increasing number of jobs are being replaced by automation. For example, there have been speculations that in the near future, delivery drivers could be replaced by drones which deliver groceries to the users’ doorsteps. (Observation)

The result of this could be that there would be less human-to-human interaction as users will no longer be able to communicate with people from the grocery delivery industry, who may be replaced by intelligent services like chatbots. This could eventually lead to various social and psychological issues with decreasing communication between people.(Problem)

There is also the possibility that this decrease is face-to-face interaction will discourage people from using such services due to worries about the integrity of automated services. (Greater Consequence)

According to Forbes' Carol Goman, "While digital communication is often the most convenient method, face-to-face interaction is still by far the most powerful way to achieve business goals. Having a personal connection builds trust and minimizes misinterpretation and misunderstanding. With no physical cues, facial expressions/gestures, or the ability to retract immediately, the risk of disconnection, miscommunication, and conflict is heightened." People can be less inclined to use services that lack face-to-face interaction because they fear the risks involved, as the research shows.

Similarly, Sherry Turkle, professor of Social Studies of Science and Technology at the Massachusetts Institute of Technology, warns that when we first "speak through machines, [we] forget how essential face-to-face conversation is to our relationships, our creativity, and our capacity for empathy", but then "we take a further step and speak not just through machines but to machines." The long-term issue involved with the lack of face-to-face, human interaction is that people will become more like the machines they interact with - emotionless, cold, and automatic. (Research)

STEP 2. Craft the Underlying Problem

Incorporating Challenge(s) # **1, 2, 3**

Underlying Problem

Given that it is necessary for users to share their personal information with grocery delivery companies and data-mining is prevalent, it appears that the database of grocery delivery companies may be vulnerable to hackers who want to access the users' data. (Condition Phrase) How might we increase public confidence in grocery delivery services (Key Verb Phrase) so as to attract more consumers for such services (Purpose) in Singapore in the year 2030 and beyond? (Future Scene Parameters)

STEP 3. Produce Solution Ideas

Generate solution ideas to the Underlying Problem in Step 2. Choose the 5 most effective solutions and write the elaborated ideas in the space provided. Include applicable research with appropriate in-text citations.

Solution #1

We, the Cyber Security Agency (CSA), will enforce that grocery delivery companies must constantly review their cybersecurity structure and keep up with the highest standards of cybersecurity measures such as data encryption, network firewalls and intrusion prevention systems to keep user data safe from threats of hackers accessing the data. This will give potential consumers of grocery delivery companies the confidence that their personal information is safe and encourages them to start using such services.

According to Kris Lahiri of internet software company Egnyte, "The keys to preventing data leakage are manifold. Identifying critical data, monitoring access and activity with a combination of DLP or DAM solutions, utilizing encryption, retaining control of your network and using endpoint security measures all equal a fine-tuned and customizable program to protect your entire organization." There are many different aspects of internet security that companies need to look into to ensure their whole security structure is effective.

Also, based on the Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database, "It is imperative for organisations to give sufficient prominence to technology when formulating and implementing an overall cybersecurity strategy. Of course, it is important that the correct governance structure and policies are in place – technology cannot replace those elements. However, no matter how sophisticated, no paper document or process will thwart an attack until you have strong IT security technologies in place."

Solution #2

We, the Ministry of Communications and Information, will develop a "Safe With Us" cybersecurity campaign to release posters and videos on a weekly basis on social media platforms such as Instagram and Youtube. These posters and videos will feature how grocery delivery companies and other companies who have access to user data keep this data safe from threats such as hacking. This will help the community to recognise that efforts are being made to protect user data and encourages them to start using grocery delivery services without the fear of their data being leaked or stolen.

Singaporean Technology website TechGoondu claims that "Only 23 per cent of Singapore consumers believe that their personal data will be treated in a trustworthy manner by organisations offering digital services...Half of the Singapore respondents would either switch to another organisation, reduce the usage (43 per cent) of the digital service or stop using (38 per cent) the digital service altogether." The existing mindsets and attitudes towards the treatment of personal data by companies are clearly not very positive.

Additionally, Andrus Ansip, the European Commission's vice-president for the digital single market said in a statement that "only three in ten Europeans have heard of all their new data rights...and for companies, their customers' trust is hard currency and this trust starts with the customers' understanding of, and confidence in, privacy settings.” He believes that customer data protection begins with the customers. Thus, it is important that grocery delivery consumers are first made aware of how their data is and should be treated.

