Level of Cybersecurity Readiness of Small and Medium Nonprofit Organizations (NPOs) During COVID-19

Natalia Bell
Marymount University

Xiang Liu
Marymount University

Considering the unprecedented COVID-19 pandemic crisis, many NPOs, like other types of institutions, have migrated their operations to remote, virtual platforms to maintain at least a minimum level of activity. Consequently, the NPOs are experiencing increased online activity during COVID-19. This study assesses NPOs' readiness during COVID-19 through the lens of three components of the ISO 22301:2019 - Business Continuity Management Systems (BCMS) – labeled as 3Ps: Policy, People, and Processes. A snowball sampling study was conducted to examine information security readiness in small and medium-sized NPOs during the Covid-19 pandemic in D.C., Maryland, and Virginia (DMV) area. Each item in the three aspects of readiness was measured at high, moderate, or low. The findings of the study demonstrate that the NPOs should emphasize developing and implementing cybersecurity policies during crises to increase awareness and preparedness. The empirical results of this study further shed light on the aspects and factors of cybersecurity readiness that are often less prioritized by NPOs' senior management but should be taken into more consideration when creating cybersecurity policies and procedures.

Keywords: NPOs, cybersecurity, readiness, crisis, management, COVID-19

INTRODUCTION

Cybersecurity During COVID-19 and NPs

Microsoft's *Nonprofit Guidelines for Cybersecurity and Privacy* highlights that in 2016, nearly one-third of the top fifteen contract recipients of the city of New York were nonprofits, awarded contracts worth a combined total of 404 million dollars[9]. The increasing prevalence of such awards has irrevocably altered nonprofit operations and management. Today, NPOs face an ever-changing landscape of technology, economy, and culture[11] Therefore, each nonprofit organization's cybersecurity standards should be aligned with its industry peers and their private counterparts.

These new roles lead to new strategies, like data sharing between various partner organizations and NPOs' increasing turn to ideas of e-governance and accountability through the Internet[5]. Digital interaction of this kind with donors, beneficiaries, the public, and partners subsequently increases the possibility of NPO data exposure.

Contrary to common perceptions, nonprofit organizations, much the same as for-profit businesses, engage in various activities involving data collection[10]. Despite managing a lot of data, as[12] noted,

technology isn't often a top priority for NPOs, given the required resources and costs. On the other hand, research indicates that the information systems of NPOs are vulnerable to cybercrimes[5]. Moreover, considering the unprecedented COVID-19 pandemic crisis, many NPOs, like other institutions, have migrated their operations onto remote, virtual platforms to maintain at least a minimum level of activity. Consequently, NPOs are experiencing an increased level of online activity during COVID-19. According to[1], although charities face similar cybersecurity threats as their for-profit counterparts, the NPOs experienced particularly aggressive phishing attacks in the COVID-19 work-from-home setting.

A recent report published by Deloitte[2] that analyzes their Cyber Intelligence Center cases has concluded that while the entire globe has focused on the health, economic, and financial risks that the COVID-19 pandemic has created, cybercriminals have used these circumstances to perform even more illicit activity[2] recorded a spike in phishing attacks, Malspam, and ransomware attacks since the escalation of the COVID-19 pandemic.

NPOs, now more than ever, can become victims of cyberattacks. Is this circumstance influencing cybersecurity readiness levels within nonprofit organizations? How should the senior management of NPOs adjust the risk control strategies of their organizations to respond? To the best of our knowledge, this is one of the few studies to address the academic and industry gap in the less-researched field of nonprofit organizations in conjunction with the unprecedented COVID-19 pandemic crisis.

The Business Continuity Management Systems (BCMS) Components: 3Ps - Policy, People, and Processes

ISO (International Organization for Standardization) 22301:2019 (EN) Security and Resilience — Business Continuity Management Systems (BCMS) documents a set of generic requirements that can be adopted by any organization when implementing and maintaining a management system, with the purpose of improving an organization's capability to prepare for, respond to, and recover from disruptions when they arise[7]. Similar to any other management system, a BCMS includes the following components specified by this standard:

a) a policy;
b) competent people with defined responsibilities;
c) management processes; and
d) documented information supporting operational control and enabling performance evaluation[7].

