Project to Improve Provincial Economic Statistics

Data Security Task Force

Projet d'amélioration des statistiques économiques provinciales

Groupe de travail de la sécurité des données

Technical Series

Number 45

Série technique

Numéro 45

Internet: www.statcan.ca
Intranet: http://pipes

Statistics Canada Statistique Canada

Canada

Data Security Task Force

Ensuring confidentiality and the security of data is one of the highest priorities at Statistics Canada. The Business and Trade Statistics Data Security Task Force was created to look into data security issues in an attempt to ensure that the greatest efforts are being made to protect the confidentiality and security of all data throughout the statistical process. The following report contains the task force's recommendations related to issues such as authorization, processing, disposal and general good practices necessary to continue to ensure the confidentiality of sensitive data.

Note of appreciation

Canada owes the success of its statistical system to a long-standing partnership between Statistics Canada, the citizens of Canada, its businesses, governments and other institutions. Accurate and timely statistical information could not be produced without their continued cooperation and goodwill.

For further information on the materials covered in this paper, please contact Bonnie Bercik (613) 951-6790, Diane Proulx (613) 951-7192 or Robert McKenzie (613) 951-9991
Fax: (613) 951-0411

November 1999
Ottawa

Data Security Task Force

Mark Steski

In response to concerns related to the practices and procedures governing access to confidential micro data, the UESP Transition Advisory Committee (UTAC) created the Business and Trade Statistics Data Security Task Force. The task force's mandate was to establish principles and practices for the maintenance of security with respect to the extended Business and Trade Statistics Field's surveys, tax and other micro-data holdings. The task group was comprised of individuals representing a subset of divisions within the extended Business and Trade Statistics Field. In addition to representing their own division, each member was "twinned" with a division that did not have direct representation in the group. This ensured that the needs of the entire field were covered. The following table lists the membership along with the "twinned" division for each member.

Member	Division	Twinned Division
Mark Steski (chair)	Tax Data	
Gordon Baldwin	Services	Small Business and Special Surveys
Terry Evers	Business Register	Standards
Mel Jones	Manufacturing, Construction and Energy	Agriculture
Mark Marcogliese	Industrial Organization and Finance	Distributive Trades
Helen McDonald	Transportation	Investment and Capital Stocks
Stephen Moses	International Trade	Science and Technology Redesign Project
Bernie Theriault	Enterprise Statistics	Prices
Peter Demmons	Labour	

The group's first task was to develop a set of principles that would be used to guide the discussions on security practices. The second objective was to create a set of recommendations that would be reviewed by UTAC. Clearly, discussions on topics such as data security could incorporate and encompass a variety of issues and perspectives. However, due to the limited amount of time available for discussion and the desire to produce valid recommendations by the end of the year, the group concentrated its attention on improving current practices. For the purpose of this document, current practices have been broken down into the following sections: Authorization, Processing, Disposal, and Miscellaneous. This break down reflects the actual implementation policies concerning data security.

Finally, existing policies already cover the confidentiality and security aspects of sensitive statistical information. The work done by this group is an attempt to understand the implications of these policies and to suggest methods of making them more operational.

Principles

As mentioned above, the group's first objective was to create a set of guiding principles that would steer discussions on security issues. The entire group quickly agreed on a consensus, enumerating the guiding principles listed below. It is important to keep these principles in mind when reading the recommendations contained in this document.

The following are the principles outlined by the group.

1. The security practices will satisfy the requirements of the Statistics Act and the commitments to Revenue Canada as stated in the "Memorandum of Understanding" between the Department of National Revenue and Statistics Canada dated October 28, 1994.

2. Directors are responsible for determining, implementing, and communicating adequate data security practices for their respective division.

3. Security practices will not obstruct workflow and productivity.

4. Management has confidence and trusts its employees, however regular communication of security practices is essential.

5. The development of security practices is an on going, evolving process; not all problems are solvable at once.

6. Security practices will adopt modern approaches reflecting current technology.

7. Security practices will be as simple as possible, efficient and avoid unnecessary bureaucracy.

8. Access to all secure data will be on a need to know basis only.

9. Data security practices will be the same for all micro data regardless of the source.

Authorization for Internal Access to Data

Inter-divisional access to sensitive statistical data must be formally requested in writing at the director level according to Policy 4.7, "Security of Sensitive Statistical Information". A justifiable description of the uses to which the information is going to be put must accompany and support the request. Currently, the policy's implementation guidelines stipulate that a form clearly indicating the justification, description of uses, and director's signature must accompany each request for specific micro data.

Recommendations

1. The custodian divisions should create and maintain one formal agreement for each client division. This agreement would contain the justification, description of uses, and the complete list of micro data used to support the client division program. Access to micro data outside the scope of the agreement would require a separate justification and description of the uses of that specific data.

2. The task force has identified three possible scenarios with respect to client divisions wanting to identify individuals who should be granted access to micro data. A client division may identify individuals who have access to:

I. All the micro data required to support their divisional programs for a period of one year.

II. All the micro data required to support their divisional programs for a period less than one year.

III. Some of the micro data required to support their divisional programs for a period less than one year. This type of access would be useful for contracting resources.

3. Policy 4.7 contains an appendix that refers to the acquisition, custody, access and protection of taxation-derived micro data. This appendix should be integrated into the main body of the policy in order to reflect the principle that all micro data are treated equally with respect to security.

Processing

The following section covers the issues that deal with the actual processing of confidential data. This is the next logical step once an individual has access to the protected data.

Network A / Network B Switch

EDP Security Policy 4.5, clearly states that individuals processing confidential data on workstations equipped with disk drives are not allowed an A/B network switch. Informatics Security defines "processing" as reading, writing or updating confidential data. Given this definition, many employees in the field should not have the A/B network switch.

There was a great deal of discussion concerning this policy as it does hinder productivity for many employees. In the end however, despite the infringement on productivity, there was a consensus that the policy should be maintained. Please note that this restriction does not apply to those individuals using diskless workstations.

Copying

Policy 4.7 states that the director responsible for the control of sensitive statistical information must approve the copying of that particular information.

Recommendations

1. Allow copying of micro data to secure servers for operational reasons. The director overseeing the control of sensitive statistical information is responsible for determining if the server is secure. All secure servers would be subject to physical and logical security measures.

2. The custodian divisions should be responsible for creating and maintaining one formal agreement for each client division (as mentioned in the Authorization for Access section). The agreement should list the micro data files copied to support the client division program. The length of time the copied micro data files are to exist should also be stated. Copying micro data outside the scope of the agreement should be negotiated on a case by case basis.

