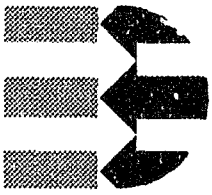

Decima
Research Inc.

MARKET RESEARCH REPORT

YEAR 2000 COMPLIANCE AMONG SMALL BUSINESSES

Prepared for: Industry Canada

Date: May 1999

Table of Contents

LIST OF FIGURES

EXECUTIVE SUMMARY

The arrival of January 1st 2000 is quickly approaching. There have been countless studies conducted and articles written on the impact this date will have on the business community. One such study was conducted by Statistics Canada among medium and large businesses (businesses with 6 or more employees). To complement this effort, Industry Canada commissioned Decima Research Inc. (Decima) to conduct a similar study among small businesses - in other words, businesses with 5 employees or less. A total of 600 small businesses across Canada completed the study.

The following are some of the study highlights discussed throughout the report:

- It is estimated that there are about 1.4 million businesses in Canada with five or less employees.
- About 26% of these businesses have no vulnerabilities to Y2K, although there may exist vulnerabilities based on interdependencies.
- Conversely, approximately 74% of small businesses own or use technologies and systems that can potentially be impacted by Y2K. **All the results below and throughout the report are based on these businesses only (74%).**
- Approximately 31% of businesses have not taken any steps towards preparing their technologies and systems for Y2K. There were no significant regional disparities.
- It is estimated that 38% of technologies and systems are 100% now. A high ramp-up of Y2K compliance activity is expected as businesses anticipate approximately 83% of their technologies and systems to be ready by January 1st 2000.
- About 45% of small businesses have tested at least one of their technologies or systems.
- Approximately 36% of small businesses have contacted at least on critical supplier regarding Y2K issues.
- Only 9% of small businesses have contacted their customers.
- Finally, about 64% of small businesses have or will consider a contingency plan.

INTRODUCTION

BACKGROUND

The arrival of January 1st 2000 is quickly approaching. There have been countless studies conducted and articles written on the impact this date will have on the business community. One such study was conducted by Statistics Canada among medium and large businesses (businesses with 6 or more employees). To complement this effort, Industry Canada commissioned Decima Research Inc. (Decima) to conduct a similar study among small businesses - in other words, businesses with 5 employees or less. A total of 600 small businesses across Canada completed the study.

The main focus of the study was to determine the preparedness of Canadian small businesses for Y2K. More specifically, businesses were asked:

- About their critical systems and technologies,
- Whether they have taken any steps in preparing their systems and technologies for Y2K,
- Whether they have tested their systems and technologies,
- Whether critical suppliers and customers have been contacted, and,
- Whether certain contingency plans have been considered.

DATA COLLECTION

Data was collected by trained, bilingual interviewers. Interviews were randomly monitored by a supervisor to ensure compliance with questionnaire script. A minimum of 15% of completed surveys were monitored in their entirety.

Data collection was completed using Decima's Computer Assisted Telephone Interviewing (CATI) system. Numeric variables, scale questions, and other fixed-response variables were keyed into CATI directly during the interview. Branching and skip logic was handled by the CATI system.

Open-ended variables and commentary were keyed in verbatim to the electronic coding system for review by supervisors and by the client authority. The complete list of open-ended responses was used to develop a code list. After approval by the project prime, the list was used to apply numeric codes to the open-ended variables. A single coder was used for this purpose in order to maximize consistency.

Sample tracking was accomplished using the CATI tracking and control system. Potential respondents were selected randomly from the electronic database; once selected, a minimum of six call attempts were made before a new respondent was chosen. Appointment times were recorded electronically, and priority given to first-selected respondents.

QUESTIONNAIRE DESIGN

The study was designed in English by a Decima consultant around a 15-minute telephone-administered questionnaire and then translated by Industry Canada.

The sponsor of the survey was revealed to respondents. The survey was described as a study aimed at assessing for Industry Canada the potential risk of the Year 2000 issue to businesses across Canada.

The survey instrument is included in Appendix A.

SAMPLE FRAME

The total number of completions was 600, stratified by province. The table below shows the number of completed interviews (*n*) by province. The sample stratification was purposely constructed to proportionately represent the distribution of small businesses across Canada.

	Sample Size
BC / NWT / Yukon	**89**
Alberta	**59**
Saskatchewan	**23**
Manitoba	**24**
Ontario	**222**
Quebec	**141**
New Brunswick	**14**
Nova Scotia	**16**
PEI	**3**
Newfoundland	**9**
Total	**600**

ACCURACY

Sampling error is the margin of error attributable only to random variation within a sample of specific size drawn from a population. The size of sampling error for any question is dependent on the extent of variation for that question within the population as a whole, and on the number of responses to the question. Assuming maximum variation (the conservative assumption), this study's sample size of 600 would result in a margin of error of approximately +/- 4.1%. The reader is cautioned that, for questions or subgroup results with fewer than 600 responses, the margin of error will be larger.

RESULT PRESENTATION AND INTERPRETATION

Only small businesses with 5 or less employees were interviewed – therefore results presented throughout this report are based on only this business segment and in no way represent the business community in general.

Furthermore, respondent screening selected businesses that use or own at least one type of technology or system that could be affected by Y2K. A total of nine technology groups were used (see Q1a of questionnaire in Appendix A). Respondents that only owned a basic wireline telephone were excluded from the study.

Results show that about 26% of all small businesses have no vulnerabilities to Y2K, although there may exist vulnerabilities based on interdependencies.

Conversely, approximately 74% of small businesses own or use technologies and systems other than a basic wireline telephone that can potentially be impacted by Y2K. **Results throughout the report are exclusively based on the 74% of businesses that indicated owning or using a technology or system other than a basic wireline telephone.**

SUB-GROUP ANALYSIS

Results for the following sub-groups are presented throughout the report. The sample size and margin of error for each sub-group are highlighted below.