Solution #3

We, the Ministry of Communications and Information, will form a partnership with all grocery delivery companies through the Cyber Security Authority (CSA). The CSA will facilitate threat intelligence sharing, and strengthen partnerships with Internet Service Providers. Behavioural analytics will be applied to the industry’s servers, allowing all companies in the industry to work together towards collective cybersecurity. This will increase public confidence that grocery delivery companies will always have a high standard of data security and the public will be more inclined to use them.

Lior Div of the International Data Group (IDG) notes that “companies need help if they’re going to face adversaries who use nation-state attack techniques. And both the public and private sectors would benefit greatly from collaborating on information security. The government would learn about the unique issues the private sector faces, such as dealing with a remote workforce that doesn’t necessarily follow corporate security policies or the shortage of security talent. The private sector gains access to detailed threat information and help figuring out how to harden their networks.” This details the win-win situation that such partnerships will put all parties in.

GCN Technology’s Levi Gundert also states that “this unique public-private partnership leverages private threat researchers’ deep knowledge of the cyber underground, including nation-states, and provides government investigators with information and perspective that can make a critical difference in solving cyber whodunnits and stopping future attacks.” As can be seen, creating partnerships between the public and private sectors can only increase the collective cybersecurity of the industry.

Solution #4

We, the Ministry of Communications and Information (MCI), will create more detailed incident response plans to deal with data breaches. This ensures that all possible data breaches of grocery delivery companies are resolved or counteracted within the minimum possible time and with the least effect on their operations, employees and customers. This will help grocery delivery companies deal better with these breaches and reduce the chances of it happening again. This will increase public confidence in the safety of grocery delivery services, hence they will be more inclined to use them.

The Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database writes that “an effective incident response plan can reduce the extent and impact of an attack by identifying its source and shutting it down quickly. In the event of a cyber attack, warnings may come at short notice and the pace at which an attack escalates may be rapid. The correlation between the effectiveness of an incident response plan and recovery is evident, with organisations recovering from attacks proportionally to their incident response preparedness.” The situation encountered by Singhealth could have been made less damaging if the incident response plans set up were detailed and effective.

According to James Gaskin from technology blog ChannelProNetwork, “having an incident response plan prevents knee-jerk reactions; protects digital assets according to their value; ensures the confidentiality, integrity, and availability of data; and preserves operational continuity. It also minimizes impacts and reputational harm, and expedites detection, mitigation, remediation, and recovery.” The benefits of such response plans are explicit and cost-effective.

Solution #5

We, the Committee for Ethical Hacking, will work with the Ministry of Communications of Information (MCI), to conduct ethical hacks on grocery delivery companies. This white-hat hacking is done regularly in a lawful and legitimate manner to assess the security of computer systems of these companies. This will allow companies to know and fix any weaknesses and vulnerabilities that they have, hence reducing the chances of them getting attacked by malicious hackers. This will allow the public to feel that their confidential information is more safely kept, hence they will use grocery delivery services more often.

An article published in 2017 by India Today states that “cyber crimes are becoming more common and attackers more sophisticated with rogue nation-states and terrorist organisations funding criminals to breach security networks either to extort hefty ransoms or compromise national security features. Businesses are faced with the challenge of dealing with complex security requirements that need to be updated as per changing hacking tactics, handling hidden vulnerabilities and evolving technologies. Ethical hacking firms with specially trained professionals come to the rescue of businesses while ensuring effectiveness of service and confidentiality.” However, ethical hacking has to be done explicitly and with a clear intention.

American cybersecurity website StaySafeOnline adds that “it is essential that ethical hacking assessments are as transparent as possible. An ethical hacker will always share findings and offer remediation advice to ensure that vulnerabilities are reported and addressed. They should be contactable throughout engagements and provide clear written reports to summarize findings and recommendations.” In essence, ethical hackers must have clear goals and intentions and must make their results fully transparent for the companies to improve on.

Group ID: **10-07**

STEP 4a. Select Criteria

Generate criteria to determine which solution idea does the best job of solving your Underlying Problem and/or addressing the Future Scene situation. Select the 5 most important criteria for measuring solution ideas and write them in the spaces provided.

Criteria #1

Which solution will be the **fastest to implement** for Sheng Siong so as to increase public confidence in its services as quickly as possible?

