JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 14, Issue. 2
June 2021
ISSN: 1946-1836

In this issue:

4. **Privacy Concerns and Data Sharing Habits of Personal Fitness Information Collected via Activity Trackers**
Jamie Pinchot, Robert Morris University
Donna Cellante, Robert Morris University

14. **A Prototype for Distributed Computing Platform using Smartphones**
Jeffrey Wagner, Grand Valley State University
Xiang Cao, Grand Valley State University

22. **A Comparative Study on Information Technology (IT) Infrastructure and Disaster Recovery Methodology**
Delester Brown Jr., Colorado Technical University
Samuel Sambasivam, Woodbury University

31. **The Promise and Peril of Drone Delivery Systems**
Victoria Fowler, Lowes Companies, Inc
Austin Eggers, Appalachian State University
Sandra A. Vannoy, Appalachian State University
B. Dawn Medlin, Appalachian State University

42. **Towards a Leader-Driven Supply Chain Cybersecurity Framework**
Manoj Vanajakumari, University of North Carolina Wilmington
Sudip Mittal, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
Kasey Miller, Naval Postgraduate School

iscap
Information Systems & Computing Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three issues a year. The first date of publication was December 1, 2008.

JISAR is published online (https://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (https://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP/EDSIG who perform the editorial and review processes for JISAR.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Privacy Concerns and Data Sharing Habits of Personal Fitness Information Collected via Activity Trackers

Jamie Pinchot
pinchot@rmu.edu

Donna Cellante
cellante@rmu.edu

Computer and Information Systems Department
Robert Morris University
Moon Township, PA 15108 USA

Abstract

Activity trackers such as FitBit and Apple Watch have become popular for collecting fitness and health data. Few studies have examined privacy concerns and risks regarding the use of activity trackers and the sharing of personal fitness information (PFI). This study presents findings from a survey of activity tracker users (n = 325) to explore the privacy concerns, perceptions, and habits of users. Findings indicate that several factors impact the PFI data sharing habits of users, including understanding privacy policies, understanding device privacy settings, and the level of value placed on PFI. Further, knowledge of privacy policies and settings had a clear impact on perceptions of the sensitivity and value of PFI.

Keywords: privacy, Internet of Things, personal fitness information, health information, activity trackers, fitness trackers

1. INTRODUCTION

Devices that are able to connect to a network and interact with other apps and devices are referred to as the Internet of Things (IoT). Typical examples of IoT devices are smart phones, tablets, smart watches, activity trackers, home appliances, home assistants, smart cars, and smart parking meters. The number of global IoT devices connected to the Internet has been increasing at a rapid pace, from 18.4 billion networked devices in 2018 to an estimated 29.3 billion devices in 2023. This includes multiple devices per person, with a global average of 2.4 devices per individual in 2018 and an estimated increase to 3.6 devices per individual in 2023 (Cisco, 2020).

The Pew Research Center estimates that 60 percent of all Americans engage in some sort of fitness tracking (Boran, 2017). Many people own a wearable activity tracker such as a Fitbit, Apple Watch, Garmin, or Samsung Gear, and use associated mobile apps to track fitness and activity data. If worn continuously, these trackers can monitor the user 24/7, and collect a large amount of data. Among IoT devices, activity trackers are among those that have the greatest number of sensors, which are capable of collecting sensitive information, such as step count, location, heart rate, exercise activities, distance travelled, calories burned, weight, and even sleep habits (Torre, Sanchez, Koceva, & Adorni 2018). This can be a serious privacy concern. Collectively, the health-related data

captured by activity trackers is referred to as personal fitness information (PFI).
Activity trackers fall into the category of IoT devices called wearables. The term "wearable technology" refers to an electronic device or product which can be worn by a person to integrate computing into daily activity or work and use technology to avail advanced features and characteristics (PR Newswire, 2013). While wearables can conveniently provide access to an overabundance of PFI for individuals, there are potential privacy risks to consider. Scholars have been spreading the word about the risk of possible data loss, leakage, or compromise with self-tracing wearable technologies (Ajana 2017; Fotopoulou & O'Riordan 2016; and Lanzing 2016).

2. RELATED WORK

Security risk is defined as a "circumstance, condition, or event with the potential to cause economic hardship to data or networked resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste and abuse" (Balta-Ozkan et al., 2013). In the U.S., citizens' Constitutional right to privacy is implied in the language of the 4th Amendment, where it states: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated" (Legal Information Institute, n.d.). While some studies have found that users of wearable devices are concerned with privacy (Fuller et al., 2017; Seguar Anaya et al., 2018; Vitak et al., 2018), others suggest that individuals have low levels of concern when it comes to disclosing information collected with wearable devices (Lehto & Lehto, 2017; Motti & Caine, 2015; Truong, 2019).

Vitak et al. (2018) studied 361 activity tracker users to understand how concerns about privacy affected users' mental models of personal fitness information (PFI) privacy. The study found that the majority of users were lacking general knowledge about how fitness companies collect, store, and share activity data. Vitak et al. (2018) found no significant relationships between user's disclosure of activity data and privacy concerns. They note that this finding echoes another study that found that the privacy paradox does exist and attributes it largely to the apathy of Internet users who do value privacy, but feel that once information is shared, it is out of their control (Hargittai & Marwick, 2016).

Lehto and Lehto (2017) conducted a qualitative study focused on user experiences of using a wearable device and associated privacy concerns. The study found that information collected with wearable devices was not perceived by participants as sensitive or private, although health information stored in medical records was considered to be very sensitive and private. This disconnect is of increasing concern as more health information that was only stored in medical records is now being stored in a variety of places including activity trackers, mobile apps, and cloud services.

Torre et al. (2018) conducted a study on FitBit wearables and associated mobile apps, including FitBit's own app and the Lose It! app. They found that during installation of the FitBit app, which is required in order to use the device, users are prompted to allow a number of permissions on their smart phone including: identity, contacts, location, SMS, photos/media, camera, Bluetooth, and device ID/call information. Installation requires name, gender, height, weight, and birthday as mandatory inputs. The study's findings illustrate the privacy risks for FitBit data due to the possibility of using shared data to correlate to third party app data or infer undisclosed personal information.

One privacy risk with wearable devices and the associated services is that individuals may not understand how their information is stored and handled (Patterson, 2013). Further, it is possible that risk awareness regarding the uses of health information data, even in aggregate form, is not well understood by users. In fact, device manufacturers of activity trackers have claimed that health and fitness data of users is de-identified and aggregated, and therefore does not pose a privacy risk (FitBit, n.d.). FitBit's privacy policy, for example, states "We may share non-personal information that is aggregated or de-identified so that it cannot reasonably be used to identify an individual" (FitBit, n.d., para. 21). However, this can be misleading to users who may not know that there are often ways to re-identify this data if it was only partially aggregated or aggregated in ways that might be possible to reverse engineer. Any partial demographic data that can be associated with the anonymized data could allow for reidentification (Na et al., 2018).

Machine learning can also be used for reidentification of de-identified and aggregated health information collected from activity trackers (Na et al., 2018). Na et al. (2018)

conducted a cross-sectional study of national physical activity data collected for 14,451 individuals between 2003 and 2006. The data sets included fitness data such as step count that was collected from activity trackers. Though this data was de-identified and partially aggregated, the authors were able to use machine learning to re-identify individuals by learning their daily footstep patterns via 20-minute-level physical activity data and connecting those patterns to demographic data. Approximately 95% of adults and 80% of children in the study were successfully identified (Na et al., 2018).

Another privacy risk is that increasing quantities of health data are being created outside of the protection of the Health Insurance Portability and Accountability Act (HIPAA). This includes data generated via activity trackers and mobile health apps as well as other social media (Glenn & Monteith, 2014). The companies that collect this health data include data brokers and Internet companies, often combining this data with other known information about users and then sell it for advertising or other purposes (Pinchot et al., 2018). In some cases, employers have begun to collect heath data on employees and treat it in similar fashion (Brown, 2016).

A final privacy risk of activity trackers is that location information can be used to track an individual or locate sites that an individual frequently visits. For example, location information from activity trackers published as a heat map by Strava.com, an exercise-focused social network, has been used to identify the location of military sites (Perez-Pena & Rosenberg, 2018).

3. CURRENT STUDY

While it is clear that there are risks to data privacy for users of activity trackers, these devices continue to grow in popularity and use. The global market for activity trackers was valued at $17.9 million in 2016 and is forecasted to grow 19.6% by 2023 (Loomba & Khairnar, 2018). Even for users who express concern for privacy, there is often a mismatch between attitude and behavior. This is known as the privacy paradox, and has been studied extensively in relation to the use of social media (Acquisti & Gross, 2006; Barnes, 2006; Kokolakis, 2017; Taddicken, 2014).

The purpose of this study is to explore data privacy concerns, perceptions, and habits among users of activity trackers. The first research question will explore a number of factors related to PFI privacy:

RQ1: What are activity tracker users' PFI privacy concerns, perceptions about PFI sensitivity, perceptions about PFI value, understanding of privacy settings, understanding of privacy policies, and PFI data sharing habits?

The second research question probes further by examining the relationship between these concerns, perceptions, and habits:
RQ2: What is the relationship between activity tracker users' PFI privacy concerns, perceptions about PFI sensitivity, perceptions about PFI value, understanding of privacy settings, understanding of privacy policies, and their PFI data sharing habits?

4. RESEARCH METHODOLOGY

This study used an electronic survey consisting of 20 quantitative questions. The sample (n=325) for the study includes adults 18 and older who have used an activity tracker such as a FitBit, Apple Watch, etc. Participants were first asked about their frequency of use for their activity tracker, specifically asking for the average number of days (on a scale from 0 to 30) they wear their tracker in a typical month. Participants were then asked a set of questions focusing on their privacy concerns, a set of questions focusing on their PFI data sharing habits, a set of questions focused on their understanding of privacy settings for their activity tracker, and questions regarding their understanding of the privacy policy and data sharing activities of the company that makes their activity tracker, their perception of the sensitivity of PFI data, and their perception of the value of PFI data.

Mobile User's Information Privacy Scale (MUIPC)

To measure the participants' privacy concerns regarding activity trackers and their associated mobile apps, we used the Mobile Users' Information Privacy Scale (MUIPC) that was developed by Xu et al. (2012). MUIPC was developed as an evolution of two prior scales focused on privacy: the Concern for Information Privacy (CFIP) scale developed by Smith et al. (1996) to measure individuals' concern about organizational privacy and the Internet User's Information Privacy (IUIPC) scale, developed by Malhotra et al. (2004) to adapt CFIP to an online environment for Internet users concerned about information privacy (Malhotra et al., 2004;

Smith et al., 1996; Xu et al., 2012). MUIPC is a 9-item scale that was developed "to reflect mobile users' concerns about information privacy" (Xu et al., 2012, p. 13). Items were measured on a five-point Likert scale anchored with "Strongly disagree" = 1 and "Strongly agree" = 5. The scale includes three dimensions: perceived surveillance, perceived intrusion, and secondary use of personal information (Xu et al., 2012).

Perceived Surveillance (SURV)
(1) I believe that the location of my activity tracker is monitored at least part of the time.
(2) I am concerned that the mobile app associated with my activity tracker is collecting too much information about me.
(3) I am concerned that mobile apps may monitor my activities on my activity tracker.
Perceived Intrusion (INTR)
(4) I feel that as a result of my using an activity tracker, others know about me more than I am comfortable with.
(5) I believe that as a result of my using an activity tracker, information about me that I consider private is now more readily available to others than I would want.
(6) I feel that as a result of my using an activity tracker, information about me is out there that, if used, will invade my privacy.
Secondary Use of Personal Information (SUSE)
(7) I am concerned that mobile apps with access to my activity data may use my personal information for other purposes without notifying me or getting my authorization.
(8) When I give personal information to use mobile apps, I am concerned that apps with access to my activity data may use my information for other purposes.
(9) I am concerned that mobile apps with access to my activity data may share my personal information with other entities without getting my authorization.

Table 1: Adapted Mobile Users' Information Privacy Scale (MUIPC)
Note: Adapted from Xu et al. (2012)

Perceived surveillance has been defined as, "the watching, listening to, or recording of an individual's activities" (Solove, 2006, p. 490). Perceived intrusion is defined as, "invasive acts that disturb one's tranquility or solitude" (Solove, 2006, p. 491). Table 1 shows the items used for the MUIPC scale.

The MUIPC scale has good internal consistency, with a Cronbach alpha coefficient above .7 reported for all three subscales (Xu et al., 2012; Degirmenci et al., 2013).

PFI Data Sharing Habits (SHARE)
As personal fitness information (PFI) can often include sensitive data that users may not want shared in certain contexts, it was important to understand how respondents disclose PFI in an online environment. We adapted three yes/no questions from Vitak et al. (2018) that focused on activity tracker data sharing habits. Respondents were asked whether they had (1) shared fitness data online, (2) configured their tracker to automatically post fitness data online, and (3) shared fitness data with other users. These three items were reported individually and averaged to create an index of PFI data sharing habits.

Understanding of Privacy Settings (SET)
Users of activity trackers may not always know how to review and configure privacy settings on their devices. Or, users may be aware of how to configure privacy settings but do not make an effort to do so. Two items were used to measure understanding of the privacy settings of their activity tracker. Respondents were asked (1) how confident they are that they understand how to use the privacy settings of their activity tracker (measured on a scale from 0 = not at all confident to 100 = very confident) and (2) how much effort they have put into reviewing and configuring privacy settings of their activity tracker (measured on a scale from 0 = no effort to 100 = much effort). These two items were averaged to create an index of understanding of privacy settings.

Understanding of Privacy Policies (POL)
Many companies have data sharing policies and practices that allow users' personal data to be shared, individually or in aggregate, with third parties. To address this important concept, we adapted one question from Vitak et al. (2018) that asked respondents how confident they are that they understand the privacy policy and data sharing practices of the company that makes their activity tracker. This question was measured on a scale from 0 = not at all confident to 100 = very confident.

Perception of PFI Sensitivity (SENS)
It is important to understand how respondents feel about PFI in relation to other types of personally identifiable information (PII). To address data sensitivity, we asked respondents how concerned they would be if their activity tracker data were compromised (such as via a security breach). Responses were measured on a scale from 0 = not at all concerned to 100 = very concerned.

Perception of PFI Value (VAL)
To address data value, respondents were asked how valuable their activity tracker data is to them, in comparison to other types of PII, such as financial data. Responses were measured on a scale from 0 = not at all valuable to 100 = very valuable. Both questions were adapted from Vitak et al. (2018).

Sample
The sample for this study was obtained via Amazon Mechanical Turk (MTurk), a crowdsourcing tool that has been used extensively by academic researchers for survey research and allows access to a pool of participants that meet inclusion criteria (Lovett, 2018; Redmiles et al., 2017). This tool allows a survey to be posted with a specified compensation amount. For short surveys, the compensation amount per survey completion is typically between $.10 and $.50 (Lovett, 2018). This study provided compensation within the recommended range. Redmiles et al. (2017) found that samples from MTurk studies are largely representative of the entire U.S. population and are comparable to census web-panel and telephone survey respondents. However, they also note that respondents on MTurk differ from their demographic peers in their online skill and experience level (Redmiles et al., 2017). This higher level of online skill and experience should be taken into account for a study focused on mobile device and Internet privacy issues.

The survey used in this study was created in Question Pro and posted on Amazon Mechanical Turk targeting between 300-350 responses. Data was collected in April 2020. A total of 386 people started the survey, but 325 (84%) participants completed usable surveys.

4. FINDINGS

Of the participants who completed the survey (n=325), the majority of the participants were in the 25-34 year old range. We did, however, have four participants above 64 years old. Table 2 is details the breakdown of the ages.

Age Range	No. of Participants	Percentage
18-24	52	16%
25-34	172	52.9%
35-44	55	16.9%
45-54	34	10.5%
55-64	8	2.5%
Above 64	4	1.2%

Table 2: Participants by Age

The participants came from a variety of countries, with the majority of participants, 56.9%, from the United States and significant numbers of participants from India, 18.5%; Brazil, 7.7%; and Canada, 3.4%, as shown in Table 3. The remainder of participants, 13.5%, came from a variety of other countries including France, Spain, Columbia, and Venezuela.

Country	Frequency	Percentage
United States	185	56.9%
India	60	18.5%
Brazil	25	7.7%
Canada	11	3.4%
Other (17 countries)	44	13.5%

Table 3: Participants by Country

The average days per month that the participants used their activity tracker was between 21-30 days. This indicates that the sample included users who actively used their activity trackers. Table 4 shows the breakdown of usage:

Days Per Month	No. of Respondents	Percentage
0-10 days	41	12.6%
11-20 days	112	34.5%
21-30 days	172	52.9%

Table 4: Activity Tracker Usage by Days per Month

Addressing RQ1
RQ1 asked "What are activity tracker users' PFI privacy concerns, perceptions about PFI sensitivity, perceptions about PFI value, understanding of privacy settings, understanding of privacy policies, and PFI data sharing habits?" PFI privacy concern (MUIPC) was measured using the MUIPC scale. Of the 325 respondents, 296 had completed all questions used in the scale and were included in the index. The scale

showed good internal consistency (Cronbach's a=.89). The median value of the index score was used to divide the users into high and low privacy concern categories. As shown in Figure 1, the high and low concern categories were nearly equally split, with low concern having a slight edge (50.9%) over high concern (49.1%). This result clearly showed that there was not a strong level of opinion regarding privacy concern, in either direction, for this sample. The majority of the respondents had an average score that fell into the Neutral response category (mean = 3.52, median = 3.67).

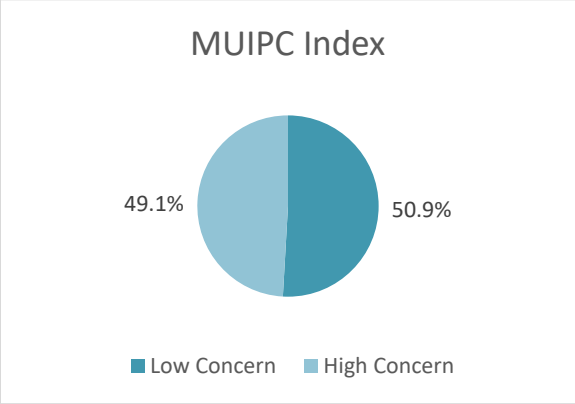

Figure 1: MUIPC Index Showing High and Low Privacy Concern Categories

PFI sensitivity (SENS), PFI value (VAL), understanding of privacy policies (POL), and understanding of privacy settings (SET) were each measured on a sliding scale of 0 to 100. Table 5 shows the breakdown of responses for each of these variables.

