Operational Essentials

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

We have a terrific student chapter< http://www.acm.org/chapters/students > of the Association for Computing Machinery(ACM)< http://www.acm.org/ > at my university< http://www.norwich.edu >. The School of Business and Management< http://programs.norwich.edu/business/ > provides the students with a clubroom that is next to the academic computer lab and to the rooms reserved for the Cyber Weapons Range War Room< http://www.7dvt.com/2010norwich-university-advanced-computing-center >.

The academic lab is for classes requiring access to specific software (e.g., statistical packages) and supporting access to the University's electronic classrooms where many of us post links to resources, assignments, quizzes, and facilities for uploading and grading assignments. Examples drawn from this semester's schedule include classes in Chinese language, construction engineering management, basic computer skills, introduction to business, college algebra, nursing informatics, construction project management, differential equations, experimental psychology, and applied statistics.

The War Room is used for specialized courses and events such as network attack/defend exercises and contests, system administrator training, live demonstrations for security conferences (using telepresence), digital forensics analysis and cyber criminalistics. The War Room has state-of-the-art wall-mounted large-screen displays, top-quality digital video cameras for interactive presentations, two dozen workstations and access to high-speed intranet and Internet connections. Much of the work is done through virtualized systems running on rack-mounted servers described in the article referenced earlier< http://www.7dvt.com/2010norwich-university-advanced-computing-center >.

Recently I had a meeting with computer club members who currently run the servers we depend on for the War Room and for many of our online courses. These are some of our brightest kids; they're fascinated by a wide range of knowledge, eager to pursue answers to interesting questions, friendly to each other and to less gifted students, and committed to supporting the progress of our computer science, information assurance, and cyber-forensics programs.

The team of six students and I spent 90 minutes late on a Friday afternoon brainstorming about how to convert a student club oriented towards learning – and fun – into an operationally sound team that can guarantee quality of service defined in service-level agreements – and maintain the fun.

We started off with some brainstorming to identify what has to be done to maintain and further the services and to list specific problems facing the group. Within a few minutes, we'd identified and classified the following points as key issues:

- Operations (keeping the hardware and operating environment running
    - We have commitments to paying customers such as the College of Graduate and Continuing Studies who depend on the online courses we make available.
    - Although we haven't formalized our quality of service (QoS) into service-level agreements (SLAs), we still face implicit expectations among our users about

availability and response time.

- Production (meeting the requirements for specific projects)
    - We are constantly given new requirements as the reputation of the service expands.
    - We have to formalize the procedures for scheduling and building the resources for specific tasks.
- Business Continuity Planning
    - We have too many single points of failure, including individuals we count on who are the only ones with specific critical knowledge.
    - We have a big uninterruptable power supply that can handle critical servers and an external electrical generator; neither has been installed because we don't have the budget yet to move them over to our installation.
    - We need to plan and effect regular off-hours and then live testing of our capabilities.
    - Our network infrastructure is vulnerable; we have only two Internet Service Providers (ISPs) and both are local services. A major wind- or ice-storm such as Tropical Storm Sandy< http://alerts.weather.gov/cap/wwacapget.php?x=VT124CCABB19AC.HighWindWarning.124CCABD2D50VT.BTVNPWBTV.0a502f8f5bf8e0d07e392425a6f0e1d4 > could disrupt services to remote and local users.
    - Much of our operational infrastructure is either completely undocumented or is documented only on scraps of paper that are impossible to search quickly or to backup effectively.
    - We need to re-evaluate our backup policy, including off-site storage.
- Disaster Recovery Planning
    - If the systems must be replaced due to major disruptions such as physical damage and extended failure of our network infrastructure, how will we resume operations?
- Personnel Management
    - We don't have a formal recruitment program to encourage younger students to join the group and develop their technical skills.
    - We have no one who monitors all contact information for every member of the team.
    - We're still using e-mail for communications instead of a permanent user group where our messages and documentation files are archived for future team members to be able to access.

So what lessons can readers derive from this situation?

- Enthusiastic amateurs are a great resource for testing out ideas and building prototypes – but they cannot substitute for thorough, meticulous planning once we move to a production environment.
- The natural aversion to documentation cannot be permitted to interfere with development of a corporate knowledge base that will allow future members to come up to speed quickly.
- Policies and procedures are necessary for a production environment to survive.
- Someone has to be in charge of personnel management: the future of a student organization depends on a steady supply of fresh enthusiasts who can be trained quickly.
- Business continuity planning and disaster recovery may be minor issues during the prototyping phase, but as systems move into production, they become essential.

As you can imagine, the students left with an extensive TO DO list. We'll keep meeting every week and I’ll occasionally report on our progress.

In the meantime, here are some resources about operations and system management that readers may find helpful.

- Documentation for Less Work: Will this Have to be Done Again?< http://www.mekabay.com/opsmgmt/documentation.pdf >
- Facilities Management in the Age of Information Warfare< http://www.mekabay.com/opsmgmt/facmgmt.pdf >
- Review of Visible Ops Security< http://www.mekabay.com/opsmgmt/vos.pdf >
- Staffing the Data Center< http://www.mekabay.com/opsmgmt/staffing.pdf >
- System Logging< http://www.mekabay.com/opsmgmt/logging.pdf >
- Computer Security Incident Response Team Management< http://www.mekabay.com/infosecmgmt/csirtm.pdf >
- Facilities Security Audit Checklist< http://www.mekabay.com/infosecmgmt/facilities_checklist.pdf >
- Preparing for the Next Solar Max< http://www.mekabay.com/infosecmgmt/solarmax.pdf >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *