Computing Services
Biennial Report
2008 - 2009
Working as a New Division in a New Setting
Message from the Vice Provost’s Office

August 2010

Carnegie Mellon University has identified information technology (IT) as critically important and supports Computing Services in fulfilling its mission of “enhancing the university’s information technology (IT) infrastructure and providing services that support the university’s research and education missions.” As the central IT service organization, the vision of Computing Services from our 2006 strategic plan is to “strive to be among the best information technology organizations in higher education by continually learning about the rapidly evolving IT needs of research, education, and institutional administration at Carnegie Mellon and how to combine industry-standard production services with innovative solutions to meet those needs.”

We are delighted to share this inaugural “Biennial Report” in which we focus on highlights of Computing Services’ progress in 2008 and 2009 toward goals specified in our 2006 strategic plan. We believe that these successes are built on long-term architectural designs that form a technological foundation, and best practices in project and process management that facilitate the work across and beyond the division. These activities have supported our ongoing development as a unified organization following the merger of Administrative Computing and Information Services (ACIS) and a previous version of Computing Services (“Classic”) in January 2005. The report describes work that is most usually and increasingly accomplished cross-organizationally.

We appreciate the partnership of IT support providers in the schools as well as colleagues in the central administrative offices. These relationships are critical to serving a world-class research university that thrives on distributed governance.

We recognize the unsung heroes who keep IT operations running smoothly and particularly appreciate the Computing Services staff whose consistent performance, spirit of innovation, and dedication to improvement serve a global university every single day. We admire this “learning organization’s” commitment to moving the trajectory “up and to the right.” Their hearts are in the work.

Best,
Carrie E. Regenstein
Executive Director

Joel M. Smith
Vice Provost for Computing
Chief Information Officer
Computing Services

Working as a New Division in a New Setting

The IT world is in a constant state of change. Computing Services must keep pace with these changes in order to support the research, education and administrative needs of the university on a global scale. Significant efforts continue to build effective, efficient and secure information technology services to meet the expanding needs of the global campus.

The information presented in this report covers significant accomplishments of the Computing Services division over the 2008-2009 calendar years. These accomplishments are aligned with the technological goals and themes defined in Computing Services’ 2006 Strategic Plan (see https://www.cmu.edu/computing/about/strategic/2006StrategicPlan.pdf).

1. Redefine services to accommodate an evolving university.
2. Create a secure computing environment.
3. Evolve management strategies and organizational structure.

Mission Statement
Computing Services provides information technology (IT) infrastructure and services to support the research and education missions of Carnegie Mellon.

Vision Statement
Computing Services strives to be among the best information technology organizations in higher education by continually learning about the rapidly evolving IT needs of research, education, and institutional administration at Carnegie Mellon and how to combine industry-standard production services with innovative solutions to meet those needs.

VALUES

- Outstanding service enabling world-class research and education
- A welcoming workplace for the highest quality staff
- Collaboration
- Planning, project management, evaluation
- Initiative and innovation
# Table of Contents

**Message from the Vice Provost’s Office**  i  
**Mission Statement, Vision Statement and Values**  ii  
**Table of Contents**  iii  

1  **Redefine Services to Accommodate an Evolving University** 1  
   1.1  **Academic Technology Services**  1  
   1.2  **Global IT Services**  4  
   1.3  **Modernization of Legacy Infrastructure**  7  

2  **Create a Secure Computing Environment** 13  
   2.1  **Information Security Office**  13  
   2.2  **Secure Integrated Infrastructure**  18  
   2.3  **The Identity Management Program**  20  

3  **Evolve Management Strategies** 23  
   3.1  **Architecture**  23  
   3.2  **Project Planning**  23  
   3.3  **Revitalized attention to Human Resources and Internal Communications** 26  

4  **Goals for Fiscal Year 2013** 27  
   4.1  **Redefinition of Clusters**  27  
   4.2  **Network Cost Model**  27  
   4.3  **Enterprise Applications**  28  
   4.4  **Disaster Recovery (DR) and Business Continuity (BC)**  29  
   4.5  **Authentication Roadmap**  29  
   4.6  **Undergraduate Email**  30  
   4.7  **Service Management**  30  
   4.8  **Computing Services and the Mobile Environment**  31  
   4.9  **Common Practices**  31  

**Acknowledgements**  32
To meet the evolving business needs of the university, Computing Services must redefine services and modernize the legacy infrastructure on which those services are built.

A key goal of the division’s November 2008 reorganization was to enhance our support of teaching and learning. To that end, we created a department whose mission is to focus on “academic technology” support, achieved, in part, through enhanced collaboration with teaching and learning experts on campus.

1.1 Academic Technology Services

Academic Technology Services (ATS) supports the educational mission of Carnegie Mellon by providing and maintaining reliable, usable infrastructure for teaching, learning, and collaborative activities. ATS services include installation and maintenance of technology infrastructure to support teaching and learning, consultation on technology and technology enhanced spaces, support for collaborative technologies, support for events and digital video production, educational programs on computing at Carnegie Mellon, and support for academic leadership in exploring new uses of technology for teaching and learning. These services leverage the overall information technology infrastructure and services provided by Computing Services.

This department focuses on the technology needs of faculty and students, specifically, the technology available in Computing Services’ public computer labs or “clusters” and University Registrar controlled classrooms across campus. The Cluster Services and Media Technology Services groups within ATS work closely with campus academic leadership to ensure that the technology enhanced space and technological needs of the faculty and students are being met. Working with guidance from the Eberly Center for Teaching Excellence, Office of Technology in Education, faculty and students, ATS has begun work to redefine classroom, cluster and instructional services to better suit the needs of their consumers.

- **Redefinition of classroom services**
  As part of a multi-year bond project, Media Technology Services (MediaTech) upgraded and standardized the audio and video presentation technologies in University Classroom Services.
Redefine Services to Accommodate an Evolving University

1.1 Academic Technology Services

Registrar controlled classrooms and auditoriums across the Pittsburgh campus. All classrooms and auditoriums are now equipped with the same updated equipment and user interfaces to provide consistency for faculty and facilitate ease of use. The updated equipment includes new lecterns that offer a touch panel, document cameras, DVD/CD players and ports for laptops and other auxiliary devices.

MediaTech also acts in an advisory capacity to develop a standard audio and video technology experience for remote campuses and department owned teaching spaces. In 2009, MediaTech collaborated with the School of Computer Science (SCS) to develop 18 new SCS teaching spaces within the Gates and Hillman Centers. These facilities were designed, installed and managed as a joint effort in order to integrate some of the MediaTech campus-wide standards for media-rich facilities. This further simplifies the transition for faculty members in the Gates and Hillman Centers providing continuity with other classrooms on campus.

By the start of the fall 2009 semester, MediaTech installed the i>clicker Classroom Response System in all large University Registrar controlled classrooms and auditoriums. The service is jointly supported by the Office for Technology for Education (OTE), the Eberly Center of Teaching Excellence and MediaTech. It is available for installation in all University Registrar controlled classrooms, upon request by interested faculty. The i>clicker technology was also introduced to our Qatar campus. Qatar staff members were trained on the system by their Pittsburgh counterparts through videoconferencing.

- **Redefinition of Clusters or Computer Labs**
  The Cluster Services group of ATS embarked on a multi-year Redefinition of Clusters program. The purpose of the program was to assess the value that Cluster Services brings to campus and to investigate possible improvements that would enhance IT services currently provided for faculty and students. As part of this program, Cluster Services completed several pilots and initiatives including the University Center Web Stations pilot, School of Music cluster upgrades, new SCS Gates Clusters and expanded Andrew printing.

- **2008 MediaTech Statistics**
  - 79 University Registrar Controlled Classrooms
  - 1512 Event Support Requests
  - 105 Classroom Support Requests
  - 201 Pickup Items
  - 560 Network Media Requests
  - 120 Videoconferencing (Qatar)
  - 62 Videoconferencing (non-Qatar)

- **2009 MediaTech Statistics**
  - 87 University Registrar Controlled Classrooms
  - 1221 Event Support Requests
  - 99 Classroom Support Requests
  - 116 Pickup Items
  - 442 Network Media Requests
  - 144 Videoconferencing (Qatar)
  - 84 Videoconferencing (non-Qatar)

◊ In April 2008, five centrally located web stations were installed in the University Center providing convenient access to the web, email and printing. This pilot was sponsored by the Undergraduate
Student Senate. The web stations serve approximately 6300 individuals per semester.

◊ The School of Music has several public computing facilities that are open to all students on campus. These facilities were severely outdated which negatively impacted the teaching and learning activities they support. In a cooperative effort with the School of Music, Computing Services purchased 20 new machines and upgraded the facilities in January 2009 to better support music technology on campus. This included upgrades to both the Margaret Morrison Music Cluster and the College of Fine Arts Editing Suites which are equipped for music technology editing.

◊ During 2009, three new Computing Clusters were created in collaboration with the School of Computer Science (SCS).

◊ In response to student and departmental requests, Andrew printing was expanded to new locations that include: Tepper, SCS and Mudge.

- **Redefinition of Computing@ Carnegie Mellon**
  Computing @Carnegie Mellon (C@CM) is a required course aimed at providing new undergraduate students with a quick introduction to the skills that will allow them to navigate the local computing environment. This was historically a hands-on instructor led course conducted in the computing clusters. During 2009, 58 sections of C@CM undergraduate course were offered, serving 1493 students with a 95% pass rate. To reduce the impact on clusters availability and instructor staffing, ATS explored alternative delivery methods.

  Throughout 2008, ATS partnered with the Open Learning Initiative (OLI) hosted in the Office of Technology for Education (OTE) to plan and develop the pilot of a new hybrid course model for C@CM. The pilot, released in fall 2009, was delivered through a combination of live, hands-on classroom instruction and the OLI’s online course environment. The pilot focused on file storage and sharing where students learned to apply strategies for efficient, dependable and secure file storage and sharing options they are afforded as members of the Carnegie Mellon community. The success of this first phase led to continued collaboration with OLI, the Eberly Center for Teaching Excellence and the C@CM Advisory Committee to develop a complete course to be delivered in fall 2010. This course contains materials on safe and responsible computing and information literacy.

Looking to the future, ATS will continue with this theme, concentrating on infrastructure for instruction, redefining infrastructure services to meet the defined needs and continuing
collaboration with faculty and divisions whose focus is defining those needs. Future projects include the evaluation of video services offered, more efficient methods for software access, and delivery to students and improvements to teaching clusters. All of this work will require continued direction from and collaboration with academic leadership to explore new uses of technology for teaching and learning.

1.2 Global IT Services

Throughout 2009, the newly aligned first line (non-instructional) services of Global IT Services (GITS) worked to ensure that Computing Services delivered a unified support message to the Pittsburgh campus community. Additionally, the department began to enhance relationships with campus partners and internal division development partners in order to provide an improved customer experience. The group continues to lay the foundation to ultimately provide 24x7 global services including Disaster Recovery/Business Continuity (DR/BC) since providing 24x7x365 service includes efficient recovery from disasters so that business processes are interrupted as minimally as possible.

- **Redefinition of Help Center Support Model**

  Over the course of 2009, the Computing Services Help Center began to evaluate and redefine its support models for services. The goal of this evaluation was to find ways to decrease time to resolution by pushing problem resolution to first line support and by providing customers access to self-service tools to expedite resolution. Changes included an updated staffing model, development of internal operational level agreements, enhanced partnerships both within the division and with campus peers and outsourcing of support where it made sense.

  The Help Center staffing model was transformed to eliminate reliance on student employees. The previous dependence on student workers was inefficient, lengthened time to resolution, prohibited the Help Center from handling services that require higher levels of security assurance and was not cost effective. In addition to these direct impacts on service, one full-time resource was dedicated to management of student consultants because of high turn-over. This resulted in a heavy training burden and sporadic work schedules. The new full-time staffing model positions the group to better balance workload, cross-train the team, and raise the confidence of second level support groups. These factors have significantly freed Help Center staff hours to allow them to obtain a deeper level of product knowledge ultimately enabling the group to reduce the need for second level problem escalation; more problems are resolved on first customer contact. Additionally, the group has become more involved in the implementation and development phases of projects, representing support concerns and advocating for customers earlier in the process.
• **Service Evaluation**
In addition to changing the base staffing model in the Help Center, a focused evaluation of resource time revealed that a substantial number of Help Center resource hours were being consumed by requests for assistance in rebuilding infected machines. This was a costly business that did not make the most efficient use of limited Help Center resources and involved staff in a level of personal computer repair for students and faculty that was not scalable with current resources. Computing Services worked with the University Store to leverage their existing relationship with a third party vendor to negotiate and successfully outsource software and virus repair services in fall 2009. Although the Help Center continues to provide high level diagnostic support for machine failure, customers are now referred to the University Store for access to third party repair services when their machine needs to be cleaned and rebuilt.

• **Operational Level Agreement**
To enhance the Help Center’s ability to resolve issues quickly, Computing Services initiated a project to have its directorates or departments develop Operational Level Agreements (OLA) that clearly define organizational support responsibilities and escalation paths. OLAs were written for the Andrew Printing service, C@CM, ISO Incident Management Support, Oracle Calendar and Wireless Andrew. An added benefit of the OLA was an increase in knowledge shared between secondary application support groups and the first line support team in the Help Center. This ultimately resulted in improved resolution time for Computing Services’ clients. Following implementation of the Calendar OLA, the Help Center resolutions increased significantly over 2008 and 2009. Also, there was a marked decrease in the number of inquiries that required escalation to second level support.

The OLAs are one step toward the Help Center’s goal to implement a knowledge centered service strategy that will better position the group to provide quality service any time, any place. Continued staff involvement and development will allow this first line support group to build solution data in its ticketing tool and manage support knowledge to improve customer resolution time, self-service and satisfaction.

• **Partnering for Improvement**
Since Carnegie Mellon’s governance is highly distributed, outstanding service can only be provided through strong partnerships between central and local IT support providers. Computing Services redefined existing relationships with the Departmental Computing Effort (DCE) and the Student Advisory Council (SAC) and continues to work with these groups to gather campus insight.

Additional relationships have been fostered with IT help representatives across campus through the formation of the Federation of Service Centers. IT service representatives from the School of Computer Science (SCS), Software Engineering Institute (SEI), Electrical and Computer Engineering (ECE), and Tepper School of Business were brought together for a discovery effort to explore unified service tracking and knowledge base solutions. This group has a strong interest in exploring methods to enable expedited escalations of incidents and knowledge.
sharing across campus IT service centers. Projects are underway to further investigate tools and processes to support development of rich information sharing across IT service centers and the campus community.

Computing Services also continued its monthly meetings with directors and key staff of all major distributed IT support organizations including SCS, ECE, Tepper, the SEI, and the Pittsburgh Supercomputing Center (PSC). These meetings have created more active collaboration among these groups on services ranging from email to virtual private networking to information security.