Response	SENS	VAL	POL	SET
0 to 20	34	55	59	38
21 to 40	42	67	58	62
41 to 60	75	86	68	83
61 to 80	86	63	83	75
81 to 100	78	52	55	33
Mean	59.8	50.9	52.6	50.7
Median	61	50	52	50.5

Table 5: Breakdown of Responses for SENS, VAL, POL, and SET

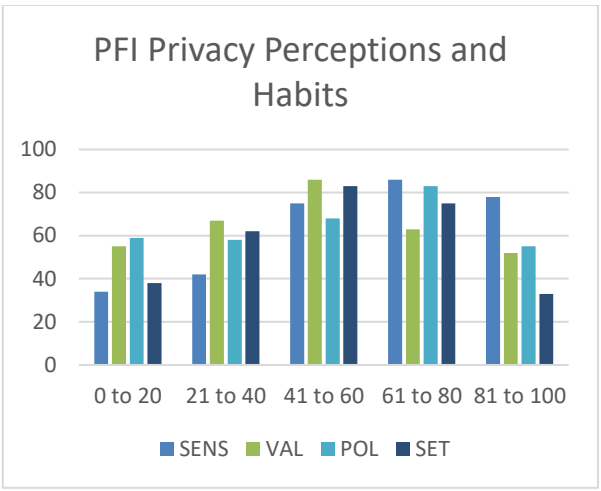

Figure 2: PFI Privacy Perceptions and Habits

Figure 2 visually depicts the breakdown of responses. The mean is near the midpoint of the scale for all four variables, though PFI sensitivity is skewed very slightly more toward the higher end of the scale.

Three questions on the survey addressed the PFI data sharing habits of respondents. Of the 325 participants, 112 never shared any information at all. Forty-three participants shared at least one aspect. Fifty-nine respondents shared at least two aspects, and 94 participants shared everything. Seventeen respondents did not answer the questions.

Table 6 shows the breakdown of the data sharing habits:

Amount of Sharing	Frequency	Percent
0% (nothing)	112	34.5%
33% (1 part)	43	13.2%
66% (2 parts)	59	18.2%
100% (3 parts)	94	28.9%
No answer	17	5.2%

Table 6: PFI Data Sharing Habits

An interesting point about this table is that there are about the same number of participants who share nothing (112) as those that share everything (94). An inverted bell curve as shown in Figure 3 visually demonstrates the breakdown.

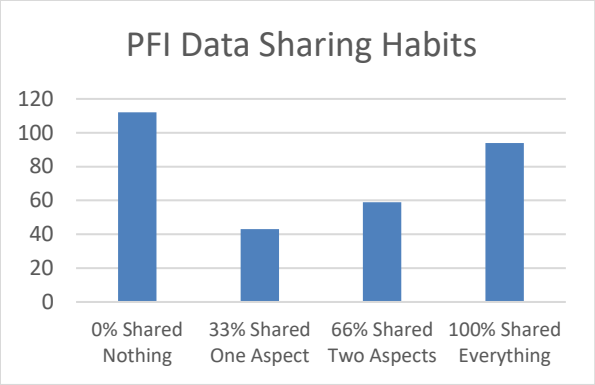

Figure 3: PFI Data Sharing Habits of Participants

Addressing RQ2

RQ2 asked, "What is the relationship between activity tracker users' PFI privacy concerns (MUIPC), perceptions about PFI sensitivity (SENS), perceptions about PFI value (VAL), understanding of privacy settings (SET), understanding of privacy policies (POL), and their PFI data sharing habits (SHARE)?" Relationships between the privacy factors were investigated using the Pearson's product-moment correlation coefficient.

Impacts on PFI Data Sharing Habits (SHARE)

There was a statistically significant, negative correlation between understanding of privacy policies (POL) and PFI data sharing habits (SHARE), $r = -.139$, $n = 307$, $p < .05$. This indicates that high levels of understanding of privacy policies were associated with low levels of PFI data sharing habits. Additionally, there was a statistically significant, negative correlation between understanding of privacy settings (SET) and PFI data sharing habits (SHARE), $r = -.251$, $n = 284$, $p < .001$. This indicates that high levels of understanding of privacy settings were associated with low levels of PFI data sharing habits. This clearly shows that the more understanding a user has of the privacy policies in place for the company that makes their activity tracker, and the more knowledgeable a user is of the device's privacy settings, the less likely they will be to share PFI data online.

A statistically significant, negative correlation was also found between perceptions of PFI value and PFI data sharing habits, $r = -.284$, $n = 306$, $p < .001$. This indicates that high perceptions of PFI value were associated with low levels of PFI data sharing habits. So, the more value that a user placed on PFI, the less likely they were to share PFI data online.

Notably, there was no correlation found between the respondents' PFI privacy concern (as measured by MUIPC) or PFI sensitivity and PFI data sharing habits.

Impacts of Understanding Privacy Policies (POL) and Device Privacy Settings (SET)

There was a statistically significant correlation between understanding of privacy policies (POL) and PFI sensitivity (SENS), $r = .191$, $n = 313$, $p < .005$. This indicates that high levels of understanding of privacy policies were associated with high perceptions of PFI sensitivity. There was also a statistically significant correlation between POL and PFI value (VAL), $r = .383$, $n = 321$, $p < .001$. This indicates that high levels of understanding of privacy policies were associated with high perceptions of PFI value. There was a statistically significant correlation between understanding of privacy settings (SET) and PFI sensitivity (SENS), $r = .334$, $n = 292$, $p < .001$. This indicates that high levels of understanding of privacy settings were associated with high perceptions of PFI sensitivity. Additionally, there was a statistically significant correlation between SET and PFI value (VAL), $r = .542$, $n = 296$, $p < .001$. This indicates that high levels of understanding of privacy settings were associated with high perceptions of PFI value. Lastly, there was a strong, statistically significant correlation between POL and SET, $r = .702$, $n = 296$, $p < .001$. This indicates that high levels of understanding of privacy policies were associated with high levels of understanding of privacy settings.

The more knowledgeable a user was on privacy policies, the higher they valued PFI and the higher they found PFI's sensitivity in comparison to other types of data. Additionally, the more knowledgeable a user was on privacy policies, the more likely they were to be knowledgeable on privacy settings on their device. The inverse was also true; the more knowledgeable a user was on the privacy settings of their device, the more knowledgeable they would be of privacy policies and the higher they valued PFI and the higher they found PFI's sensitivity.

Another interesting significant finding was related to POL. There was a statistically significant, negative correlation between POL and privacy concerns (MUIPC), $r = -.132$, $n = 296$, $p < .05$. This indicates that high levels of privacy concern were associated with low levels of understanding of privacy policies.

Impacts on Privacy Concerns (MUIPC)

There was a statistically significant correlation between PFI data sensitivity (SENS) and MUIPC ($r = .366$, $n = 286$, $p < .001$) and PFI value (VAL) and MUIPC ($r = .166$, $n = 294$, $p < .005$). This indicates that high perceptions of PFI data sensitivity and data value were associated with high levels of privacy concern.

5. CONCLUSIONS

First, the authors acknowledge some possible limitations to this research. The use of Amazon Mechanical Turk (MTurk) for data collection may have introduced a limitation in that users of MTurk often skew toward the online-savvy, which could impact the generalizability of results if participants had more online experience and perhaps used this experience to more readily find and learn about privacy policies and settings for their activity trackers (Redmiles et al., 2017). Future studies could minimize this potential bias by utilizing a sample that is not skewed in terms of online experience and may better represent a general audience of activity tracker users. Additionally, volunteer response bias is always a possibility when conducting an online survey, and this could be exacerbated by paying participants via MTurk. This bias could result in overrepresentation of participants with strong opinions on the survey topic.

The participants surveyed showed an interesting mix of privacy factors related to the use of wearable activity trackers. Participants were active users of activity trackers, with the majority using a tracker between 21 and 30 days in an average month. They showed a neutral stance in terms of overall privacy concern for PFI, with the majority of participants averaging a neutral score on the MUIPC scale. Their PFI data sharing habits were somewhat dichotomous, with the majority of participants either sharing no PFI online (35%) or sharing all aspects of PFI data online (29%).

Findings indicated that the factors that significantly impacted activity tracker users' personal fitness information (PFI) data sharing habits (SHARE) included understanding privacy policies (POL), understanding privacy settings on the device (SET), and the level of value they placed on PFI data (VAL). Each of these factors had an inverse relationship with data sharing habits, meaning that the more a user understood privacy policies and settings, and the more they valued PFI, the less likely they were to share PFI online. Their level of privacy concern (as measured by MUIPC) and the level of sensitivity they placed on PFI in comparison to other types of data (SENS) did not have any impact on data sharing habits (SHARE). As privacy concern did not have an impact on data sharing habits, there is no support from these results for the concept of a privacy paradox for IoT wearables such as activity trackers.

Additionally, knowledge of privacy policies (POL) and device privacy settings (SET) for activity trackers had a significant impact on both perceptions of PFI sensitivity (SENS) and PFI value (VAL). There was a clear connection between this knowledge and how sensitive or valuable a user found PFI. This could indicate that a user gains a clearer understanding of the types of risks associated with disclosure of PFI via the knowledge gained by learning more about the company's privacy policies and settings that are available to secure PFI data on an activity tracker device. There was also a significant inverse relationship between knowledge of privacy policies (POL) and level of privacy concern (MUIPC) such that as knowledge of privacy policies increased, the level of privacy concern decreased. This could be interpreted that privacy policies were found to be reassuring to users and thus decreased their concerns about PFI privacy.

Higher perceptions of the sensitivity and value of PFI had a significant impact on privacy concern. This logically shows that the higher the importance a user placed on PFI, the more concerned they were about PFI privacy. However, as PFI privacy concern was not shown to have impacted data sharing habits, the results of this study did not support the idea of a privacy paradox for PFI shared via activity trackers.

While this study has shed some insights on PFI privacy concerns, perceptions, and data sharing habits, additional work is warranted. We are moving into an era where personal fitness information (PFI) can be auto-generated by a variety of IoT wearables and other devices and used, individually or in aggregate, in ways that users may not anticipate. This kind of data can potentially be used to evaluate healthcare and insurance applications and claims, as well as other employer-sponsored programs. Other applications for this type of data may not have been discovered yet, but could prove to be a privacy risk for individuals. It is imperative that users of IoT wearables, such as activity trackers, are empowered with knowledge about the PFI privacy risks, and also the policies and settings that can be used to mitigate those risks.

6. REFERENCES

Acquisiti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. PET 2006: International Workshop on Privacy Enhancing Technologies. Springer, 36-58. https://doi.org/10.1007/11957454_3

Ajana, B. (2017). Digital health and the biopolitics of the quantified self. *Digital Health, 3,* 2. Doi: 10.1177/2055207616689509

Balta-Ozkan, N., Davidson, R., Bicket, M., and Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy, 63,* 363-374.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). https://doi.org/10.5210/fm.v11i9.1394

Boran, M. (2017, June 15). *Fitness trackers run into data security concerns: Self-tracking boom has prompted consumer worries about keeping personal data safe. The Irish Times.* https://www.irishtimes.com/business/technology/fitness-trackers-run-into-resistance-over-data-security-concerns-1.3119483

Brown, E. (2016). The FitBit fault line: Two proposals to protect health and fitness data at work. *Yale Journal of Health Policy, Law, and Ethics, 16*(1), 1-50.

Cisco (2020, March 9). *Cisco annual Internet report 2018-2023.* White paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Fotopoulou, A., & O'Riordan, K. (2016). Training to self-care: Fitness tracking, biopedagogy and the healthy consumer. *Health Sociology Review, 25(*3*)*. http://sro.sussex.ac.uk/60044/

Fuller, D., Shareck, M., & Stanley, K. (2017). Ethical implications of location and accelerometer measurement in health research studies with mobile sensing devices. *Social Science & Medicine, 191*, 84-88.

Glenn, T., & Monteith, S. (2014). Privacy in the digital world: Medical and health data outside of HIPAA protections. *Current Psychiatry Reports, 16*(494), 3-11.

Hargittai, E., & Marwick, A. (2016). 'What can I really do?' Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737-3757.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

Legal Information Institute. (n.d.). *Fourth amendment*. Cornell Law School. https://www.law.cornell.edu/constitution/fourth_amendment

Lehto, M., & Lehto, M. (2017). Health information privacy of activity trackers. Proceedings of the 16th European Conference on Cyber Warfare and Security. University College Dublin. Dublin, Ireland, 243-251.

Loomba, S., & Khairnar, A. (2018, March). *Fitness trackers market overview.* Allied Market Research. https://www.alliedmarketresearch.com/fitness-tracker-market

Lovett, M., Bajaba, S., Lovett, M., & Simmering, M. (2018). Data quality from crowdsourced surveys: A mixed method inquiry into perceptions of Amazon's Mechanical Turk Masters. *Applied Psychology, 67*(2), 339-366. doi: 10.1111/apps.12124

Motti, V., & Caine, K. (2015). Users' privacy concerns about wearables: Impact of form factor, sensors and type of data collected. *FC 2015: Financial Cryptography and Data Security, 8976*, 231-244. Doi: 10.1007/978-3-662-48051-9_17

Na, L., Yang, C., Lo, C., Zhao, F., Fukuoka, Y., & Aswani, A. (2018). Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. *JAMA Network Open, 1*(8), 1-13. doi:10.1001/jamanetworkopen.2018.6040

Patterson, H. (2013). Contextual expectations of privacy in self-generated health information flows. *41st Research Conference on Communication, Information, and Internet*

Policy. http://dx.doi.org/10.2139/ssrn.2242144

Perez-Pena, R., & Rosenberg, R. (2018, January 29). Strava fitness app can reveal military sites, analysts say. *New York Times.* https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html

Pinchot, J., Chawdhry, A., & Paullet, K. (2018). Data privacy issues in the age of data brokerage: An exploratory literature review. *Issues in Information Systems, 19*(3), 92-100.

Privacy policy. (n.d.). FitBit. https://www.fitbit.com/us/legal/privacy

PR Newswire. (August 19, 2013). Wearable electronics market and technology analysis (2013-2018): By components (sensors, battery, display, networking); Applications. *PR Newswire*.

Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154,3,* 477-560.

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273.

Torre, I., Sanchez, O.R., Koceva, F., & Adorni, G. (2018). Supporting users to take informed decisions on privacy settings of personal devices. Springer. doi 10.1007/s00779-017-1068-3

Truong, K. (2019). *How private health info can be identified through fitness tracker data.* MedCityNews. https://medcitynews.com/2019/01/how-private-health-info-can-be-identified-through-fitness-tracker-data/

Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. *International Conference on Information, iConference 2018: Transforming Digital Worlds*, 229-239. Springer.

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Kritikos, K. (2018). 'There's nothing really they can do with this information': Unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication, & Society.* doi: 10.1080/1369118X.2018.154344

Editor's Note:

This paper was selected for inclusion in the journal as an CONISAR 2020 Distinguished Paper. The acceptance rate is typically 7% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2020.

A Prototype for Distributed Computing Platform using Smartphones

Jeffrey Wagner
wagnejef@mail.gvsu.edu

Xiang Cao
caox@gvsu.edu

School of Computing and Information Systems
Grand Valley State University
Allendale, Michigan 49401, USA

Abstract

Distributed computing usually provides a mechanism for multiple computers to participate in computing tasks. In distributed computing, a large computing job can be divided and sent to many computers, which communicate and coordinate via networks. In recent years, mobile devices like smartphones continue to grow in power and number, so that their combined computing capacity has increased as well. However, much of this computing capacity is wasted, because smartphones sit idle from time to time throughout the day and while charging at night. In this paper, we explore the possibility of harnessing that otherwise unused computing power of smartphones through the implementation of a mobile-based distributed computing platform designed to tackle large computing tasks. To demonstrate the capabilities of the system, we use identification of genes associated with the development of renal cancer as the computing task. Our prototype is set to identify such genes mainly using only the computing power of smartphones for statistical analysis. Performance evaluation shows our prototype design is feasible and promising compared to a centralized system running on a desktop computer.

Keywords: Distributed Computing, Prototype, Mobile Device, Smartphone, Gene Identification

1. INTRODUCTION

Distributed computing has been very prevalent in recent years. Instead of providing services in a centralized solution, distributed computing often involves multiple computers to participate in computing tasks. There are many applications in this broad idea of distributed/decentralized computing, such as Peer-to-Peer (P2P), Blockchain, Internet of Things (IoT).

In distributed computing, a large computing intensive job can be divided and assigned to many computers, which communicate and coordinate via networks. Each computer can work on a small part of the original job respectively. With multiple computing devices working together, many distributed/decentralized computing applications are expected to produce results more efficiently.

Admittedly, there are some research work such as (Appuswamy, Gkantsidis, & Narayanan, 2013) and (Karanasos, Rao, Curino, Douglas, Chaliparambil, Fumarola, Heddaya, Ramakrishnan, & Sakalanaga, 2015), which discuss the advantages and disadvantages of distributed computing paradigm, compared with more centralized approaches. Also, using idle computing power is a way to increase utilizations and efficiently explore the available computing resources. However, different from other work,

we focus on the idle computing power of smartphones. In this paper, we look at the distributed computing from a different perspective - exploring the unused computing resource of smartphones.

Recently, mobile devices like smartphones have more and more improved computing power, so that each of them can be viewed as a computing device. When Apple released the iPhone in 2007, it started a technological revolution that cellphone continues to grow in popularity and power today. Also, the number of smartphones has grown tremendously. As 2019, 81% of Americans owned a smartphone (Pew Research Center, 2019) and those smartphones have gone from iPods that can make phone calls to very capable computers that fit into our pockets. Hence, the combined computing capacity of smartphones have become a significant resource.

With so many powerful smartphones always on and often sitting unused (smartphones are idle from time to time throughout the day and while charging at night), a lot of this computing resource is wasted. In this paper, inspired by the idea of "Citizen Science" (Wikipedia – Citizen Science, n.d.) and "Crowdsourcing" (Wikipedia – Crowdsourcing, n.d.), we explore the possibility of harnessing that otherwise unused computing power of smartphones.

We implement a mobile-based distributed computing platform designed to tackle large computing tasks. We develop a prototype consisting of smartphones as the main computing resource. To demonstrate the effectiveness and efficiency of our system, we use identification of genes associated with the development of renal cancer as the computing task. Our prototype is set to identify such genes mainly using only the computing power of smartphones to run statistical analysis tasks. Compared to a centralized system running on a desktop computer, performance evaluation shows our prototype design is feasible and promising.

The rest of this paper is organized as follows. Section 2 is the literature review. In Section 3, we introduce the prototype architecture. We show our implementation in Section 4. In Section 5, we show the performance evaluation and discuss our results. Finally, we conclude our paper and present the future work in Section 6.

2. LITERATURE REVIEW

Citizen science (Wikipedia – Citizen Science, n.d.) has been popular in recent years. In citizen science, amateur scientists have chances to participate in scientific research projects, by offering their data, knowledge, experience, equipment, devices and so on. Similarly, crowdsourcing (Wikipedia – Crowdsourcing, n.d.) is a model that assigns and divides tasks among participants to obtain a combined result. Nowadays, Internet is widely utilized in citizen science and crowdsourcing to involve participants. Related to this paper, we believe if some people could contribute the idle time of their smartphones, extra computing resources would be available.

