State of Nebraska

Microsoft Exchange Environment

Jayne Scofield
Annie King
Kevin Waechter, and Jason Meyer

Current Environment

Exchange

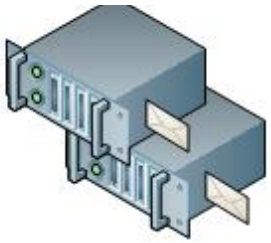
- Exchange 2007 CCR
  (Cluster Continuous Replication)
- 3 Mailbox Clusters
- 2 HUB Roles
- 2 CAS Roles
- 2 Physical Sites
- 5 Virus Engines

Current Environment
IronPort

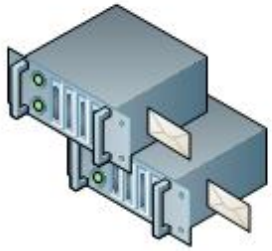
- 5 IronPort Appliances
  (2 C660, 2 IEA, 1 M660)
- SPAM and Virus filters are updated every five minutes
- Hardware refreshed summer of 2009, expires 2013.

State of Nebraska Exchange 2007 Organization

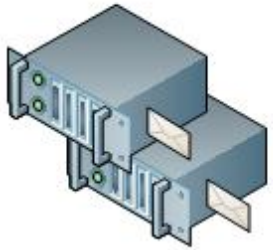
Mailbox Cluster 1



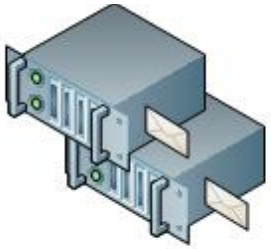
Mailbox Cluster 2



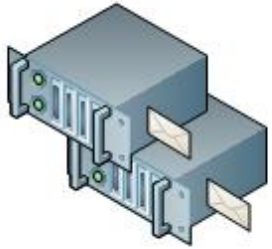
Mailbox Cluster 3

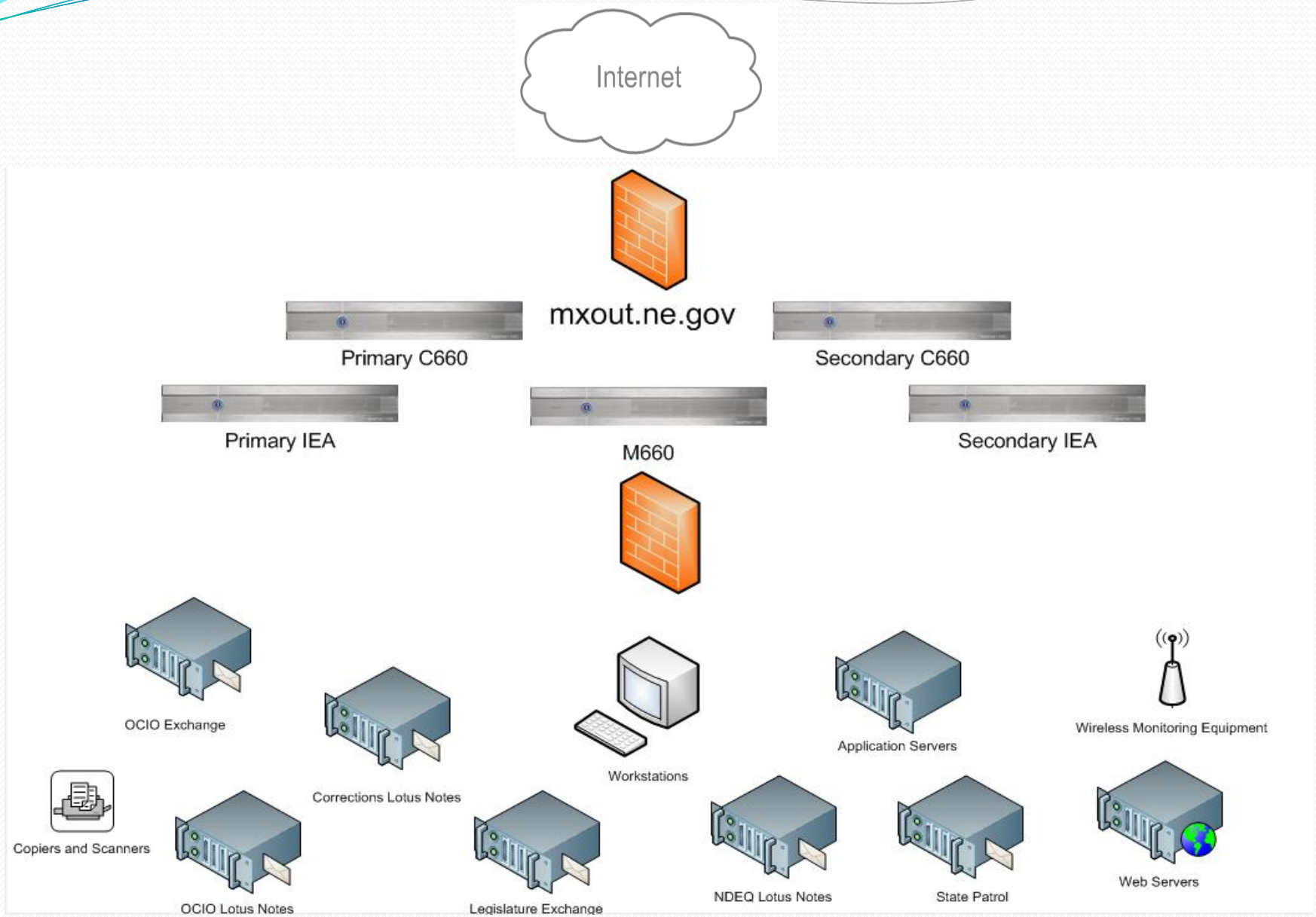


Hub Transport



Client Access



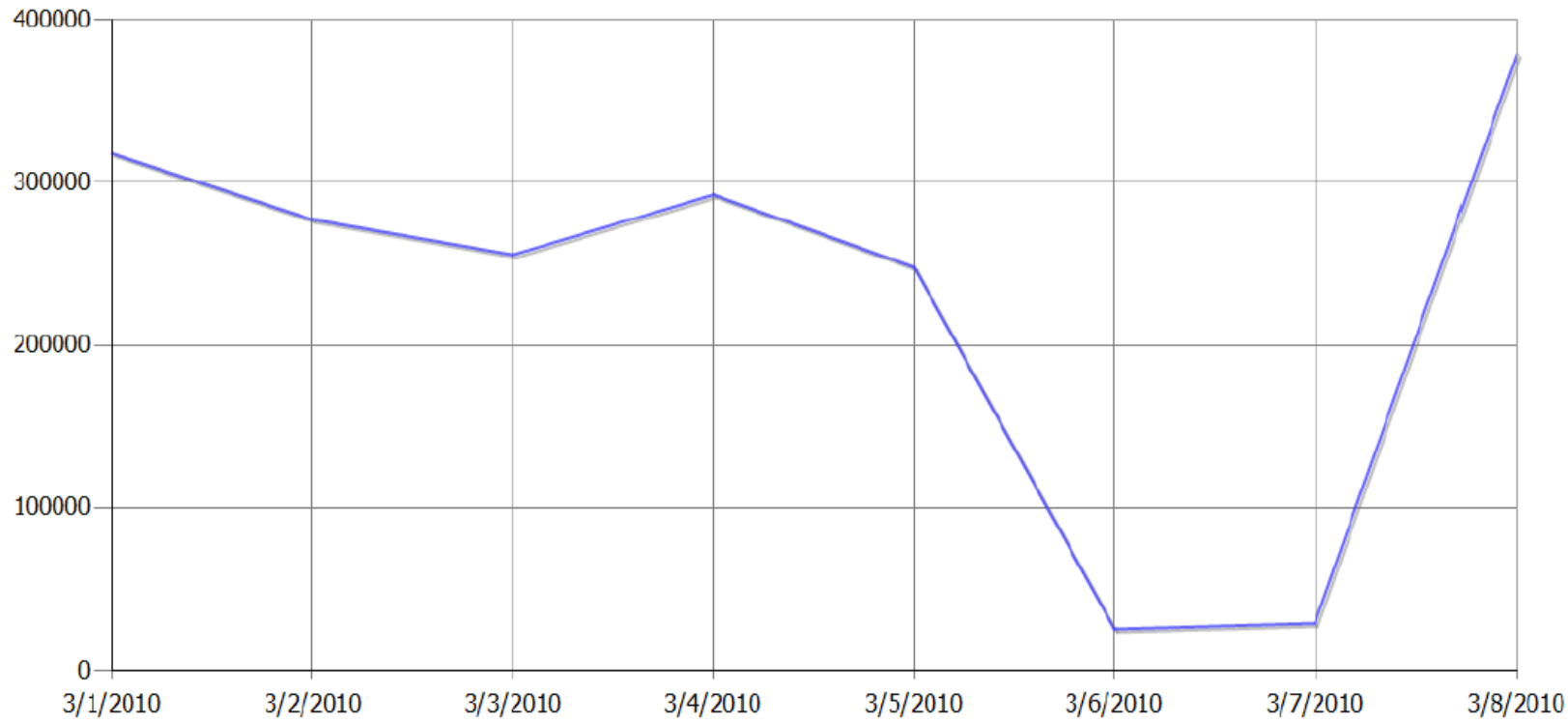

Internet
mxout.ne.gov
Primary C660
Secondary C660
Primary IEA
M660
Secondary IEA
OCIO Exchange
Corrections Lotus Notes
Workstations
Application Servers
Wireless Monitoring Equipment
Copiers and Scanners
OCIO Lotus Notes
Legislature Exchange
NDEQ Lotus Notes
State Patrol
Web Servers

Exchange Statistics

- 21 thousand mailboxes (17,080 active)
- 3 thousand distribution groups
- 100+ million total e-mails (avg. 180 thousand e-mails per day)
- 10 thousand users connected daily
- 99.982% uptime for the year. (93 minutes)

Exchange Messages Delivered

