Tip #3

ENSURING ANONYMITY IN YOUR EMPLOYEE SURVEY

One of the primary reasons for lower participation in an employee survey is employees' fear that their responses are not really anonymous – that whatever they say can come back to hurt them. If employees do not trust the survey process, you will have a difficult time fostering enthusiasm or securing participation. Following are some best practices to help reassure employees.

Don't promise confidentiality if you really mean anonymity.

Rule #1

Know the difference between anonymity and confidentiality. Many people use these terms interchangeably, but they are very different. For most surveys, you may not want to promise confidentiality – but you absolutely have to guarantee anonymity.

Anonymity means survey responses will not be tied back to individuals, i.e., no one will know "who said what." This is an absolute necessity for employee surveys.

Confidentiality means aggregated responses will be seen only by relevant parties, typically departments or divisions. For example, IT people see only IT results; they cannot access Finance results. However, in many organizations, data are shared in some fashion; often certain groups and/or individuals (e.g., executive leaders, HR) have access to all results. So it is important to define "confidentiality" for your organization. Don't promise confidentiality if you really mean anonymity.

Communicate!

Thoroughly communicate the purpose of the survey, how data will be gathered (especially important if you are doing your own data collection), and how the results are to be used. Explain your definitions of confidentiality and anonymity. Reiterate the information as often as necessary. In most organizations, the "grapevine" moves quickly to fill in the blanks when information is absent. You must pre-empt possible rumors with facts.

- Put the details in writing and post them on your intranet or on bulletin boards; send them in individual emails or memos.
- Make sure managers understand and can explain your procedures.
- Have a "hot line" available for questions and concerns – manned by an external source, if necessary.

Fears will be higher if you are using the Internet for your survey. Most people believe that any action done via web can be traced back to an individual. Your survey vendor should have security policies which you can then communicate to your employees (e.g., surveys are hosted on the vendor's website, not yours, and no one from your company has access to it). If you are doing your own electronic data collection, you will need to develop your own policies and communicate them to employees.

Explain coding procedures

There are obvious reasons why it is necessary to code (or categorize) survey data. If you can't tell where someone works, you can't

QUESTAR

The problem arises when it is not necessary for the individual to tell you where he or she works because you already know.

provide meaningful, localized information to enable action. If you are asking for this information on the survey itself, you can explain why these questions are necessary and make them optional.

The problem arises when it is not necessary for the individual to tell you where he or she works <u>because you already know</u>. This is of particular concern with online surveying.

With Internet surveys, the individual passcodes that employees use to access the survey are often tied to an HRIS database. You not only know where someone works, but you also have all of the demographic information contained in the file – you know who they report to, their job, how long they've been with the company, their gender, etc. In many cases, no demographic questions need to appear on the survey itself.

To alleviate potential concerns, many organizations use third-party vendors to administer surveys. If the file linking passcodes and HRIS information is kept by the vendor – inaccessible to anyone in the client organization – anonymity is preserved.

Whether you administer internally or use an external third-party, if you use passcodes to link to a database as a means of collecting demographic information, be sure to explain what you are doing and why. If an employee sees a report broken out by tenure – and knows that question was not asked on the survey – the credibility of any anonymity promise will suffer.

Limit personal demographics

Minimize the number of personal demographic questions on the survey. These are the questions that are most threatening to employees. It is easy to explain why you want to know department or division. It is more difficult to explain why you need to know gender, age, ethnicity or other personal data. If you are the only Hispanic female manager over 40 in your division, it's pretty obvious that you can be identified.

- Make sure that you have a compelling reason beyond just curiosity for asking such questions. Are you willing to take action on what you learn, e.g., if women are more negative than men about advancement, will you initiate programs aimed specifically at them?
- If you are asking these questions as a means of updating your HR database, be aware that employees have been known to deliberately enter false information because of anonymity concerns. One company had over 8% of responding employees check the first category on the alphabetical "ethnicity" list, which was American Indian/Alaskan Natives – a result the company knew was false.

If you do want to ask personal demographics, tell people why you need them and what you plan to do with them. Offer a "Do not wish to say" option to increase comfort levels. And be sure to get your legal department's approval. Employee survey data has been subpoenaed in some class action suits to illustrate work environments.

Be careful with paper

Some feel that paper surveys are less likely to generate concerns about anonymity. That is not necessarily so. Take the issue of **pre-coding**. We have seen cases where employees have blacked out or cut out simple form numbers, thinking they were some sort of individual tracking number. If you pre-code your paper surveys, be prepared for some codes being unreadable, making the return impossible to categorize.

QUESTAR

On-site sessions (i.e., bringing in groups to take the survey together) are popular because they often result in high response rates. However, they also pose some anonymity concerns. Some options:

- Invite people randomly or alphabetically; do not bring in whole departments together. That way no one feels forced to participate and absences are not readily noticed.
- Don't track participation using "sign-in" sheets or name check-offs.
- Have a large enough space so employees don't feel crowded or need to worry about others seeing their responses.
- Make use of third-party facilitators if you can.
- Ask your facilitators not to wander about the room.

If you want to use **on-site sessions and still use pre-coded surveys**, your options are few. You can put the surveys into envelopes with individual names on them to ensure the right survey gets to the right person. This can be difficult logistically; it can also fuel fears about anonymity – if my name is on the envelope, it's easy for me to believe the code on the survey identifies me.

A better method is to bring departments in together and explain that the code identifies the department, not the individual. Encourage people to exchange surveys to reinforce the message that it doesn't matter which person completes which survey.

With on-site surveys, you must have strict rules about what happens with completed surveys. Even the appearance of unauthorized access can cause problems. In one organization, a manager was seen in a conference room thumbing through what looked like a stack of surveys. Rumors spread and participation plummeted. What the manager had actually been doing was counting a stack of blank surveys to see if there were enough for the next session – but the damage was done.

That situation could have been avoided if the company had used a secure "lock box" (a simple box that is taped shut on all sides with a slit in the top). Have employees put their completed surveys into envelopes and drop them into the box through the slit. Do not leave the box unattended. At the end of administration, seal the top and mail the box to your survey vendor.

For individually mailed surveys, use pre-paid envelopes that go directly to the survey vendor, or use centrally located "drop-off" boxes which can then be bulk shipped at the end of administration.

Have a minimum N

With employee surveys, it is important to **generate results only for groups** – and there should be a minimum number of surveys returned in any one group before results can be reported. This number is referred to as the "minimum N," and it will vary according to the size and needs of the organization. The standard is usually between 5-10 respondents, though some organizations have gone as high as requiring 20. Questar recommends a minimum N of no fewer than five. Minimum Ns for comment reports are often higher because of the ease of identifying people through their writing.

Make sure your rules for protecting anonymity are enforced. Do not make exceptions. If you have publically stated that there must be a minimum number of five respondents in a group to generate data, do not break the rules for a senior manager with only four direct reports.

QUESTAR