There are many distributed computing projects (Wikipedia – List of Distributed Computing Projects, n.d.) that allow the public to contribute their spare computing power. For example, the Folding@Home project (Folding@Home, n.d.) allows users with home computers, particularly those with powerful GPUs, to contribute towards disease research by allowing their machines to be used as part of Folding@Home's distributed system, which processes immense datasets related to protein folding. SETI@Home (SETI@Home, n.d.) is a volunteering computing project to analyze data for searching intelligent life in the universe. Users connected to Internet can participate in this project by downloading and analyzing radio signal data using their personal computers.

Some distributed computing projects involve smartphone usages. For example, SPOTTERON (SPOTTERON, n.d.) is a platform offering solutions for citizen science and volunteering monitoring projects. Customized smartphone Apps are provided in the platform. iNaturalist (iNaturalist, n.d.) allows users to observe and share biodiversity on the earth using smartphone Apps. In (Graham, Henderson, Schloss, 2011), three examples of involving citizen scientists in research using mobile phones have been discussed.

Research work in (Arslan, Singh, Singh, Madhyastha, Sundaresan, & Krishnamurthy, 2012), (Duan, Kubo, Sugiyama, Huang, Hasegawa, & Walrand, 2014), and (Remédios, Teófilo, Paulino, & Lourenço, 2015) have studied smartphone issues in distributed computing. In (Arslan et al., 2012), several aspects of smartphones have been investigated, including profiling battery charging behaviors, task migration and task scheduling on smartphones.

In (Duan et al., 2014), different incentive mechanisms about motivating smartphone users to participate in data acquisition and distributed computing are analyzed and proposed. Study in (Remédios et al., 2015) describes a preview of a distributed mobile system to process locally generated data in a network of smartphones without infrastructure support.

In this paper, we present a hands-on experimental study that shows the feasibility and effectiveness of distributed computing using smartphones.

3. PROTOTYPE ARCHITECTURE

Our prototype consists of two components, a simple (central) server and multiple (client) smartphones, as shown in Figure 1.

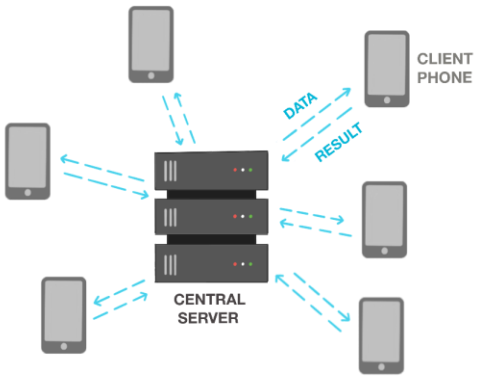

Figure 1. Prototype Architecture

The (central) server in our prototype does not participate in running the actual computing tasks (i.e., statistical analysis of gene identification). Instead, it divides the large computing task, communicates with all the (client) smartphones and coordinates them. The (central) server sends the partitioned data to multiple (client) smartphones, waits for the results returned by them, and finally assembles results into a meaningful output.

The (client) smartphones in our prototype receive the data from the server, do the actual computing for statistical analysis of gene identification, and send the results back to the server.

The detail of the implementation is presented in the next section.

4. IMPLEMENTATION

Server

The server divides the entire input file into many pieces and sends them one by one to different client smartphones for processing. The server makes use of multithreading and concurrency in its design. There is a command line interface that accepts user inputs and acts accordingly, a thread that listens for new clients (smartphones) connecting and provides them with TCP socket connections, and threads that interact with each of the client smartphones to send data and receive results. The server program runs in a regular desktop machine in Java using JetBrains IDEs, IntelliJ.

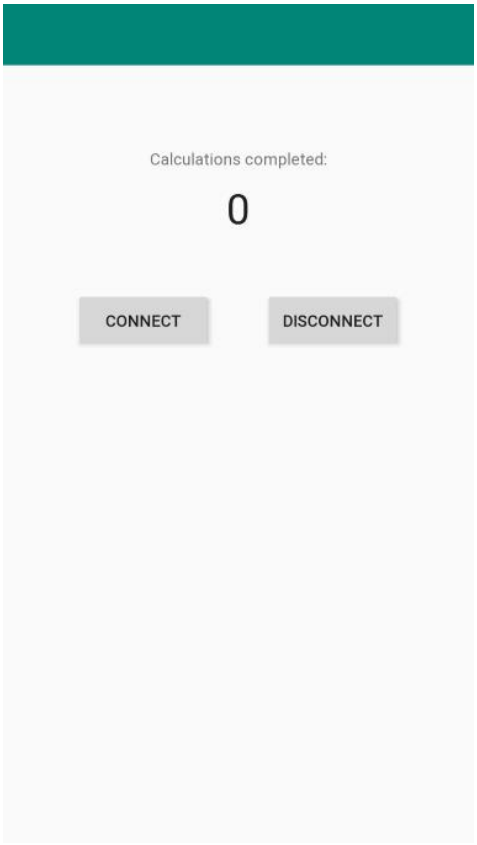

Figure 2. Mobile App Interface

Client Smartphones

Client smartphones can connect to the server for data and return the results. Each smartphone runs an Android mobile App implemented in Java using Android Studio. The App consists of a simple user interface as shown in Figure 2, along with a back end for handling data processing. When the user of the smartphone wants to contribute some processing power, the App can be launched and the "CONNECT" button is

pressed to join the system. The App will then listen for data coming in and process it on arrival, then return the result back to the server and await the next job. A counter in the interface shows the number of calculations completed. In this example case, it is the number of genes that have been analyzed for their association to renal cancer. Once a gene analysis job is complete, the client smartphones wait on standby and the server outputs a CSV file with the compiled results.

Statistical Analysis
For statistical analysis jobs run by smartphones, a Cohen's d (d-score) is calculated for each gene using data from 8 renal cancer patients and 52 non-renal cancer patients from the National Cancer Institute's NCI-60 dataset (CellMiner, n.d.). In our experiments, calculating the d-score involves calculating the mean, standard deviation, and t-statistic for the 60-item dataset, then repeatedly shuffling the dataset and recalculating the statistics until a final comparison result in the d-score.

Efficiency
For better efficiency, the server keeps listening for results from the smartphones. As soon as it receives one from a smartphone, the server sends that smartphone another piece of data to continue to work on.

In our experiments and in the real practical system, smartphones have different data processing speed because of their various specifications. Some smartphones process data faster with better CPUs and others run experiments slower. If there are only a few pieces of input data left and the slower smartphones are still processing them, the server will also send these data to the faster smartphones to take advantage of their higher processing speed, preventing them from going idle. The server will use whichever results come back first from slower and faster smartphones to assemble the compiled result.

Robustness
Our prototype is also designed to be robust in its handling of client smartphones. When other smartphones are running their jobs, a new client smartphone can still connect to the server for its task. When a smartphone is disconnected, it will not cause issues. Its work will be reassigned to another available client smartphone. The robustness is tested by intentionally connecting and disconnecting smartphones during trial runs, and no result is corrupted due to that.

5. PERFORMANCE EVALUATION AND DISCUSSION

Devices
In our experiments, we use 5 smartphones to test our platform, as shown in Table 1. The Google Pixel 2 XL was a former flagship smartphone (released in October 2017), but now it is considered mid-range in today's market. The Motorola Moto X4 is a more budget friendly model, and the Blue Advance A4 is a very inexpensive Android smartphone. We choose these smartphones because the Google Pixel 2 XL and Motorola Moto X4 are the ones we have had, and the Blue Advance A4 is the cheapest smartphones we could find. These smartphones run Android systems, so that IOS implementation is not included.

For the desktop machine, its CPU is AMD FX 8350, and the GPU is Nvidia GTX 980.

Device	Processor	Retail Price	Quantity
Google Pixel 2 XL	Snapdragon 835	$175	1
Motorola Moto X4	Cortex A53	$140	1
Blue Advance A4	Cortex A7	$40	3

Table 1. Smartphones for Performance Evaluation

Dataset
The dataset for gene analysis in our experiments is a pre-processed copy of "RNA: Affy HG-U133 Plus 2.0" from the National Cancer Institute's NCI-60 dataset (CellMiner, n.d.). The size of the dataset is about 1.8MB. Each gene is shuffled 10,000 times before the final result comes out.

Performance Metric
The experiments are measured by their processing time as the performance metric. In our experiments using smartphones, the processing time is the wall-clock time from the server sending out the first piece of data, to the moment when the server receives the last result. For the server-only experiments, the processing time is the time for the desktop machine to finish the entire gene analysis job. For each experiment, we run three times and show the average as the result.

Experiments
(1) Server-only
In the first group of experiments, we run our gene statistical analysis jobs on the desktop

machine, exploring its computing capability. We also utilize the desktop machine to simulate the performance of a typical centralized (non-distributed) server solution. This set of experiments is a benchmark compared with the performance of smartphones.

The CPU of the desktop machine is AMD FX 8350, which has 8 threads. In order to test the impact of concurrency, we run our gene analysis program on the desktop machine using different number of threads. The result is shown in Figure 3.

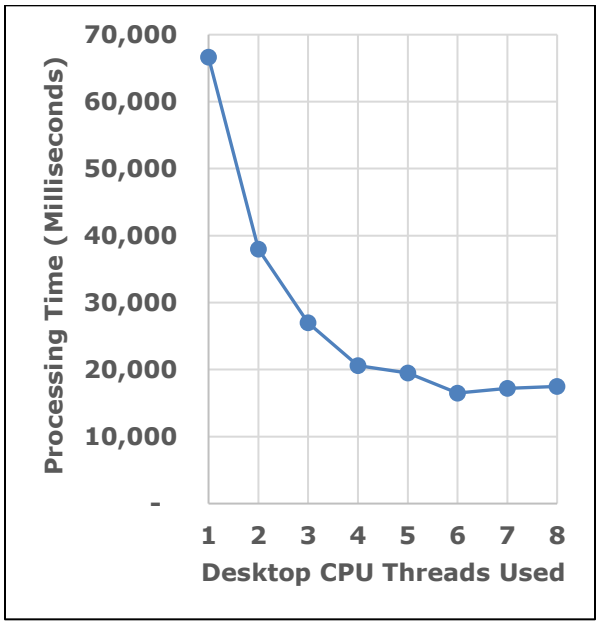

Figure 3. Processing Time vs. Number of Threads

From the result, we can see that when the number of threads used is small, the processing time decreases as the number of threads increases, because of the concurrency. However, the decrease in processing time does not scale exactly with the number of threads used. For example, the 2-thread run is about 1.8 times as fast as the single thread run, and the 3-thread run is about 2.5 times as fast.

When the number of threads reaches a certain value, the performance is little changed. Hence, the concurrency cannot improve the performance unlimitedly.

(2) Smartphones
We conduct experiments to test the computing capabilities of smartphones. We first run the gene identification jobs using the slowest but most affordable smartphone in our device pool - Blue Advance A4, exploring the performance related to the number of smartphones.

Figure 4 shows the result. We can see that the performance is reversely proportional to the number of smartphones, because of the parallelism. The processing time of 2-phone run is almost exactly half as that of the single phone run, and the 3-phone run takes three times faster. This trend of inverse proportionality is more accurate and direct than that of desktop machine's performance with multiple threads. This is because each smartphone runs tasks separately as independent small computers.

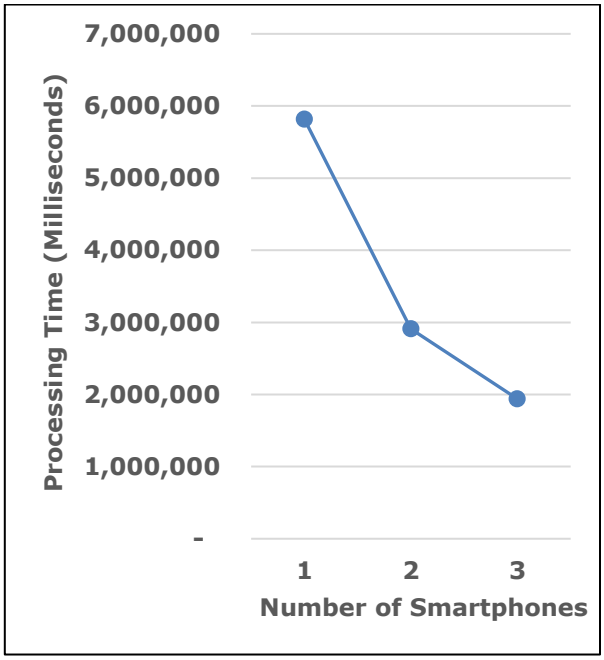

Figure 4. Performance of Blue Advance A4

We then conduct three sets of experiments on 1 Google Pixel 2 XL, 1 Motorola Moto X4, and a group of all smartphones (1 Google Pixel 2 XL, 1 Motorola Moto X4 and 3 Blue Advance A4s) respectively, compared with desktop machine (1 thread). The result is shown in Figure 5.

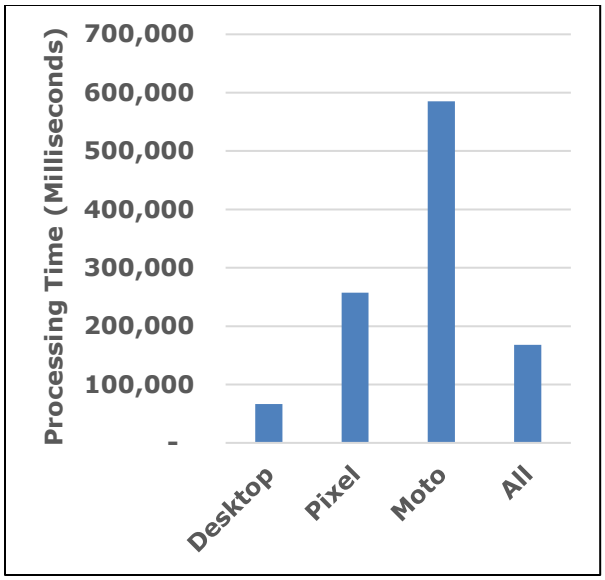

Figure 5. Performance of Different Devices

From Figure 5, we can see that the Google Pixel 2 XL has a better performance compared the Motorola Moto X4. Although the desktop machine still performs the best, a group of all 5 smartphones reduces the processing time by taking advantage of parallelism. Along with the fact of inverse proportionality shown in Figure 4, we believe with more and more smartphones, a group of smartphones will eventually outperform the desktop machine.

Projection

It would be ideal to further test the system with more high-end smartphones by spending thousands of dollars. However, due to our budget and resource limit, we show the performance of a large-scale system by projection based on the fact of inverse proportionality shown in Figure 4 and the actual data from Figure 5. Our extrapolation is shown in Figure 6 in the Appendix.

We extrapolate the performance of up to 36 Google Pixel 2 XL and Motorola Moto X4 smartphones respectively. In Figure 6, the first data points (shown in triangles as markers) of Motorola Moto X4 and Google Pixel 2 XL are actual performance data (the same as shown in Figure 5), while the rest of their data points (shown in circles) are projected according to the pattern demonstrated by the Blue Advance A4 shown in Figure 4.

As shown in Figure 6, it would take 4 Google Pixel 2 XLs or 9 Motorola Moto X4s to outperform a single thread of the desktop machine. It would take 16 Google Pixel 2XLs to outperform the desktop machine's best multithreaded run (6 threads as shown in Figure 3) or 36 Motorola Moto X4s to accomplish the same feat. We can see that, while a single smartphone does not excel at speed compared with the desktop machine, a group of them together can reduce the processing time. Hence, with more and more smartphones, the performance of the system would be better and better.

Discussion

From all the previous results, we can see that parallelism indeed improves the system's performance, so that multiple smartphones provide better results than a single one.

In today's computing intensive world, computing resources are in high demand. More and more servers are being purchased and added into the computing pool. On the other hand, the processing power of smartphones has been growing rapidly. Consumers have continued to demand more performance from their smartphones for over a decade and manufacturers have been happy to provide support. However, much of computing power of smartphones is wasted when they are sitting idle from time to time throughout the day and while charging at night.

With billions of smartphone users worldwide (Statista, 2020), it would be a wise idea to harness that otherwise tremendous unused "almost free" computing power of smartphones. Our results show that with only several or dozens of smartphones, their processing capabilities can outperform a traditional desktop machine.

Like citizen science, if the computing platform intends to expand its processing power, or accelerate its processing speed on a project, it can consider encouraging people to contribute their smartphones' computing power. Some incentives can be given to attract smartphone users to participate. Based on our experimental results, we have showed that it is a feasible and promising solution, at least from the technical perspective.

6. CONCLUSIONS

In this paper, we investigate the possibility of harnessing that otherwise unused computing power of smartphones. We implement a mobile-based distributed computing prototype using smartphones to tackle large computing tasks.

Our experimental results show the prototype is technically feasible and promising.

Our idea of this prototype is supported by two key facts: (1) the number of smartphones has been growing continuously along with their computing power, so that their combined computing capacity has increased in a rapid rate; (2) Much of the computing capacity is wasted when smartphones are sitting idle from time to time throughout the day and while charging at night. Hence, it would be ideal if we could efficiently utilize the computing resources of smartphones.

In future work, we plan to run other types of tasks in smartphones and investigate their impacts on the prototype's performance, compared with the desktop machine. We also plan to investigate the impact of task processing on the smartphones themselves, e.g., CPU and memory usage, power consumption of smartphones. Additionally, more smartphones can be involved to further test the feasibility of the system.

7. REFERENCES

Appuswamy, R., Gkantsidis, C., & Narayanan, D. (2013). Scale-up vs Scale-out for Hadoop: Time to rethink? Publishing in ACM *SoCC*, *20*, 1-13.

Arslan, M., Singh, I., Singh, S., Madhyastha, H., Sundaresan, K., & Krishnamurthy, S. (2012). Computing While Charging: Building a Distributed Computing Infrastructure Using Smartphones. Publishing in ACM *CoNEXT*, 193-204.

CellMiner (n.d.). Retrieved from https://discover.nci.nih.gov/cellminer/loadDownload.do

Duan, L., Kubo, T., Sugiyama, K., Huang, J., Hasegawa, T., & Walrand, J. (2014). Motivating Smartphone Collaboration in Data Acquisition and Distributed Computing. Publishing in IEEE *Transactions on Mobile Computing, 13(10)*, 2320-2333.

Folding@Home (n.d.). https://foldingathome.org

Graham, E., Henderson, S., & Schloss A. (2011). Using mobile phones to engage citizen scientists in research. Publishing in AGU *EOS, 92(38), 313-315*.

iNaturalist (n.d.). https://www.inaturalist.org/

Karanasos, K., Rao, S., Curino, C., Douglas, C., Chaliparambil, K., Fumarola, G., Heddaya, S., Ramakrishnan, R., & Sakalanaga, S. (2015). Mercury: Hybrid Centralized and Distributed Scheduling in Large Shared Clusters. Publishing in USENIX *ATC*, 485-497.

Pew Research Center (2019). Mobile Fact Sheet. Retrieved from https://www.pewresearch.org/internet/fact-sheet/mobile/

Remédios, D., Teófilo, A., Paulino, H., & Lourenço, J. (2015). Mobile Device-to-Device Distributed Computing Using Data Sets. (2015). Publishing in EAI *MOBIQUITOUS*, 297-298.