	Sample Size	Margin of Error
Region		
Quebec	141	+/-8.3%
Ontario	222	+/-6.6%
Rest of Canada (ROC)	237	+/-6.4%
Home Business		
Yes	175	+/-7.4%
No/ Don't Know	425	+/-4.8%
Years in Business		
4 years or less	136	+/-8.4%
5 to 10 years	153	+/-8.0%
10 years or more	308	+/-5.6%
Location		
City / suburb 100K or less	242	+/-6.3%
City/ town 30K-100K	106	+/-9.6%
Town/ rural area <30K	241	+/-6.4%
Revenues		
$0-$50K	129	+/-8.6%
$50-$250K	254	+/-6.2%
$250K or more	119	+/-9.7%
Type of Business		
Retail	155	+/-7.9%
Services	328	+/-5.4%
Goods	117	+/-9.1%
Technology Adoption		
Low (1 – 2 technologies)	182	+/-7.2%
Medium (3 – 4 technologies)	347	+/-5.3%
High (5 or more technologies)	71	+/-11.8%

TECHNOLOGY USED

All businesses were asked whether or not they owned or used any of the systems and technologies listed in the figure below (for examples of each technology and system surveyed, refer to the questionnaire found in Appendix A). For every technology and system owned, the respondent was then asked whether they considered this technology or system "critical". The following definition of critical was used:

> **Critical systems and technologies are those that are essential to the on-going delivery of products or services to clients or to the public or those that impact on the health and safety of your employees or the public.**

Incidences of each general and critical technology and system are presented below.

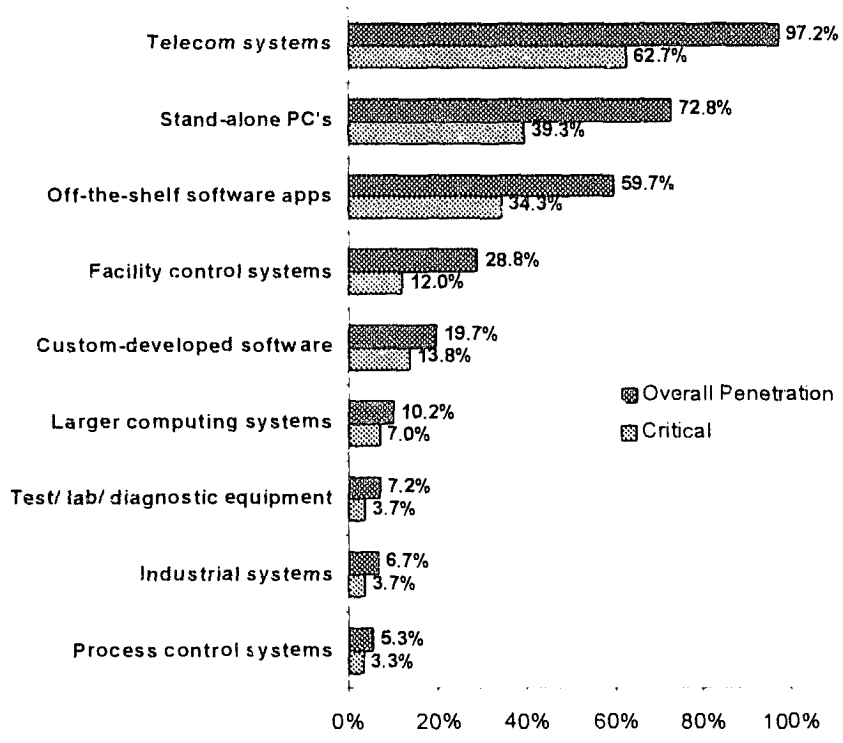

Figure 1: Penetration of General and Critical Technology

Understandably, the most common system was telecommunications related (97.2%), followed by stand-alone PC's (72.8%) and off-the-shelf software applications (59.7%). The least common technologies were industrial systems (6.7%) and process control systems (5.3%).

Detailed analysis was conducted for key market sub-groups. As the table below shows, small businesses own approximately 3.2 technologies and systems overall and about 1.8 critical technologies. The number of technologies is more likely to be higher if the business is located in Ontario, earns over $250K, is located in a city and has been operating for 5 to 10 years.

	Average # of Technologies	Average # of Critical Technologies	% of Technologies Considered Critical
Overall	3.2	1.8	52.7%
Region			
Quebec	3.1	2.1	64.2%
Ontario	3.4	1.8	49.2%
Rest of Canada (ROC)	3.1	1.6	49.2%
Home Business			
Yes	3.0	1.8	54.0%
No/ Don't Know	3.3	1.8	52.1%
Years in Business			
4 years or less	3.2	1.9	56.0%
5 to 10 years	3.4	2.0	54.6%
10 years or more	3.1	1.7	50.2%
Location			
City/ suburb 100K or less	3.4	1.9	53.2%
City/ town 30K-100K	3.3	1.9	54.9%
Town/ rural area <30K	3.0	1.7	51.6%
Revenues			
$0-$50K	2.8	1.4	45.2%
$50-$250K	3.2	1.8	53.8%
$250K or more	3.6	2.0	50.6%
Type of Business			
Retail	3.1	1.5	47.4%
Services	3.3	1.9	54.4%
Goods	3.2	1.8	55.0%
Technology Adoption			
Low (1 – 2)	2.0	0.7	35.7%
Medium (3 – 4)	3.4	2.0	58.9%
High (5 or more)	5.6	3.7	66.3%

PREPARATION FOR Y2K

Having identified the technologies and systems used, respondents were led through a series of questions aimed at establishing their level of "preparedness" for the Year 2000 (Y2K). For each technology and system owned, respondents were asked:

1. If they have taken steps towards preparing this technology or system for Y2K.
2. What percent of that technology is ready for Y2K.
3. If the technology is not 100% ready or if no steps were taken, respondents were asked if they believed the technology or system will be 100% compliant come January 1st 2000.
4. Finally they were asked if they have tested their technology or system, and if not, whether formal plans exist for such testing.

GENERAL STEPS

The first in the series of questions touching on Y2K preparedness asked respondents whether their organization has taken any steps to ensure that its technologies and systems are prepared for the Year 2000.[1]

Results based on all technologies and systems used show that slightly over 2 out of every 3 business has taken steps towards Y2K compliance (69.0%). For the purposes of this analysis, a business was considered to have taken steps if they answered "yes" to at least one of their technologies or systems.