- **Increased focus and dedication to Disaster Recovery and Business Continuity**
  The goal of the Disaster Recovery and Business Continuity (DR/BC) effort is to develop plans, methodologies, and infrastructure that will allow the university to carry on key business processes in the event that the primary systems that support those business processes are unavailable for a prolonged period of time. Sensitive to the fact that development of a business continuity plan requires significant resource commitment from business units across campus, Computing Services decided to direct its initial focus on an IT centric approach, focusing mostly on the disaster recovery aspects of DR/BC.

  The discussions surrounding the initial DR effort focused on three areas: infrastructure, process and operations.

  ◊ **Infrastructure**
  Computing Services determined that the current DR facility cannot adequately provide sustained service to multiple key university business units in the event of a prolonged outage of the university’s primary data center. For this reason, the infrastructure component of this effort has begun work to provide the current DR equipment with a better interim home that will afford additional capacity for development of new DR solutions. In parallel, work has proceeded on designing the long-term solution. This could involve making the interim solution permanent or seeking some alternative.

  ◊ **Process**
  At the core of the overall DR/BC effort is the DR process. The division has identified key university applications and services and developed a preliminary DR process. Work is underway to assess, implement and test this process on the first key application. After completing the cycle on the first application, the process will be re-evaluated and improvements made before moving on to the next key application. This process will be repeated until the DR infrastructure for each pilot service has been built in the interim DR site.
Operations
Throughout the development of this process, the division realized that there is significant work required to “operationalize” the DR effort within Computing Services. As the division pilots the DR process with key applications, plans are in place to document the process and best practices for future expansion into DR/BC efforts both within and beyond the division.

The DR/BC team will continue to work with departments internal to Computing Services to develop the plans, methodologies and processes that will eventually make DR planning a standard operating practice. Once this work is established the group will reach out to business units to evaluate and build continuity plans for critical business functions.

1.3 Modernization of Legacy Infrastructure
Providing secure and robust IT support for a global university requires a robust IT infrastructure. In 2008, Computing Services brought to completion five bond projects ($12.5m) that helped lay a foundational infrastructure that will support more contemporary IT services.

Services Oriented Architecture
Modularization of software services and the provisioning of those services across the Internet is an emerging trend in information systems. Services Oriented Architecture (SOA) is one set of design and implementation strategies designed to facilitate such modularization. SOA is founded on writing software code that is modularized in the sense that it responds to standardized requests from other code that consumes the services it provides. This contrasts with current practices in which the bits of code exchanging services are typically designed to support that unique exchange, creating a condition of “tight coupling” of much of the code in large scale systems. This tight coupling limits flexibility in changing and upgrading systems. Computing Services recently partnered with third party consultants in a multi-year plan to develop a new suite of services that will replace our current Student Information System (SIS)—and these services are based on SOA and on other strategies designed to make our systems more flexible and less expensive to upgrade. The multi-year project is evolutionary: service needs are prioritized and implemented in steps, addressing the needs of campus through software development or acquisition within a modularized framework that will serve Carnegie Mellon well into the future.

Tiered Separation of Applications
The division made significant strides to implement new architecture strategies for the separation of applications within our infrastructure. Using a tiered approach, application performance, security, and our ability to comply with auditable IT processes are significantly enhanced. The work involves three different kinds of separation: separation of disparate business applications onto separate servers; separation of development, testing, and production instances of the same application; and tiering of the fundamental layers of a particular application. In the past, applications that spanned various business functions resided on one server, as did the instances of an application used to develop modifications, test those modifications, and run the application in production. Also, the separable pieces of an application, namely the web front end, the application itself, and the
In the mid-1980s, the Andrew Project was first launched at Carnegie Mellon's Information Technology Center in cooperation with IBM. The purpose of the project was to develop a cutting-edge distributed computing environment, portions of which have been in use at Carnegie Mellon ever since. The parts of the environment still in use consist of the Andrew File System, modified versions of UNIX and Linux operating systems, and other associated infrastructure for supporting these operating systems. Because
the Andrew operating system environment is reliant on an outdated infrastructure, build, and configuration mechanism, Computing Services felt it necessary to replace this component with one that was more modern and sustainable.

In response to this need, a completely new management infrastructure was developed and implemented called “Andy III.” Andy, or Andrew III is Computing Services’ next-generation server management system. It is based on a standard RedHat Enterprise Linux 5.x operating system and offers multiple significant benefits, including:

- Use of a standard, well-known operating system which minimizes the learning curve since many system administrators across campus have previous experience with RedHat.
- Support for various commercial software that is easier to obtain; installation is also faster and easier.
- Simplers deployment of vendor patches to Andy III systems. This includes operating system and application-level security patches that will result in Andy III systems that are inherently more secure.
- Support for installing and upgrading particular software packages without upgrading the whole system. This is important in dealing with the reality of different development and testing procedures across the organization.
- Support for system inventory and auditing.

In addition to being built with a core RedHat 5.x operating system, Andy III allows for management of some or all local files configured on server machines. It also ensures that multiple systems of the same type maintain the same configuration. This consistency in configuration of servers allows for more robust services for our customers.

Virtualization of Servers

Adoption of virtualization technology is transforming the way that Computing Services provides computing resources and the way it is modernizing its infrastructure. Virtualization technology provides the ability to run multiple virtual (aka guest) machines on a single physical machine. Previously, hardware was only capable of running one operating system; therefore, the hardware and processing power of a given server was largely underutilized.

Initiative and Innovation

Core Administrative Computing Applications

<table>
<thead>
<tr>
<th>Enrollment</th>
<th>Human Resources/Payroll</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Student Information System</td>
<td>• Human Resource Information System/ Human Resource Employee Module</td>
</tr>
<tr>
<td>• Student Services Suite</td>
<td>• Benefits</td>
</tr>
<tr>
<td>• QSIS</td>
<td>• Talent Management System</td>
</tr>
<tr>
<td>• Student Health Services</td>
<td>• ADP</td>
</tr>
<tr>
<td>• Academic Audit</td>
<td>• Learning &amp; Development</td>
</tr>
<tr>
<td>• Faculty Information Online</td>
<td>• HR Data Warehouse</td>
</tr>
<tr>
<td>• Student Information Online</td>
<td>Other</td>
</tr>
<tr>
<td>• Online Registration</td>
<td>• Credit Card</td>
</tr>
<tr>
<td>• Course Information Online</td>
<td>• SpaceQuest</td>
</tr>
<tr>
<td>• Faculty Course Evaluations</td>
<td>• Resource25</td>
</tr>
<tr>
<td>Finance</td>
<td>• Maximo</td>
</tr>
<tr>
<td>• Oracle Financials</td>
<td>• UGrant</td>
</tr>
<tr>
<td>• Oracle Web Reports</td>
<td>• Advance</td>
</tr>
<tr>
<td>• Applications Desktop Integrator</td>
<td></td>
</tr>
<tr>
<td>• Financial Data Warehouse</td>
<td></td>
</tr>
</tbody>
</table>
By December 2009, the capability to run approximately twelve or more virtual guest machines (i.e., independent operating systems) on one physical server was adopted. This ability to scale/grow guest virtual machines maximized efficiency through the use of 509 virtual machines.

The benefits of virtualization include:

- **Improved utilization of data center hardware.** Virtualization allows multiple operating systems to run simultaneously—by merging multiple physical servers together, the utilization of our physical hardware has increased dramatically.

- **Higher availability, better redundancy, and improved performance for customers.** In most situations, virtualization technologies allow our systems to automatically recover from outages. This lowers the recovery time needed in these situations. It also allows for network and storage multi-path redundancy, preventing problems or outages that might otherwise have occurred.