The task force also discussed the issue of saving confidential data on personal workstations. This practice is not recommended as it violates data security policies. The following items illustrate why confidential data should never be saved on personal workstations:

- Workstation hard disks are rarely, if ever, backed up. Important work may be lost in the event of a hard disk crash.

- In the past, hard drives have been stolen from workstations within the Statistics Canada complex. In this scenario, confidential data stored on a stolen hard drive would be lost.

- Users can grant access to their hard drive to any employee in the bureau via the network. Consequently, employees may have unauthorized access to confidential data.

- The roaming profile used in the Business and Trade Statistics Field allows employees to log onto different machines within the field. Once logged onto a machine, the employee has access to that computer's hard drive. This example illustrates again how staff members may gain unauthorized access to confidential data.

- Whenever copies of data exist, there is a risk that the data becomes out of date or inconsistent with the data source. There is a potential for inconsistencies, for example, when copied data is modified and the corresponding changes are not made to the source data.

Email

Appendix "E" in the "Memorandum of Understanding" between the Department of National Revenue and Statistics Canada allows for the transmission of encrypted confidential data. The task group has determined that "transmission" refers to the actual electronic transmission of a stream of data on publicly accessible lines. Since Statistics Canada's email is internal only, and protected from the outside by a firewall, it does not constitute "transmission" as defined by the "Memorandum of Understanding". Therefore, there is a clear distinction between transmission of data, as defined by the "Memorandum of Understanding" and Statistics Canada internal email. This interpretation of "transmission" is supported by a threat-risk assessment study conducted on the corporate email infrastructure in 1995. This assessment found that sending confidential information on Network A did not exceed what was considered an acceptable level of risk. It should be noted however, that this assessment does not include the Network A to Network B email service, as it was not in place at that time.

It is worthwhile stating that the current practices in TAX and ESD do not allow transmittal of confidential data by email. This is explicitly stated in the "Data Access Form", signed by all client directors.

Given the current restrictions, members of the task force agreed that working effectively under these conditions is virtually impossible. Given this situation the task force recommends:

1. Permitting the use of email to send confidential information within Statistics Canada. However, this does not include sending complete micro data files via email.

2. Informing employees of the risk of unwittingly sending out confidential information to Network B email users.

3. That Informatics Technology Services Division conducts a threat-risk assessment on the email infrastructure taking into consideration the robotic A/B switch and the new email software.

4. Conducting a pilot study in co-operation with Informatics Technology Services Division using Public Key Infrastructure (PKI) to determine its potential for data security.

Printing

The issue of printing confidential data is not, in itself, contentious. The problem lies in the control of this printed confidential information. The "Memorandum of Understanding" dictates that all printed materiel be marked "Protected", locked in a cabinet when not in use, and shredded on disposal.

Recommendations

1. Directors should continue to be made responsible for the confidential data that is printed on divisional printers.

2. Divisions are to take reasonable measures to control access to printers.

3. Mainframe printouts of confidential data should continue to use the method described in the EDP Policy and on the Data Access Forms.

4. The task group also felt that controlled printers would not be required if the perimeter security of the premises was enhanced. The security methods used to control access to the Statistics Canada premises should incorporate a "swipe card" access plan. All Statistics Canada identification cards are equipped with a magnetic strip that could be used for this type of access. The task force is not implying that security guards be removed, but rather, that requirements enabling access to work areas be increased.

Off-Site Access

Policy 4.5 of the EDP Security Policy states that all confidential data is to be processed, stored and transmitted only on network A. The policy makes provisions for exceptions, exclusions and "special circumstances" such as field interviewers using portable microcomputers.

This policy is in line with the agreement on the data access forms. Therefore, there are no recommendations to make on this point.

Record Linkages

As we move towards integrated data across divisional boundaries, the opportunity for record linkages increases. Employees are reminded that there is a policy concerning record linkages.

Disposal

The "Memorandum of Understanding" between Statistics Canada and the Department of National Revenue clearly states that confidential information is to be properly disposed of.

Currently, LAN administrators and MCC operators remove all information from hardware devices that are to be discarded but the issue surrounding the disposal of confidential micro data on paper remains unresolved.

Recommendations

1. Each division should formulate an easy to use strategy for collecting, and disposing paper hardcopies of confidential micro data.

2. The contents of the containers that make up the "blue box" program should be shredded before the materiel leaves Statistics Canada buildings.

Miscellaneous

Audit

Periodically, Revenue Canada conducts audits on how Statistics Canada uses and protects confidential tax data.

Recommendations

1. Statistics Canada should conduct internal audits on data security practices every two years. The audit would determine if adequate security practices are in place and it would stimulate the exchange of new ideas on data security implementation between the two departments. These internal audits would act as input into the Revenue Canada audit process.

On Going Field Security Officers

Technology is having a profound impact on every aspect of the work carried out at Statistics Canada. Our working environment is constantly changing and evolving as technology challenges our organization to keep abreast of emerging developments. Ironically, as technology evolves it enables us to enhance data security while simultaneously providing tools that could potentially compromise the security of information as well.

Recommendation

1. Directors of the Business Register, Enterprise Statistics and Tax Data divisions should provide leadership in the field for on going discussions concerning data security issues as they evolve. As a group, they would communicate changes in data security policy, practices and technology to the employees of the field. They would also articulate evolving data security needs to the committees responsible for forming policies and practices.

Awareness

The task group feels the best way to ensure that employees adhere to valid and up to date security procedures is to communicate data security policies and practices to all staff members of the field on a regular basis.

Recommendations

1. Use the Intranet as a vehicle to communicate data security practices. The task force is not implying here that we simply reproduce or duplicate the policy manual, as it already exists on the Intranet.

Instead, the type of information communicated via the Intranet would be in the form of tips and/or reminders related to certain security practices. A reminder, for example, would be- visitors should be escorted at all times by their Statistics Canada sponsors. An example of a tip is- use password-protected screensavers to enhance security. These tips and/or reminders could take the form of pop up messages on the PIPES, TAX, BRD or ESD home pages.

2. Develop a one-page user-friendly summary of data security guidelines for accessing confidential data. Distribute the guidelines to all personnel who require access to confidential data.

3. Develop a lecture or workshop session on data security practices. Offer the lecture or workshop to those divisions requesting such a service, including the infrastructure divisions. The lecture or workshop should be added to the BEST course and SSDC programs, as well as to the new employee initiation program.

4. Make signs or stickers for the garbage cans and the recycling bins to remind staff of the proper disposal methods for confidential data.

5. Display signs or posters by network printers reminding employees to pick up their printed documents and to dispose of confidential printed materiel properly.

6. Display data security posters in the divisions as visible reminders to both statistics Canada employees and visitors of the importance of data security.

7. Encourage directors to use their divisional state of the union address to re-enforce the importance of data security.

8. Use Statistics Canada internal publications such as "SCAN" to promote data security practices, tips and reminders.

Best Practices

This section deals, in general terms, with voluntary practices that would enhance data security.

1. Store only Network B email addresses in the "Personal Address Book". This would separate internal and external email addresses, which in tum would reduce the risk of sending confidential data to an external email address.

2. When using email to send confidential micro data to internal Statistics Canada users, clearly state that the contents of the email are "Protected". Using the "confidential" message flag in Outlook could highlight the profile of confidential data. This would remind the recipient to take extra care when printing or forwarding the email. In addition, this precaution would act as a constant reminder to senders and recipients of the importance of data security.

3. Send a password-protected attachment in order to enhance data security when using email to send confidential micro data. Alternatively, send a "shortcut" to a document that is stored in a password protected shared folder. This would ensure that only those people having the password to the document or the folder could actually access the confidential micro data contents in the document.

4. When employees are away from the office they should be encouraged to use the "out of office" assistant as well as the "delegate" tools in Microsoft Outlook. The "delegate" tool allows an employee to identify a specific colleague to read his/her email, calendar, tasks, etc. The use of

these tools would avoid having to divulge passwords protecting secure data and would thereby enhance security.

5. Use password protected screensavers. This ensures that workstations are locked automatically at regular intervals and the contents of the screen are masked.

6. Lock the workstation whenever leaving for planned events, such as meetings or breaks. This also masks the contents of the screen. Pressing the Ctrl-Alt-Del keys simultaneously and selecting "lock workstation" enables an employee to lock his/her workstation.

7. Log off the workstation at night.

8. Pick up output from the printer as soon as it is printed.

9. Lock up confidential data printouts in a filing cabinet when not in use.

10. Always escort your sponsored visitors while they are at Statistics Canada. Escort them to the security desk when the visit is complete.

11. Wear ID badges in such a way that they are clearly visible.

Conclusion

The Business and Trade Statistics Data Security Task Force, in this report, has attempted to bring forth recommendations based on existing data security policies here at Statistics Canada. The group feels that existing policies contain the basis for maintaining effective confidentiality and protection of secure data. However, more needs to be done, through better communication for example, to ensure maximum protection at all levels of the statistical process. As well, the task force feels that directors need to continue to take on leadership roles in areas of policy and communication. Finally, continuing efforts to increase awareness and implement secure practices on an individual level will ensure that Statistics Canada can continue to deal with security issues resulting from technological and other changes that will affect us in the future.

Technical Series - Index

November 24, 1999

PIPES has a series of technical paper reprints primarily for internal purposes. A list of the reprints currently available is presented below. For copies, contact Bonnie Bercik at (613) 951-6790 or Diane Proulx at (613) 951-7192, fax number (613) 951-0411 or write to Statistics Canada, 13th Floor, Jean Talon Building, Tunney's Pasture, Ottawa, Ontario, K1A 0T6

1. Unified Enterprise Statistics Program – Project to Improve Provincial Economic Statistics – May 5, 1997 – PIPES Project Managers.

2. PIPES Evaluation Framework – September 15, 1997 – Philip Smith.

3. Report on the Unified Enterprise Survey & Reporting Arrangements Business Consultations – August 1997 – Guy Gellatly, Larry Murphy and Junior Smith.

4. Update on PIPES Progress: Notes for a Briefing for Federal and Provincial Finance Officials, Halifax, Nova Scotia, March 12, 1997 – Philip Smith.

5. An Overview of The Project to Improve Provincial Economic Statistics – November 1997 – George Beelen, Francine Hardy and Don Royce.

6. Using Databases to Design, Generate and Store Business Questionnaires at Statistics Canada – November 5, 1997 – Alana M. Boltwood.

7. The How and Why of Business Statistics – January 1999 – Elise Mennie. *(Not for external dissemination)*

8. An update on PIPES Fifteen Months into the Project – April 24, 1998 – Philip Smith.

9. Key Provider Manager (KPM) – 1997-98 Annual Report – May 1998 – Vicki Crompton.

10. A Framework for Planning Unified Enterprise Survey Data Collection – October 28, 1998 – Alana Boltwood.

11. Impact of the PIPES Funding on the Services Division Programme and Achievements in 1997-98 – April 1998 – Gordon Baldwin. *(Not for external dissemination)*

12. PIPES Organization and Decision-Making Structure – August 17, 1998 – Philip Smith. *(Not for external dissemination)*

13. The Central Goal of PIPES – November 17, 1997 – Philip Smith.

14. The Terminology and Framework of the Unified Enterprise Questionnaire – Revised March 1999 – Philip Smith.

15. Realizing and Measuring Quality Improvements in Provincial Economic Accounts – August 1998 – Philip Smith.

16. Annual Report 1997-98 – Ombudsman for Small Business Response Burden – July 1998, – Michael Issa. *(Not for external dissemination)*

17. Decision Making in PIPES – October 1, 1998 – Philip Smith.

18. Task Force on Electronic Data Reporting – April, 1998 – George Andrusiak, Monique Gaudreau, Laurie Hill, Anne Ladouceur, Denis Leblanc, Mario Ménard, Guy Parent, Joe Wilkinson, Doug Zinnicker.

19. PIPES Information Package – October 1998 – Philip Smith.

20. UES and the Non-Business Sectors – September 17, 1997 – Art Ridgeway.

21. CATS User Guide – April 1998 – Janet Howatson. *(Not for external dissemination)*

22. Report on Collection and Data Capture Operation OID for UES 1997 – September 3, 1998 – Anne Ladouceur. *(Not for external dissemination)*

23. SDD Contribution to PIPES 1998-1999 – September 1998 – Shirley Dolan.

24. The Harmonized Sales Tax Revenue Allocation Formula – August 1998 – Karen Hall. *(Not for external dissemination)*

25. Data Acquisition Strategy Report – July 22, 1998 – François Maranda and Don Royce.

26. Roles and Responsibilities in the Unified Enterprise Statistics Program – December 15, 1998 – George Andrusiak, Richard Barnabé, Albert Meguerditchian, Ray Ryan and Philip Smith. *(Not for external dissemination)*

27. Paper on the Project to Improve Provincial Economic Statistics from the Joint IASS/IAOS Conference – July 22, 1998 – Don Royce.