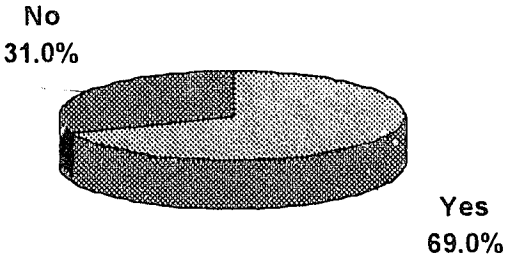

Figure 2: Has Taken Steps in Preparing Technologies for Y2K

[1] This was individually asked for each technology and system that was identified earlier by the respondent.

Sub-group results are presented below **Businesses most likely to have taken steps** towards preparing their technologies or systems for Y2K are located in the city, earn over $50K in revenues, operate in the goods industry and have over three technologies or systems **Businesses the least likely to have taken steps** are located in a town or rural area with a population less than 30K, earn less than $50K, operate in retail, and own less than three technologies or systems

	% That Have Taken Steps
Overall	**69.0%**
Region	
Quebec	71.6%
Ontario	7.
Rest of Canada (ROC)	68.8%
Home Business	
Yes	66.9%
No/ Don't Know	69.8%
Years in Business	
4 years or less	66.9%
5 to 10 years	72.5%
10 years or more	68.5%
Location	
City / suburb 100K or less	74.8%
City/ town 30K-100K	71.7%
Town/ rural area <30K	61.8%
Revenues	
$0-$50K	51.9%
$50-$250K	72.4%
$250K or more	77.3%
Type of Business	
Retail	63.9%
Services	68.6%
Goods	76.9%
Technology Adoption	
Low (1 – 2)	41.2%
Medium (3 – 4)	79.0%
High (5 or more)	91.5%

REASONS FOR NOT HAVING TAKEN STEPS

The 31% of businesses that indicated not having taken any steps towards preparing their technologies and systems for Y2K were asked to provide reasons for their lack of preparedness The most common reason among these respondents was that they "won't be affected by Y2K", which was mentioned by 40.3% of businesses that have not taken steps

Another 19.4% indicated that it was not their responsibility This probably pertains to an issue highlighted earlier when telecommunications systems and facility control systems were discussed The results presented earlier showed that a lower than average proportion of businesses had taken steps towards preparing these systems for Y2K A likely explanation was that users were assuming that the service providers and building management would ensure compliance for the technologies and systems used Results presented below support this potential explanation Finally, approximately 14.5% indicated they don't use much technology

	% of Businesses That Have Not Taken Steps (n=189)
Won't be affected by Y2K	**40.3%**
Not my responsibility/ Others are responsible/ Assumes already compliant	**19.4%**
Don't use much technology	**14.5%**
We have backup/ Can operate manually	**9.7%**
Systems are new, assume they will work properly	**9.1%**
Plan to look at it in near future	**6.5%**
Plan on buying new equipment	**5.4%**
Don't know enough about the issue	**4.8%**
Don't know how to prepare for Y2K	**4.3%**
Not enough time to fix or prepare for Y2K	**4.3%**
Can't afford to fix or prepare for Y2K	**3.8%**
Company is small	**3.2%**
Rather wait and see	**2.7%**
Seasonal company / Would close temporarily	**2.2%**
Haven't thought about it	**1.6%**
Approaching retirement	**1.1%**
Other	**3.2%**
Don't Know	**2.7%**

***Total will not add to 100% because of multiple mentions.**

Results specific to each technology and system are displayed in the table below. The first two columns of results relate to all the technologies and systems identified by the respondent. The results in the last two columns are limited to the technologies and systems that the respondent considered critical. Finally, results in both columns are based only on respondents that indicated owning the respective technologies or systems, thus the varying sample sizes (N).

	% That Have Taken Steps			
	Overall*		Critical**	
	%	N	%	N
Larger computing systems	85.2%	61	90.5%	42
Custom-developed software	79.7%	118	84.3%	83
Stand-alone personal computers	76.2%	437	81.4%	236
Process control systems	71.9%	32	75.0%	20
Off-the-shelf software applications	65.1%	358	74.8%	206
Test/ lab/ diagnostic equipment	53.5%	43	59.1%	22
Industrial systems	50.0%	40	45.5%	22
Facility control systems	42.2%	173	56.9%	72
Telecommunications systems	32.1%	583	33.8%	376

***Base: Businesses that use the given technology or system**

****Base: Businesses that use the given technology or system and consider it critical**

Results show that the technologies and systems that have attracted the most attention in terms of Y2K compliance are all computer related. Approximately 85.2% of respondents with larger computing systems indicated having taken steps towards preparing these systems for Y2K. This is followed by 79.7% among respondents with custom-developed software and 76.2% among businesses with stand-alone personal computers.

Respondents were less likely to have taken steps towards preparing their telecommunications systems (32.1%) and their facility control systems (42.2%). These results are likely attributable to the belief among the users of these technologies and systems that it is not their responsibility to ensure Y2K compliance. For instance, businesses that use or own a telecommunications system probably assume that the service provider is responsible for ensuring compliance, especially since numerous telecommunications equipment and services are rented or belong to the service supplier outright. As for the facility control systems (such as security systems, elevators and building control), users of such systems probably assume that the building management company or landlord will ensure system compliance.

Across most technologies and systems, the more critical the system, the more likely businesses have already taken steps to ensure Y2K compliance.

If businesses indicated having taken steps towards preparing a given technology, they were asked to specify if the technology was 100% ready. If it was not 100% ready, they were to estimate percent readiness. For the purposes of this analysis, it was assumed that if the respondent indicated they had not taken any steps that the percent readiness was "0%".

Results specific to each technology and system are displayed in the table below. Interpretation of the results is the same as the table on the previous page.

	Average Percent Readiness			
	Overall*		Critical**	
	%	N	%	N
Larger computing systems	79.0%	58	82.9%	40
Custom-developed software	74.5%	115	78.8%	81
Stand-alone personal computers	70.2%	420	74.2%	225
Process control systems	68.3%	30	71.1%	19
Off-the-shelf software applications	60.6%	354	69.4%	204
Test/ lab/ diagnostic equipment	52.4%	42	59.1%	22
Industrial systems	46.7%	39	42.4%	21
Facility control systems	39.3%	169	53.9%	70
Telecommunications systems	29.7%	574	30.9%	368

***Base: Businesses that use the given technology or system**

****Base: Businesses that use the given technology or system and consider it critical**

Once again, results show that the technologies and systems that have attracted the most attention in terms of Y2K compliance are all computer related. Respondents with larger computing systems indicated that these systems are approximately 79.0% compliant. This is followed by 74.5% readiness for custom-developed software and 70.2% for stand-alone personal computers.