- **More efficient deployment capabilities.** Through virtualization, we have mechanisms that provide application or operating system based templates. These templates allow us to deploy new servers within an hour, versus the previous, lengthy process needed to procure and build dedicated physical boxes.

- **Reduced capital costs.** Merging multiple operating systems on a single set of hardware allows us to streamline our operations. This simplifies maintenance, purchasing, and other operational procedures.

- **Improved energy efficiency.** Potentially, we can reduce our power consumption by half through using virtualized (aka guest) servers.

### Wireless Andrew 2.0 (Bond Funded Project)

In 1998, Carnegie Mellon gained recognition for establishing the first wireless network on a university campus. Ten years later, we broke new ground with the Wireless Andrew 2.0 project. Through Wireless Andrew 2.0, our network team worked with hardware vendors Aruba Networks and Xirrus to update Carnegie Mellon's wireless network to higher speed 802.11n technology. The project spanned the 79 buildings and 4.2 million square feet of the Pittsburgh campus to replace all wireless access points with new equipment that supports the 802.11n standard. Where the previous network offered throughput speeds of between 11-54 megabits per second (Mbps), the upgraded

### Bond Projects

**Instructional Support**
- Classroom technology upgrades

**Network**
- 10 GIG backbone upgrade
- IBM cabling replacement
- Wireless Andrew upgrade

**Data Center**
- Present data center remediation

---

**Virtualization of Servers** is the process of dividing one physical server into several, separate virtual servers to maximize efficiency.
network allows up to 300 Mbps with a norm of 100 Mbps, matching or even exceeding performance of some parts of the campus wired network. By increasing the original 1093 access points to over 3000, we also improved or eliminated spotty coverage areas.

**IBM Cabling and Backbone Upgrade (Bond Funded Projects)**

To support wired network technology, IBM cabling was replaced with Cat5e cabling in Baker Hall and Mellon Institute. Cabling in the Cyert Hall A-100 data center, where hundreds of computers that serve the campus’ centralized services are housed, was also upgraded. Also in the data center, cabling was moved to overhead trays that carry structured copper and fiber optic cabling. To assure uninterrupted power, a new emergency generator was installed. Overall, the Cyert Hall data center renovation increased redundancy, capacity, and functionality. To meet expected increases of bandwidth consumption in the future, the backbone network infrastructure and most building uplinks were upgraded from redundant 1 gigabit per second to redundant 10 gigabits per second wiring and electronics.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>A-100</th>
<th>A-84</th>
<th>Penn Ave</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>529</td>
<td>97</td>
<td>10</td>
<td>636</td>
</tr>
<tr>
<td>Storage</td>
<td>86</td>
<td>6</td>
<td>19</td>
<td>111</td>
</tr>
<tr>
<td>Switch</td>
<td>115</td>
<td>30</td>
<td>5</td>
<td>150</td>
</tr>
<tr>
<td>Other</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>14</td>
</tr>
<tr>
<td><strong>Total Devices</strong></td>
<td><strong>737</strong></td>
<td><strong>140</strong></td>
<td><strong>34</strong></td>
<td><strong>911</strong></td>
</tr>
</tbody>
</table>

Figure 2: Cyert Hall Data Center Equipment Overview
August 2009
Carnegie Mellon is an internationally recognized leader in computer security, through its research and information programs in cyber security, survivable systems, computer security incident response, and policy. In August 2004, the Information Security Office (ISO) was established with dedicated resources to coordinate and sustain an information security program to address vulnerabilities and risks to information and technology infrastructure across campus. Since the inception of the ISO, the division has aggressively taken steps to move from a default open to a default “protect” infrastructure and to address the need to reduce decentralized storage of sensitive data. Computing Services continues to deliver and evolve services to improve security and reduce institutional risk. The following accomplishments have enhanced the security of the computing environment and helped address current compliance standards and policies.

2.1 Information Security Office

Incident Response

The Information Security Office managed twelve major security incidents between November 2008 and February 2009 alone. Although these incidents consumed more than 650 ISO person hours, they afforded the opportunity to refine the ISO’s forensic methodology, identify additions for the developing roadmap of projects designed to improve security and define standard operating procedures for analysis involving data breach notification.

Incident Detection

From 2008-2009, the ISO Security Engineering and Operations team expanded their Intrusion Detection System (IDS). This system monitors various points on the university’s network for evidence of attack and compromise and alerts incident responders. The diversity of the campus computing environment creates a broad attack surface with ample vectors for attack as depicted in Figure 3.
In 2009, the Open Source Security Host-based Intrusion Detection System (OSSEC HIDS) was deployed as a pilot within Computing Services. The OSSEC application is an additional defense mechanism as it monitors systems and reacts as appropriate and defined for each event.

**Incident Prevention Tools**
Information security for individuals begins with the First Connect web site. All users connecting to the Carnegie Mellon network for the first time are directed to this site where, through a step-by-step process, they register and secure their computer. Faculty, staff and students are also encouraged to mitigate identity theft and data leak risks through the Identity Finder tool released to campus in 2008. Originally a Windows-only tool, the ISO released the Macintosh version in the fall of 2009. A surprising amount of sensitive Personally Identifiable Information or (PII, e.g., passwords, credit card numbers, and social security numbers) may be retained on a computer simply from daily use along with personal and work

<table>
<thead>
<tr>
<th>Networks</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 578 subnets</td>
<td>• ASP, JSP, PHP, Perl, C, Java</td>
</tr>
<tr>
<td>• Wireless and Wired</td>
<td>• Oracle, MySQL, SQLServer, Ingres, Interbase</td>
</tr>
<tr>
<td>• Cisco, Aruba Xirrus</td>
<td>• Tomcat, JRUN, JBOSS</td>
</tr>
<tr>
<td>• 3 VPN services in Computing Services</td>
<td>• Custom and Commercial</td>
</tr>
<tr>
<td>• Limited separation of clients and servers</td>
<td>• Open and Closed Source</td>
</tr>
<tr>
<td>• Limited filtering at our border(s)</td>
<td>• No Secure Software Development Life Cycle (SDLC)</td>
</tr>
<tr>
<td>• No “clean access”</td>
<td>• Limited change control</td>
</tr>
<tr>
<td>• No Media Access Control (MAC) spoofing protection</td>
<td>• 30,188 PHP attacks</td>
</tr>
<tr>
<td>• Limited rogue network service detection</td>
<td>• 240 SQL Injection attempts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Systems</th>
<th>Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 15,314 active IP addresses on campus (Windows, Linux, HP-UX, Solaris, etc.)</td>
<td>• 28,579 Andrew accounts</td>
</tr>
<tr>
<td>• 4,187 Web servers (Apache, IIS, Tomcat, Netscape, etc.)</td>
<td>• Double that for Active Directory</td>
</tr>
<tr>
<td>• 4,473 SSH servers</td>
<td>• Add in application accounts</td>
</tr>
<tr>
<td>• 465 FTP servers</td>
<td>• At least five different authentication sources in Computing Services</td>
</tr>
<tr>
<td>• 331 Database servers (Oracle, MySQL, MS-SQL, Ingres, etc.)</td>
<td>• No group membership auditing</td>
</tr>
<tr>
<td>• 1,707 FTP attacks</td>
<td>• File system Access Control Lists are not audited or detailed</td>
</tr>
<tr>
<td>• 1,220 Web include file attacks</td>
<td>• 1,509,553 SSH attacks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applications</th>
<th>Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Oracle, MySQL, SQLServer, Ingres, Interbase</td>
<td>• 30,188 PHP attacks</td>
</tr>
<tr>
<td>• Tomcat, JRUN, JBOSS</td>
<td>• 240 SQL Injection attempts</td>
</tr>
<tr>
<td>• Custom and Commercial</td>
<td>• 30,188 PHP attacks</td>
</tr>
<tr>
<td>• Open and Closed Source</td>
<td>• 240 SQL Injection attempts</td>
</tr>
<tr>
<td>• No Secure Software Development Life Cycle (SDLC)</td>
<td>• 30,188 PHP attacks</td>
</tr>
<tr>
<td>• Limited change control</td>
<td>• 240 SQL Injection attempts</td>
</tr>
<tr>
<td>• No group membership auditing</td>
<td>• 240 SQL Injection attempts</td>
</tr>
</tbody>
</table>

Figure 3: Attackers and Attack Surface
files. This tool assists in preventing identity theft by finding Personally Identifiable Information and providing a means to easily and quickly protect or securely dispose of it. It also lowers the university’s risk by allowing data that is subject to breach notification to be removed or redacted before it can be compromised.