(Sample Report: 3/1 – 3/8/2010)



IronPort Average Daily Statistics (Incoming Mail)

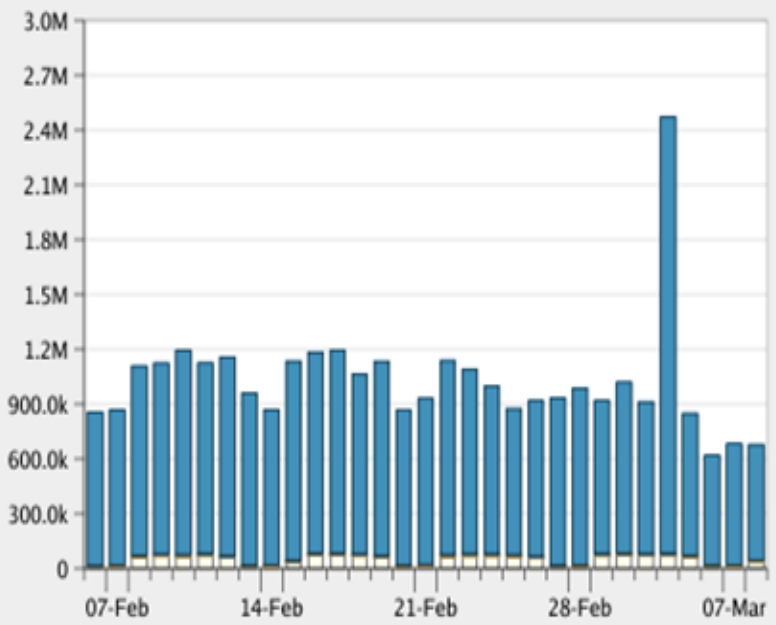
- 1 Million connections attempted (95% are denied)
- 4 Thousand declined based on invalid recipient
- 5 Thousand e-mails quarantined as SPAM
- 12 e-mails quarantined containing viruses
- 28 e-mails quarantined based on Content Filters
- 5% of attempted e-mail is allowed through (60-80 thousand)
- 100% uptime outside of scheduled downtimes

IronPort Monthly View (Incoming Mail)

Time Range: Month (30 days) **View Data for:** All Email Appliances

06 Feb 2010 00:00 to 08 Mar 2010 13:51 (GMT -0600) Data in time range: 100.0 % complete

Incoming Mail Graph



Info... | Export...

Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	94.4%	30.1M
Stopped as Invalid Recipients	0.4%	115.2k
Spam Detected	0.5%	158.5k
Virus Detected	0.0%	352
Stopped by Content Filter	0.0%	846
Total Threat Messages:	**95.3%**	**30.3M**
Clean Messages	4.7%	1.5M
Total Attempted Messages:		**31.8M**

Info... | Export...

Microsoft Health Check

When: Week of March 29th

What: Microsoft will be coming in and evaluating the current Exchange organization.

Purpose: Exchange has been live for two years, time to stand back and take a look at the overall picture.

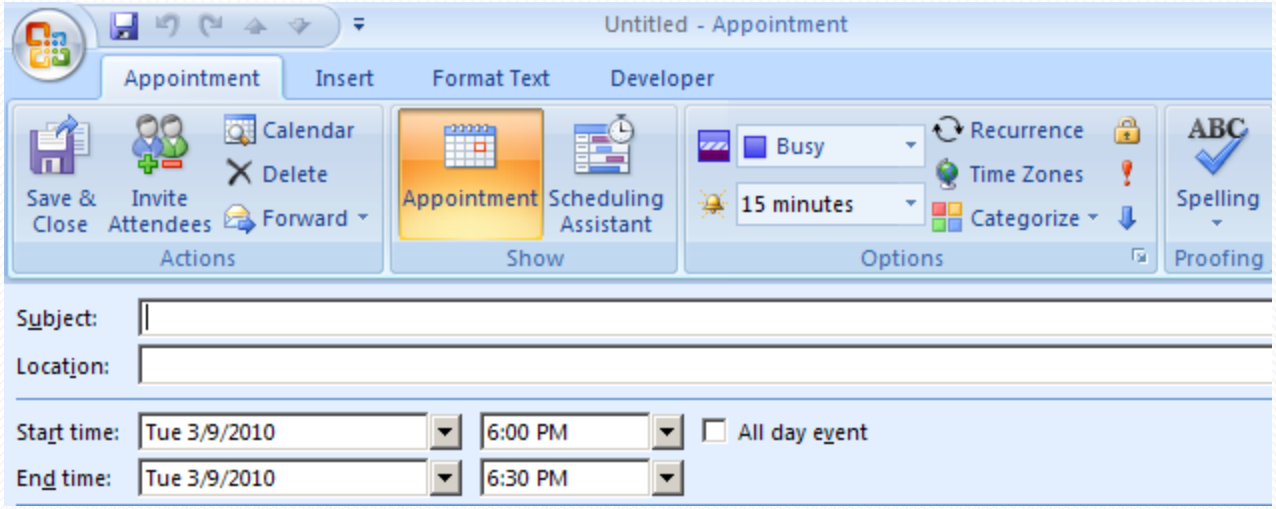
- *Best Practices and General Health*
- *Downtime Process*
- *Problem Handling*
- *Active Directory*
- *Agency Communications*

Resources – How are they Handled Differently?

- **Active Directory Account Administrator Guidelines:**
  - Disabled AD object
  - Don't fill in e-mail address
  - Use permissions to manage Resource, no need to login to account directly
  - Use Auto Accept for requests if possible

Resources – How are they Handled Differently?

- **Resource User Guidelines**:
  - Remember to reserve rooms by inviting them to the meeting.
  - The location field is a free text field that you can type anything in. If left blank the reserved room will populate this field automatically.
  - Use the **Scheduling Assistant**



Delivery Failures

What Do They Look Like?

Delivery has failed to these recipients or distribution lists:

Jasons.meyer@nebraska.gov
The recipient's e-mail address was not found in the recipient's e-mail system. Microsoft Exchange will not try to redeliver this message for you. Please check the e-mail address and try resending this message, or provide the following diagnostic text to your system administrator.

Delivery has failed to these recipients or distribution lists:

Meyer, Jason
You are not allowed to send this message because you are trying to send on behalf of another sender without permission to do so. Please verify that you are sending on behalf of the correct sender, or ask your system administrator to help you get the required permission.

Delivery Failures

How Can We Help Prevent Them?

