Kansas Small Organizations Cybersecurity Survey 2024

DOCKING INSTITUTE
of Public Affairs
FORT HAYS STATE
UNIVERSITY

May 2024

Conducted for

FHSU RCOBE Cybersecurity Institute and Technology Incubator

Brett Zollinger, Ph.D.
Director

Jian Sun, Ph.D.
Assistant Director

Michael S. Walker, M.S.
Research Scholar

Marisa M. Johnson, M.B.A.
Administrative Specialist

Leslie Watson-Divittore, M.S.
Research Coord. Admin. Specialist

Hannah Cross
Graduate Research Assistant

Mission:

To facilitate effective public policy decision-making among governmental and nonprofit entities

Docking Institute of Public Affairs
Fort Hays State University
600 Park Street
Hays, Kansas 67601-4099
Telephone: (785) 628-4197
www.fhsu.edu/docking

Kansas Small Organizations Cybersecurity Survey 2024

Prepared By:

Brett Zollinger, Ph.D.
Director
Docking Institute of Public Affairs

Prepared For:
FHSU RCOBE Cybersecurity Institute and Technology Incubator

This report was prepared by the Docking Institute of Public Affairs. All statements, findings, and conclusions of the report are those of the author(s) and do not necessarily reflect the views of the client.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

Executive Summary

From April 19 to May 22, 2024, the Docking Institute collected responses from 502 randomly selected small organizations across Kansas. The vast majority of responses were received by a mailed questionnaire that was returned to the Institute via USPS, and 22 of the responses were received via the online response option. The survey, commissioned by the Robbins College of Business and Entrepreneurship on behalf of its Cybersecurity Institute and Technology Incubator, had as its primary research objectives to assess organizations' cybersecurity awareness, attitudes/perceptions, and behaviors. The 502 completions received from a presumed 10,739 eligible targets, results in a response rate of 4.7%. The sample margin of error for 502 completions is +/- 4.4%, assuming no response bias.

Among the full set of respondents, the survey finds:

- The NAICS industry code profile of the 502 completions mirrors well the NAICS profile of the original 12,000 randomly selected targets.
- The majority, 65%, of respondents are with businesses (35% for-profit corporation, 21% LLC, 7% sole proprietorship, and 2% partnership). Another 15% are with a nonprofit/not-for-profit, 11% government agency/office, and 6% are with a school.
- About 40% of all responding organizations do not use an online payment system. About 28% do use one for both client and vendor transactions, about 24% for client transactions only, and about 8% for vendor transactions only.
- 37% of respondents indicate they have had formal cybersecurity training.
- 61% indicate their organization has never, to their knowledge, experienced a malicious cybersecurity event.
- 58%, say their organization has not experienced a non-malicious data loss event, to their knowledge.
- 92% agree or strongly agree that they understand the potential impact of breaches.
- 87% agree or strongly agree that they are aware of common cybersecurity threats.
- 54% agree or strongly agree that they are aware of various cybersecurity measures.
- Only slightly more agree/strongly agree (33%) than disagree/strongly disagree (29%) that they are familiar with current cybersecurity regulations, and there is also a relatively high percentage of neutral (24%) and don't know (12%) on this question.
- 74% agree or strongly agree that employee cybersecurity training is crucial for safety.
- 72% agree or strongly agree that investing in cybersecurity is crucial for safety.
- 64% agree or strongly agree that their organization regularly makes hardware and software security updates.
- 61% agree or strongly agree that cybersecurity training helps save money in the long run.

- 56% agree or strongly agree that they are willing to invest in employee security training.
- Only 43% agree or strongly agree that they are confident identifying and responding to potential threats.
- 51% agree or strongly agree that their organization lacks cybersecurity policy and incident response preparedness.
- 42% agree or strongly agree that their organization has difficultly ensuring safe employee behavior.
- 35% agree or strongly agree their organization faces challenges in managing third-party vendor risks
- 27% agree or strongly agree the organization has insufficient back-up and recovery measures.
- 43% agree or strongly agree that they themselves need cybersecurity training.
- 37% agree or strongly agree that the organization needs cybersecurity training.
- 68% agree or strongly agree that they find it challenging to stay updated with evolving cybersecurity regulations and standards.
- 56% agree or strongly agree that the organization lacks the technical expertise to fully understand and mitigate complex cybersecurity threats.
- 30% agree or strongly agree that a barrier to their organization's cybersecurity is a lack of qualified cybersecurity trainers.
- 56% agree or strongly agree that "Limited resources have made it difficult to invest in advanced cybersecurity measures."
- 43% agree or strongly agree that time for cybersecurity training is a barrier for their organization.
- 43% agree or strongly agree that costs and technical constraints limit updates to systems.
- 38% agree or strongly agree that cybersecurity training cost is an organizational barrier.
- 70% agree or strongly agree that trainings should be regularly updated to latest cybersecurity threats.
- Just under half, 49%, agree or strongly agree that hands-on training is more beneficial than theoretical training.
- 47% agree or strongly agree that access to a local support center would greatly benefit the organization.
- 43% agree or strongly agree they are interested in training on topics specific to my organization.
- 28% agree or strongly agree they are willing to allocate budget and resources for regular employee training.
- 24% agree or strongly agree they are aware of local or online security training resources.
- Finally, there is little variation in response across six items in the section measuring a respondent's perception of their own understanding of how significant cybersecurity is for their organization. Vast majorities express agreement in the importance of cybersecurity on all statements, with "agree" response ranging from 39%-47% and "strongly agree" ranging from 24% to 44%.

A breakout of response by respondent/organization demographic types is provided in Appendix 2, and narrative of notable differences in these breakouts is provided in the report by subsections of the cybersecurity questions.

METHODS

The Fort Hays State University (FHSU) Robbins College of Business and Entrepreneurship on behalf of its Cybersecurity Institute and Technology Incubator commissioned the Docking Institute of Public Affairs (Institute) to survey Kansas organizations with 3 to 300 employees. The 300-employee upper limit is set to still allow for fairly sizable organizations but still be well below the minimum employee limit to qualify as a "small business" under U.S. Small Business Administration standards[1]. For all business classifications the SBA's floor threshold is 500 and several classifications have higher thresholds. The Institute collaborated with representatives of RCOBE to finalize survey item content. The Institute was responsible for survey construction, printing, mailing, online response option programming, data entry, data management, cleaning, analysis, and authoring a report with color charts of results. The primary research objectives of the survey were to assess organizations' cybersecurity awareness, attitudes/perceptions, and behaviors.

The Institute used a national sampling vendor to obtain a random, addressed-based sample of small organizations in Kansas. The survey cover letter asked that the questionnaire be completed by someone responsible for cybersecurity implementation/protocols -- see Appendix 1 for the cover letter and full questionnaire. The survey involved up to three USPS mailings to randomly selected small organizations in Kansas. The first mailing was a pre-notice postcard, and this was followed a few days later by mailing of the questionnaire booklet. The booklet questionnaire is designed such that once completed, a person simply tapes it shut and drops it in the mail. The back cover of the questionnaire is pre-addressed and postage-paid for return directly to the Institute. The third mailing was a follow-up postcard to non-responders as final appeal to participate and offering an online response option as a means to respond should the target prefer it over returning the questionnaire booklet by mail. The online survey was fielded using the Qualtrics platform and accessible by QR code or by URL address. Only 22 chose to use the online response option.

Of the 12,000 randomly targeted respondents, the Institute received confirmation 1,261 could not be delivered with the information in-hand. Often the cause of an undeliverable is a move with forwarding or the organization ceases to exist. This left 10,739 presumed eligible targeted respondents. Questionnaires began arriving on April 19, 2024, and data collection ended on May 22, 2024. The Institute received a total of 502 usable questionnaires from the 10,739 presumed eligible targets, resulting in an overall response rate of 4.7%. The sample margin of error for 502 completions is +/- 4.4%, assuming no response bias.

The full questionnaire in Appendix 1 uses question numbering that is retained in displays of results throughout this report. Appendix 2 contains a breakout of response by demographic type among all cybersecurity content questions.

[1] https://www.sba.gov/document/support-table-size-standards

Respondent and Organizational Demographics

Table 1 compares the final set of respondents to the full sampling frame purchased from the national sampling vendor in terms of its representativeness as measured by the two-digit NAICS sector code. In all but one sector (Accommodation and Food Services), the difference between the percentage of respondents in a sector differs by less than the sampling margin of error (+/- 4.4%) from the presence of the sector in the full sampling frame. For Accommodation and Food Services the under-representation of the final set of respondents (-4.6%) is only slightly outside the MOE.

Table 1. North American Industry Classification System (NAICS) of Respondents Compared to Full Sample Frame

A	B	C	D	E	F	G
NAICS Sector	Tw NAICS Sector Code two-digit	Survey All Respondents*	**Survey All Respondents**	Frame of 12,000	**Frame of 12,000**	Over- (+) / Under (-) Representation in Final Sample (column D-F)
		n	**(%)**	**N**	**(%)**	**(%)**
Agriculture, Forestry, Fishing and Hunting	11	18	**3.8**	349	**2.9**	0.9
Mining, Quarrying, and Oil and Gas Extraction	21	4	**0.9**	80	**0.7**	0.2
Utilities	22	3	**0.6**	56	**0.5**	0.1
Construction	23	32	**6.8**	848	**7.1**	-0.3
Manufacturing	31	2	**0.4**	81	**0.7**	-0.3
Manufacturing	32	6	**1.3**	168	**1.4**	-0.1
Manufacturing**	33	12	**2.6**	344	**2.9**	-0.3
Wholesale Trade	42	28	**6**	628	**5.2**	0.8
Retail Trade	44	21	**4.5**	812	**6.8**	-2.3
Retail Trade	45	27	**5.7**	619	**5.2**	0.5
Transportation and Warehousing	48	5	**1.1**	294	**2.5**	-1.4
Transportation and Warehousing	49	5	**1.1**	96	**0.8**	0.3
Information	51	18	**3.8**	232	**1.9**	1.9
Finance and Insurance	52	42	**8.9**	580	**4.8**	4.1
Real Estate and Rental and Leasing	53	18	**3.8**	430	**3.6**	0.2
Professional, Scientific, and Technical Services	54	39	**8.3**	968	**8.1**	0.2
Management of Companies and Enterprises	55	1	**0.2**	8	**0.1**	0.1

Administrative and Support and Waste Management and Remediation Services	56	11	**2.3**	504	**4.2**	-1.9
Educational Services	61	26	**5.5**	563	**4.7**	0.8
Health Care and Social Assistance	62	45	**9.6**	1603	**13.4**	-3.8
Arts, Entertainment, and Recreation	71	10	**2.1**	207	**1.7**	0.4
Accommodation and Food Services	72	13	**2.8**	884	**7.4**	-4.6
Other Services (except Public Administration)	81	52	**11.1**	1168	**9.7**	1.4
Public Administration	92	32	**6.8**	478	**4**	2.8
TOTALS		470	**100**	12000	**100**	

*32 cases could not be matched to frame on NAICS 2-digits

** At the 2-digit code level some sectors are repeated (e.g. “manufacturing” three times), but subsequent digits further differentiate various subtypes in the sector

Turning to respondent answers to personal and organizational demographic questions, respondents were asked from a pre-defined list to choose the best category representing their organization's type. Figure 1 shows that the majority, 65%, of respondents are with businesses (35% for-profit corporation, 21% LLC, 7% sole proprietorship, and 2% partnership). Another 15% are with a nonprofit/not-for-profit, 11% government agency/office, and 6% are with a school.

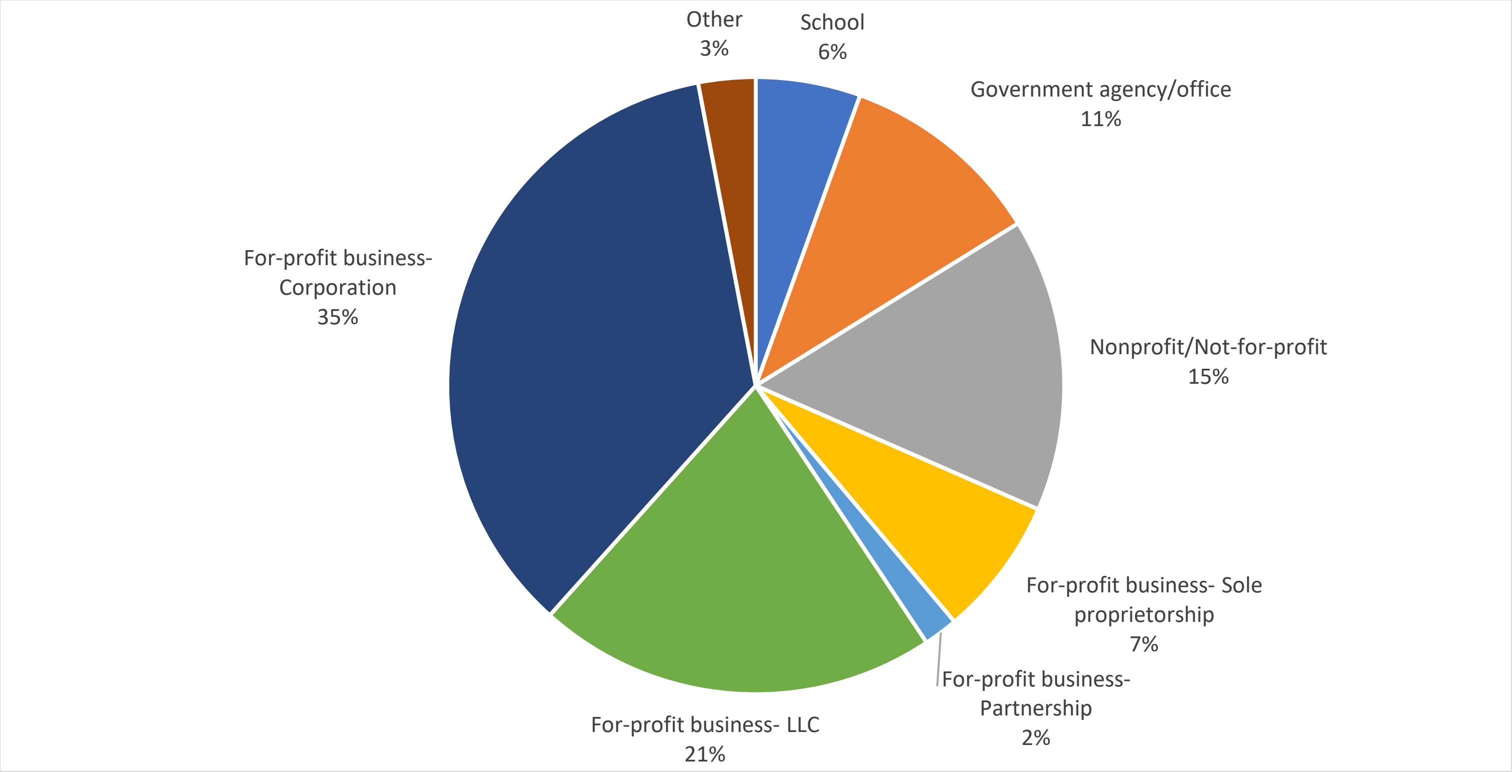


Figure 1. Best Descriptor of Respondent's Organization

Respondents were also asked to choose from a list the major activity/purpose of the organization. About 23% of respondents chose professional services, followed by 21% who chose "other," 14% retail, and 13% personal services. All remaining types are in the single digit percentages. The 103 respondents who answered "other" were asked to write in the major activity/purpose of the organization, and the Institute coded the open responses (see Figure 3), with large percentages of those being religious (31%) and agriculture (24%).

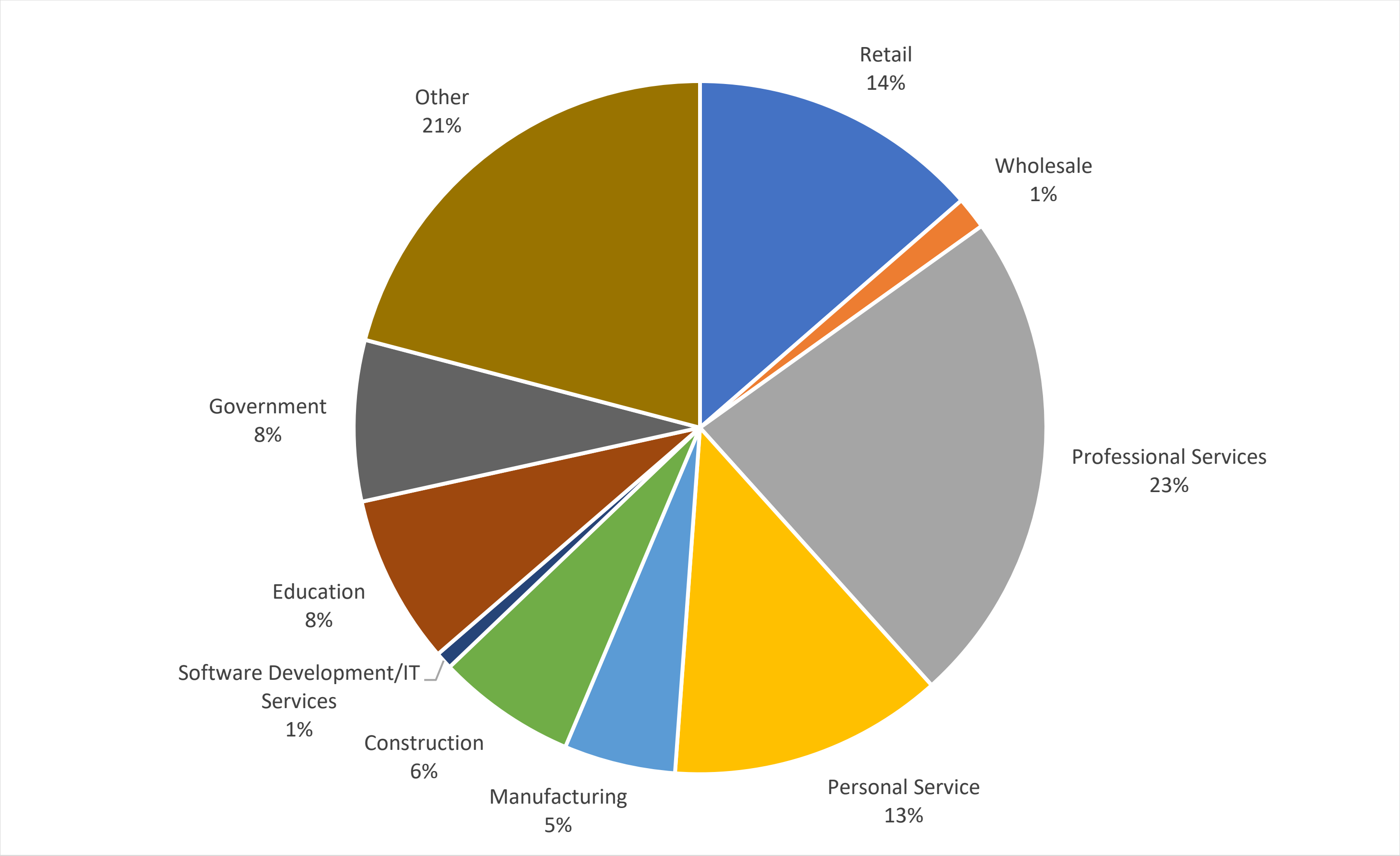


FIGURE 2. MAJOR ACTIVITY/PURPOSE OF ORGANIZATION

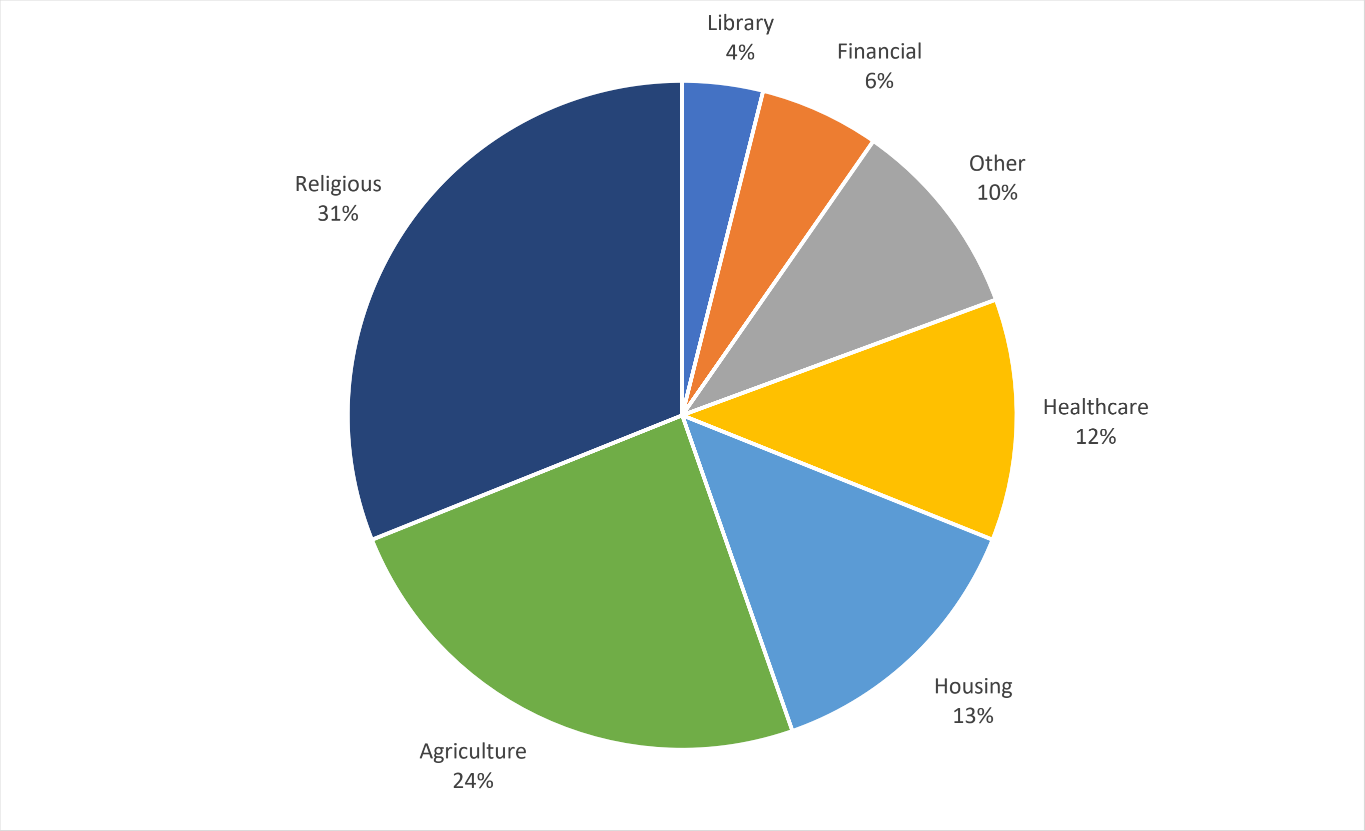


Figure 3. Coding of "Other" Responses on Major Activity/Purpose of Organization (n=103)

Figure 4 shows the distribution of numbers of employees by range size bands. The single largest percentage employee up to 4 full-time employees, while another 17% report 5-9 full-time employees. Thus, about 50% of the sample have fewer than 10 full-time employees. Figure 5 shows that a vast majority, 72%, have 0-4 part-time employees.

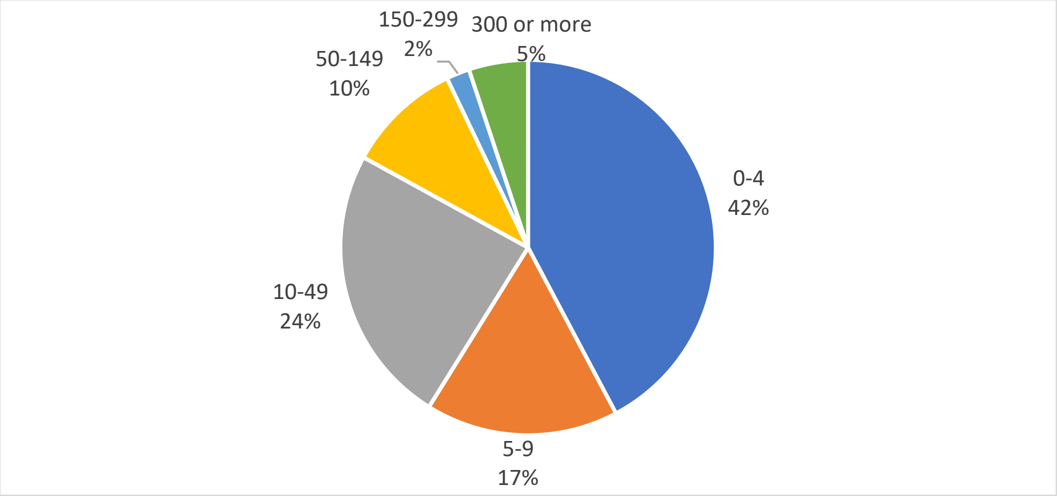


FIGURE 4. NUMBER OF FULL-TIME EMPLOYEES

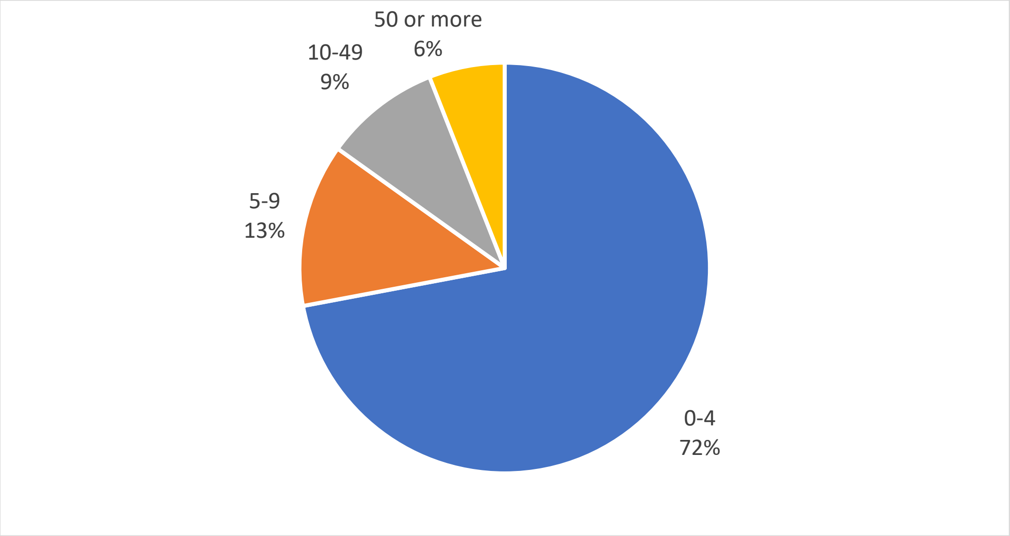


FIGURE 5. NUMBER OF PART-TIME EMPLOYEES

Respondents were also asked to report the number of contract employees in their organization. As can be seen in Figure 6, only about 14% indicate having 5 or more contract employees, while 86% indicate 0 to 4 contract employees. Over three-fourths (78%) indicate their organization is 25 years or older as shown in Figure 7.

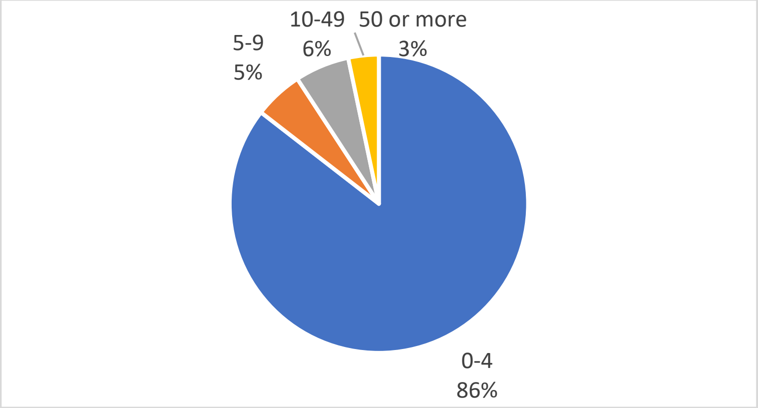


FIGURE 6. NUMBER OF CONTRACT EMPLOYEES

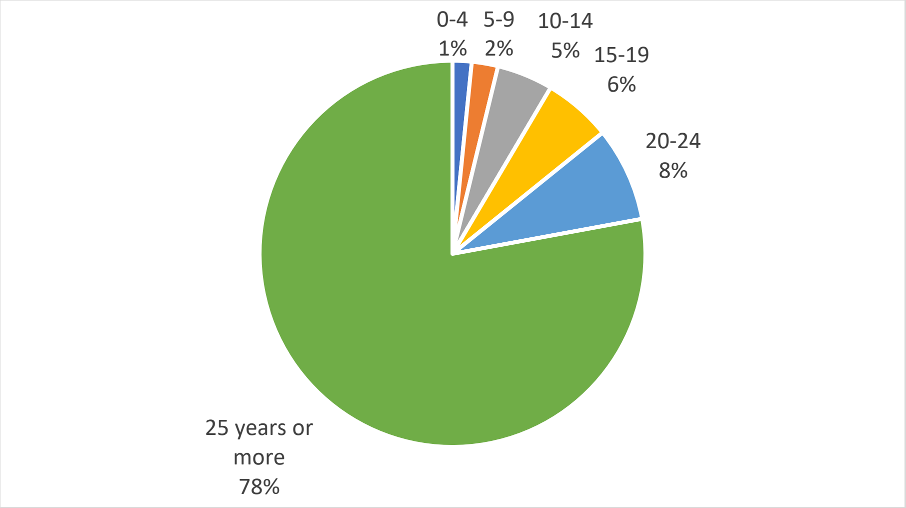


FIGURE 7. YEARS THAT ORGANIZATION HAS EXISTED

By far the single largest percentage (28%) of respondents report being in cities of 100,000 or more in population, followed by about 14% being in a city of 20,000-49,999, and about 11% are in towns 1,500-2,999. Only single digit percentages are in cities among the other population ranges in Figure 8. 2022 U.S. Census Bureau estimates of metropolitan counties' (roughly places with a city of 50,000 or more) percentage of the Kansas population is 62%. The distribution in Figure 8 with a percentage of about 37% of respondents living in cities of 50,000 or more almost certainly reflects the targeting of small organizations (up to 300 employees) for this survey.