In addition, vulnerability scanning and monitoring expanded in 2008 as a self-service to campus departments and their computing systems through the distribution of the commercial tool called Nexpose. Departmental administrators use this tool to proactively scan for vulnerabilities on their locally managed computers and networks. The results enable them to prioritize patching and other remediation activities with the goal of avoiding a costly compromise.

**Security Assessment**

Working with the university’s contract office and other units within Computing Services, the ISO iterated its security assessment methodology and contract review process with regard to Software as a Service (SaaS) vendors. The ISO performed over thirteen security assessments including attack and penetration of prospective and operational third party application solutions. These assessments identify vulnerabilities and provide an opportunity for remediation before they are exploited in a production scenario. They provide a great opportunity to deliver security awareness content to application and infrastructure providers. Ultimately, these assessments increase institutional confidence that sensitive data is being managed appropriately by those entrusted to protect it. When all else fails, the contract provisions developed and reviewed by the ISO as a partner to the contracts office, provide for the requisite audit and response activities and serve as a model for other institutions.

**Training and Awareness**

Through security classes like Malware Removal, Security 101 and Identity Theft, faculty and staff were made aware of the importance of security. In addition, security awareness content was made available in 2009 through the ISO and Computing Services web sites. Topics included: File Sharing and Digital Copyright, Brute-force SSH Attacks, Spyware and Social Engineering Using a USB.

In June of 2009, approximately 70 technical staff from various campus departments attended the ISO sponsored SANS DEV 422 Web Application Security Essentials class. This class provided instruction aimed at improving security for servers and applications that are not centrally maintained.

As shown in Figure 4, there has been a steady downward trend in network suspensions for “vulnerability” i.e., computers that have been removed from the campus network because they are vulnerable to compromise or infection. The ISO attributes this trend to a more educated and responsive campus community and to successful communication campaigns regarding the need for timely patching. The ISO is the designated Digital Millennium Copyright Act (DMCA) agent for the university, responding to all incoming infringement notices from copyright holders or their representatives. The number of copyright violations reflects
the number of infringement claims received and processed by the ISO. Since the processes used to generate these claims vary, few conclusions can be drawn from trend analysis. On the other hand, trend analysis of general suspension data is more meaningful especially in light of other trends like attack profiles and user behaviors. In general, there has been a downward trend in suspended computers. Increased use of anti-virus software, timely patching, and tools like First Connect coupled with proactive security alerting and general security awareness communications, explains some of this trend. Changes in attack profiles, such as automation, botnets, and spear phishing contribute as well. The spike in 2009 can be attributed in large part to a couple of incidents that impacted hundreds of computers each. An infected USB drive was the culprit in one case and a compromised administrator password was the culprit in the other.

**Policy and Compliance**

As part of the security policy roadmap, the university implemented a new Information Security Policy (see www.cmu.edu/iso/governance/policies/information-security.html) in December 2008. The ISO also published Guidelines for Data Classification, Guidelines for Data Protection and Information Security Roles and Responsibilities.

The Guidelines for Data Classification establish a framework for classifying institutional data based

![CIA Triangle](image)

*Figure 5: CIA Triangle*
on its level of sensitivity, value and criticality to the university as required by the university’s Information Security Policy. Classification of data will aid in determining baseline security controls for the protection of data. Guidelines for Data Protection define baseline security controls for protecting Institutional Data in support of the university’s Information Security Policy. Finally, Information Security Roles and Responsibilities clearly define roles and responsibilities that are essential to the implementation of the university’s Information Security Policy.

E-Discovery Support
Infrastructure to support content preservation search and production for legal purposes, often termed “e-Discovery,” was developed during this period as well. Improvements include: content aggregation, faster search capability and secure storage for the nearly 200 accounts subject to litigation hold.

Participation in the Enterprise Risk Management Program (ERM)
In the fall of 2007, the Office of General Counsel and the Chief Financial Officer launched a university initiative to develop a more formal Enterprise Risk Management (ERM) strategy for the university. ERM is the process of identifying, understanding, prioritizing and managing risks. By 2008, the University Compliance and Risk Committee (UCRC) was created. The UCRC is co-chaired by the Office of General Counsel and the Chief Financial Officer and is comprised of leaders from key functional administrative units who participate in sub-committees focused on the following areas: safety and security, student services, research, finance and administration.

Representatives from the Vice Provost’s Office (VPO) and ISO participate on the Administration Sub-committee on behalf of Computing Services. The focus of this sub-committee for much of 2008 and 2009 was on prioritizing compliance risks to the university. Computing Services identified compliance risks within the division, developed mitigation strategies for those risks and continues to report status of these mitigation strategies to the UCRC.

In late 2009 and early 2010, Computing Services worked with the UCRC to identify an initial set of operational risks and developed risk mitigation strategies for these risks. Many of these mitigation strategies pointed to division projects that were already in place to address these operational risks, such as the Identity Management and Disaster Recover and Business Continuity programs.

The UCRC is moving forward with the identification of operational risks across university business units. Computing Services continues to participate by working to identify and discuss division operational risks and possible mitigation strategies.
2.2 Secure Integrated Infrastructure (SII) Program

As Computing Services has grown to accommodate the expanding technology needs of the university, it became increasingly important to consolidate our technical infrastructures and develop and maintain a secure scalable production environment for systems and applications. The Secure Integrated Infrastructure (SII) effort was instituted to develop a secure computing environment and supporting process that complement the work underway to upgrade legacy infrastructures. As aged production environments are evaluated for modernization, security and future upgrade capabilities are evaluated and implemented as part of the newly designed SII environment.

The need for a focused SII effort is a bi-product of the 2005 merger of the ACIS and Computing Services organizations. In 2007, Computing Services began discussions surrounding the need for a plan to consolidate and secure our infrastructure and networks. As our technical infrastructures grew to accommodate expanding business challenges, the division found itself with a number of technical architectures which were not working in the most effective or secure manner. The decentralized environment lacked the necessary security controls to implement a default protect policy. With this increased awareness, the division made great strides throughout 2008 and 2009 toward building a secure infrastructure. Applications were initially migrated to an interim network that was firewalled and configured to deny external access...
by default. This initial prototype provided valuable insight for the development of the current SII environment, but presented scalability issues.

Today, the SII environment consists of a set of firewalled networks that are organized into sections. The networks are configured by default to deny access from one network to all others. Access across networks and from the external Internet is evaluated and configured based on the business requirements and data classification of the content. This provides granular control in regard to network and infrastructure access and allows for increased security precautions for our enterprise data and applications. For example, one network may permit traffic from the Internet where another requires Virtual Private Networking (VPN) access for off-campus access or 2-factor authentication for administrative access.