For this project, three (3) components of the BCMS were used as the metrics to estimate the cybersecurity readiness of an organization, each assessing the cybersecurity measures taken by the NPOs from a different perspective, including policy, people, and processes. They are referred to in this project as the 3Ps. Operational control and performance evaluations do not constitute the subject of the current study; therefore, data corresponding to these two aspects were not collected in line with the scope of this study.

METHODOLOGY

The present research was conducted initially as part of the author's dissertation work at Marymount University. The current paper represents an extension of Section 1, Chapter 5 of the author's D.Sc. Thesis[3]. The present paper describes only the "readiness" aspect of the findings by using the descriptive analysis to identify the mean value as a measure of the readiness level, following[8] methodology of reporting the Level of Readiness of disaster recovery and information technology security, readiness, and awareness levels.

RESEARCH DESIGN

The current research study used a postpositivist, quantitative, nonexperimental survey research approach. For this project, a snowball approach was used to collect data. The survey response rate was monitored through a chain of control and custody. Seventy-two (72) responses were recorded, and seven (7) were not considered in the data analysis, following the bias-reduction methods. A total of sixty-five (65) valid responses have been used in data analysis. The respondents self-identified as "part of the NPO's

leadership team," and through the survey, they expressed their perceptions of their cybersecurity readiness as an organization during COVID-19.

INSTRUMENT – SURVEY

The current research project used an existing, previously utilized instrument – the National Cyber Security Alliance (NCSA) survey for assessing small businesses' cybersecurity practices[14]. This research project's instrument replaced the original instrument's usage of "small business/business" with "nonprofit" and added a time frame statement: "during COVID-19." The original survey instrument was directly collected from the NCSA's website, and no special permission was required as per NCSA's Public License Grant to Use Website Contents. The corresponding Survey Questions for the 3 Ps (BCMS components) are listed in Annex 1.

POPULATION – NPOS IN DMV AREA

This research project considers nonprofit organizations in the D.C., Maryland, and Virginia (DMV) area as its target population. More elaborations are provided as follows.

What is "the DMV Area"? The study exclusively considers organizations that are physically located in Washington, DC (full geographical area), Maryland (Prince George's County and Montgomery County), and Virginia (Arlington County, Fairfax County, and Census-designated places in Fairfax County, including Falls Church City, Alexandria City, and Fairfax City (Fairfaxcounty.gov, 2020). The current research study used corresponding ZIP Codes to determine the NPOs in the designated geographic area.

What are nonprofit organizations (NPOs)? The Internal Revenue Services (IRS) defines nonprofits as charitable organizations that "must not be organized or operated for the benefit of private interests"[6] and fall under section 501(c)(3) of the Internal Revenue Code, which covers the following purposes: "charitable, religious, educational, scientific, literary, testing for public safety, fostering national or international amateur sports competition, and preventing cruelty to children or animals"[6].

According to the current project's research design, the only organizations that have been considered are those that are registered 501(c)(3) organizations that fulfill the following criteria: (1) an annual income of less than $49,999,999; (2) a primary exempt activity serving human beneficiaries; and (3) several employees less than 250[6]. Additionally, only organizations that filed taxes with the IRS in 2019 were considered, as their information is publicly available on the IRS website.

RESEARCH APPROACH

The current research paper used a quantitative method to assess the perception of cybersecurity readiness of the NPOs during Covid-19. The SPSS statistical software was used for data analysis and focused on descriptive statistics to obtain the mean value (Table 1) as a measure of readiness level, following[8] methodology of reporting the Level of Readiness for disaster recovery and information technology security. Readiness and awareness levels can be calculated by taking the highest mean score minus the lowest mean score and dividing it by 3. The result has been added to the minimum and maximum values to create three measurement levels at low, moderate, and high, with respective value ranges for each measurement. Although the findings do not represent the Level of Cybersecurity Readiness in absolute terms, the methodology does help in ranking the readiness and awareness levels between the variables and in comparison with the clusters. This allows a better understanding of the level of readiness in relative terms and within the model; therefore, it was considered suitable for the current research paper.

KEY FINDINGS

Table 1 presents the Descriptive Statistics information – including the Variable, the Scale, the Mean value, the Standard Deviation, and Minimum & Maximum.