SETI@Home (n.d.). https://setiathome.berkeley.edu

SPOTTERON (n.d.). https://www.spotteron.net/

Statista (2020). Number of smartphone users worldwide from 2016 to 2021. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Wikipedia – Citizen Science (n.d.). Retrieved from https://en.wikipedia.org/wiki/Citizen_science

Wikipedia – Crowdsourcing (n.d.). Retrieved from https://en.wikipedia.org/wiki/Crowdsourcing

Wikipedia – List of Distributed Computing Projects (n.d.). Retrieved from https://en.wikipedia.org/wiki/List_of_distributed_computing_projects

Appendix

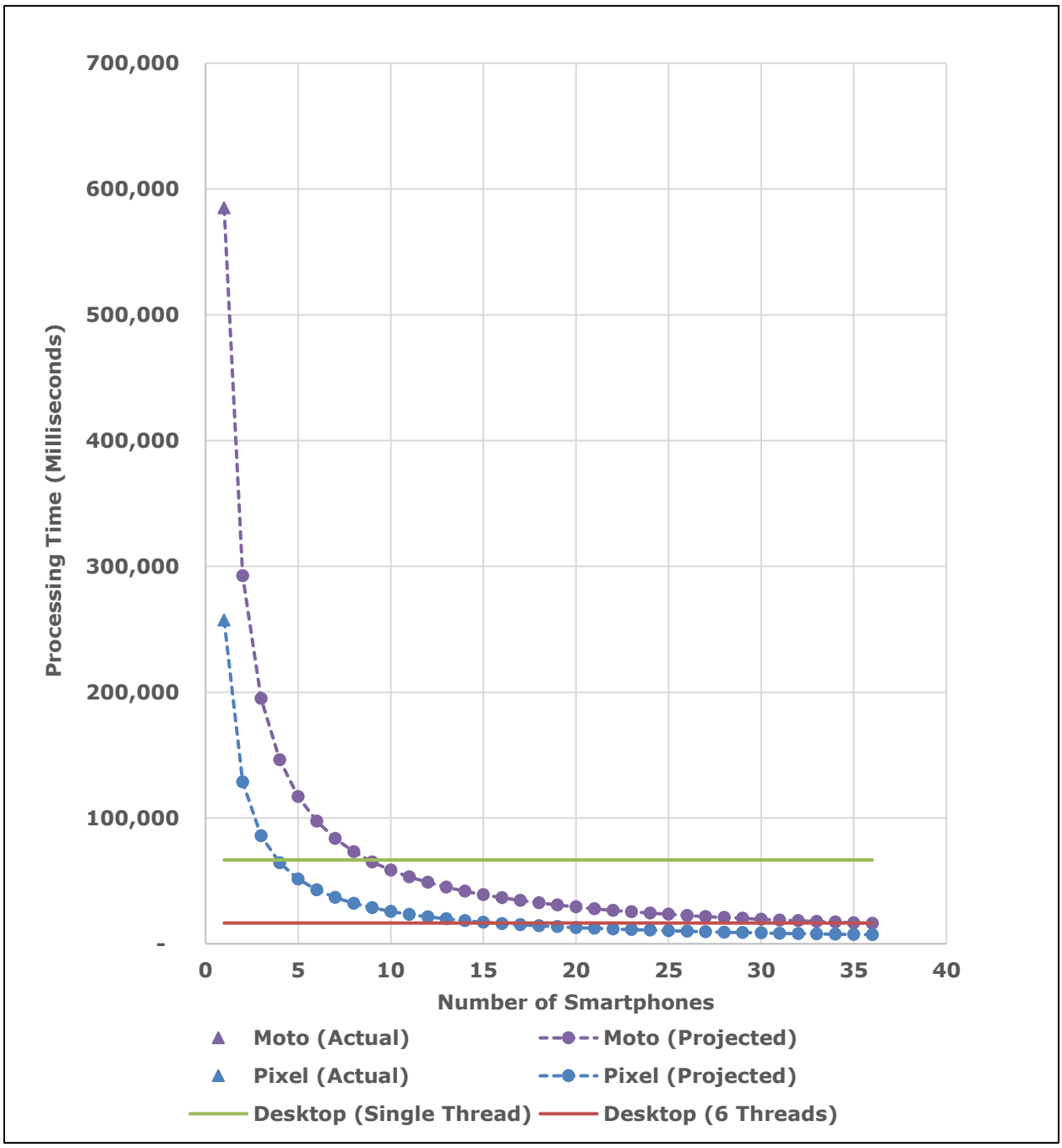

Figure 6. Actual and Projected Performance

A Comparative Study on Information Technology (IT) Infrastructure and Disaster Recovery Methodology

Delester Brown Jr.
dbrownjr@gmail.com
Colorado Technical University
Colorado Springs, CO

Samuel Sambasivam
Samuel.Sambasivam@Woodbury.edu
Woodbury University
Burbank, CA

Abstract

The threats of disruptions to business continuity loom over companies as they enhance more capabilities using information technology (IT) infrastructures. What is the best way to divert a disaster that occurs in IT infrastructure? Many individuals are unsure as to the best method. A comprehensive literature covering subjects like software-defined network principles, business continuity, and their connection to unified theory of acceptance and use of technology included in the study. The participants, information technology professionals, located in the Southeastern region of the U.S. will benefit from the anticipated value or impact to the problem domain. The research intends to determine which backup methods are considered most representative of an IT population based on distinct variables emphasized by the textbook authors. This study analyzes variables such as key performance indicators of education, recovery experience, and professions to develop insight concerning the current type of recovery methodology. Our summarized results lead to several conclusions that are relevant to the choice of recovery methodologies; traditional backup and virtualization, for IT disaster recovery.

Keywords: information technology; key performance indicators; network function virtualization; traditional backup; disaster recovery; UTAUT;

1. INTRODUCTION

Disaster recovery has become a focal point in business impact analysis (BIA) according to Zio (2016), especially for IT professionals employed in a network or database infrastructure. Moreover, the importance of determining the appropriate backup method that supports the recovery was paramount to ensure business continuity. Zio (2016) asserted that having an adequate disaster recovery plan has a massive influence on the BIA, which strengthens the organizational structure.

The goal of this study was to examine IT disasters from a quantitative perspective to provide a determination for the best suited recovery method. In the study, a hypothesis highlighted an underlying analysis that interprets the correlations to participants' professional experiences, perceptions, and opinions of information technology (IT) professionals. These key performance indicators (KPIs) are defined variables like recovery time objectives (RTO), recovery point objectives (RPO), and cost on the development of an IT

disaster recovery plan (Kerzner, 2017). Frank Webster (2014) found that valid backup methods like traditional or network function virtualization (NFV) are critical to establishing a sound disaster recovery plan (DRP). Known to reduce IT catastrophes, Tucker (2015) believed that determining backup methods in DRPs rely on the different IT personnel's professional experiences, considerations, and opinions. Analysts concentrated more on critical variables such as recovery time objectives and recovery point objectives, found in business impact analyses (Lemieux, 2004).

Research Purpose

The purpose of the quantitative study enhance IT professionals' assessment of their IT posture during an IT disaster. This investigation taps into IT professionals at mid-size information technology organizations in the Southeastern region of the United States. The study explored the influence of the rate of accepting emerging technologies; unified theory of acceptance and use of technology theory on IT professionals in the disaster recovery area. At that point, a sound assessment can be made as to the best recovery method at acceptable service levels. IT professionals gain quality decision-making abilities in areas that lacks constant innovation like disaster recovery.

2. METHODOLOGY

The direction from the hypothesis's position plus measures and practices for data gathering that provide a theoretical context for quantitative methodology (Newton & Rudestam, 2014). The research question is: what is the relationship between key performance indicators (KPIs), education, recovery experience, profession and the selection of a backup method?

Quantitative data gathering methodologies depended on random sampling and structured data collection instrument that are appropriate for various experiences into prearranged reaction groupings. The data gathering generates results that are straightforward to generalizations, versatility, and standardization amongst all participants.

Data Collection

By extracting information from a survey questionnaire instrument, data is analyzed primarily using binary logistic regression calculations. The instrument was pre-designed and tested by Howard Marks for Information Week Research. For this study the survey was delivered by Survey Monkey. The platform distributes survey instruments across multiple platforms (Windows and Apple) and various devices such as mobile devices, tablets, and computers (Bryson, 2015).

Overlooking to acknowledge variables and data sets involved will produce disparities in the research data thereby causing more difficulties in drawing a comprehensive conclusion. Every survey will incorporate the following typical practice: (1) introduce the research study (2) inform its objective and constrictions; (3) acquire an endorsed permission accord form (d) use the survey protocol to ensure all questions are asked and are in the correct format, (4) recognition of respondent's participation.

3. ANALYSIS OF DATA

The soundest analytic technique for this study was a binary logistic regression. Binary logistic regression has two or more independent variables, and the dependent variable (nominal) has only two outcomes available. In SPSS, the binary logistic regression had three methods to determine the best model: forced entry, forward, or backward stepwise (George & Mallery, 2016). Binary logistic regression estimates the probability that a characteristic was present.

The study was intended to determine whether there was a need for a specific recovery method. This approach's execution follows assessing the correlation amid the independent variables of KPIs, education, and recovery experience, profession, and the dependent variable required backup method. The value of the independent variables was entered in the binary logistic regression to determine if there was a need for a specific backup method; network function virtualization and traditional.

IBM's SPSS will be used for investigation in this study. SPSS was one of the well-known programs used for statistical assessment and file managing. This investigative tool can assist in business, educational, and, perform statistical analyses with the information. It was an instrument for intermediary to sophisticated clients (Field, 2013). Attaining expert technical support for troubleshooting software issues and assess present probes confirming adherence of ethical standards.

4. FINDINGS

The research study consists of participants that are located in the Southeastern region of the United States. The region was comprised of 11 states which was the first criteria for any participant in the quantitative analysis. Participants were 200 adults who met additional criteria as a knowledge professional in the information technology field located in the Southeastern region.

The geographical location of the participants is depicted in Figure 1. Florida (N = 66) along with Virginia and West Virginia (N = 54) led in providing the most participants for this research study. North Carolina (N = 31), Kentucky (N = 18), and Georgia (N = 10) followed in participant's location. Using a diverse population was meant to provide an accurate representation of professionals within information technology unlike previous research by White (2017).

Other characteristics of the participants involve job position, level of education, and years of experience. Figure 2 displays a graphic review of the information collected from population such as job position and level of education. The majority of survey respondents held an entry level job position at 42.5 percent. That tally nearly doubled the closet groups of intermediate workers and middle management at (N = 40 and 39, respectively). Also, many of them achieved a higher level of education. In Figure 2, of the total participants surveyed (N = 200), 79 had obtained a bachelor's degree, and about half of this group were entry level (N = 29).

The survey study explored annual revenue of the participants 'organizations. Yearly income can point to a capacity of openness which allows midsize companies to adopt emerging technologies quicker. However, many respondents (69) didn't know their organizations annual revenue. Similarly, in Figure 3, 41 participants found their organizations to have between zero to $50,000. There were 33 respondents, whose organizations had over one million dollars in revenue.

As information was revealed from the results, clear designations differentiated the study from previous research. Also, the results below provided more insights and relationships into IT disaster recovery as the data was extracted from a diverse population. Of the total respondents surveyed (N = 200), 56 had obtained an associate's degree, while a large majority held a bachelor's degree (N = 79). Twenty-three respondents had attained a master's degree as their peak level of education. A large portion of respondents in the population were employed in entry level positions (N = 85). The table in Figure 4 conveys the frequency and percentage gathered from the population concerning years of experience.

The participants revealed in Figure 10 the level of quality in the organization's data backup processes. 113 or 56.5% of the participants felt the quality of the backup process was over 60 %. Only 32% or 64 respondents disclosed that their quality level 40% or below. Mounting dependence on information technology, in addition to compliance and governing obligations, has led many organizations to focus on business continuity and disaster recovery (DR) solutions. Critchley (2016) believed availability has become a significant concern for business survival. Therefore, it becomes mandatory that one should take a detailed look at disaster recovery testing and the specific steps to ensure a disaster recovery plan performs as expected. The research measured the frequency of an organization's disaster recovery testing. The data showed the effectiveness of preparedness as 67.5% hold recovery testing once a month or more. In Figure 4, 18 or 9% of participants test their recovery plans annually. Testing brings out the practical concerns implicated in executing business transactions during an outage and validates the actual efficiency of DR procedures.

5. DISCUSSION

The survey instrument measured confident in the participants' disaster recovery skillset and employer's ability to align emerging technology with their business functions. The result indicated in Figure 5 and Figure 6 respondents showed confidence in their IT recovery abilities and employer adoption of technology. In Figure 5 just one hundred and one participants, 47 (100 to 81%) and 54 (80 to 61%), were over 60% confident in their DR skillsets. There were 28 participants at zero to 20%, 40 participants with a 21% to 40%,and 31. Participants at 41 to 60% confidence in their skills. The scale is dissimilar when reviewing the population's confidence level in the organization's ability to incorporate emerging technology. The majority of the populace, 94 participants answered very confident, 63 respondents were extremely confident while no one was found to be neutral. Also, in Figure 6, 37 participate deemed themselves as slightly confident, and a mere 6

respondents felt not confident about their organizations. Graham and Kaye (2015) believed a comprehensive recovery exercise is vital to build confidence amongst IT professionals in handling outages that impacts business functions effectively.

The outcomes were logically and systematically summarized and interpreted in relation to their importance to the research questions and hypotheses. The comments on the findings address observed consistencies and inconsistencies and discuss possible alternate interpretations. What, if any, was the relationship between education (IV) and the selected backup method (DV)? The null hypothesis is there was no correlation between education (IV) and the selected backup method (DV). H1A: There was a correlation between education (IV) and the selected backup method (DV). In this research study, the binary logistic regression technique comprises of two quantifiable purposes 1) to determine which independent variables were significant and had an effect on the dependent variable and 2) establish how the logistic regression model predicted where the dependent variable binary in nature e.g. backup method [traditional backup vs. NFV].

The results show that education levels except education level (2) has a significance of 0.002 which is below 0.05. Decoded as bachelor's degrees, it is statistically significant to determine a backup method selection. Thus, the hypothesis (H1A) is accepted as education has a correlation selecting a backup method.

The secondary research question states: what, if any, was the relationship between recovery experience (IV) and the selected backup method (DV)? H20: There was no correlation between recovery experience (IV) and the selected backup method (DV). H2A: There was a correlation between recovery experience (IV) and the selected backup method (DV).

The Wald statistic indicates no contribution to the dependent variables at .305, 1.517, .349, and .755 respectively. From the information uncovered in the results recovery experience was no bearing on the dependent variable. Specifically, the null hypothesis (H20) was accepted as no correlation between recovery experience (IV) and the selected backup method (DV) was found in the research study.

The third research question suggests what, if any, was the relationship between profession (IV) and the selected backup method (DV)? The H30 null states there was no correlation between profession (IV) and the selected backup method (DV).

The Wald statistic was assessed for importance by means of a 95% confidence level. The p-values were greater than .05, then that variable was considered not a significant influence. Within the current model all predictor variables except job title (1) and (4) were not individually significant. Based upon the researcher's coding method job title (4) was any respondent that selected the employment position of owner, executive, or c-level and job title (1) is decoded as an intermediate worker. With a Wald statistic of 0.053 and 0.045, this indicated that the independent predictor variable has a slight effect on the dependent variable. All significance have been found to be greater than 0.05, thus the null hypothesis; no direct correlation between profession and backup method selection, is accepted.

The research recognized the necessity to examine whether the model is more precise than simply guessing the outcome will be the more common of the two categories. Therefore, the -2log likelihood (-2LL) was reviewed in the model summary for each variable in Figure. The likelihood establish how appropriate the regression model is once the data was input into it. The -2LL shows number for education (-2LL = 175.408), recovery experience (-2LL = 191.542), and profession (-2LL = 192.768). The smaller the -2LL the likely that variable is a better fit to predict.

6. CONCLUSIONS

The responses of 132 participants in the study were surveyed to increase comprehension into the complexion of selecting IT disaster recovery methods; traditional or network function virtualization. The results of the quantitative survey instrument were analyzed. Based on that analysis, the architecture of the recovery methodology has distinctive considerations, in addition to those in common factors. A key finding was that the certain employment positions; owner/executive/c-level and intermediate workers. The deficiency of the understanding the organization's annual revenue, the potential importance of key performance indicators classified as other.

Based on these results, recommendations for future research were proposed. While it is difficult to address the lack of knowledge, a

solution utilized by some vendors is to reduce the complexity and knowledge requirement by providing alternative mechanisms to authoring rules. These alternatives include reducing the size of rulesets and utilization of a spreadsheet-like interface to capture conditions and actions.

The key themes which materialized from the quantitative analysis are listed below:

1. Lack of diversity in decision making.

2. The common regularity of testing.

3. Satisfaction of KPIs

4. Major IT disaster recovery usage.

5. Confidence in the integration of emerging technology.

6. Regular restoration errors occurrences.

7. Confidence in skillset

Based on these themes, the importance of adequate education and position of employment is vital when selecting a solution to remedy an IT disaster. A reoccurring and fundamental model related to understanding the nature of IT catastrophes including how they link to business function, the DR methodologies, and the importance of managing event of an IT disaster. The study also exposed the importance of applying education to certain employment positions can lead to the selection of methodologies to DR solutions.

Future Research

To further create an advantageous decision-making for mid-size IT companies, professionals should focus on potential exploration. Intended future research actions comprise of the following:

1. Explore a qualitative analysis of the effects of decision making from owners, executives, and intermediate workers on information technology disaster recovery in organizations.

2. Investigate quantitative analysis of the correlation between actions variables and IT disaster recovery methodology.
3. Execute a study pertaining to the influence of a baccalaureate education on the selection of IT disaster recovery methodology.

6. REFERENCES

Bryson, J. (2015). Faster, easier, more impactful research. *Marketing Insights, 27*(5), 14-15.

Critchley, T. (2016). *High-Performance IT Services*. Auerbach Publications.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Sage.

George, D., & Mallery, P. (2016). *IBM SPSS Statistics 23 step by step: a simple guide and Reference*. Routledge.

Graham, J., & Kaye, D. (2015). *A Risk Management Approach to Business Continuity: Aligning Business Continuity and Corporate Governance*. Rothstein Publishing.

Kerzner, H. (2017). Project management metrics, KPIs, and dashboards: a guide to measuring and monitoring project performance. John Wiley & Sons. Retrieved from https://doi.org/10.1002/9781119427599

Lemieux, V. L. (2004). Two approaches to managing information risks. *Information Management Journal*, 38(5), 56-62.

Nardi, P. M. (2018). *Doing survey research:A guide to quantitative methods*. Routledge.

Newton, R. R., & Rudestam, K. E. (2014). *Surviving your dissertation: A comprehensive guide to content and process*. Sage Publications.

Tucker, E. (2015). Understanding the Standards. Business Continuity from Preparedness to Recovery, 19–32. Retrieved from https://doi.org/10.1016/B978-0-12-420063-0.00002-4

Webster, F. (2014). *Theories of the information society.* Routledge.