Now that the SII environment model has been enhanced, efforts are underway to migrate legacy applications and infrastructure from the Computing Services’ Classic and Administrative Computing (AC) networks. In 2009 approximately 75% of the infrastructure components were moved from the Classic to the SII environment and new and updated applications were placed directly into SII. Applications are no longer being placed on the Interim or Classic networks, and the next phase is to move those remaining applications to the SII environment.

SII - People, Process and Technology

The SII program is not merely a set of networks but a true integration of people, process and technology. Computing Services has made a commitment to SII by allocating cross-division resources to contribute to its success. In 2008 the division designated an SII lead as a full-time resource to support and drive the program.

The SII team is engaged in continual process improvement and devoted much of 2009 to revisiting and redefining the initial SII pre-production review process. SII consultants are now available earlier in the process to provide guidance and support for project leads as they develop the technical documentation necessary to make a viable submission for review by the SII audit team. The SII program is steadily becoming standard operating procedure for the division and its success will serve as a model for future initiatives.

What’s next?

In 2010, the SII team will continue to move the remaining 25% of our Classic infrastructure into the SII environment. Additionally, those applications that were part of the Interim SII will be migrated to the SII networks as well.

To support the program, development of SII design rules and principles is already underway. The SII principles will serve as guidance for decisions made on new projects and updates to existing infrastructure and applications. The principles will be living documents intended to educate both SII team members and division staff regarding the expectations and objectives for deployment in the SII production environment.
2.3 Identity Management Program (IdM)

End-user service needs and expectations continue to grow. In the contemporary environment, it is essential to ensure that services are provided only to end-users who have been authorized for access to specific services. To do so requires ensuring an enterprise identity for each end-user. To provide efficiencies, it also requires the ability to group end-users in their access to service (e.g., based on the role they fulfill at the university).

Great strides were made in 2008 and 2009 as Computing Services defined and developed an overall Identity Management (IdM) Program to streamline the secure provisioning of disparate services to end-users.

Sun Identity Manager System

The Sun Identity Manager system generates basic accounts for Carnegie Mellon students, faculty, staff, departments and university guests and affiliates. A basic account includes an Andrew username, password, email box and access to common services (e.g., network registration, file storage). It provides the appropriate permissions based on a person’s role and dynamically ensures they can access the services and resources to which they are entitled. It is also flexible enough to change as a person’s role changes.

Prior to 2008, accounts were generated by an in-house system that was difficult to maintain. The new IdM system offers modern account and role provisioning functionality and is maintained by Sun Microsystems (now Oracle Corporation).

Laying the foundation with the Sun Identity Manager system, we were able to:

- **Integrate Active Directory Passwords with IdM**
  In August 2008, Computing Services deployed the Sun Identity Manager system to streamline the change password process and improve security for Andrew passwords and Active Directory passwords used to log into Windows machines. At the same time, the Andrew password policy was set for those who access enterprise applications: Oracle Financials (OF), Student Information System (SIS), Human Resources Information System (HRIS) and Property Accounting System (PAS). Anyone with access to these systems is now required to have a strong Andrew account password. IdM verifies that the password choice meets the defined password requirements. This was the first of several security improvements.

- **Implement Single Sign-On for Enterprise Applications**
  In September 2009, a single password replaced multiple passwords for enterprise application access. Previously, those authorized to access multiple applications (i.e., SIS, HRIS, PAS) had a different password for each service. Through this project, a single password was implemented. A strong password policy was also applied to maintain security of the enterprise applications. It ensures that the chosen application password meets consistent and strong strength requirements. To meet certain compliance requirements, this password also expires and needs to be reset quarterly.

- **Apply Andrew Password Strength**
  Carnegie Mellon students, faculty and staff use their Andrew username and password to access various campus services and resources (e.g., email, calendar, course registration, Blackboard). Prior to December 2009, account holders were encouraged to set a strong password. However, the system did not check the individual’s password choice, except in the case of those accessing enterprise applications (i.e., OF, HRIS, SIS, PAS).
The Andrew Password Strength project set a password policy and the Identity Management system verifies that the password choice meets the defined password requirements. A stronger password for all Andrew account holders improves the overall security of information, computing and networking at Carnegie Mellon.

- **Join InCommon**
  Carnegie Mellon has joined other universities, government organizations and companies as a member of the InCommon Federation. Membership is an essential step in allowing Carnegie Mellon students, faculty and staff to use their Andrew username and password to access services provided by other federation members. Similarly, Carnegie Mellon will be able to offer reciprocal services to constituents of federation members.

Membership in a federation such as InCommon means abiding by a specific set of identity management practices. Our updated password policy (December 2009) is an important step to meeting these compliance requirements. A future step is certification. The certification process is meticulous, but recent security accomplishments are the first step on the path toward certification.

- **Transition Middleware Infrastructure to Oracle**
  Following the announcement of Oracle’s acquisition of Sun in late 2009, preparations have begun to transition the Sun Identity Manager module to the Oracle Identity Manager module. Oracle is now beginning to assist in defining a migration path. In the meantime, work continues on the IdM roadmap plan, which is developed and reviewed in collaboration with campus partners.

**Looking to the Future - Identity, Authentication, and Access Management (IAAM)**

The initial Identity Management program focused on the need to establish authenticated identities and associated roles. This program is beginning to evolve into the Identity, Authentication, and Access Management (IAAM) initiative that takes identity management a step further to include authentication and authorization. IAAM focuses on the stages of the university relationship following the life cycle of an individual identity from prospective student, employee or faculty to alumni or retiree. Through the IAAM life cycle, an identity is established, authenticated and then authorized. Authentication requires individuals to prove their identity and role within the organization; based on that role, entitlements are then granted or authorized.
As a technology organization serving a sophisticated university community, it is our responsibility to base IT planning on a sound architectural roadmap implementing technologies that satisfy the evolving needs of our clients. This architecture must also fulfill our commitment to develop a sound and secure environment that is consistent with industry standards. The organizational separation of the Architecture and Project Planning and Management units allows us to proactively focus on technology leadership for the university.

3.1 Architecture

Senior architects work closely with senior management to develop a technical roadmap for the division that addresses the projected needs of our global campus three years into the future. Annual white papers and other artifacts focus on system integration, identity and access management, infrastructure choices, and consistency for an environment that supports robust systems and interoperable applications. The current roadmap identifies strategic goals related to authentication, infrastructure security and identity management. The annual architecture white paper provides the tool to ensure the division’s alignment with strategic goals.

Senior architects are now engaged earlier in the development process during the proposal review stage including deep engagements for enterprise projects such as HRIS, Enterprise Service Bus (ESB), IdM, Student Services Suite (S3) and the internal audit group. This early involvement institutes a conscious evaluation of the security, infrastructure design and standards implemented for new technology. Their external partnerships with peer institutions keep the division abreast of industry trends and standards that should be considered as we plan for the future.

Throughout 2008 and 2009, the Architecture team was instrumental in initiating the SII effort, designing the IdM and Authentication Programs, and helping to define ESB Governance. Senior Architects also served on IT planning teams with vendors.

3.2 Project Planning

The Planning and Project Management Office (PPMO) supports Computing Services’ commitment to more structured planning and project management. The PPMO helps the
division select projects that best meet its strategic goals and maximize the use of division resources. To support the successful implementation of this work, dedicated project managers are assigned to complex programs that span multiple departments and involve external customers. For smaller initiatives, project managers serve in a consulting capacity.