Criteria #2

Which solution has the **greatest positive impact** for Sheng Siong's database security so as to ensure public confidence in its services?

Criteria #3

Which solution will require the **least resources** for Sheng Siong to implement so as to allow Sheng Siong to further develop its services?

Criteria #4

Which solution will be the **most sustainable** for Sheng Siong so as to benefit both Sheng Siong and customers in the long term?

Criteria #5

Which solution will be the **most appealing** to Sheng Siong's customers so as to attract more customers for such services as effectively as possible?

STEP 4b. Apply Criteria

List the solution ideas from Step 3 on the grid. Use each criterion to rank the solutions on a scale from 1 (poorest) to 5 (best). The weighting for one important criterion may be doubled if necessary.

Step 3 Sol'n #	**Solution Idea**	**Criteria**					**Total**
		1	**2**	**3**	**4**	**5**	
#1	**Up-to-Date Cybersecurity**	1	5	3	4	4	**17**
#2	**Government Campaigns**	2	3	1	2	5	**14**
#3	**Government Partnership**	5	4	5	5	3	**22**
#4	**Incident Response Plans**	4	2	4	3	2	**15**
#5	**Ethical Hacking**	3	1	2	1	1	**8**

STEP 5. Develop an Action Plan and Evaluate its Feasibility

Develop your top-scoring solution idea into an Action Plan. Thoroughly explain how the Underlying Problem is solved, how the plan will be implemented, and how the community / organisation will be affected. Explain how this Action Plan is feasible with secondary research consulted, preferably also with primary research (feedback from chosen community / organization)

Action Plan

Note: This action plan was formulated with our best solution but also incorporates Solutions 1 and 4 as well, after survey respondents of our survey indicated that infrastructure, appropriate action plans and working towards collective security were equally important in ensuring the safety of user data and it is necessary for all components to be present for our action plan to be effective.

We, the Ministry of Communications and Information (MCI), working with the Cyber Security Agency (CSA), will form a partnership with various grocery delivery companies by the year 2020. By 2022, all past incidents related to data issues of grocery delivery service users should have been reviewed and appropriate action plans to similar incidents should be formed with the use of appropriate AI technologies and data analytics. By 2023, grocery delivery companies are to begin making plans for a new multi-layered security system (similar to that of Virtual Privacy Networks but on a larger scale) to keep user data safe, with advice from IT professionals. By 2026, the new security system will be launched for all grocery delivery companies.

From then on, grocery delivery companies will be kept in check and the government will ensure that the companies constantly review their cyber security structure and keep up with the highest standards of cybersecurity measures such as data encryption, network firewalls and physical intrusion prevention systems and protocols to keep user data safe from threats of hackers. By ensuring that grocery delivery companies are taking concrete measures towards protecting public data from hackers as well as drones used to deliver groceries to users, we can increase overall public confidence in such delivery services, such that the public will be more inclined to use them.

We will be assisted by IT companies of varying scales that can provide the required expertise and software resources to enhance the security of existing systems, carry out structural security reviews and provide constructive input during the formulation of individual action plans and protocols. These companies will be incentivised to help us as they would be recognised as partners of the government as well, improving their company image.

We have to acknowledge that there will be some potential resistors to this plan, one example is drivers who may find the commercial use of drones unsafe. With a large number of drones flying above and across roads, drivers may fear that the drones may lose control and crash into vehicles, causing a traffic hazard. Thus, we will ensure that during the implementation of such technology by grocery delivery companies, the safeguarding of drones or other forms of technology used to deliver groceries to grocery delivery users will also be taken into consideration.

Infrastructure put into place will ensure that all drones are tracked and are following the correct route with the use of AI technology, and that service providers will be required to set specific paths for drones that minimise disruption to drivers, and minimise the impact that would be caused by a potential accident. The creation of this security system will follow the same timeline as the security system for user data, and is expected to be launched by 2034. This system will also ensure that in the case that a drone goes off-course, relevant staff will be notified and the drone would be halted and manual control would be given to a staff member while the AI system is checked by IT personnel.

