University of Rochester Monthly Security Scorecard – February 2017
Updates and Intel

Information Security Threat Level

National Healthcare & Public Health Cybersecurity Alert Level

- Low
- **Guarded**
- Elevated
- High
- Severe

Source: NH-ISAC

Internet Storm Center Public Internet Infrastructure Threat Level

- **Green**
- Yellow
- Orange
- Red

Source: SANS

University of Rochester Information Security Updates

- Cory Tylenda & Kathee Tyo passed their **ISO Lead Implementer 23301** exam
- A number of UR WWW Wordpress sites were compromised between February 4th and 6th due to an unpatched Wordpress vulnerability. Emergency Wordpress upgrade was completed on February 6th and affected websites were rolled back to a clean version.
- Cylance chosen as new AntiVirus Solution for UR & MC
- March begins socializing USB Device lockdown
- Security, Privacy, & Legal responding to open OCR Flash Drive Incident
- New risk registry process just built into Service Desk to track and report on risk & mitigation process. Detailed list to start next month.

IT Security News from around the World

- Stolen Health Record Databases Sell for $500,000 In The Deep Web
- Cloudbleed – How to Deal With It
- SHA1 Collision Attack
- HPH Sector Cyber Notice: Grizzly Steppe- Russian Malicious Cyber Activity
- ISIS encourages lone wolf attacks on hospitals and other facilities
- Amazon Web Service outage causes trouble across the Internet

February 2017 IT Security Education Focus

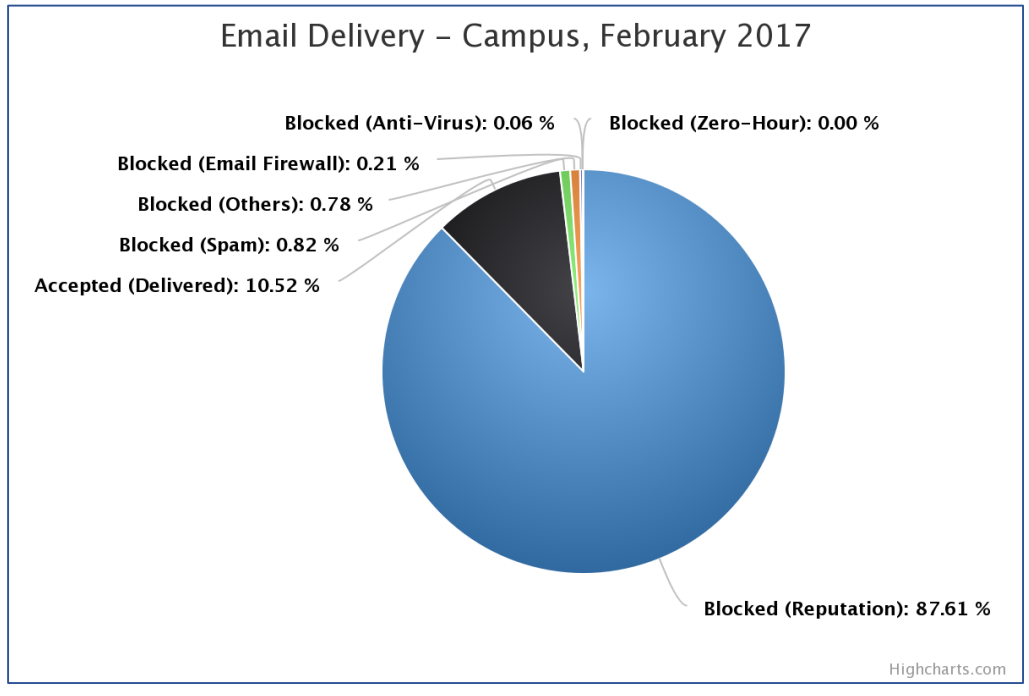
@Rochester Security Tip Focus : Device Security & Scam Protection