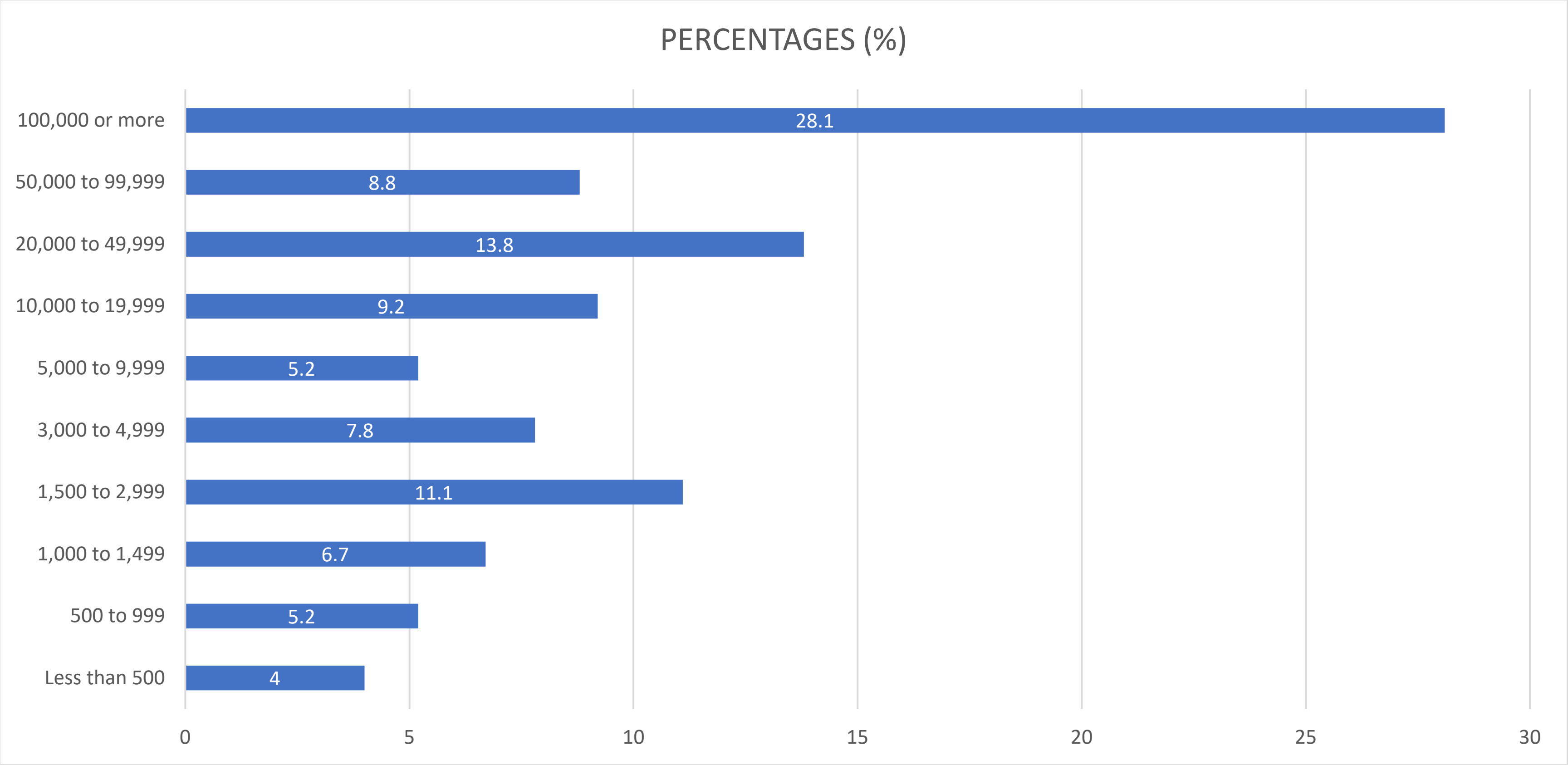


FIGURE 8. POPULATION OF RESPONDENT'S CITY

Upon coding open-ended answers to the question “What is your role/job in the organization?”, the single largest percentage (22%) indicate a manager/director role (Figure 9). About 19% are owners/partners, and 15% are CEO/CFO/COO or President.

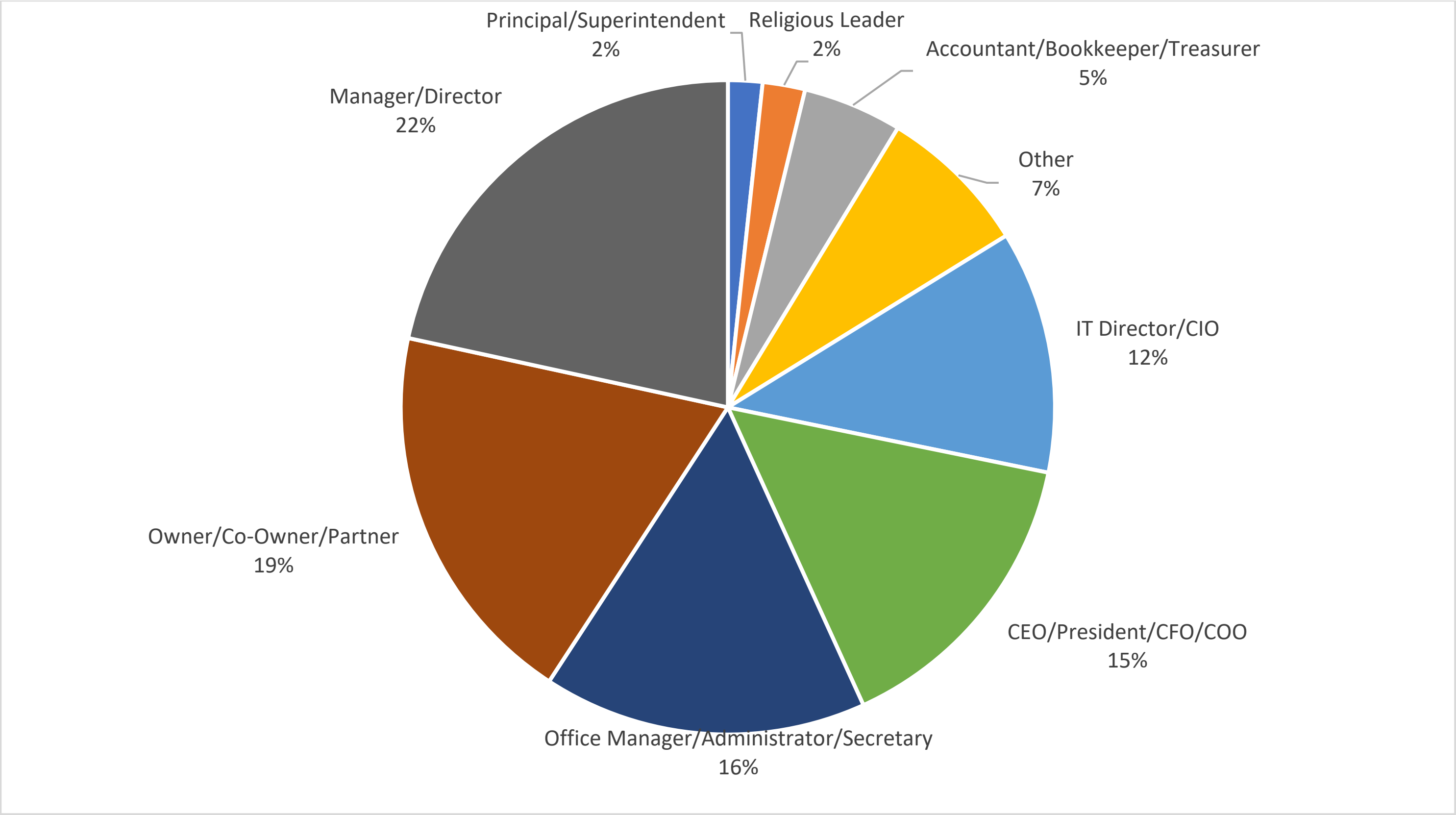


FIGURE 9. PRIMARY ROLE/JOB IN THE ORGANIZATION

Respondents were asked whether they use an online payment system and, if so, whether they use it with vendors, clients, or both. As shown in Figure 10, about 40% do not use an online payment system. About 28% do use one for both client and vendor transactions, about 24% for client transactions only, and about 8% for vendor transactions only.

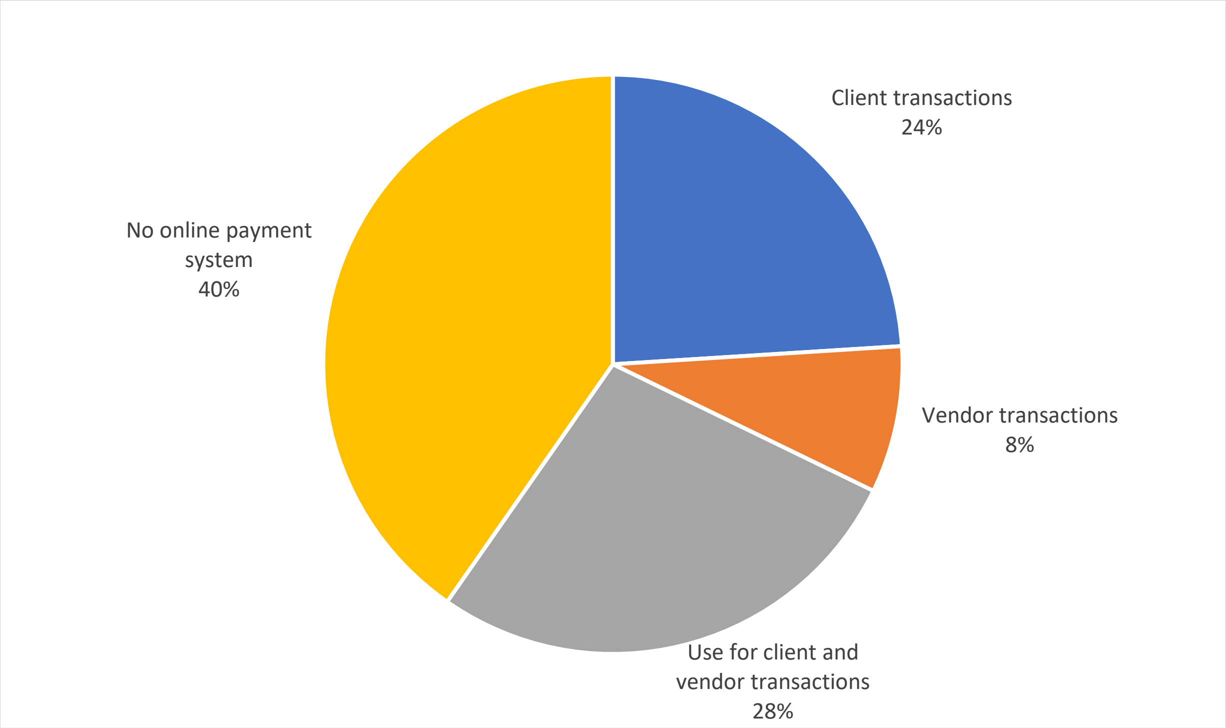


FIGURE 10. USES AN ONLINE PAYMENT SYSTEM

CYBERSECURITY

Multiple sets of cybersecurity questions were administered. Each set was prefaced with a heading printed in the questionnaire, although, there were no strict content boundaries between the sections and some items across the sets were very similar to items in other sets. All questions in these sets used a 5-point strongly disagree to strongly agree metric, with neutral as the middle point. Don't know responses and no answer were given separate codes and included in response distributions for graphing results below. Figures 11 through 18 shows results for all of these question sets. Presentation of results across these sets of questions follows the section order as presented to respondents, however, stacked bar chart displaying results from these sections have items ordered by response distributions.

Awareness

In Figure 11, a combined 92% agree (42%) or strongly agree (50%) that they understand the potential impact of breaches, and this is followed closely by a combined 87% who agree (49%) or strongly agree (38%) that they are aware of common cybersecurity threats. About 54% agree (37%) or strongly agree (17%) that they are aware of various cybersecurity measures. Only slightly more agree than disagree that they are familiar with current cybersecurity regulations, and there is also a relatively high percentage of neutral (24%) and don't know (12%) on this question.

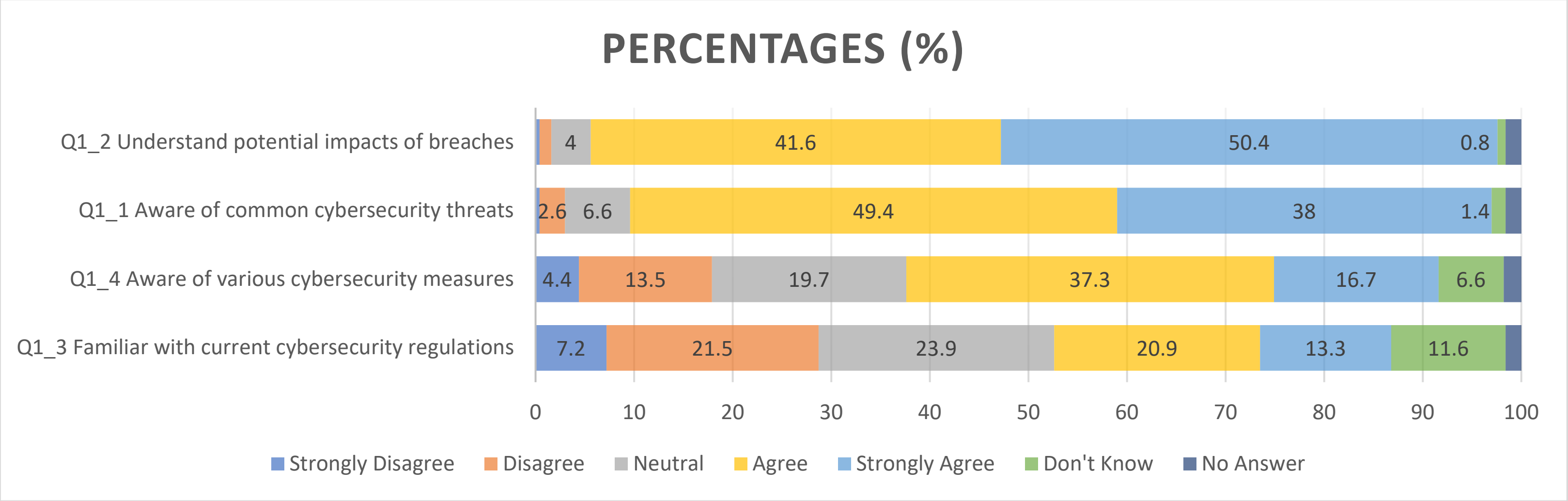


FIGURE 11. AWARENESS OF CYBERSECURITY THREATS, REGULATIONS, MEASURES

Appendix 2 provides breakouts of response by demographic type on all cybersecurity questions measured on the strongly disagree to strongly agree metric. When a difference by demographic type exceeds the survey's sampling margin of error, it suggests a possible difference not attributable to sampling variation. The report narrative notes differences that exceed 6% but leaves to the reader the question of whether it is substantively interesting/actionable difference, and further formal tests of statistically significant difference might be desired.

Breakout results on questions in Figure 11 by several sociodemographic characteristics (see Q1 series in Appendix 2) finds these demographic types tending to express higher percentages of strong agreement: use an online payment system for both client and vendor transactions, organization has experienced a malicious attack, organization has experienced a non-malicious data loss, government/school, organizations with 10 or more full-time employees, organizations of 25 years or more, organizations with professional services/financial/healthcare as main purpose/activity, organizations with government/education/library services as main purpose/activity, and have formal cybersecurity training. And, as might be expected, IT Directors/CIOs express far higher levels of strong agreement with all items in the figure.

Attitudes

Figure 12 shows over 70% expressing some level of agreement that investing in cybersecurity is crucial for safety (41% agree, 31% strongly agree) and employee cybersecurity training is effective (44% agree, 30% strongly agree). Well over 50% also at least agree that their organization regularly makes hardware and software security updates[2] (36% agree, 28% strongly agree), cybersecurity training helps save money in the long run (34% agree, 28% strongly agree), and they are willing to invest in employee security training (36% agree, 20% strongly agree). Less than 50% agree or strongly agree that they are confident identifying and responding to potential threats.

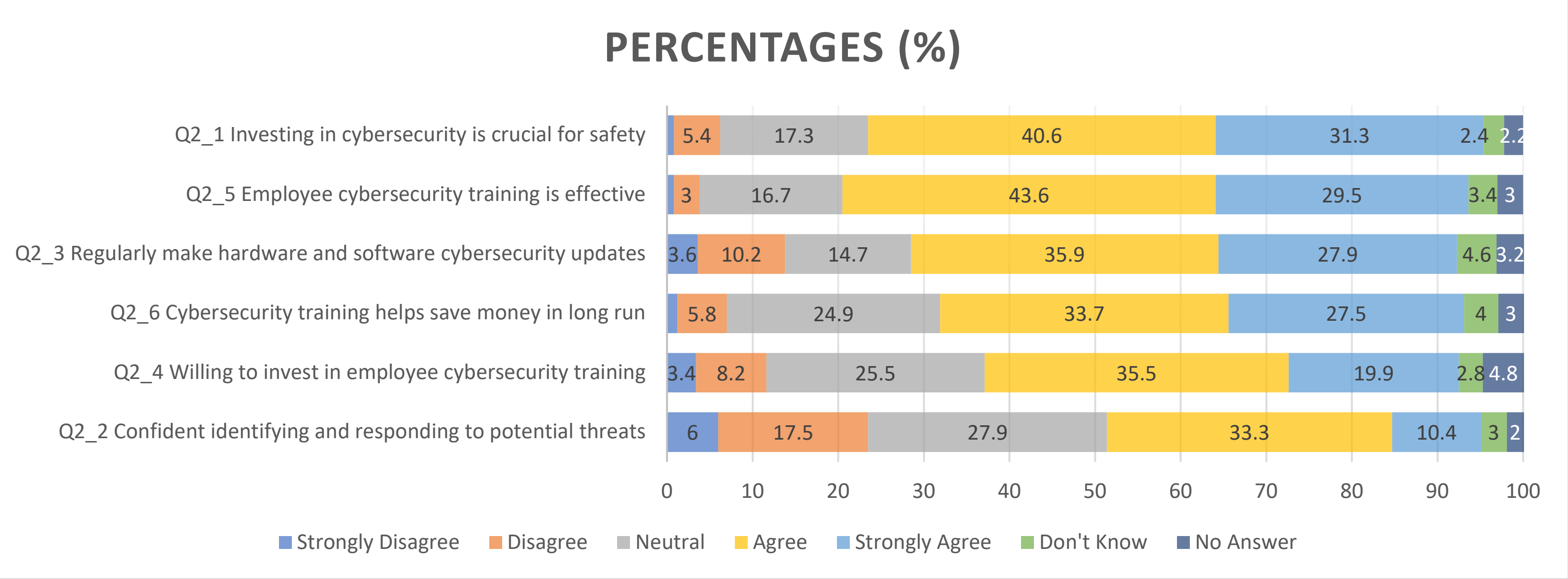


FIGURE 12. ATTITUDES ON EFFICACY OF SECURITY TRAINING

Examining breakout results in Appendix 2 by demographic type on items in Figure 12 (except for "regularly making hardware and software cybersecurity updates" for which breakout type tendencies are less consistent) the following demographic types tend to more strongly agree: use an online payment system for both client and vendor transactions, organization has experienced a malicious attack, organization has experienced a non-malicious data loss, government/school, organizations with 10 or more full-time employees, organizations of 25 years or more, organizations with professional services/financial/healthcare as main purpose/activity, organizations with government/education/library

[2] Of course, this question measures behavior but may be influenced by attitudes about the need for and efficacy of updating regularly.

services as main purpose/activity, and have formal cybersecurity training. And not surprisingly, IT Directors/CIOs express far higher levels of strong agreement with all items in the figure.

Needs

The "Needs" section had 13 questions tapping into various perceptions about the respondent's organizational cybersecurity needs. Figures 13 through 16 group those 13 questions in the section into subsets that measure organizational vulnerability, training needs, technical assistance needs, and resource limitations.

Organizational Vulnerability

Figure 13 shows results on questions that express some level of organizational vulnerability. About 50% agree that their organization lacks cybersecurity policy and incident response preparedness (32% agree, 19% strongly agree). About 42% at least agree that the organization has difficultly ensuring safe employee behavior. About 35% at least agree their organization faces challenges in managing third-party vendor risks, and about 27% at least agree the organization has insufficient back-up and recovery measures.

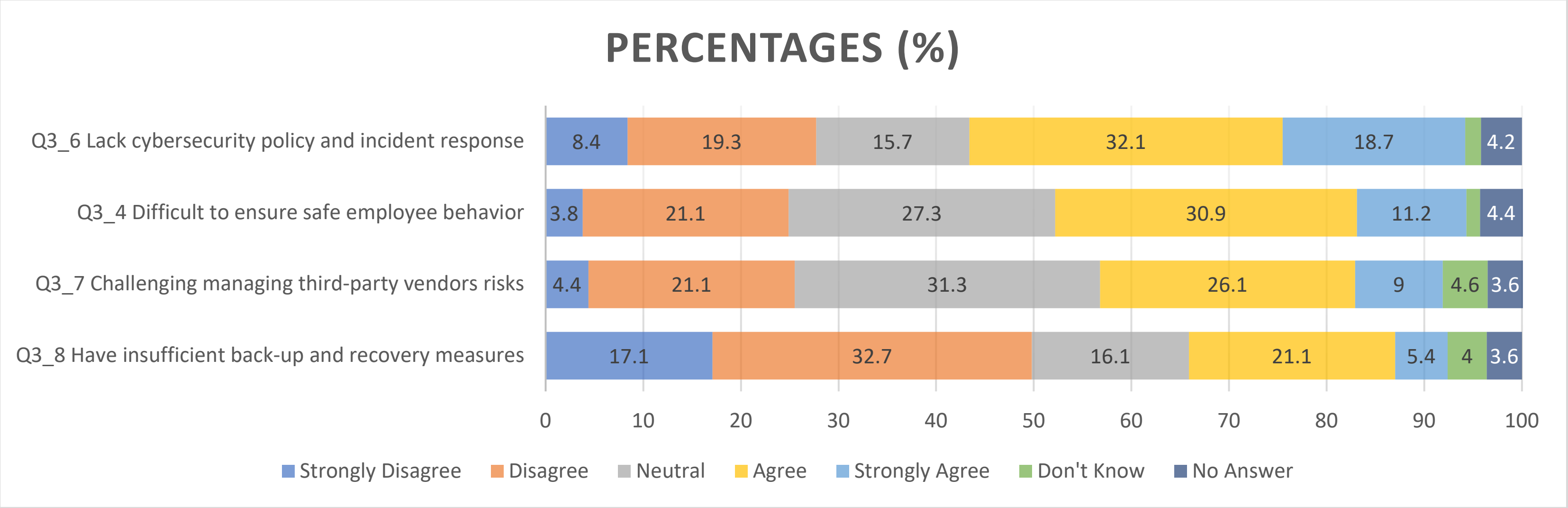


FIGURE 13. NEEDS – ORGANIZATIONAL VULNERABILITY

Breakouts of response in Appendix 2 finds strong agreement with the statement that it is difficult to ensure safe employee behavior (Q3_4) is higher among: those using an online payment system for both client and vendor transactions, nonprofit/not-for-profit organizations, IT Directors/CIOs, and those in cities with a population 50,000 or above.

Strong disagreement with the statement that the organization lacks cybersecurity policy and incident response plan (Q3_6) is higher for: those using an online payment system for both client and vendor transactions, organization has experienced a malicious attack, organization has experienced a non-malicious data loss, government/school, organizations with 10 or more full-time employees, organizations with professional services/financial/healthcare as main purpose/activity, organizations with government/education/library services as main purpose/activity, IT Directors/CIOs, and those who have formal cybersecurity training.

Strong disagreement with the statement that the organization has insufficient back-up and recovery measures (Q3_8) is higher for: organization has experienced a malicious attack, organizations with 10 or more full-time employees, directors/managers, IT Director/CIOs, and those who have formal cybersecurity training.

Organizational Training

Also included in the Needs section of the questionnaire were two items measuring perceived cybersecurity training needs to protect the organization. Figure 14 shows that about 43% at least agree (34% agree, 9% strongly agree) that they themself need training, "…to help me understand my company's cybersecurity risks and how to mitigate them." About 37% at least agree (29% agree, 8% strongly agree) that "My organization needs cybersecurity training to help protect our data and systems from cyber threats."

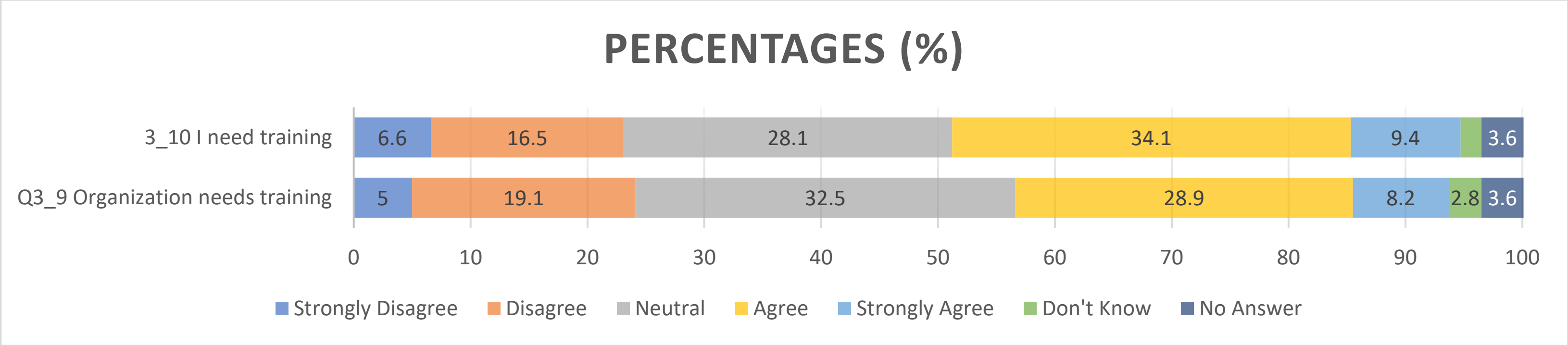


FIGURE 14. NEEDS – ORGANIZATIONAL TRAINING

Breakouts of response in Appendix 2 finds that strong disagreement with the statement "I need cybersecurity training to help me understand my company's cybersecurity risks and how to mitigate them" (Q3_10) is higher for: organization has experienced a malicious attack, organizations with 10 or more full-time employees, IT Directors/CIOs, and those who have formal cybersecurity training. Also, strong agreement with this same statement is higher for: those using an online payment system for both client and vendor transactions, those who don' know whether organization has experienced a malicious attack, those who don' know organization has experienced a non-malicious data loss, office administrator/manager/accountant/bookkeeper/treasurer, and director/manager.

Strong agreement with the statement the organization needs cybersecurity training (Q3_9) is higher for: those who don' know whether organization has experienced a malicious attack, organizations with government/education/library services as main purpose/activity, and directors/managers.

Technical Assistance

Figure 15 shows results from three questions pertaining to cybersecurity technical assistance needs of the organization. A solid majority of 68% at least agree (43% agree, 25% strongly agree) that they find it challenging to stay updated with evolving cybersecurity regulations and standards. About 56% at least agree (32% agree, 24% strongly agree) that the organization lacks the technical expertise to fully understand and mitigate complex cybersecurity threats. About 30% at least agree (20% agree, 10% strongly agree) that a barrier to their organization's cybersecurity is a lack of qualified cybersecurity trainers.

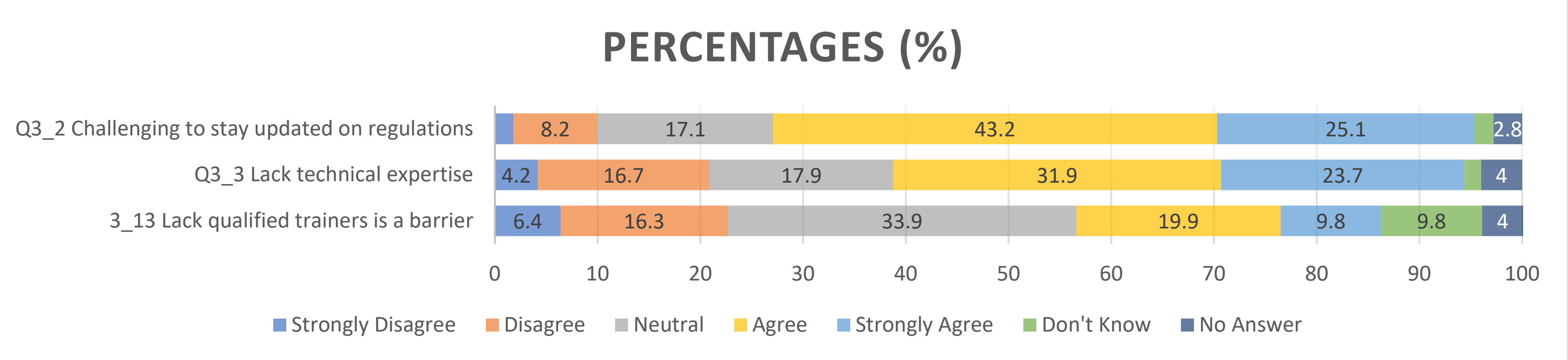


FIGURE 15. NEEDS -- TECHNICAL ASSISTANCE

Breakouts of response in Appendix 2 finds that strong agreement with the statement that "I find it challenging to keep up with evolving cybersecurity regulations and standards" (Q3_2) is higher for: those using an online payment system for both client and vendor transactions, those who don't know whether organization has experienced a malicious attack, nonprofit/not-for-profits (as compared to government/school), for-profit businesses (as compared to government/school), organizations with 0-4 or with 5-9 full-time employees (compared to 10 or more), retail and wholesale businesses, organizations in personal services/religious/housing, CEOs/Presidents/Owners/Partners, and those having no formal cybersecurity training.