Across most technologies and systems, results are slightly higher among those considered critical compared to overall technologies and systems used.

Additional analysis was conducted to determine the proportion of general and critical technologies and systems that are 100% ready now and what proportion will be 100% ready come January 1st 2000. Detailed results across sub-groups are presented below:

	General Technologies/ Systems		Critical Technologies/ Systems	
	100% Ready Now	100% Ready Jan. 1st 2000	100% Ready Now	100% Ready Jan. 1st 2000
Overall	37.9%	82.9%	39.7%	91.5%
Region				
Quebec	45.8%	82.3%	47.3%	93.3%
Ontario	34.2%	83.1%	33.5%	90.1%
Rest of Canada (ROC)	36.7%	83.1%	39.9%	91.3%
Home Business				
Yes	38.2%	82.9%	41.1%	89.8%
No/ Don't Know	37.7%	82.9%	39.0%	92.1%
Years in Business				
4 years or less	34.8%	79.3%	34.1%	89.2%
5 to 10 years	40.8%	85.2%	43.0%	89.7%
10 years or more	38.0%	83.5%	41.1%	93.9%
Location				
City / suburb 100K or less	39.0%	84.1%	38.7%	90.8%
City/ town 30K-100K	44.5%	86.7%	47.6%	92.7%
Town/ rural area <30K	33.8%	80.5%	37.0%	91.8%
Revenues				
$0-$50K	28.0%	76.1%	36.3%	90.8%
$50-$250K	40.7%	84.5%	40.9%	90.9%
$250K or more	42.0%	86.1%	46.3%	96.2%
Type of Business				
Retail	35.9%	81.8%	32.7%	89.4%
Services	36.7%	82.2%	39.5%	91.3%
Goods	43.9%	86.4%	48.9%	94.4%
Technology Adoption				
Low (1 – 2)	23.1%	65.9%	21.0%	84.5%
Medium (3 – 4)	42.0%	89.3%	42.7%	92.8%
High (5 or more)	55.9%	95.1%	56.0%	96.3%

Results displayed in the table on the previous page show that, on average, 37.9% of technologies and systems used are currently 100% Y2K compliant. This figure increases slightly to 39.7% among critical technologies only.

Results also show that the proportion of technologies and systems used that will be ready by January 1st 2000 suggests a very high ramp-up of compliance activity among small businesses over the next seven months. Whereas businesses indicated that only 37.9% of all their technologies and systems are currently ready, they anticipate that 82.9% of their technologies and systems will be compliant by the Year 2000. Anticipated Y2K compliance is even higher for critical technologies where respondents indicated that approximately 91.5% of their critical technologies and systems will be ready for Y2K come January 1st.

The appearance of a high ramp-up of compliance activity could be linked to the above estimates of current 100% compliance. These estimates could be considered conservative since many businesses probably indicated that they have not taken steps towards ensuring Y2K compliance for certain technologies because they assume others are responsible. For instance, when asked if they had taken steps to ensure that their telecommunications systems are prepared for the Year 2000, many businesses indicated they had not, probably because they assumed their telephone company would ensure compliance. This should not mean that their telecommunications systems are not 100% ready. However, in the context of the above analysis, it was assumed that these systems are 0% ready because the respondent indicated they had not taken any steps. Such cases will consequently result in underestimation of current 100% compliance and create an artificially wide gap with anticipated 100% compliance.

Current 100% compliance is **highest** among:

- Businesses in Quebec,
- Businesses earning over $50K per year, and,
- Businesses with three or more technologies overall, especially those with five or more.

Current 100% compliance is **lowest** among:

- Businesses earning less that $50K per year, and,
- Businesses with less than three technologies overall.

TECHNOLOGY / SYSTEM TESTING

Another important step in ensuring Y2K compliance is testing. In the context of this research, testing was described as having someone input potential problem dates to make sure the systems will work with those dates. Respondents were asked it they tested each technology they own or use. However, if the respondent indicated not having taken any steps towards compliance for a given technology, testing for that technology was not asked.

For the purposes of this analysis, a business was considered to have tested their technology or system if they answered "yes" to at least one of their technologies or systems.

Results, as displayed below, show that approximately 45.0% of small businesses have tested at least one of their technologies or systems.

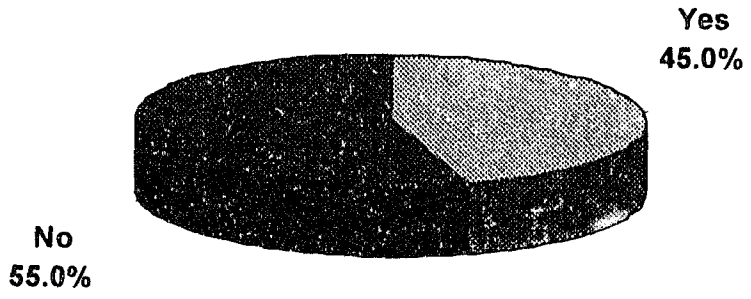

Figure 3: Has Tested At Least One Technology / System

Detailed sub-group results are presented below. Generally, results are quite consistent across the various sub-groups. Of note, businesses more likely to have tested at least one of their technologies or systems have been operating for 5 to 10 years, earn over $250K, and have at least three technologies (especially if they have five or more technologies). Businesses less likely to have tested their technologies or systems have been in operation for four years or less, earn less than $50K and own only one or two technologies.

