



Volume 6, Issue 1 – January 28, 2014

## Considering data security risks

- **Data is a valuable agency asset that must be adequately protected.**
- **Data security risks can come both from outside the organization as well as from the inside.**
- **It is important to consider all risks, including data security risks, when doing risk assessments**

Time and time again, we hear about data breaches or data misuse. Recently, Target Corporation reported that hackers had broken into their checkout reader system and stolen credit and debit card numbers, mailing addresses, and phone numbers from over 70 million accounts. In a February 2013 program evaluation report, the Minnesota Legislative Auditor stated that, of 11,000 law enforcement personnel who had accessed driver and vehicle services (i.e. driver's license) data in fiscal year 2012, at least 88 had misused the data. These two stories point out that data security risks are significant and can come both from outside the organization, as well as from the inside.

What is behind all of this data leakage? Part of the trend is clearly caused by current technology. In the not-too-distant past, government data consisted predominantly of structured, paper forms and documents. Because this data was in physical form, it was easier to protect or lock up. However, now there is a continuous stream of digital data, including database files, email, electronic documents and spreadsheets. All of these technology advances allow quick access to the data you need, but also provide a much heightened risk of inappropriate access and use.

When performing risk assessments on key business processes, it is important to remember that, for many agencies, data is a valuable asset. As a result, when considering risks, make sure you also include in your brain-storming financial and reputational risks related to data.

Some potential questions to ask regarding data security are the following:

- What data do we collect and retain in this business process?
- Is it necessary to collect and retain the data? Is there some other way to achieve the program objectives without retaining the data, especially if it is classified not public?

- How is the data stored? Who has access to the data, especially if it is classified not public?
- Are employees familiar with the provisions of Minnesota Statute Chapter 13, regarding data practices? Does your agency have a data inventory pursuant to Minnesota Statute Section 13.025, Subdivision 1?
- Do employees know what data can be shared? Is not public data encrypted if sent electronically to parties outside the state?
- Do employees know and comply with all applicable statewide data policies, including MnIT Services standards on portable computing, electronic mail, physical security, and data destruction?

When performing risk assessments, it is important to consider all program risks, including risks of data security. There are several statewide policies and procedures that can help agencies develop and maintain strong internal controls over data.

*Suggested action steps:* Do you have a good understanding of what data your agency collects, where it is stored, and how it is protected? Are your agency employees adequately trained on data practices and data security? Make sure you consider data security risks as part of your agency business process risk assessments.

If you have questions, please contact Jeanine Kuwik at [Jeanine.Kuwik@state.mn.us](mailto:Jeanine.Kuwik@state.mn.us) or (651) 201-8148