Strong agreement with the statement that "We lack technical expertise to fully understand and mitigate complex cybersecurity threats" (Q3_3) is higher for: those whose organization has never experienced a malicious attack, those who don't know whether organization has experienced a malicious attack, those whose organization has never experienced non-malicious data loss, those who don't know whether organization has experienced a non-malicious data loss, nonprofit/not-for-profit, organizations with 0-4 and with 5-9 full-time employees (compared to 10 or more), retail and wholesale businesses, and those who have no formal cybersecurity training.

Strong agreement with the statement that “We lack technical expertise to fully understand and mitigate complex cybersecurity threats” (Q3_13) is higher for: those using an online payment system for both client and vendor transactions, those who don’t know whether organization has experienced a malicious attack, government/school (as compared to for-profits), nonprofit/not-for-profits (as compared to for-profit), organizations with 0-4 full-time employees, organizations younger than 25 years, office administrator/manager/accountant/bookkeeper/treasurer, those who have no formal cybersecurity training, and those living in cities of less than 5,000 population.

Resource Limitations

Figure 16 shows results for four questions that tap into perceived resource limitations hampering their organization’s level of cybersecurity. About 56% at least agree (36% agree, 20% strongly agree) that “Limited resources have made it difficult to invest in advanced cybersecurity measures.” Similar percentages of about 43% at least agree that time for cybersecurity training is a barrier for their organization and that costs and technical constraints limit updates to systems. Closely following is the 38% who at least agree that cybersecurity training cost is an organizational barrier.

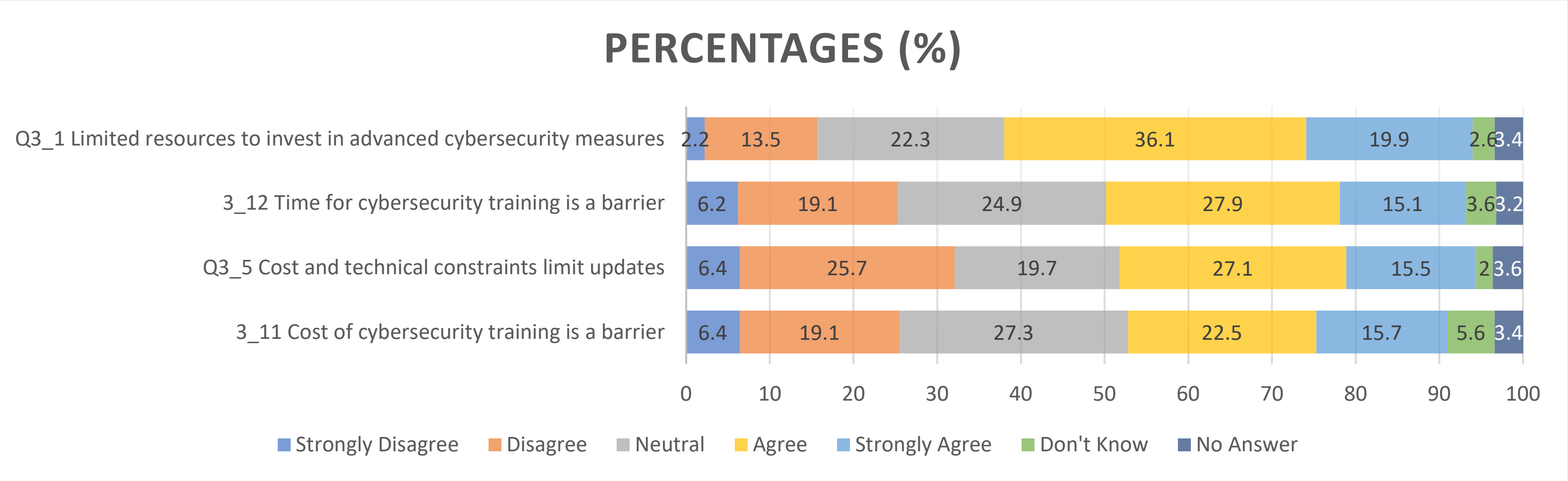


Figure 16. Needs -- Resource Limitations

As shown in breakouts of response in Appendix 2, strong agreement that organizational resources limitations make it difficult to invest in cybersecurity measures (Q3_1) is higher for: nonprofit/not-for-profits, organizations with 0-4 or with 5-9 full-time employees (compared to 10 or more), retail and wholesale businesses, organizations in personal services/religious/housing, CEOs/Presidents/Owners/Partners, directors/managers, and those having no formal cybersecurity training.

Strong agreement that time for cybersecurity training is a barrier (Q3_12) is higher for: nonprofit/not-for-profits, retail and wholesale businesses, organizations in personal services/religious/housing, government/education/libraries, and those having no formal cybersecurity training.

Strong agreement that cost and technical constraints limit updates (Q3_5) is higher for: those using an online payment system for both client and vendor transactions, those whose organization has never experienced non-malicious data loss, those who don't know whether organization has experienced a non-malicious data loss, nonprofit/not-for-profits, organizations with 0-4 or with 5-9 full-time employees (compared to 10 or more), retail and wholesale businesses, organizations in personal services/religious/housing, CEOs/Presidents/Owners/Partners, directors/managers, and those having no formal cybersecurity training.

Strong agreement that cost of cybersecurity training is a barrier (Q3_11) is higher for: those who don't know whether organization has experienced a malicious attack, those whose organization has never experienced non-malicious data loss, those who don't know whether organization has experienced a non-malicious data loss, nonprofit/not-for-profits, organizations with 0-4 full-time employees, retail and wholesale businesses, organizations in personal services/religious/housing, government/education/libraries, and those having no formal cybersecurity training.

Understanding

The next section of the questionnaire measured a respondent's perception of their own understanding about various aspects of cybersecurity significant to organizations[3]. Figure 17 shows there is little variation in response across items in the section measuring a respondent's perception of their own understanding of how cybersecurity is significant for their organization. Vast majorities express agreement to all statements, with "agree" response ranging from 39%-47% and "strongly agree" ranging from 24% to 44%.

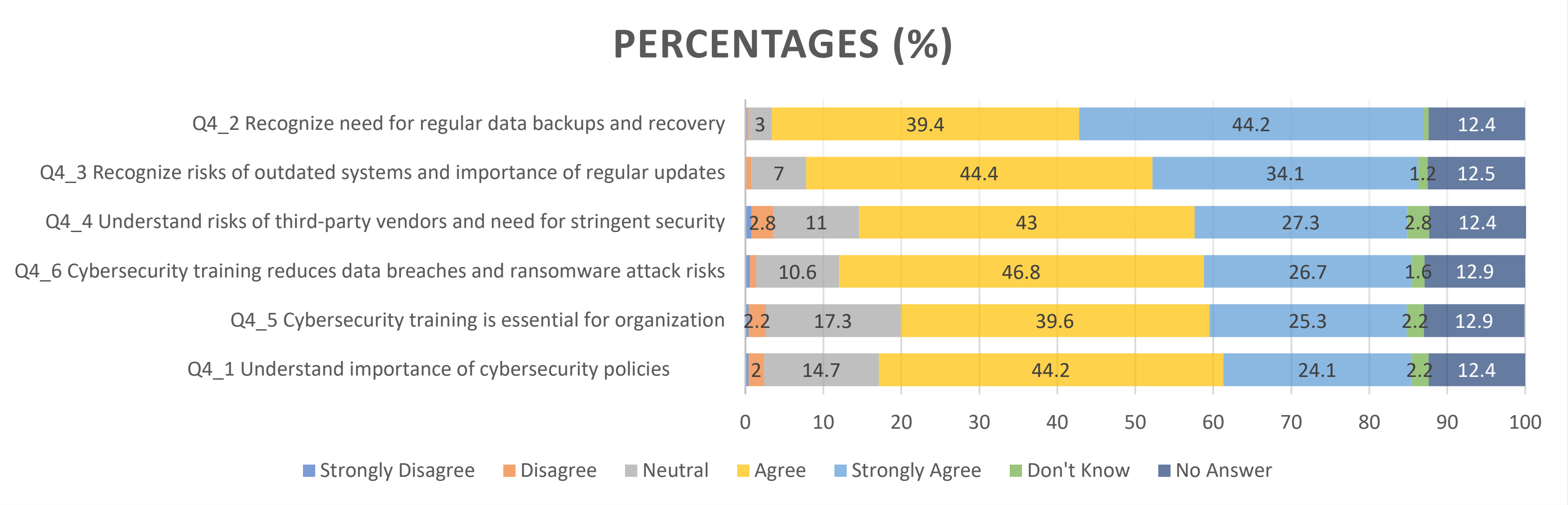


FIGURE 17. UNDERSTANDING SIGNIFICANCE OF ORGANIZATIONAL CYBERSECURITY

Breakout results on questions in Figure 17 by several sociodemographic characteristics finds the following demographic types tending to express higher percentages of strong agreement: use an online payment system for both client and vendor transactions, organization has experienced a

[3] This is a methodological note on the reason for relatively high "No Answer" in Figures 17 – 20. It appears that the inner-most booklet questionnaire pages (pages 3 and 4) were missed by about 40 respondents. Thus, the vast majority of the No Answer response on these pages did not come from respondents circling No Answer on the questionnaire. Instead, the pages were left blank and during keyed entry of data the numeric code for No Answer (9) was entered in the absence of a response to the questions on pages 3 and 4. Lower levels of No Answer resumed on items from page 5 to end.

malicious attack, organization has experienced a non-malicious data loss, governments/schools, organizations with 10 or more full-time employees, organizations of 25 years or more, organizations with professional services/financial/healthcare as main purpose/activity, organizations with government/education/library services as main purpose/activity, and have formal cybersecurity training. And, as might be expected, IT Directors/CIOs express far higher levels of strong agreement with all items in the figure.

Training

The final section of questions posed on the strongly disagree to strongly agree metric pertained to various dimensions of training. Figure 18 shows a combined 70% agree (47% agree, 23% strongly agree) that trainings should be regularly updated to latest cybersecurity threats. Almost half at least agree (42% agree, 17% strongly agree) that hands-on training is more beneficial than theoretical training. And agreement still exceeds disagreement on the following: interest in training on topics specific to my organization; access to a local support center would greatly benefit my organization; and willing to allocate budget and other resources for regular employee cybersecurity training. A separate "yes/no/unsure" question posed in the demographics section asked "Have you ever had any formal cybersecurity training?", to which only 37% responded affirmatively. This 37% is consistent with the 38% who agreed or strongly agreed with the statement "I have participated in training" shown in Figure 18.

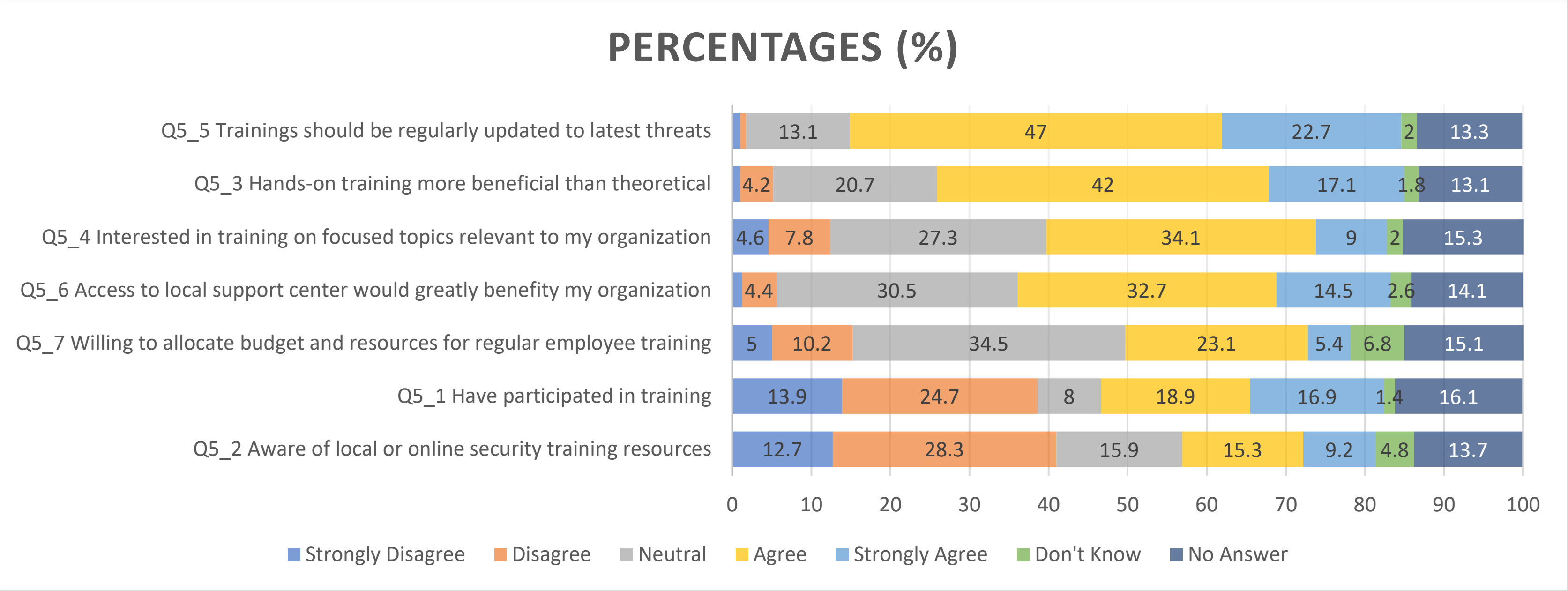


Figure 18. Training Attitudes, Awareness, Behavior

Breakout results on questions in Figure 18 by several sociodemographic characteristics finds the following demographic types tending to express higher percentages of strong agreement (but the tendencies are less consistent and of less magnitude than for those observed across items in Figures 11, 12, and 17): use an online payment system for both client and vendor transactions, organization has experienced a malicious attack, organization has experienced a non-malicious data loss, governments/schools, organizations of 25 years or more, organizations with professional services/financial/healthcare as main purpose/activity, organizations with government/education/library services as main purpose/activity, and have formal cybersecurity training. And, as might be expected, IT Directors/CIOs express far higher levels of strong agreement with all items in the figure.

Attack or Data Loss Experience

The organizational cybersecurity questions concluded with a question about experience with a malicious event and a question about experience with non-malicious data loss. Figure 19 shows that 61% indicate their organization has never, to their knowledge, experienced a malicious cybersecurity event, and Figure 20 shows that a very similar percentage, 58%, say their organization has not experienced a non-malicious data loss event, to their knowledge.

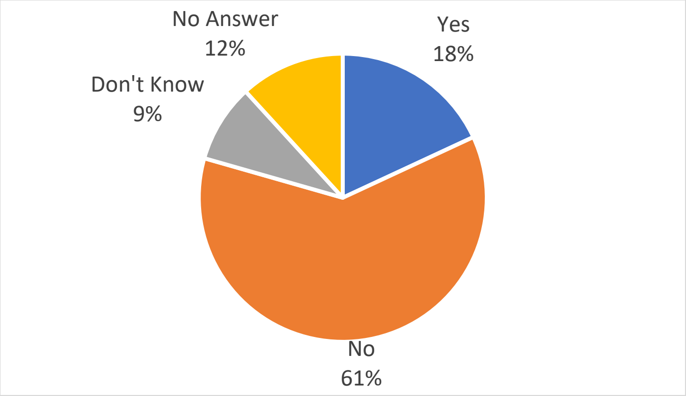


FIGURE 19. ORGANIZATION EVER EXPERIENCED A MALICIOUS CYBERSECURITY EVENT

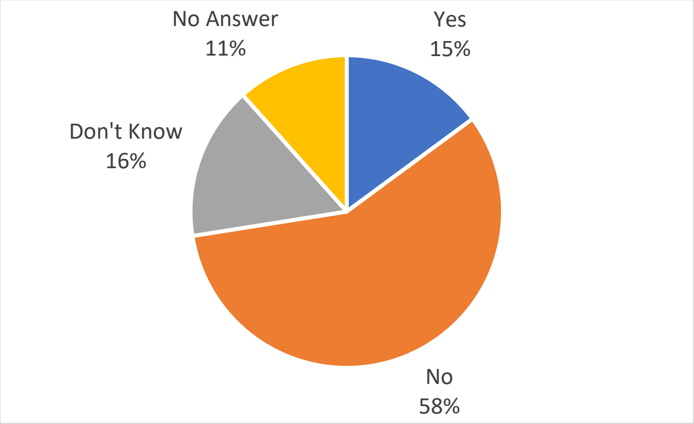
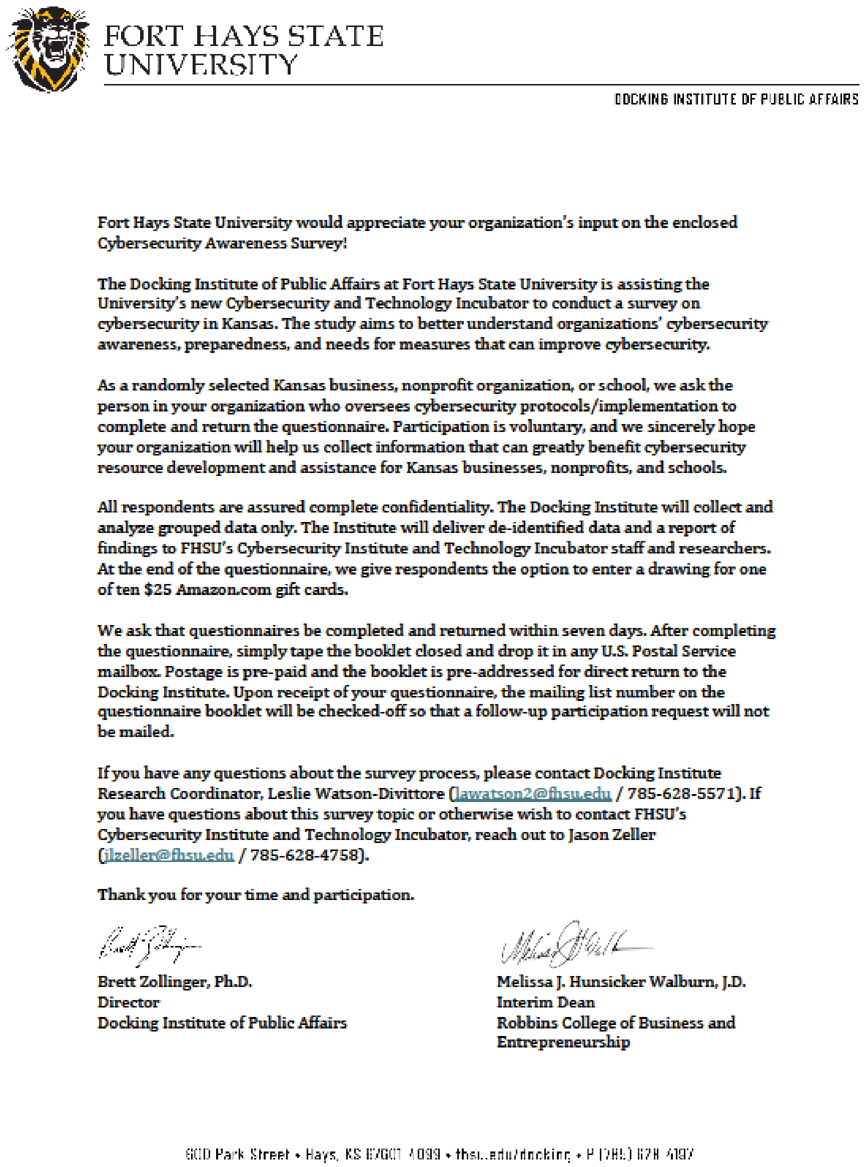


FIGURE 20. ORGANIZATION EVER EXPERIENCED NON-MALICIOUS DATA LOSS EVENT

Appendix 1: Questionnaire



FORT HAYS STATE
UNIVERSITY

DOCKING INSTITUTE OF PUBLIC AFFAIRS

Fort Hays State University would appreciate your organization's input on the enclosed Cybersecurity Awareness Survey!

The Docking Institute of Public Affairs at Fort Hays State University is assisting the University's new Cybersecurity and Technology Incubator to conduct a survey on cybersecurity in Kansas. The study aims to better understand organizations' cybersecurity awareness, preparedness, and needs for measures that can improve cybersecurity.

As a randomly selected Kansas business, nonprofit organization, or school, we ask the person in your organization who oversees cybersecurity protocols/implementation to complete and return the questionnaire. Participation is voluntary, and we sincerely hope your organization will help us collect information that can greatly benefit cybersecurity resource development and assistance for Kansas businesses, nonprofits, and schools.

All respondents are assured complete confidentiality. The Docking Institute will collect and analyze grouped data only. The Institute will deliver de-identified data and a report of findings to FHSU's Cybersecurity Institute and Technology Incubator staff and researchers. At the end of the questionnaire, we give respondents the option to enter a drawing for one of ten $25 Amazon.com gift cards.

We ask that questionnaires be completed and returned within seven days. After completing the questionnaire, simply tape the booklet closed and drop it in any U.S. Postal Service mailbox. Postage is pre-paid and the booklet is pre-addressed for direct return to the Docking Institute. Upon receipt of your questionnaire, the mailing list number on the questionnaire booklet will be checked-off so that a follow-up participation request will not be mailed.

If you have any questions about the survey process, please contact Docking Institute Research Coordinator, Leslie Watson-Divittore (lawatson2@fhsu.edu / 785-628-5571). If you have questions about this survey topic or otherwise wish to contact FHSU's Cybersecurity Institute and Technology Incubator, reach out to Jason Zeller (jlzeller@fhsu.edu / 785-628-4758).

Thank you for your time and participation.

Brett Zollinger, Ph.D. Director Docking Institute of Public Affairs	Melissa J. Hunsicker Walburn, J.D. Interim Dean Robbins College of Business and Entrepreneurship

600 Park Street • Hays, KS 67601-4099 • fhsu.edu/docking • P (785) 628-4197

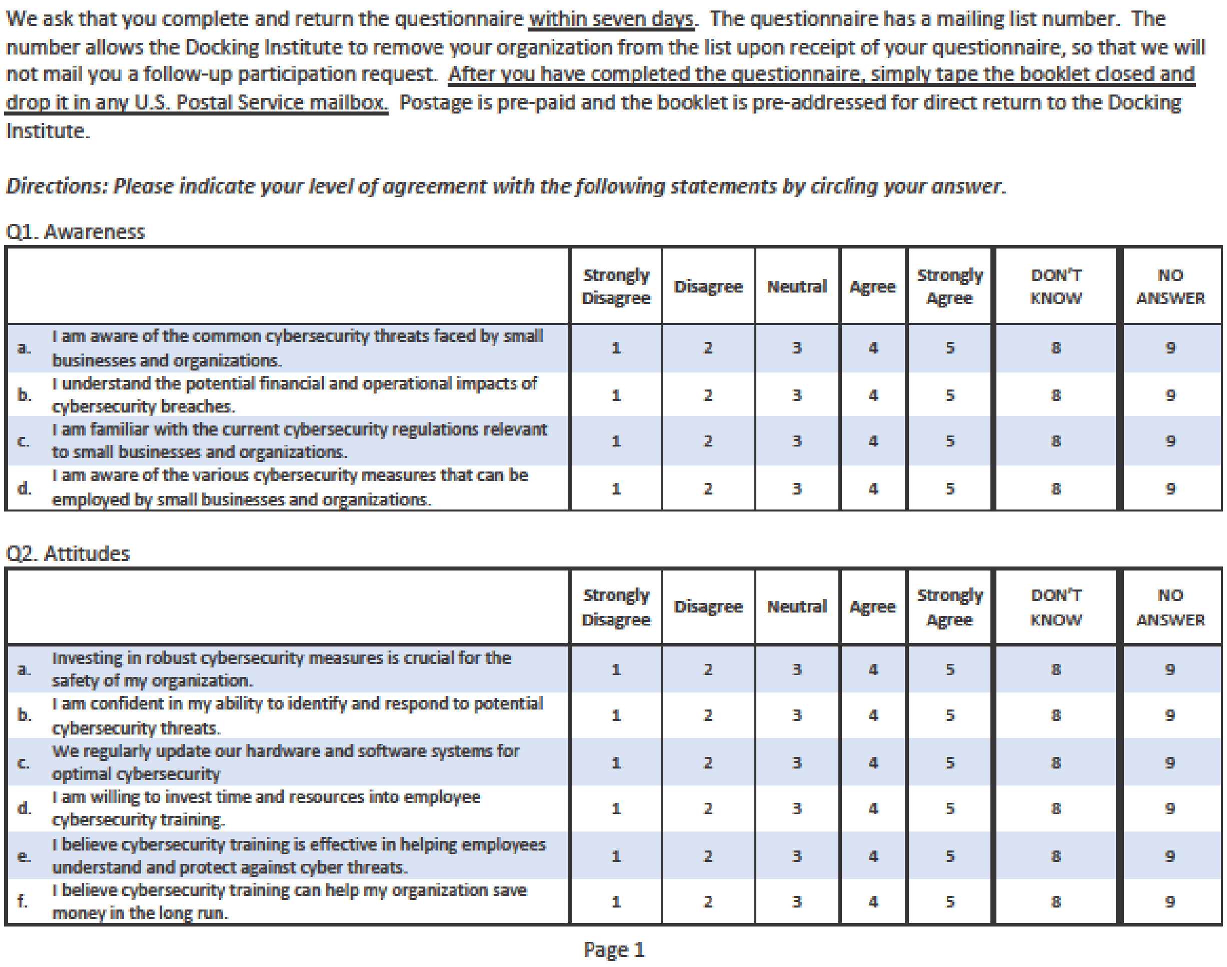
FORT HAYS STATE UNIVERSITY
ROBBINS COLLEGE OF BUSINESS AND ENTREPRENEURSHIP

Cybersecurity Awareness Survey

Sponsored by
FHSU Cybersecurity and Technology Incubator

Conducted by
FHSU Docking Institute of Public Affairs

DOCKING INSTITUTE Of Public Affairs
FORT HAYS STATE UNIVERSITY



We ask that you complete and return the questionnaire within seven days. The questionnaire has a mailing list number. The number allows the Docking Institute to remove your organization from the list upon receipt of your questionnaire, so that we will not mail you a follow-up participation request. After you have completed the questionnaire, simply tape the booklet closed and drop it in any U.S. Postal Service mailbox. Postage is pre-paid and the booklet is pre-addressed for direct return to the Docking Institute.

Directions: Please indicate your level of agreement with the following statements by circling your answer.