TABLE 1
DESCRIPTIVE STATISTICS

Variable	Scale	Mean	Standard Deviation	Minimum	Maximum
People1	5-Point Likert Scale	2.52	1.348	1	5
People2	5-Point Likert Scale	2.68	1.348	1	5
People3	5-Point Likert Scale	1.92	0.924	1	5
People4	5-Point Likert Scale	1.98	1.431	1	5
Policy1	5-Point Likert Scale	1.6	1.356	1	5
Policy2	5-Point Likert Scale	1.34	1.02	1	5
Policy3	5-Point Likert Scale	1.68	1.239	1	5
Policy4	5-Point Likert Scale	2.00	1.25	1	5
Process1	5-Point Likert Scale	2.38	1.476	1	5
Process2	5-Point Likert Scale	2.38	1.343	1	5
Process3	5-Point Likert Scale	2.63	1.206	1	5
Process4	5-Point Likert Scale	2.94	1.478	1	5

CALCULATING THE LEVEL OF READINESS FOR PEOPLE COMPONENT WITHIN ITS CLUSTER -

Following[8] methodology, the readiness level for the BCMS Component People was calculated by taking the highest mean score (2.68) minus the lowest mean score (1.92) and dividing by 3 (result = 0.25). The resulting ranges for the three measurement levels are the following

- 1.92 - 2.17 - low
- 2.18 - 2.42 - moderate
- 2.43 - 2.68 - high

TABLE 2
LEVEL OF READINESS FOR PEOPLE WITHIN ITS CLUSTER

BCMS Component – People	Mean	Level of Readiness
People 1	2.52	High
People 2	2.68	High
People 3	1.92	Low
People 4	1.98	Low

CALCULATING THE LEVEL OF READINESS FOR PROCESS COMPONENT WITHIN ITS CLUSTER -

Following[8] methodology, the readiness level for each BCMS Component Process was calculated by taking the highest mean score (2.94) minus the lowest mean score (2.38) and dividing by 3 (result = 0.18). The resulting ranges for the three measurement levels are the following

- 2.38 - 2.56 - low
- 2.57 - 2.75 - moderate
- 2.76 - 2.94 - high

TABLE 3
LEVEL OF READINESS FOR PROCESS WITHIN ITS CLUSTER

BCMS Component – Process	Mean	Level of Readiness
Process 1	2.38	Low
Process 2	2.38	Low
Process 3	2.63	Moderate
Process 4	2.94	High

CALCULATING THE LEVEL OF READINESS FOR POLICY COMPONENT WITHIN ITS CLUSTER -

Following[8] methodology, the readiness level for each BCMS Component Policy was calculated by taking the highest mean score (2.00) minus the lowest mean score (1.34) and dividing by 3 (result = 0.22). The resulting ranges for the three measurement levels are the following

- 1.34 - 1.56 - low
- 1.57 - 2.77 - moderate
- 1.78 - 2.00 - high

TABLE 4
LEVEL OF READINESS FOR POLICY WITHIN ITS CLUSTER

BCMS Component – Policy	Mean	Level of Readiness
Policy 1	1.6	Moderate
Policy 2	1.34	Low
Policy 3	1.68	Moderate
Policy 4	2.00	High

Comparing the Level of Readiness for All Components Within the Same Scalable Measure - 5-Point Likert Scale

Following[8] methodology, the readiness level for BCMS Components was calculated by taking the highest mean score (2.94) minus the lowest mean score (1.34) and dividing by 3 (result = 0.53). The resulting ranges for the three measurement levels are the following

- 1.34 - 1.87 - low
- 1.88 - 2.40 - moderate
- 2.41 - 2.94 - high

Considering the Mean values presented in Table 1, the Level of Readiness for each BCMS has been established. Tables 5, 6, and 7 showed the Level of Readiness for BCMS Components: People, Policy, and Processes of the small and medium-sized NPOs in the DMV Area.