- Take a moment to read the failure; it probably failed for a simple reason.
- Use the GAL to send e-mails
- Type a portion of the name and hit CTRL + K to resolve the address
- No need to have everyone in your personal address book

Using Invalid FROM Addresses

- E-mail is simple to automate
- E-mail sent with an invalid FROM address has no path to bounce back
- E-mail with an invalid FROM address will never fail, because it can't.
- Using invalid FROM addresses causes e-mail to get stuck

Using Invalid FROM Addresses

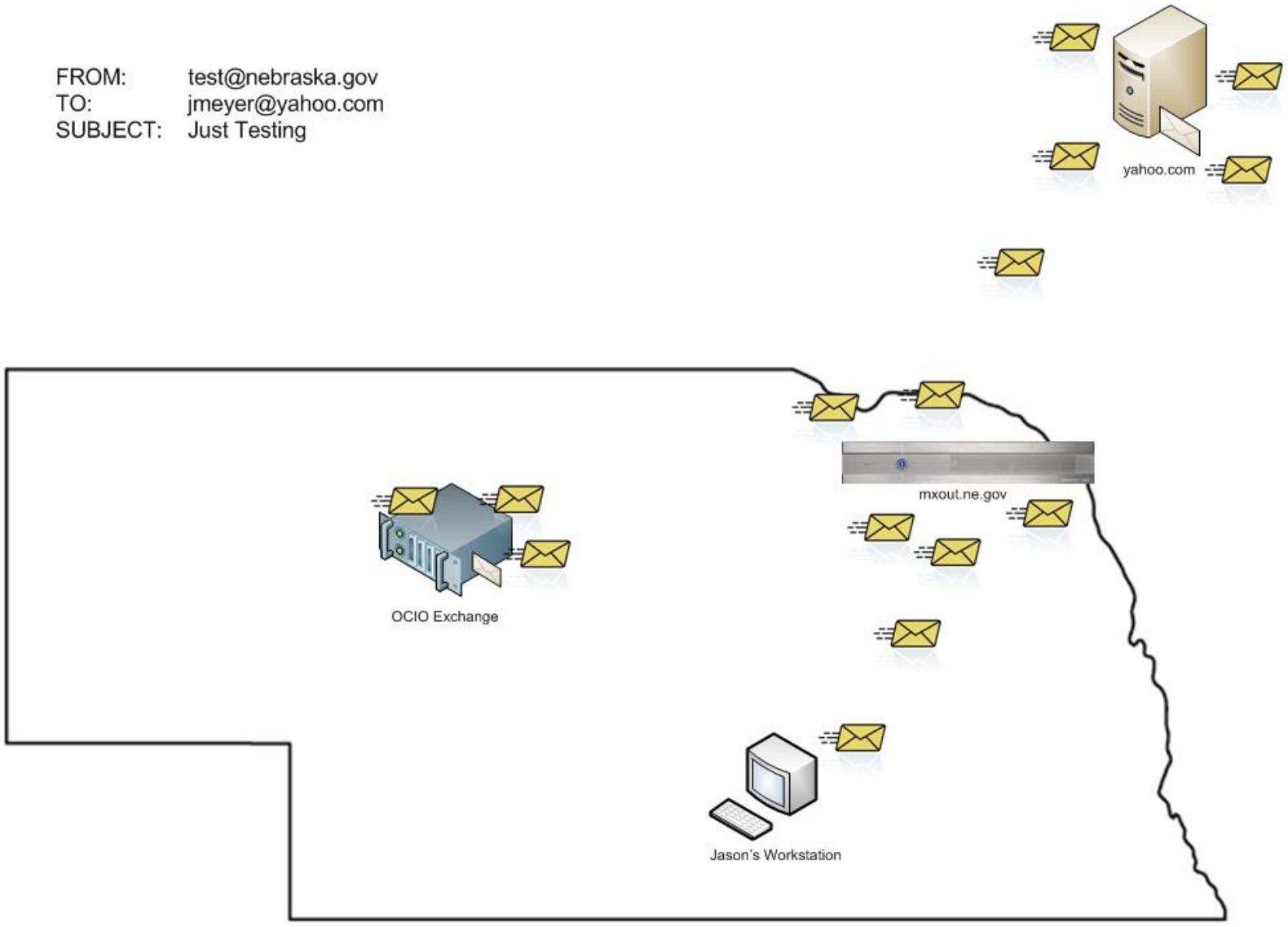
- “What if we don’t want them to respond?”
- E-mail stuck on a recipient system causes our reputation for e-mail to decline
- This leads to grey listing and blacklisting causing critical communications to not be delivered (Amber Alerts, Health Alerts, etc.)