**Project Management Methodology**

Established in 2003, the PPMO has steadily grown and empowered division staff to use standardized processes and tools to effectively plan, manage and analyze the project portfolio and operational work. The initial project management methodology was built on process and templates from peer institutions, particularly the Massachusetts Institute of Technology and Princeton University. During the management of the five IT infrastructure bond projects from 2005-2008, the PPMO instituted a more formal planning phase and rigorous review schedule for project management. This enhanced project management model was instrumental in the delivery of five bond projects worth $12.5 million on time and within budget. The bond projects were a prime example of the division's dedication to project management for large projects. This effort was a key factor in the development of a new baseline project management methodology for the division.

In 2009, following the bond projects, the PPMO released a full Project Management Methodology (PMM) based on a modified Project Management Body of Knowledge (PMBOK) model. The updated process incorporates improvements to project submission, consultation for project management and architecture, a division-wide open comment period, reviews of resources and strategic alignment,

---

**Figure 8: Project Planning Process**
and final Vice Provost’s Office (VPO) review and approval. (The VPO includes the CIO/Vice Provost and the Executive Director.) This methodology is a true cross-functional effort that has proven to be invaluable in our pursuit to build internal partnerships and operate as a cohesive unit working toward a common goal.

Supporting the Planning Process
Evaluation and selection of a standard tool for project management tracking and analysis was completed in 2009 and a software tool, Team Dynamix was chosen. The tool was integrated with the new PM methodology to facilitate the process of vetting and approving project requests. In a continued effort to support staff and the division commitment to sound project management, the PPMO conducted internal training and education sessions throughout the summer of 2009. These training sessions focused on both the new methodology and minimum project documentation requirements within the Team Dynamix tool. These minimum requirements include a project plan, resources, budget and monthly status reporting.

Governance
The PPMO purview has expanded to include work with external business partners across campus. The Executive Steering Committee on Computing (ESCC) provides information and advice to help Computing Services plan the schedule for the portfolio of critical enterprise level projects. (Members of the ESCC include the Provost, all the Vice Presidents, two Deans, and a representative from the Administrative Leadership Group (ALG).) Computing Services leadership works with the ESCC to develop technology commitments based on the strategic plan. These commitments are then extracted to a roadmap of specific project efforts to meet these goals. This allows the Vice Provost’s Office to sequence and execute the university’s mission-critical applications while considering staff resources within both central IT and impacted business units.

Service Portfolio
In 2008, the PPMO developed a Service Portfolio that identifies the work or services that Computing Services offers to the campus community. A well defined service portfolio will increase Computing Services’ credibility within the university, assist with management of budgeting, productivity and operations and help to address compliance issues. The first phase of development focused on external-facing services to demonstrate our range of activities to customers, partners and executives. The current portfolio defines service attributes including description, support contact, access rights, availability, and applicable service fees. The portfolio facilitates development of Service Level Agreements with customers and internal Operational Level Agreements to improve support workflow on the back end. Future plans for enhancing the service portfolio will include internal service attributes such as service owner and dependent systems and services.
3.3 Revitalized attention to Human Resources and Internal Communications

Per the hope expressed in Computing Services’ 2006 Strategic Report, by 2008, the division had hired its own human resource manager whose first assignment was to finalize the new performance review process. Bringing together disparate forms and processes from the two legacy organizations, a series of performance review modules, including a mandatory self-evaluation, now provides divisional consistency while allowing for local customizations in the units. Computing Services is committed to 100% compliance each year.

Division-wide Efforts

- **Departmental Insights**
  In an effort to learn more about all the efforts of the merged organization, we ran a series of “Departmental Insights” in 2008. Every department presented its work to the Computing Services leadership. It was an opportunity to provide recognition to the operational work that sustains the university. The presentations, and the subsequent Management Team discussions also provided a venue to raise issues and concerns. A number of staff found the process to be an unanticipated professional development opportunity.

- **Internal Communications**
  A discovery project focusing on Internal Communications was completed in 2009 and yielded suggestions about the never-ending quest to share information more effectively in a large and complex organization. A number of practices were instituted as a result of the project; new ideas are always welcome and considered very seriously.

Individual Professional Development

In 2008 and 2009, Computing Services continued its commitment to sending two rising leaders to the EDUCAUSE Management and Leadership Institutes each session—semi-annual and annual, respectively. Two members of the division were also accepted into the inaugural class of Carnegie Mellon’s Leadership Academy in 2009.

Beyond its own team-building work with an external facilitator, Computing Services’ Senior Management Team members also participated in the intensive Information Technology Leadership Program (IT•LP) offered by MOR Associates in 2008 and 2009. The IT•LP experience also provided an opportunity to invite IT leaders from campus as members of the two cohorts, six each year, adding an invaluable element of team-building across campus.
The following goals were defined by the Computing Services Senior Management Team in 2010 as activities or projects that we should work on over the next three years. Much of the work is already in progress to meet significant fiscal year 2013 milestones. Several initiatives (e.g., service management, mobility environment and some of the Common Practices) are new to the division portfolio. This work also represents some of the agreements with key constituents, such as the Executive Steering Committee on Computing (ESCC), a faculty classroom technology group, business units, Campus Facilities Group, and Department Computing Administrators.

4.1 Redefinition of Clusters
During class time, students and faculty expect the teaching spaces to support faculty-to-student interaction, group student collaboration, and various instructional activities—all within one space. After class hours, teaching spaces must provide software access as well as collaborative and individual workspaces for students. Students and faculty also require that the software they need for academic classes and educational purposes be available to them and consistently installed. Reliability and fast response time for software installation are high priorities for faculty. Student access to facilities and to the software they need is often sacrificed during high course reservation times.

Goal
Focus on new delivery models for accessing academic software, thereby reducing reliance on centrally managed computer labs (clusters) and allowing us to refocus cluster services to provide teaching and collaborative technology enhanced spaces.

Initiatives Under Consideration
- Deliver controlled academic software directly to student computers.
- Leverage relationships with department managed computer labs and collaborative environments to increase the availability of technology enhanced spaces for teaching and collaborative work.

4.2 Network Cost Model
Our current network funding mechanisms, such as outlet activation fees and DataNet charges, do not adequately provide for the maintenance and refresh of the campus data network. This funding is also being threatened by shifts in technology preferences (e.g., as phone lines are eliminated, revenue from DataNet fees is also lost). Many of our peer institutions have solved similar funding issues by increasing central allocations or instituting a variety of different chargeback models (per-FTE, fee for service, etc.).
Goal
Develop, vet and explore implementation of a more sustainable funding model for our network services, with an eye toward extending the model to other communication services, such as telephone service.

Initiatives Under Consideration

- Develop a new cost model for network services, specifically, the campus wired and wireless networks, by documenting the various network cost components and examining peer chargeback models. Work with the university administration to explore implementation of the model.
- Complete a service-by-service analysis of network services to discover opportunities where we can optimize operational spending. The residential wired network is the first service planned for review.

4.3 Enterprise Applications
With the goal of delivering effective enterprise applications to campus, due diligence was directed to assessing possible vendors and evaluating community source projects, as well as prioritizing work with business partners and the Executive Steering Committee on Computing (ESCC). Providing contemporary enterprise applications should increase the satisfaction level of customers and build trust with business and executive partners, as well as provide a more secure, compliant and maintainable base for future growth and enhancements.

Goal
Complete the implementation of new applications or upgrades to existing applications that will provide more robust business solutions.

Initiatives Under Consideration
Student Services Suite (S3)
- Continual upgrades to the student interface with expanded functionality and an improved user experience.
- Plan progressive enhancements related to multiple developmental tracks:
  - Application Development and Integration—implementation of new Student Financials module.
  - Functional Package Integration—implementation of Financial Aid module.
  - Infrastructure Services—replacement of Ingres database, character-based administrative interface, and HP servers.
- Possible implementation of Kuali Student Enrollment modules.

