**IT Governance Meeting**
Wednesday, April 10, 2013
3:00 PM – 4:30 PM
Engineering Conference Room 1-214

**Committee Members:**
Marty Schmidt
Tony Sharon
Armand Doucette
Dan Hastings
Frans Kaashoek
Maria Zuber (not in attendance)

**Guests:**
Mark Silis

**Meeting Minutes:**
Rita Geller

**AGENDA**
Deferred Maintenance Proposal
Mark Silis
Network Security Update
Mark Silis
IS&T Search Process
Frans Kaashoek & Tony Sharon

**IT Governance Meeting Minutes**
Minutes approved from January 23, 2013 meeting.
Next meeting is scheduled for Wednesday, May 22, 2013 in 4-105 3:00 PM – 4:30 PM.

**Deferred Maintenance Proposal:**

The goal of this proposal is to assess and evaluate the infrastructure maintenance costs, looking back over the last ten years and taking into account the usable life of network cabling, network switches, wired and wireless network, optical networks, data center, VoIP, servers and storage (excludes construction costs).

Since 2001, the growth spend has been 45.5M and the maintenance spend has been 16.3M. The majority of the expenditures have focused on adding new services such as wireless, VoIP, data centers, and new buildings. There are competing priorities for the same funds that support both maintenance and growth of the IT infrastructure.

One Potential Plan:

- Replace approximately 20% of the installed switches each year, 400 switches at a cost of $2.1M.
- Replace approximately 33% of the installed wireless access points each year, 1400 APs at a cost of $1M.
- Replace approximately 6.5% of the installed cabling each year, 6500 ports at a cost of approximately $1.65M.
- Replace approximately 15% of the core and distribution network each year at a cost of approximately $1M.
- Replace approximately 20% of the installed VoIP phones each year, 2400 phones at a cost of approximately $600k.
- Replace 25% of the servers and storage at an annual cost of approximately $650k.
• Target approximately $7M of TNSC’s $11M annually in network maintenance. Need to ensure remaining funds adequate for remaining expenditures.

Trends & Challenges:

• Ensuring that we do not lose focus of infrastructure maintenance.
• The increased use of cloud services has a potential impact on our budgets as it shifts capital expenditures into operational expenditures.
• The migration to the x86 platform and use of virtualization have allowed us to continue to sustain our server portfolio with flat funding.
• Storage growth continues at an accelerated rate, driven primarily by server virtualization. This is not sustainable long-term with the current funding and based on current projection we will be faced with difficulty in FY17.

Network Security Update in response to Israel Ruiz’s letter to Academic Council:

April 2, 2013

To Members of Academic Council:

The recent hoax incident of February 23 and hacks to MIT’s information network have given us the opportunity to reassess our emergency preparedness, emergency communication protocols, and network security practices. Today I want to share with you the improvements we are making to our systems and procedures to ensure the safety of our community and the integrity of our campus. I ask that you disseminate this information throughout your respective areas, so that we can build awareness of the important enhancements we are pursuing.

Safeguarding our community

We have upgraded our emergency-preparedness training program, and are reaching out to all parts of our community through our Security and Emergency Management Office (SEMO). It is critical that each department, laboratory and center (DLC) have an emergency coordinator and a concrete emergency plan. SEMO staff will connect with DLCs to provide guidance in crafting and communicating these plans, to share training materials and provide in-person training.

We are also working with housemasters in our residence halls and staff members in the Office of the Dean for Student Life to strengthen the safety of our students and enhance the preparedness of our dormitories and fraternities, sororities and independent living groups (FSILGs).

Reaching people in an emergency

We have revised our emergency communication protocols so that we are able to notify people within minutes of an emergency situation, and are working to expand our addressable alerts system to include all members of our community on all devices. We currently send text-message alerts to all Institute owned mobile telephones and email to all MIT email addresses.

In addition, approximately 60% of our faculty, students and staff have elected to participate in MIT’s
alert program so that they may receive alerts through personal mobile telephones and email addresses.  

*We will be sending email to those who have not yet signed up to urge them to participate in this expanded system of alerts, so that we are able to reach everyone quickly in the case of an emergency.*

**Improving MIT’s cyber security**

With guidance from CSAIL Professor Frans Kaashoek, who serves as technology domain expert for the Information Technology Governance Committee, we have examined how we deliver network services to our community. We have determined that we can modify practices to establish a higher level of resilience for our network while accommodating the needs of our faculty, students and staff.

MIT has a long history of operating an open network environment, allowing devices on MIT’s network unrestricted incoming and outgoing access to the Internet. The Institute remains committed to providing open Internet access to support the core mission of teaching, learning and research, while also providing a more secure network environment for our community.