	% That Have Tested
Overall	**45.0%**
Region	
Quebec	50.4%
Ontario	43.2%
Rest of Canada (ROC)	43.5%
Home Business	
Yes	40.6%
No/ Don't Know	46.7%
Years in Business	
4 years or less	39.7%
5 to 10 years	51.6%
10 years or more	44.5%
Location	
City / suburb 100K or less	46.7%
City/ town 30K-100K	48.1%
Town/ rural area <30K	42.3%
Revenues	
$0-$50K	29.5%
$50-$250K	49.2%
$250K or more	51.3%
Type of Business	
Retail	38.1%
Services	46.6%
Goods	49.6%
Technology Adoption	
Low (1 – 2)	17.0%
Medium (3 – 4)	52.2%
High (5 or more)	81.7%

Results specific to each technology and system are displayed in the table below:

	% That Have Tested			
	Overall*		Critical**	
	%	N	%	N
Custom-developed software	79.8%	94	82.9%	70
Industrial systems	75.0%	20	60.0%	10
Process control systems	73.9%	23	86.7%	15
Larger computing systems	73.1%	52	78.9%	562
Test/ lab/ diagnostic equipment	69.6%	23	76.9%	13
Off-the-shelf software applications	62.7%	233	61.7%	154
Stand-alone personal computers	61.3%	333	66.7%	192
Facility control systems	57.5%	73	63.4%	41
Telecommunications systems	46.5%	187	44.9%	127

***Base: Businesses that use the given technology or system and indicated having taken steps.**
****Base: Businesses that use the given technology or system, consider it critical and indicated having taken steps.**

Results show that nearly 80% of respondents that use custom-developed software and have taken steps towards ensuring its Y2K compliance have also tested it with potential problem dates. Testing was also quite common among businesses with industrial systems, process control systems and larger computing systems.

As has been the case in previous results, telecommunications systems and facility control systems make up the bottom ranks. Only 46.5% of respondents that use telecommunications systems and have taken steps towards ensuring their Y2K compliance have also tested them with potential problem dates. The equivalent statistic for facility control systems is 57.5%.

Additional analysis was conducted to determine the proportion of general and critical technologies that have been tested. The first column represents the total number of technologies that have been tested divided by the total number of technologies owned or used. The second column represents the total number of critical technologies that have been tested divided by the total number of critical technologies owned or used. Results are presented in the table on the following page.

Overall results show that slightly more than a quarter of all the technologies and systems owned or used by small businesses have been tested. This proportion increases slightly to 29.7% for critical technologies and systems. Results are generally consistent across sub-groups. However, important differences continue to arise across revenue brackets and the levels of technology adoption. There are also differences across types of business, especially for critical technologies.

	% of General Technologies That Have Been Tested	% of Critical Technologies That Have Been Tested
Overall	26.8%	29.7%
Region		
Quebec	33.0%	33.4%
Ontario	24.5%	26.6%
Rest of Canada (ROC)	25.2%	29.9%
Home Business		
Yes	24.2%	27.3%
No/ Don't Know	27.8%	30.7%
Years in Business		
4 years or less	24.4%	28.6%
5 to 10 years	30.7%	33.8%
10 years or more	26.2%	28.3%
Location		
City / suburb 100K or less	27.2%	28.0%
City/ town 30K-100K	29.5%	34.4%
Town/ rural area <30K	25.9%	30.0%
Revenues		
$0-$50K	17.3%	24.8%
$50-$250K	28.8%	29.6%
$250K or more	30.2%	34.8%
Type of Business		
Retail	22.9%	23.0%
Services	26.8%	30.2%
Goods	31.8%	36.7%
Technology Adoption		
Low (1 – 2)	1.0%	< 1%
Medium (3 – 4)	31.6%	32.7%
High (5 or more)	47.3%	47.4%

Respondents that indicated that they have taken steps towards compliance but have not tested their technologies or systems were asked whether any formal plans exist to test these technologies. Results for each technology and system are presented below. Generally, few respondents have established a formal plan to test their systems.

It is important to note the small sample sizes when interpreting these results.

	% That Plan on Testing			
	Overall*		Critical**	
	%	N	%	N
Test/ lab/ diagnostic equipment	85.7%	7	0.0%	3
Custom-developed software	57.9%	19	83.3%	12
Process control systems	33.3%	6	50.0%	2
Facility control systems	32.3%	31	33.3%	15
Larger computing systems	28.6%	14	37.5%	8
Stand-alone personal computers	27.9%	129	35.9%	64
Off-the-shelf software applications	24.1%	87	28.8%	59
Industrial systems	20.0%	5	50.0%	4
Telecommunications systems	15.0%	100	15.7%	70

***Base: Businesses that use the given technology or system and indicated having taken steps but no testing has been conducted yet.**

****Base: Businesses that use the given technology or system, consider it critical, indicated having taken steps but no testing has been conducted yet.**

SERVICE PROVIDERS AND SUPPLIERS

Important components of a comprehensive business Y2K compliance initiative are the identification and contact of critical service providers and suppliers. The study identified the incidence of critical suppliers and the proportion that have been contacted for Y2K compliance issues.

The table below shows that the suppliers most commonly considered critical are electrical, oil or gas companies, telecommunications service providers, financial institutions and transportation services. Although electrical companies are considered critical by over two-thirds of businesses, only 12.0% have contacted their supplier regarding Y2K compliance. The contact incidence is much higher among respondents that consider telecommunications service providers (24.3%) and financial institutions (36.3%) critical. Suppliers of production materials, machinery or equipment are also critical suppliers that were more likely to have been contacted (32.0%).

	% That Consider the Supplier Critical	% That Have Contacted Their Critical Supplier*
Electrical companies or oil and gas providers	69.5%	12.0%
Providers of telecommunications services such as telephone companies or dispatch systems	68.0%	24.3%
Financial institutions such as banks, trust companies, investment firms or insurance companies	55.2%	36.3%
Transportation services such as air, rail, water or road transport	53.7%	19.6%
Municipal utilities that provide water and sewage	48.0%	12.8%
Government agencies that provide regulatory and licensing services	25.3%	15.8%
Providers of emergency services such as police, fire department or ambulance agencies	21.8%	15.3%
Suppliers of production materials, machinery or equipment	20.8%	32.0%
Health care institutions such as hospitals, medical laboratories or any other health care institution	6.8%	22.0%

***Base: Businesses that considered the supplier critical (i.e. column 2 is the base for column 3)**

An overall incidence of businesses that have contacted at least one critical supplier was calculated. Results show that approximately 36.2% of small businesses have contacted at least one critical supplier. Furthermore, a proportion of critical suppliers contacted has been computed. Results below show that, on average, approximately one-fifth of critical suppliers used has been contacted. Results for both statistics are fairly consistent across sub-groups.