Another obstacle to overcome in this plan is acquiring the funding required to carry out this action plan. As of now, there is a significant percentage of people who do not use grocery delivery services often, and thus the Singapore government may not find a need to fund these processes as the grocery delivery industry does not appear to be a significant contributor to Singapore's economy. However, the grocery delivery industry is expected to grow rapidly, especially as different sectors of Singapore become more digitalised. Thus, by carrying out this plan of improving public confidence in services via cybersecurity, not only will the grocery delivery industry benefit from enhanced growth, but similar methods can be transferred to other industries and companies as well.

Therefore, we, the Ministry of Communications and Information, will lobby to the government to receive funds for the implementation of our action plan.

Evaluation of Action Plan

Primary Evaluation

After gathering feedback from the respondents of our survey, we have concluded that our action plan is effective in addressing the Underlying Problem as it improves cybersecurity within Grocery delivery companies. [Data found in Appendix A on Page 13] 61.1% of our survey respondents agreed that our action plan which involves IT companies will effectively counter the act of data mining and occurence of data leaks and 55.6% of survey respondents agreed that this action plan can maintain a high standard of cybersecurity in such companies for a long period of time. Furthermore, our action plan achieves its purpose by increasing public confidence in grocery delivery services, as two-thirds of respondents believe that our action plan will improve public perception of grocery delivery services as respondents generally felt that consumers would have confidence while shopping. It has also encouraged the public towards using grocery delivery services as two-thirds of respondents would be encouraged to start using grocery delivery services after our action plan has been implemented and almost half of the respondents agreed that they would use such services more frequently.

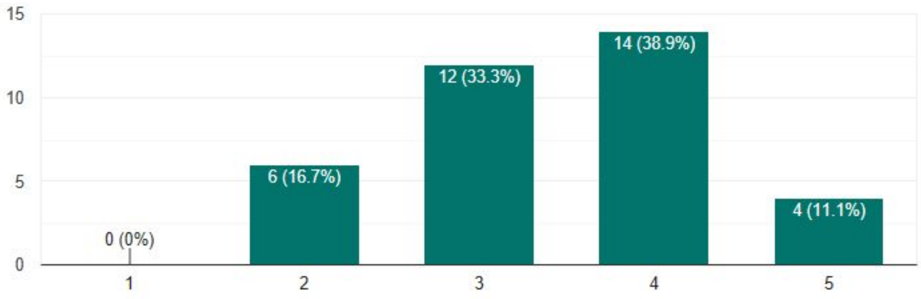
However, our action plan still has flaws. Many survey respondents felt that our action plan would be able to minimise the possibilities of data leaks but would not fully protect them from threats. Thus, several respondents were still unwilling to share their personal information with grocery delivery companies. This fear may be due to the fact that our process of creating protocols for companies was not done in detail. Thus, our action plan can be improved to focus on ensuring that clear, up to date protocols are run through with staff on a regular basis to prepare them in the case of a data leak, to put consumers at ease that their data will be protected.

Furthermore, one-third of respondents were neutral over whether there would be public resistance to this action plan, indicating that the effectiveness of our action plan could be undermined. 80% of respondents felt that this was due to a lack of contextual knowledge of the existing issue, leading to the public not seeing the need for such an action plan. Thus, to maximise the impact of our action plan on the public to achieve our purpose, we should publish videos to increase awareness on the current problem of data leaks and the efforts done by our action plan, in order to convince the public on the effectiveness of our action plan.

Appendix A

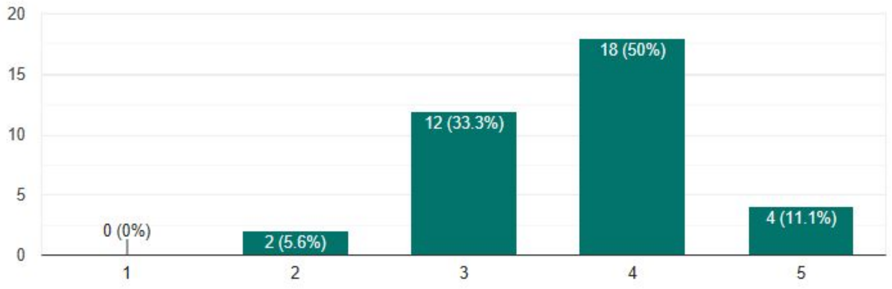
Do you think our action plan can be reasonably undertaken by the grocery delivery industry? (In terms of manpower and financial resources)