White, G. R. (2017). *Enhancing existing disaster recovery plans using backup performance Indicators* (Doctoral dissertation, Walden University).

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, 137-150.

Appendices and Annexures

Variable		N	Percentage
Location			
	Alabama	4	2
	Florida	66	33
	Georgia	10	5
	Kentucky	18	9
	Mississippi	7	3.5
	North Carolina	31	15.5
	South Carolina	3	1.5
	Tennessee	4	2
	Maryland	3	1.5
	Virginia and West Virginia	54	27
	Total	200	100

Figure 1. Participants Demographic

Demographic Variable		N	Percentage
Job Position			
	Owner / Executive / C-Level	14	7
	Senior Management	22	11
	Middle Management	39	19.5
	Intermediate	40	20
	Entry Level	85	42.5
	Total	200	100
Level of Education			
	Master's Degree	23	11.5
	Bachelor's Degree	79	39.5
	Associates' Degree	56	28
	Other (i.e. training, high school)	35	17.5
	No education	7	3.5
	Total	200	100

Figure 2. *Occupation and Educational Breakdown*

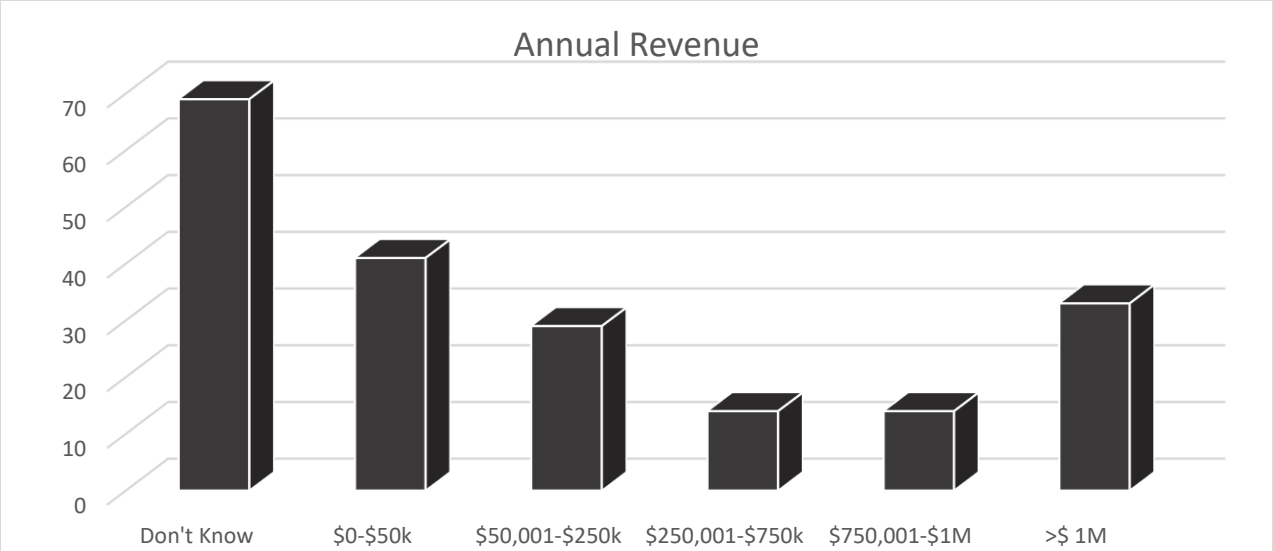

Figure 4. *Annual Revenue*

Primary Disaster Recovery Method Option		
	N	Percentage
Traditional Backup	105	52.50%
Network Function Virtualization	95	47.50%

Figure 5. *Backup Method Selection*

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I.for EXP(B) Lower	Upper
What was your education level?	.288	.382	.568	1	.451	1.333		
What was your education level? (1)	.118	.990	.014	1	.905	1.125	.162	7.824
What was your education level? (2)	-1.936	.620	9.757	1	.002	.144	.043	.486
What was your education level? (3)	-.150	.464	.104	1	.747	.861	.347	2.137
What was your education level? (4)	.405	.629	.415	1	.519	1.500	.437	5.148

Note: base= other (i.e. training, high school), 1=associate degree, 2=bachelor's degree, 3=master's degree, 4=PhD or doctorate,

Figure 6. *Education Analysis*

Recovery Work Experience

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I.for EXP(B) Lower	Upper
How many years have your work in IT disaster recovery?(1)	.351	.636	.305	1	.581	1.420	.408	4.939
How many years have your work in IT disaster recovery?(2)	.679	.552	1.517	1	.218	1.973	.669	5.816
How many years have your work in IT disaster recovery?(3)	-.525	.887	.349	1	.555	.592	.104	3.370
How many years have your work in IT disaster recovery?(5)	-.169	.194	.755	1	.385	.845		

Figure 7. *Recovery Experience Analysis*

Profession

	B	S.E.	Wald	df	Sig.	Exp(B)
Which of the]following best describes your job title?	-.201	.26	.598	1	.439	.82
Which of the]following best describes your job title?(1)	.114	.492	.053	1	.817	1.120
Which of the]following best describes your job title?(2)	.424	.466	.826	1	.363	1.528
Which of the]following best describes your job title?(3)	.201	.538	.139	1	.709	1.222
Which of the]following best describes your job title?(4)	-.136	.640	.045	1	.832	.873

Note: base=entry level, 1=intermediate, 2=frontline management, 3=senior management, 4=owner/executive/c-level

Figure 8. *Profession Analysis*

Demographic Variable		N	Percentage
Years of Experience			
	5 to 7 years	157	78.5
	8 to 10 years	14	7
	11 to 13 years	18	9
	15 or more years	11	5.5
	Total	200	100

Figure 9. *Recovery Work Experience*

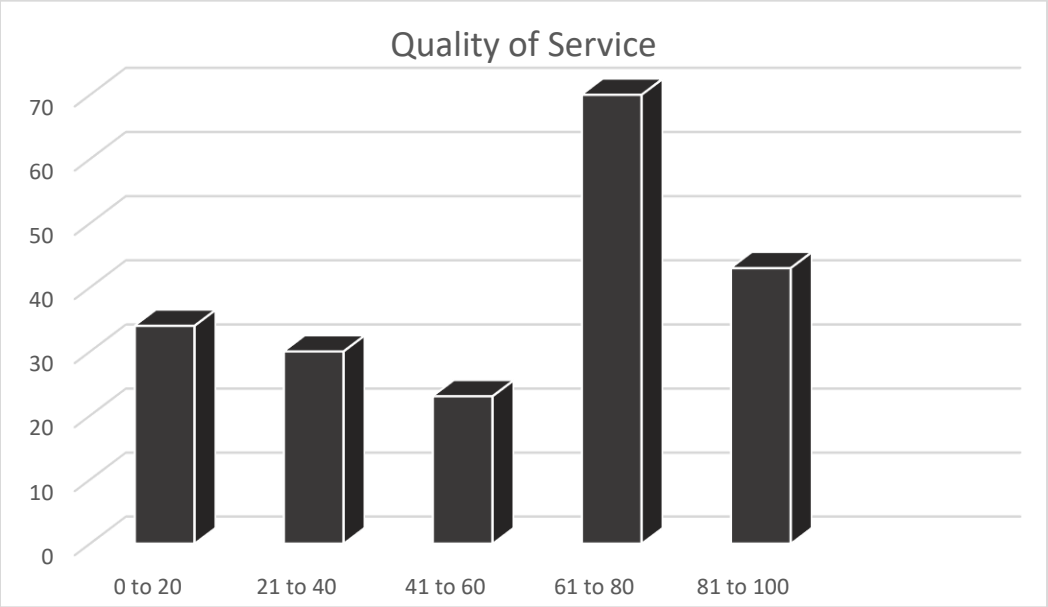

Figure 10. *Quality of Data Recovery Process*

The Promise and Peril of Drone Delivery Systems

Victoria Fowler
Victoria.fowler@lowes.com
Lowes Companies, Inc.
Mooresville, North Carolina 28117, USA

Austin Eggers
eggeraf@appstate.edu
Department of Finance, Banking, & Insurance

Sandra A. Vannoy
vannoysa@appstate.edu
Department of Computer Information Systems

B. Dawn Medlin
medlinbd@appstate.edu
Department of Computer Information Systems

Appalachian State University
Boone, North Carolina 28608, USA

Abstract

Despite increasing demand for quick product delivery in today's supply chains, delivery by drone is relatively rare in the United States. Security and privacy concerns along with legislative issues are often cited as barriers to the adoption of home and commercial drone delivery services. The purpose of this study is to examine the current state of drone deliveries, and to identify some of the adoption barriers as well as factors that contribute to the adoption of drone delivery services. Interestingly, the study shows several factors that affect an individual's inclination to adopt delivery by drones such as rural versus urban locations, drone ownership, and propensity to shop online. Academic and practical implications are drawn from these findings to conclude this study.

Keywords: Drone, Supply Chain Management, Logistics, Legislation, Privacy, Security

1. INTRODUCTION

Supply Chain Management (SCM) has been an integral part of our business history. With the integration of technology into supply chain management processes, supply chains can be used to provide quicker deliveries of products and services. A supply chain involves various participants such as customers, vendors, and others who perform a sequence of tasks or activities that can move physical goods or services from one location to another (Crandall et al., 2015). Therefore, each supplier, vendor, and customer is linked together through the transfer of goods, information, services and payments.

The term "logistics" is often used synonymously with supply chain management. While, logistics focuses more on the movement and coordination of goods and services, supply chain management is the overarching theme of the

entire operation. Ultimately, logistics and supply chain management have become key factors in achieving a competitive advantage in the marketplace. Recently, many industries have begun to pay closer attention to the potential benefits of smart supply chain decisions and the immediate impact upon the company's bottom line.

In an effort to use logistics toward positive impacts upon the bottom line, companies such as Amazon and Walmart are continually seeking ways to move products faster. In 2018, Amazon reported that over 60% of its US consumers were Prime members, paying a premium in order to receive goods in two days without paying additional shipping costs (Kuntze et al., 2018). One way that Amazon and other companies are addressing their. commitment to better logistics is by using drones to deliver products efficiently and lower cost than package and service deliveries.

As an, example Amazon began employing drone deliveries in 2013 as they raised the bar for other companies around the globe, announcing the implementation of Prime Air Drone Delivery. The Amazon announcement was a large step towards the adoption and use of logistics to further enhance product and service deliveries, while enhancing the bottom line. However, after receiving little to no support in the United States, Amazon moved its efforts in 2016 to a more supportive global marketplace in Cambridge, England. The United Kingdom hastily permitted Amazon's continuation of the exploration of drone deliveries (Abdulla, 2017). With the United States' Federal Aviation Association (FAA) realization that drone deliveries were behind in the U.S., they have become more active in addressing and revising airspace restrictions, allowing for more forms of drone delivery possibilities.

In the last several years, delivery companies such as Flirtey have completed several FAA-approved drone deliveries, including medical supplies to remote area medical health clinics such as in Wise, Virginia, in 2015. Additionally, Domino's Pizza Company is currently delivering pizzas by drones in some areas. Walmart has launched a small pilot program in Fayetteville, North Carolina, delivering packages weighing up to 6.6 pounds within a 6.2 miles round trip (Vincent, 2020). In October 2019, UPS (United Parcel Service) received U.S. Government approval to operate a drone airline and made an inaugural flight from WakeMed's hospital campus in Raleigh, N.C. ("UPS Flight Forward Attains FAA's First Full Approval For Drone Airline," 2020). The company has also been approved for the use of drones that weigh 10 pounds or less and can cover a 30-minute flight time.

Drone delivery has also helped to address "the last mile" issue. The last mile is a vital portion of supply chain logistics, as it generally consists of approximately 28% of the overall cost of the delivery transaction. Therefore, a major factor in ensuring consumer satisfaction is making sure that the right item is delivered at the right time. Companies adopting the use of drones, both in delivery throughout the entire stage of the process as well as the last mile, can significantly help in increasing overall efficiency and subsequently decreasing the total time of the delivery, thus addressing time expectations of consumers, suppliers, and vendors.

Given the new emphasis upon drones for delivery of products, more investigation is needed to better understand both the positive and negative impacts. While drones seem to offer an array of benefits, including cheaper costs and faster deliveries, there could also appear negative consequences. Little is known about consumers' perceptions of this new delivery phenomenon, nor do we fully understand the impacts upon traditional delivery methods. Furthermore, does existing policy fully address drones, or is additional legislation needed?

The purpose of this study is to increase understanding of people's perceptions of drone delivery. In the following sections we present a literature review comprising our current understanding of drones as a delivery mechanism, legislative issues, and matters of security and privacy. A survey-based study was conducted and findings are presented. We conclude with recommendations and suggestions for future research.

2. LITERATURE REVIEW

Drones are generally identified as unmanned aerial vehicles (UAV) or unmanned aircraft systems (UAS), essentially flying robots that can be controlled remotely or fly autonomously through embedded software and sensors that interface with global positioning systems (GPS). These unmanned flying robots have been classified based upon their size, intended use, flight range, speed, power system, among other categories (Hassanalian & Abdelkefi, 2017). Drones evolved from the military, which used them initially for intelligence gathering, and

were further expanded for use as weapons and supplies carriers beginning in the early 2000s. They have been especially useful to strike specific targets, and without harming innocent civilians.

Much of the world has quickly outpaced the United States in terms of home and commercial use of drones by dramatically loosening governmental restrictions, as is the case with Poland and South Africa (Smith, 2016). McNeal (2012) suggested that the emergence of drones into the general public in the United States occurred due to the FAA Modernization and Reform Act of 2012, which loosened restrictions and provided greater airspace for drone flight. Also, in 2015 the FAA granted hundreds of new exemptions for companies to operate drones in the commercial segment including insurance, construction, and agriculture, but most of these exemptions (over 90%) were granted to small businesses having fewer than 10 employees (Joshi, 2017).

Placing drones within the congested nature of commercial airspace in the United States has proven quite complex, contributing to the United States' questioning the viability of the use of drones for commercial purposes (Atwater, 2015). Nonetheless, the promise of drone usage within the commercial realm is growing, with the global market expected to surpass $120 billion worldwide by 2021 (Joshi, 2017).

With encouragement from governmental bodies as well as changes in regulations in the commercial use of airspace, businesses around the world are starting to enter the consumer drone delivery market. Beyond simple convenience to the consumer, drone delivery offers much promise in terms of the delivery of medicine and food in hard to reach areas. Furthermore, drones can often provide services or deliveries to allow for a last mile delivery to the home, which can offer significant reductions in CO2 emissions (Goodchild & Toy, 2017).

In order to compete in the global market place for drones, in October 2017, then President of the United States, Barack Obama, approved a UAS Integration Pilot Program. The program was created to provide an opportunity for local governments to partner with private sector organizations to accelerate safe UAS integration into national airspace. The program was touted as expecting to provide immediate opportunities for new and expanding commercial UAS operations.

Legislative Issues

A variety of laws may be applicable to drones and their usage including trespassing, publication of public facts, and stalking and harassment (Vallesenor, 2013). To complicate things further, different localities such as states and towns may each have differing laws in relation to airspace usage according to federal legislation.

The FAA enacted the FAA Modernization and Reform Act of 2012 (FMRA) that initiated the integration of unmanned aircraft systems (UAS), or "drones," into the national airspace by September 2015. Under federal law, all UAVs must apply to the FAA for permission to fly unless they fall under the exception clause (Thompson, 2015).

The process for obtaining permission to operate drones differs depending on whether the drones are to be operated by private or public commercial operators. In the aviation industry, rules and regulations guiding flight are imposed to ensure safety. Some rules have been applied to UAV's so that the UAV's are operated for legitimate purposes only and not to act as a distraction or threat to the security of people or other items. It is important that organizations as well as companies who need to fly manned aircraft apply for an AOC (air operator certificate). These restrictions can be strict and can also be put in place regarding the ownership and use of the drone. With these restrictions in place the government can monitor airspace usage and put in measures the unapproved use of drones.

One of the key takeaways from the 2012 legislation is the visual line-of-sight (VLOS) mandate. VLOS ensures that the pilot will only operate the drone as far as he or she can see. Everyone's vision is different, but the drone would not be legally able to travel very far. It is expected that it will take time for the FAA to further loosen restrictions in order to address issues such as these. With the use of drones in both commercial and home deliveries it will be quite difficult to always maintain a line of sight. Therefore, it is assumed that newly adopted FAA regulations may relax some of the regulations for specific classes of UAS operations (Schlag, 2017) and companies may apply for waivers from some restrictions, including VLOS ("Part 107 Waivers," n.d.).

Amazon was one of the first companies to receive approval from the FAA to operate its fleet of Air Prime delivery drones in the United

States. Amazon's certification granted in 2010 will also grant the company an exemption under Part 135 of the FAA regulations which will allow the business to carry property on small drones beyond the visual line of sight of the operator (Palmer, 2020).

Since that time several companies have requested waivers from the FAA to promote commercial drone deliveries. In April 2019, the Alphabet-owned Wing Company became the first drone delivery company to receive FAA approval for commercial deliveries in the United States after implementing many of the safety regulations required of a traditional airline (Jones, 2019). In that same year, the United Parcel Service further obtained permission from the FAA to fly its new fleet of drones as an airline. ("UPS Flight Forward Attains FAA's First Full Approval For Drone Airline," 2019).

Focusing on the privacy and safety concerns of commercial drone operations, the FAA passed a federal law in December 2015 requiring all drones weighing over 250g and their users to be registered online. The law was partly enacted as a result of the 1133 reported cases of unsafe drone usage reported to the FAA that year (FAA.gov). Due to the increasing number of UAVs it was posited that with this increase comes the possibility of technical failure either due to the technology or users' experiences. As a result of this law, a user without a certificate, and even on their own property, can face both civil and criminal sanctions including fines and imprisonment.

Further prompting the use of drone technology, in October 2017, President Donald Trump signed a memo to the Department of Transportation (DOT), directing them to begin the process of developing rules to allow commercial drone operators to fly more freely in the United States. The memo directed the DOT to take proposals from local, state, and tribal leaders over several months, and then select the most promising proposals (Stewart, 2017).

As of 2020, the US Department of Transportation has selected 10 state, local and tribal governments as participants. It is expected that this program will help to address some of the most significant challenges to integrating drones into the national airspace and will reduce risks to public safety and security (U.S. Dept. of Transportation, 2020).
In addition, and despite the many restrictions currently regulating drone usage, it appears government agencies are beginning to recognize the practicality and inevitability of commercial drone deliveries. As noted on December 28, 2020, the FAA issued new policies that would allow drones under fifty-five pounds to operate at night and over people (Diaz, 2020). These revised regulations are a significant step forward in the utilization of drone technology in a commercial setting by obviating some of the most obvious and constraining regulatory impediments prohibiting commercial drone usage in the United States.

Even with guidelines in place, it is expected that drone operators whether intentionally or unintentionally may create scenarios whereby they violate privacy and security laws as well as other established legislation.

Privacy and Security Issues
Though the FAA may not have strict rules for drone use in relation to privacy issues, many states and localities have strict Peeping Tom regulations that may apply if a drone were to hover over private residences. However, the FAA is relying on local law enforcement agencies to address this issue.