	% That Have Contacted At Least 1 Critical Supplier	% of Critical Suppliers Contacted
Overall	36.2%	20.7%
Region		
Quebec	34.0%	21.1%
Ontario	40.5%	22.1%
Rest of Canada (ROC)	33.3%	19.1%
Home Business		
Yes	34.9%	18.8%
No/ Don't Know	36.8%	21.5%
Years in Business		
4 years or le	35.3%	21.8%
5 to 10 years	40.5%	22.0%
10 years or more	34.7%	19.8%
Location		
City / suburb 100K or less	36.0%	21.4%
City/ town 30K-100K	34.9%	20.3%
Town/ rural area <30K	36.9%	19.6%
Revenues		
$0-$50K	27.1%	17.6%
$50-$250K	37.4%	20.5%
$250K or more	42.0%	23.6%
Type of Business		
Retail	38.7%	23.1%
Services	34.8%	18.9%
Goods	36.8%	22.5%
Technology Adoption		
Low (1 – 2)	29.7%	18.0%
Medium (3 – 4)	35.2%	20.0%
High (5 or more)	57.7%	30.7%

CUSTOMER CONTACT

Businesses were also asked whether they had contacted their customers to verify whether their Year 2000 preparedness will impact their organization. Overall, approximately 9.2% of small businesses indicated having contacted their customers and 2.1% did not know. The low incidence of customer contact can be attributable to the following factors:

- Small businesses do not believe their customers' Year 2000 preparedness will have an impact on their organization.
- Small businesses do not have enough customers to warrant worrying about the impact they will have on their organization.
- Small businesses are not aware that their customers' year 2000 preparedness could have an impact on their organization.

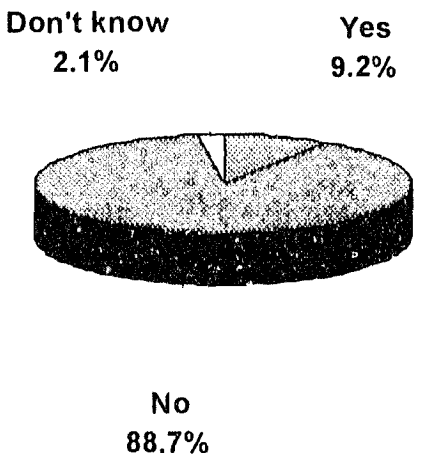

Figure 4: Has Contacted Their Customers

The incidence of customer contact has been calculated across the various sub-groups Results, as presented in the table below, show that incidence rates are very consistent across sub-groups

	% That have Contacted Customers
Overall	9.2%
Region	
Quebec	10.6%
Ontario	10.4%
Rest of Canada (ROC)	7.2%
Home Business	
Yes	12.0%
No/ Don't Know	8.0%
Years in Business	
4 years or less	5.9%
5 to 10 years	7.8%
10 years or more	11.4%
Location	
City / suburb 100K or less	9.9%
City/ town 30K-100K	6.6%
Town/ rural area <30K	10.0%
Revenues	
$0-$50K	5.4%
$50-$250K	11.4%
$250K or more	11.8%
Type of Business	
Retail	3.2%
Services	10.4%
Goods	13.7%
Technology Adoption	
Low (1 – 2)	6.0%
Medium (3 – 4)	10.1%
High (5 or more)	12.7%

CONTINGENCY PLANS

Many businesses are preparing contingency plans for January 1st 2000 in the eventuality that something unforeseen should occur The study asked small businesses if they have or will consider any of the following contingency plans

- Alternative processes such as paper or manual processes.
- Additional inventories of key components, materials or final products.
- Identification of alternative suppliers or service providers that have achieved Year 2000 compliance.
- Purchase of special equipment or products such as generators.
- Special staff arrangements for the period of change-over (e g holidays extended or cancelled, extra staff hired, etc).
- Plans to suspend any activities that are essential to the delivery of products or services to clients or to the public

Overall results show that nearly two out of every three small business (64 3%) has or will consider at least one of the contingency plans listed above

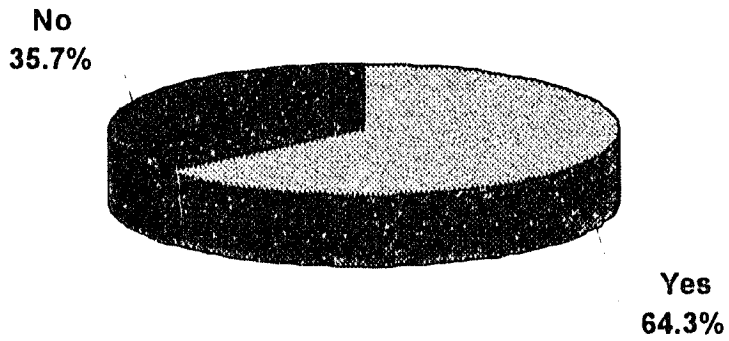

Figure 5: Has or Will Consider a Contingency Plan

Among the plans presented to respondents, the most common one considered was "alternative processes such as paper or manual processes" (50.8%). A distant second was "additional inventories of key components, materials or final products" (23.2%). The least popular options were "plans to suspend any activities that are essential to the delivery of products or services to clients or to the public" (9.5%).

	% [2]
Alternative processes such as paper or manual processes	**50.8%**
Additional inventories of key components, materials or final products	**23.2%**
Identification of alternative suppliers or service providers that have achieved Year 2000 compliance	**18.8%**
Purchase of special equipment or products such as generators	**14.2%**
Special staff arrangements for the period of change-over (e.g. holidays extended or cancelled, extra staff hired, etc.)	**10.0%**
Plans to suspend any activities that are essential to the delivery of products or services to clients or to the public	**9.5%**

[2] Results will not add to 100% because of multiple mentions. Respondents were to indicate "Yes" or "No" for each contingency plan – therefore it is possible for a business to have agreed to more than one contingency plan.