*In order to provide the community with a more secure network environment, Information Services and Technology (IS&T) will soon implement several changes to our network.* For most of the MIT community, particularly those engaged in research, teaching, and learning activities, these changes to our network will be invisible. Connections to MIT’s communications (email and Web) and academic services (Stellar and WebSIS) will not be impacted. Some administrative users, particularly those who work while away from campus, may see changes to how they interact with MIT’s administrative systems. Questions about planned changes highlighted below can be directed to cybersecurity-questions@mit.edu.

- Network traffic policies are being strengthened. By default, traffic originating from outside MIT’s network (from non-MIT IP addresses) will be blocked to reduce the potential for damage to MIT information systems. This will not impact open services such as email and publicly accessible websites.
- Access to MIT administrative applications such as the Data Warehouse, SAP and MITSIS will require connecting from MIT’s network on-campus (from MIT IP addresses) or by making use of MIT’s virtual private network (VPN) service.
- MIT will implement stronger password quality and expiration policies.
- Those engaged in research, teaching and learning activities will be given the option to opt out of the default network security policy through a self service mechanism.
- Community members requiring access to their computer systems from non-MIT IP addresses are encouraged to use MIT’s VPN service for access rather than opting out.
- Individuals whose work involves access to legally protected or otherwise sensitive information are advised to take additional precautions on devices used for confidential data access, such as use of two-factor authentication and full-disk encryption.

I am deeply and personally committed to safeguarding our community, protecting our campus and securing our systems. Together with our colleagues dedicated to campus safety and security, with the support of senior academic leadership and in collaboration with the campus community, we are deploying all necessary resources to this effort. It will require the dedication of all of us to promote
safety awareness, complete necessary emergency training, and adhere to reinforced cyber security guidelines. IS&T staff members are working with information technology (IT) leadership and partners across campus in making the changes described above. We continue to explore all opportunities to further strengthen our preparedness, and will communicate additional information as these plans evolve.

Sincerely,
Israel Ruiz

Update to the Network Security Roadmap as of April 10, 2013:

• Border protection – Equipment deployed, installed and generating data.
• Network access – Authenticated wireless challenges, re-approach and combine with a network registration process
• Managed user experience – Completed windows domain internal assessment and first phase improvements. Virtual desktop delayed.

The recent events and their impact to the MIT community have provided us an opportunity to step back and review both the security roadmap and other vulnerabilities on our network.

We reviewed specific areas of vulnerability:

• Resiliency of key infrastructure including the MIT web site and DNS
• Resiliency of our network infrastructure to DOS and DDOS attacks
• Passwords as a single authentication mechanism
• Data and application risks such as SAP, Data Warehouse and MITSIS
• Network security and monitoring

Mitigating threats and vulnerabilities:

• Implemented two-factor authentication with Duo Security and integrated with MIT Kerberos.
• Migrated all administrative access to IS&T servers, and core network infrastructure to two-factor authentication.
• Implemented Akamai web acceleration and security for the MIT web site (web.mit.edu and www.mit.edu)
• Migrating MIT external DNS to Akamai to offer high-levels of resiliency and protection.
• Implementing DOS/DDOS protection for the MIT network with Verisign.

Next Steps:

• FAQ is now available on IS&T knowledge base: Campus Network Security (living document with continuous updates).
• Continue to communicate and engage with the MIT community as we work to develop and implement the proposed security improvements.
• Develop “opt-out” mechanism infrastructure and interface components for host firewalling. Pilot for the community to evaluate will be available in May.
• Implement changes for improving security for SAP, Data Warehouse, and MITSIS. Scheduling and implementation will be done with the relevant MIT business units.
• Implement password policy changes and password expirations. Currently targeting certificate renewal time period. The strength of passwords is our weakest part of security.

**IS&T Search Process:**

A selection committee will be convened. There will be representation from Education, Research and Administration.

The first step is in devising the position description. In order to do so a multitude of points of view will need to be gathered. Listening tours to gather input from across the Institute will be conducted. Some of the committee members could each take on pieces of the listening tour. Information can also be gathered from other colleges and universities and the Advisory Council Report. It will be important to look at the job requirements for the last three searches for this position.

A memo will be drafted outlining the process.

**Timeline:**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appoint Selection Committee</td>
<td>April</td>
</tr>
<tr>
<td>Develop Position Description</td>
<td>April - June</td>
</tr>
<tr>
<td>Candidate Search</td>
<td>June - August</td>
</tr>
<tr>
<td>Interviews</td>
<td>August - September</td>
</tr>
<tr>
<td>Selection</td>
<td>September - October</td>
</tr>
</tbody>
</table>