Outside of the United States legal system, an international framework that exists in the form of the International Covenant on Civil and Political Rights (ICCPR) exists in order to address issues related to security and privacy. In some countries, civil rights may be protected by their constitution, however some of these rights are insufficient to significantly curb the use of drones in the area of visual surveillance. In the United States, the Fourth Amendment is primary to the issue of privacy and UAS operations. Under the Fourth Amendment, Americans are guaranteed a certain right to privacy through the right "to be secure in their persons, houses, papers, and effect against unreasonable searches and seizures" (U. S. Const. amend. IV).

There are dissenting opinions concerning the strength of the Fourth Amendment in relation to consumers and their privacy protections from the use of drones and their capabilities. Some advocates of the U.S. Constitution believe that there will be a much stronger measure of protection against government UAS privacy abuses than is widely appreciated, while others suggest that that there is further need for substantial statutory and common law protections that will protect individuals and their privacy rights.

According to some legal scholars, drones, with their current and projected capabilities, present a perfect storm of issues that fall outside of the current Fourth Amendment jurisprudence, but still appear to implicate the Fourth Amendment (Bomboy, 2014). As drones can travel on public airways at low or high altitudes, undetected and with little or no undue noise, and use technologies to gather an abundance of intimate details and information, law enforcement will likely increasingly use drones for domestic surveillance, and all of these actions will likely propel drones to the forefront of courts' dockets.

The abilities of drones to hover over or enter private property undetected and to capture information significantly offers opportunities for privacy and security breaches. According to several privacy theorists, when privacy is invaded or violated, it is lost (Margulis, 2005). Privacy can be an unclear term that differs among industries, contexts, and consumers. The ambiguity of the word "privacy" becomes apparent when attempting to apply traditional privacy concepts to newer technologies, such as drones. Further, the concept of a "private life" means separation from others and generally includes the ability of one to select the information and mode with which to disclose their personal matters. Privacy can also fluctuate according to cultural, national, individual particularities of a country or region. It has often been associated with the west European culture, where the concept of privacy was developed (Serbua & Rotariua, 2015).

While privacy and data security are important considerations, physical security is also in question. As drones become more popular, increases in accidents are also expected. As for instance, in February 2018 a helicopter crash occurred in South Carolina which was shown most likely to be triggered by a civilian drone, and will most likely not be the last. Though it is noted to be the first drone-related crash of an aircraft in the U.S., it is expected that more of these occurrences will happen as more drones are being purchased (Bloomberg, 2018). The drone nor the owner of this accident could be identified, thus creating another level of justice to be addressed.

Though this may have been the first noted crash, there have been drone near misses that have created serious and almost deadly results. Another example of near misses occurred when a commercial jet and a drone came within 200 feet of colliding near Los Angeles' LAX airport in March 2016 and a JetBlue pilot taking off at JFK Airport reported a near collision with a drone at about 5,800 feet in January of 2017. The FAA chronicled 583 near misses between aircraft and drones between Aug. 21, 2015, and Jan. 31, 2016. That averages out to approximately 116 reported incidents monthly (FAA.gov, 2017).

According to John Villasenor (2013), in his article, Observations from Above: Unmanned Aircraft Systems and Privacy, "Thus, while it is important to proactively consider how to protect against the privacy abuses UAS [Unmanned Aircraft Systems] could make possible, in doing so it is important to recognize the near impossibility of predicting all of the ways that a rapidly developing technology can be used—for good or for ill—in future years."

Understanding the risks and liabilities of using drones that can be taken over by hackers, or even the inside threats of employees, will be an issue that must be addressed (Pozzi, 2014). Furthermore, legislative actions that protect individual's privacy rights such as the Fourth Amendment to the U.S. Constitution will also need to be addressed in relation to individuals and expectations of privacy.

Security, like privacy, has different meanings in different contexts. Arnold Wolfer's (1952) article entitled "National Security as an Ambiguous Symbol" appears to be just as applicable and accurate today as it was in the 1950s. Wolfer stated that the meaning of security is 'the absence of threats to acquired values' (Wolfer, 1952). This statement captures the basic intuitive notion underlying most uses of the term security and can be applied to many different generic situations.

Security, as related to drone technology, leads to a range of concerns that is not typically seen with other emerging technologies. One of the primary issues is the lack of clarity. With all connected devices related to drone operation, there are very few clear rules or regulations indicating the necessary steps to securing drones from being tampered with by malicious hackers (Glaser, 2016). It could be surmised that, organizations are more concerned with their bottom line than the issues of privacy and security, as there are currently only a few legal ramifications.

Drone units are vulnerable to two different kinds of attacks that can corrupt their GPS navigational systems. Spoofing entails the sending of strong, fake GPS signals towards a drone. It is essentially "hijacking" and

redirecting the drone instead of allowing it to follow the intended directions. The drone can then be manipulated to crash or be flown to another destination, such as the attacker's location. This could open the door for employees of drone companies to be held responsible for the consequences of spoofed drone shipments. Since it is very difficult to prove the origin of the navigation signals, it would be challenging to determine who is at fault in this situation. It was not until 2014 that a successful spoofing attack was conducted against a drone by a researcher at the U.S. Department of Homeland Security facility.

Currently, few commercial drones use encryption methods that render them invulnerable to the presently known spoofing attacks, but they are all still susceptible to "jamming." In a jamming attack, the drone is overwhelmed with signals to the GPS antenna. The encryption ensures that no fake signal is mistaken for the true one, but the true signal cannot get through either. Unintended collisions seem to be unavoidable in such scenarios, especially in an unregulated environment (Rao et al., 2016).

As mentioned earlier, the FAA enacted the FAA Modernization and Reform Act of 2012 (FMRA), that called for the integration of unmanned aircraft systems (UAS), or "drones," into the national airspace by September 2015. Unfortunately during that time, as indicated by Thompson (2015), "the substantive legal privacy framework relating to UAS on the federal level has remained relatively static; Congress has enacted no law explicitly regulating the potential privacy impacts of drone flights, the courts have had no occasion to rule on the constitutionality of drone surveillance, and the Federal Aviation Administration (FAA) did not include privacy provisions in its proposed rule on small UAS" (para. 1). Under federal law all UAVs must apply to the FAA for permission to fly, unless they fall under the exception clause. The process for obtaining permission to operate drones differs depending on whether the operator is a public operator or a private commercial operator.

The advantages of drone delivery are enticing, but there are important questions to be addressed. The U.S. Federal Trade Commission has raised several questions surrounding the topic of privacy and security concerns as FTC researchers were able to hack into three different off-the-shelf drones. Furthermore, they took over the camera feed on each drone; for two of the drones, they were able to turn off the aircraft to make it fall from the sky and seize complete control of the flight path (Glass, 2016). While President Obama was in Office, Congress held hearings related to privacy issues and the use of drones, with over half of the states enacting some type of drone legislation after the fact. But once again, the issues of privacy and security were not directly addressed. In fact, in every state where laws were passed, the new legislation focused more on the technology itself, rather than the harm that surveillance, for example, could create (Thompson, 2015).

Surveillance can include both passive and active data collection. This collection of data may include the indiscriminate recording of people in a broad sweep that passively gathers information as it is on the way to deliver or return a product or service. For instance, a drone can use a camera sensor that will locate their customer's address, while simultaneously collecting other types of data in the area. The information obtained is certainly necessary for accurate deliveries, but the collection and storing of such data within the drone's path while searching for a specific address begs the question of the public's right to privacy. Though the delivery or return is to a specifically targeted address, the drone's surveillance may bring forth questions related to the issues of secrecy, autonomy, and anonymity of those in the surrounding area (Thompson, 2015).

In 2013, the U.S. Air Force Intelligence, Surveillance and Reconnaissance (ISR) Agency was streaming over 7 terabytes of data a day into their system from drones. That's about 1,600 hours every single day as early as 2013 (Arash, 2017). Between the public and private sector, that number is expected to quickly increase. With that much data coming in, the question remains "What are they doing with it once they've collected this info?" (Arash, 2017).

According to Jeff McCandless, Founder and CEO of Project44, "Amazon can leverage information about your vehicles, the exterior of your home and any property visible from the outside and use that to market related products to people. They can even obtain information about when people are home, when they are outside, and what activities that they may be participating in. From a consumer's perspective, this may be unnerving.

3. RESEARCH METHODOLOGY

Data Collection

A 22-question online survey was developed to collect data on the public's perspective on home

and commercial drone deliveries and the related issues of legislation, privacy and security. A pilot study was conducted with thirteen respondents who best represented the typical general population. After receiving feedback from the pilot study, several changes were implemented to improve the clarity of the instrument. A link to the survey was posted on Facebook, LinkedIn, and emailed to other participants to include as wide a range as possible of individuals representing the general population in the United States. A total of 227 usable surveys were collected.

Of the 227 respondents, approximately 70% fell between the ages of 18-25 years old, with the overall age range falling from 18 to 83 years. Fifty-two percent of the respondents were male, with the remaining 48 percent being female. Within the housing segment, 56.83% of the respondents were urban dwellers and 43.18% were rural dwellers. Additionally, more than half of the respondents answered that they shop online approximately once per month. Most of the respondents did not own a drone, but approximately 11% intended to buy one in the future. Of the 227 respondents, over 25% of them have had personal information stolen at some point in their lives (see Table 1).

Table 1. Descriptive Statistics of Categorical Variables

Variables	Description	Frequency	Percent
Age	18-25	159	70.05
	26-35	23	10.12
	36-45	7	3.08
	46 +	38	16.72
Gender	Male	118	51.98
	Female	109	48.02
Housing	Urban	129	56.83
	Rural	98	43.17
Online Shopping	2-3 Times per Week	18	7.93
	Once per Week	64	28.19
	Once per Month	124	54.63
	Once per Year	17	7.49
	Do not shop online	4	1.76
Own a drone	Yes, I own a drone	15	6.61
	No, but I intend to buy one	25	11.01
	No, I do not own a drone	187	82.38
Information Stolen	Yes	57	25.11
	No	170	74.89

Furthermore, the survey contained questions based on consumer perceptions and attitudes which were measured on a Likert scale anchored by 1 = Not at All and 5 = Extremely or 1 = Extremely Unlikely and 5 = Extremely Likely. The dependent variable, Intention to Use Drones, was measured on a scale of 1 = Extremely Unlikely and 5 = Extremely Likely (see Table 2). Like variables were then grouped and renamed according to their factor loadings. The loadings of exploratory factor analysis show that the items within each question highly loaded with their corresponding latent constructs showing sufficient discriminant validity. Prior to factor analysis the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO = .789) and Bartlett's Test of Sphericity (p = .000) were conducted. Items were maintained to make up three factors. The latent constructs are named, legislation, feelings, and skepticism. Indicator validity can be assumed if all indicator loadings are higher than the threshold of .70 (Chin, 2010). Items with loadings below .70 were discarded (see Table 2).

Analysis and Results

In this research, factor analysis and step-wise linear regression was conducted using IBM SPSS Version 24. After analyzing the data through visual representation in addition to skewness and kurtosis measures, the continuous variables appear to be normally distributed. In order to determine the degree of multicollinearity, variance inflation factors (VIF) are calculated. The VIFs indicate that there is no multicollinearity problem within this model, since they are all less than 10 (Chin, 2010).

The results of the stepwise regression analysis as shown below in Table 3, suggest that consumers are more likely, and not surprisingly so, to choose drone deliveries if they include cheaper shipping costs and faster deliveries. While the consumers' perspective of drone legislation, feelings of skepticism, and their frequency of online shopping also played a role, shipping cost and delivery speed again played a primary role in their decision.

Table 2. Descriptive Statistics and Factor Loadings of Continuous Variables

Description	Construct	Loadings	Mean	Std Dev
How would you feel if you saw a drone flying near your home?	Excited/ Feelings	.832	2.69	1.21
	Curious/ Feelings	.832	3.74	1.19
	Nervous/ Skepticism	.781	2.69	1.27
Identify your level of concern for the following statement: I am concerned that delivery drones will collect personal information for other purposes without my permission	Skepticism	.780	3.04	1.26
Identify your level of concern for the following statement: I am concerned that too much of my personal information will be collected during drone deliveries.	Skepticism	.871	2.82	1.26
Identify your level of concern for the following statement: I am concerned about my privacy during drone deliveries.	Skepticism	.853	2.90	1.33
How likely are you to believe the following statement: I believe current legislations that protect personal privacy from drone delivery services are serious against unauthorized access?	Legislation	.725	2.56	1.02
How likely are you to believe the following statement: I believe current legislations that protect personal privacy from drone delivery services are enough to combat contemporary technologies?	Legislation	.882	2.33	1.04
How likely are you to believe the following statement: I believe current legislations that protect personal privacy from drone delivery services are strong enough to protect my personal privacy?	Legislation	.792	2.38	1.10

Note: Likert Scale 1-5

Table 3. Regression Analysis Results

Model	Unstd B	Std Err	Std	Model	Unstd B	Std. Err
(Constant)	1.519	.416		3.647	.000	
Shipping Cost	.282	.088	.314	3.200	.002	4.552
Delivery Speed	.262	.087	.293	2.991	.003	4.555
Legislation	.249	.072	.167	3.436	.001	1.113
Skepticism	-.226	.064	-.187	-3.531	.001	1.328
Frequency	-.187	.075	-.114	-2.482	.014	1.003

The final model eliminated six factors: Age, Gender, Housing, Owning a Drone, Having Information Stolen, and Feelings. Interestingly, these demographics seem to be irrelevant to consumers' perceptions of drone deliveries. Initially, it was assumed age would influence decisions, since older individuals are generally less trusting of technology (Vaportzis et al., 2017). Since the participants were almost perfectly split between genders, it would have been easy to see if one gender had a preference over the other. It was also surmised that if a consumer owned a drone and was familiar with how they operate, they would automatically be more open to drone deliveries. However, these initial assumptions were not supported.

Additionally, the results indicated that consumers are more than likely not well-versed in current legislation concerning drone usage. Therefore, their decisions about the use of drones would not necessarily be based upon what is or what is not legal. Even if an individual orders online packages every day, there is not enough evidence to demonstration a significant impact upon their decision to choose drone deliveries based upon their privacy and security concerns. All factors are outweighed by the consumer's desire for faster and cheaper deliveries.

4. CONCLUSION

Our study indicates that consumers do indeed value cheap and fast delivery, regardless of age, gender, or even concerns about privacy and security. Given consumer demand as well as positive impacts in the supply chain, it is expected that drone deliveries will increase.

The final question of the survey allowed participants to fill in what they would like to see implemented as it relates to drone delivery. Of the 122 that chose to respond to this question, many of them suggested new laws surrounding data collection, noise pollution controls, and delivery insurance measures. Others suggested that they would prefer drones not be used for delivery at all.

While we have much yet to learn, the COVID-19 pandemic of 2020 has further emphasized the importance of alternative delivery methods. We have witnessed the need for deliveries of items like prescriptions, food, educational supplies, etc., as individuals are working, studying, and even quarantined in their homes. While our study showed that fast and cheap delivery is important to the consumer, we need to keep in mind that this is a nascent phenomenon. We understand little as of yet about the true impact of drone deliveries on a mass scale and further and additional research in needed.

5. REFERENCES

Abdulla, H. (2017). Amazon mulls drone hubs on trains, ships and trucks. Retrieved from https://www.juststyle.com/news/amazon-mulls-drone-hubs-on-trains-ships-and-trucks_id131444.aspx.

Air we go: UPS in drone delivery. (2017, February). Retrieved from http://link.galegroup.com/apps/doc/A482080053/BIC1?u=boon41269&xid=3adae98e.

Arash, A. (2017). Only Taking What They Want. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/01/03/data-from-drones-how-companies-cancollect-store-and-use-these-insights/#578da298397d.

Atwater, D. (2015). The Commercial Global Drone Market: Emerging Opportunities for Social and Environmental Uses of UAVs. Graziadio Business Review 18(2).

Bamburry, D. (2015). Drones: Designed for product delivery. Wiley Online Library. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/drev.10313/pdf.

Behavioral Targeting (2017). Retrieved from https://www.bluefountainmedia.com/glossary/behavioraltargeting/.

Chin, W.W. (2010). How to Write Up and Report PLS Analyses. Handbook of Partial Least Squares, Springer, Berlin Heidelberg, pp. 655-690.

Collins, J. (2016). Drones: Is drone delivery simply pie in the sky? Retrieved from https://www.journalofaccountancy.com/issues/2016/dec/drone-delivery.html.

Crandall, R.E., Crandall, W. R., & Chen, C.C. (2015). Principles of Supply Chain Management. CRC Press, Boca Raton.

Diaz, J. (2020). U.S. Announces New Rules for Drones and their Operators. Retried from https://www.npr.org/2020/12/29/951010863/u-s-announces-new-rules-for-drones-and-their-operators.

DHL Completes Three-Month Test of Delivery Drone (2016). Retrieved from

http://www.ttnews.com/articles/dhl-completes-three-month-test-delivery-drone.

Donahoe, S. (2016). Amazon and Drone Delivery: The Pros and Cons. Retrieved from http://imsuccesscenter.com/amazon-and-drone-delivery-the-pros-and-cons/.

Etherington, D. (2017). Google's Project Wing team takes a key step towards making drone delivery real. Retrieved from https://techcrunch.com/2017/06/07/googles-project-wing-team-takes-a-key-steptowards-making-drone-delivery-real/.

UPS Flight Forward Attains FAA's First Full Approval For Drone Airline. Retrieved from https://pressroom.ups.com/pressroom/ContentDetailsViewer.page?ConceptType=PressReleases&id=1569933965476-404.

Flirtey Continues to Lead Drone Delivery Industry (2017, July). PR Newswire. Retrieved from http://link.galegroup.com/apps/doc/A499279501/BIC1?u=boon41269&xid=55fd4fed.

Gilchrist, K. (2017, August). World's first drone delivery service launches in Iceland. Retrieved from https://www.cnbc.com/2017/08/22/worlds-first-drone-delivery-service-launches-in-iceland.html.

Glasser, A. (2016). Obama says the U.S. government still doesn't know who shut down the internet last week. Retrieved from https://www.recode.net/2016/10/25/13406546/internet-shutdown-outagebotnet-attack-ddos-denial-of-service.

Goodchild, A., & Toy, J. (2017). Delivery by drone: An evaluation of unmanned aerial vehicle technology in reducing CO 2 emissions in the delivery service industry. Transportation Research Part D: Transport and Environment. In press.

Hassanalian, M., & Abdelkefi, A. (2017). Classifications, applications, and design challenges of drones: A review. Progress in Aerospace Sciences. 91, 99-131.

Jacobsen, M. (2016). The Promise of Drones. Harvard International Review, 37 (3), 27-31.

Joshi, D. (2017, August). Commercial Unmanned Aerial Vehicle (UAV) Market Analysis – Industry trends, companies and what you should know. Retrieved from http://www.businessinsider.com/commercial-uavmarket-analysis-2017-8.