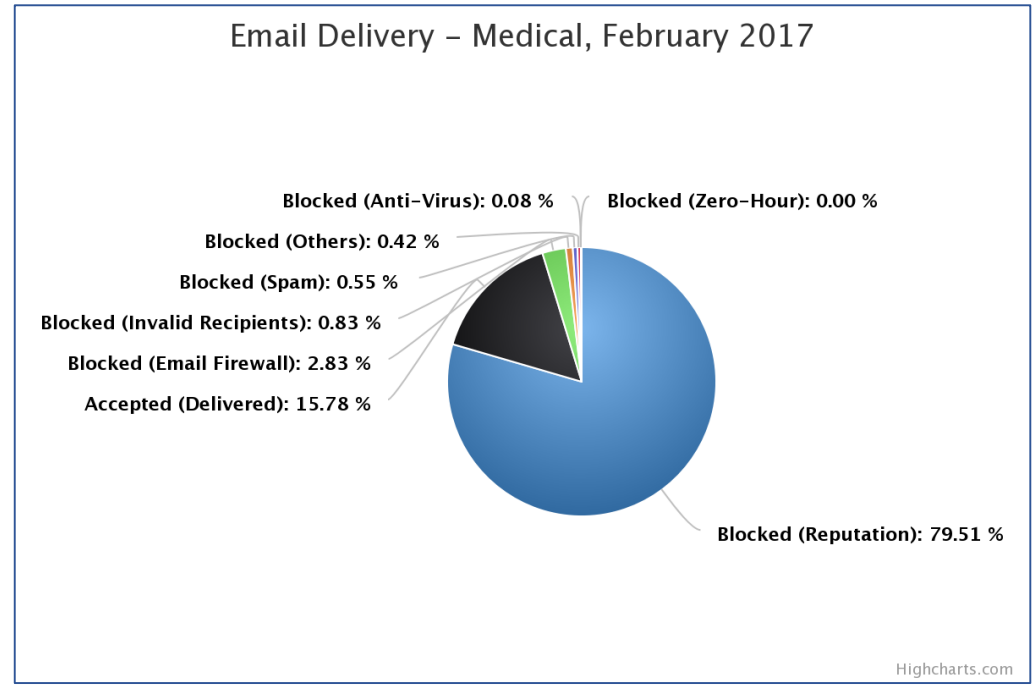
HIPAA Highlight Topic: Encrypted Devices

Risk Registry – Top Risks

- Personal device usage on clinical network
- Loss / accidental disclosure of legally restricted information
- Lack of visibility to some departmental IT practices
- Incomplete Business Continuity Management Planning for some systems