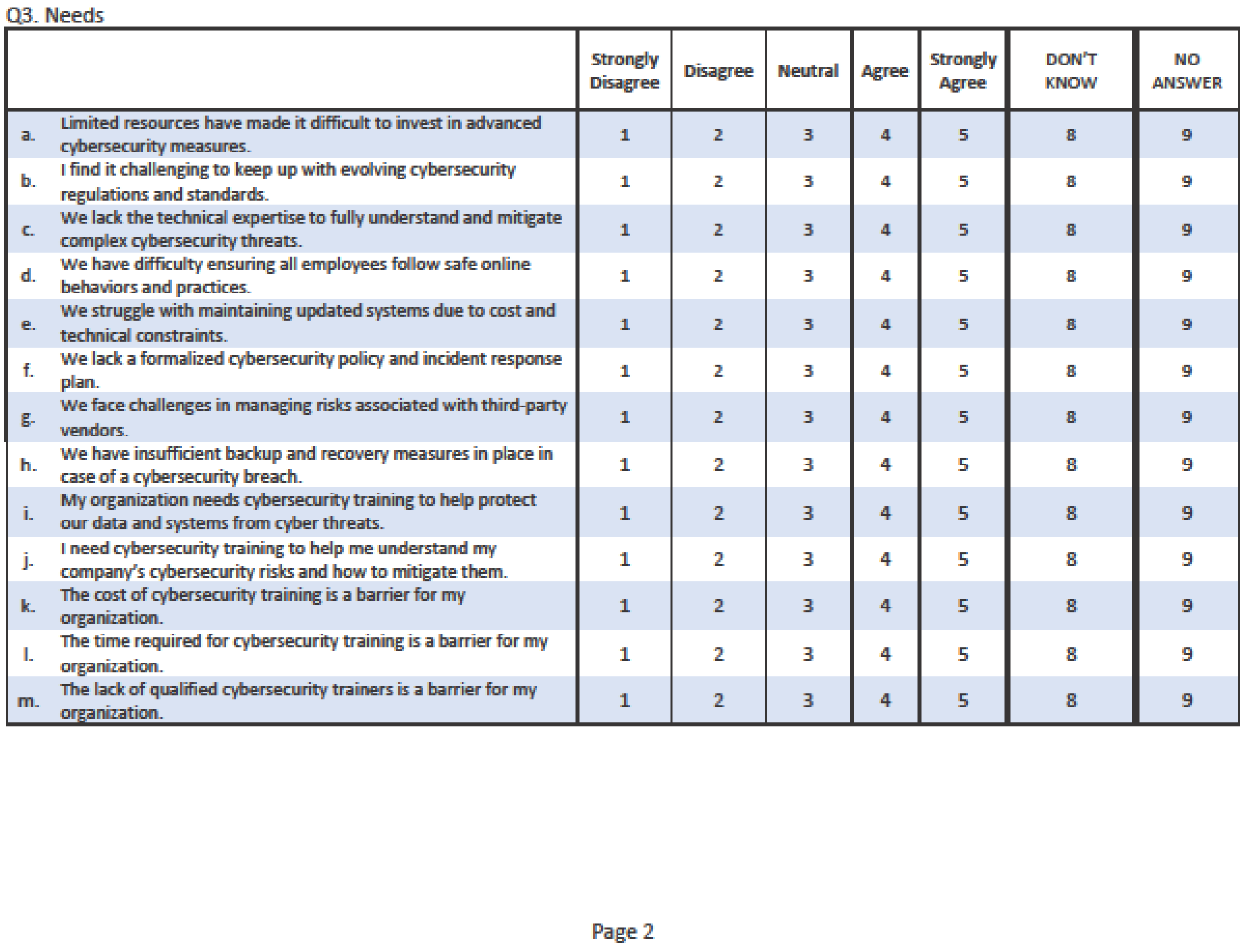
Q1. Awareness

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	DON'T KNOW	NO ANSWER
a.	I am aware of the common cybersecurity threats faced by small businesses and organizations.	1	2	3	4	5	8	9
b.	I understand the potential financial and operational impacts of cybersecurity breaches.	1	2	3	4	5	8	9
c.	I am familiar with the current cybersecurity regulations relevant to small businesses and organizations.	1	2	3	4	5	8	9
d.	I am aware of the various cybersecurity measures that can be employed by small businesses and organizations.	1	2	3	4	5	8	9

Q2. Attitudes

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	DON'T KNOW	NO ANSWER
a.	Investing in robust cybersecurity measures is crucial for the safety of my organization.	1	2	3	4	5	8	9
b.	I am confident in my ability to identify and respond to potential cybersecurity threats.	1	2	3	4	5	8	9
c.	We regularly update our hardware and software systems for optimal cybersecurity	1	2	3	4	5	8	9
d.	I am willing to invest time and resources into employee cybersecurity training.	1	2	3	4	5	8	9
e.	I believe cybersecurity training is effective in helping employees understand and protect against cyber threats.	1	2	3	4	5	8	9
f.	I believe cybersecurity training can help my organization save money in the long run.	1	2	3	4	5	8	9

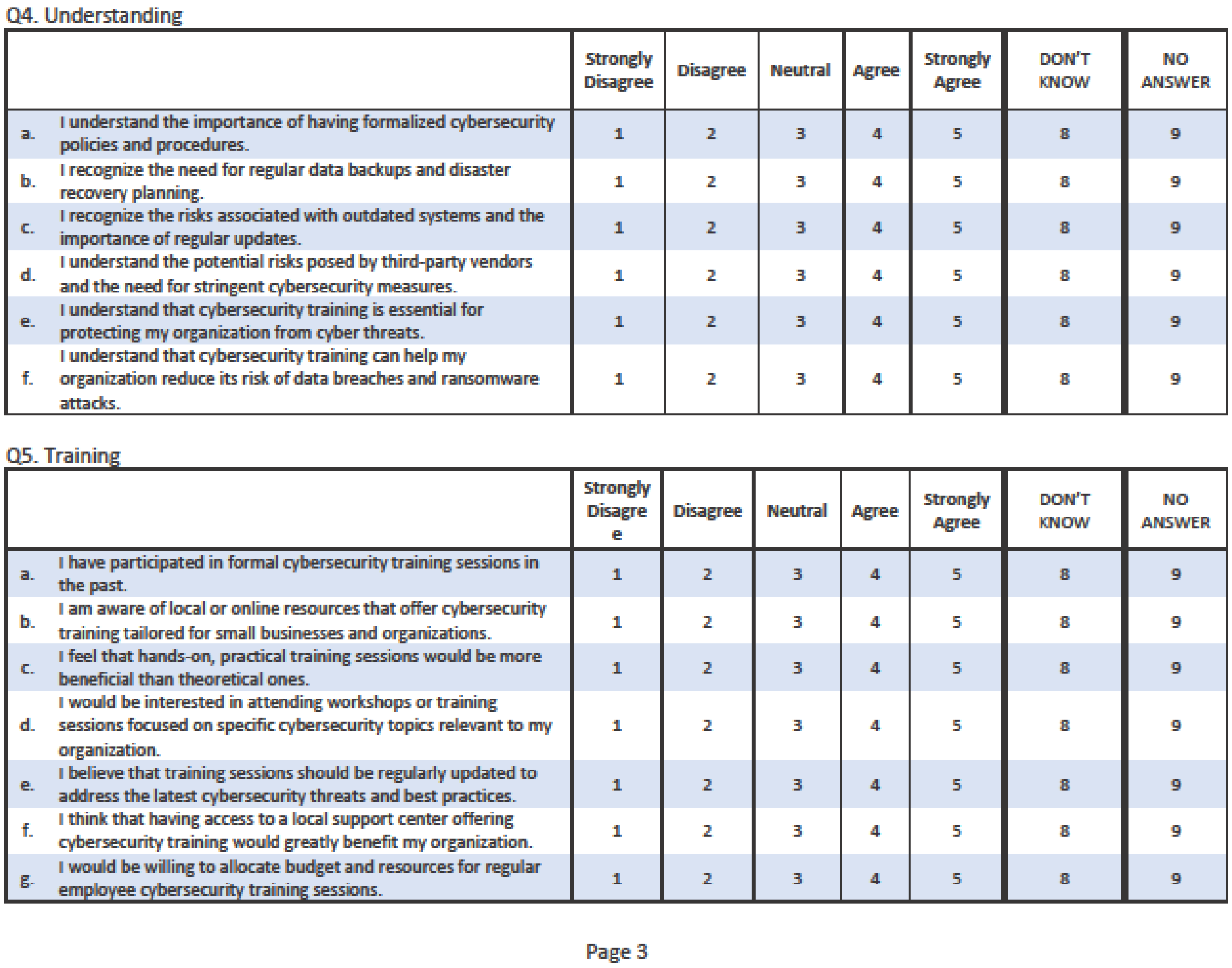
Page 1



Q3. Needs

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	DON'T KNOW	NO ANSWER
a.	Limited resources have made it difficult to invest in advanced cybersecurity measures.	1	2	3	4	5	8	9
b.	I find it challenging to keep up with evolving cybersecurity regulations and standards.	1	2	3	4	5	8	9
c.	We lack the technical expertise to fully understand and mitigate complex cybersecurity threats.	1	2	3	4	5	8	9
d.	We have difficulty ensuring all employees follow safe online behaviors and practices.	1	2	3	4	5	8	9
e.	We struggle with maintaining updated systems due to cost and technical constraints.	1	2	3	4	5	8	9
f.	We lack a formalized cybersecurity policy and incident response plan.	1	2	3	4	5	8	9
g.	We face challenges in managing risks associated with third-party vendors.	1	2	3	4	5	8	9
h.	We have insufficient backup and recovery measures in place in case of a cybersecurity breach.	1	2	3	4	5	8	9
i.	My organization needs cybersecurity training to help protect our data and systems from cyber threats.	1	2	3	4	5	8	9
j.	I need cybersecurity training to help me understand my company's cybersecurity risks and how to mitigate them.	1	2	3	4	5	8	9
k.	The cost of cybersecurity training is a barrier for my organization.	1	2	3	4	5	8	9
l.	The time required for cybersecurity training is a barrier for my organization.	1	2	3	4	5	8	9
m.	The lack of qualified cybersecurity trainers is a barrier for my organization.	1	2	3	4	5	8	9

Page 2



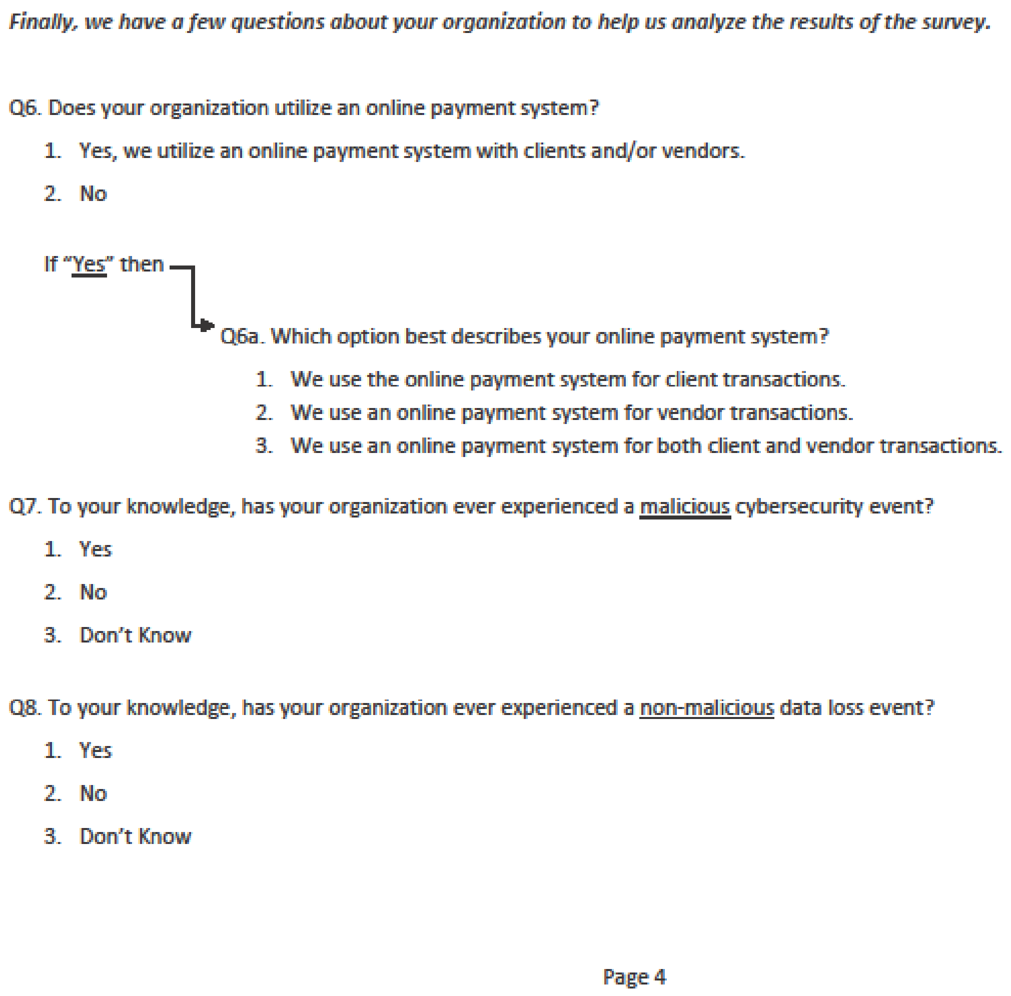
Q4. Understanding

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	DON'T KNOW	NO ANSWER
a.	I understand the importance of having formalized cybersecurity policies and procedures.	1	2	3	4	5	8	9
b.	I recognize the need for regular data backups and disaster recovery planning.	1	2	3	4	5	8	9
c.	I recognize the risks associated with outdated systems and the importance of regular updates.	1	2	3	4	5	8	9
d.	I understand the potential risks posed by third-party vendors and the need for stringent cybersecurity measures.	1	2	3	4	5	8	9
e.	I understand that cybersecurity training is essential for protecting my organization from cyber threats.	1	2	3	4	5	8	9
f.	I understand that cybersecurity training can help my organization reduce its risk of data breaches and ransomware attacks.	1	2	3	4	5	8	9

Q5. Training

		Strongly Disagre e	Disagree	Neutral	Agree	Strongly Agree	DON'T KNOW	NO ANSWER
a.	I have participated in formal cybersecurity training sessions in the past.	1	2	3	4	5	8	9
b.	I am aware of local or online resources that offer cybersecurity training tailored for small businesses and organizations.	1	2	3	4	5	8	9
c.	I feel that hands-on, practical training sessions would be more beneficial than theoretical ones.	1	2	3	4	5	8	9
d.	I would be interested in attending workshops or training sessions focused on specific cybersecurity topics relevant to my organization.	1	2	3	4	5	8	9
e.	I believe that training sessions should be regularly updated to address the latest cybersecurity threats and best practices.	1	2	3	4	5	8	9
f.	I think that having access to a local support center offering cybersecurity training would greatly benefit my organization.	1	2	3	4	5	8	9
g.	I would be willing to allocate budget and resources for regular employee cybersecurity training sessions.	1	2	3	4	5	8	9

Page 3



Finally, we have a few questions about your organization to help us analyze the results of the survey.

Q6. Does your organization utilize an online payment system?

1. Yes, we utilize an online payment system with clients and/or vendors.
2. No

If "Yes" then

Q6a. Which option best describes your online payment system?

1. We use the online payment system for client transactions.
2. We use an online payment system for vendor transactions.
3. We use an online payment system for both client and vendor transactions.

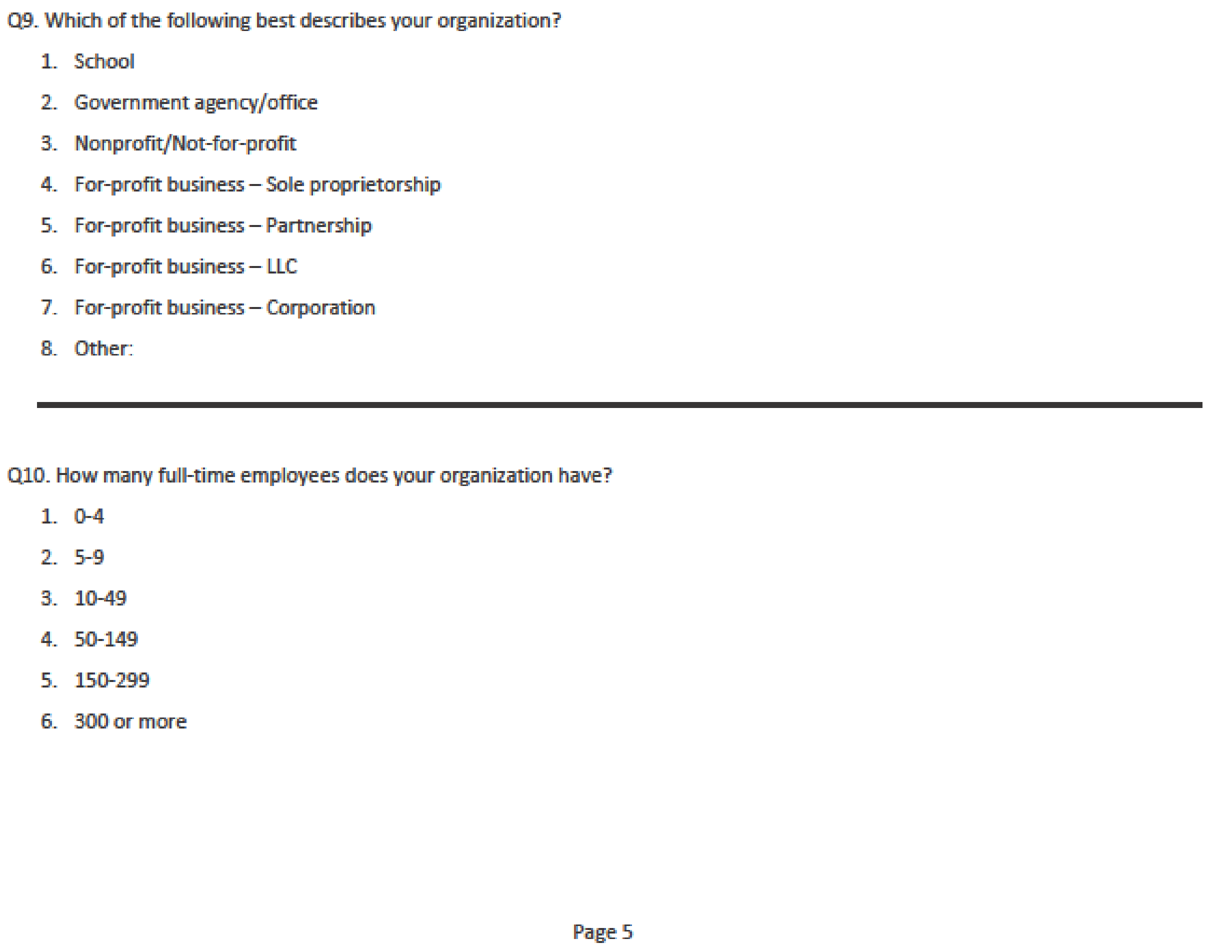
Q7. To your knowledge, has your organization ever experienced a malicious cybersecurity event?

1. Yes
2. No
3. Don't Know

Q8. To your knowledge, has your organization ever experienced a non-malicious data loss event?

1. Yes
2. No
3. Don't Know

Page 4

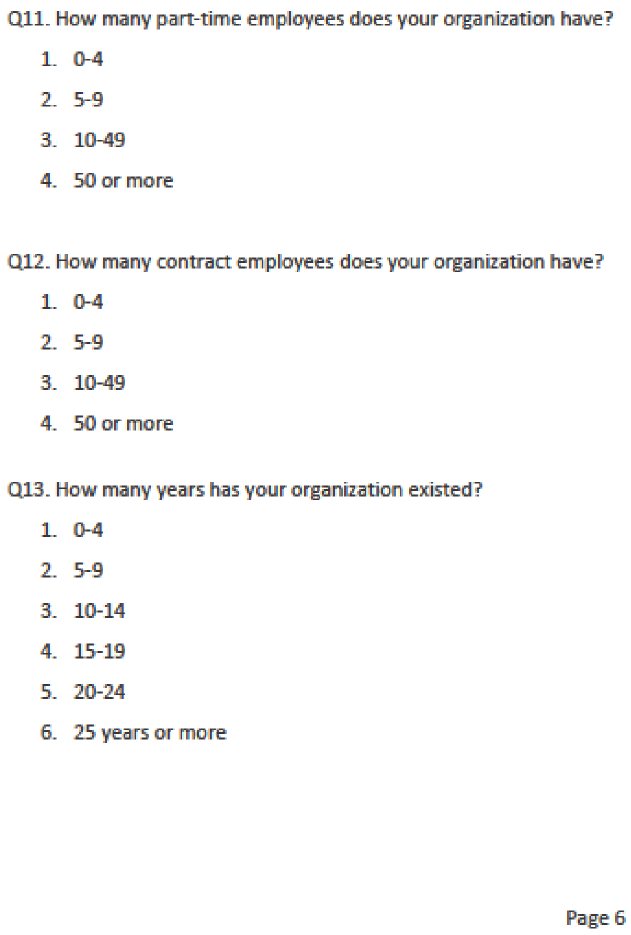


Q9. Which of the following best describes your organization?

1. School
2. Government agency/office
3. Nonprofit/Not-for-profit
4. For-profit business – Sole proprietorship
5. For-profit business – Partnership
6. For-profit business – LLC
7. For-profit business – Corporation
8. Other:

Q10. How many full-time employees does your organization have?

1. 0-4
2. 5-9
3. 10-49
4. 50-149
5. 150-299
6. 300 or more



Q11. How many part-time employees does your organization have?

1. 0-4
2. 5-9
3. 10-49
4. 50 or more

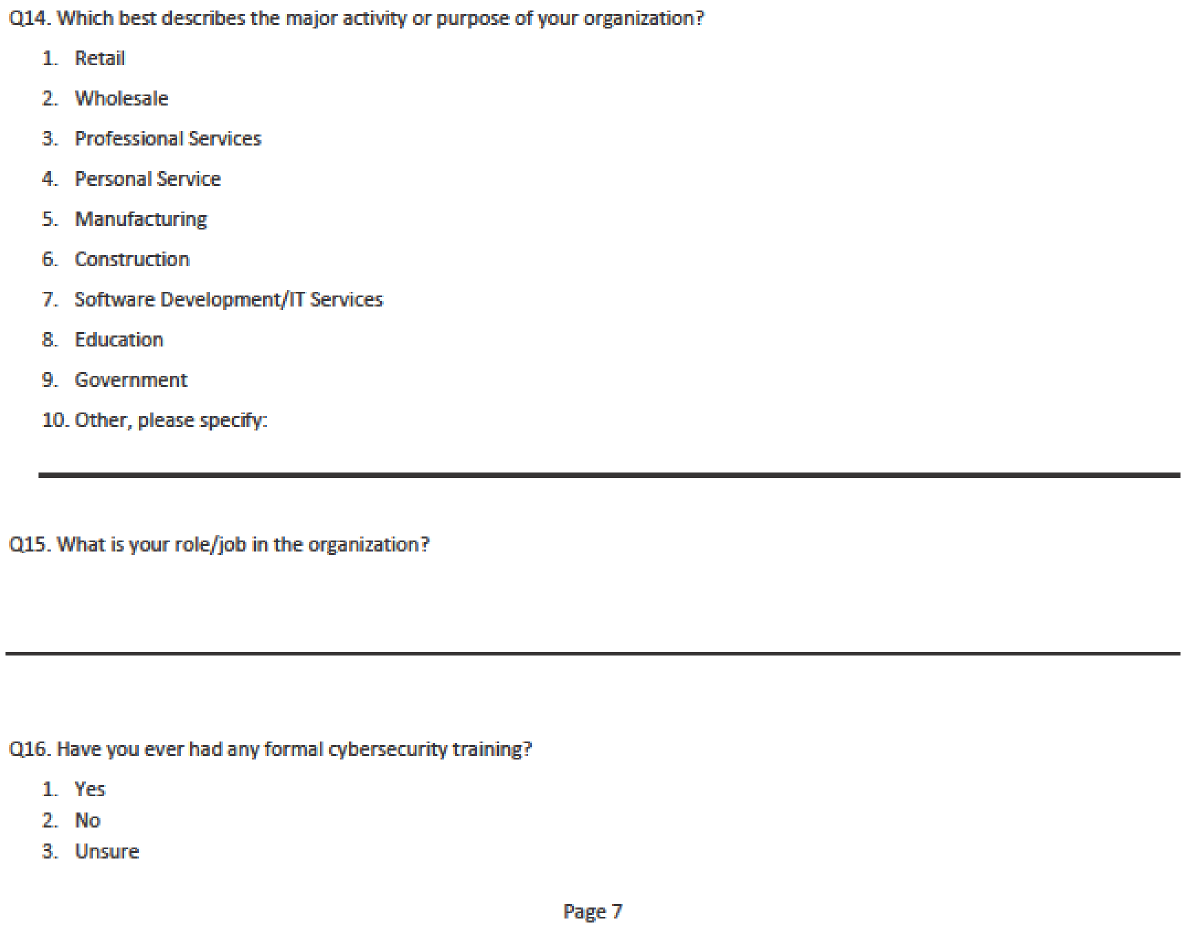
Q12. How many contract employees does your organization have?

1. 0-4
2. 5-9
3. 10-49
4. 50 or more

Q13. How many years has your organization existed?

1. 0-4
2. 5-9
3. 10-14
4. 15-19
5. 20-24
6. 25 years or more

Page 6



Q14. Which best describes the major activity or purpose of your organization?

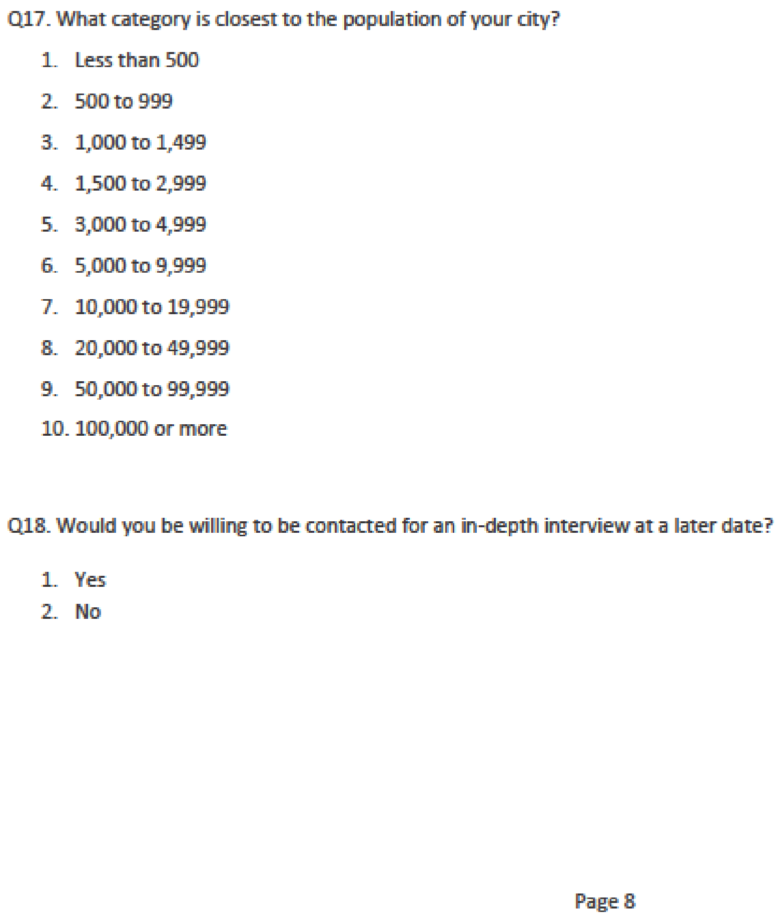
1. Retail
2. Wholesale
3. Professional Services
4. Personal Service
5. Manufacturing
6. Construction
7. Software Development/IT Services
8. Education
9. Government
10. Other, please specify:

Q15. What is your role/job in the organization?

Q16. Have you ever had any formal cybersecurity training?

1. Yes
2. No
3. Unsure

Page 7

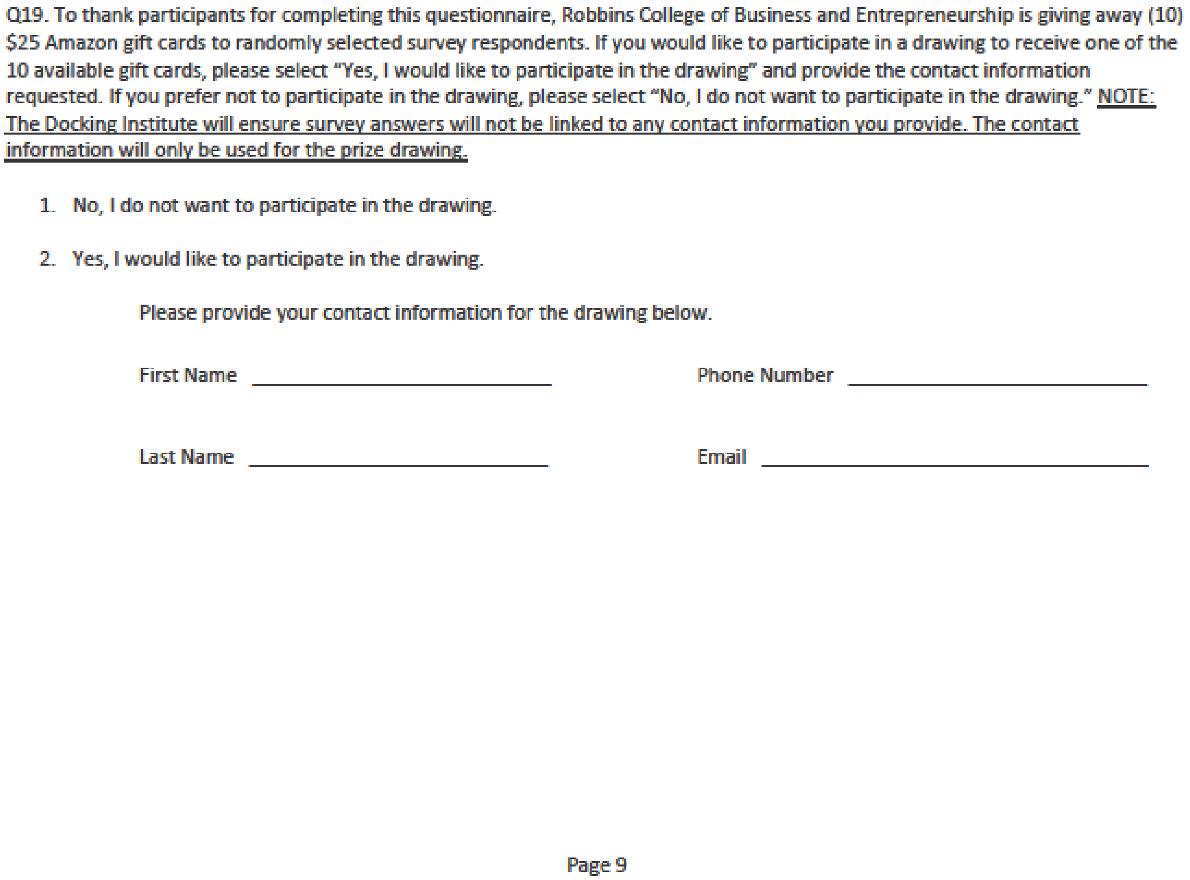


Q17. What category is closest to the population of your city?

1. Less than 500
2. 500 to 999
3. 1,000 to 1,499
4. 1,500 to 2,999
5. 3,000 to 4,999
6. 5,000 to 9,999
7. 10,000 to 19,999
8. 20,000 to 49,999
9. 50,000 to 99,999
10. 100,000 or more

Q18. Would you be willing to be contacted for an in-depth interview at a later date?