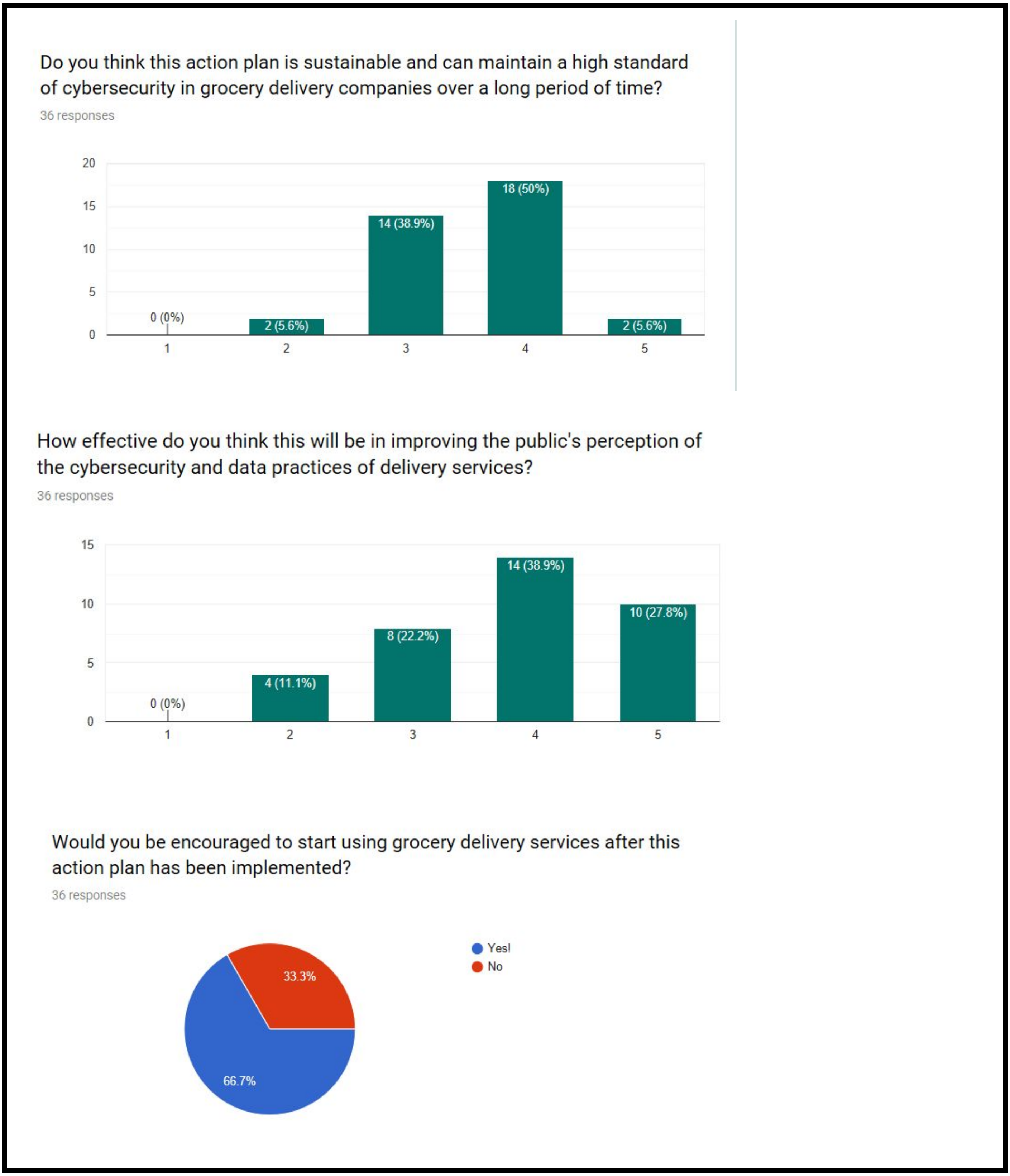
36 responses



How effective is our action plan in countering the acts of data mining and the occurrence of data leaks?

36 responses





Do you think this action plan is sustainable and can maintain a high standard of cybersecurity in grocery delivery companies over a long period of time?

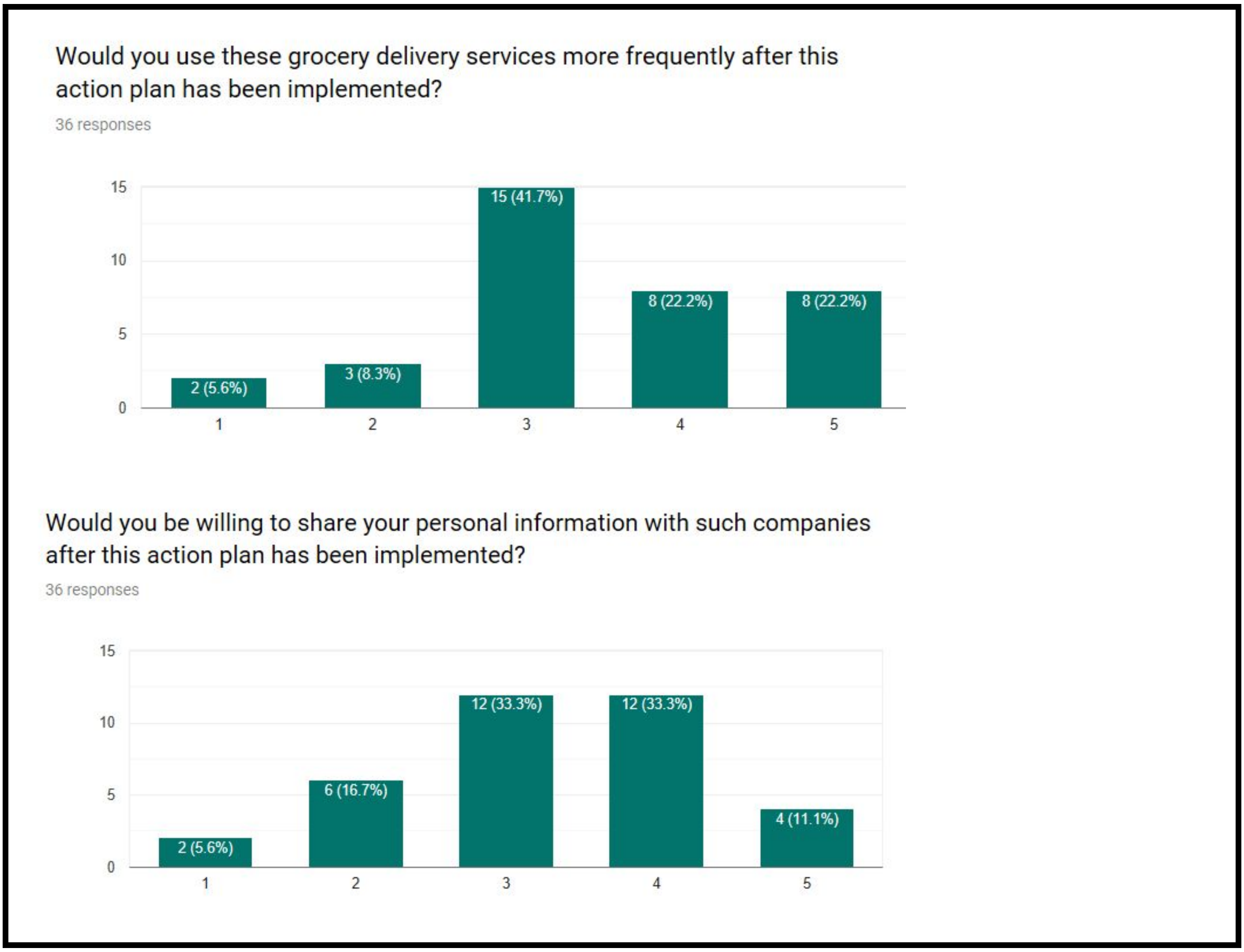
36 responses

How effective do you think this will be in improving the public's perception of the cybersecurity and data practices of delivery services?

36 responses

Would you be encouraged to start using grocery delivery services after this action plan has been implemented?

