ITS eNews R·I·T
Information & Technology Services at the Rochester Institute of Technology

We've Got Mail

An Estimated 45 Million Email Messages Come Into Campus in April 2007

This information was compiled by Mike Young, in his role as part of the ITS Infrastructure and Systems Support team. It is only a snapshot of the day-to-day challenges of keeping the legitimate email flowing to and from campus customers. Mike, as well as the other TSS staff, has been instrumental in preventing spam, viruses and other online nuisances from infiltrating the campus email system. While the spammers have gotten more creative (as Mike detailed in his feature article) he has become equally vigilant - and creative. - ed

Over the course of time, ITS measures the overall volume of email coming to the RIT campus from the Internet. The volume is measured by adding the number of connections the central email server rejected and the number of recipients for all email messages that were accepted.

In January 2001, volume was measured at **1.6 million** for the month.

In January 2004, volume was measured at **6.6 million** for the month.

In April 2007, volume is coming in at a rate of **45 million** for the month, based on the first 15 days. In the first half of April alone, ITS measured a **48% increase in daily spam**.

Conservative estimates are that if the mail servers weren't rejecting connections, they would be accepting email addressed to more than 300 million recipients per month. That's more than 400 messages per person per day on the RIT campus.

RIT receives more mail in one day today than it did in an entire month in 2001.

You're probably asking the question: What is all of this email? More than 95% of it is spam, and is rejected, discarded, or quarantined.

The good stuff: After spam processing, RIT's central email servers deliver messages addressed to 83,000 recipients daily. This is a relatively small increase above the 45,000 in 2001. Email coming from sites such as Myspace, Facebook, and Xanga account for half of this increase.

The bottom line: 4.78 good messages per person per day, 86.24 spam per person per day, thrown away.

Security Challenges Now Include Vulnerabilities in Hardware and Device Drivers As Well As Software

By Mike Young, Technical Support Services, Michael.Young@rit.edu

The following article is a reprint of one submitted on 2/14/07 to ITSTech, a listserv for systems administrators, network engineers, security and desktop support staff at RIT. The IT professionals in this group are keenly aware of the Internet threats and software vulnerabilities that plague networks, disrupt business and make systems (and individuals) ripe for identity theft. Several new trends in security vulnerabilities have emerged, making updates, patches and other preventive measures more important than ever. – ed.

Are you up to date? Is your (virtual) neighbor? Is your child's toy??

Almost everything we use today from kitchen gadgets to the latest high definition televisions has some sort of computer chip within it. Like desktop computers, much of this electronic equipment needs regular updates and preventive measures. Often these are disregarded—who would think that you have to upgrade your television?

Keeping up to date is becoming increasing difficult, and not just with Microsoft's products. If the list of vendors that require security updates on a periodic basis seems endless, that's because it is. No software is safe and, as we learned last year, no document type is safe. Not only are executable attachments vulnerable, but any other type can be as well. This is either due to executable content (Word, HTML), or even issues with rendering engines (images, movies). No software should be considered safe.

Vulnerability vectors aren't limited to software either. Vulnerabilities were discovered in hardware, and device drivers. And if Bluetooth and Blue Pill are examples, new products will be adopted widely even if a potential vulnerability is discovered in the development or testing stages. Convenience and innovation still wins out over security in the mind of the consumer, though even that appears to be slowly changing due to increasing awareness to identity and information theft.

Zero-day vulnerabilities have also become the norm. You can pretty much count on it now. On Black Tuesday, Microsoft releases its patches, and on Zero-Day Wednesday, the bad guys release their new exploits. Email borne viruses are making a comeback, though we now (seem to) have better protection.

Phishing is also widespread and targeted and blended stealth attacks have become more common. An attack may get in the door one way, and then spread behind the firewall using another way. Once inside, it may lie dormant for months hidden by a root kit. The security of any one computer is now directly related to the security of the all of the computers within its trusted realm. On our campus that often means the entire campus. This could be the desktop next door, or the antique computer across campus running an application that hasn't been updated in 10 years on Windows NT (or earlier).