1. Yes
2. No



Q19. To thank participants for completing this questionnaire, Robbins College of Business and Entrepreneurship is giving away (10) $25 Amazon gift cards to randomly selected survey respondents. If you would like to participate in a drawing to receive one of the 10 available gift cards, please select "Yes, I would like to participate in the drawing" and provide the contact information requested. If you prefer not to participate in the drawing, please select "No, I do not want to participate in the drawing." NOTE: The Docking Institute will ensure survey answers will not be linked to any contact information you provide. The contact information will only be used for the prize drawing.

1. No, I do not want to participate in the drawing.
2. Yes, I would like to participate in the drawing.

Please provide your contact information for the drawing below.

First Name ____________________________ Phone Number ____________________________

Last Name ____________________________ Email ____________________________________

Page 9

Appendix 2: Survey Response by Selected Sociodemographic Characteristic

This appendix contains breakout response by select sociodemographic types.

For reviewing these crosstabs, use the Zoom feature in Adobe.

Q1_1 – Q1_4: Demographic Group A (Q6Combined, Q7, Q8, Q9_CodedCombined)

		Q6Combined Online payment system usage				Q7 Experienced a malicious cybersecurity event			Q8 Experienced a non-malicious data loss			Q9_CodedCombined Organization		
		Client transactions	Vendor transactions	Both	No online payment system	Yes	No	Don't Know	Yes	No	Don't Know	Govt/School	Nonprofit/not-for-profit	For-profit business
Q1_1 Aware of common cybersecurity threats	Strongly Disagree	1.9%	0.0%	0.0%	0.0%	0.0%	0.7%	0.0%	0.0%	0.3%	1.3%	0.0%	0.0%	0.6%
	Disagree	1.9%	5.6%	2.5%	2.3%	0.0%	3.0%	7.0%	1.3%	2.1%	6.3%	1.3%	4.5%	2.5%
	Neutral	2.9%	11.1%	5.0%	7.5%	2.2%	7.2%	7.0%	4.0%	5.6%	10.1%	3.8%	9.0%	6.6%
	Agree	50.0%	52.8%	51.3%	53.4%	50.5%	51.8%	51.2%	50.7%	53.8%	44.3%	40.0%	52.8%	51.9%
	Strongly Agree	42.3%	30.6%	39.5%	35.1%	46.2%	36.1%	32.6%	44.0%	37.1%	34.2%	55.0%	32.6%	36.5%
	Don't Know	1.0%	0.0%	1.7%	1.7%	1.1%	1.3%	2.3%	0.0%	1.0%	3.8%	0.0%	1.1%	1.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_2 Understand potential impacts of breaches	Strongly Disagree	1.0%	0.0%	0.0%	0.0%	0.0%	0.3%	0.0%	0.0%	0.0%	1.3%	0.0%	0.0%	0.6%
	Disagree	1.0%	5.6%	0.8%	0.6%	1.1%	1.3%	2.3%	1.3%	0.7%	3.8%	0.0%	1.1%	1.6%
	Neutral	4.8%	5.6%	2.5%	4.6%	4.4%	3.6%	9.3%	5.3%	3.5%	6.3%	3.8%	6.7%	2.8%
	Agree	43.8%	41.7%	42.0%	43.4%	31.9%	47.5%	30.2%	38.7%	46.2%	32.9%	37.5%	43.8%	42.8%
	Strongly Agree	49.5%	47.2%	54.6%	49.7%	62.6%	46.6%	55.8%	54.7%	49.3%	53.2%	58.8%	48.3%	50.9%
	Don't Know	0.0%	0.0%	0.0%	1.7%	0.0%	0.7%	2.3%	0.0%	0.3%	2.5%	0.0%	0.0%	1.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_3 Familiar with current cybersecurity regulations	Strongly Disagree	7.6%	8.3%	4.2%	9.2%	2.2%	9.2%	4.7%	1.3%	8.4%	8.9%	6.3%	11.4%	6.6%
	Disagree	21.9%	30.6%	21.0%	22.0%	23.1%	23.3%	18.6%	21.3%	21.7%	27.8%	15.0%	23.9%	22.9%
	Neutral	29.5%	33.3%	19.3%	24.9%	18.7%	25.9%	30.2%	16.0%	28.0%	21.5%	20.0%	29.5%	24.1%
	Agree	22.9%	19.4%	26.9%	16.8%	29.7%	19.3%	16.3%	34.7%	19.6%	15.2%	28.7%	15.9%	20.7%
	Strongly Agree	11.4%	2.8%	19.3%	12.1%	20.9%	11.1%	11.6%	20.0%	11.2%	13.9%	25.0%	8.0%	12.2%
	Don't Know	6.7%	5.6%	9.2%	15.0%	5.5%	11.1%	18.6%	6.7%	11.2%	12.7%	5.0%	11.4%	13.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_4 Aware of various cybersecurity measures	Strongly Disagree	6.7%	5.7%	2.5%	5.7%	0.0%	6.2%	7.0%	1.4%	5.6%	6.3%	2.5%	6.7%	4.4%
	Disagree	13.5%	17.1%	13.4%	12.6%	5.6%	15.7%	14.0%	13.5%	12.9%	15.2%	12.5%	13.5%	14.2%
	Neutral	24.0%	17.1%	16.0%	23.0%	14.4%	21.0%	32.6%	14.9%	21.3%	24.1%	11.3%	27.0%	19.9%
	Agree	32.7%	45.7%	41.2%	37.4%	46.7%	36.7%	25.6%	40.5%	38.5%	32.9%	38.8%	38.2%	37.9%
	Strongly Agree	20.2%	5.7%	22.7%	12.1%	30.0%	13.1%	14.0%	25.7%	14.7%	15.2%	32.5%	9.0%	15.5%
	Don't Know	2.9%	8.6%	4.2%	9.2%	3.3%	7.2%	7.0%	4.1%	7.0%	6.3%	2.5%	5.6%	8.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q1_1 – Q1_4: Demographic Group B (Q10_Coded Q11_Coded Q12 Q13_Coded Q14_CodedCombine)

		Q10_Coded Full-time employees			Q11_Coded Part-time employees		Q13_Coded Years of organization		Q14_CodedCombined Purpose of organization				
		0-4	5-9	10 and Above	0-4	5 and Above	Under 25 years	25 years or over	Retail, wholesale	Professional services, financial, healthcare	Personal services, religious, housing	Manufacturing, construction, agriculture	Government, education, library
Q1_1 Aware of common cybersecurity threats	Strongly Disagree	0.5%	0.0%	0.8%	0.3%	0.8%	1.9%	0.0%	1.4%	0.0%	1.1%	0.0%	0.0%
	Disagree	2.4%	3.8%	4.2%	2.6%	3.0%	3.7%	2.4%	2.9%	0.0%	4.3%	5.0%	2.3%
	Neutral	9.2%	5.1%	6.8%	6.6%	6.8%	4.6%	7.1%	5.8%	8.1%	7.6%	7.5%	4.7%
	Agree	54.1%	59.0%	47.5%	53.2%	42.1%	55.6%	48.4%	50.7%	43.5%	55.4%	58.8%	43.0%
	Strongly Agree	31.4%	30.8%	40.7%	35.9%	45.9%	33.3%	40.5%	37.7%	46.0%	30.4%	26.3%	50.0%
	Don't Know	2.4%	1.3%	0.0%	1.4%	1.5%	0.9%	1.6%	1.4%	2.4%	1.1%	2.5%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_2 Understand potential impacts of breaches	Strongly Disagree	0.5%	0.0%	0.8%	0.3%	0.8%	0.9%	0.3%	0.0%	0.0%	2.2%	0.0%	0.0%
	Disagree	1.5%	1.3%	1.7%	1.7%	0.0%	2.8%	0.8%	4.3%	0.0%	0.0%	3.7%	0.0%
	Neutral	5.3%	2.6%	3.4%	3.4%	4.5%	2.8%	4.0%	5.8%	4.0%	5.4%	1.2%	4.7%
	Agree	49.5%	46.2%	36.4%	46.4%	30.8%	45.4%	41.0%	37.7%	35.5%	42.4%	55.6%	38.8%
	Strongly Agree	41.7%	48.7%	57.6%	47.3%	63.2%	48.1%	52.9%	50.7%	59.7%	50.0%	37.0%	56.5%
	Don't Know	1.5%	1.3%	0.0%	0.9%	0.8%	0.0%	1.1%	1.4%	0.8%	0.0%	2.5%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_3 Familiar with current cybersecurity regulations	Strongly Disagree	11.2%	6.4%	5.9%	6.6%	9.8%	11.1%	6.3%	10.1%	6.5%	6.6%	9.9%	3.5%
	Disagree	26.2%	25.6%	19.5%	22.7%	20.3%	21.3%	22.0%	26.1%	21.8%	19.8%	30.9%	18.6%
	Neutral	24.8%	34.6%	24.6%	25.9%	21.8%	25.0%	24.3%	26.1%	25.0%	29.7%	19.8%	23.3%
	Agree	15.0%	15.4%	27.1%	21.0%	21.8%	25.0%	19.8%	14.5%	20.2%	24.2%	16.0%	24.4%
	Strongly Agree	6.8%	3.8%	16.1%	10.3%	20.3%	8.3%	15.1%	8.7%	19.4%	11.0%	3.7%	20.9%
	Don't Know	16.0%	14.1%	6.8%	13.5%	6.0%	9.3%	12.4%	14.5%	7.3%	8.8%	19.8%	9.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_4 Aware of various cybersecurity measures	Strongly Disagree	7.8%	2.6%	3.4%	4.3%	5.3%	8.3%	3.4%	8.7%	4.9%	3.3%	3.7%	3.5%
	Disagree	19.5%	16.7%	7.6%	13.3%	15.8%	16.7%	13.0%	13.0%	13.0%	13.2%	22.2%	9.3%
	Neutral	21.5%	21.8%	22.9%	21.9%	15.0%	18.5%	20.2%	23.2%	21.1%	29.7%	16.0%	14.0%
	Agree	35.1%	39.7%	42.4%	39.5%	35.3%	43.5%	36.3%	36.2%	34.1%	33.0%	43.2%	40.7%
	Strongly Agree	5.4%	10.3%	22.0%	13.0%	26.3%	8.3%	19.6%	13.0%	21.1%	15.4%	6.2%	26.7%
	Don't Know	10.7%	9.0%	1.7%	8.1%	2.3%	4.6%	7.4%	5.8%	5.7%	5.5%	8.6%	5.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q1_1 – Q1_4: Demographic Group C (Q15_CodedCombined Q16 Q17_Coded)

		Q15_CodedCombined Role				Q16 Have formal cybersecurity training			Q17_Coded City population		
		CEO/Pres/Owner/Partner	Office administrator/manager, accountant/bookkeeper/treasurer	Director/manager	IT Director/CIO	Yes	No	Unsure	Less than 5,000	5,000 to 49,999	Above 50,000
Q1_1 Aware of common cybersecurity threats	Strongly Disagree	0.6%	0.0%	1.0%	0.0%	0.0%	0.7%	0.0%	0.6%	0.0%	0.6%
	Disagree	2.6%	2.1%	3.0%	1.8%	0.0%	3.9%	6.3%	2.4%	3.0%	2.3%
	Neutral	7.7%	8.4%	7.0%	0.0%	1.2%	10.3%	6.3%	9.1%	5.3%	5.2%
	Agree	55.8%	51.6%	48.0%	35.7%	37.0%	58.2%	56.3%	52.4%	44.4%	53.5%
	Strongly Agree	30.8%	36.8%	39.0%	62.5%	61.3%	24.8%	31.3%	34.1%	45.1%	37.2%
	Don't Know	2.6%	1.1%	2.0%	0.0%	0.6%	2.1%	0.0%	1.2%	2.3%	1.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_2 Understand potential impacts of breaches	Strongly Disagree	0.0%	1.1%	1.0%	0.0%	0.0%	0.7%	0.0%	0.6%	0.0%	0.6%
	Disagree	1.3%	3.2%	0.0%	0.0%	0.0%	2.1%	0.0%	1.8%	0.8%	1.2%
	Neutral	5.1%	2.1%	5.0%	3.6%	1.7%	5.7%	6.3%	3.7%	4.5%	4.6%
	Agree	49.7%	40.4%	40.0%	23.2%	28.7%	49.5%	56.3%	46.6%	39.8%	40.5%
	Strongly Agree	42.0%	52.1%	54.0%	73.2%	69.5%	40.6%	37.5%	46.6%	53.4%	52.6%
	Don't Know	1.9%	1.1%	0.0%	0.0%	0.0%	1.4%	0.0%	0.6%	1.5%	0.6%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_3 Familiar with current cybersecurity regulations	Strongly Disagree	9.6%	5.3%	9.0%	1.8%	2.9%	10.0%	6.3%	8.5%	6.1%	6.9%
	Disagree	26.1%	27.4%	18.0%	10.7%	13.8%	27.8%	18.8%	22.6%	18.2%	25.4%
	Neutral	26.1%	31.6%	26.0%	16.1%	16.7%	28.8%	37.5%	21.3%	24.2%	27.2%
	Agree	15.3%	13.7%	24.0%	32.1%	31.6%	14.2%	18.8%	22.6%	22.0%	19.1%
	Strongly Agree	7.0%	12.6%	8.0%	35.7%	28.2%	4.6%	0.0%	13.4%	13.6%	12.7%
	Don't Know	15.9%	9.5%	15.0%	3.6%	6.9%	14.6%	18.8%	11.6%	15.9%	8.7%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q1_4 Aware of various cybersecurity measures	Strongly Disagree	8.3%	2.1%	6.0%	0.0%	1.1%	6.8%	6.3%	3.7%	5.3%	5.2%
	Disagree	16.0%	20.0%	9.0%	1.8%	5.7%	18.2%	18.8%	17.8%	10.5%	12.2%
	Neutral	19.9%	24.2%	25.0%	10.7%	10.3%	27.1%	18.8%	15.3%	20.3%	25.0%
	Agree	36.5%	35.8%	36.0%	39.3%	44.3%	32.9%	43.8%	39.9%	39.8%	34.3%
	Strongly Agree	9.6%	13.7%	16.0%	48.2%	36.8%	5.4%	6.3%	17.2%	15.0%	18.6%
	Don't Know	9.6%	4.2%	8.0%	0.0%	1.7%	9.6%	6.3%	6.1%	9.0%	4.7%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q2_1 – Q2_6: Demographic Group A (Q6Combined, Q7, Q8, Q9_CodedCombined)

		Q6Combined Online payment system usage				Q7 Experienced a malicious cybersecurity event			Q8 Experienced a non-malicious data loss			Q9_CodedCombined Organization		
		Client transactions	Vendor transactions	Both	No online payment system	Yes	No	Don't Know	Yes	No	Don't Know	Govt/School	Nonprofit/not-for-profit	For-profit business
Q2_1 Investing in cybersecurity is crucial for safety	Strongly Disagree	1.9%	0.0%	0.0%	0.6%	0.0%	0.7%	2.4%	0.0%	0.7%	1.3%	0.0%	0.0%	1.3%
	Disagree	9.5%	8.6%	0.8%	6.4%	3.3%	6.6%	4.8%	4.1%	7.3%	1.3%	3.8%	7.9%	5.4%
	Neutral	17.1%	22.9%	10.1%	21.4%	8.9%	20.0%	14.3%	8.1%	21.0%	11.5%	7.5%	19.1%	19.7%
	Agree	35.2%	45.7%	48.7%	41.6%	44.4%	42.6%	38.1%	40.5%	40.9%	50.0%	37.5%	53.9%	39.0%
	Strongly Agree	35.2%	17.1%	38.7%	26.6%	43.3%	27.5%	33.3%	44.6%	28.7%	29.5%	51.2%	19.1%	30.8%
	Don't Know	1.0%	5.7%	1.7%	3.5%	0.0%	2.6%	7.1%	2.7%	1.4%	6.4%	0.0%	0.0%	3.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_2 Confident identifying and responding to potential threats	Strongly Disagree	6.7%	8.3%	5.0%	5.8%	1.1%	7.3%	7.0%	2.7%	5.3%	11.4%	3.8%	11.2%	5.1%
	Disagree	19.2%	22.2%	16.8%	17.4%	12.1%	19.8%	18.6%	17.3%	18.7%	16.5%	12.5%	16.9%	19.3%
	Neutral	32.7%	36.1%	25.2%	27.9%	19.8%	30.7%	37.2%	28.0%	29.2%	29.1%	25.0%	30.3%	29.1%
	Agree	33.7%	22.2%	38.7%	33.7%	50.5%	31.0%	20.9%	36.0%	34.9%	30.4%	40.0%	34.8%	32.0%
	Strongly Agree	6.7%	5.6%	13.4%	9.9%	15.4%	7.9%	11.6%	13.3%	8.8%	10.1%	18.8%	3.4%	10.8%
	Don't Know	1.0%	5.6%	0.8%	5.2%	1.1%	3.3%	4.7%	2.7%	3.2%	2.5%	0.0%	3.4%	3.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_3 Regularly make hardware and software cybersecurity updates	Strongly Disagree	4.9%	2.8%	1.7%	4.7%	2.2%	4.3%	2.3%	2.7%	4.6%	1.3%	2.5%	3.5%	4.2%
	Disagree	9.7%	22.2%	13.4%	9.5%	10.1%	11.6%	14.0%	14.7%	10.3%	13.0%	6.3%	15.1%	9.9%
	Neutral	16.5%	25.0%	12.6%	14.8%	9.0%	17.9%	11.6%	10.7%	17.0%	14.3%	10.0%	17.4%	16.0%
	Agree	36.9%	22.2%	37.8%	39.1%	43.8%	35.9%	27.9%	38.7%	37.2%	32.5%	37.5%	41.9%	35.8%
	Strongly Agree	29.1%	19.4%	33.6%	23.7%	33.7%	24.9%	32.6%	32.0%	27.0%	26.0%	41.3%	17.4%	28.8%
	Don't Know	2.9%	8.3%	0.8%	8.3%	1.1%	5.3%	11.6%	1.3%	3.9%	13.0%	2.5%	4.7%	5.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_4 Willing to invest in employee cybersecurity training	Strongly Disagree	1.9%	3.1%	3.4%	4.7%	1.1%	4.4%	2.5%	1.4%	4.3%	2.6%	1.3%	3.4%	4.3%
	Disagree	4.8%	12.5%	4.3%	13.0%	5.6%	9.7%	5.0%	10.8%	8.6%	5.3%	5.0%	6.9%	9.5%
	Neutral	28.8%	28.1%	23.1%	28.4%	16.9%	30.5%	25.0%	12.2%	32.0%	23.7%	18.8%	29.9%	28.0%
	Agree	39.4%	43.8%	37.6%	35.5%	41.6%	35.6%	42.5%	45.9%	34.5%	39.5%	35.0%	44.8%	36.2%
	Strongly Agree	22.1%	12.5%	29.9%	13.6%	33.7%	16.4%	20.0%	29.7%	18.3%	19.7%	37.5%	11.5%	19.1%
	Don't Know	2.9%	0.0%	1.7%	4.7%	1.1%	3.4%	5.0%	0.0%	2.2%	9.2%	2.5%	3.4%	3.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_5 Employee cybersecurity training is effective	Strongly Disagree	1.0%	2.9%	0.9%	0.6%	0.0%	1.0%	2.4%	0.0%	1.1%	1.3%	0.0%	0.0%	1.3%
	Disagree	0.0%	5.9%	0.0%	4.7%	0.0%	3.3%	0.0%	1.4%	2.8%	1.3%	2.5%	1.1%	3.2%
	Neutral	22.9%	20.6%	11.1%	16.3%	13.3%	18.5%	11.9%	12.2%	18.1%	16.5%	15.2%	12.6%	19.1%
	Agree	38.1%	50.0%	46.2%	51.7%	45.6%	46.4%	45.2%	45.9%	46.8%	43.0%	30.4%	57.5%	45.2%
	Strongly Agree	38.1%	17.6%	38.5%	22.7%	41.1%	26.8%	33.3%	37.8%	28.7%	30.4%	50.6%	25.3%	27.1%
	Don't Know	0.0%	2.9%	3.4%	4.1%	0.0%	4.0%	7.1%	2.7%	2.5%	7.6%	1.3%	3.4%	4.1%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_6 Cybersecurity training helps save money in long run	Strongly Disagree	1.9%	0.0%	1.7%	0.6%	0.0%	1.3%	2.4%	0.0%	1.4%	1.3%	0.0%	0.0%	1.9%
	Disagree	1.9%	8.8%	2.6%	9.9%	1.1%	7.6%	2.4%	6.8%	7.1%	0.0%	5.1%	4.6%	6.4%
	Neutral	27.9%	20.6%	23.9%	27.3%	15.6%	29.1%	24.4%	16.2%	28.7%	24.4%	13.9%	27.6%	28.3%
	Agree	36.5%	44.1%	30.8%	36.6%	41.1%	33.8%	34.1%	33.8%	34.8%	38.5%	35.4%	42.5%	32.8%
	Strongly Agree	31.7%	20.6%	37.6%	20.3%	42.2%	23.5%	29.3%	41.9%	25.2%	25.6%	43.0%	21.8%	25.8%
	Don't Know	0.0%	5.9%	3.4%	5.2%	0.0%	4.6%	7.3%	1.4%	2.8%	10.3%	2.5%	3.4%	4.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q2_1 – Q2_6: Demographic Group B (Q10_Coded Q11_Coded Q12 Q13_Coded Q14_CodedCombine)

		Q10_Coded Full-time employees			Q11_Coded Part-time employees		Q13_Coded Years of organization		Q14_CodedCombined Purpose of organization				
		0-4	5-9	10 and Above	0-4	5 and Above	Under 25 years	25 years or over	Retail, wholesale	Professional services, financial, healthcare	Personal services, religious, housing	Manufacturing, construction, agriculture	Government, education, library
Q2_1 Investing in cybersecurity is crucial for safety	Strongly Disagree	1.0%	1.3%	0.0%	0.9%	0.8%	1.9%	0.5%	1.4%	1.6%	0.0%	0.0%	1.2%
	Disagree	9.4%	2.6%	4.2%	6.1%	4.5%	6.5%	5.3%	4.3%	1.6%	6.7%	12.3%	5.9%
	Neutral	22.2%	29.5%	13.6%	19.7%	12.0%	20.4%	16.8%	24.6%	15.4%	24.4%	18.5%	8.2%
	Agree	44.8%	37.2%	44.9%	41.4%	42.1%	44.4%	40.5%	40.6%	33.3%	45.6%	48.1%	37.6%
	Strongly Agree	18.2%	25.6%	37.3%	28.7%	39.8%	25.9%	33.9%	24.6%	44.7%	22.2%	16.0%	47.1%
	Don't Know	4.4%	3.8%	0.0%	3.2%	0.8%	0.9%	2.9%	4.3%	3.3%	1.1%	4.9%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_2 Confident identifying and responding to potential threats	Strongly Disagree	9.7%	5.2%	4.3%	4.9%	9.0%	11.1%	4.5%	7.4%	4.9%	8.8%	6.2%	2.3%
	Disagree	22.3%	22.1%	13.7%	17.6%	18.0%	19.4%	17.3%	26.5%	18.7%	15.4%	21.0%	15.1%
	Neutral	31.1%	28.6%	28.2%	30.9%	22.6%	27.8%	28.7%	19.1%	30.9%	36.3%	25.9%	25.6%
	Agree	27.7%	32.5%	37.6%	33.5%	36.1%	30.6%	34.8%	32.4%	29.3%	31.9%	37.0%	39.5%
	Strongly Agree	3.9%	6.5%	16.2%	9.2%	12.8%	10.2%	10.9%	8.8%	13.8%	5.5%	3.7%	17.4%
	Don't Know	5.3%	5.2%	0.0%	3.8%	1.5%	0.9%	3.7%	5.9%	2.4%	2.2%	6.2%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_3 Regularly make hardware and software cybersecurity updates	Strongly Disagree	7.6%	2.6%	0.8%	3.8%	3.8%	5.7%	3.2%	5.9%	2.5%	2.3%	6.2%	3.6%
	Disagree	13.1%	15.4%	7.6%	10.5%	9.1%	8.5%	10.8%	17.6%	4.9%	18.2%	12.3%	6.0%
	Neutral	21.7%	17.9%	5.1%	16.7%	11.4%	16.0%	15.1%	13.2%	19.7%	14.8%	13.6%	13.1%
	Agree	32.3%	41.0%	44.1%	36.3%	40.2%	36.8%	37.1%	35.3%	27.0%	39.8%	40.7%	41.7%
	Strongly Agree	19.2%	17.9%	36.4%	27.5%	31.8%	29.2%	28.8%	20.6%	40.2%	22.7%	19.8%	33.3%
	Don't Know	6.1%	5.1%	5.9%	5.3%	3.8%	3.8%	5.1%	7.4%	5.7%	2.3%	7.4%	2.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_4 Willing to invest in employee cybersecurity training	Strongly Disagree	5.8%	2.6%	1.7%	3.9%	3.0%	4.8%	3.3%	2.9%	4.2%	1.1%	7.9%	2.4%
	Disagree	11.0%	15.4%	5.1%	8.7%	7.6%	6.7%	8.7%	13.0%	7.6%	6.8%	11.8%	6.0%
	Neutral	34.0%	29.5%	24.8%	28.5%	22.0%	28.8%	26.2%	31.9%	18.5%	31.8%	30.3%	26.2%
	Agree	38.2%	34.6%	39.3%	38.7%	35.6%	41.3%	36.3%	36.2%	37.0%	39.8%	35.5%	33.3%
	Strongly Agree	7.3%	11.5%	28.2%	17.1%	28.8%	15.4%	22.4%	11.6%	30.3%	17.0%	10.5%	29.8%
	Don't Know	3.7%	6.4%	0.9%	3.0%	3.0%	2.9%	3.0%	4.3%	2.5%	3.4%	3.9%	2.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_5 Employee cybersecurity training is effective	Strongly Disagree	1.5%	1.3%	0.0%	0.9%	0.8%	1.9%	0.5%	0.0%	1.6%	0.0%	1.3%	1.2%
	Disagree	5.5%	2.6%	0.0%	2.9%	2.3%	2.8%	2.7%	7.2%	2.5%	1.1%	3.8%	1.2%
	Neutral	19.6%	21.8%	17.8%	18.8%	13.5%	19.8%	16.6%	23.2%	12.3%	16.5%	22.8%	16.7%
	Agree	49.2%	50.0%	40.7%	46.0%	42.1%	49.1%	43.7%	47.8%	42.6%	56.0%	41.8%	35.7%
	Strongly Agree	19.1%	20.5%	38.1%	27.6%	38.3%	22.6%	33.0%	17.4%	37.7%	24.2%	25.3%	42.9%
	Don't Know	5.0%	3.8%	3.4%	3.8%	3.0%	3.8%	3.5%	4.3%	3.3%	2.2%	5.1%	2.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_6 Cybersecurity training helps save money in long run	Strongly Disagree	2.0%	1.3%	0.0%	1.8%	0.0%	2.8%	0.8%	0.0%	2.4%	0.0%	2.5%	1.2%
	Disagree	10.1%	3.8%	4.2%	7.0%	3.0%	5.7%	5.9%	8.7%	3.3%	4.5%	10.0%	6.0%
	Neutral	32.7%	34.6%	18.6%	26.4%	23.3%	28.3%	24.9%	33.3%	17.9%	28.1%	33.8%	20.2%
	Agree	33.7%	42.3%	38.1%	35.8%	34.6%	40.6%	33.5%	36.2%	35.0%	34.8%	32.5%	28.6%
	Strongly Agree	15.1%	14.1%	35.6%	24.9%	34.6%	19.8%	30.3%	17.4%	35.0%	29.2%	16.3%	41.7%
	Don't Know	6.5%	3.8%	3.4%	4.1%	4.5%	2.8%	4.6%	4.3%	6.5%	3.4%	5.0%	2.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q2_1 – Q2_6: Demographic Group C (Q15_CodedCombined Q16 Q17_Coded)

