

HIT Standards Committee

Hearing on Health Information Technology Security Issues, Challenges, Threats, and Solutions

November 19, 2009

Systems Stability and Reliability Panel – address security challenges related to maintaining the stability and reliability of EHRs in the face of natural and technological threats.

Questions:

1. Briefly describe your organization and your information security approach to system stability and reliability.

Mayo Clinic is a non-profit organization and internationally renowned group medical practice headquartered in Rochester, Minnesota. Its headquarters consist of the Mayo Medical School, the Mayo Graduate School, the Mayo College of Graduate Medical Education, and several other health science schools. Its research facilities are in Rochester, Minnesota, in addition to hospitals and clinics in Jacksonville, Florida, Scottsdale, Arizona, and Phoenix, Arizona. Mayo Clinic partners with a number of smaller clinics and hospitals in Minnesota, Iowa, and Wisconsin, an organization known as the "Mayo Health System."

Information is a key asset because it is integral to Mayo Clinic's mission, primary value, and operations. Regardless of the media on which the information is stored or transmitted (e.g., paper, computer hard drives, fiber-optic cables, wireless networks), information must be safeguarded. At Mayo Clinic, computer information systems are used in many ways, such as to automate the intake of patient information, assist in diagnoses, track medical histories, expand knowledge through research, share information, and bill patients. To maximize business value, Information Security plays a governance and risk management role, partnering with business areas, Information Technology and other functions to align system stability and reliability objectives with business directions by developing policy and designing controls

By focusing on protecting institutional information assets and its workforce awareness, information security helps to protect the reputation, legal position and financial resources of the institution. Most importantly, information security helps to ensure that the patient receives the best care by assuring that information assets are confidential, available, and has integrity.

2. Provide one or two examples of information security issues you have faced recently related to system stability and reliability, and describe how you addressed these issues.

Network-borne threat events, such as computer viruses, worms, distributed denial of service attacks, and the like prompted Mayo Clinic to take action on a couple fronts. An eight-point network security strategy was adopted a few years ago by the oversight committee responsible for information security. These objectives are, for the most part, accomplished:

- Know what's on the network (Networks responsibility): Real-time or near real-time device inventories are needed to locate (map), identify and describe all network devices in order to perform timely and effective threat analysis. Device descriptions must include basic configuration information to include operating system descriptions and security status such as anti-virus and security patch status. Identifying a person responsible for each device is also necessary.
- Establish configuration standards and assign implementation responsibility (Security responsibility): Develop security baselines—the platform-unique configurations and implementations necessary to mitigate risk. All networked devices capable of employing anti-virus countermeasures, service packs and security patches should do so. An operational group must be identified to broadly implement this beginning with the highest risk systems—those running Microsoft operating systems. An enforcement function must also be identified and empowered.
- Control what's connected to the network (Networks responsibility): An infrastructure feature should exist to allow and disallow device connections to the network. Only devices that meet configuration standards and are necessary to the business should be allowed to connect. This implies a process to evaluate every connection request.
- Articulate and communicate expectations (Security responsibility): A philosophy of *the needs of the many outweigh the wants of the few* must be adopted. This is counter culture at Mayo and will require strong administrative backing. It is not possible to accomplish most of these strategies without establishing a communal sense of responsibility and accountability.
- Create protective architectures to isolate high risk devices (Networks responsibility): Adopt a proactive strategy of protecting the greater network from devices that cannot protect themselves. This implies a network consisting of multiple logical partitions (subnets) designed to contain adverse incidents, limit damage and protect the medical practice from nonstandard, unmanageable systems prone to compromise. Communication between partitions would be controlled by firewalls or routers with access control lists. Three broad risk categories are identified:
 - High risk but well-managed: Microsoft devices are traditional targets and vehicles of malicious software. In centrally managed mode, secure Microsoft devices receive timely security patches and virus definition updates in an automated fashion.

- Low risk and generally acceptable: Other devices, such as Macintoshes, Tandems, VAX & Linux systems, are not traditional targets of malicious software. Although these devices are at low risk for adverse events, it may be prudent to be prepared for incidents that may adversely impact them as risk models change.
- High risk and unmanageable: Microsoft devices that are not centrally managed must be subject to communication filters to prevent them from adversely impacting the rest of the network when malicious software compromises them. These nonstandard, non-compliant devices should be isolated. Developing this partition is a high priority.
- Develop drawbridge capability to quickly isolate network segments (Networks responsibility): Installing numerous “valves” on the greater network to reactively stop the spread of malicious software and thwart denial of service attacks by compromised devices at or near the sources could mean a quick recovery and staying in business vs. lengthy outages. This strategy is relatively inexpensive and straightforward, but it must be agreed that it is a capability that will be employed. It could mean disconnecting network segments, MGPs or MHS sites in emergencies where the needs of the many will prevail.
- Adopt a more homogenous environment (Philosophy change, shared responsibility): Microsoft products are targets of, and conduits for, malicious software. Using old, unsupported and un-patched operating systems place the organization at heightened risk. Adopting a short list of supported products and eliminating them when they reach the end of their vendor support cycles would minimize the numbers of vulnerable systems on the network. Enforcement of this strategy hinges on controlling what connects to the network and assigning responsibility for enforcement. There are also cost considerations to retiring classes of devices prior to the end of their useful lives.
- Centralize management and control (Philosophy change, shared responsibility): It is unrealistic to expect individual users and departmental support staff to efficiently apply technical security countermeasures to network devices. The ability to quickly push virus definition updates, service packs and security patches to tens of thousands of networked devices from a central management point is necessary. This implies enhanced central control of network devices and keeping numbers of uncontrolled devices to a minimum.

3. What kinds of trade-offs have you had to make between security and usability, and other operational considerations?

One timely example stems from the implementation of the Cerner EMR across the Mayo Health System sites. Access control is role-based, and the application limits users to one role. Some staff serve in multiple roles, such as nurse and coder, that require different access authorizations. There is no straightforward, efficient way to switch access profiles for a given user, so multiple login identities are required. This in turn raises issues with identity management and directory services.

Another challenge is maintaining individual accountability for access to electronic health information in a highly integrated team medical practice where, for example, a nurse, a physician’s assistant, a medical resident and a staff physician all access a patient’s chart during an encounter. Each individual logging on and off – and multiply this by the number of patients seen per day – is intolerably inefficient. Solutions began with team logons where one account

was shared and the staff physician accepted responsibility for the team's access. More recently custom coded user switching functionality effectively transfers accountability from one team member to another. Unfortunately this is not an option for vended software for which source code is unavailable.

4. What information security standards are you currently using to meet your business needs for system stability and reliability?

Mayo Clinic recently adopted the Sarbanes-Oxley controls intended for financial integrity to more broadly cover core business areas like the medical practice. Separation of duties, change management and security access, authorization and audit controls contribute to enhanced stability and reliability. In addition, Mayo Clinic is performing a cost/benefit analysis of the applicable ISO and SAS 70 standards

Industry best practices for business continuity management are under adoption. These include a phased approach to program initiation, business impact analysis, plan development and implementation, testing and maintenance.

Comprehensive information security policy applicable to all sites and business lines address backup and recovery, business continuity management, anti-virus controls, device security and domain membership, e-mail host security, information integrity controls, network-connected devices, and physical access to computing facilities and equipment.

On the medical front the adoption of standard, identical device configurations has enhanced system stability and reliability as well as the user's experience. Providers who interact with familiar, predictable equipment are better able to focus on their patients.

5. What challenges have you had to address in implementing these standards (e.g., training)?

Organization size, geography, complexity, technical diversity and culture challenge our ability to implement standards. Our experience implementing technology standards is a microcosm of what the nation will experience. With increasing technology changes, implementing technology standards is challenge for any organization to stay a head of.

6. What is the role/value of interoperable information security standards in helping assure system stability and reliability?

All information processing, storage and transmission must address the critical aspects of confidentiality, integrity and availability. The Internet and all connected entities depend upon standard ways of controlling access to everything from bank accounts to online newspapers, controlling authorizations (privileges) to allow some to read an article and others to modify it, and securing connections to prevent unauthorized persons from capturing and reading credit card data. The parallels to healthcare are clear, particularly as organizations attempt to share information for the benefit of patients. With [interoperable information security standards](#), [organizations can rely on other organizations to ensure vulnerabilities are minimal and quickly addressed when exposed.](#)

7. What are the current limitations or gaps in interoperable information security standards with respect to system stability and reliability?

Diversity among existing systems and applications is significant. Large organizations like Mayo Clinic focus on internal standardization largely for quality and efficiency reasons. It is practical for centralized services, such as networks, to adopt security standards. For example, if a device does not support the current wireless networking security protocol it cannot connect and incentive exists for the owner to implement the standard. That incentive does not necessarily exist at the system and application level across business lines. A department may choose not to replace equipment past end-of-life for financial reasons and knowingly or unknowingly expose itself to outages when malicious software strikes for which there is no vendor-provided security patch.

8. What new and emerging issues around system stability and reliability do you foresee over the next 2-3 years?

Power supply and grid dependability is a growing risk area. Demands for power are increasing and taxing the ability to provide it. Uninterruptable power supplies are sometimes not. Localized power outages within the organization occur for various reasons that sometimes seem avoidable. Grid outages are usually more severe and public power infrastructure is increasingly computerized to the point where disgruntled individuals with determination and access have caused problems.

Another emerging issue is increasing dependency upon network and computing assets. Within our organization e-mail was recently classified as a critical function because it is now engrained in workflows to the point where outages have fairly significant impact. Along these lines is the issue of unpreparedness. An outage is not the optimal time to develop alternate processes.

Finally, an existing risk but will emerge in new facets is the education and role of every employee in mitigating the various information security risks. The wide spectrum of awareness and knowledge is so great that any hard control will be limited by the novice employee population.