28. Respondent Relations Task Force – March 5, 1999 – Wayne Smith.

29. Response Analysis Follow-up Survey – March 1999 – Kristen Underwood.

30. Data Sharing Information Package – March 1999 – John Crysdale. *(Not for external dissemination)*

31. Coherence Analysis – Case Study from the Key Provider Manager Program – April 23, 1999 – Rachel Bernier and Julie Mandeville.

32. Evaluation of Collection Support Material used during the 1997 Unified Enterprise Survey – November 16, 1998 – Yvele Paquette.

33. Waiver Information Package – May 1999 – John Crysdale. *(Not for external dissemination)*

34. The PIPES Plan for 1999-00 – June 14, 1999 – Philip Smith. *(Not for external dissemination)*

35. BTS + Forum Post-conference Actions – April 1999 – Cornwall Conference Participants.

36. Report of the Task Force on Sources of Business Information – March 1999 – Vicki Crompton and Mark Marcogliese.

37. Field 5 Task Force Report on Improving Generic Boards – August 1999 – Mel Jones.

38. Study of Business Survey Questionnaires – June 1999 – Jason Gilmore.

39. Complexity Scale for Business Questionnaires – June 1999 – Jason Gilmore.

40. Update on PIPES- September 1999 – September 1999 – Philip Smith.

41. Exclusion Thresholds & Sampling Practices for Business Surveys – Implementation Strategy – September 1999 – Implementation Strategy Team.

42. Use of Tax Data in the Production of Provincial Economic Statistics – October 1999 – Peter Bissett.

43. Data Quality Survey 1996 – March 1999 – Ed Bunko. *(Not for external dissemination)*

44. Estimates of Information Cost to Business Respondents, 1998 – September 16,1999 – Linda Grant and Michael Issa. *(Not for external dissemination)*

45. Data Security Task Force – January, 1999 – Mark Steski. *(Not for external dissemination)*

Projet d'amélioration des statistiques économiques provinciales

Groupe de travail de la sécurité des données

Série technique

Numéro 45

Project to Improve Provincial Economic Statistics

Data Security Task Force

Technical Series

Number 45

Internet : www.statcan.ca
Intranet : http://pasep

Statistique Canada Statistics Canada

Canada

Groupe de travail de la sécurité des données

Une des principales priorités de Statistique Canada est d'assurer la confidentialité et la sécurité des données. Le Groupe de travail de la sécurité des données de la statistique du commerce et des entreprises a été mis sur pied pour examiner les questions de sécurité des données de façon que l'on s'efforce dans toute la mesure du possible de protéger la confidentialité et d'assurer la sécurité de l'ensemble des données relevant du processus statistique. On trouvera dans le rapport qui suit les recommandations du Groupe de travail relativement à des questions comme l'autorisation, le traitement, l'élimination et les bonnes pratiques générales nécessaires à la protection permanente de la confidentialité des données de nature délicate.

Note de reconnaissance

Le succès du système statistique du Canada repose sur un partenariat bien établi entre Statistique Canada et la population, les entreprises, les administrations canadiennes et les autres organismes. Sans cette collaboration et cette bonne volonté, il serait impossible de produire des statistiques précises et actuelles.

Pour plus de renseignements sur ce document, veuillez communiquer avec Bonnie Bercik (613) 951-6790, Diane Proulx (613) 951-7192 ou Robert McKenzie (613) 951-9991
Télécopieur : (613) 951-0411

Novembre 1999
Ottawa

Groupe de travail de la sécurité des données

Mark Steski

Donnant suite à des préoccupations liées aux pratiques et procédures régissant l'accès aux microdonnées confidentielles, le Comité consultatif sur la transition du PUSE (CCTP) a mis sur pied le Groupe de travail de la sécurité des données de la statistique du commerce et des entreprises. Ce groupe avait comme mandat d'établir les principes et pratiques assurant la sécurité des microdonnées d'enquête, fiscales et autres du secteur élargi de la statistique du commerce et des entreprises. Le Groupe de travail était constitué de personnes qui représentaient un sous-ensemble de divisions au sein du secteur élargi de la statistique du commerce et des entreprises. En plus de représenter sa propre division, chaque membre était « jumelé » à une division qui ne comptait pas de membre au sein du groupe. Ainsi, les besoins du secteur tout entier ont été considérés. La liste ci-dessous énumère les membres et les divisions « jumelées ».

Membre	Division	Division jumelée
Mark Steski (président)	Données fiscales	
Gordon Baldwin	Services	Petites entreprises et enquêtes spéciales
Terry Evers	Registre des entreprises	Normes
Mel Jones	Fabrication, construction et énergie	Agriculture
Mark Marcogliese	Organisation et finances de l'industrie	Statistique du commerce
Helen McDonald	Transports	Investissement et stocks de capital
Stephen Moses	Commerce international	Projet de remaniement des sciences et de la technologie
Bernie Theriault	Statistique des entreprises	Prix
Peter Demmons	Travail	

La première tâche du groupe a été de préparer une série de principes pouvant orienter les discussions sur les pratiques de sécurité. Le deuxième objectif était de formuler une série de recommandations que le CCTP pourrait examiner. Bien sûr, les échanges sur des sujets comme la sécurité des données pouvaient englober un choix de questions et de points de vue. Toutefois, compte tenu des contraintes de temps et puisqu'il s'agissait de présenter des recommandations valides avant la fin de l'année, le Groupe s'est penché sur l'amélioration des pratiques existantes. Aux fins du présent document, les pratiques existantes sont réparties en quatre catégories : autorisation, traitement, élimination et divers. Cette répartition reflète les politiques concrètes de mise en œuvre de la sécurité des données.

Enfin, les politiques mises en place abordent déjà la confidentialité et la sécurité des renseignements statistiques de nature délicate. Le Groupe de travail cherche à cerner les répercussions de ces politiques et à proposer des façons de les rendre plus opérationnelles.

Principes

Comme il a été mentionné ci-dessus, le premier objectif du Groupe a été de préparer une série de principes directeurs servant à orienter les discussions sur les questions de sécurité. Le Groupe tout entier a rapidement recueilli un consensus, établissant les principes directeurs énumérés ci-dessous. Il importe de garder ces principes à l'esprit en lisant les recommandations qui se trouvent dans le présent document.

Les principes établis par le Groupe sont énumérés ci-dessous.