		Q15_CodedCombined Role				Q16 Have formal cybersecurity training			Q17_Coded City population		
		CEO/Pres/Owner/Partner	Office administrator/manager, accountant/bookkeeper/ treasurer	Director/manager	IT Director /CIO	Yes	No	Unsure	Less than 5,000	5,000 to 49,999	Above 50,000
Q2_1 Investing in cybersecurity is crucial for safety	Strongly Disagree	1.9%	1.1%	0.0%	0.0%	0.0%	1.4%	0.0%	0.6%	1.5%	0.6%
	Disagree	6.4%	4.3%	4.0%	3.6%	2.9%	7.6%	6.3%	4.3%	6.0%	7.1%
	Neutral	26.9%	16.1%	17.0%	3.6%	5.7%	25.2%	18.8%	17.2%	17.3%	18.2%
	Agree	35.9%	43.0%	49.0%	28.6%	39.1%	41.7%	43.8%	42.9%	42.9%	38.2%
	Strongly Agree	23.1%	33.3%	30.0%	64.3%	51.7%	20.1%	31.3%	31.9%	29.3%	34.1%
	Don't Know	5.8%	2.2%	0.0%	0.0%	0.6%	4.0%	0.0%	3.1%	3.0%	1.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_2 Confident identifying and responding to potential threats	Strongly Disagree	8.3%	4.3%	6.0%	1.8%	1.7%	8.6%	0.0%	5.5%	7.6%	4.6%
	Disagree	26.8%	21.5%	15.0%	5.4%	6.9%	24.7%	37.5%	19.6%	13.7%	21.4%
	Neutral	28.7%	30.1%	31.0%	19.6%	19.5%	32.3%	37.5%	27.0%	29.8%	26.6%
	Agree	24.2%	33.3%	38.0%	53.6%	49.4%	25.8%	18.8%	35.6%	33.6%	34.7%
	Strongly Agree	6.4%	8.6%	10.0%	19.6%	21.3%	4.3%	6.3%	9.8%	12.2%	9.8%
	Don't Know	5.7%	2.2%	0.0%	0.0%	1.1%	4.3%	0.0%	2.5%	3.1%	2.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_3 Regularly make hardware and software cybersecurity updates	Strongly Disagree	7.7%	2.2%	1.0%	0.0%	0.6%	5.8%	0.0%	4.4%	4.5%	2.4%
	Disagree	12.3%	13.2%	8.2%	5.4%	8.1%	13.1%	0.0%	9.4%	8.3%	14.1%
	Neutral	18.1%	13.2%	14.3%	8.9%	8.1%	18.9%	37.5%	15.7%	17.4%	13.5%
	Agree	33.5%	38.5%	42.9%	33.9%	35.3%	36.7%	37.5%	35.8%	37.1%	35.9%
	Strongly Agree	22.6%	24.2%	31.6%	50.0%	46.8%	18.2%	18.8%	29.6%	27.3%	29.4%
	Don't Know	5.8%	8.8%	2.0%	1.8%	1.2%	7.3%	6.3%	5.0%	5.3%	4.7%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_4 Willing to invest in employee cybersecurity training	Strongly Disagree	5.4%	3.3%	2.0%	0.0%	1.2%	5.6%	0.0%	3.2%	5.4%	3.0%
	Disagree	12.8%	10.0%	4.0%	7.1%	1.7%	12.6%	13.3%	10.2%	5.4%	9.6%
	Neutral	26.8%	34.4%	25.3%	12.5%	15.0%	34.2%	33.3%	31.2%	26.2%	24.1%
	Agree	40.3%	30.0%	41.4%	28.6%	36.4%	36.4%	46.7%	36.3%	36.9%	36.7%
	Strongly Agree	12.1%	16.7%	24.2%	51.8%	42.8%	7.8%	6.7%	15.9%	22.3%	24.7%
	Don't Know	2.7%	5.6%	3.0%	0.0%	2.9%	3.3%	0.0%	3.2%	3.8%	1.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_5 Employee cybersecurity training is effective	Strongly Disagree	2.0%	0.0%	0.0%	0.0%	0.0%	1.4%	0.0%	0.0%	2.3%	0.6%
	Disagree	7.2%	1.1%	1.0%	0.0%	0.6%	4.0%	12.5%	4.4%	2.3%	2.4%
	Neutral	19.6%	23.7%	14.3%	12.5%	9.3%	22.0%	18.8%	22.0%	10.5%	18.2%
	Agree	48.4%	47.3%	50.0%	23.2%	36.6%	50.2%	50.0%	44.0%	45.1%	46.5%
	Strongly Agree	18.3%	24.7%	33.7%	62.5%	52.9%	17.3%	18.8%	27.7%	34.6%	29.4%
	Don't Know	4.6%	3.2%	1.0%	1.8%	0.6%	5.1%	0.0%	1.9%	5.3%	2.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q2_6 Cybersecurity training helps save money in long run	Strongly Disagree	2.6%	1.1%	0.0%	0.0%	0.0%	2.2%	0.0%	0.0%	3.0%	1.2%
	Disagree	7.7%	7.6%	4.1%	3.6%	1.2%	9.1%	6.3%	8.1%	5.3%	4.7%
	Neutral	31.6%	28.3%	22.4%	14.3%	17.3%	30.8%	25.0%	26.9%	23.5%	25.9%
	Agree	36.1%	34.8%	37.8%	23.2%	31.8%	35.5%	43.8%	36.3%	31.8%	34.1%
	Strongly Agree	16.1%	22.8%	34.7%	57.1%	48.0%	16.7%	18.8%	25.6%	30.3%	30.0%
	Don't Know	5.8%	5.4%	1.0%	1.8%	1.7%	5.8%	6.3%	3.1%	6.1%	4.1%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q3_1 – Q3_6: Demographic Group A (Q6Combined, Q7, Q8, Q9_CodedCombined)

		Q6Combined Online payment system usage				Q7 Experienced a malicious cybersecurity event			Q8 Experienced a non-malicious data loss			Q9_CodedCombined Organization		
		Client transactions	Vendor transactions	Both	No online payment system	Yes	No	Don't Know	Yes	No	Don't Know	Govt/School	Nonprofit/not-for-profit	For-profit business
Q3_1 Limited resources to invest in advanced cybersecurity measures	Strongly Disagree	1.9%	0.0%	1.7%	1.7%	2.2%	1.7%	2.4%	1.3%	2.1%	1.3%	2.6%	0.0%	2.9%
	Disagree	13.5%	5.7%	17.9%	14.5%	31.9%	8.9%	17.1%	21.3%	12.7%	14.3%	15.4%	3.4%	17.0%
	Neutral	26.9%	31.4%	17.1%	23.3%	14.3%	26.2%	19.5%	14.7%	25.4%	22.1%	17.9%	21.6%	24.7%
	Agree	32.7%	34.3%	41.0%	38.4%	30.8%	39.1%	34.1%	44.0%	36.4%	32.5%	46.2%	43.2%	34.0%
	Strongly Agree	24.0%	20.0%	20.5%	19.2%	18.7%	22.2%	19.5%	17.3%	22.3%	20.8%	16.7%	30.7%	17.9%
	Don't Know	1.0%	8.6%	1.7%	2.9%	2.2%	2.0%	7.3%	1.3%	1.1%	9.1%	1.3%	1.1%	3.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_2 Challenging to stay updated on regulations	Strongly Disagree	1.0%	0.0%	2.5%	2.3%	5.5%	1.0%	0.0%	1.3%	1.8%	2.6%	5.1%	0.0%	1.6%
	Disagree	9.6%	2.8%	9.3%	8.7%	12.1%	7.2%	9.8%	18.7%	6.0%	7.8%	12.8%	3.4%	8.9%
	Neutral	21.2%	8.3%	18.6%	18.0%	20.9%	17.4%	17.1%	20.0%	17.9%	18.2%	25.6%	20.2%	15.3%
	Agree	40.4%	58.3%	36.4%	47.1%	38.5%	46.7%	31.7%	34.7%	47.4%	37.7%	37.2%	48.3%	44.6%
	Strongly Agree	27.9%	27.8%	31.4%	20.9%	23.1%	26.0%	34.1%	24.0%	26.0%	28.6%	19.2%	28.1%	26.8%
	Don't Know	0.0%	2.8%	1.7%	2.9%	0.0%	1.6%	7.3%	1.3%	1.1%	5.2%	0.0%	0.0%	2.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_3 Lack technical expertise	Strongly Disagree	1.9%	0.0%	7.7%	3.6%	9.9%	3.0%	0.0%	9.5%	3.9%	0.0%	7.8%	0.0%	4.8%
	Disagree	19.4%	8.3%	21.4%	14.8%	27.5%	12.4%	29.3%	24.3%	14.9%	19.5%	22.1%	13.6%	17.4%
	Neutral	15.5%	16.7%	17.9%	20.7%	22.0%	18.1%	14.6%	20.3%	19.6%	13.0%	26.0%	22.7%	15.8%
	Agree	34.0%	41.7%	28.2%	37.3%	23.1%	38.5%	26.8%	29.7%	35.9%	31.2%	23.4%	29.5%	36.8%
	Strongly Agree	28.2%	30.6%	23.9%	21.3%	16.5%	26.8%	24.4%	16.2%	24.9%	29.9%	20.8%	34.1%	22.6%
	Don't Know	1.0%	2.8%	0.9%	2.4%	1.1%	1.3%	4.9%	0.0%	0.7%	6.5%	0.0%	0.0%	2.6%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_4 Difficult to ensure safe employee behavior	Strongly Disagree	6.9%	0.0%	4.3%	3.5%	3.3%	4.4%	5.0%	5.3%	3.9%	3.9%	3.8%	1.1%	4.9%
	Disagree	22.5%	17.6%	21.6%	22.2%	18.7%	22.1%	27.5%	24.0%	22.2%	18.4%	23.1%	18.2%	23.5%
	Neutral	30.4%	35.3%	22.4%	28.7%	23.1%	30.5%	22.5%	16.0%	31.2%	28.9%	25.6%	29.5%	28.7%
	Agree	29.4%	32.4%	35.3%	33.3%	44.0%	29.9%	27.5%	42.7%	30.5%	31.6%	38.5%	31.8%	30.6%
	Strongly Agree	10.8%	11.8%	16.4%	9.4%	11.0%	11.7%	12.5%	10.7%	11.5%	13.2%	9.0%	19.3%	10.1%
	Don't Know	0.0%	2.9%	0.0%	2.9%	0.0%	1.3%	5.0%	1.3%	0.7%	3.9%	0.0%	0.0%	2.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_5 Cost and technical constraints limit updates	Strongly Disagree	7.8%	2.9%	6.8%	6.4%	10.0%	6.0%	5.0%	5.4%	8.1%	2.6%	10.3%	0.0%	7.7%
	Disagree	28.2%	17.1%	29.9%	25.1%	31.1%	25.2%	27.5%	27.0%	26.9%	25.0%	23.1%	18.2%	29.9%
	Neutral	22.3%	25.7%	17.1%	21.1%	23.3%	20.5%	17.5%	25.7%	19.4%	21.1%	15.4%	22.7%	21.2%
	Agree	27.2%	28.6%	28.2%	29.2%	20.0%	30.5%	27.5%	32.4%	27.2%	27.6%	35.9%	35.2%	24.1%
	Strongly Agree	12.6%	25.7%	17.1%	14.6%	14.4%	15.9%	17.5%	8.1%	17.0%	18.4%	11.5%	23.9%	14.8%
	Don't Know	1.9%	0.0%	0.9%	3.5%	1.1%	2.0%	5.0%	1.4%	1.4%	5.3%	3.8%	0.0%	2.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_6 Lack cybersecurity policy and incident response	Strongly Disagree	6.7%	5.6%	12.1%	6.6%	17.6%	5.7%	5.0%	14.7%	6.5%	7.8%	19.2%	1.1%	8.1%
	Disagree	25.0%	11.1%	23.3%	19.2%	29.7%	17.8%	22.5%	30.7%	19.8%	15.6%	24.4%	14.9%	20.1%
	Neutral	13.5%	13.9%	13.8%	21.0%	12.1%	18.8%	10.0%	6.7%	20.9%	10.4%	15.4%	14.9%	17.5%
	Agree	30.8%	44.4%	29.3%	37.7%	29.7%	35.2%	35.0%	37.3%	30.9%	41.6%	17.9%	46.0%	34.0%
	Strongly Agree	22.1%	25.0%	20.7%	13.2%	11.0%	20.8%	22.5%	10.7%	20.5%	20.8%	21.8%	23.0%	18.1%
	Don't Know	1.9%	0.0%	0.9%	2.4%	0.0%	1.7%	5.0%	0.0%	1.4%	3.9%	1.3%	0.0%	2.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q3_1 – Q3_6: Demographic Group B (Q10_Coded Q11_Coded Q12 Q13_Coded Q14_CodedCombine)

		Q10_Coded Full-time employees			Q11_Coded Part-time employees		Q13_Coded Years of organization		Q14_CodedCombined Purpose of organization				
		0-4	5-9	10 and Above	0-4	5 and Above	Under 25 years	25 years or over	Retail, wholesale	Professional services, financial, healthcare	Personal services, religious, housing	Manufacturing, construction, agriculture	Government, education, library
Q3_1 Limited resources to invest in advanced cybersecurity measures	Strongly Disagree	0.5%	0.0%	2.6%	2.0%	3.1%	2.8%	2.2%	1.4%	4.9%	1.1%	1.3%	1.2%
	Disagree	4.5%	15.6%	22.4%	13.1%	17.1%	12.3%	14.8%	15.9%	12.3%	7.7%	24.7%	14.5%
	Neutral	22.8%	23.4%	25.9%	26.2%	14.7%	28.3%	21.6%	18.8%	27.9%	27.5%	20.8%	14.5%
	Agree	40.1%	35.1%	36.2%	36.2%	41.1%	34.0%	38.5%	30.4%	34.4%	35.2%	37.7%	45.8%
	Strongly Agree	28.7%	23.4%	11.2%	19.8%	20.9%	20.8%	19.9%	27.5%	18.9%	26.4%	13.0%	21.7%
	Don't Know	3.5%	2.6%	1.7%	2.6%	3.1%	1.9%	3.0%	5.8%	1.6%	2.2%	2.6%	2.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_2 Challenging to stay updated on regulations	Strongly Disagree	1.0%	0.0%	1.7%	1.4%	3.1%	1.9%	1.9%	1.4%	1.7%	1.1%	2.5%	3.6%
	Disagree	3.4%	3.8%	16.2%	8.4%	8.5%	8.4%	8.6%	7.2%	7.4%	6.6%	8.8%	13.1%
	Neutral	14.3%	15.4%	24.8%	17.1%	20.8%	15.0%	18.8%	10.1%	19.8%	22.0%	13.8%	20.2%
	Agree	40.4%	56.4%	46.2%	44.9%	40.8%	48.6%	42.6%	43.5%	43.0%	41.8%	50.0%	45.2%
	Strongly Agree	37.4%	23.1%	11.1%	25.8%	26.2%	24.3%	26.3%	33.3%	26.4%	28.6%	21.3%	17.9%
	Don't Know	3.4%	1.3%	0.0%	2.3%	0.8%	1.9%	1.9%	4.3%	1.7%	0.0%	3.8%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_3 Lack technical expertise	Strongly Disagree	1.0%	3.9%	6.0%	3.8%	6.2%	4.9%	4.3%	4.3%	4.1%	2.3%	5.1%	6.0%
	Disagree	7.5%	9.2%	29.1%	17.9%	16.3%	13.6%	18.6%	10.1%	22.3%	13.6%	14.1%	20.2%
	Neutral	13.0%	17.1%	21.4%	16.8%	23.3%	18.4%	18.6%	11.6%	17.4%	22.7%	14.1%	22.6%
	Agree	40.0%	40.8%	27.4%	35.6%	27.1%	36.9%	32.3%	36.2%	34.7%	34.1%	42.3%	27.4%
	Strongly Agree	36.0%	26.3%	15.4%	23.5%	27.1%	23.3%	24.8%	30.4%	20.7%	27.3%	21.8%	23.8%
	Don't Know	2.5%	2.6%	0.9%	2.4%	0.0%	2.9%	1.3%	7.2%	0.8%	0.0%	2.6%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_4 Difficult to ensure safe employee behavior	Strongly Disagree	2.5%	3.9%	5.2%	4.7%	2.3%	5.8%	3.5%	1.5%	5.9%	2.2%	5.1%	4.9%
	Disagree	21.3%	28.6%	25.9%	24.9%	16.3%	24.3%	22.0%	11.8%	28.6%	18.9%	20.5%	22.0%
	Neutral	33.0%	24.7%	25.9%	29.9%	24.0%	28.2%	28.5%	32.4%	27.7%	35.6%	24.4%	26.8%
	Agree	26.4%	31.2%	33.6%	29.0%	39.5%	31.1%	32.2%	39.7%	22.7%	31.1%	38.5%	32.9%
	Strongly Agree	14.2%	10.4%	8.6%	10.1%	16.3%	9.7%	12.2%	11.8%	13.4%	12.2%	7.7%	13.4%
	Don't Know	2.5%	1.3%	0.9%	1.5%	1.6%	1.0%	1.6%	2.9%	1.7%	0.0%	3.8%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_5 Cost and technical constraints limit updates	Strongly Disagree	2.0%	5.1%	10.3%	6.7%	6.9%	9.6%	5.9%	4.3%	9.1%	3.4%	8.9%	7.2%
	Disagree	17.6%	24.4%	37.6%	27.6%	23.8%	26.9%	26.6%	21.7%	34.7%	21.3%	19.0%	26.5%
	Neutral	18.6%	23.1%	18.8%	18.8%	25.4%	20.2%	20.7%	27.5%	15.7%	22.5%	27.8%	15.7%
	Agree	34.2%	28.2%	22.2%	28.2%	26.9%	22.1%	29.6%	20.3%	26.4%	33.7%	30.4%	31.3%
	Strongly Agree	26.1%	15.4%	8.5%	16.7%	14.6%	19.2%	15.1%	21.7%	12.4%	19.1%	11.4%	15.7%
	Don't Know	1.5%	3.8%	2.6%	2.1%	2.3%	1.9%	2.2%	4.3%	1.7%	0.0%	2.5%	3.6%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_6 Lack cybersecurity policy and incident response	Strongly Disagree	1.0%	1.3%	16.2%	7.4%	12.3%	4.8%	9.8%	3.0%	11.6%	4.5%	5.1%	14.5%
	Disagree	9.7%	17.9%	27.4%	19.2%	20.8%	21.9%	19.3%	10.4%	33.1%	18.0%	11.4%	21.7%
	Neutral	14.8%	17.9%	18.8%	17.5%	14.6%	15.2%	16.8%	16.4%	14.0%	13.5%	20.3%	16.9%
	Agree	43.9%	38.5%	24.8%	35.5%	27.7%	32.4%	34.0%	41.8%	27.3%	43.8%	41.8%	21.7%
	Strongly Agree	28.6%	21.8%	11.1%	18.3%	23.8%	23.8%	18.5%	25.4%	14.0%	20.2%	17.7%	22.9%
	Don't Know	2.0%	2.6%	1.7%	2.1%	0.8%	1.9%	1.6%	3.0%	0.0%	0.0%	3.8%	2.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q3_1 – Q3_6: Demographic Group C (Q15_CodedCombined Q16 Q17_Coded)

		Q15_CodedCombined Role				Q16 Have formal cybersecurity training			Q17_Coded City population		
		CEO/Pres/Owner/Partner	Office administrator/manager, accountant/bookkeeper/treasurer	Director/manager	IT Director/ CIO	Yes	No	Unsure	Less than 5,000	5,000 to 49,999	Above 50,000
Q3_1 Limited resources to invest in advanced cybersecurity measures	Strongly Disagree	1.3%	3.4%	1.0%	5.4%	5.3%	0.7%	0.0%	1.3%	3.0%	2.9%
	Disagree	9.0%	14.6%	18.0%	25.0%	19.9%	10.2%	31.3%	13.2%	14.4%	15.3%
	Neutral	27.1%	22.5%	19.0%	16.1%	22.8%	22.9%	25.0%	21.4%	28.0%	19.4%
	Agree	36.1%	41.6%	34.0%	33.9%	34.5%	37.5%	31.3%	39.6%	32.6%	37.1%
	Strongly Agree	21.3%	15.7%	27.0%	17.9%	16.4%	25.1%	6.3%	22.6%	18.9%	21.8%
	Don't Know	5.2%	2.2%	1.0%	1.8%	1.2%	3.6%	6.3%	1.9%	3.0%	3.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_2 Challenging to stay updated on regulations	Strongly Disagree	0.6%	2.2%	2.0%	3.6%	4.7%	0.4%	0.0%	1.3%	3.0%	1.7%
	Disagree	1.3%	10.8%	12.0%	14.3%	16.3%	3.6%	13.3%	6.9%	9.1%	9.9%
	Neutral	15.5%	15.1%	19.0%	23.2%	22.7%	15.1%	6.7%	16.3%	18.9%	18.6%
	Agree	49.0%	48.4%	39.0%	42.9%	36.6%	48.2%	66.7%	46.9%	40.2%	45.3%
	Strongly Agree	30.3%	21.5%	28.0%	16.1%	19.2%	30.2%	13.3%	26.9%	26.5%	23.3%
	Don't Know	3.2%	2.2%	0.0%	0.0%	0.6%	2.5%	0.0%	1.9%	2.3%	1.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_3 Lack technical expertise	Strongly Disagree	2.6%	4.3%	5.1%	7.1%	9.9%	1.5%	0.0%	3.2%	5.3%	5.3%
	Disagree	10.5%	15.2%	22.4%	25.0%	31.6%	8.1%	18.8%	16.6%	19.5%	16.6%
	Neutral	13.2%	7.6%	22.4%	37.5%	25.7%	12.8%	25.0%	15.3%	19.5%	19.5%
	Agree	42.1%	40.2%	24.5%	17.9%	19.3%	42.9%	37.5%	35.7%	30.1%	35.5%
	Strongly Agree	28.3%	29.3%	25.5%	12.5%	12.3%	32.6%	18.8%	27.4%	23.3%	21.9%
	Don't Know	3.3%	3.3%	0.0%	0.0%	1.2%	2.2%	0.0%	1.9%	2.3%	1.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_4 Difficult to ensure safe employee behavior	Strongly Disagree	2.6%	3.3%	6.1%	1.8%	5.8%	3.0%	0.0%	1.9%	4.6%	5.4%
	Disagree	23.2%	19.8%	23.5%	21.4%	31.6%	15.2%	31.3%	24.7%	18.3%	22.8%
	Neutral	31.1%	31.9%	25.5%	17.9%	25.1%	30.7%	43.8%	29.7%	32.1%	25.7%
	Agree	27.2%	33.0%	32.7%	42.9%	27.5%	34.1%	25.0%	32.3%	32.8%	28.7%
	Strongly Agree	12.6%	9.9%	12.2%	16.1%	9.9%	14.4%	0.0%	10.8%	9.2%	16.2%
	Don't Know	3.3%	2.2%	0.0%	0.0%	0.0%	2.6%	0.0%	0.6%	3.1%	1.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_5 Cost and technical constraints limit updates	Strongly Disagree	3.3%	6.5%	6.1%	14.3%	14.6%	2.2%	0.0%	5.7%	7.6%	7.1%
	Disagree	20.4%	24.7%	31.3%	42.9%	36.8%	19.6%	25.0%	27.2%	25.0%	26.5%
	Neutral	23.7%	18.3%	19.2%	17.9%	14.6%	23.3%	37.5%	17.1%	21.2%	22.9%
	Agree	30.3%	35.5%	24.2%	16.1%	20.5%	33.1%	31.3%	31.0%	27.3%	27.1%
	Strongly Agree	19.7%	14.0%	19.2%	7.1%	11.7%	19.3%	6.3%	17.1%	15.9%	14.7%
	Don't Know	2.6%	1.1%	0.0%	1.8%	1.8%	2.5%	0.0%	1.9%	3.0%	1.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_6 Lack cybersecurity policy and incident response	Strongly Disagree	2.6%	4.4%	6.1%	28.6%	21.1%	1.1%	0.0%	9.6%	8.4%	7.6%
	Disagree	20.4%	13.2%	25.3%	25.0%	32.7%	11.0%	37.5%	19.2%	18.3%	22.4%
	Neutral	16.4%	18.7%	20.2%	12.5%	12.3%	19.4%	6.3%	15.4%	18.3%	15.9%
	Agree	38.2%	40.7%	23.2%	25.0%	18.7%	43.2%	43.8%	31.4%	32.1%	37.1%
	Strongly Agree	19.7%	20.9%	23.2%	8.9%	13.5%	23.4%	12.5%	23.1%	19.1%	16.5%
	Don't Know	2.6%	2.2%	2.0%	0.0%	1.8%	1.8%	0.0%	1.3%	3.8%	0.6%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q3_7 – Q3_11: Demographic Group A (Q6Combined, Q7, Q8, Q9_CodedCombined)

		Q6Combined Online payment system usage				Q7 Experienced a malicious cybersecurity event			Q8 Experienced a non-malicious data loss			Q9_CodedCombined Organization		
		Client transactions	Vendor transactions	Both	No online payment system	Yes	No	Don't Know	Yes	No	Don't Know	Govt/School	Nonprofit/not-for-profit	For-profit business
Q3_7 Challenging managing third-party vendors risks	Strongly Disagree	2.9%	0.0%	4.3%	5.8%	6.6%	4.0%	2.4%	4.0%	5.4%	1.3%	5.1%	4.5%	4.5%
	Disagree	23.3%	19.4%	19.1%	26.3%	20.9%	24.7%	14.6%	21.3%	25.4%	15.6%	12.8%	18.2%	25.4%
	Neutral	34.0%	41.7%	31.3%	28.7%	29.7%	31.8%	39.0%	29.3%	31.8%	36.4%	37.2%	35.2%	30.2%
	Agree	28.2%	19.4%	30.4%	25.7%	31.9%	26.4%	17.1%	32.0%	25.0%	27.3%	28.2%	36.4%	24.4%
	Strongly Agree	9.7%	13.9%	10.4%	6.4%	8.8%	9.0%	7.3%	12.0%	8.9%	5.2%	12.8%	2.3%	10.0%
	Don't Know	1.9%	5.6%	4.3%	7.0%	2.2%	4.0%	19.5%	1.3%	3.6%	14.3%	3.8%	3.4%	5.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_8 Have insufficient back-up and recovery measures	Strongly Disagree	17.3%	11.4%	19.7%	20.0%	25.6%	17.9%	7.3%	20.0%	20.8%	9.5%	18.2%	11.5%	19.8%
	Disagree	35.6%	37.1%	36.8%	30.6%	41.1%	31.2%	41.5%	36.0%	34.2%	32.4%	36.4%	28.7%	34.5%
	Neutral	19.2%	14.3%	16.2%	18.2%	13.3%	18.9%	17.1%	14.7%	17.6%	20.3%	14.3%	20.7%	16.0%
	Agree	18.3%	20.0%	21.4%	21.8%	15.6%	22.9%	12.2%	20.0%	19.7%	23.0%	19.5%	25.3%	21.4%
	Strongly Agree	6.7%	8.6%	3.4%	4.1%	4.4%	4.0%	14.6%	5.3%	3.9%	9.5%	7.8%	8.0%	4.5%
	Don't Know	2.9%	8.6%	2.6%	5.3%	0.0%	5.0%	7.3%	4.0%	3.9%	5.4%	3.9%	5.7%	3.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_9 Organization needs training	Strongly Disagree	2.9%	0.0%	6.0%	6.9%	6.7%	5.3%	0.0%	2.7%	7.0%	0.0%	6.4%	2.3%	5.8%
	Disagree	22.5%	8.6%	19.7%	20.2%	22.2%	18.8%	25.0%	20.3%	20.8%	17.1%	17.9%	12.6%	22.4%
	Neutral	33.3%	31.4%	28.2%	37.6%	25.6%	36.0%	30.0%	29.7%	34.5%	31.6%	28.2%	41.4%	33.3%
	Agree	31.4%	34.3%	32.5%	26.0%	36.7%	28.4%	25.0%	32.4%	26.8%	38.2%	32.1%	33.3%	27.9%
	Strongly Agree	8.8%	14.3%	13.7%	4.6%	8.9%	7.9%	15.0%	12.2%	7.7%	10.5%	14.1%	10.3%	6.7%
	Don't Know	1.0%	11.4%	0.0%	4.6%	0.0%	3.6%	5.0%	2.7%	3.2%	2.6%	1.3%	0.0%	3.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
3_10 I need training	Strongly Disagree	9.8%	0.0%	5.1%	7.0%	12.2%	6.0%	0.0%	10.8%	7.1%	1.3%	11.5%	3.4%	6.7%
	Disagree	16.7%	11.4%	20.5%	18.0%	23.3%	15.9%	22.5%	24.3%	16.3%	18.4%	21.8%	11.5%	17.9%
	Neutral	27.5%	28.6%	21.4%	33.1%	18.9%	30.5%	30.0%	17.6%	31.1%	26.3%	17.9%	37.9%	29.2%
	Agree	38.2%	40.0%	35.9%	32.6%	36.7%	36.8%	22.5%	40.5%	33.9%	35.5%	34.6%	32.2%	35.9%
	Strongly Agree	6.9%	14.3%	17.1%	6.4%	8.9%	8.6%	22.5%	6.8%	9.9%	14.5%	12.8%	13.8%	8.0%
	Don't Know	1.0%	5.7%	0.0%	2.9%	0.0%	2.3%	2.5%	0.0%	1.8%	3.9%	1.3%	1.1%	2.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
3_11 Cost of cybersecurity training is a barrier	Strongly Disagree	2.9%	2.8%	7.8%	6.4%	12.1%	4.3%	0.0%	5.3%	6.7%	2.6%	15.4%	0.0%	6.4%
	Disagree	27.9%	13.9%	22.4%	18.0%	30.8%	17.9%	24.4%	34.7%	19.4%	14.3%	23.1%	6.8%	23.1%
	Neutral	26.9%	27.8%	26.7%	28.5%	23.1%	29.5%	26.8%	24.0%	28.3%	29.9%	23.1%	37.5%	27.2%
	Agree	21.2%	27.8%	24.1%	21.5%	19.8%	24.2%	14.6%	21.3%	23.0%	20.8%	21.8%	22.7%	22.8%
	Strongly Agree	17.3%	19.4%	15.5%	16.9%	12.1%	17.5%	22.0%	9.3%	17.7%	20.8%	12.8%	29.5%	13.5%
	Don't Know	3.8%	8.3%	3.4%	8.7%	2.2%	6.6%	12.2%	5.3%	4.9%	11.7%	3.8%	3.4%	7.1%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q3_7 – Q3_11: Demographic Group B (Q10_Coded Q11_Coded Q12 Q13_Coded Q14_CodedCombine)