Which vendors do you trust?

The big vendors would seem to be the worst because they're the most targeted. Microsoft is riddled with vulnerabilities (more than 150 patched in 2006 and with more than 20 already in 2007). Sony quietly deployed a root kit in the name of copy protection. McDonald's handed out computerized toys that were infected at the factory. And do you trust your anti-malware tools? They don't seem to be invulnerable either. Three of them have patches just this month, from vendors like Symantec, Micro Trend, and Microsoft.

What to Expect in 2007 and What to DO

Vista is here with vastly improved security (theoretically). EMI has recently broken from the pack on copy protection, stating that it is likely hurting sales. (It's about time!) Spam from bots may take a hit due to Spamhaus' new policy block list. SPF (sender-policy-framework) may finally work with SRS (sender-rewriting-scheme), although it may be very unpopular due to the way it changes email addresses. Encryption tools are maturing, and we might actually see some user-friendly ones this year. Even banks are changing—starting to deploy two-factor authentication for access to accounts. How effective these encryption tools are will depend on how widely they are adopted.

The adoption of best practices is more important than ever. Security standards, defense in depth, anti-virus, anti-spam, anti-phishing, least privilege, encryption, internal firewalls, disabling of unnecessary services, password storage (or lack of), and software inventories are all important. There is no one thing that will protect your computer and your data. You must know what you have, how you're using it, and who can access it.

Software Vulnerability Information and Resources

Adobe/Macromedia

Adobe Reader and Acrobat have had their share of vulnerabilities in the past year. This includes a patch on 1/9/2007 for all versions 4.x through 7.x and 3D on both Windows and Macintosh. The general recommendation is to upgrade to version 8, if your hardware will support it. Lesser used JRUN and ColdFusion MX products have cross-site scripting vulnerabilities, with patches released February 13, 2007. For a complete listing of Adobe security bulletins, visit http://www.adobe.com/support/security/index.html.

The Adobe site now includes products once under the Macromedia name, including Flash Player, and Shockwave Player, Breeze server, Dreamweaver, Adobe Download Manager, and other lesser-deployed products. Many of these, particularly those mentioned, have had some significant vulnerabilities in the past year.

Apple

Many people have switched to the Macintosh as a safe haven. True, it hasn't been as targeted, but the Macinosh isn't devoid of vulnerabilities. Most of the vulnerabilities have appeared in Microsoft products, but others have been found in the past year, including in the widely used Quicktime and iTunes products.

In the past month, patches for Quicktime (Windows/Macintosh) and AirPort Extreme (OS X 10.4.8) have been released, and Apple released security update 2007-002 for Mac OS X (http://docs.info.apple.com/article.html?artnum=305102). The patch fixes some code execution/elevation-of-privilege issues. (These are similar in nature to the problems that have plagued Microsoft Windows.)

For a complete listing of Apple security information, visit http://www.apple.com/support/security. Current bulletins are at, http://docs.info.apple.com/article.html?artnum=61798.

Microsoft

In January, Microsoft issued four bulletins. In February, there were twelve more. The previous trend continues, with zero-day attacks immediately following the release of patches for previous vulnerabilities. Mass mailing worms appear to be back, likely due in part to a rash of vulnerabilities discovered in Word. Even the greatly improved IE7 (Internet Explorer7) has new security vulnerabilities.

In the twelve bulletins there are twenty vulnerabilities documented and patched. Five of them in Word and Excel products are known to be actively exploited. One of them has the capability to automatically spread via a worm,using the Malware Protection Engine (ironic).

As we have seen in the past, newer versions of operating systems and software often have lower risk associated with them due to improvements in security.

Mozilla

Mozilla's products have been a popular alternative to Microsoft's due to the number of vulnerabilities. Just like Apple, however, Mozilla has been plagued by vulnerabilities.

