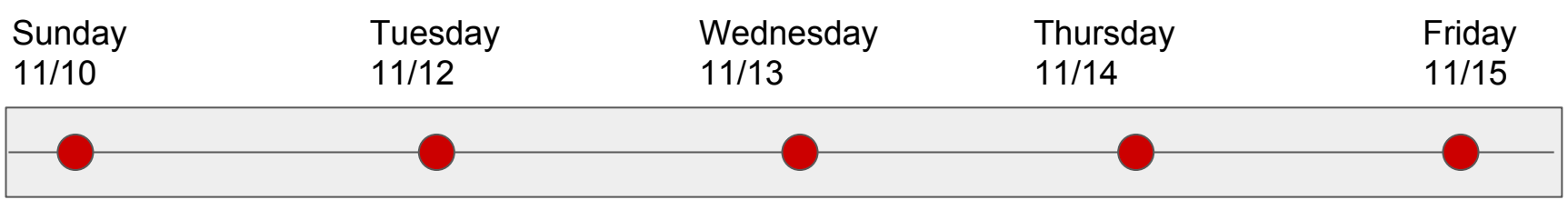
Ransomware 2013

IT Professionals Conference
June 22, 2017

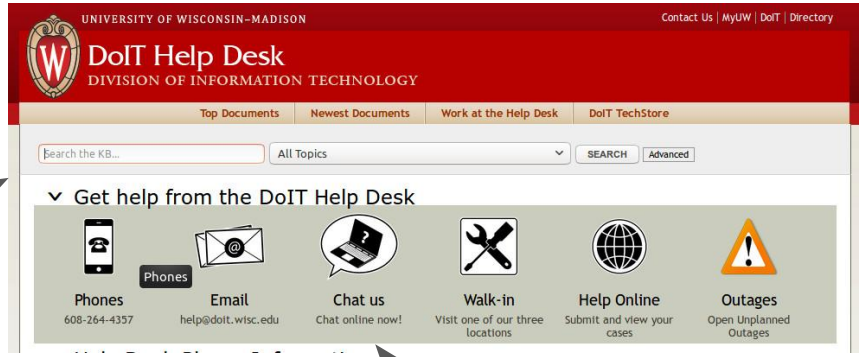
A little context

- Sue Weier, L&S Learning Support Services (LSS)
- Incident occurred in an entity that was migrating into L&S from another College.
- The entity was loosely affiliated with a department that LSS supports, thus we also supported this entity.
- The migration mechanics were mostly handled by the department they were affiliated with.


Sunday
11/10
Tuesday
11/12
Wednesday
11/13
Thursday
11/14
Friday
11/15
I went on vacation.
Victim contacted the HelpDesk.
LSS began investigation.
Backup problems.
Cybersecurity took over (OCIS then).

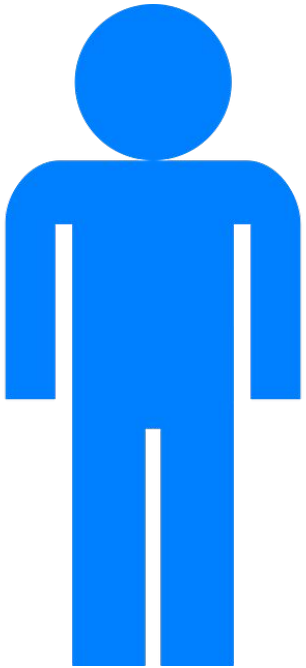
Tuesday. Someone needs help.

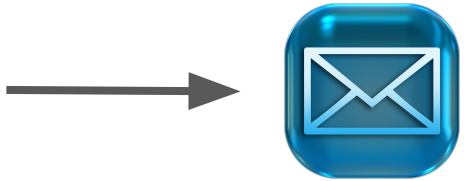
Tuesday.



#67906

Wednesday. Help arrives. Kind of.





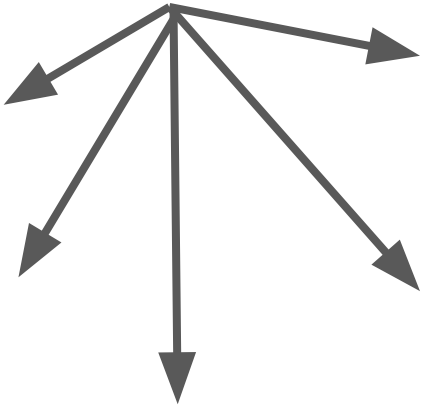
LSS TechZone
Ticketing System

Wednesday.

- TechZone point person assigned.
- On-site assessment
  - Unmanaged Windows computers with varying configurations.
  - Previously used a departmental file server.
  - Now using DoIT Shared Drive, with permissions managed by someone in the department.
  - Bucky Backup. Single 30-day backup, overwritten.
- Lots of confusion.
- Compromised laptop was brought back to the TechZone offices.

Thursday. Picking up the pieces.

File management begins.



LSS staff left a voice mail message with OCIS.

Configured the security baseline for other machines in the department.

Bucky Backup service contract upgraded.

Thursday. Backups.

- The backup was partially encrypted. The ransomware had activated before the files were backed up. About 25% of the data was saved, thanks to an observant DoIT employee.
- We found an earlier backup that had some of the files on it. Staff went through the backup to find needed data.
- File management --
  - Checking Bucky Backup to see what files were accessible.
  - Checking external HD to see what files were useful.
  - Checking individual hard drives to see if copies of files had been retained.

Friday.

- OCIS got involved. They took over investigation.
- More communication with department staff.
- Continued efforts to locate missing files.
- Eventually it was determined that nothing had been transferred off campus.

Problems and best practices

New patrons

- Before support is transferred, request and receive:
  - an inventory of machines.
  - a list of assigned software.
  - a description of the security configuration on the machines.
- Assess machines personally, if possible.
- Assign a point person to work with new patrons/units as they migrate into TechZone support.
- Have a point person within the new unit to receive and disseminate communications.
- Tell the new patrons how to contact you.

Problems and best practices

Poor communication

- Establish at least one contact in each supported department that knows you and knows how to get help.
- Have regular contact with your patrons through email. (ex. bi-weekly patching emails)
- Integrate email replies into your case tracker, if possible.
- Put your contact information on everything.
- Don’t rely on a middleman. Things fall through the cracks.
- Do ask for help from colleagues if needed.
- Signage.

Problems and best practices

Non-standard configurations

- Security baseline configuration
  - Establish baseline security configuration.
  - Re-image new clients, or configure security baseline manually.
  - Treat the security baseline as a gatekeeper - new patrons don’t go online with support unit until it is configured.
- Don’t allow exceptions to the security baseline.

Problems and best practices

Permission configuration

- For shared storage, be choosy about who can write to what folders.
- If a department staff member is configuring shared storage, recommend stinginess and make sure he/she is comfortable with this responsibility.

Case tracking

- Integrate email replies into your case tracker.
- Make sure someone is always checking for new cases.
- Make sure your voice mail message is up-to-date.
- Document everything.
- Consider an “urgent” tag for incoming cases.