36 responses

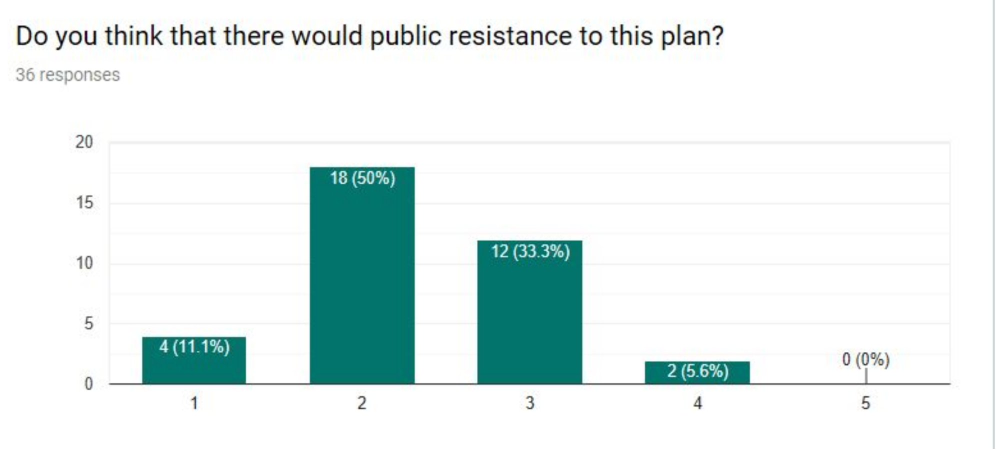


Would you use these grocery delivery services more frequently after this action plan has been implemented?

36 responses

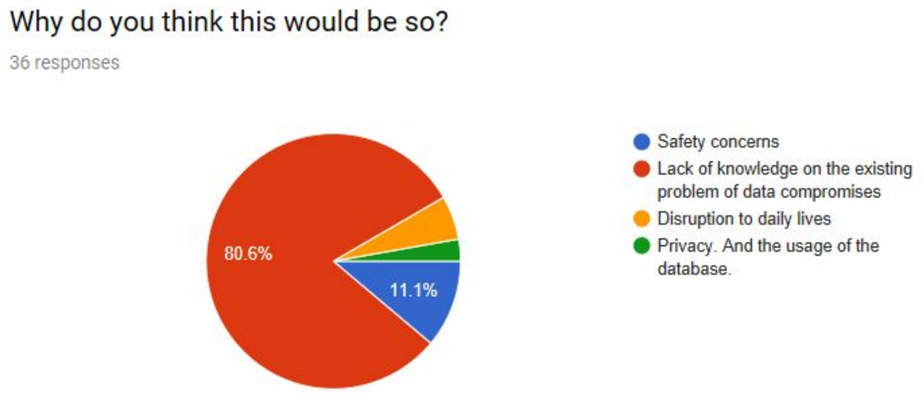
Would you be willing to share your personal information with such companies after this action plan has been implemented?

36 responses



Do you think that there would public resistance to this plan?

36 responses



Why do you think this would be so?

36 responses

Secondary Research

Based on secondary research we conducted, our ideas were supported by our research as well.
The Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database mentions that "It is imperative for organisations to give sufficient prominence to technology when formulating and implementing an overall cybersecurity strategy [...] no matter how sophisticated, no paper document or process will thwart an attack until you have strong IT security technologies in place." This supports our stand that the focus on creation of protocols and individual action plans in the case of a cyber attack is justified. Furthermore, this emphasizes the need for the Ministry of Communications and Information to ensure that there are up to date and adequate cybersecurity measures in place across the industry to protect user data from threats.

Lior Div of the International Data Group also mentions that "companies need help if they're going to face adversaries who use nation-state attack techniques. And both the public and private sectors would benefit greatly from collaborating on information security. The government would learn about the unique issues the private sector faces, such as dealing with a remote workforce that doesn't necessarily follow corporate security policies or the shortage of security talent. The private sector gains access to detailed threat information and help figuring out how to harden their networks." This shows that the presence of an overhead Ministry to head the cybersecurity sector in the grocery delivery industry is mutually beneficial and necessary. These benefits will be enhanced by the use of data analytics and appropriate AI software in our action plan, ensuring that these trends observed can be utilised by the government to impact other industries as well, indicating that our action plan has a greater impact.

Furthermore, the Public Report of the COI on the SingHealth data breach case also mentions that “an effective incident response plan can reduce the extent and impact of an attack by identifying its source and shutting it down quickly. In the event of a cyber attack, warnings may come at short notice and the pace at which an attack escalates may be rapid. The correlation between the effectiveness of an incident response plan and recovery is evident, with organisations recovering from attacks proportionally to their incident response preparedness.” This shows that our action plan of ensuring that concrete steps are being taken towards improving cybersecurity, especially with the aid of expert IT companies, has the capability to minimise the occurrence and impacts of data breaches, so as to protect user data to the greatest extent. Combined with the use of social media to spread awareness on the effectiveness of our action plan, we can significantly improve public confidence in grocery delivery services, and increase their usage of such services.