		Q10_Coded Full-time employees			Q11_Coded Part-time employees		Q13_Coded Years of organization		Q14_CodedCombined Purpose of organization				
		0-4	5-9	10 and Above	0-4	5 and Above	Under 25 years	25 years or over	Retail, wholesale	Professional services, financial, healthcare	Personal services, religious, housing	Manufacturing, construction, agriculture	Government, education, library
Q3_7 Challenging managing third-party vendors risks	Strongly Disagree	3.5%	3.9%	7.0%	5.0%	3.8%	3.8%	4.9%	3.0%	3.3%	6.7%	6.3%	4.8%
	Disagree	19.8%	24.7%	25.2%	24.0%	16.2%	33.0%	18.9%	22.4%	27.3%	18.9%	23.8%	14.3%
	Neutral	28.7%	36.4%	35.7%	33.1%	31.5%	29.2%	33.2%	23.9%	34.7%	38.9%	28.7%	35.7%
	Agree	28.2%	22.1%	26.1%	24.6%	33.8%	20.8%	28.9%	31.3%	23.1%	26.7%	23.8%	29.8%
	Strongly Agree	13.4%	9.1%	1.7%	8.2%	10.8%	12.3%	8.1%	14.9%	7.4%	5.6%	8.8%	10.7%
	Don't Know	6.4%	3.9%	4.3%	5.0%	3.8%	0.9%	5.9%	4.5%	4.1%	3.3%	8.8%	4.8%
Q3_8 Have insufficient back-up and recovery measures	Strongly Disagree	9.5%	11.5%	32.8%	20.2%	13.2%	22.9%	16.7%	7.5%	22.8%	18.0%	20.0%	14.6%
	Disagree	28.5%	44.9%	29.3%	33.6%	34.1%	31.4%	34.5%	41.8%	36.6%	22.5%	28.7%	39.0%
	Neutral	21.5%	11.5%	12.1%	16.1%	17.1%	19.0%	15.6%	19.4%	10.6%	19.1%	21.3%	18.3%
	Agree	28.0%	23.1%	18.1%	21.6%	22.5%	18.1%	22.9%	23.9%	19.5%	29.2%	23.8%	14.6%
	Strongly Agree	7.5%	3.8%	3.4%	4.7%	8.5%	4.8%	5.9%	4.5%	5.7%	5.6%	2.5%	9.8%
	Don't Know	5.0%	5.1%	4.3%	3.8%	4.7%	3.8%	4.3%	3.0%	4.9%	5.6%	3.8%	3.7%
Q3_9 Organization needs training	Strongly Disagree	4.0%	5.1%	6.8%	5.3%	5.4%	5.7%	5.1%	2.9%	8.3%	2.3%	5.0%	4.8%
	Disagree	19.1%	17.9%	24.8%	22.3%	13.8%	21.7%	19.2%	15.9%	24.8%	15.9%	12.5%	19.3%
	Neutral	36.7%	34.6%	33.3%	34.9%	30.8%	34.9%	33.8%	42.0%	19.8%	45.5%	43.8%	26.5%
	Agree	28.1%	34.6%	26.5%	28.2%	33.8%	28.3%	30.0%	27.5%	31.4%	28.4%	31.3%	33.7%
	Strongly Agree	7.5%	3.8%	7.7%	6.2%	14.6%	8.5%	8.6%	5.8%	12.4%	6.8%	2.5%	14.5%
	Don't Know	4.5%	3.8%	0.9%	3.2%	1.5%	0.9%	3.2%	5.8%	3.3%	1.1%	5.0%	1.2%
3_10 I need training	Strongly Disagree	3.0%	5.1%	11.1%	6.5%	8.5%	3.8%	7.8%	4.3%	9.8%	3.4%	5.1%	8.4%
	Disagree	14.6%	19.2%	18.8%	19.4%	12.3%	20.0%	16.4%	11.6%	19.7%	12.5%	12.7%	20.5%
	Neutral	34.2%	24.4%	29.1%	29.6%	26.2%	28.6%	29.1%	33.3%	21.3%	40.9%	30.4%	24.1%
	Agree	34.7%	43.6%	29.9%	35.5%	34.6%	36.2%	34.8%	34.8%	35.2%	35.2%	43.0%	33.7%
	Strongly Agree	11.1%	5.1%	9.4%	7.3%	16.2%	11.4%	9.4%	13.0%	11.5%	6.8%	6.3%	12.0%
	Don't Know	2.5%	2.6%	1.7%	1.8%	2.3%	0.0%	2.4%	2.9%	2.5%	1.1%	2.5%	1.2%
3_11 Cost of cybersecurity training is a barrier	Strongly Disagree	2.0%	3.8%	10.3%	5.8%	9.2%	5.7%	7.0%	4.3%	8.2%	3.3%	6.3%	9.6%
	Disagree	8.5%	19.2%	25.6%	19.6%	20.8%	21.0%	19.9%	15.9%	24.6%	13.3%	19.0%	19.3%
	Neutral	29.0%	28.2%	30.8%	28.9%	26.9%	25.7%	29.3%	31.9%	25.4%	35.6%	24.1%	24.1%
	Agree	31.0%	24.4%	15.4%	24.3%	17.7%	23.8%	22.0%	18.8%	24.6%	18.9%	32.9%	24.1%
	Strongly Agree	23.0%	16.7%	12.0%	15.2%	20.0%	18.1%	15.9%	23.2%	12.3%	23.3%	7.6%	18.1%
	Don't Know	6.5%	7.7%	6.0%	6.1%	5.4%	5.7%	5.9%	5.8%	4.9%	5.6%	10.1%	4.8%

Q3_7 – Q3_11: Demographic Group C (Q15_CodedCombined Q16 Q17_Coded)

		Q15_CodedCombined Role				Q16 Have formal cybersecurity training			Q17_Coded City population		
		CEO/Pres/Owner/Partner	Office administrator/manager, accountant/bookkeeper/treasurer	Director/manager	IT Director/ CIO	Yes	No	Unsure	Less than 5,000	5,000 to 49,999	Above 50,000
Q3_7 Challenging managing third-party vendors risks	Strongly Disagree	1.9%	6.7%	4.0%	5.4%	7.6%	3.3%	0.0%	4.4%	5.4%	4.7%
	Disagree	21.9%	16.7%	25.3%	28.6%	24.6%	19.7%	31.3%	26.3%	20.8%	18.8%
	Neutral	29.7%	37.8%	30.3%	26.8%	29.8%	34.3%	25.0%	31.3%	34.6%	32.4%
	Agree	26.5%	24.4%	32.3%	28.6%	25.7%	27.4%	37.5%	23.8%	23.8%	31.8%
	Strongly Agree	12.3%	11.1%	4.0%	8.9%	7.6%	10.2%	0.0%	10.6%	8.5%	7.6%
	Don't Know	7.7%	3.3%	4.0%	1.8%	4.7%	5.1%	6.3%	3.8%	6.9%	4.7%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_8 Have insufficient back-up and recovery measures	Strongly Disagree	11.0%	12.1%	20.4%	39.3%	27.1%	13.5%	0.0%	17.1%	16.0%	20.5%
	Disagree	34.8%	30.8%	32.7%	39.3%	34.7%	30.5%	62.5%	30.4%	34.4%	35.7%
	Neutral	20.6%	18.7%	18.4%	7.1%	11.2%	20.4%	25.0%	18.4%	16.0%	15.8%
	Agree	23.2%	27.5%	18.4%	7.1%	18.2%	24.4%	6.3%	24.7%	19.8%	20.5%
	Strongly Agree	4.5%	5.5%	8.2%	5.4%	5.3%	6.5%	0.0%	7.0%	5.3%	5.3%
	Don't Know	5.8%	5.5%	2.0%	1.8%	3.5%	4.7%	6.3%	2.5%	8.4%	2.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q3_9 Organization needs training	Strongly Disagree	3.9%	3.3%	5.1%	10.7%	5.8%	5.1%	6.3%	5.6%	8.4%	3.0%
	Disagree	17.5%	18.5%	21.2%	25.0%	23.4%	15.0%	37.5%	15.0%	19.8%	22.5%
	Neutral	34.4%	28.3%	37.4%	30.4%	26.3%	38.7%	18.8%	35.0%	33.6%	31.4%
	Agree	33.8%	37.0%	19.2%	25.0%	31.6%	29.2%	37.5%	34.4%	24.4%	30.8%
	Strongly Agree	3.9%	9.8%	16.2%	8.9%	12.3%	7.3%	0.0%	7.5%	9.2%	10.1%
	Don't Know	6.5%	3.3%	1.0%	0.0%	0.6%	4.7%	0.0%	2.5%	4.6%	2.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
3_10 I need training	Strongly Disagree	3.9%	4.3%	5.1%	19.6%	11.7%	4.4%	0.0%	6.3%	9.9%	5.3%
	Disagree	11.0%	18.5%	20.2%	26.8%	22.8%	10.9%	37.5%	14.5%	16.8%	18.2%
	Neutral	30.5%	23.9%	31.3%	23.2%	28.1%	29.2%	31.3%	30.2%	25.2%	30.0%
	Agree	44.8%	35.9%	26.3%	28.6%	26.3%	42.7%	25.0%	38.4%	34.4%	34.7%
	Strongly Agree	6.5%	15.2%	16.2%	0.0%	10.5%	9.9%	6.3%	10.1%	9.9%	10.0%
	Don't Know	3.2%	2.2%	1.0%	1.8%	0.6%	2.9%	0.0%	0.6%	3.8%	1.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
3_11 Cost of cybersecurity training is a barrier	Strongly Disagree	3.2%	6.6%	3.0%	17.9%	13.5%	3.3%	0.0%	5.0%	8.3%	7.6%
	Disagree	13.6%	14.3%	22.2%	41.1%	29.8%	12.7%	18.8%	19.5%	18.2%	20.6%
	Neutral	29.9%	24.2%	34.3%	21.4%	25.7%	28.7%	43.8%	25.2%	33.3%	25.9%
	Agree	30.5%	28.6%	15.2%	8.9%	16.4%	27.6%	12.5%	28.9%	15.9%	23.5%
	Strongly Agree	16.2%	17.6%	22.2%	7.1%	12.3%	20.0%	12.5%	17.6%	18.2%	15.3%
	Don't Know	6.5%	8.8%	3.0%	3.6%	2.3%	7.6%	12.5%	3.8%	6.1%	7.1%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q3_12 – Q3_13: Demographic Group A (Q6Combined, Q7, Q8, Q9_CodedCombined)

		Q6Combined Online payment system usage				Q7 Experienced a malicious cybersecurity event			Q8 Experienced a non-malicious data loss			Q9_CodedCombined Organization		
		Client transactions	Vendor transactions	Both	No online payment system	Yes	No	Don't Know	Yes	No	Don't Know	Govt/School	Nonprofit/not-for-profit	For-profit business
3_12 Time for cybersecurity training is a barrier	Strongly Disagree	4.8%	2.8%	6.8%	6.4%	11.0%	4.6%	4.9%	4.0%	6.7%	5.2%	10.3%	1.1%	7.0%
	Disagree	26.9%	11.1%	24.8%	16.9%	26.4%	17.2%	34.1%	28.0%	18.3%	23.4%	30.8%	19.3%	17.6%
	Neutral	26.0%	22.2%	24.8%	27.3%	23.1%	28.1%	17.1%	20.0%	28.2%	23.4%	15.4%	29.5%	27.8%
	Agree	26.9%	36.1%	28.2%	25.0%	24.2%	28.1%	29.3%	26.7%	27.5%	27.3%	24.4%	27.3%	29.4%
	Strongly Agree	13.5%	22.2%	13.7%	18.0%	14.3%	17.5%	9.8%	17.3%	15.5%	16.9%	17.9%	20.5%	13.4%
	Don't Know	1.9%	5.6%	1.7%	6.4%	1.1%	4.6%	4.9%	4.0%	3.9%	3.9%	1.3%	2.3%	4.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
3_13 Lack qualified trainers is a barrier	Strongly Disagree	1.9%	2.8%	7.8%	7.6%	12.1%	5.0%	0.0%	6.8%	6.7%	2.6%	11.7%	1.2%	7.1%
	Disagree	19.4%	11.1%	22.4%	16.5%	26.4%	15.0%	25.0%	25.7%	16.7%	17.1%	19.5%	9.3%	18.9%
	Neutral	39.8%	27.8%	30.2%	37.6%	31.9%	36.3%	35.0%	33.8%	35.5%	35.5%	33.8%	40.7%	34.3%
	Agree	22.3%	30.6%	20.7%	18.8%	18.7%	22.7%	12.5%	17.6%	22.0%	19.7%	13.0%	19.8%	22.4%
	Strongly Agree	8.7%	16.7%	10.3%	8.2%	4.4%	9.7%	17.5%	9.5%	9.2%	10.5%	16.9%	14.0%	7.4%
	Don't Know	7.8%	11.1%	8.6%	11.2%	6.6%	11.3%	10.0%	6.8%	9.9%	14.5%	5.2%	15.1%	9.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q3_12 – Q3_13: Demographic Group B (Q10_Coded Q11_Coded Q12 Q13_Coded Q14_CodedCombine)

		Q10_Coded Full-time employees			Q11_Coded Part-time employees		Q13_Coded Years of organization		Q14_CodedCombined Purpose of organization				
		0-4	5-9	10 and Above	0-4	5 and Above	Under 25 years	25 years or over	Retail, wholesale	Professional services, financial, healthcare	Personal services, religious, housing	Manufacturing, construction, agriculture	Government, education, library
3_12 Time for cybersecurity training is a barrier	Strongly Disagree	2.0%	7.7%	8.5%	6.1%	7.7%	6.7%	6.4%	5.8%	8.2%	4.4%	5.1%	8.4%
	Disagree	11.9%	14.1%	25.6%	17.8%	24.6%	19.0%	20.4%	10.1%	24.6%	20.0%	11.4%	28.9%
	Neutral	29.4%	25.6%	24.8%	28.3%	20.8%	26.7%	26.0%	27.5%	22.1%	27.8%	29.1%	18.1%
	Agree	32.8%	34.6%	21.4%	28.9%	26.2%	27.6%	28.2%	29.0%	29.5%	24.4%	40.5%	24.1%
	Strongly Agree	19.4%	14.1%	15.4%	15.2%	16.9%	16.2%	15.3%	23.2%	13.1%	18.9%	7.6%	18.1%
	Don't Know	4.5%	3.8%	4.3%	3.8%	3.8%	3.8%	3.8%	4.3%	2.5%	4.4%	6.3%	2.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
3_13 Lack qualified trainers is a barrier	Strongly Disagree	2.5%	3.9%	9.4%	6.2%	8.6%	5.7%	7.1%	4.3%	9.3%	5.6%	6.3%	8.4%
	Disagree	10.6%	13.2%	23.9%	17.0%	16.4%	16.0%	17.7%	14.5%	21.2%	9.0%	15.0%	20.5%
	Neutral	35.2%	35.5%	35.9%	33.7%	40.6%	38.7%	34.5%	37.7%	25.4%	40.4%	33.8%	34.9%
	Agree	25.1%	23.7%	15.4%	22.6%	14.1%	17.0%	21.2%	21.7%	22.0%	21.3%	27.5%	19.3%
	Strongly Agree	15.1%	7.9%	6.8%	9.4%	12.5%	17.0%	8.2%	10.1%	12.7%	9.0%	6.3%	9.6%
	Don't Know	11.6%	15.8%	8.5%	11.1%	7.8%	5.7%	11.4%	11.6%	9.3%	14.6%	11.3%	7.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q3_12 – Q3_13: Demographic Group C (Q15_CodedCombined Q16 Q17_Coded)

		Q15_CodedCombined Role				Q16 Have formal cybersecurity training			Q17_Coded City population		
		CEO/Pres/Owner/Partner	Office administrator/manager, accountant/bookkeeper/treasurer	Director/manager	IT Director /CIO	Yes	No	Unsure	Less than 5,000	5,000 to 49,999	Above 50,000
3_12 Time for cybersecurity training is a barrier	Strongly Disagree	3.2%	6.5%	8.1%	8.9%	12.3%	3.6%	0.0%	3.8%	8.3%	8.2%
	Disagree	10.4%	18.5%	22.2%	39.3%	33.3%	10.9%	25.0%	21.4%	20.3%	18.2%
	Neutral	29.2%	25.0%	32.3%	12.5%	18.7%	30.4%	12.5%	23.9%	27.1%	24.7%
	Agree	35.1%	27.2%	21.2%	26.8%	23.4%	31.2%	37.5%	30.8%	23.3%	31.2%
	Strongly Agree	17.5%	16.3%	15.2%	10.7%	11.7%	18.5%	18.8%	17.6%	15.8%	14.7%
	Don't Know	4.5%	6.5%	1.0%	1.8%	0.6%	5.4%	6.3%	2.5%	5.3%	2.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
3_13 Lack qualified trainers is a barrier	Strongly Disagree	3.9%	3.3%	8.2%	12.5%	13.6%	3.3%	0.0%	5.0%	6.9%	8.9%
	Disagree	11.7%	15.4%	16.3%	35.7%	29.0%	8.4%	31.3%	17.6%	15.3%	17.9%
	Neutral	35.1%	34.1%	41.8%	21.4%	29.6%	37.2%	43.8%	31.4%	42.7%	30.4%
	Agree	29.2%	17.6%	15.3%	21.4%	16.6%	24.8%	12.5%	25.2%	14.5%	23.8%
	Strongly Agree	9.7%	16.5%	9.2%	5.4%	5.3%	13.5%	0.0%	15.1%	7.6%	7.1%
	Don't Know	10.4%	13.2%	9.2%	3.6%	5.9%	12.8%	12.5%	5.7%	13.0%	11.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q4_1 – Q4_6: Demographic Group A (Q6Combined, Q7, Q8, Q9_CodedCombined)

		Q6Combined Online payment system usage				Q7 Experienced a malicious cybersecurity event			Q8 Experienced a non-malicious data loss			Q9_CodedCombined Organization		
		Client transactions	Vendor transactions	Both	No online payment system	Yes	No	Don't Know	Yes	No	Don't Know	Govt/School	Nonprofit/not-for-profit	For-profit business
Q4_1 Understand importance of cybersecurity policies	Strongly Disagree	0.0%	0.0%	0.0%	1.2%	0.0%	0.7%	0.0%	0.0%	0.7%	0.0%	0.0%	0.0%	0.7%
	Disagree	3.8%	2.8%	1.7%	1.2%	2.2%	2.3%	2.3%	1.3%	1.8%	5.1%	1.5%	1.3%	2.8%
	Neutral	14.3%	25.0%	10.1%	21.1%	8.8%	18.8%	18.6%	12.0%	18.7%	13.9%	11.9%	17.5%	16.7%
	Agree	52.4%	41.7%	51.3%	52.0%	56.0%	51.2%	37.2%	52.0%	51.4%	46.8%	44.8%	57.5%	50.2%
	Strongly Agree	28.6%	22.2%	35.3%	21.6%	31.9%	24.8%	34.9%	32.0%	25.7%	29.1%	41.8%	22.5%	26.1%
	Don't Know	1.0%	8.3%	1.7%	2.9%	1.1%	2.3%	7.0%	2.7%	1.8%	5.1%	0.0%	1.3%	3.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_2 Recognize need for regular data backups and recovery	Strongly Disagree	0.0%	0.0%	0.0%	0.6%	0.0%	0.3%	0.0%	0.0%	0.4%	0.0%	0.0%	0.0%	0.3%
	Disagree	1.0%	0.0%	0.0%	0.0%	0.0%	0.0%	2.3%	0.0%	0.0%	1.3%	0.0%	0.0%	0.3%
	Neutral	1.9%	0.0%	5.0%	3.5%	1.1%	3.3%	9.3%	4.0%	2.8%	5.1%	3.0%	2.5%	3.5%
	Agree	40.0%	63.9%	38.7%	49.1%	30.8%	50.5%	37.2%	37.3%	47.5%	43.0%	34.3%	46.3%	47.4%
	Strongly Agree	57.1%	33.3%	56.3%	45.6%	68.1%	45.2%	48.8%	58.7%	48.6%	49.4%	62.7%	51.2%	47.4%
	Don't Know	0.0%	2.8%	0.0%	1.2%	0.0%	0.7%	2.3%	0.0%	0.7%	1.3%	0.0%	0.0%	1.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_3 Recognize risks of outdated systems and importance of regular updates	Disagree	2.9%	0.0%	0.0%	0.6%	0.0%	0.7%	4.7%	0.0%	0.4%	3.8%	0.0%	1.3%	1.0%
	Neutral	5.7%	11.1%	5.9%	9.4%	5.5%	8.6%	9.3%	4.0%	8.8%	8.9%	10.4%	10.0%	6.6%
	Agree	48.6%	52.8%	52.1%	52.9%	42.9%	54.3%	46.5%	52.0%	50.5%	51.9%	32.8%	51.2%	54.5%
	Strongly Agree	42.9%	33.3%	42.0%	34.7%	51.6%	35.1%	37.2%	42.7%	39.2%	34.2%	56.7%	37.5%	35.7%
	Don't Know	0.0%	2.8%	0.0%	2.4%	0.0%	1.3%	2.3%	1.3%	1.1%	1.3%	0.0%	0.0%	2.1%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_4 Understand risks of third-party vendors and need for stringent security	Strongly Disagree	1.0%	0.0%	0.8%	1.2%	0.0%	1.3%	0.0%	0.0%	1.1%	1.3%	0.0%	1.3%	1.0%
	Disagree	6.7%	2.8%	0.8%	2.9%	4.4%	2.6%	4.7%	1.3%	2.8%	6.3%	0.0%	3.8%	3.8%
	Neutral	9.6%	11.1%	7.6%	16.9%	7.7%	13.5%	16.3%	8.0%	14.4%	10.1%	11.9%	15.0%	12.2%
	Agree	49.0%	47.2%	50.4%	50.6%	42.9%	52.8%	39.5%	45.3%	51.4%	45.6%	37.3%	52.5%	50.2%
	Strongly Agree	32.7%	25.0%	39.5%	25.0%	44.0%	26.7%	32.6%	42.7%	27.8%	31.6%	49.3%	25.0%	28.9%
	Don't Know	1.0%	13.9%	0.8%	3.5%	1.1%	3.0%	7.0%	2.7%	2.5%	5.1%	1.5%	2.5%	3.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_5 Cybersecurity training is essential for organization	Strongly Disagree	0.0%	0.0%	0.0%	1.2%	0.0%	0.7%	0.0%	0.0%	0.7%	0.0%	0.0%	1.3%	0.4%
	Disagree	4.8%	0.0%	0.8%	3.0%	4.4%	2.0%	2.4%	1.3%	3.2%	1.3%	0.0%	2.5%	3.2%
	Neutral	16.3%	30.6%	15.1%	22.5%	13.2%	22.3%	16.7%	17.3%	20.9%	17.9%	14.9%	22.5%	20.4%
	Agree	45.2%	44.4%	44.5%	47.9%	47.3%	45.8%	42.9%	40.0%	47.9%	43.6%	37.3%	48.8%	46.5%
	Strongly Agree	32.7%	16.7%	38.7%	21.9%	35.2%	26.2%	33.3%	38.7%	25.9%	30.8%	47.8%	22.5%	26.8%
	Don't Know	1.0%	8.3%	0.8%	3.6%	0.0%	3.0%	4.8%	2.7%	1.4%	6.4%	0.0%	2.5%	2.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_6 Cybersecurity training reduces data breaches and ransomware attack risks	Strongly Disagree	0.0%	0.0%	0.0%	1.8%	0.0%	1.0%	0.0%	0.0%	1.1%	0.0%	0.0%	1.3%	0.7%
	Disagree	1.0%	0.0%	0.0%	1.8%	1.1%	0.7%	2.3%	0.0%	0.7%	2.6%	0.0%	0.0%	1.4%
	Neutral	8.7%	20.0%	12.7%	11.7%	5.6%	14.3%	11.6%	8.1%	14.1%	9.0%	10.4%	12.5%	12.3%
	Agree	59.6%	57.1%	46.6%	55.6%	55.6%	54.2%	48.8%	52.7%	54.1%	53.8%	40.3%	65.0%	53.9%
	Strongly Agree	29.8%	17.1%	40.7%	26.3%	37.8%	27.6%	34.9%	36.5%	28.3%	33.3%	49.3%	21.3%	28.9%
	Don't Know	1.0%	5.7%	0.0%	2.9%	0.0%	2.3%	2.3%	2.7%	1.8%	1.3%	0.0%	0.0%	2.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q4_1 – Q4_6: Demographic Group B (Q10_Coded Q11_Coded Q12 Q13_Coded Q14_CodedCombine)

		Q10_Coded Full-time employees			Q11_Coded Part-time employees		Q13_Coded Years of organization		Q14_CodedCombined Purpose of organization				
		0-4	5-9	10 and Above	0-4	5 and Above	Under 25 years	25 years or over	Retail, wholesale	Professional services, financial, healthcare	Personal services, religious, housing	Manufacturing, construction, agriculture	Government, education, library
Q4_1 Understand importance of cybersecurity policies	Strongly Disagree	1.1%	0.0%	0.0%	0.6%	0.0%	1.0%	0.3%	1.6%	0.9%	0.0%	0.0%	0.0%
	Disagree	2.3%	1.4%	1.9%	2.2%	2.7%	4.0%	1.8%	1.6%	1.8%	1.2%	3.8%	3.8%
	Neutral	27.4%	14.9%	10.2%	19.0%	8.0%	14.1%	16.8%	16.4%	15.2%	16.9%	21.8%	14.1%
	Agree	43.4%	63.5%	53.7%	50.6%	52.2%	53.5%	49.7%	52.5%	45.5%	50.6%	55.1%	46.2%
	Strongly Agree	21.7%	17.6%	33.3%	24.7%	35.4%	24.2%	29.0%	24.6%	33.0%	30.1%	14.1%	35.9%
	Don't Know	4.0%	2.7%	0.9%	2.8%	1.8%	3.0%	2.4%	3.3%	3.6%	1.2%	5.1%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_2 Recognize need for regular data backups and recovery	Strongly Disagree	0.6%	0.0%	0.0%	0.3%	0.0%	0.0%	0.3%	1.6%	0.0%	0.0%	0.0%	0.0%
	Disagree	0.0%	1.4%	0.0%	0.3%	0.0%	1.0%	0.0%	0.0%	0.0%	0.0%	0.0%	1.3%
	Neutral	5.1%	2.7%	0.9%	3.8%	1.8%	4.0%	3.0%	4.9%	2.7%	6.0%	0.0%	3.8%
	Agree	52.6%	51.4%	41.7%	47.5%	38.9%	46.5%	44.6%	47.5%	37.5%	49.4%	59.0%	33.3%
	Strongly Agree	40.6%	43.2%	57.4%	47.2%	59.3%	48.5%	51.2%	45.9%	59.8%	44.6%	37.2%	61.5%
	Don't Know	1.1%	1.4%	0.0%	0.9%	0.0%	0.0%	0.9%	0.0%	0.0%	0.0%	3.8%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_3 Recognize risks of outdated systems and importance of regular updates	Disagree	1.1%	2.7%	0.0%	0.6%	1.8%	1.0%	0.9%	1.6%	0.9%	1.2%	0.0%	1.3%
	Neutral	9.8%	5.4%	8.3%	7.0%	9.7%	4.1%	9.0%	4.9%	4.5%	13.3%	7.8%	10.3%
	Agree	56.9%	56.8%	47.2%	55.9%	37.2%	55.1%	49.1%	60.7%	46.4%	47.0%	64.9%	35.9%
	Strongly Agree	29.9%	32.4%	44.4%	34.6%	51.3%	38.8%	39.5%	31.1%	46.4%	38.6%	23.4%	52.6%
	Don't Know	2.3%	2.7%	0.0%	1.9%	0.0%	1.0%	1.5%	1.6%	1.8%	0.0%	3.9%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_4 Understand risks of third-party vendors and need for stringent security	Strongly Disagree	1.7%	1.4%	0.0%	1.0%	0.9%	0.0%	1.2%	3.3%	0.9%	1.2%	0.0%	0.0%
	Disagree	1.7%	5.5%	5.6%	3.2%	3.5%	4.0%	3.0%	3.3%	3.6%	3.6%	3.8%	2.6%
	Neutral	17.6%	6.8%	13.0%	14.0%	8.8%	13.1%	12.6%	11.5%	7.1%	14.5%	14.1%	17.9%
	Agree	53.4%	57.5%	42.6%	52.4%	39.5%	49.5%	48.2%	55.7%	43.8%	49.4%	61.5%	33.3%
	Strongly Agree	22.2%	26.0%	34.3%	26.3%	43.9%	31.3%	31.4%	24.6%	41.1%	28.9%	14.1%	43.6%
	Don't Know	3.4%	2.7%	4.6%	3.2%	3.5%	2.0%	3.6%	1.6%	3.6%	2.4%	6.4%	2.6%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_5 Cybersecurity training is essential for organization	Strongly Disagree	1.2%	0.0%	0.0%	0.6%	0.0%	0.0%	0.6%	0.0%	0.9%	1.2%	0.0%	0.0%
	Disagree	4.1%	2.7%	1.9%	3.5%	0.0%	4.1%	2.1%	3.2%	0.9%	0.0%	6.5%	1.3%
	Neutral	28.5%	18.9%	14.8%	22.1%	14.0%	18.4%	20.5%	21.0%	16.4%	23.2%	24.7%	16.7%
	Agree	39.5%	58.1%	50.0%	46.5%	43.9%	45.9%	45.2%	50.0%	41.8%	47.6%	50.6%	37.2%
	Strongly Agree	23.3%	17.6%	31.5%	25.0%	39.5%	28.6%	29.5%	21.0%	37.3%	25.6%	14.3%	44.9%
	Don't Know	3.5%	2.7%	1.9%	2.2%	2.6%	3.1%	2.1%	4.8%	2.7%	2.4%	3.9%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_6 Cybersecurity training reduces data breaches and ransomware attack risks	Strongly Disagree	1.7%	0.0%	0.0%	1.0%	0.0%	1.0%	0.6%	0.0%	0.9%	1.3%	1.3%	0.0%
	Disagree	0.6%	1.4%	1.9%	1.3%	0.0%	2.1%	0.6%	0.0%	0.0%	0.0%	3.8%	1.3%
	Neutral	19.2%	12.2%	5.6%	13.1%	8.8%	12.4%	12.0%	11.5%	8.9%	16.3%	10.3%	12.8%
	Agree	50.6%	64.9%	56.5%	55.4%	50.9%	56.7%	52.9%	65.6%	47.3%	53.8%	62.8%	39.7%
	Strongly Agree	23.8%	20.3%	36.1%	26.9%	39.5%	27.8%	31.5%	19.7%	41.1%	28.7%	16.7%	46.2%
	Don't Know	4.1%	1.4%	0.0%	2.2%	0.9%	0.0%	2.4%	3.3%	1.8%	0.0%	5.1%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q4_1 – Q4_6: Demographic Group C (Q15_CodedCombined Q16 Q17_Coded)