TABLE 5
LEVEL OF READINESS FOR PEOPLE

BCMS Component – People	Mean	Level of Readiness
People 1	2.52	High
People 2	2.68	High
People 3	1.92	Moderate
People 4	1.98	Moderate

TABLE 6
LEVEL OF READINESS FOR PROCESS

BCMS Component – Process	Mean	Level of Readiness
Process 1	2.38	Moderate
Process 2	2.38	Moderate
Process 3	2.63	High
Process 4	2.94	High

TABLE 7
LEVEL OF READINESS LEVEL FOR POLICY

BCMS Component – Policy	Mean	Level of Readiness
Policy 1	1.6	Low
Policy 2	1.34	Low
Policy 3	1.68	Low
Policy 4	2.00	Moderate

The following color-coded rules have been used for the visual representation of the Level of Readiness:

TABLE 8
COLOR-CODDED RULE

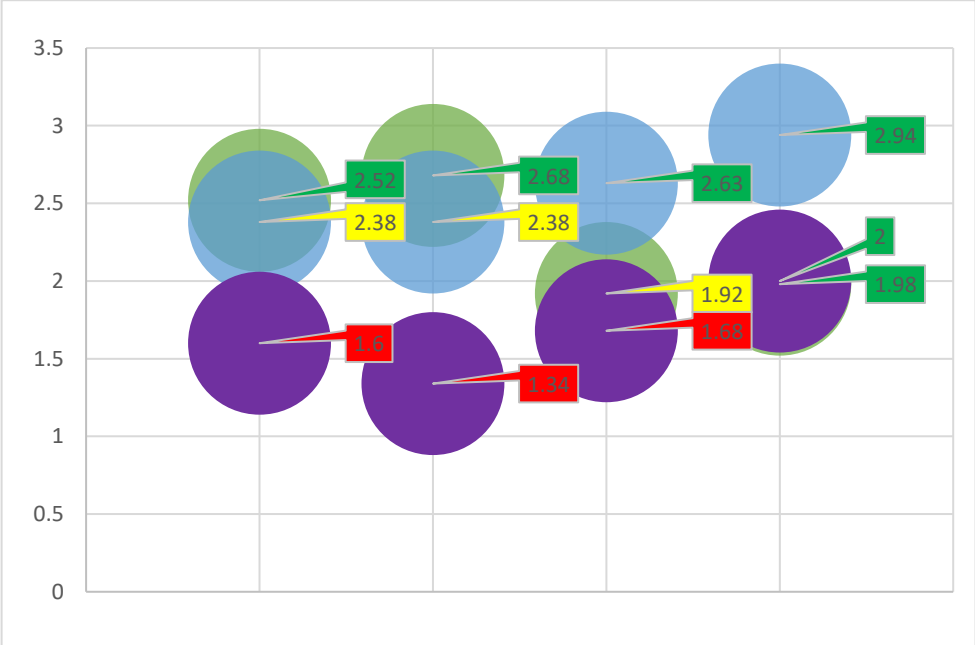
Color	Level of Readiness
Red	Low
Yellow	Moderate
Green	High

Figure 1 represents a visual color-coded demonstration of the various Levels of Readiness for each BCMS Component. The vertical numeric values represent the ranges for the Mean value. The color-coded squared values represent the actual Mean value for each BCMS Component according to the color-coded Level of Readiness.

FIGURE 1
INDIVIDUAL LEVELS OF READINESS FOR PEOPLE, POLICY, AND PROCESS

Figure 2 represents the Combined Levels of Readiness for People, Policy, and Process BCMS components with the actual Mean values for each BCMS Component according to the color of Level of Readiness. Figure 2 gives a general perspective of the Level of Readiness of each component, facilitating the visual comparison of the Process BCMS components.

FIGURE 2
COMBINED LEVELS OF READINESS LEVEL FOR PEOPLE, POLICY, AND PROCESS



DISCUSSION

According to[4], the readiness level is defined as "the level of an organization's awareness, preparedness, and commitment to prevent and combat cyber-attacks." Therefore, the findings of the current research should serve as proof for senior NPO managers to focus their cybersecurity strategies on People, Processes, and Policies. NPOs can use existing cybersecurity frameworks like the NIST Risk Management Framework (RMF) to improve their risk management strategies and protect organizations from cyber threats in such an unprecedented circumstance as COVID-19.

The current paper describes a finding from a more complex study that surveyed 65 NPOs employees, part of the NPOs' leadership, to determine their perceptions of their cybersecurity readiness as an organization.

Data analysis of the current research project showed that within the People component, the NPOs' leaders have a higher perception of readiness when talking about the level of support and emphasis from the senior management; however, their readiness perception is lowest when it comes to the ability of the employees to detect spear-phishing (and other types) attacks and given the number of hours of cybersecurity training.