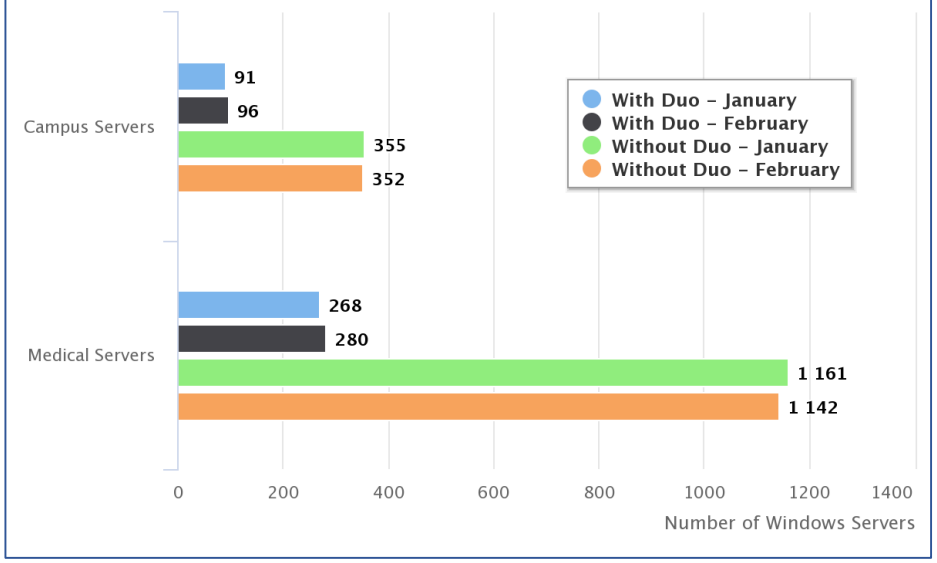
Key Security Metrics – February 2017



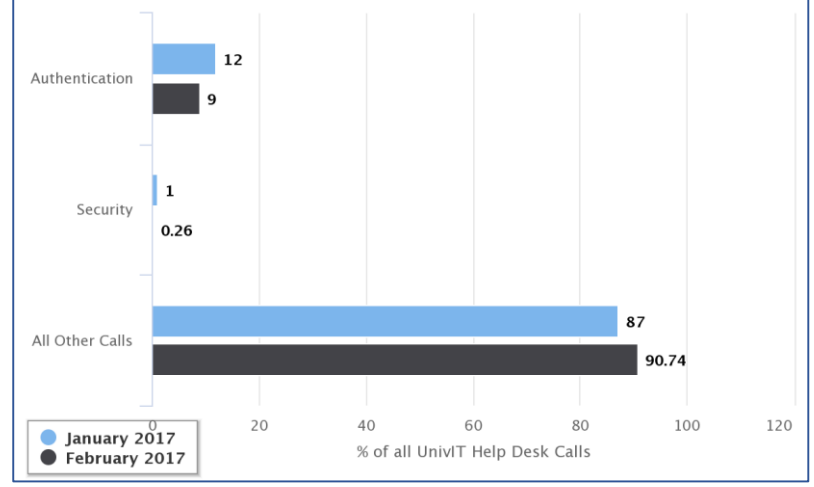


Confidential

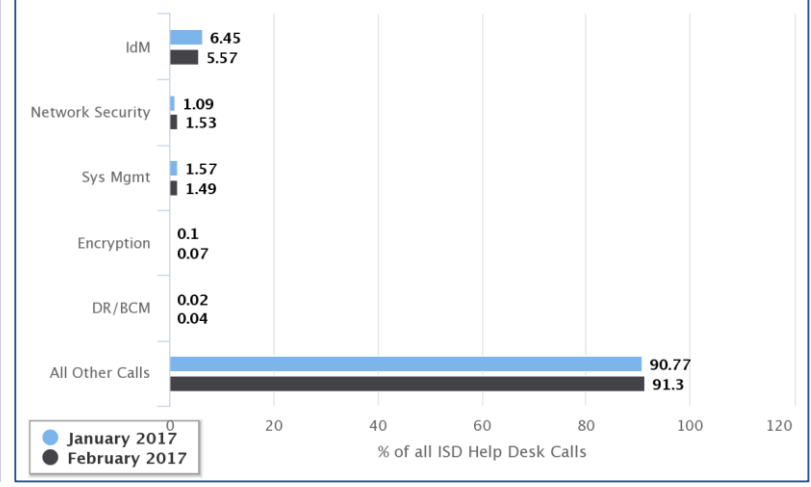
Duo Installations



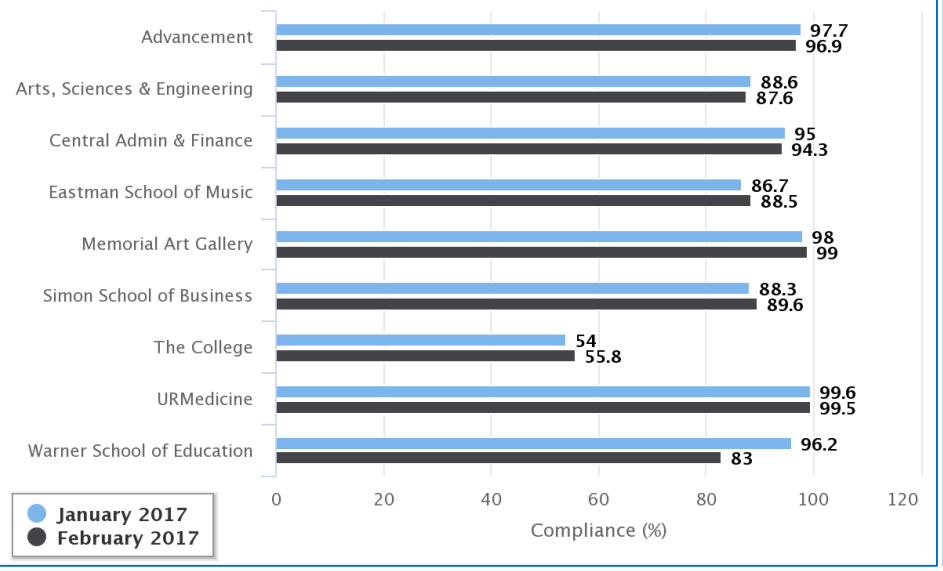
UnivIT Help Desk Calls