Kang, Hyun. (2013, May). The prevention and handling of the missing data. Korean Journal of Anesthesiology. www.ncbi.nlm.nih.gov/pmc/articles/PMC3668100/

Krol, C. (2015, November). Is delivery by drone the future of shopping? Telegraph Online Biography in Context. Retrieved from http://link.galegroup.com/apps/doc/A433568818/BIC1?u=boon4126.

Kuntze, C., Martin, A., Regnier, C., & Silva, I. (2018). Deliver on time or pay the fine: Speed and precision as the new supply-chain drivers. Retrieved from https://www.mckinsey.com/business-functions/operations/our-insights/deliver-on-time-or-pay-the-fine-speed-and-precision-as-the-new-supply-chain-drivers#.

Jones, P. (2019, April). Alphabet's Wing drones get FAA approval to make deliveries in the U.S. Retrieved from www.theverge.com2019/4/23/18512658/google-alphabet-wing-drone-delivery-servce-faa-approval-commercial-deliveries.

Laguna, J., & Marklund, M. (2005). Business Process Modeling, Simulation, and Design. Prentice Hall, New Jersey.

McNeal, G. (2012, April). A primer on domestic drones: Legal, policy, and privacy implications. Forbes. Retrieved from www.forbes.com/sites/gregorymcneal/2012/04/10/a-primeron-domestic-drones-andprivacy-implications/.

Margulis, S. (2005). Privacy as a Social Issue and Behavioral Concept. Journal of Social Issues, 59(2), 243-261.

Murray, C. C., & Chu, A. G. (2015). The flying sidekick traveling salesman problem: Optimization of drone assisted parcel delivery. Transportation Research Part C: Emerging Technologies, 54, 86-109.

Palmer, Annie. (2020). Amazon wins FAA approval for Prime Air drone delivery fleet. Retrieved from https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html.

Part 107 Waivers. (2019). Retrieved from https://www.faa.gov/uas/commercial_operators/part_107_waivers/.

Pogue, David. (2016). Amazon reveals details about its crazy drone delivery program. Yahoo Tech. Retrieved from

https://www.yahoo.com/tech/exclusive-amazon-reveals-detailsabout-1343951725436982.html.

Pozzi, S. R. (2014). Drones in our future. Best's Review, 115(2), 56. Retrieved from http://web.b.ebscohost.com/ehost/detail/detail?vid=2&sid=f34c5299-d508-4ea9-860d573932ebf745%40sessionmgr113&hid=106&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=bth&AN=96327351.

Pritchard, M. (2013, January). Who Are the Joneses and Why Are We Trying to Keep Up With Them? Retrieved from https://www.huffingtonpost.com/mary-pritchard/keeping-up-with-thejoneses_b_2467957.html.

Rao, B., Gopi, A., & Maione, R. (2016). The societal impact of commercial drones. Technology in Society, 45, 83-90.

Rubin, E. (2017, August). Buzzing Over BDS, Israeli Firm Launches World's First Drone Delivery Service. Retrieved from https://www.haaretz.com/israel-news/business/1.809072.

Rupprecht, J. (2018, January 29). Drone Delivery – 3 Big Legal Problems (2018) -. Retrieved https://jrupprechtlaw.com/amazon-drone-delivery-3-major-legal-problems-amazon-prime-air.

Serba, R. (2015). 22nd International Economic Conference – IECS 2015 "Economic Prospects in the Context of Growing Global and Regional Interdependencies", IECS 2015.

Sifton, J. (2012, February). A brief history of drones. The Nation. Retrieved from http://www.thenation.com/article/166124/briefhistory-drones.

Smith, G. (2016, May). Here Comes the Latest Drone Army. Retrieved from http://fortune.com/2016/05/09/here-comes-the-latest-drone-army/.

Thompson, R. (2015, March). Domestic Drones and Privacy: A Primer. Retrieved from https://fas.org/sgp/crs/misc/R43965.pdf.

Unmanned Aircraft Systems. (2012). Retrieved from FAA Seal. Retrieved from www.faa.gov/uas/.

U. S. Const. art. IV.

U.S. Department of Transportation. Retrieved from https://www.transportation.gov/connections/unmanned-aircraft-systems-integration-pilot-program-selectees-0 on June f28.

Vaportzis, E., Clausen, M. G., & Gow, A. J. (Oct. 7, 2017). Older Adults Perceptions of Technology and Barriers to Interacting with Tablet Computers: A Focus Group Study. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5649151/.

Villasenor, J. (2013). Observations from Above: Unmanned Aircraft Systems and Privacy. Retrieved from https://pdfs.semanticscholar.org/ec9a/8458e8fe4c2511c2e18f557eae8ddedb2289.pdf.

Vincent, J. (2020). Walmart begins testing drone deliveries for household goods and groceries. Retrieved from https://www.theverge.com/2020/9/10/21430280/walmart-drone-delivery-pilot-program-north-carolina-flytrex.

Towards a Leader-Driven Supply Chain Cybersecurity Framework

Manoj Vanajakumari
Business Analytics
manojuv@uncw.edu

Sudip Mittal
Computer Science
mittals@uncw.edu

Geoff Stoker
Information Systems
stokerg@uncw.edu

Ulku Clark
Information Systems
clarku@uncw.edu

University of North Carolina Wilmington
Wilmington, NC 28403

Kasey Miler
Kcmiller1@nps.edu
Naval Postgraduate School
Monterey, CA 93943

Abstract

Supply chains (SC) often span multiple cultures, countries, and time zones with security concerns that, at a high level, can be grouped into two broad areas: 1) products/assets; 2) information technology (IT). SCs can achieve higher operational efficiency if participating entities are highly connected since rapid information transfer helps SC participants be agile, adaptable, and aligned. To be antifragile, a key requirement of highly interconnected systems is strong overall cybersecurity. We posit that individual partners independently enhancing their security may not sufficiently improve the overall SC cybersecurity posture; rather, what is required is that coordinated cybersecurity efforts be driven by the SC's most powerful member. We propose a conceptual framework for the leader in the SC that involves two broad elements: 1) supplier/member selection; 2) continuous training, development, and risk assessment of SC members from a cybersecurity perspective. A use case is provided to expound on the presented ideas.

Keywords: Supply Chain, Cybersecurity, Framework, Powerful Member

1. INTRODUCTION

The National Institute of Standards and Technology (NIST) states that:

> Supply chains are complex, globally distributed, and interconnected sets of resources and processes between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user (NIST, 2018b, p. 15).

Supply Chain (SC) entities include suppliers, manufacturers, wholesalers/distributors, and retailers. SCs that focus exclusively on speed and cost often break down over time, so to be resilient and effective, SCs require agility, adaptability, and alignment (Lee, 2004). Agility is needed to accommodate sudden changes in supply and demand; adaptability helps SCs respond to market changes; and better alignment is gained via strong collaboration among SC members. These traits develop among SC entities during long-term relationships during which they share information on a timely basis and adapt new technology as needed.

Power asymmetries exist in SCs (Munson, Rosenblatt, & Rosenblat, 1999). Certain characteristics confer organizational power of one SC member over the others e.g., a partner has reward power if it can help other SC members achieve their goals. Other types include expert, referent, coercive, and legitimate power. For example, Walmart has huge financial clout and can require suppliers to do packaging, RFID tagging, and delivery in the way that best suits Walmart, even if some suppliers would have to operate sub-optimally. Often the power of one member is sufficiently transcendent that the SC is recognized by that member's name, e.g. Walmart, Target, Boeing, etc. We will generically refer to the partner with the most organizational power as the *powerful member*. The terms leader and powerful member are equivalent in the context of this paper, and we will use powerful member from this point forward.

A cybersecurity disruption to any partner can cause dysfunction along the entire SC. Securing the information and information technology (IT) along the SC is extremely difficult given the degree of complexity involved and suggests several questions:

- Who has overall responsibility for SC cybersecurity?
- What do those responsibilities entail?
- How would a cybersecurity risk assessment of the SC be done?

As we will discuss in Section 2, the SC powerful member has an important role to play in SC cybersecurity. That role involves including cybersecurity considerations when selecting new SC members and maintaining a healthy SC ecosystem. Cybersecurity-specific risk assessments involve considerations of people, process, and technology.

Figure 1 depicts a typical stylized SC model. Products/material flow (solid, black arrows) from upstream to downstream. Money and information flow (dotted, gold, two-headed arrows) both upstream and downstream. To facilitate communication and information sharing, SC entities use technologies that link the various partners in an SC forming a chain of cyber-physical systems.

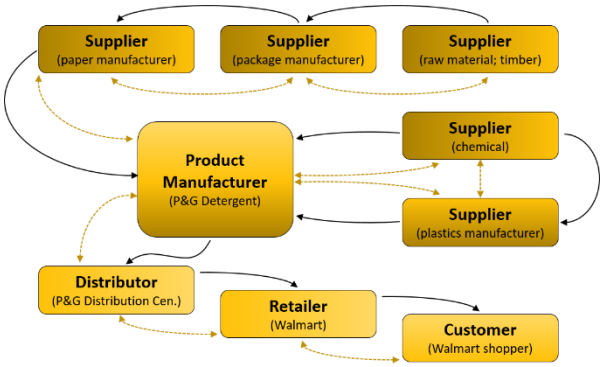

Figure 1 –SC stylized diagram (*products/material: black arrows; funds/information: dotted, gold arrows*)

SC security encompasses both the physical systems (products/assets) and the information technology (IT). Smith, et al., identify the cyber system portion of SCs as a network of IT infrastructures used to connect partners and further define:

> Supply Chain Information Security Risk (SCISR) as degradation or disruption to a supply chain's infrastructure or structural resources resulting from the successful exploitation of IT vulnerabilities by threats within an organization, within the supply chain network, or in the external environment (Smith, Watson, Baker, & Pokorski, 2007).

In this research, we examine the SCISR in the context of cybersecurity risk management.

There have been many reports of large-scale cybersecurity incidents (McCandless & Evans, 2020). Examples include the 2013 Target breach where network credentials were stolen from a third-party HVAC vendor (Krebs, 2014); the 2017 Verizon breach where a software and data firm partner misconfigured a cloud-based repository (UpGuard, 2017); and the 2017 Equifax breach where an open-source software component available from a third-party contained a five-year old flaw (Gutzmer, 2017). A recent survey of companies in the USA, UK, Switzerland, Mexico, and Singapore found that 92% of respondents had suffered a SC-partner-related breach in the previous 12 months (BlueVoyant, 2020).

Mulligan & Schneider report that several past cybersecurity doctrines such as prevention, risk management, and deterrence through accountability did not bear fruit (Mulligan & Schneider, 2011). They recommend viewing cybersecurity as a collective interest like public health and suggest that incentive mechanisms must be in place to prompt system developers, operators, and users to improve information system security.

We suggest that for cybersecurity risk assessment and management to succeed, the powerful member of the SC must take special initiative. The other SC members (non-powerful members – *note: we use this term to differentiate only, not to imply that the other members have no power per se*) are often smaller firms that do not possess the same resources to conduct cybersecurity activities to protect their cyber systems from cyber threats as the powerful member, as well, they often lack perspective on the *bigger picture*.

The vulnerabilities introduced to the SC ecosystem by the least cybersecurity-capable companies weaken the cybersecurity posture of the entire SC since the chain is only as strong as the weakest link. A rigorous analysis of potential SC partners before selection is essential. After selection, the contracts between SC partners need to detail the management of third-party risk in addition to other SC requirements. One example, the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) framework addresses vendor accreditation for cybersecurity and helps determine if contractors are doing due diligence to protect sensitive data that resides on their networks (Webmaster A&S, 2020).

In this paper, we introduce a framework designed to help businesses with SC partner selection and management processes to reduce the risk of cyber-attacks on SC partners' cyber systems. Our framework proposes guidelines on how the powerful member manages the process to mitigate the risks in the SC to an acceptable level.

Failure to protect SC cyber systems could lead to loss of revenue, reputation, and customers. With emerging technologies being integrated into the industrial processes, we are now in the era of Industry 4.0, which is enabled by Artificial Intelligence, Big Data Analytics, Autonomous Robots, Horizontal and Vertical Integration, Internet of Things, Augmented Reality, Additive Manufacturing, Cloud, and Cybersecurity. As empowering as these technologies are for businesses, they make the cyber-systems more complex. The more complex they are, the more vulnerable they are.

Examples of interconnected IT systems for the sake of efficiency are everywhere. Walmart's Retaillink system enables suppliers to successfully support Vendor Managed Inventory initiatives. Through this system, suppliers can see the store-level inventory at any time. Target gives access rights to HVAC vendors to remotely monitor energy consumption at its stores. Lean manufacturing systems require firms to carry as little inventory as possible to support a production schedule. Raw material suppliers have access to shop-floor inventory levels to support Just-in-Time production. It is imperative that the professionals who manage cyber-SC systems have a well-established risk management system in place. The interdependencies between SC partners create additional attack vectors that need to be addressed. A breach that leads to data theft or other unauthorized activity in the systems of any SC component could potentially compromise data of other SC players.

The rest of the paper is organized as follows. In Section 2 we propose a framework for SC cybersecurity. Section 3 provides a short use-case. Our conclusion remarks are in Section 4.

2. CYBERSECURITY FRAMEWORK FOR SUPPLY CHAIN STAKEHOLDERS

2.1 Building the Framework

Efficient suppliers are integral to SC profitability. As discussed above, they also play an important role in keeping the SC secure. The Japanese manufacturing philosophies like Just-in-Time and Toyota Production System view suppliers as long-term partners. Hence, it is critical to identify the right suppliers to join the SC. Building a long-term relationship not only helps the SC meet customer demand effectively, but it also helps secure the SC. Knowing that there is a long-term association with the SC powerful member, the other partners will be more willing to adopt process and technology recommendations to secure the SC.

NIST's Cyber Supply Chain Risk Management (C-SCRM) program started in 2008. The program defines C-SCRM as "the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT [information and operational technology] products and service supply chains" (NIST, 2020). Within NIST's Framework for Improving Critical Infrastructure (FICI), it elaborates that C-SCRM is

> the set of activities necessary to manage cybersecurity risk associated with external parties. More specifically, cyber SCRM addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization (NIST, 2018b, p. 16).

It goes on to explicitly state that the examples provided for how it can be used "are not intended to address C-SCRM comprehensively," thus leaving room for flexible use and extension by practitioners. Our proposed framework is complementary to and fits within the larger FICI and is currently called Stakeholder Cyber Supply Chain Risk Management (SC-SCRM). The elements of the framework are shown in Figure 2.

The framework has two main parts, the Supplier Selection process and what happens after a supplier is selected to become a SC member which is comprised of four key components: Training, Development, Technology, and Risk Assessment (TDTR) – all informed by the Supply Chain Cybersecurity Strategy (SCCS). Readers familiar with concepts like Kaizen (Imai, 1986) may find it helpful to think about the TDTR in the same terms. The SC powerful member can lead SC-SCRM with well-established TDTR components for SC members and by integrating a sound SCCS. The SCCS should be primarily derived from the goals of the powerful member, but with an eye towards synergistic benefit to all SC members. Below, we explain the framework in more detail.

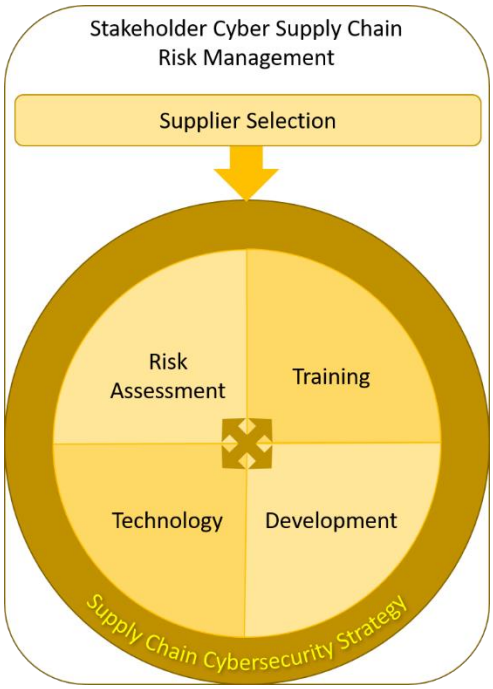

Figure 2 – Framework for Stakeholder Cyber Supply Chain Risk Management (SC-SCRM)

2.2 Supplier Selection Process

The supplier selection process is pivotal in ensuring a working SC-SCRM. To get to these details, we will need first to briefly run through the broad strokes of the larger framework encompassing SC-SCRM.

The risk management process (RMP) has variously been defined by many organizations such as NIST and the International Standards Organisation (ISO). NIST enumerates four components of the RMP as follows (NIST, 2011):

- frame risk – establish the context for risk-based decisions
- assess risk
- respond to risk
- monitor risk, continuously over time

The NIST RMP and information/communication flows among the components are depicted in Figure 3.

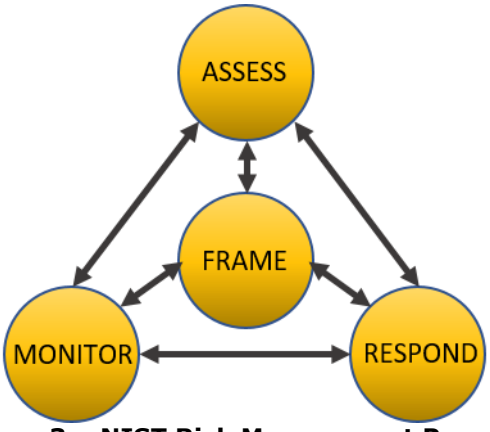

Figure 3 – NIST Risk Management Process; arrows indicated information and communications flows (NIST, 2011, p. 8)

Within NIST's FICI, the framework core expands on the above-mentioned elements to enumerate five functions: Identify, Protect, Detect, Respond, and Recover (Figure 4).

Further, they enumerate four implementation tiers to "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk" (NIST, 2018, p. 8). These tiers range from Partial (Tier 1), which is informal and reactive, to Adaptive (Tier 4), which is agile and risk-informed, and are briefly summarized as follows:

Tier 1, Partial. Cybersecurity risk is managed in an ad hoc/reactive manner; practices are not formalized; generally unaware of cyber SC risks of the products/services provided and used.

Tier 2, Risk Informed. Cybersecurity risk management practices are approved by management; practices may not be organizational-level policy; generally aware of cyber SC risks, but does not act consistently or formally.

Tier 3, Repeatable. Cybersecurity risk management practices are formally approved and organizational policy; generally aware of cyber SC risks and acts formally upon the risks.

Tier 4, Adaptive. Cybersecurity risk management practices are adaptive and informed by previous and current cybersecurity activities; aware of SC risks, contributes to the SC community's understanding of risks; communicates proactively to maintain strong SC relationships.

Figure 4 – Five Functions of NIST's Framework for Improving Critical Infrastructure (NIST, 2018a)

A firm must consider which Tier a potential SC partner needs to occupy before it could become a SC member. This is somewhat analogous to setting ISO certification as a basic qualifier to be a supplier. To mitigate risks to acceptable levels, if the determined prerequisite Tier is lower than Tier 4, a road map for a SC member to gradually reach Tier 4 would minimize the exposure factor of the SC ecosystem. It is important to note that tiers assist in risk management of the power player and do not correspond to the maturity levels (NIST, 2018b).