Within the Process component, the NPOs' leaders have a higher perception of readiness if a manual backup procedure would be needed in case of an attack; however, they have a lower perception of readiness regarding a process for employees to report cyber-attacks to leadership or data and equipment security. The NPOs' leaders perceive a moderate level of readiness concerning the immediate data breach response process.

And finally, within the Policy component, the NPOs' leaders have a moderate perception of readiness when considering a clearly defined cybersecurity policy, business continuity, and disaster recovery policy; a high perception of readiness thinking about the escalation of suspicious events; and moderate perception of readiness regarding the knowledge management of cybersecurity policy.

When comparing the clusters, the Perceived Level of Readiness for Policy is considerably lower than the Level of Readiness for People and Processes. This finding suggests that small and medium-sized NPOs

should emphasize developing and implementing cybersecurity policies during crises to increase the level of awareness and preparedness among employees.

The authors acknowledged the limitations of this study as per its research design. The nonprobability sampling procedure generally does not control for selection bias and does not permit the calculation of sampling error[13] [p.172]. However, two bias reduction methods have been used in this study to alleviate such limitations: chain of control and custody and purposeful sampling. Purposeful nonprobability sampling is an appropriate technique that rejects biases in cases with precise selection criteria in which only qualifying participants will be considered in data collection and analysis. The current project used the following exact criteria for the respondents:

1. Physical location of the NPO (DMV Area)
2. Restricted number of employees (less than 250)
3. Restricted size of the annual budget (less than $50 million)
4. Respondent participant is part of the NPO's leadership team

As the current research project is considered an exploratory study aiming to enlarge the limited body of knowledge on the topic rather than an in-depth explanatory analysis, a nonprobability sampling procedure was selected as it is regarded suitable for the exploratory type of research.

CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

The existing literature suggested that three factors influence security preparedness among NPOs: (1) [lack of] information security culture; (2) [lack of] information security awareness; and (3) [lack or misuse of] information security policies[5].

This being said it is recommended that small NPOs should have higher cybersecurity awareness and establish information security practices to ensure the safeguarding of their informational assets. Additionally, these entities should be supported through accessible or affordable cybersecurity programs since they face budget limitations and restrictions as their income is socially mission-oriented.

We consider that the findings of the current paper are contributing to the enhancement of business and management practice and also elevating the understanding of workforce behavior when evaluating information security: a relatively new priority for businesses and nonprofit entities. Central to the entire discipline of cybersecurity is the human aspect of information security. As the current study shows, the challenges experienced by nonprofit organizations over the past two years remain unprecedented; therefore, there is an increasing need for entities to introduce new measures and practices that would align with the evolving cybersecurity threats.

To our knowledge, little research has surveyed nonprofit organizations regarding their information security preparedness in conjunction with the unprecedented COVID-19 pandemic crisis. The primary objective of this study was to address both the academic and industry gap in the less-researched field of a nonprofit organization and highlight the evolving necessity of cybersecurity awareness in both for-profit and nonprofit entities.

The current study highlights that cybersecurity awareness must be considered urgent when discussing the improvement of business concepts and concrete, practical measures to be implemented (e.g., enforcement of cybersecurity policy and procedures). To increase awareness and shape workforce behavior, cybersecurity needs to be embraced by organizations as an indispensable component in business development and success. This paper has advanced the practice of business management by placing cybersecurity awareness as the top priority of NPOs and urging nonprofit leaders to take active steps in developing cybersecurity strategies, policies, procedures, and employee training programs, as the cybersecurity threats are evolving and are so dangerous for cyber-vulnerable entities such as nonprofits.

Additionally, the authors identified several future research directions delineated as follows. First, the current study targeted NPOs in the DMV area with less than 250 employees and an annual budget of less than $50 million. To increase the generalizability of the study findings, larger samples from more diverse geographical locations can be recruited for data analysis. Second, the current research project targeted organizations that have primarily human beneficiaries. Therefore, organizations labeled with letter code C:

Environmental Quality, Protection and Beautification and D: Animal-Related according to the National Taxonomy of Exempt Entities (NTEE) code[6] have been excluded, as well as other organizations that do not describe themselves as having "human beneficiaries." A future study may extend the focus to the non-human beneficiaries and compare the findings across different types of beneficiaries. Finally, when taking a closer look at the People component, volunteer participation becomes a unique feature of NPOs. The number of volunteers involved and the level of cybersecurity awareness of those volunteers emerge as interesting variables to examine further.