Firefox, the popular alternative to Internet Explorer, has been plagued by vulnerabilities. (There was only one zero-day exploit that I can remember, however.) The rate of discovery is growing. A new update was just released (version 2.0.0.2) which fixes eight more vulnerabilities. There also appear to be a handful of newly discovered vulnerabilities that could lead to information disclosure or code execution. This includes a cross-site cookie-stealing vulnerability, a vulnerability that would allow a web site to modify the about:config or about:blank pages and insert any content (potentially a phisher's dream), and one that could result in information cached from previously visited web sites being stolen.

A complete list of patches to Mozilla products can be found at http://www.mozilla.org/projects/security/known-vulnerabilities.html

Sun Microsystems

On Tuesday, Internet Storm Center (ISC) researchers announced a zero-day flaw in telnet on Solaris 10 and 11. Best practices recommend not using and disabling telnet altogether, yet Sun still ships its operating systems with telnet enabled by default. More information is available at

http://isc2.sans.org/diary.html?storyid=2220

http://www.informationweek.com/shared/printableArticle.jhtml?articleID=197005178

http://www.theregister.co.uk/2007/02/12/solaris_zeroday/print.html

http://www.informationweek.com/shared/printableArticle.jhtml?articleID=197005473

Symantec

Symantec's products have had their share of vulnerabilities, including their anti-virus and backup products. The most recent issues this past month are in their Web Security product.

A complete list of advisories can be found at http://www.symantec.com/avcenter/security/SymantecAdvisories.html

Trend Micro

Trend issued a patch on February 8th for a remote code execution/buffer overflow vulnerability in its anti-virus engine. The flaw could be exploited with a specially crafted UPX compressed executable file. It affects virtually every Trend product. Information is available at

http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034289

http://www.computerworld.com (Full URL too long to display)

http://news.com.com/2102-1002_3-6157554.html?tag=st.util.print

While many people may not know what UPX is, the malware community does. It's a favorite for compressing and hiding malware.

As you can see, following good security practices (as detailed in the Desktop and Server Standards (http://security.rit.edu/standards/) is critical as vulnerabilities and attacks continue to grow in frequency and severity.

(Some links within the document point to Wikipedia, the ubiquitous online encyclopedia. While not the last word in technology definitions, it is certainly an interesting and easily accessible resource that can provide both basic and more sophisticated technology information. -ed.)

Microsoft Windows Vista: ITS Recommends Postponing Upgrades - For Now

By Dave Pecora, Associate Director, ITS, dave.pecora@rit.edu

ITS recommends that users hold off on Windows Vista upgrades for RIT-owned computers – for now.

There has been a lot of publicity on the release of Microsoft's newest operating system – Vista. Although ITS will eventually recommend an upgrade to Vista for RIT Windows systems, ITS strongly recommends that RIT faculty and staff users hold off upgrading at this time. (Note: If you are part of an effort to test the new operating system, please inform your local systems administrator or IT support staff of your upgrade.)

The main reason ITS is making this recommendation is that many key software vendors have yet to certify their products as compatible with Vista. For example, products such as Cisco VPN and the McAfee Host Intrusion Prevention software (formerly known as the McAfee desktop firewall) have known compatibility issues with Vista. Each of these vendors is working on upgrading their products to be fully compatible with Vista. Once upgrades are released, we will need additional time to test and deploy them before recommending a general campus-wide upgrade to Vista. In addition to these factors, there is a minimum hardware requirement to run Vista that many campus PCs may not meet.

We have had a working group monitoring the status of vendor upgrades and performing some in-house testing on Vista. This team has been researching and testing Vista prior to the general release last November. The team has compiled a list of critical software applications that must be tested or at least vendor certified before we will plan or recommend an upgrade. This list is available on the team's website http://www.rit.edu/its/initiatives/vista. If you are aware of additional software that we should monitor, or would like to be part of our testing effort, please contact Kristi Ziehl at Kristi.Ziehl@rit.edu.