An extensive list of criteria can be considered during a supplier selection process (Thanaraksakul & Phruksaphanrat, 2009). The list is quite comprehensive but can be broadly classified into five perspectives: (i) Financial (ii) Customer (iii) Internal Business Process, (iv) Learning and Growth, (v) Corporate Social Responsibility. The financial aspect is related to the ability of a vendor to have long term profitability. The customer aspect is related to the ability of the vendor to provide goods and services quickly as the firm's customer requirement changes. The internal business process relates to the vendor's ability to provide quality products and services at the right time and in the right quantities. The learning and growth measure is the flexibility of the vendor to adapt to changing market conditions. And, the corporate social responsibility is the ability of the vendor to be a good citizen company adhering to legal, societal, and environmental commitments.

In addition to the factors listed above, we propose that cybersecurity has reached sufficient importance, that a supplier selection process should explicitly incorporate criteria relevant to the key layers of cybersecurity – people, processes, and technology – explained as follows:

- People refers to having cybersecurity experts with appropriate qualifications in key positions as well as periodically training employees and testing their knowledge in cybersecurity awareness.
- Processes are there to ensure that SC risk tolerance and business objectives are aligned.
- The technology layer refers to having proper technology and tools in place, and that these tools are utilized in the way that would be aligned with the cybersecurity strategy of the powerful member.

An example scorecard template is in Table 1 and would help to rank potential SC participants (we provide a scored example for the use case in section 3). The specific criteria beneath the three key parts are examples and not meant to be comprehensive or specifically required in keeping with the spirit of the flexibility of FICI.

Organizations will want to craft the scorecard with items of specific importance to them and informed by their cybersecurity policy. Good sources for scorecard criteria are the categories and subcategories of the FICI framework core. Evaluating the criteria based on implementation tiers and then summing the result can provide a quantitative manner of comparison where higher scores would indicate a better potential SC partner from a cybersecurity perspective.

2.2 Training

The training component of the framework focuses on the powerful member's strategy on education, training, and awareness of the SC partners in all areas of the selection process: people, processes, and technology. The minimal tier requirement for each SC partner determined by the powerful member provides guidance on the minimal acceptable cyber hygiene levels for the SC ecosystem. Aligned cybersecurity policy and procedures of the SC ecosystem would be a means to make sure that every SC partner maintains the expected minimal cybersecurity posture.

The policies and procedures should detail important items like incident handling, incident monitoring, incident response plan, etc. Each SC partner doing periodic audits of their systems and users is necessary for the integrity of the system and user provisions. Any exploits found through the audits need to be addressed by every partner of the SC with the lead of the powerful member. The policies and procedures should address the management of data and user access for the partners leaving the SC ecosystem.

SC-SCRM Evaluation Scorecard	
People	Tier
CISO	
Network Security Engineer	
Security Analyst	
Etc. …	
Processes	Tier
Cyber Incident Response Plan	
Endpoint Monitoring	
Vulnerability Management	
Etc. …	
Technology	Tier
Email Security	
Firewalls	
Security Log Maintenance	
Etc. …	

Table 1 – Cybersecurity-focused Evaluation Scorecard template for potential SC partners

The training component would address improving the security posture of SC partners. If a partner is at the minimum acceptable tier at selection time, the training, coupled with development process of the framework progressively work towards bringing the partner as close as possible to Tier 4. It is important to note that some supply chain partners may never reach Tier 4 based on their firm size and available resources.

2.3 Development

Supplier development includes activities like site visits and personnel training with the goal of improving the capabilities and performance of the supplier. Since this requires financial investment in suppliers, Talluri, et al. propose optimization models for allocating resources among multiple suppliers to minimize risk and maintain an acceptable level of return (Talluri et al., 2010).

In the context of SC cybersecurity, natural questions to ask include: should the investment be made based on security weakness or should it be done based on the organization's ability to scale up the technological capabilities. Both are important since management may have to optimize the investment in both areas. The dynamic nature of the market requires the

entities to evolve on a continuous basis. The role of the powerful member cannot be emphasized enough to achieve the continuous improvement of the SC. As the business evolves, the organizational goals evolve for the powerful member. When the organizational goals evolve, the cybersecurity strategy evolves as well. This may require that suppliers move up the Tier structure of FICI. The powerful member should take an active role in developing the road map for other members to achieve the required Tier.

2.4 Technology

Industry 4.0 utilizes emerging technologies to improve efficiencies in SCs. Most of the emerging technologies come with unidentified cybersecurity risks. When an emerging technology is introduced to the SC ecosystem, the powerful member should vet the technology and outline the acceptable configuration/use of it for the other partners of the SC before it becomes embedded into the SC.

As an example, when considering embedded automotive network parts, researchers have identified the need to design and implement key security mechanisms to improve the cybersecurity posture of the parts, and, ultimately, the automobiles being produced, specifically: communication encryption, anomaly detection, and embedded software integrity (Studnia et al., 2013). It is likely that this category can be extended to other industries as well, especially where embedded electronic components are used.

One extension is the use of blockchain technology to provide decentralized secure ledgers for SC partners. Blockchain technology is a promising driver of common digital SC standards, but is not currently something that even the largest companies can impose on others and will require real collaboration to make it work end-to-end in a SC (Korpela et al., 2017). As SCs continue to digitize and integrate, many SMBs lack key functionalities (e.g. standards, transaction timestamps, secure information flow) that are already designed into blockchain technology.

There are many benefits that blockchain technology could bring to SCs including:

- tracing the origin (provenance) of the product/process, that is verifiable, thus preventing counterfeits
- improved trust among the members because every member has the same verified information
- improvement in data integrity because any incorrect information can be easily traced to the member who entered it
- IoT (Internet of Things) devices can be easily connected to the SC and the data is available throughout the SC thus ensuring the products conform to the requirements (e.g., pick and pack dates, storage temperatures, etc.)
- financial transactions happen quickly
- helps to achieve JIT production.

The impact of blockchain technology just on reducing counterfeit products could be tremendous. According to a 2018 report, the value of counterfeit goods in 2017 was estimated at $1.2 trillion and is likely to rise 50% to $1.82 trillion by 2020 (Research and Markets, 2017).

2.5 Risk Assessment

Managing SC risk requires a collaborative effort among the members to identify, evaluate, mitigate, and monitor events that may adversely affect the functioning of the SC (Ho et al., 2015). Cybercriminals usually exploit the weakest link in the SC. One study attempting to differentiate sources of security incidents indicates that 23% of SC security incidents involve current partners while 45% involve former partners (PwC, 2014). Hence, the risk management strategies in an SC context must include all partners.

SCs face a myriad of security threats to products/assets as well as information systems. The National Cyber Security Center (NCSC) classifies cybersecurity threats into un-targeted and targeted attacks (NCSC, 2016). Targeted attacks are directed towards a specific entity. Examples include distributed denial of service (DDoS), subverting the supply chain (attacking equipment or software used by the organization), and spear-phishing. Ransomware, phishing, spoofing, and water holing are examples of untargeted attacks as they don't have a specific target. The organizations need to know the weak points in their SCs to ensure a robust risk mitigation strategy (Smith et al., 2007). Ghadge, et al. classify these weak points into three dimensions: technical, human, and physical (Ghadge et al., 2019). Boone suggests that the strength of an SC's defense against cyber threats is only as good as the most susceptible member in the supply chain (Boone, 2017).

Now, we suggest a scorecard for conducting a cybersecurity risk assessment of SC members

assessed from the perspective of the SC powerful member.

NIST has defined risk as

> a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST, 2012, p. 6).

This definition implies:

$$\boldsymbol{impacts} * \boldsymbol{likelihood} = \boldsymbol{risk}$$

Switching the term order, substituting consequences for the word impacts, and further understanding likelihood as the combination of a threat exploiting a vulnerability (NIST, 2012), we can extrapolate to the well-known formula:

$$(\boldsymbol{threat} * \boldsymbol{vulnerability}) * \boldsymbol{consequence} = \boldsymbol{risk}$$

Driving one of the variables in the formula to zero will make the risk go away; however, a zero value for any variable may well require infinite resources and is generally impractical. Hence, the SC members will generally expend resources in a balanced manner to minimize the value of each of the variables.

Table 2 shows the general structure of the proposed risk assessment matrix template integrating the key layers of cybersecurity within the organization of the powerful member, current SC partners, and former partners.

The people aspect ensures that each SC partner employs key, qualified cybersecurity personnel and implements a thorough cybersecurity awareness training program to address one of the biggest threats: insiders. Process evaluation ensures that any changes to SC partner structure do not impact the alignment of that partner within the SC ecosystem. Also, if any changes happen to the powerful member's cybersecurity processes, due to the introduction of new tools for example, the alignment is updated appropriately for each partner. The technology layer ensures that partners update their tools and monitor their use IAW guidelines provided by the powerful member.

	Threat	Vulnerability	Consequence	Risk
Organization 1. People 2. Process 3. Technology				
Current Partners 1. People 2. Process 3. Technology				
Former Partners 1. People 2. Process 3. Technology				
			Total Risk	

Table 2 – Risk Assessment Matrix Template

The primary risk assessment by the powerful member does not preclude each SC partner also conducting assessments in this manner. The most cybersecurity-mature SC will encourage this and have key personnel meet periodically to more thoroughly evaluate the overall cybersecurity risk of the SC ecosystem.

3. SUPPLY CHAIN SUPPLIER SELECTION USE CASE

This lightweight use case is presented as a thought experiment and motivated in part by the 2013 Target breach and the 2017 breach of a casino (DarkTrace, 2017). Hackers stole 40,000,000 credit card numbers and cost Target $202 million after they were able to steal network credentials from a vendor that Target used to provide and monitor refrigeration and HVAC systems. An unnamed casino had its list of wealthy patrons stolen through a compromised "smart" fish tank thermometer used to monitor and regulate temperature, salinity, and feeding schedules.

We imagine a company, BigAg, selling agricultural products wholesale to supermarkets. Considering current pandemic conditions, BigAg wants to adjust their business practices to gain better visibility on the daily health of the workers throughout their SC. One way they would like to do this is to have worker temperatures regularly reported to the BigAg HQ.

BigAg looks for a new SC partner to handle the gathering of the worker temperatures and reduces the viable candidates to three different companies with different solutions. ManualTemp (MT) company hires local health care workers part-time to take worker temperatures. The data is collected periodically throughout each day in a

traditional manner and reported via apps that workers download to their personal phones. HatTemp (HT) manufactures hats designed to take worker temperatures at time intervals as often as every five minutes and is collected wirelessly. TempStation (TS) installs contactless infrared thermometers at strategic locations around company facilities capable of taking temperatures from up to 15 feet away. The stations can be wired into a network or a wireless access point for wireless transmission of data.

From this sketch, we will present a portion of the process envisioned with the framework as the powerful member considers the supplier selection process and the follow-on TDTR. Table 3 shows a hypothetical abbreviated and consolidated SC-SCRM evaluation scorecard for a few of the very many areas that would be assessed during the selection process.

In this truncated example, we will consider two criteria as exemplars for how the scorecard will be used. First, in the People section of the scorecard, we find that MT does not have anyone formally assigned to the position of a CISO, though someone is handling some of the duties normally associated with that position; HT established the position within the past year; and TS has had the position in place for several years. Second, from the Processes section, we note that Endpoint Monitoring is done by MT in an ad-hoc manner (employees whose phones act up are directed to contact tech support); HT and TS have an established and repeatable process for monitoring their hats and infrared thermometers, respectively.

Assuming the full scorecard is like the snippet (Table 3), we expect TS to be selected as the new SC partner due to higher tier scores across the board. (*NOTE: this evaluation is strictly cybersecurity-based; it is entirely reasonable that the selection might be different for other reasons e.g., budget constraints.*)

Carefully considering TempStation's cyber-security posture during selection does not complete the SC-SCRM process, but merely ensures it is well-begun. As long as TS is a SC member, they will need to regularly cycle through the bottom portion of the SC-SCRM (Figure 2) to ensure that training, development, technology, and risk assessment (TDTR) are informed by BigAg's SC cybersecurity strategy and continually improved.

SC-SCRM Evaluation Scorecard			
People	Tier		
	MT	HT	TS
CISO	1	2	3
Network Security Eng	2	2	3
Processes	MT	HT	TS
Cyber Incident Response Plan	1	3	3
Endpoint Monitoring	1	3	3
Technology	MT	HT	TS
Intrusion Detection System	2	3	3
Security Log Maintenance	2	3	4

Table 3 – Abbreviated and Consolidated Example Selection Evaluation Scorecard Comparing ManualTemp, HatTemp, and TempStation.

BigAg training might include adding the TS CISO to a peer group of all SC partner CISOs to meet quarterly for general professional development as well as table-top evaluations of the SC cybersecurity risk. The development example reads more like technology to me than development. Maybe something in line with the following might fit better: Development activities might include tracking the efforts made by TS to obtaining a higher tier in the various categories evaluated during selection. Cybersecurity efforts related to technology could involve coordinating improvements in wireless security (e.g. ensuring all SC partner WLANs incorporate WPA2). Finally, conducting regular cybersecurity-focused risk assessments should require annual formal evaluation with the use of a tool like the matrix in table 2 to identify risks to the overall SC.

4. CONCLUSIONS

Cybersecurity has been attracting a lot of attention for the past 20 years and that attention seems to be only intensifying based on the increasing need for cybersecurity professionals ((ISC)2, 2019). Suggested tools and techniques for dealing with SC cybersecurity have generally lagged other areas as evidenced by NIST not adding a Supply Chain category to the FICI until 2018.

SCs are often characterized by power asymmetries. We have argued that the onus of responsibility for overall SC cybersecurity falls on the shoulders of the *powerful member*. Naturally, the question arises as to what role the powerful member plays and to what degree. We

suggest that they begin the cybersecurity focus when identifying the right members to include in the SC. To this end, we formulated a Stakeholder Cyber Supply Chain Risk Management (SC-SCRM) framework which includes: Supplier Selection and four components intended for use as a continuous improvement process – Training, Development, Technology, and Risk Assessment (TDTR). The TDTR are all informed by the Supply Chain Cybersecurity Strategy (SCCS). We present the above framework in order to set the stage for future studies to determine where leader-driven decision makes the most sense and how to quantify it in application.

5. REFERENCES

BlueVoyant. (2020). *Global Insights: Supply Chain Cyber Risk* [Brochure]. New York, New York: Opinion Matters.

Boone, A. (2017, February). Cyber-security Must be a C-suite Priority. Computer Fraud & Security 2017(2), pp. 13-15. DOI: https://doi.org/10.1016/S1361-3723(17) 30015-5

Darktrace. (2017). *Global Threat Report 2017, Selected Case Studies* (Rep.). Retrieved from https://cdn2.hubspot.net/hubfs/2784256/1_nat_2017_recap/Presentations/Darktrace%20-%20Global%20Threat%20Report%202017.pdf?t=1528334118161

Ghadge, A., Weiß, M., Caldwell, N.D. & Wilding, R. (2019), Managing Cyber Risk in Supply Chains: A Review and Research Agenda. Supply Chain Management, 25(2), pp. 223-240. Retrieved from https://dspace.lib.cranfield.ac.uk/bitstream/handle/1826/14843/Managing_cyber_risk_in_supply_chains-2019.pdf?sequence=4

Gutzmer, I. (2017, September 26). Equifax Announces Cybersecurity Incident Involving Consumer Information. Retrieved from https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/

Ho, W., Zheng, T., Yildiz, H. & Talluri, S. (2015). Supply Chain Risk Management: A Literature Review. International Journal of Production Research, 53:16, 5031-5069. DOI: 10.1080/00207543.2015.1030467

(ISC)2. (2019). Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 Cybersecurity Workforce Study, 2019. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

Imai, M. (1986). The Key to Japan's Competitive Success. McGraw-Hill.

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital Supply Chain Transformation toward Blockchain Integration. Retrieved from http://128.171.57.22/bitstream/10125/41666/paper0517.pdf

Krebs, B. (2014, February 5). Target Hackers Broke in Via HVAC Company. Retrieved from https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Lee, H.L. (2004, October). The Triple-A Supply Chain. *Harvard Business Review*, 82 102-12, 157. Retrieved from https://hbr.org/2004/10/the-triple-a-supply-chain

McCandless, D., & Evans, T. (2020, December 09). World's Biggest Data Breaches & Hacks. Retrieved from https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Mulligan, D.K. & Schneider, F.B. (2011). Doctrine for Cybersecurity. *Daedalus*, 140(4), 70-92.

Munson, C.L., Rosenblatt, M.J., & Rosenblatt, Z. (1999). The Use and Abuse of Power in Supply Chains. *Business Horizons*. 42. 55-65. Retrieved from https://www.researchgate.net/publication/4884612_The_Use_and_Abuse_of_Power_in_Supply_Chains

National Institute of Standards and Technology (NIST). (2018a, August 10). Cybersecurity Framework: The Five Functions. Retrieved from https://www.nist.gov/cyberframework/online-learning/five-functions

National Institute of Standards and Technology (NIST). (2020, June 22). Cyber Supply Chain Risk Management: C-SCRM. Retrieved from https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management

National Institute of Standards and Technology (NIST). (2018b, April 16). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology (NIST). (2012, September). Guide for Conducting Risk Assessments. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology (NIST). (2011, March). Managing Information Security Risk. Retrieved from https://nvlpubs .nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

PwC. (2014, September 30). Managing Cyber Risks in an Interconnected World. Retrieved from https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

Research and Markets. (2017, December). Global Brand Counterfeiting Report, 2018. Retrieved from https://www.researchandmarkets.com /reports/4438394/global-brand-counterfeiting-report-2018

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020, February). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://nvlpubs.nist.gov /nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Smith, G.E., Watson, K.J., Baker, W.J., & Pokorski II, J.A. (2007) A Critical Balance: Collaboration and Security in the IT-Enabled Supply Chain, International Journal of Production Research, 45:11, 2595-2613, DOI: 10.1080/00207540601020544

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M. & Laarouchi, Y. (2013). Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks. 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop. Retrieved from https://hal .archives-ouvertes.fr/hal-00852244/file /Studniaetal.pdf

Talluri, S., Narasimhan, R. & Chung, W. (2010, November 16). Manufacturer Cooperation in Supplier Development Under Risk. European Journal of Operational Research, 207(1), pp 165-173.

Thanaraksakul, W. & Phruksaphanrat, B. (2009). Supplier Evaluation Framework Based on Balanced Scorecard with Integrated Corporate Social Responsibility Perspective. Proceedings of the International MultiConference of Engineers and Computer Scientists (IMECS). Retrieved from http://www.iaeng.org/publication/IMECS2009/IMECS2009_pp1929-1934.pdf.

UpGuard. (2017, July 12). Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts: UpGuard. Retrieved from https://www.upguard.com/breaches/verizon-cloud-leak

Webmaster, A&S. (2020, December 10). Cybersecurity Maturity Model Certification (CMMC). Retrieved from https://www.acq .osd.mil/cmmc/