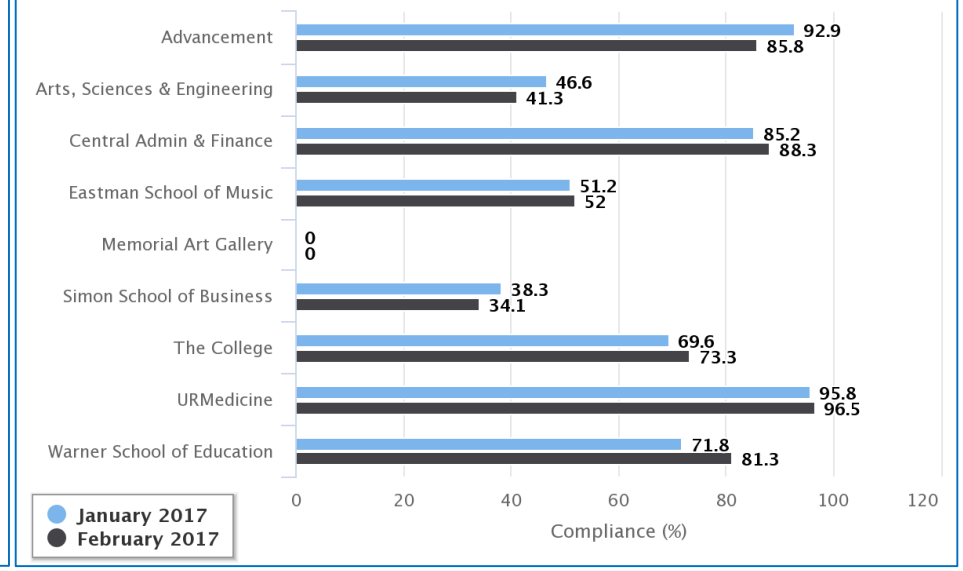
ISD Help Desk Calls



Anti-Virus Compliance

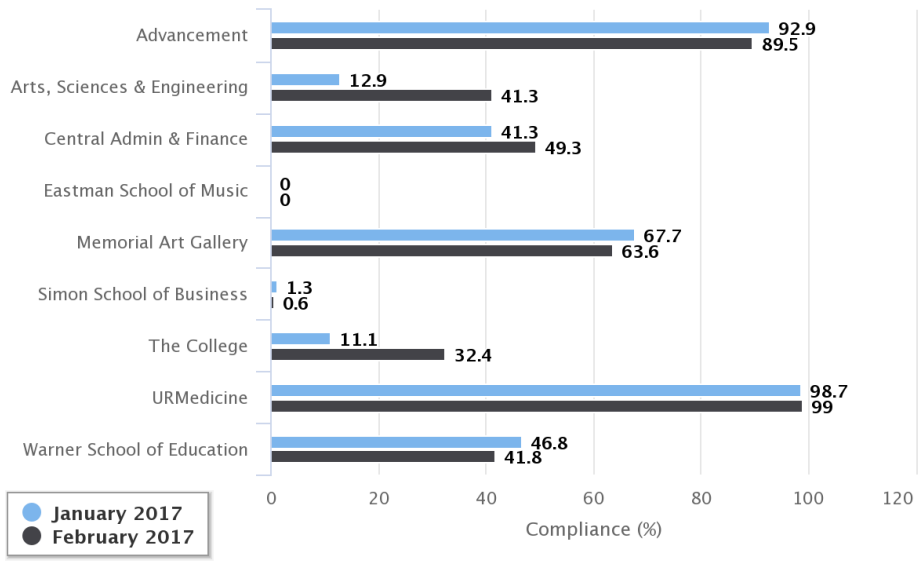


Patch Agent Compliance

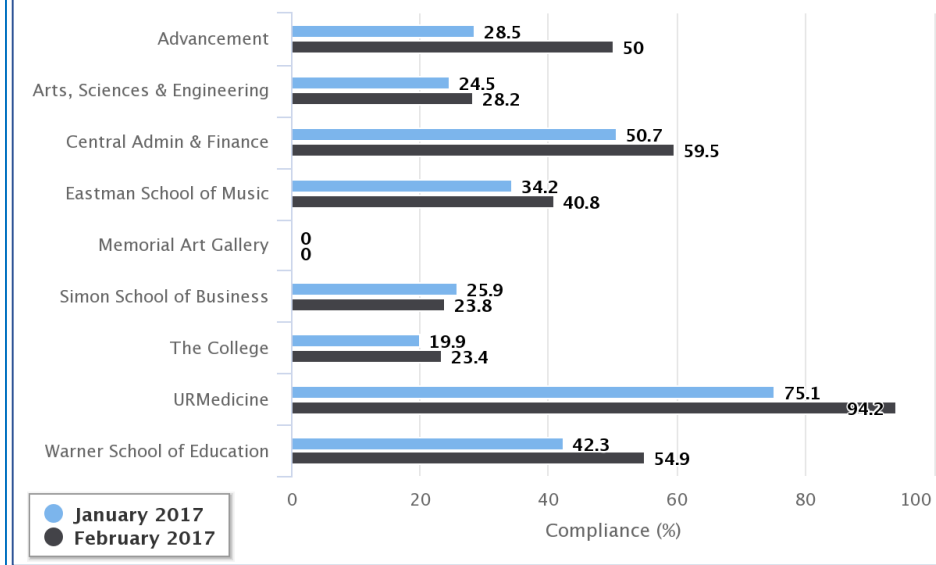


Due to a Vulnerability Management transition from one product to another product, no vulnerability management metrics are available this month.

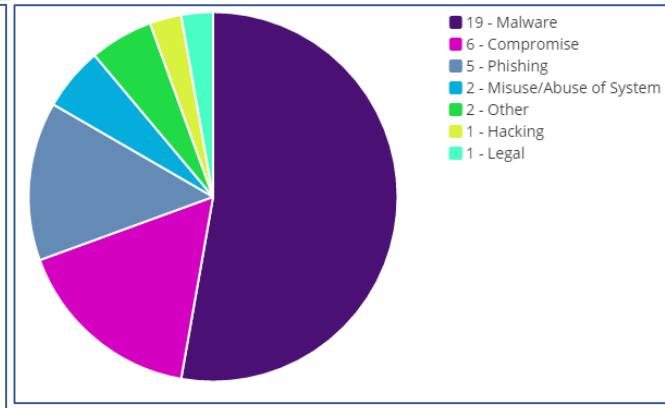
Encryption Compliance



Patch Compliance



Security Incidents - Campus



Security incidents are not currently tracked for medical.

Confidential