1. Les pratiques de sécurité doivent satisfaire les dispositions de la *Loi sur la statistique* et les engagements pris vis-à-vis de Revenu Canada, énoncés dans le protocole d'entente qui a été conclu entre le ministère du Revenu national et Statistique Canada le 28 octobre 1994.

2. Les directeurs sont responsables de l'établissement, de la mise en œuvre et de la communication de pratiques de sécurité convenables dans leur division.

3. Les pratiques de sécurité ne doivent pas nuire au déroulement du travail ni à la productivité.

4. Malgré la confiance faite au personnel, il est essentiel de rappeler régulièrement les pratiques de sécurité.

5. L'établissement de pratiques de sécurité est un processus qui évolue; il n'est pas possible de résoudre tous les problèmes en même temps.

6. Les pratiques de sécurité doivent intégrer des stratégies modernes qui reflètent la technologie existante.

7. Les pratiques de sécurité doivent être aussi simples que possible et efficaces et éviter les démarches bureaucratiques inutiles.

8. L'accès aux données protégées se fonde sur le besoin de savoir uniquement.

9. Les pratiques de sécurité sont les mêmes pour toutes les microdonnées, peu importe la source.

Autorisation de l'accès interne aux données

L'accès interdivisionnaire à des renseignements statistiques de nature délicate doit faire l'objet d'une demande écrite officielle, au niveau du directeur, en conformité avec la politique 4.7 relative à la sécurité des renseignements statistiques de nature délicate. Une description justifiant l'utilisation prévue des renseignements doit accompagner et appuyer la demande. À l'heure actuelle, les lignes directrices régissant la mise en œuvre de la politique exigent que chaque demande d'accès à des microdonnées particulières soit accompagnée d'un formulaire indiquant la justification, décrivant les applications et portant la signature du directeur.

Recommandations

1. Les divisions gardiennes devraient établir une entente officielle pour chaque division cliente. Cette entente engloberait la justification, la description de l'utilisation des données et la liste complète des microdonnées appuyant le programme de la division cliente. L'accès à des microdonnées

dépassant le cadre de l'entente exigerait une justification distincte et une description de l'utilisation des données en question.

2. Le Groupe de travail a cerné trois scénarios se rapportant aux divisions clientes qui souhaitent identifier des personnes qui devraient avoir accès aux microdonnées. Une division cliente peut désigner des personnes qui ont accès à :

   I. toutes les microdonnées appuyant les programmes de la division pendant une période d'un an;

   II. toutes les microdonnées appuyant les programmes de la division pendant une période de moins d'un an;

   III. certaines microdonnées appuyant les programmes de la division pendant une période de moins d'un an (ce type d'accès serait utile pour la négociation de contrats).

3. La politique 4.7 comporte une annexe qui a trait aux procédures d'acquisition, de garde, d'accès et de protection des microdonnées tirées des déclarations d'impôt. Cette annexe devrait être intégrée au texte même de la politique en conformité avec le principe selon lequel toutes les microdonnées sont traitées de façon égale relativement à la sécurité.

Traitement

La section qui suit aborde les sujets qui se rapportent au traitement même des données confidentielles. Il s'agit de la prochaine étape logique, lorsque l'accès à des données protégées a été obtenu.

Commutation entre les réseaux A et B

La politique 4.5 relative à la sécurité informatique précise clairement que les personnes qui traitent des données confidentielles à un poste de travail muni d'unités de disque ne doivent pas avoir de commutateur A/B. En sécurité informatique, le « traitement » se définit comme la lecture, l'écriture ou la mise à jour des données confidentielles. Compte tenu de cette définition, de nombreux employés œuvrant dans le secteur ne devraient pas avoir de commutateur A/B.

Cette politique a fait l'objet d'une longue discussion car elle nuit à la productivité de certains employés. En fin de compte, toutefois, malgré l'atteinte portée à la productivité, il y a eu consensus que la politique devrait être conservée. À noter que cette restriction ne s'applique pas aux personnes travaillant à un poste de travail sans unité de disque.

Renseignements copiés

La politique 4.7 précise que c'est le directeur responsable du contrôle des renseignements statistiques de nature délicate qui accorde l'autorisation de copier cette information.

Recommandations

1. Permettre de copier des microdonnées dans des serveurs protégés pour des raisons opérationnelles. Le directeur chargé de contrôler les renseignements statistiques de nature délicate doit déterminer si le serveur est protégé. Des mesures de sécurité physiques et logiques s'appliqueraient à tous les serveurs protégés.

2. Les divisions gardiennes devraient être responsables de la création et du maintien d'une entente officielle pour chaque division cliente (comme il a été mentionné à la section sur l'autorisation de l'accès). L'entente devrait énumérer les fichiers de microdonnées copiés pour appuyer le programme de la division cliente. La durée de vie des fichiers de microdonnées copiés devrait également être précisée. La reproduction de microdonnées dépassant le cadre de l'enquête doit être négociée de façon ponctuelle.

Le Groupe de travail a également abordé la question de la sauvegarde de données confidentielles à un poste de travail personnel. Cette pratique n'est pas recommandée car elle enfreint la politique sur la sécurité des données. Les constatations ci-dessous indiquent pourquoi des données confidentielles ne devraient jamais être sauvegardées à un poste de travail personnel :

- Il est rare que le disque dur d'un poste de travail soit sauvegardé. Un travail important risque d'être perdu si le disque dur tombe en panne.

- Dans le passé, des unités de disque dur ont été volées de postes de travail du complexe de Statistique Canada. Dans une telle situation, des données confidentielles sauvegardées dans une unité de disque dur volée seraient perdues.

- Les utilisateurs peuvent accorder à tout employé de SC l'accès à leur unité de disque dur par l'entremise du réseau. Par conséquent, les employés peuvent avoir accès sans autorisation à des données confidentielles.

- Le profil itinérant utilisé dans le Secteur de la statistique du commerce et des entreprises permet à des employés d'entrer en communication avec différents appareils du secteur. Une fois la communication établie, l'employé a accès à l'unité de disque dur de l'ordinateur en question. Cet exemple illustre encore une fois comment les membres du personnel peuvent avoir accès sans autorisation à des données confidentielles.

- S'il existe une copie des données, les données risquent d'être périmées ou de ne pas correspondre à la source des données. Il y a possibilité d'un manque d'uniformité, par exemple, lorsque des données copiées sont modifiées et que les changements correspondants ne sont pas apportés aux données originales.

Courriel

L'annexe E du protocole d'entente conclu entre le ministère du Revenu national et Statistique Canada autorise la transmission de données confidentielles chiffrées. Le Groupe de travail a décidé que « transmission » signifie la transmission électronique d'un flux de données par des lignes accessibles au public. Puisque le courriel de Statistique Canada est strictement interne et puisqu'il est protégé de l'extérieur à l'aide d'une cloison pare-feu, il ne correspond pas à la « transmission » définie dans le protocole d'entente. Par conséquent, la transmission des données, selon la définition du protocole d'entente, se distingue nettement du courrier électronique interne de Statistique Canada. Cette interprétation du terme « transmission » est confirmée par une évaluation des menaces et des risques menée en 1995 sur l'infrastructure du courrier électronique du Bureau, indiquant que l'envoi de renseignements confidentiels sur le réseau A ne dépassait pas le cadre de ce que l'on considérait comme un risque acceptable. À noter, toutefois, que cette évaluation n'englobait pas le service de courrier électronique entre le réseau A et le réseau B, puisque ce service n'existait pas à l'époque.

Il importe de souligner que les pratiques en cours à la DDF et à la DSE n'autorisent pas la transmission de données confidentielles par courrier électronique. Cette pratique est énoncée explicitement dans le formulaire d'accès aux données, signé par tous les directeurs clients.

Compte tenu des restrictions actuelles, les membres du Groupe de travail ont jugé qu'il est pratiquement impossible dans un tel contexte de travailler de façon efficace. Par conséquent, le groupe de travail recommande :

1. Que le recours au courrier électronique soit autorisé pour l'envoi d'informations confidentielles au sein de Statistique Canada. Cette autorisation n'englobe pas l'envoi de fichiers complets de microdonnées par courrier électronique.

2. Que les employés soient informés du risque d'une transmission involontaire de renseignements confidentiels à des utilisateurs du courrier électronique du réseau B.

3. Que la Division des services de technologie informatique mène une évaluation des menaces et des risques relativement à l'infrastructure du courrier électronique, compte tenu du commutateur A/B robotique et du nouveau logiciel de courrier électronique.

4. Qu'une étude pilote soit menée en collaboration avec la Division des services de technologie informatique, à l'aide de l'infrastructure à clé publique (ICP), afin de déterminer son utilité pour la sécurité des données.

Impression

En soi l'impression de données confidentielles n'est pas une question épineuse. Le problème relève du contrôle de ces données confidentielles imprimées. Le protocole d'entente prévoit que tout document imprimé porte la mention « protégé », qu'il soit gardé sous clé dans un classeur lorsqu'il n'est pas utilisé et qu'il soit déchiqueté au moment de son élimination.

Recommandations

1. Les directeurs devraient continuer d'assumer la responsabilité des données confidentielles qui sont imprimées à l'aide d'imprimantes de leur division.

2. Les divisions doivent prendre des mesures raisonnables pour contrôler l'accès aux imprimantes.

3. Les sorties d'imprimante de l'ordinateur central comportant des données confidentielles devraient continuer de respecter les mesures décrites dans la politique relative à la sécurité informatique et dans les formulaires d'accès aux données.

4. Le Groupe de travail estime également que le contrôle des imprimantes ne serait pas nécessaire si l'on rehaussait la sécurité périphérique des locaux. Les mesures de sécurité servant à contrôler l'accès aux locaux de Statistique Canada devraient intégrer un plan d'accès à l'aide de « cartes à glissement ». Toutes les cartes d'identité de Statistique Canada portent une bande magnétique qui pourrait servir à ce genre d'accès. Le groupe de travail ne suggère pas que l'on élimine les agents de sécurité, mais bien que l'on renforce les modalités d'accès aux locaux de travail.

Accès à distance

La politique 4.5 relative à la sécurité informatique exige que toutes les données confidentielles soient traitées, stockées et transmises uniquement à l'aide du réseau A. La politique prévoit des exceptions, des exclusions et des « circonstances spéciales », par exemple le cas des intervieweurs régionaux qui utilisent des micro-ordinateurs portatifs.

Cette politique respecte l'entente pour ce qui est des formulaires d'accès aux données. Par conséquent, il n'y a aucune recommandation à formuler sur ce point.

Couplages d'enregistrements

À l'approche de l'intégration des données d'une division à l'autre, les possibilités de couplages d'enregistrements augmentent. Les employés doivent noter qu'il existe une politique relative aux couplages d'enregistrements.

Élimination

Le protocole d'entente conclu entre Statistique Canada et le ministère du Revenu national précise clairement que les renseignements confidentiels doivent être éliminés convenablement.

À l'heure actuelle, les administrateurs de réseau local et les opérateurs du CPO retirent tous les renseignements du matériel à éliminer, mais la question de l'élimination des microdonnées confidentielles sur papier n'a toujours pas été résolue.

Recommandations

1. Chaque division devrait établir une stratégie conviviale pour la collecte et l'élimination des copies sur papier de microdonnées confidentielles.

2. Le contenu des récipients qui relèvent du programme « boîte bleue » devrait être déchiqueté avant de quitter les locaux de Statistique Canada.

Divers

Vérification

Périodiquement, Revenu Canada mène des vérifications de l'utilisation et de la sécurité des données fiscales confidentielles à Statistique Canada.

Recommandation

1. Statistique Canada devrait mener une vérification interne, tous les deux ans, des pratiques liées à la sécurité des données. La vérification permettrait de déterminer si de bonnes pratiques de sécurité sont en place et elle favoriserait un échange d'idées nouvelles sur la sécurité des données au sein des deux organismes. Ces vérifications internes seraient intégrées au processus de vérification de Revenu Canada.

Agents de sécurité régionaux permanents

La technologie exerce une influence profonde sur tous les aspects du travail qui se fait à Statistique Canada. Notre milieu de travail évolue constamment comme suite aux démarches prises par le Bureau pour intégrer les progrès technologiques. Ironiquement, les changements technologiques nous

permettent de rehausser la sécurité des données tout en fournissant des outils qui pourraient compromettre la sécurité de l'information.

Recommandation

1. Les directeurs des divisions du Registre des entreprises, de la statistique des entreprises et des données fiscales devraient jouer un rôle de direction dans le secteur pour ce qui est des discussions sur la sécurité des données. Ensemble, ils communiqueraient les changements en matière de politique, de pratique et de technologie de la sécurité des données aux employés du secteur. Ils cemeraient également les besoins en matière de sécurité des données pour les comités responsables de la formulation des politiques et pratiques.

Sensibilisation

Le Groupe de travail estime que la meilleure façon de veiller à ce que les employés respectent les procédures de sécurité en vigueur est de rappeler périodiquement au personnel du secteur les politiques et pratiques en matière de sécurité des données.

Recommandations

1. Recours à Intranet comme moyen de communiquer les pratiques de sécurité des données. Le Groupe de travail ne propose aucunement un simple dédoublement du manuel des politiques, que l'on peut déjà consulter dans Intranet. Plutôt, il s'agirait de transmettre, par l'entremise d'Intranet, des conseils ou des rappels au sujet de certaines pratiques. Un exemple de rappel serait que l'on doit toujours accompagner les visiteurs à Statistique Canada. Un exemple de conseil serait le recours à un programme de protection d'écran protégé par mot de passe comme moyen de rehausser la sécurité. Ce genre de conseil ou de rappel pourrait se présenter sous forme de message-éclair dans les pages d'accueil du PASEP, de la DDF, de la DRE ou de la DSE.

2. Préparation d'un résumé convivial d'une page des lignes directrices régissant l'accès aux données confidentielles. Distribution des lignes directrices à tout le personnel qui doit avoir accès aux données confidentielles.

3. Préparation d'un exposé ou d'un atelier sur les pratiques en matière de sécurité des données. L'exposé ou l'atelier serait offert aux divisions qui demandent ce genre de service, y compris les divisions de l'infrastructure. L'exposé ou l'atelier devrait être ajouté comme module du PRISE ou du CBE, de même que du programme d'initiation des nouveaux employés.

4. Préparation de panneaux ou de collants pour les poubelles et les bacs de recyclage afin de rappeler au personnel les méthodes appropriées d'élimination des données confidentielles.

5. Mise en place de panneaux ou d'affiches, près des imprimantes du réseau, pour rappeler aux employés qu'il faut passer prendre les documents imprimés et utiliser la bonne façon d'éliminer les données confidentielles imprimées.

6. Mise en place, dans les divisions, d'affiches bien visibles afin de souligner l'importance de la sécurité des données tant pour le personnel de Statistique Canada que pour les visiteurs.

7. Appel lancé aux directeurs d'utiliser leur bilan divisionnaire comme moyen de souligner l'importance de la sécurité des données.

8. Recours aux publications internes de Statistique Canada, à Scan par exemple, pour faire connaître les pratiques en matière de sécurité des données et pour diffuser des conseils et rappels.

Meilleures pratiques

La présente section décrit de façon générale des pratiques volontaires qui favoriseraient la sécurité des données.

1. Ne sauvegardez que des adresses de courrier électronique du réseau B parmi les adresse personnelles. Vous pourrez ainsi séparer les adresses de courrier électronique interne des adresses de courrier électronique externe, et réduire le risque que des données confidentielles soient transmises à une adresse de courrier électronique externe.

2. Expliquez bien clairement, lorsque vous envoyez des microdonnées confidentielles par courrier électronique à des utilisateurs internes de Statistique Canada, que le contenu est « protégé ». L'utilisation de l'indicateur de message « confidentiel » sous Outlook permettrait de souligner la présence de données confidentielles. Le récipiendaire saurait ainsi qu'il faut faire preuve de prudence lors de l'impression ou de l'envoi du courrier électronique. De plus, ce serait un moyen pour l'expéditeur et le récipiendaire de garder constamment à l'esprit l'importance de la sécurité des données.

3. Envoyez une pièce jointe protégée par mot de passe afin de rehausser la sécurité des données lors de l'envoi de microdonnées confidentielles par courrier électronique. Une autre façon de procéder est d'envoyer un « shortcut » à un document conservé dans un dossier partagé qui est protégé par mot de passe. Ainsi, seules les personnes ayant le mot de passe du document ou du dossier auront accès aux microdonnées confidentielles qui se trouvent dans le document.

4. Lorsque les employés quittent le bureau, on devrait les encourager à utiliser la fonction « out of office » de même que l'outil « delegate » sous Outlook (Microsoft). L'outil « delegate » permet à un employé de désigner un collègue particulier qui puisse lire son courrier électronique, son calendrier, ses tâches et ainsi de suite. Le recours à ces stratégies éviterait la divulgation du mot de passe qui protège les données et servirait donc à rehausser la sécurité.

5. Utilisez des économiseurs d'écran protégés par mot de passe. Ainsi, après un certain temps, le poste de travail sera verrouillé et le contenu de l'écran sera masqué.

6. Lorsque vous quittez un poste de travail (réunion, pause, etc.), verrouillez-le. Même le contenu de l'écran sera masqué. Le fait d'appuyer en même temps sur les touches Ctrl-Alt-Del et de choisir l'option « lock workstation » permet de verrouiller le poste de travail.

7. Effectuez une fin de session avant de quitter un poste de travail jusqu'au lendemain.

8. Allez chercher votre sortie d'imprimante le plus tôt possible.

9. Placez les données confidentielles sous clé dans un classeur lorsqu'elles ne servent pas.

10. Accompagnez vos visiteurs parrainés en tout temps dans les locaux de Statistique Canada, et jusqu'au comptoir de sécurité à la fin de la visite.

11. Portez votre insigne d'identité bien visiblement.

Conclusion

Dans le présent rapport, le Groupe de travail de la sécurité des données de la statistique du commerce et des entreprises formule des recommandations qui se fondent sur les politiques actuelles de Statistique Canada en matière de sécurité des données. Le groupe estime que les politiques en vigueur contiennent les éléments nécessaires au maintien de la confidentialité et à la protection des données. Toutefois, il faut aller de l'avant, grâce à de meilleures communications, par exemple, afin d'assurer un maximum de protection à tous les niveaux du processus statistique. De plus, le Groupe de travail estime que les directeurs doivent continuer de jouer un rôle de direction pour ce qui est des politiques et des communications. Enfin, c'est grâce à une sensibilisation accrue et à la mise en œuvre de pratiques de sécurité à un niveau individuel que Statistique Canada pourra continuer d'aborder les questions de sécurité soulevées par les changements technologiques et autres qui surviendront à l'avenir.

Série technique - Index

24 novembre, 1999

Dans le cadre du PASEP, on a réimprimé une série de documents techniques, principalement pour usage interne. Voici la liste des réimpressions disponibles. Pour obtenir des copies communiquez avec Bonnie Bercik au (613) 951-6790 ou Diane Proulx au (613) 951-7192, numéro de télécopieur (613) 951-0411 ou écrire à Statistique Canada, 13^{e} étage, Immeuble Jean Talon, Parc Tunney, Ottawa, Ontario, K1A 0T6

1. Programme unifié des statistiques sur les entreprises – Projet d'amélioration des statistiques économiques provinciales – le 5 mai 1997 – Programme de Gestionnaire du PASEP.