While ITS is recommending that departments hold off on Vista upgrades, we strongly recommend that all departments purchasing new computers make sure they purchase "Vista Premium Ready" machines. Additional information on what that means can be found at http://www.rit.edu/its/initiatives/vista/#requirements. We have updated the RIT Standard Desktop and Laptop systems on the RIT Dell premier site to be Vista Premium Ready.

We understand the importance of keeping current and will keep you posted on progress. When we believe the time is right, ITS will communicate this to the campus. We will also plan an upgrade with each of the areas that receives IT support from either our ITS HelpDesk staff or our DSS (Distributed Support Services) organization.

Computer Security Survey Results Detailed

CS Student Survey Includes Some National Results

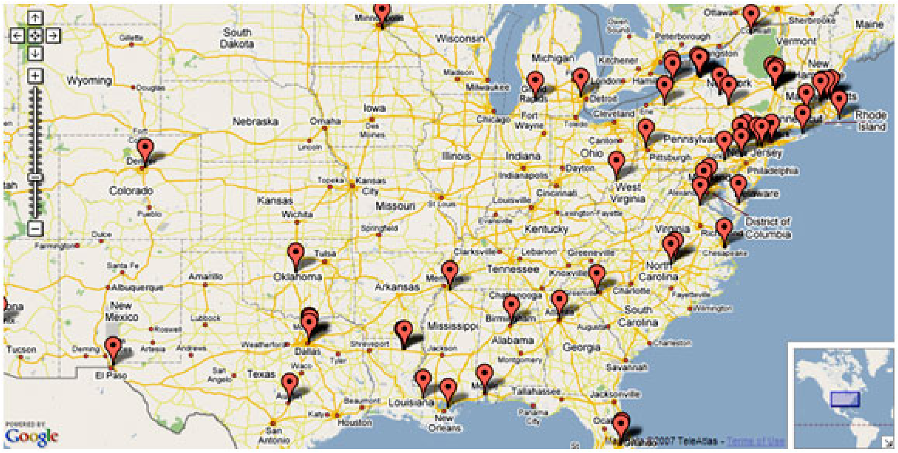
By Kurt Alfred Kluever, Department of Computer Science, 4th Year BS/MS Student, kak2112@rit.edu

Survey Overview

As part of the Security Measurement and Testing course, taught by Professor Leon Reznik, a computer security survey was recently conducted to investigate the common practice of computer users regarding computer security. A group of eight students designed the questions, distributed the survey using RIT's Clipboard survey tool, and analyzed the responses of 913 participants. The organizers were trying to diversify the surveyed population: graduate and undergraduate students both at RIT and other US schools, RIT faculty and staff, relatives and friends took part in this survey. On behalf of all organizers, we want to express our gratitude to all participants for their help and encouragement. This article presents a summary of the analysis. More details can be found in the final report at www.cs.rit.edu/~lr/survey.htm.

The survey result analysis was kept completely anonymous. Although the results do contain the IP address of the respondent, the IP address was never associated with specific responses during the analysis. The only time the IP address was used was during the geo-locating process. Geo-locating is the process of obtaining a location based on an IP address. It is not a precise science, as IP addresses are not tied to specific physical addresses. However, they are typically tied to a general region.

An open source, free API for geo-locating was used to provide IP to location lookups. The downside of using a non-commercial geo-locating service is that the free service was only able to successfully resolve 70% (646 of 913 survey responses). Of the 646 resolved responses, there were only 333 unique locations (since many came from RIT's campus which resolves to a single point). As the map shows below, we received responses from all over the United States, and even one from Mexico.



The survey questionnaire consisted of two parts. The first part of the survey was designed to identify which demographic group the respondent represented in relation to RIT affiliation, gender, age, level of education, whether they have taken a computer security course before, and what operating system they used. The next nine questions were used to determine how secure the user's computing practices were. The questions covered the topics of operating system patching, password habits, publishing of personal information online, use of anti-virus software, and use of personal firewalls.

