



# Security & YOU

Think.  
Assess.  
Protect.

## Learning Minute:

# Majordomo email list risks

*Based on true stories from real life at SNL*



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. **SAND2015-5806 TR**

# What Happened

Gerald belongs to a Majordomo\* email group at SNL. Gerald doesn't realize that Outlook does not display the presence of external e-mail addresses in a Majordomo list. Gerald sends an OOO message to his Majordomo list without realizing that some of the recipients have non-Sandia email addresses.

\*Majordomo is a program that automates the management of distribution lists. Lists are created and stored on a list server and are accessible through Outlook and other email utilities.

What concerns do you see with this situation?

# Think

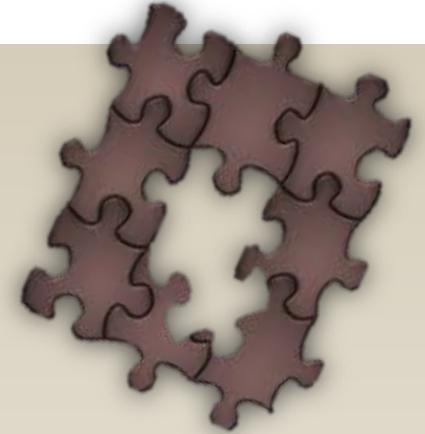
- Does everyone on the Majordomo list have a need to know (NTK) the information being sent?
- Does the information need to be protected?



These questions should be considered for all types of information.

# Assess

- An email list that does not identify the recipients puts the sender at risk.
- An adversary may have access to sensitive information sent via email.
- Unprotected information may be the missing piece needed by an adversary to create a complete picture.
- Any lost information could harm Sandia's reputation or national security.



Protecting Sandia's information  
keeps everyone safe!

# Protect

To ensure *whatever happened doesn't happen again*, follow these steps:

- Ensure that any sensitive information sent via email is sent to an OUO-safe mailing list for sandia.gov addresses only.
- When in doubt, verify with CCHD.



These OPSEC countermeasures help ensure that information is protected and not inadvertently sent to those who do not have NTK.

# Final Thoughts

Careful consideration must always be given when determining what information may be shared with co-workers, colleagues, collaborators and other audiences. Ensure that the audience has a need-to-know before sending out sensitive information.

By ***thinking*** about our information, ***assessing*** vulnerabilities, and implementing ***protections***, we protect ourselves and our information.

**Think. Assess. Protect.**

# Questions? Ideas?

**Phone: 321 (from any Sandia phone) or 845-1321**

**Web: [security.sandia.gov](http://security.sandia.gov)**

**Email: [security@sandia.gov](mailto:security@sandia.gov)**

Contact the Communications Team at [securityed@sandia.gov](mailto:securityed@sandia.gov) with ideas and suggestions for future topics.