
# You've been breached: Now What?

# Minnesota's Data Breach Preparation and Notification for Electronic Data

Enterprise IT Management Initiative
State of Minnesota
Jenna Covey, jenna.covey@state.mn.us, 651-201-1199
Project start: September 2014; Project end: November 2015

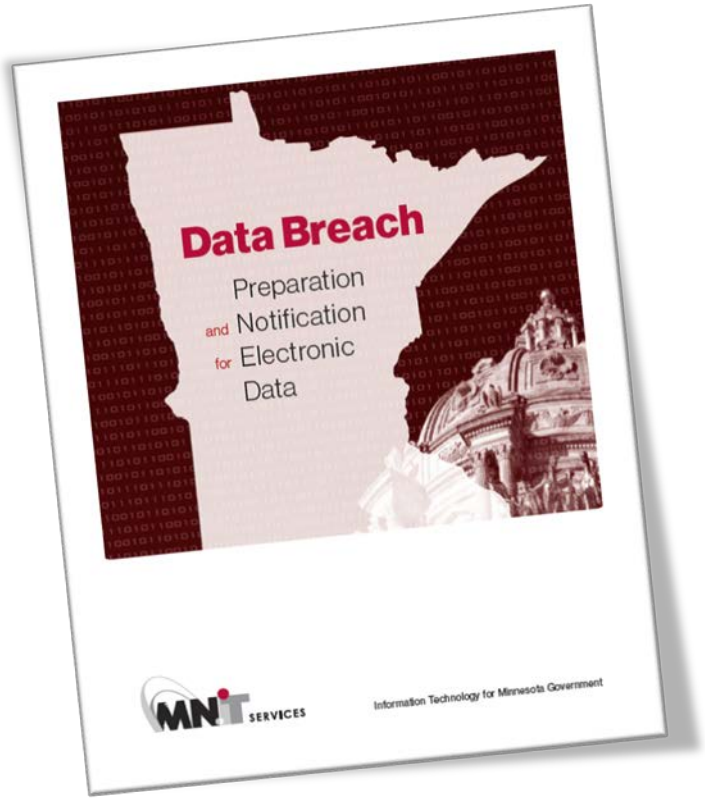
# Executive Summary

Electronic data breaches are not a matter of "if," but "when." Discovering a breach can create chaos for a state agency because of the numerous things to consider during these types of incidents. MN.IT Services saw an opportunity to help agencies prepare for a data breach and to better understand the role of the agency and MN.IT during a data breach.

As a result, MN.IT created a Breach Response and Notification manual. This manual is a vital tool that can be used both to prevent breaches and to ensure preparedness in case of a data breach. It is aimed at encouraging agencies to voluntarily put in place a Data Breach Preparation and Notification Plan.

The guide emphasizes preplanning. Being in the midst of a data breach is not the time to be deciding which resources you need in the room to guide you through the process, or looking up the numbers for those you need to contact. The manual provides step-by-step instructions of tasks that should be accomplished to preserve evidence, gather information and communicate about the incident.

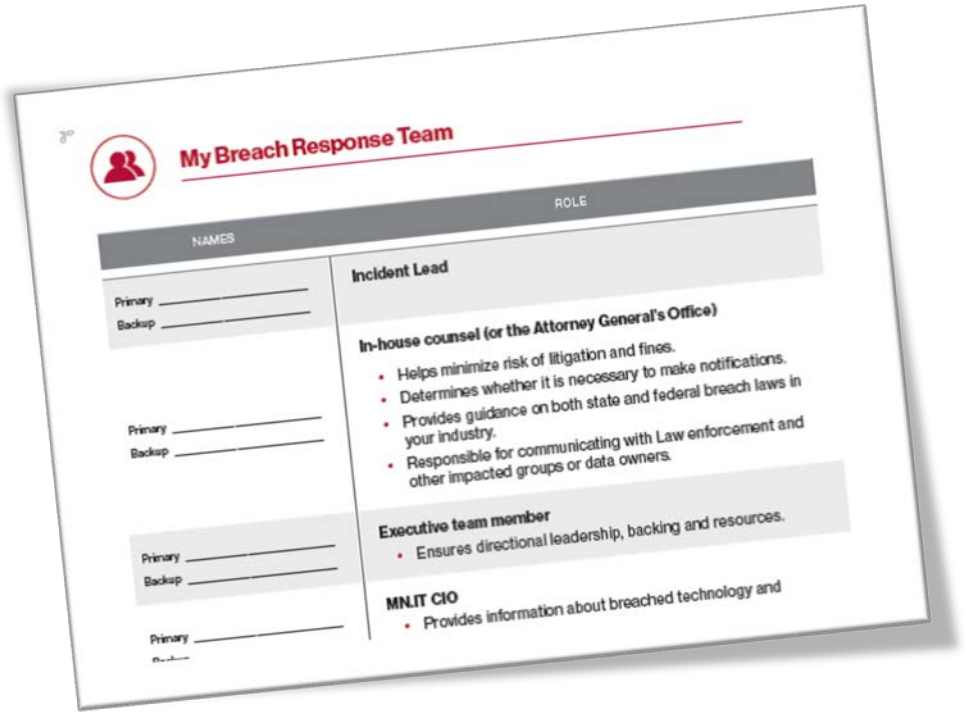
The manual was unveiled at a meeting for state agency leaders about security in the State of Minnesota. The meeting showcased cyber security as MN.IT's number one priority and what it is doing to help secure the state. The manual reinforced the MN.IT message by showing how we partner with agencies to help them protect their data.



# Concept

Breaches create upheaval in an organization. There are questions about what to do first, who to contact, who makes decisions, and what decisions need to be made. In creating a breach manual, MN.IT Services looked at how these very complicated processes could be presented in a way to help decision-makers with the gathering and disseminating of information, while stopping the threat and protecting data.

The concept was to make the manual into a working document. This included creating enough space to fill in names, contact information and notes. Emphasis was on preplanning to assure agencies would have all necessary information in one place during an incident.




MN.IT Communications, Legal and Security worked together to draft the document. The process was started by looking at similar breach documents in the public and private sector. The public sector documents aligned with the information and steps MN.IT would recommend, while the private sector documents were good models for presenting the information in a clean, easy-to-follow format.

Once the information was gathered, Legal wrote most of the document to assure data privacy and security laws were addressed. Communications worked on the notification and press release templates. Security assured the cyber aspects, controls and data preservation were met. After the three areas agreed on a solid draft, the manual was sent to a number of state agencies to see if it was something that made sense to them and that they could follow. After receiving additional feedback, a final draft was created. The document was distributed during an information technology security meeting of state agency leaders.

MN.IT will follow up with agencies later this year to see how the document is working for them. For those who have filled it out, MN.IT will ask if anything was missed, if there was enough room to add all of the information they had, and if the processes were clear. For those who haven't filled it out, MN.IT will do an educational outreach about the prevalence of breaches and the importance of having a response plan in place.

# Significance

Cyber criminals attack the state every day. While the state needs to be good at stopping attacks every time, the cyber criminal only has to be good once to cause an incident that makes front-page news. The Minnesota Data Breach Preparation and Notification for Electronic Data was created to help agencies protect state government data, but also to help them recover if the worst happens. Nothing like this existed in the state, so this became an important manual to begin discussion and thought around what agencies need to do to prepare for the inevitable.

This document addresses both MN.IT and NASCIO priorities. For MN.IT, the breach manual meets priorities of securing the state and improving our services through collaboration. For NASCIO, the manual meets the priorities of Security and Risk Management, and Disaster Recovery/Business Continuity.

## PART 3: BREACH RESPONSE

Although there is no single way of responding to a data breach and each breach will need to be dealt with on a case-by-case basis, the following Breach Response Checklist can assist an agency to move forwarded in a quick and coordinated manner.

A breach has occurred. What you do in the next hours and days will help you halt the security threat, uncover and preserve information and protect your agency's reputation. Below are the steps you need to take now.

### Ten steps in the first 24 hours

- **Record the date and time** the breach was discovered and when the response efforts began.
- **Alert and activate** the Breach Response Team in order to begin executing your preparedness plan.
- **Contact your MNJT CIO.** Your agency-based CIO will work with MNJT's Forensics Team to stop any additional data loss and will properly gather and protect evidence that may be needed for law enforcement purposes.
- **Contain the breach.** For example, recover the mishandled paper files, shut down the system that was breached, revoke computer access privileges.
- **Document everything** known about the breach – who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what data was compromised, what systems are affected, what devices are missing, etc.
- **Determine the cause and extent** of the breach.
- **Determine who is or who may be impacted.**
- **Review protocols** regarding notification about the incident.
- **Assess priorities** and risks based on what you know about the breach.
- **Launch crisis communications process.**

MNJT Services | mn.gov/mnit 13

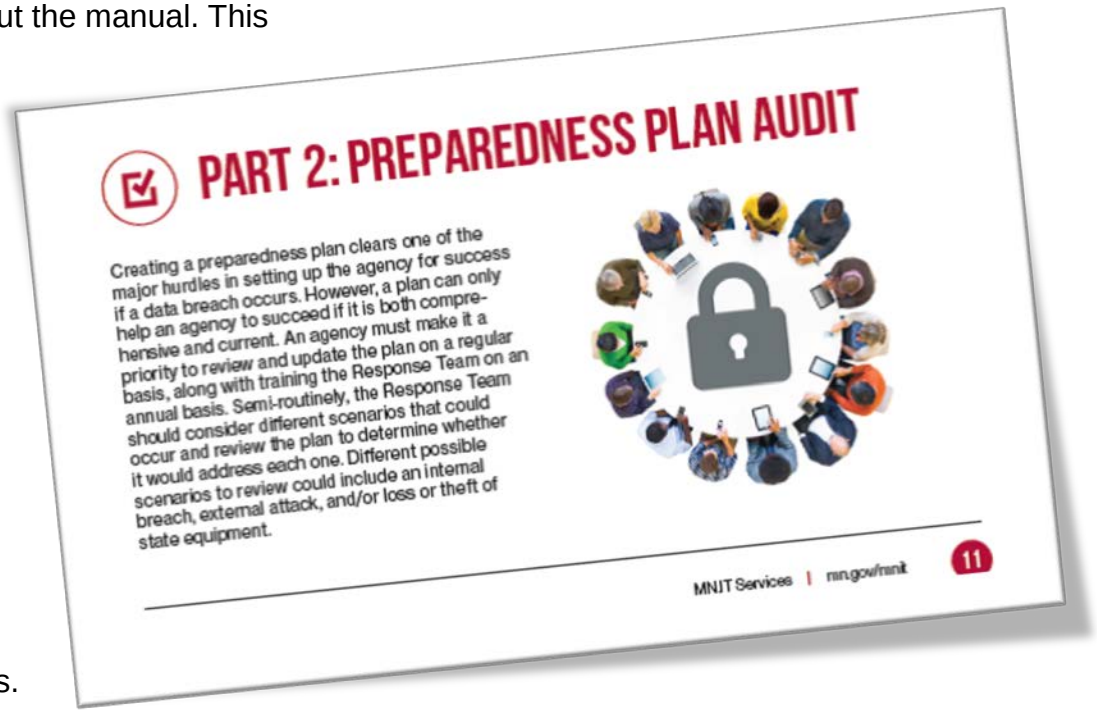
# Impact

In conjunction with the Data Breach Preparation and Notification for Electronic Data manual, MN.IT has hosted Breach Tabletop Exercises for our agency partners. The exercises are meant to simulate an actual breach situation. The exercises enhance general awareness of how to handle a breach situation, validate that agencies have proactively put in place plans and procedures from the manual that are sufficient to handle a potential breach situation, and rehearse how an agency would respond to an actual breach situation.

During the 90-minute exercise, agencies use the breach manual in order to have an opportunity to:

- Activate their Breach Response Team
- Follow the Breach Response Checklist
- Activate their IT team for forensics assistance
- Review agency determined protocols
- Determine if an actual breach occurred
- Determine the type of data breached
- Determine the breach requirement notifications and if notifications need to be sent
- Launch their crisis communications process

These exercises ensure that agencies are getting the most benefit from the manual by completing and testing the Data Breach Preparation and Notification Plan that is referenced throughout the manual. This testing of the Plan during the exercises is essential to ensure that an agency is prepared for a breach situation. The combination of the exercise and the manual assists agencies with both better securing their data and with assuring readiness during a time of crisis.


PART 2: PREPAREDNESS PLAN AUDIT

Creating a preparedness plan clears one of the major hurdles in setting up the agency for success if a data breach occurs. However, a plan can only help an agency to succeed if it is both comprehensive and current. An agency must make it a priority to review and update the plan on a regular basis, along with training the Response Team on an annual basis. Semi-routinely, the Response Team should consider different scenarios that could occur and review the plan to determine whether it would address each one. Different possible scenarios to review could include an internal breach, external attack, and/or loss or theft of state equipment.

MN.IT Services | mn.gov/mnit 11