Survey Results: RIT affiliated vs. Non-RIT affiliated

Of the 913 responses received, over 80% were affiliated with RIT (students, faculty, staff, or alumni). The good news reported by the survey is that, generally speaking, RIT affiliated respondents were more secure in their computer usage than non-RIT affiliated respondents.

Categories were created for response sets that we deemed demonstrated "ultra secure" computer practices and "ultra in-secure" computer practices. Over 16% of RIT affiliated respondents can be classified as practicing ultra secure computer habits while only 13% of non-RIT affiliated can be. Less than 1.3% of RIT affiliated respondents and less than 2.4% of non-RIT affiliated respondents fall into the "ultra in-secure" category.

Survey Results: Male vs. Female

About 59% of the respondents were male and 41% were female. Using the same ultra secure and ultra in-secure requirements as above, it was found that only 15% of men are ultra secure while 16% of women are ultra secure. Over 75% of men and over 78% of women update their antivirus software.

However, women were not as diligent as men in applying updates to their firewalls or operating systems. Women also tend to be less secure in password practices. It was found that over 72% of men always create hard-to-crack passwords for important accounts while only 59% of women do. Over 13% of women never create hard passwords for their accounts while only 8% of men fail to create hard passwords.

Survey Results: RIT faculty/staff vs. RIT students

The survey results show that RIT employees (faculty/staff) tend to be more secure in their computing practices than RIT students do. RIT employees change their passwords more frequently than students, are more likely to always create hard passwords than students, and are also more likely not to use the same password for all accounts than students. In fact, over 82% of RIT employees regularly update their antivirus software while only 72% of RIT students do.

The only category that RIT students proved to be more secure than the RIT employees was in regards to regularly updating their firewall software where the students edged out the RIT employees by only 3%. One of the largest separations between RIT employees and students was in regards to the individual's concern of publishing their personal information online (through social networking sites, online resumes, posting on bulletin boards, etc). Over 80% of RIT employees were at least somewhat concerned with publishing this type of information online while only 59% of students were. This can most likely be attributed to the huge growth of social networking sites over the past few years where many students feel comfortable publishing personal information.

Survey Results: Security Practices and Education

Another goal of this survey was to analyze the effects, if any, that education has on security practices. In the survey, respondents were asked what their highest level of education was. For the sake of analysis, we have combined related levels of education into three groups: No college (Some high school + Graduated high school, also referred to as 'High School' in some data sets), College, non-computer related field (Some college in a non-computer related field + Graduated college in a non-computer related field), and College, computer related field (Some college in a computer related field + Graduated college in a computer related field).

The survey questions where education levels had the most impact on the results were questions:

7. Describe how updates/patches are installed on your operating system
9. Do you make passwords intentionally hard to crack?
14. Which of the following best describes your use of a firewall on your primary computer?

The responses to other security questions showed similar responses between education levels, thus making them irrelevant to the discussion. When looking at question 7, it is clear that people who have attended college in a computer related field have better security practices than the other education levels. Over 94% answered that they regularly update/patch their operating system either automatically or by themselves. The other two education levels answered as follows: College, non-computer related field, 84.27%, No college, 76.19%.

Question 9 follows the same trend, with respondents who attended college in a computer related field having the best security practices (i.e., always making their password hard to crack, or at least making their password hard to crack for important accounts). 83.68% of respondents who attended college in a computer related field demonstrated good password practices, compared to only 59.71% of respondents who attended college for a non-computer related field and only 70.24% of respondents who did not attend college.

An interesting analysis of question 14 (firewall usage) revealed that respondents who did not attend college had the highest percentage (75.00%) of firewall best practice (I have a firewall that is automatically updated or by myself), followed closely by respondents who attended college in a computer related field (70.49%), and not so closely by respondents who attended college in a non-computer related field (64.52%).