2. Cadre d'évaluation du PASEP – le 15 septembre 1997 – Philip Smith.

3. Rapport de l'Enquête unifiée sur les entreprises et les modalités de déclaration – Consultations auprès des entreprises – août 1997 – Guy Gellatly, Larry Murphy et Junior Smith.

4. Bilan de l'évolution du PASEP : Notes d'une séance d'information à l'intention des représentants fédéral et provinciaux des finances, qui a eu lieu à Halifax (Nouvelle-Écosse), le 12 mars 1997 – Philip Smith.

5. Aperçu du Projet d'amélioration des statistiques économiques provinciales – novembre 1997 – George Beelen, Francine Hardy et Don Royce.

6. Des bases de données pour la conception, la génération et le stockage des questionnaires-entreprises à Statistique Canada – le 5 novembre 1997 – Alana M. Boltwood.

7. La statistique des entreprises : sa raison d'être – janvier 1999 – Elise Mennie. *(Diffusion interne seulement)*

8. Bilan du PASEP 15 mois après son lancement – le 24 avril 1998 – Philip Smith.

9. Programme des gestionnaires des répondants clés (GRC) – Rapport annuel pour 1997-1998 – mai 1998 – Vicki Crompton.

10. Un cadre de planification de la collecte des données de l'Enquête unifiée sur les entreprises – le 28 octobre 1998 – Alana Boltwood.

11. Répercussions du financement du PASEP sur le programme et les réalisations de la Division des services en 1997-1998 – avril 1998 – Gordon Baldwin. *(Diffusion interne seulement)*

12. L'organisation et la structure décisionnelle du PASEP – le 17 août 1998 – Philip Smith. *(Diffusion interne seulement)*

13. Les buts principaux du PASEP – le 17 novembre 1997 – Philip Smith.

14. Terminologie et cadre de référence du questionnaire de l'Enquête unifiée sur les entreprises – Révisé en mars 1999 – Philip Smith.

15. Amélioration de la qualité des statistiques économiques provinciales et mesure des changements apportés – août 1998 – Philip Smith.

16. Rapport annuel 1997-1998 – Médiateur – Fardeau de réponse de la petite entreprise – juillet 1998 – Michael Issa. *(Diffusion interne seulement)*

17. Le processus décisionnel du PASEP le 1er octobre 1998 – Philip Smith.

18. Groupe de travail sur la déclaration électronique des données (DED) – avril 1998 – George Andrusiak, Monique Gaudreau, Laurie Hill, Anne Ladouceur, Denis Leblanc, Mario Ménard, Guy Parent, Joe Wilkinson, Doug Zinnicker.

19. Trousse d'information sur le PASEP – octobre 1998 – Philip Smith.

20. L'EUE et les secteurs non commerciaux – le 17 septembre 1997 – Art Ridgeway.

21. Le guide de l'utilisateur du SASC – avril 1998 – Janet Howatson. *(Diffusion interne seulement)*

22. Compte rendu de la collecte et la saisie de données DOI pour l'EUE de 1997 – le 3 septembre 1998 – Anne Ladouceur. *(Diffusion interne seulement)*

23. Contribution prévue de la DDS au PASEP, 1998-1999 – septembre 1998 – Shirley Dolan.

24. La formule de répartition des recettes de la taxe de vente harmonisée – août 1998 – Karen Hall. *(Diffusion interne seulement)*

25. Groupe de travail sur l'acquisition des données auprès des entreprises – le 22 juillet 1998 – François Maranda et Don Royce.

26. Rôles et responsabilités dans le cadre du Programme unifié des statistiques sur les entreprises – le 15 décembre 1998 – George Andrusiak, Richard Barnabé, Albert Meguerditchian, Ray Ryan et Philip Smith. *(Diffusion interne seulement)*

27. Document sur le Projet d'amélioration des statistiques économiques Provinciales de la conférence mixte de l'AISE/AISO – le 22 juillet 1998 – Don Royce.

28. Groupe de travail sur les relations avec les répondants – le 5 mars 1999 – Wayne Smith.

29. Enquête de suivi et d'analyse des réponses – mars 1999 – Kristen Underwood.

30. Dossier d'information sur le partage des données – mars 1999 – John Crysdale. *(Diffusion interne seulement)*

31. Analyse de cohérence – Étude de cas du programme des Gestionnaires des répondants clés – le 23 avril 1999 – Rachel Bernier et Julie Mandeville.

32. Évaluation des documents de soutien de la collecte utilisés durant l'Enquête unifiée sur les entreprises de 1997 – le 16 novembre 1998 – Yvele Paquette.

33. Trousse d'information sur les renonciations – mai 1999 – John Crysdale. *(Diffusion interne seulement)*

34. Plan du PASEP pour 1999-2000 – le 14 juin 1999 – Philip Smith. *(Diffusion interne seulement)*

35. Forum SCE + Mesures de suivi de la conférence – avril 1999 – Participants de la conférence de Cornwall.

36. Rapport du groupe d'étude des sources d'information sur les entreprises – mars 1999 – Vicki Crompton et Mark Marcogliese.

37. Rapport du Groupe de travail du secteur 5 sur l'amélioration de la dotation générique – août 1999 – Mel Jones.

38. Étude des questionnaires des enquêtes auprès des entreprises – juin 1999 – Jason Gilmore.

39. Échelle de complexité des questionnaires sur les entreprises – juin 1999 – Jason Gilmore.

40. Rapport sur l'avancement du PASEP- septembre 1999 – septembre 1999 – Philip Smith.

41. Seuils d'exclusion et méthodes particulières d'échantillonnage pour les enquêtes-entreprises – Stratégie de mise en oeuvre – septembre 1999 – L'Équipe de la stratégie de la mise en oeuvre.

42. Utilisation des données fiscales pour la production des statistiques économiques provinciales – octobre 1999 – Peter Bissett.

43. Enquête sur la qualité des données de 1996 – mars 1999 – Ed Bunko. *(Diffusion interne seulement)*

44. Estimations des coûts d'information pour les entreprises répondantes, 1998 – le 16 septembre 1999 – Linda Grant et Michael Issa. *(Diffusion interne seulement)*

45. Groupe de travail de la sécurité des données – janvier 1999 – Mark Steski. *(Diffusion interne seulement)*