HR/Payroll Replacement team
- Develop Request for Proposal (RFP) to procure a replacement Human Resources (HR)/Payroll system.
- Evaluate possible business process changes and adopt those which are judged both feasible and worthy of implementation.
- Replace the HR/Payroll system.

Financial Systems
- Update Oracle Financials to Release 12 (R12).
- Develop data management strategy, including an updated data retention policy and archiving/purging solution.
- Replace client budgeting tool (ADI).
- Replace Financial Data Warehouse.
Application Infrastructure
- Deploy an Enterprise Service Bus (ESB) and service registry in production.
- Begin integration with major enterprise systems.
- Develop governance processes around operation of the ESB.

4.4 Disaster Recovery (DR) and Business Continuity (BC)

The university relies on information technology (IT) services to perform many of its core business functions. In order to ensure that the university’s business can carry on in the event of disruptions of IT services, Computing Services has been charged with improving the disaster recovery (DR) capabilities of our IT infrastructure and services.

Goal
Focus on the DR effort to develop plans and methodologies that will allow key business processes to function in the event that primary systems supporting those processes are unavailable for a prolonged period of time (i.e., up to six weeks).

Initiatives Under Consideration
- DR Infrastructure - Provide current DR equipment with a better interim home and additional capacity for key university applications and services. Additionally, per the Future Data Center (FDC) project, provide a second university data center capable of serving as a DR site as well as a growth area for production data center applications and services.
- DR Process - Create Disaster Recovery approaches and solutions for key university applications and services (e.g., Payroll/HR, SIS, Oracle Financials, Advance and the Card System).
- DR Operations – Work to operationalize the Disaster Recovery effort with Computing Services and possibly expand beyond DR into Business Continuity (BC) within and outside the division. This includes efforts such as Sustainable Recoverability, piloting best BC practices with the division and sharing those best practices with other business units in the university.

4.5 Authentication Roadmap

In the last 15 years, with the addition of web and Windows computing, the authentication mechanisms on campus have grown without coordination or a central strategy. Maturation of the Identity Management program has created an opportunity and exposed the gap in multiple authentication mechanisms, and it is time to pull these efforts together with a common strategy.

Goal
Develop an Authentication Roadmap to serve as a focal point for governance and a guide for decisions and efforts related to authentication services, especially in the context of the identity management efforts of the division.

Initiatives Under Consideration
- Consider requirements and relationships for authentication services within the division and for the enterprise and issue a set of principles to guide service evolution through the next phase of maturity.
- Within the principles, represent common understanding of the relationship between each authentication service and represent policies, practices and governance to manage changes related to the service.
• Provide short-term guidance regarding imminent deadlines and insight into long-term strategies for authentication infrastructure as part of the overall Identity, Authentication, and Access Management (IAAM) infrastructure of the division.

• Integrate identity proofing and attestation needs with a credential issuance policy to match Level of Assurance targets for each constituent population.

• Consolidate vendor investigations related to ongoing authentication projects in the hopes of leveraging commercial solutions for the breadth of authentication and credential translation/transport services across the spectrum of application requirements.

• In collaboration with the Identity Management program and the Information Security Office, identify and engage campus stakeholders and application owners in authentication policy, credential management issues, and leveraging the IAAM infrastructures.

4.6 Undergraduate Email

The potential migration of faculty, staff and graduate student email and calendar services, along with the end of support for Oracle calendar, makes this an appropriate time to address the current service we offer for undergraduates regarding email and calendaring.

Goal

Analyze current email and calendaring services offered to undergraduates and make a decision regarding the continuation of those services.

Initiatives Under Consideration

• Initiate an outreach and discovery effort to determine undergraduate email service needs.

• Evaluate the total cost of ownership for providing email and calendar services for the undergraduate student population.

• Benchmark existing options that our peer institutions have implemented.

4.7 Service Management

Computing Services has improved project planning as well as management tools and processes resulting in faster completion of key division initiatives. As a service organization, we need to better understand and manage our services from the campus customer perspective. By understanding our customers’ requirements and measuring our service outcomes, we can make better informed decisions about introducing new services and identifying services to phase out.

Goal

Explore methods for moving to a service management model that would result in IT service and system development based on customers’ perspectives of the contribution to their business. This may represent a change in the way Computing Services operates, shifting focus from managing the technology itself to better aligning services with the business needs of the university community.

Initiatives Under Consideration

• Identify internal “owners” for the services we provide.

• Develop metrics to allow us to understand how well the services are being delivered.

• Develop processes to keep the service portfolio current by integrating updates into SII, OLAs, biennial reports, and the project management and portfolio processes.
• Perform a periodic review of the entire service portfolio to ensure alignment with strategic goals and to identify services that are candidates for upgrades, replacement, phase-out or outsourcing.
• Create a gap analysis to identify needed services we are not currently offering.
• Work with Global IT Services and other divisional groups to institute a Customer Relationship Management function that will result in an improved understanding of customer needs.

4.8 Computing Services and the Mobile Environment

Many students (according to some studies, most students) are coming to the university with their own mobile devices. Faculty and staff also have their own sophisticated mobile devices. These smartphones, tablets and laptops are increasingly capable of providing a rich computing experience.

Goal
Enable access to information and services at Carnegie Mellon at anytime and from any location.

Initiatives Under Consideration
• Enable access from mobile devices for a few key applications where the vendor has built in capabilities and where major renovations to the service would not be required. Examples include WebISO authentication, Blackboard and the Carnegie Mellon web portal.
• Include access from mobile devices in the requirements for new or upgraded services such as calendar, email, and authentication.
• Redefine the problem statement from mobile computing support to using virtualization as a way to provide device independence and allow scalability.
• Define virtualization exploration to explicitly include mobile and non-mobile devices for both university owned and individually owned devices.

4.9 Common Practices

There were thirteen summary recommendations from the Common Practices Working Group (CPWG) of the Computing Services’ Senior Management Team (SMT) representing potential improvements in internal processes. The raw materials for these recommendations were gleaned from six hours of focus groups that were conducted with twenty-two members of the division. They were subsequently organized, summarized, evaluated, and prioritized by the CPWG for consideration.

Goal
Define and implement standardized common practices to create a more efficient organization with respect to providing services and defining areas of excellence that can be measured in an effective manner. The goals include less redundancy in tools and methods, greater efficiency in documented processes, more agility in responding to business needs, and improved staff morale through clarification of roles and collaboration across the division.

Initiatives Under Consideration
• Adopt an overall change management process.
• Clarify delegation, roles, responsibilities, and basic tasks.
• Separate operational roles from development roles.
• Create an inventory of approved tools and practices.
• Clarify responsibilities, activities, and plans for services and systems.
• Consolidate monitoring and measurement of services.
• Create a common documentation repository.
• Develop a comprehensive staff training program.
• Create and follow a process for revisiting open issues, expediencies, and exceptions.
• Define and implement standards and processes for divisional desktop client configuration and management.
• Define process development guidelines, rightsizing, ownership and understanding for whom it serves, as well as its relationship to other processes.
• Conduct regular project status and activity communication at all levels and between all directorates, including financial and strategic reporting.
• Develop and communicate core requirements: infrastructure and operational processes and technologies should be well documented and broadly communicated with a single owner.

Acknowledgments

Credit is given to the following individuals or groups who contributed information, developed text or edited portions of this report.

Contributors
Brian Bennett
Carrie Regenstein
Joel Smith
Computing Services’ Senior Management Team
Computing Services’ Staff Members

Authors
Dot Foote
Dawn Jackson
Patty Riether
Lisa Zirngibl