It seems odd that respondents who did not attend college would have the highest percentage of firewall best practice. The analysis of other questions shows that people who attended college in a computer related field tend to have the best security practices. It is possible that because of a small sample size of respondents who did not attend college (84 of 913 responses), the data is somewhat skewed. Further analysis of a broader sample of this demographic would be needed to see if these results are correct, or just a data anomaly.

Survey Results: Overall Best Practices

Based on the data above, it would seem that males, over the age of 31, who have attended college for a computer related field, have the best overall security practices. To support this conclusion, analysis was done to see what percentage of the “ultra secure” users consisted of this demographic.

The ultra secure users were respondents who answered each question with the best possible security practices. That is, they regularly apply updates/patches to their operating system, firewalls, and anti-virus software either automatically or by themselves, they change their passwords every 6 months or less, do not use the same password for all accounts, and intentionally make their passwords hard to crack (at least on important accounts). Out of the 913 respondents, only 143 respondents were given this distinction of ultra secure.

Respondents over the age of 31 who attended college for a computer related field made up the bulk of the ultra secure group. As for gender, there is no discernable difference between males and females in this group. Accordingly, age and education are the more important factors in this grouping, not gender. More data and further analysis would be needed to confirm these assertions.

As a result of being a university-based survey given in a short amount of time, the cross-section of respondents is one that is not fully representative of the general population. In particular, almost all of the respondents over the age of 31 in this survey had at least some college education in a computer related field. This is not so in the general population, and could lead to incorrect assumptions about that demographic as a whole.

If given on a larger scale to a truly random sample of participants across a larger timescale, this survey could be very useful in assessing the security practices of the general population, and would perhaps yield different results than those found herein.

Survey: A success!

We are pleased that about one third of participants responded positively to the question “Do you feel that participation in this survey has helped you learn a bit about computer security and employ more secure computer use practices?” This lets us conclude that the survey was a success, as it not only provided us with valuable data to analyze, but it also increased the computer security awareness and the computer security practices of many of the participants. Also many students participating in the survey invited their family members and friends from all over the country and gave them another reason to stay in touch while away from home during the cold and dark winter months here at RIT.

For more information or to discuss the survey results further, contact Kurt Alfred Kluever, at kak2112@rit.edu or Professor Reznik lrvcs@rit.edu. More details can be found in the final report at www.cs.rit.edu/~lr/survey.htm.

Work-at-Home Rights for Windows XP Professional Available

Windows Vista Media Forthcoming

By Shawn Thomas, Sr. Desktop Systems Engineer, ITS, shawn.thomas@rit.edu

Now that Microsoft Windows Vista has been officially launched for the retail market, you may have questions about what this means for the RIT "Work At Home" (WAH) coverage in place for Windows XP Professional.

The Microsoft Campus agreement allows for select software and upgrades to be applied to any RIT-owned computer covered by the program. The agreement also allows for easier home use for RIT employees for the products covered in the agreement. Home use CDs are available for a nominal fee to faculty and staff at the Campus Connections bookstore. Purchase of these CDs provide faculty and staff the ability to keep their home machines up to date with the latest Microsoft software through the Microsoft Campus Licensing Agreement. More about the agreement and the software covered can be found at: http://www.rit.edu/its/services/software_licensing/ms_campus_agreement.html

The basic premise of how the WAH program works today will not change as a result of the release of Microsoft Windows Vista. Some final details are still unknown at this time and are being actively investigated. Currently, the only WAH media that can be purchased from the RIT Campus Connections bookstore is Windows XP Professional. The Microsoft Windows Vista WAH media is not yet available.

The Vista project team continues to evaluate Vista's business impact to the RIT network environment. Team members are testing the compatibility of the new software with current versions and will communicate to RIT customers regularly about their findings.