		Q15_CodedCombined Role				Q16 Have formal cybersecurity training			Q17_Coded City population		
		CEO/Pres/Owner /Partner	Office administrator/manager, accountant/bookkeeper/treasurer	Director/manager	IT Director/CIO	Yes	No	Unsure	Less than 5,000	5,000 to 49,999	Above 50,000
Q4_1 Understand importance of cybersecurity policies	Strongly Disagree	1.4%	0.0%	0.0%	0.0%	0.6%	0.4%	0.0%	0.7%	0.8%	0.0%
	Disagree	1.4%	4.8%	1.1%	3.8%	1.3%	3.1%	0.0%	1.4%	0.8%	4.4%
	Neutral	21.1%	20.5%	17.4%	1.9%	3.9%	23.5%	28.6%	17.8%	12.4%	19.4%
	Agree	51.4%	37.3%	54.3%	50.9%	48.7%	51.2%	50.0%	51.4%	57.9%	43.1%
	Strongly Agree	19.0%	34.9%	27.2%	43.4%	45.5%	18.1%	14.3%	26.0%	25.6%	30.6%
	Don't Know	5.6%	2.4%	0.0%	0.0%	0.0%	3.8%	7.1%	2.7%	2.5%	2.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_2 Recognize need for regular data backups and recovery	Strongly Disagree	0.7%	0.0%	0.0%	0.0%	0.0%	0.4%	0.0%	0.7%	0.0%	0.0%
	Disagree	0.7%	0.0%	0.0%	0.0%	0.0%	0.4%	0.0%	0.0%	0.0%	0.6%
	Neutral	4.9%	4.8%	3.3%	0.0%	0.6%	5.0%	0.0%	4.1%	0.8%	4.4%
	Agree	52.8%	48.2%	44.6%	22.6%	31.2%	52.3%	64.3%	53.4%	46.3%	36.3%
	Strongly Agree	38.7%	47.0%	52.2%	77.4%	68.2%	40.8%	35.7%	41.1%	52.1%	58.1%
	Don't Know	2.1%	0.0%	0.0%	0.0%	0.0%	1.2%	0.0%	0.7%	0.8%	0.6%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_3 Recognize risks of outdated systems and importance of regular updates	Disagree	1.4%	1.2%	1.1%	0.0%	0.0%	1.5%	0.0%	0.0%	0.8%	1.9%
	Neutral	8.5%	10.8%	5.4%	5.7%	3.2%	10.4%	14.3%	11.0%	7.4%	5.6%
	Agree	61.7%	54.2%	52.2%	13.2%	38.3%	57.5%	64.3%	56.6%	46.3%	48.8%
	Strongly Agree	24.1%	33.7%	41.3%	81.1%	58.4%	28.2%	21.4%	31.0%	43.0%	43.1%
	Don't Know	4.3%	0.0%	0.0%	0.0%	0.0%	2.3%	0.0%	1.4%	2.5%	0.6%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_4 Understand risks of third-party vendors and need for stringent security	Strongly Disagree	1.4%	1.2%	1.1%	0.0%	0.6%	1.2%	0.0%	0.7%	0.8%	1.3%
	Disagree	4.9%	1.2%	3.3%	3.8%	1.9%	4.2%	0.0%	1.4%	1.7%	5.6%
	Neutral	13.3%	14.6%	8.7%	5.7%	6.5%	15.8%	14.3%	12.9%	9.2%	14.4%
	Agree	55.2%	52.4%	52.2%	28.3%	40.3%	53.5%	64.3%	55.1%	52.5%	41.3%
	Strongly Agree	18.2%	30.5%	33.7%	58.5%	50.0%	20.8%	14.3%	29.3%	30.0%	33.8%
	Don't Know	7.0%	0.0%	1.1%	3.8%	0.6%	4.6%	7.1%	0.7%	5.8%	3.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_5 Cybersecurity training is essential for organization	Strongly Disagree	0.0%	0.0%	0.0%	0.0%	0.6%	0.4%	0.0%	0.7%	0.8%	0.0%
	Disagree	4.3%	0.0%	2.2%	1.9%	1.3%	3.5%	0.0%	2.8%	1.7%	3.1%
	Neutral	26.2%	17.1%	16.3%	11.3%	7.8%	26.4%	30.8%	18.6%	19.3%	20.6%
	Agree	46.8%	54.9%	50.0%	32.1%	40.3%	48.4%	53.8%	49.7%	44.5%	43.1%
	Strongly Agree	17.7%	25.6%	31.5%	52.8%	48.7%	17.8%	15.4%	25.5%	31.1%	30.6%
	Don't Know	5.0%	2.4%	0.0%	1.9%	1.3%	3.5%	0.0%	2.8%	2.5%	2.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q4_6 Cybersecurity training reduces data breaches and ransomware attack risks	Strongly Disagree	0.7%	0.0%	0.0%	0.0%	0.7%	0.8%	0.0%	1.4%	0.8%	0.0%
	Disagree	1.4%	0.0%	0.0%	1.9%	0.7%	1.2%	0.0%	0.7%	0.8%	1.3%
	Neutral	16.2%	14.6%	11.0%	7.5%	6.5%	15.9%	7.1%	12.4%	13.2%	11.4%
	Agree	57.0%	52.4%	59.3%	37.7%	41.8%	59.3%	71.4%	55.2%	48.8%	55.1%
	Strongly Agree	19.7%	31.7%	29.7%	52.8%	50.3%	19.8%	21.4%	28.3%	33.9%	31.0%
	Don't Know	4.9%	1.2%	0.0%	0.0%	0.0%	3.1%	0.0%	2.1%	2.5%	1.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q5_1 – Q5_4: Demographic Group A (Q6Combined, Q7, Q8, Q9_CodedCombined)

		Q6Combined Online payment system usage				Q7 Experienced a malicious cybersecurity event			Q8 Experienced a non-malicious data loss			Q9_CodedCombined Organization		
		Client transactions	Vendor transactions	Both	No online payment system	Yes	No	Don't Know	Yes	No	Don't Know	Govt/School	Nonprofit/not-for-profit	For-profit business
Q5_1 Have participated in training	Strongly Disagree	16.8%	21.2%	8.0%	20.5%	12.6%	18.2%	15.4%	8.3%	17.6%	21.6%	6.1%	16.9%	19.1%
	Disagree	20.8%	42.4%	38.1%	26.5%	21.8%	32.9%	20.5%	16.7%	33.7%	25.7%	12.1%	36.4%	31.6%
	Neutral	7.9%	9.1%	6.2%	13.3%	9.2%	10.3%	5.1%	8.3%	10.3%	8.1%	6.1%	9.1%	10.3%
	Agree	26.7%	9.1%	25.7%	21.7%	23.0%	22.6%	23.1%	33.3%	22.0%	14.9%	34.8%	19.5%	20.6%
	Strongly Agree	25.7%	15.2%	22.1%	15.7%	33.3%	14.7%	28.2%	33.3%	15.0%	25.7%	40.9%	15.6%	16.5%
	Don't Know	2.0%	3.0%	0.0%	2.4%	0.0%	1.4%	7.7%	0.0%	1.5%	4.1%	0.0%	2.6%	1.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_2 Aware of local or online security training resources	Strongly Disagree	14.4%	20.0%	10.9%	16.3%	11.2%	16.1%	14.3%	6.7%	16.8%	15.6%	3.0%	23.1%	15.6%
	Disagree	34.6%	37.1%	33.6%	30.7%	24.7%	36.1%	26.2%	24.0%	34.8%	35.1%	28.4%	33.3%	33.3%
	Neutral	11.5%	17.1%	18.5%	22.9%	16.9%	17.4%	28.6%	17.3%	20.1%	13.0%	20.9%	20.5%	17.4%
	Agree	19.2%	20.0%	19.3%	16.3%	23.6%	17.7%	7.1%	26.7%	16.8%	13.0%	25.4%	16.7%	16.3%
	Strongly Agree	15.4%	0.0%	11.8%	7.8%	18.0%	8.0%	11.9%	20.0%	7.5%	11.7%	17.9%	3.8%	10.6%
	Don't Know	4.8%	5.7%	5.9%	6.0%	5.6%	4.7%	11.9%	5.3%	3.9%	11.7%	4.5%	2.6%	6.7%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_3 Hands-on training more beneficial than theoretical	Strongly Disagree	1.9%	0.0%	1.7%	0.6%	1.1%	1.0%	2.4%	1.3%	1.1%	1.3%	0.0%	1.3%	1.4%
	Disagree	1.9%	0.0%	7.6%	5.9%	5.5%	4.0%	9.5%	10.7%	3.6%	3.8%	1.5%	1.3%	6.7%
	Neutral	18.3%	22.2%	16.1%	32.0%	22.0%	24.0%	23.8%	21.3%	27.0%	14.1%	25.4%	20.3%	24.3%
	Agree	50.0%	52.8%	50.0%	45.6%	44.0%	51.3%	38.1%	37.3%	49.1%	56.4%	41.8%	48.1%	50.0%
	Strongly Agree	27.9%	19.4%	22.9%	13.0%	27.5%	17.0%	23.8%	28.0%	17.4%	20.5%	31.3%	27.8%	14.8%
	Don't Know	0.0%	5.6%	1.7%	3.0%	0.0%	2.7%	2.4%	1.3%	1.8%	3.8%	0.0%	1.3%	2.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_4 Interested in training on focused topics relevant to my organization	Strongly Disagree	6.9%	2.8%	2.6%	7.4%	4.5%	6.1%	2.6%	4.2%	6.1%	4.0%	3.2%	3.8%	6.5%
	Disagree	2.9%	11.1%	8.6%	13.6%	6.8%	10.2%	7.7%	9.9%	10.1%	5.3%	4.8%	7.6%	10.8%
	Neutral	25.5%	44.4%	32.8%	32.7%	26.1%	32.5%	41.0%	25.4%	33.9%	32.0%	25.8%	36.7%	32.4%
	Agree	43.1%	25.0%	44.8%	37.7%	45.5%	40.0%	30.8%	36.6%	41.2%	40.0%	45.2%	35.4%	40.3%
	Strongly Agree	21.6%	11.1%	10.3%	4.3%	12.5%	9.5%	15.4%	21.1%	7.6%	12.0%	21.0%	15.2%	6.8%
	Don't Know	0.0%	5.6%	0.9%	4.3%	4.5%	1.7%	2.6%	2.8%	1.1%	6.7%	0.0%	1.3%	3.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q5_1 – Q5_4: Demographic Group B (Q10_Coded Q11_Coded Q12 Q13_Coded Q14_CodedCombine)

		Q10_Coded Full-time employees			Q11_Coded Part-time employees		Q13_Coded Years of organization		Q14_CodedCombined Purpose of organization				
		0-4	5-9	10 and Above	0-4	5 and Above	Under 25 years	25 years or over	Retail, wholesale	Professional services, financial, healthcare	Personal services, religious, housing	Manufacturing, construction, agriculture	Government , education, library
Q5_1 Have participated in training	Strongly Disagree	23.6%	15.1%	17.0%	17.4%	15.2%	14.3%	17.3%	21.4%	13.5%	9.0%	30.7%	13.2%
	Disagree	36.0%	41.1%	25.5%	32.1%	22.3%	31.9%	28.5%	42.9%	27.9%	37.2%	30.7%	9.2%
	Neutral	9.9%	9.6%	10.4%	9.4%	9.8%	13.2%	8.4%	8.9%	13.5%	9.0%	8.0%	9.2%
	Agree	17.4%	21.9%	21.7%	21.7%	25.9%	23.1%	22.6%	17.9%	18.0%	25.6%	17.3%	30.3%
	Strongly Agree	9.9%	11.0%	24.5%	17.4%	25.9%	16.5%	21.4%	8.9%	25.2%	16.7%	9.3%	38.2%
	Don't Know	3.1%	1.4%	0.9%	2.0%	0.9%	1.1%	1.9%	0.0%	1.8%	2.6%	4.0%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_2 Aware of local or online security training resources	Strongly Disagree	21.6%	12.5%	15.0%	14.9%	15.9%	14.6%	15.2%	15.3%	15.5%	14.8%	22.1%	10.3%
	Disagree	37.4%	40.3%	29.0%	32.0%	34.5%	32.3%	32.4%	54.2%	30.9%	32.1%	28.6%	24.4%
	Neutral	18.7%	15.3%	16.8%	21.4%	11.5%	19.8%	18.2%	11.9%	13.6%	16.0%	26.0%	24.4%
	Agree	9.9%	23.6%	22.4%	17.2%	20.4%	21.9%	16.7%	8.5%	21.8%	22.2%	9.1%	20.5%
	Strongly Agree	2.9%	5.6%	14.0%	9.1%	12.4%	4.2%	12.4%	3.4%	16.4%	9.9%	5.2%	15.4%
	Don't Know	9.4%	2.8%	2.8%	5.5%	5.3%	7.3%	5.2%	6.8%	1.8%	4.9%	9.1%	5.1%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_3 Hands-on training more beneficial than theoretical	Strongly Disagree	1.7%	2.7%	0.0%	1.3%	0.9%	4.0%	0.3%	1.6%	0.0%	1.2%	1.3%	1.3%
	Disagree	3.5%	8.2%	2.8%	4.5%	6.2%	7.1%	4.2%	6.6%	6.4%	0.0%	5.1%	2.6%
	Neutral	23.7%	13.7%	31.8%	26.0%	17.7%	23.2%	23.9%	27.9%	22.7%	23.5%	21.8%	25.6%
	Agree	46.2%	58.9%	49.5%	47.8%	49.6%	49.5%	47.9%	49.2%	46.4%	50.6%	55.1%	42.3%
	Strongly Agree	22.0%	13.7%	14.0%	18.3%	23.9%	15.2%	21.2%	13.1%	22.7%	22.2%	11.5%	28.2%
	Don't Know	2.9%	2.7%	1.9%	2.2%	1.8%	1.0%	2.4%	1.6%	1.8%	2.5%	5.1%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_4 Interested in training on focused topics relevant to my organization	Strongly Disagree	7.6%	4.2%	4.7%	6.2%	3.6%	7.4%	5.0%	3.3%	6.5%	3.8%	9.1%	2.7%
	Disagree	12.4%	12.7%	3.8%	10.2%	7.3%	10.5%	9.0%	8.2%	9.3%	7.6%	10.4%	5.5%
	Neutral	31.2%	36.6%	33.0%	32.1%	30.9%	27.4%	33.4%	36.1%	28.0%	39.2%	29.9%	26.0%
	Agree	36.5%	31.0%	48.1%	40.0%	41.8%	43.2%	39.3%	45.9%	42.1%	35.4%	40.3%	46.6%
	Strongly Agree	9.4%	9.9%	9.4%	8.5%	15.5%	10.5%	10.5%	4.9%	11.2%	11.4%	5.2%	19.2%
	Don't Know	2.9%	5.6%	0.9%	3.0%	0.9%	1.1%	2.8%	1.6%	2.8%	2.5%	5.2%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q5_1 – Q5_4: Demographic Group C (Q15_CodedCombined Q16 Q17_Coded)

		Q15_CodedCombined Role				Q16 Have formal cybersecurity training			Q17_Coded City population		
		CEO/Pres/Owner/Partner	Office administrator/manager, accountant/bookkeeper/treasurer	Director/manager	IT Director/ CIO	Yes	No	Unsure	Less than 5,000	5,000 to 49,999	Above 50,000
Q5_1 Have participated in training	Strongly Disagree	21.8%	19.8%	13.8%	5.8%	0.6%	28.1%	0.0%	16.3%	18.8%	15.2%
	Disagree	34.6%	34.6%	31.0%	13.5%	3.2%	46.3%	23.1%	31.9%	26.5%	29.1%
	Neutral	10.5%	14.8%	10.3%	1.9%	4.5%	11.6%	38.5%	9.2%	12.0%	8.6%
	Agree	18.0%	16.0%	25.3%	28.8%	40.9%	9.9%	15.4%	22.7%	23.1%	20.5%
	Strongly Agree	12.0%	12.3%	19.5%	50.0%	50.6%	2.1%	7.7%	17.0%	17.9%	25.8%
	Don't Know	3.0%	2.5%	0.0%	0.0%	0.0%	2.1%	15.4%	2.8%	1.7%	0.7%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_2 Aware of local or online security training resources	Strongly Disagree	17.1%	19.5%	14.6%	3.8%	4.6%	22.4%	0.0%	14.6%	12.5%	17.3%
	Disagree	36.4%	39.0%	37.1%	18.9%	15.0%	43.3%	42.9%	36.1%	29.2%	33.3%
	Neutral	23.6%	15.9%	15.7%	11.3%	18.3%	17.7%	28.6%	18.1%	25.0%	14.1%
	Agree	10.0%	13.4%	19.1%	34.0%	34.0%	7.9%	7.1%	15.3%	16.7%	19.9%
	Strongly Agree	5.0%	7.3%	9.0%	32.1%	24.8%	2.4%	7.1%	9.7%	10.0%	12.2%
	Don't Know	7.9%	4.9%	4.5%	0.0%	3.3%	6.3%	14.3%	6.3%	6.7%	3.2%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_3 Hands-on training more beneficial than theoretical	Strongly Disagree	1.4%	0.0%	2.2%	1.9%	0.6%	1.6%	0.0%	0.7%	1.7%	1.3%
	Disagree	4.9%	6.2%	4.3%	5.7%	6.5%	3.1%	7.1%	5.5%	2.5%	5.0%
	Neutral	23.9%	19.8%	21.7%	37.7%	28.6%	21.9%	21.4%	21.2%	23.5%	28.3%
	Agree	48.6%	56.8%	52.2%	30.2%	34.4%	55.5%	64.3%	53.4%	50.4%	41.5%
	Strongly Agree	17.6%	14.8%	19.6%	22.6%	28.6%	15.2%	7.1%	16.4%	20.2%	22.0%
	Don't Know	3.5%	2.5%	0.0%	1.9%	1.3%	2.7%	0.0%	2.7%	1.7%	1.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_4 Interested in training on focused topics relevant to my organization	Strongly Disagree	6.6%	5.0%	2.2%	3.8%	5.4%	5.6%	0.0%	7.0%	4.4%	4.5%
	Disagree	7.3%	11.3%	11.1%	5.7%	8.1%	9.5%	7.7%	6.3%	12.3%	9.0%
	Neutral	30.7%	36.3%	31.1%	22.6%	33.8%	31.0%	30.8%	33.8%	30.7%	32.1%
	Agree	46.7%	37.5%	37.8%	45.3%	37.2%	42.9%	38.5%	38.7%	38.6%	43.6%
	Strongly Agree	5.1%	10.0%	14.4%	22.6%	14.2%	7.9%	23.1%	11.3%	11.4%	9.0%
	Don't Know	3.6%	0.0%	3.3%	0.0%	1.4%	3.2%	0.0%	2.8%	2.6%	1.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q5_5 – Q5_7: Demographic Group A (Q6Combined, Q7, Q8, Q9_CodedCombined)

		Q6Combined Online payment system usage				Q7 Experienced a malicious cybersecurity event			Q8 Experienced a non-malicious data loss			Q9_CodedCombined Organization		
		Client transactions	Vendor transactions	Both	No online payment system	Yes	No	Don't Know	Yes	No	Don't Know	Govt/School	Nonprofit/not -for-profit	For-profit business
Q5_5 Trainings should be regularly updated to latest threats	Strongly Disagree	1.9%	0.0%	0.0%	1.8%	0.0%	1.3%	2.3%	0.0%	1.4%	1.3%	1.5%	0.0%	1.4%
	Disagree	0.0%	0.0%	1.7%	1.2%	0.0%	1.0%	2.3%	2.7%	0.7%	0.0%	0.0%	1.3%	1.1%
	Neutral	6.7%	22.2%	10.9%	22.3%	7.8%	17.7%	14.0%	13.5%	17.1%	10.1%	6.0%	13.8%	17.7%
	Agree	51.4%	58.3%	56.3%	53.6%	52.2%	55.2%	53.5%	41.9%	57.1%	55.7%	52.2%	57.5%	53.9%
	Strongly Agree	40.0%	13.9%	30.3%	16.9%	37.8%	22.4%	25.6%	39.2%	21.8%	29.1%	38.8%	26.3%	23.4%
	Don't Know	0.0%	5.6%	0.8%	4.2%	2.2%	2.3%	2.3%	2.7%	1.8%	3.8%	1.5%	1.3%	2.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_6 Access to local support center would greatly benefit my organization	Strongly Disagree	1.0%	0.0%	0.0%	3.0%	1.1%	1.7%	0.0%	0.0%	2.2%	0.0%	1.5%	1.3%	1.4%
	Disagree	5.8%	0.0%	6.8%	4.8%	7.9%	4.4%	4.9%	10.8%	4.7%	1.3%	3.0%	2.5%	6.1%
	Neutral	25.0%	36.1%	33.3%	43.0%	28.1%	36.6%	43.9%	39.2%	37.6%	25.0%	39.4%	34.2%	35.0%
	Agree	42.3%	41.7%	38.5%	33.9%	42.7%	39.3%	17.1%	32.4%	38.7%	39.5%	30.3%	38.0%	39.6%
	Strongly Agree	26.0%	13.9%	19.7%	10.3%	19.1%	14.8%	29.3%	17.6%	14.3%	26.3%	25.8%	21.5%	13.9%
	Don't Know	0.0%	8.3%	1.7%	4.8%	1.1%	3.4%	4.9%	0.0%	2.5%	7.9%	0.0%	2.5%	3.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_7 Willing to allocate budget and resources for regular employee training	Strongly Disagree	5.8%	2.9%	1.7%	9.7%	2.3%	7.1%	5.3%	4.2%	7.6%	1.4%	1.5%	6.5%	6.9%
	Disagree	9.7%	17.6%	10.3%	13.9%	8.0%	13.8%	7.9%	15.3%	12.2%	8.1%	7.6%	11.7%	12.6%
	Neutral	34.0%	47.1%	38.8%	46.1%	36.4%	42.1%	39.5%	27.8%	43.2%	43.2%	34.8%	46.8%	40.8%
	Agree	33.0%	23.5%	30.2%	21.2%	37.5%	24.6%	26.3%	38.9%	25.2%	24.3%	31.8%	16.9%	28.5%
	Strongly Agree	9.7%	5.9%	11.2%	0.6%	10.2%	4.7%	7.9%	12.5%	4.7%	6.8%	15.2%	6.5%	4.3%
	Don't Know	7.8%	2.9%	7.8%	8.5%	5.7%	7.7%	13.2%	1.4%	7.2%	16.2%	9.1%	11.7%	6.9%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q5_5 – Q5_7: Demographic Group B (Q10_Coded Q11_Coded Q12 Q13_Coded Q14_CodedCombine)

		Q10_Coded Full-time employees			Q11_Coded Part-time employees		Q13_Coded Years of organization		Q14_CodedCombined Purpose of organization				
		0-4	5-9	10 and Above	0-4	5 and Above	Under 25 years	25 years or over	Retail, wholesale	Professional services, financial, healthcare	Personal services, religious, housing	Manufacturing, construction, agriculture	Government , education, library
Q5_5 Trainings should be regularly updated to latest threats	Strongly Disagree	1.2%	2.7%	0.9%	1.3%	0.9%	3.1%	0.6%	0.0%	1.9%	0.0%	1.3%	2.6%
	Disagree	1.2%	1.4%	0.0%	1.0%	0.9%	0.0%	1.2%	1.6%	0.0%	1.2%	1.3%	0.0%
	Neutral	20.2%	19.2%	9.3%	16.1%	12.3%	25.8%	12.1%	18.0%	16.7%	14.6%	14.1%	10.3%
	Agree	56.1%	52.1%	60.7%	55.3%	52.6%	48.5%	55.9%	54.1%	50.9%	58.5%	57.7%	51.3%
	Strongly Agree	17.9%	21.9%	28.0%	23.8%	32.5%	22.7%	27.5%	23.0%	29.6%	23.2%	20.5%	34.6%
	Don't Know	3.5%	2.7%	0.9%	2.6%	0.9%	0.0%	2.7%	3.3%	0.9%	2.4%	5.1%	1.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_6 Access to local support center would greatly benefit my organization	Strongly Disagree	1.7%	0.0%	2.8%	1.6%	0.9%	1.0%	1.5%	0.0%	2.8%	1.2%	1.3%	1.3%
	Disagree	2.9%	8.3%	4.7%	4.5%	5.4%	3.1%	5.2%	8.2%	3.7%	1.2%	6.5%	2.6%
	Neutral	39.5%	25.0%	34.6%	36.1%	34.2%	38.1%	34.9%	32.8%	32.7%	39.5%	32.5%	40.3%
	Agree	33.1%	45.8%	42.1%	40.0%	32.4%	39.2%	37.6%	42.6%	35.5%	39.5%	45.5%	31.2%
	Strongly Agree	18.0%	16.7%	14.0%	14.8%	23.4%	17.5%	17.1%	14.8%	19.6%	16.0%	9.1%	24.7%
	Don't Know	4.7%	4.2%	1.9%	2.9%	3.6%	1.0%	3.7%	1.6%	5.6%	2.5%	5.2%	0.0%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_7 Willing to allocate budget and resources for regular employee training	Strongly Disagree	8.3%	6.9%	5.7%	5.6%	7.3%	8.2%	5.3%	6.6%	6.6%	2.6%	9.0%	3.9%
	Disagree	16.7%	11.1%	7.5%	13.1%	7.3%	13.4%	10.9%	11.5%	9.4%	14.1%	11.5%	9.2%
	Neutral	41.7%	40.3%	44.3%	42.5%	37.3%	37.1%	42.2%	50.8%	34.9%	42.3%	43.6%	36.8%
	Agree	21.4%	25.0%	26.4%	25.5%	31.8%	27.8%	26.7%	26.2%	34.9%	28.2%	19.2%	26.3%
	Strongly Agree	2.4%	5.6%	8.5%	5.2%	9.1%	6.2%	6.5%	0.0%	8.5%	6.4%	3.8%	11.8%
	Don't Know	9.5%	11.1%	7.5%	8.2%	7.3%	7.2%	8.4%	4.9%	5.7%	6.4%	12.8%	11.8%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Q5_5 – Q5_7: Demographic Group C (Q15_CodedCombined Q16 Q17_Coded)

		Q15_CodedCombined Role				Q16 Have formal cybersecurity training			Q17_Coded City population		
		CEO/Pres/Owner/Partner	Office administrator/manager, accountant/bookkeeper/treasurer	Director/manager	IT Director/ CIO	Yes	No	Unsure	Less than 5,000	5,000 to 49,999	Above 50,000
Q5_5 Trainings should be regularly updated to latest threats	Strongly Disagree	2.1%	0.0%	0.0%	0.0%	0.0%	1.9%	0.0%	1.4%	0.8%	1.3%
	Disagree	0.0%	2.4%	1.1%	0.0%	0.0%	1.2%	0.0%	1.4%	0.0%	0.6%
	Neutral	18.6%	14.6%	12.0%	7.5%	8.6%	18.3%	14.3%	16.0%	16.0%	13.2%
	Agree	54.3%	63.4%	53.3%	39.6%	49.3%	57.2%	57.1%	57.6%	53.8%	51.6%
	Strongly Agree	20.0%	18.3%	31.5%	52.8%	41.4%	17.9%	28.6%	20.8%	26.1%	32.1%
	Don't Know	5.0%	1.2%	2.2%	0.0%	0.7%	3.5%	0.0%	2.8%	3.4%	1.3%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_6 Access to local support center would greatly benefit my organization	Strongly Disagree	0.7%	0.0%	0.0%	1.9%	1.3%	1.6%	0.0%	1.4%	2.5%	0.6%
	Disagree	5.0%	5.0%	6.5%	0.0%	4.7%	5.1%	0.0%	2.8%	4.2%	7.0%
	Neutral	30.2%	37.5%	33.7%	40.4%	39.3%	32.9%	35.7%	35.9%	39.5%	31.6%
	Agree	47.5%	38.8%	33.7%	34.6%	32.7%	41.6%	42.9%	40.8%	36.1%	38.6%
	Strongly Agree	10.1%	16.3%	26.1%	21.2%	20.7%	14.5%	21.4%	16.2%	16.0%	17.7%
	Don't Know	6.5%	2.5%	0.0%	1.9%	1.3%	4.3%	0.0%	2.8%	1.7%	4.4%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Q5_7 Willing to allocate budget and resources for regular employee training	Strongly Disagree	7.9%	2.5%	3.4%	5.8%	2.0%	8.7%	0.0%	6.3%	6.0%	5.8%
	Disagree	11.5%	12.7%	11.2%	7.7%	7.3%	13.9%	7.7%	11.8%	8.6%	13.0%
	Neutral	41.0%	41.8%	44.9%	26.9%	37.3%	44.0%	23.1%	41.7%	44.8%	37.7%
	Agree	29.5%	22.8%	25.8%	42.3%	36.0%	21.4%	38.5%	23.6%	26.7%	30.5%
	Strongly Agree	1.4%	7.6%	9.0%	15.4%	12.7%	2.4%	7.7%	6.3%	6.0%	6.5%
	Don't Know	8.6%	12.7%	5.6%	1.9%	4.7%	9.5%	23.1%	10.4%	7.8%	6.5%
	Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%