Patch Management Process

INCIDENT: Emergency Security Patching for Servers and Workstations

PROCESS: Once an alert has been received, conduct the following:

1. Assess the alert to determine if it applies school-wide, only to a particular department or office, or only for a select type of operating system
   - Alerts will generally come from a security listserv, an anti-virus vendor, an operating system vendor, CERT, Infragard, etc
   - Under most situations this will be a Microsoft security patch update.

2. Craft an email message similar to the following:

   SUBJECT: SECURITY ALERT: {Description of issue}
   CRITICAL/SERIOUS SECURITY ISSUE {Select one of these for the message}

   We have received an alert recommending that security patches for servers and workstations be applied out of the normal cycle. A brief description of the issue is described in the next paragraph.

   {Description of the critical or serious event goes here.}

   All LSPs should immediately obtain the appropriate security patches for their servers, test and evaluate the security patches for any problems, and install the patches as soon as possible. All LSPs should also make sure a back-out plan is in place in the event problems are encountered with the security patch.

   All workstations should be patched immediately. As before, a back-out plan should be prepared and utilized in the event problems develop with the patch.

   For more information on this vulnerability please go to:

   {List a link or web site for additional information here}

   For access to the security patch, please go to:

   {List the appropriate Microsoft patch location here}

   Thank you.
3. This email should be sent to the following:
   - IUSM LSP Listserv: MEDMAIL
   - IUSM CIO: Vince Sheehan
   - Other hospital security officers in the area as time permits

4. Coordinate with ISTM server and the desktop groups to arrange to implement emergency patching for all ISTM-maintained systems. The ISTM server and desktop groups will notify then customers. A message should be sent to the "ISTM OT CLIENTS" and the "ISTM OT DEAN'S OFFICE" email groups advising the following:

----------------------
SUBJECT: Emergency Security Patches for ISTM Servers and Workstations

Tonight at approximately {time} ISTM will invoke emergency procedures in order to install several security patches on all ISTM-maintained servers. This should only cause a momentary loss of connection to the servers and shouldn't be noticed by anyone unless you happen to be accessing the servers at midnight tonight.

Workstations supported by ISTM will have security patches installed tonight around {time} during normal updates. The workstations are automatically rebooted as part of the normal patching process. Please leave all workstations on tonight however make sure to log off the system before you go home. This will allow the patching to take place. We will begin scans tomorrow to make sure all systems have received the appropriate security patches.

Any problems or issues can be reported to the ISTM Help Desk at 274-5336.

Thank you,

----------------------

5. If the CIO and managers haven't already been briefed on this issue, make sure they are briefed now so they can answer any questions the Dean or EADs may have.

6. Continue to provide updates as determined by the severity of the issue.

7. Log the event for incident tracking purposes.