Using Invalid FROM Addresses

What can we do that is better?

- Use an existing e-mail address that is on a mailbox as the FROM address.
- Add a secondary e-mail address to an existing mailbox and use that as the FROM address.
- Setup it's own mailbox/e-mail address and use that as the FROM address.
- This way delivery failures or responses have a place to go and do not get stuck in the e-mail pipeline.

FROM: test@nebraska.gov
TO: jmeyer@yahoo.com
SUBJECT: Just Testing



Public facing port 25

- OCIO is making preparations to close Port 25 outside of the SMTP gateway (IronPort).
- NITC standard that indicates all e-mail needs to be routed through OCIO SMTP gateway.
- Legitimate mail is being routed through SMTP gateway per DNS mail exchanger (MX) records.
- Servers that are open and listening on Public facing port 25 are vulnerable to SPAM and virus attacks.
- OCIO is monitoring and beginning to contact agencies that have servers open on Port 25.

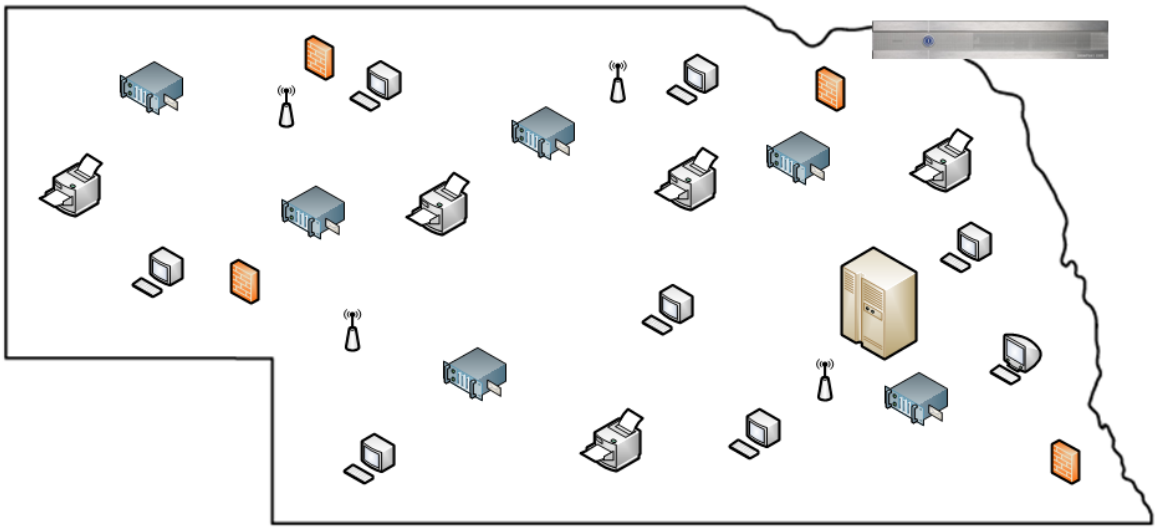
Public Facing Port 25

Agency Tasks

- If you have servers, workstations, devices, scripts, etc. that send e-mail, or have SMTP capabilities, check to see if they are open and listening on port 25 from the public Internet.
- By using mxout.ne.gov to route e-mail there is no need to have port 25 open and listening on the public interface.
- If there are any questions about this feel free to contact us.

SMTP Traffic Sources

- Thousands of internal SMTP Servers
- 2,575 unique internal IP addresses have sent e-mail to IronPort (Avg. 1,000 per day)
- OCIO has closed 5 so far
- It only takes **1** to cause a problem



Legacy Email Domains

- Migration to @nebraska.gov is complete
- OCIO starting to shutdown our legacy domains
- 73 e-mail domains have been disabled
- Roughly 200 total domains (.ne.gov, .state.ne.us)
- If you have your own e-mail server and you are ready to shut it down, give us a call.

Other Topics:

- General E-mail Guidelines
- Securemail
- Distribution Group Management
- ListServ
- Exchange 2010

Thank You!

Questions?

Office of the CIO
HelpDesk
402-471-4636 or 800-982-2468