Microsc. Microanal. 21 (Suppl 3), 2015
doi:10.1017/S1431927615002664 Paper No. 0187

Strategies for Managing Information Technology (IT) in Microscopy Facilities

John Henry J. Scott[1]

[1.] National Institute of Standards and Technology, Office of Data and Informatics, Gaithersburg, MD

Microscopy and analytical facility managers are faced with an unusually broad and difficult set of challenges, including unrealistic cost-recovery models, a diverse and unevenly-trained population of sponsors and users, a heterogeneous collection of instruments, and the constantly changing landscape of instrument manufacturers. Among the most difficult of these challenges is keeping up with rapid changes in the information technology (IT) sector. Most managers of core imaging facilities or central analytical laboratories are not IT professionals, and they have minimal training in IT infrastructure, advanced networking, digital storage solutions, and IT security practices. Yet their job requires them to find creative solutions to difficult IT problems while operating within tight budget constraints. One of many such problems facing facility managers is the end of support for Microsoft Windows XP [1,2].

This talk is focused on providing useful advice, specific concrete solutions, and general strategies for dealing with IT challenges in the context of shared-use microscopy facilities embedded within both small and large parent organizations. While many of these strategies may be valuable for federal research facilities and relatively well-funded corporate research centers, the target audience is facility directors and staff at smaller laboratories and universities. Practical solutions are favored over theoretical content, the strategies have been chosen because they are effective even when they are not elegant, and the emphasis is on free and open source software and widely available tools instead of expensive commercial platforms. When hardware is required, consideration is given to tight budget constraints and older, obsolete computers are re-purposed when possible.

Keeping the IT resources within a facility running smoothly is a high priority for most managers, and several worked examples are included that demonstrate how investing a small amount of time learning a suite of powerful software tools can pay dividends. The Sysinternals [3] suite of tools is covered, including the use of process explorer and process monitor to troubleshoot Microsoft DCOM communication problems between an Energy Dispersive X-ray (EDS) spectrometer computer and an SEM microscope control PC, and it is used to identify hidden file permission problems preventing apparently unrelated actions in light microscope image data analysis. Sysinternals AutoRuns is presented as one of several tools for enumerating the more than two dozen Windows autostart locations; such a tool is invaluable in discovering and identifying adware/spyware and maintaining system performance. The utility of SpeedFan [4], ostensibly a tool for controlling the speed of PC cooling fans, is displayed in a worked example prompted by the diagnosis of intermittent failures on a field emission TEM's control PC motherboard. By inspecting onboard temperature sensors while simultaneously detecting an imminent boot drive hardware failure via the hard drive's SMART interface [5], the hidden root cause of communications faults was revealed and costly downtime avoided. The free AutoIt [6] automation solution is introduced, including simple BASIC-like scripts and automation of graphical interfaces to simplify recurring management tasks on analytical instrument computers. Network attached storage (NAS) solutions, file sync and share services, digital data curation strategies, and other best practices for facility tuning will also be discussed briefly.

Finally, several topics in IT security will be addressed from the perspective of the facility manager. Industry best practices and pressure from an organization's Chief Information Officer (CIO) often lead to strict policies designed to improve IT hygiene, minimize data spills, limit the spread of malware, and guard against the rapidly growing threat of ransomware. Justified in part by the ubiquity of infected removable media such as flash drives, these policies are often at odds with the research needs of facility users and the efficient operation of the facility itself, with the facility manager and staff caught in the middle. This talk will provide strategies and options for balancing these needs, including an analysis and explanation of dedicated Research Equipment Networks (RENs) designed to isolate and protect instrument computers running obsolete and legacy operating systems such as Windows NT, while still permitting sufficient network-based data flow to allow end users to retrieve their images and analytical results. Figure 1 shows a typical REN configuration, based around a modest web-based dedicated firewall appliance that any facility manager can build from a discarded Pentium computer, a few $30 surplus network cards, and free and open source tools such as IPCop, pfSense, or m0n0wall [7].

References:

[1] Any mention of commercial or free open source products is for information purposes only, and does not imply recommendation or endorsement by NIST.
[2] Microsoft's extended support for Windows XP ended on April 8, 2014, and Security Essentials virus definitions and updates for the Malicious Software Removal Tool (MSRT) for XP will be discontinued on July 14, 2015. http://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx
[3] Although originally developed as an independent project, Sysinternals is now available for free from Microsoft TechNet at: https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx
[4] SpeedFan is available at http://www.almico.com/speedfan.php
[5] SMART, Self-Monitoring, Analysis and Reporting Technology, supported by most hard disk drive and solid state drive manufacturers.
[6] AutoIt is available from: https://www.autoitscript.com/site/autoit/
[7] IPCop: http://www.ipcop.org/, pfSense: https://www.pfsense.org/, m0n0wall: http://m0n0.ch/wall/

Figure 1. Network diagram showing an example Research Equipment Network (REN) used to isolate instrument PCs running obsolete operating systems such as Windows XP or Windows 2000.