The general incidence of current or anticipated contingency plans across sub-groups is presented below. Generally, results are very consistent across the sub-groups. Businesses in Quebec and those with only one or two technologies were much less likely to consider a contingency plan whereas those with five or more technologies were much more likely.

	% That Will or Have Considered a Contingency Plan
Overall	**64.3%**
Region	
Quebec	**42.6%**
Ontario	**73.4%**
Rest of Canada (ROC)	**68.8%**
Home Business	
Yes	**65.1%**
No/ Don't Know	**63.9%**
Years in Business	
4 years or less	**66.2%**
5 to 10 years	**60.8%**
10 years or more	**64.9%**
Location	
City / suburb 100K or less	**65.3%**
City/ town 30K-100K	**59.4%**
Town/ rural area <30K	**66.4%**
Revenues	
$0-$50K	**62.8%**
$50-$250K	**65.0%**
$250K or more	**65.5%**
Type of Business	
Retail	**62.6%**
Services	**62.8%**
Goods	**70.9%**
Technology Adoption	
Low (1 – 2)	**54.4%**
Medium (3 – 4)	**66.0%**
High (5 or more)	**81.7%**

Appendix A

Survey Questionnaire

INTRODUCTION

HI1 Hello, my name is _____ and I am calling from Opinion Search on behalf of Industry Canada. We are conducting a national telephone survey on preparedness for the Year 2000. May I please speak to the individual responsible for the technology your organization uses?

IF RESPONDENT HESITATES, READ: "We are assessing for Industry Canada the potential risk of the Year 2000 issue to businesses across Canada. All of your answers will be kept strictly confidential, and will be used for statistical, research purposes only."

SAME PERSON	1	CONTINUE
DIFFERENT PERSON	2	ASK TO SPEAK TO HIM OR HER REDO INTRODUCTION
NOT HERE NOW	3	SCHEDULE CALLBACK
NO TIME NOW	4	SCHEDULE CALLBACK
REFUSAL	5	CONVERT OR TERMINATE

HI2 We are assessing the potential risk of the Year 2000 issue to businesses across Canada. The survey should take about 15 minutes. Would you mind answering some questions for us today?

NO TIME NOW	1	SCHEDULE CALLBACK
REFUSAL	2	CONVERT OR TERMINATE

SCR1 First, how many people are employed full-time by your organization?

PROBE FOR BEST ESTIMATE

_____	employees	
999	DON'T KNOW/ REFUSE	TERMINATE

IF SCR1>5, TERMINATE "We are looking to speak with businesses that have less than 6 full-time employees. Thank you for your time and we are sorry to have disturbed you."

TECHNOLOGY USED

Q1 Does your organization have any of the following types of systems or technologies

	Does your organization have any...	Yes	No	DK
A	Stand-alone personal computers?	1	2	9
B	Larger computing systems such as mainframes, mid-range computers, client servers or local area networks (**IF Q1A=1, INSERT** "other than stand-alone personal computers")?	1	2	9
C	Off-the-shelf software applications such as word processors, spreadsheets and database management software?	1	2	9
D	Custom-developed software designed specifically for your firm?	1	2	9
E	Industrial systems such as computerized thermostats, heat sensors and flow sensors?	1	2	9
F	Process control systems embedded in computerized plant machinery?	1	2	9
G	Test, laboratory or diagnostic equipment or medical devices?	1	2	9
H	Facility control systems such as security systems, elevators and building control?	1	2	9
I	Telecommunications systems such as cell phones, dispatch systems, pagers, telephones, fax machines or units switched through telecommunications networks?	1	2	9

IF "YES" TO ANY OF Q1A TO Q1H, GO TO Q2
IF "YES" TO Q1I ONLY, ASK Q1J

Q1J Does your organization own telecommunications equipment other than a basic wireline telephone?

Yes	1	CONTINUE
No/ Don't Know	2	TERMINATE

Q2. Now I will ask you whether any of the systems and technologies that your organization has are considered critical.

For the purposes of this survey, critical systems and technologies are those that are essential to the on-going delivery of products or services to clients or to the public or those that impact on the health and safety of your employees or the public.

CREATE F9 HOTKEY!

ASK FOR EACH SYSTEM/ TECHNOLOGY OWNED IN Q1

	Are any of the (INSERT FROM Q1) critical?	Yes	No	DK
A.	Stand-alone personal computers?	1	2	9
B.	Larger computing systems such as mainframes, mid-range computers, client servers or local area networks (**IF Q1A=1, INSERT**: "other than stand-alone personal computers")?	1	2	9
C.	Off-the-shelf software applications such as word processors, spreadsheets and database management software?	1	2	9
D.	Custom-developed software designed specifically for your firm?	1	2	9
E.	Industrial systems such as computerized thermostats, heat sensors and flow sensors?	1	2	9
F.	Process control systems embedded in computerized plant machinery?	1	2	9
G.	Test, laboratory or diagnostic equipment or medical devices?	1	2	9
H.	Facility control systems such as security systems, elevators and building control?	1	2	9
I.	Telecommunications systems such as cell phones, dispatch systems, pagers, telephones, fax machines or units switched through telecommunications networks?	1	2	9

Q3. Has your organization taken any steps to ensure that its (INSERT FROM Q1) are prepared for the Year 2000? **IF YES, ASK:** Are they 100% ready, if not what percent would you say is ready?

ASK FOR EACH SYSTEM/ TECHNOLOGY OWNED IN Q1

	Yes*	No	DK
A. Stand-alone personal computers?	____%	2	9
B. Larger computing systems?	____%	2	9
C. Off-the-shelf software applications?	____%	2	9
D. Custom-developed software designed specifically for your firm?	____%	2	9
E. Industrial systems?	____%	2	9
F. Process control systems?	____%	2	9
G. Test, laboratory or diagnostic equipment or medical de· ·es?	____%	2	9
H. Facility control systems?	____%	2	9
I. Telecommunications systems?	____%	2	9

***ENTER 999 IF DON'T KNOW**

IF "YES" TO ANY OF Q3A-I, GO TO Q5

Q4. Why has your organization not taken any steps towards preparing its systems and technology for the Year 2000?

DO NOT READ LIST – ACCEPT ALL THAT APPLY

Plan to look at it in near future	1
Systems are new, assume they will work properly	2
Won't be affected by Y2K	3
Don't know enough about the issue	4
Don't know how to prepare for Y2K	5
Can't afford to fix or prepare for Y2K	6
Not enough time to fix or prepare for Y2K	7
Other (Specify)	8
Don't Know	99

Q5. Do you expect that your organization's (INSERT FROM Q3) will be 100% Y2K compliant before January 1st 2000?

ASK FOR EACH SYSTEM/ TECHNOLOGY THAT IS NOT 100% PREPARED IN Q3 (i.e. Q3=2 or Q3=9 or (Q3=1 and <100%))

	Yes	No	DK
A. Stand-alone personal computers?	1	2	9
B. Larger computing systems?	1	2	9
C. Off-the-shelf software applications?	1	2	9
D. Custom-developed software designed specifically for your firm?	1	2	9
E. Industrial systems?	1	2	9
F. Process control systems?	1	2	9
G. Test, laboratory or diagnostic equipment or medical devices?	1	2	9
H. Facility control systems?	1	2	9
I. Telecommunications systems?	1	2	9

Q6. Has anyone tested your organization's systems and technologies? By testing, we mean having input potential problem dates to make sure the systems will work with those dates. So, has anyone tested your organization's (INSERT FROM Q3)?

ASK FOR EACH SYSTEM/ TECHNOLOGY FOR Q3=1

	Yes	No	DK
A. Stand-alone personal computers?	1	2	9
B. Larger computing systems?	1	2	9
C. Off-the-shelf software applications?	1	2	9
D. Custom-developed software designed specifically for your firm?	1	2	9
E. Industrial systems?	1	2	9
F. Process control systems?	1	2	9
G. Test, laboratory or diagnostic equipment or medical devices?	1	2	9
H. Facility control systems?	1	2	9
I. Telecommunications systems?	1	2	9

Q7. Are there any formal plans to test your organization's (INSERT FROM Q6)?

ASK FOR EACH SYSTEM/ TECHNOLOGY FOR Q6<>1

		Yes	No	DK
A.	Stand-alone personal computers?	1	2	9
B.	Larger computing systems?	1	2	9
C.	Off-the-shelf software applications?	1	2	9
D.	Custom-developed software designed specifically for your firm?	1	2	9
E.	Industrial systems?	1	2	9
F.	Process control systems?	1	2	9
G.	Test, laboratory or diagnostic equipment or medical devices?	1	2	9
H.	Facility control systems?	1	2	9
I.	Telecommunications systems?	1	2	9

SERVICE PROVIDERS AND SUPPLIERS

We will now address the suppliers that provide critical goods or services to your organization.

Repeat definition of CRITICAL if necessary! HIT F9

******ASK Q8A AND Q8B SEQUENTIALLY FOR EACH SERVICE BELOW!**

Q8A. Are critical supplies or services provided to your organization by any [INSERT FROM BELOW]?

Q8B. Has anyone from your organization contacted these [INSERT FROM BELOW FOR Q8A=1] to ensure that service and supplies will not be disrupted come the Year 2000?

****PROGRAMMER: For Q8a, provide entire text below and remove parentheses. For Q8b, delete what is between parentheses.**	**Yes**	**No**	**DK**
A. Transportation services (such as air, rail, water or road transport)?	1	2	9
B. Financial institutions (such as banks, trust companies, investment firms or insurance companies)?	1	2	9
C. Providers of telecommunications services (such as telephone companies or dispatch systems)?	1	2	9
D. Providers of emergency services (such as police, fire department or ambulance agencies)?	1	2	9
E. Government agencies that provide regulatory and licensing services?	1	2	9
F. Health care institutions (such as hospitals, medical laboratories or any other health care institution)?	1	2	9
G. Suppliers of production materials, machinery or equipment?	1	2	9
H. Municipal utilities that provide water and sewage?	1	2	9
I. Electrical companies or oil and gas providers?	1	2	9

CUSTOMERS

Q9. How about your organization's customers? Has anyone from your organization contacted its customers to verify whether their Year 2000 preparedness will impact your organization?

Yes	1
No	2
Don't Know	9

CONTINGENCY PLANS

Q10. Some organizations are preparing themselves for the Year 2000 by resorting to certain contingency measures that will allow them to continue operating even if problems occur. Please indicate which of the following contingency plans your company has or will consider:

RANDOMIZE		Yes	No	DK
A.	Alternative processes such as paper or manual processes?	1	2	9
B.	Additional inventories of key components, materials or final products?	1	2	9
C.	Purchase of special equipment or products such as generators?	1	2	9
D.	Identification of alternative suppliers or service providers that have achieved Year 2000 compliance?	1	2	9
E.	Plans to suspend any activities that are essential to the delivery of products or services to clients or to the public?	1	2	9
F.	Special staff arrangements for the period of change-over (e.g. holidays extended or cancelled, extra staff hired, etc.)?	1	2	9

FIRMOGRAPHICS

Just a few more questions for statistical classification purposes only

A Would you describe this company as being primarily operated outside of your home or from your home?

- ☐ Mainly operated outside of home
- ☐ Mainly operated inside of home as a home-based business
- ☐ Don't Know/ Refuse

B Which of the following best describes the area where your organization is located? READ LIST

- ☐ A city with a population of 100,000 or more
- ☐ A suburb of a city that has a population of 100,000 or more
- ☐ A city or town (or associated suburb) with a population between 30,000 to 99,999
- ☐ A town or village with a population of 10,000 to 29,999
- ☐ A rural town with a population of less than 10,000
- ☐ A rural area
- ☐ Don't Know/ Refuse

C How many years has your company been in business? READ LIST

- ☐ Less than one year
- ☐ From 1 to 4 years
- ☐ From 5 to 9 years
- ☐ From 10 to 14 years
- ☐ 15 or more years
- ☐ Don't Know/ Refuse

D Which of the following categories best describes your company's 1998 gross annual revenues? READ LIST

- ☐ Between 0 to $100,000
- ☐ $100,000 to $500,000
- ☐ $500,000 to $1 million
- ☐ $1 million to $5 million
- ☐ $5 million to 10 million
- ☐ Over $10 million
- ☐ Don't Know/ Refuse

THANK AND LOG COMPLETION