Chief Information Security Officer report on the nature and frequency of University IT search requests
University IT Policy committee comments incorporated 16 April 2018
Submitted by A. White and R. Wood for incorporation in minutes for Faculty Senate meeting on 17 April 2018

General Information

- There are approximately 78,000 email inboxes maintained across multiple mail systems at UR
- Approximately 85% of incoming digital traffic (email and digital probing) is malicious, occasionally successful, and requires immediate intervention to defend university systems
- Failure to maintain our defenses has resulted in interruption of services for days and in a recent case, weeks. We provide health care to the region so lives as well as our educational and research missions are at potential risk.
- The U of R Information Technology organization is talented and professional. To ensure awareness of and compliance with University policy on the collection and retention of personal information and electronic communications, employees in both UIT and ISD are given annual updates to training and/or sign off acknowledging their responsibilities.

Search Requests

- User email account snapshots (“Legal Hold Inbox” Requests)
    - 31 Requests encompassing 108 individuals over 12-month period (~0.14 % of total UR accounts)
    - Snapshots requested by Office of General Counsel (OGC) through IT Security Office
    - IT does not review or search contents but transfers access to OGC

- Forensic Reviews that preserve the chain of evidence for potential use in legal proceedings
    - Approximately 12 per year
    - Performed by certified professionals with special training
    - Performed in response to a
        - Security incident
        - A compliance event, i.e. an incident or complaint associated with a statute or regulation to which the University of Rochester must demonstrate adherence and which are conditions for the continuance of normal operations (including routine transfer of federal funds into university accounts). This is a long list of certifications: privacy, antidiscrimination, violence in the workplace, drug-free workplace, business practices, conflict management, and ethical research conduct... to name several.
        - Request from OGC, e.g. response to subpoena
    - Full forensic imaging of a workstation, i.e. a “snapshot” not just of an email inbox but of an entire system copied to a virtual machine with documentation of the chain of evidence
    - Detailed structured searches of mailbox, file contents, logs, and similar files to detect and identify potential indicators of compromise of other machines and systems; an iterative process as evidence of concern arises with a structured process for cessation, reporting, and escalation

- Unique Incident Driven Searches – approximately 5 per month
    - Public Safety needs assistance in crime investigation
    - Public Safety needs assistance in locating a missing person
    - University systems operation troubleshooting
    - HIPAA incident investigations, e.g. was protected health information transmitted securely
    - Grand Jury subpoenas are confidential and can be viewed only by named parties