ENDNOTES

1. Anders, S.B. (2020). Cybersecurity Resources for a remote workforce: Certified public accountant. *The CPA Journal*, *90*(7), 72–73.
2. *Impact of COVID-19 on Cybersecurity*. (n.d.). Deloitte Switzerland. Retrieved from https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
3. Ermicioi, N. (2020). *Factors affecting nonprofits' information security readiness during crises: A study of COVID-19's impact on small and medium nonprofit organizations (NPOS) in the DMV area*, in *School of Technology and Innovation*. Marymount University.
4. Hasan, S., Ali, M., Kurnia, S., & Ramayah, T. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726
5. Imboden, T., Phillips, J.C., Seib, J.D., & Fiorentino, S.R. (2013). How are nonprofit organizations influenced to create and adopt information security policies? *Issues in Information Systems*, *14*(2), 166–173.
6. *Exempt Purposes - Internal Revenue Code Section 501(c)(3)*. (2019). IRS. Retrieved from https://www.irs.gov/charities-non-profits/charitable-organizations/exemptpurposes-internal-revenue-code-section-501c3
7. *ISO 22301:2019 (EN) Security and Resilience — Business Continuity Management Systems-Requirements*. (2019). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en
8. Kasim, S.A., & Mohamed, I.B. (2018). Level of Readiness in IT Disaster Recovery Plan. In *Cyber Resilience Conference (CRC)*, pp. 1–4.
9. *Nonprofit Guidelines for Cybersecurity and Privacy*. (2017). Microsoft Corporation. Retrieved from https://download.microsoft.com/download/1/D/4/1D494A7D-D153-40FC-BC18-F4C2F800E752/Nonprofit_Guidelines_for_Cybersecurity_and_Privacy.pdf
10. National Council of Nonprofits *Cybersecurity for Nonprofits*. (2019).
11. Renshaw, S., & Krishnaswamy, G. (2009). Critiquing the Knowledge Management Strategies of Non-Profit Organizations in Australia. *Proceedings of the World Academy of Science, Engineering and Technology (WASET)*, *37*, 456–464.
12. Rottkamp, D.M. (2021). Reimagining strategic vision for nonprofits: Evaluating everything after COVID-19: Certified public accountant. *The CPA Journal*, *91*(4), 22–27.
13. Singleton, B., & Straits, B. (2018). *Approaches to Social Research* (5th ed.). Oxford University Press.
14. *A new survey released by the National Cyber Security Alliance (NCSA)*. (2020). The National Cyber Security Alliance. Retrieved from https://staysafeonline.org/small-business-target-survey-data/

APPENDIX 1: BCMS COMPONENTS

Statement	Component – People
What level of support do you have for your organization's cybersecurity during COVID-19?	People 1
The organization's senior management consistently emphasizes the importance of cybersecurity during COVID-19	People 2
Most employees are sophisticated about detecting spear-phishing and other kinds of intrusion attempts during COVID-19	People 3
On average, how many hours of cybersecurity training do you require per employee during COVID-19?	People 4

Statement	Component – Process
Does your organization have a clearly articulated process for employees to report potential cyber threats to leadership during COVID-19?	Process 1
Does your organization have a clearly articulated business process that outlines how employees should securely dispose of equipment and data during COVID-19?	Process 2
If you were to have a data breach or cybersecurity incident during COVID-19, does your organization have a response process you can immediately put into action?	Process 3
If you were to have a data breach or cybersecurity incident during COVID-19 and lose access to your computers and network, do you have a process to initiate manual or backup procedures to continue operating your organization?	Process 4

Statement	Component – Policy
Does your organization have a clearly defined and documented cybersecurity policy during COVID-19?	Policy 1
If the organization had a computer system business continuity or disaster recovery policy before, was it updated in 2020?	Policy 2
Which best describes the knowledge management of cyber security policy in during COVID-19?	Policy 3
The organization has a clear, well-established policy for escalating suspicious events during COVID-19.	Policy 4

Note: Considering the variables' scale, the collected raw data was adjusted, and the values of the corresponding variables received numeric values.