Bibliography

Cite the resources you consulted using the APA format.

1. (2015, April 08). Online creep: Targeted ads may have opposite effect of marketers' intent. Retrieved from https://www.sciencedaily.com/releases/2015/04/150408171201.htm
2. Waxer, C. (2013, November 04). Big data blues: The dangers of data mining. Retrieved from https://www.computerworld.com/article/2485493/enterprise-applications-big-data-blues-the-dangers-of-data-mining.html
3. Marr, B. (2017, March 03). The 4th Industrial Revolution And A Jobless Future - A Good Thing? Retrieved from https://www.forbes.com/sites/bernardmarr/2017/03/03/the-4th-industrial-revolution-and-a-jobless-future-a-good-thing/#411d12cb44a5
4. Shank, P. (2017, December 08). The Fourth Industrial Revolution: What Happens With Employment? Retrieved from https://www.td.org/insights/the-fourth-industrial-revolution-what-happens-with-employment
5. CSO Staff (2015, December 14). Data breaches will affect 1/4 of the world's population by 2020, IDC predicts. Retrieved from https://www.csoonline.com/article/3014493/data-breaches-will-affect-14-of-the-worlds-population-by-2020-idc-predicts.html
6. Tay, R. (2019, June 19). Businesses in Singapore lost nearly S$58 million to email impersonation scams last year: CSA report. Retrieved from https://www.businessinsider.sg/businesses-in-singapore-lost-nearly-s58-million-to-cyber-attacks-last-year-csa-report/
7. (n.d.). Ordering a Food Subscription Box? The Safety Issue You Need to Know About. Retrieved from https://www.shape.com/healthy-eating/meal-ideas/food-safety-concerns-meal-kit-delivery-services
8. (n.d.). Last-Mile Challenges in Singapore's Food E-Commerce Industry. Retrieved from https://sbr.com.sg/food-beverage/commentary/last-mile-challenges-in-singapores-food-e-commerce-industry
9. Goman, C. (2018, November 14). Has Technology Killed Face-To-Face Communication? Retrieved from https://www.forbes.com/sites/carolkinseygoman/2018/11/14/has-technology-killed-face-to-face-communication/#54f4711da8cc
10. Chan, M. (2019, March 29). The dying art of conversation – has technology killed our ability to talk face-to-face? Retrieved from https://theconversation.com/the-dying-art-of-conversation-has-technology-killed-our-ability-to-talk-face-to-face-112582
11. Lahiri, K. (2017, February 13). Five ways to prevent data leaks. Retrieved from https://www.helpnetsecurity.com/2017/02/13/prevent-data-leaks/
12. (n.d.). Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database. Retrieved from https://www.mci.gov.sg/coireport

13. (2019, April 16). Less than 1 in 4 Singapore consumers trust personal data with organisations. Retrieved from https://www.techgoondu.com/2019/04/16/less-than-1-in-4-singapore-consumers-trust-personal-data-with-organisations/
14. (2019, Jun 13). EU campaigns to raise data privacy rights awareness as survey shows gap. Retrieved from https://www.channelnewsasia.com/news/world/eu-campaigns-to-raise-data-privacy-rights-awareness-as-survey-shows-gap-11625040
15. Div, L. (2016, October 28). How the government can help businesses fight cyber attacks. Retrieved from https://www.csoonline.com/article/3135864/how-the-government-can-help-businesses-fight-cyber-attacks.html
16. Gundert, L. (2019, February 28). 5 steps for a successful public-private cyber crime fighting partnership. Retrieved from https://gcn.com/articles/2019/02/28/cyber-crime-fighting-partnership.aspx?m=1
17. Gaskin, J. (n.d.) Retrieved from https://www.channelpronetwork.com/article/importance-incident-response-planning
18. (2017, September 18). The importance of Ethical Hacking. Retrieved from https://www.indiatoday.in/education-today/jobs-and-careers/story/ethical-hacking-1047211-2017-09-18
19. James, M (2019, May 1). How Can Ethical Hacking Be “Ethical”? Retrieved from https://staysafeonline.org/blog/how-can-ethical-hacking-be-ethical/