ITS Customer Satisfaction Survey 2007 Online Now…

By Dave Pecora, Associate Director, ITS, Dave.Pecora@rit.edu

It's time once again for the ITS Customer Satisfaction Survey. Now in its fifth year, the annual survey allows us to gauge overall customer satisfaction with ITS as well as satisfaction with our support, service, and technology.

We use the survey to better understand the IT needs and expectations of our customers, as well as to identify opportunities for new and improved services.

The survey is open to all faculty, staff and students. It only takes a few minutes to complete. The survey is available at:

http://clipboard.rit.edu/takeSurvey.cfm?id=2in2i0.

If there are any questions about the survey, please contact me at dave.pecora@rit.edu.

You Might Be a Technology Packrat if…

By Donna Cullen, Computer Policy Analyst, donna.cullen@rit.edu

You might be a technology packrat if…

- You have every computer you ever owned
- You fill one of your desk drawers with computer cables
- You own every issue of ITS News
- You have a copy of every email you ever sent
- You back up your resume on floppies
- You own the manuals for software that no longer runs on your computer

Can you call yourself a rodent of the packing variety? At various times you, like me, may justify this behavior when you see someone bidding on eBay for a Commodore 64 manual or see the beautiful aquarium an office mate made out of a Macintosh SE. Why just the other day, you argue, I heard of a case where a faculty member deleted a 2001 syllabus and now a student is claiming an unfair grading policy.

There is ample justification for having a touch of rodent-like behavior in all of us. Those of us exposed to compulsive cleaners have fallen victim to the occasional tossed car insurance card or the receipt gone missing for that very new and very broken appliance. We spend energy, space and time to squirrel away items that we might need someday.

It is the extremes of behavior that often get us into trouble. Even if we ignore the fire hazard in the office next door presenting itself as a stash of used machines, manuals and backup media, there are reasons to clean up our acts and encourage our colleagues and departments to do so.

Costs

Storing information, you might argue is cheap and it gets cheaper in every generation of technology. Why, we can store so much on this DVD and it took a room full of drives to store this much just a “few” years ago. “Why not save everything?” argues the packrat.

Without even considering the question enterprise wide, the career professional is likely to have seen a dozen or more computers with a number of different backup formats. At RIT, your syllabus might have been created in a text file created on the Sigma, then created in an early version of Runoff, TeX or other text formatting language. After ALL-IN-1 and WordPerfect were introduced to campus; documents were often created in these systems or one of the many editors on either the VMS or the UNIX platforms.

You also might have adopted one of the earliest microcomputers when a built-in, computer-specific word processor was used. The campus sponsored discount programs for many of these early systems. Simply put, in order to retrieve the information stored in any one of these formats, you need the original hardware and the original software. You need peripheral devices (floppy drives, printers, tape drives, etc.) to retrieve some information. For many of the once-supported devices and software, the university no longer retains viable methods for restoring the information.

The risk of saving information in formats no longer easily accessible is that you are not aware of the status of the data. Media such as tapes and floppies degrade to the point that even a suitable device can no longer access the data easily. It is also possible that people intent on collecting identity and other valuable data have the motivation and the means to collect information you are no longer safeguarding.

Increasingly, the nation's courts are imposing requirements to produce information. Agencies, businesses, universities and individuals are being asked to produce electronic evidence; sometimes with open-ended requests for all relevant records still in your possession. The associated costs for some larger organizations can run into the millions as the courts order retrieval from portable devices (floppy disks, CDs, cell phones, PDAs, pen drives, etc.) as well as company records stored in more traditional digital storage devices.

Data stored on hard drives, tapes, databases, calendaring systems, courseware, and other hardware and software are part of the discovery process in some court actions. The court assesses costs on both sides of an argument in some cases—placing the burden of discovery on the plaintiff as well as on the defendant. Settlements are sometimes reached based on the fear that the mounting costs of discovery are not worth it. Fines and penalties are levied when discoverable material is destroyed during or just previous to indictments.

Considerations

Each of us is in partial control of the retention of computer records. What considerations are needed to moderate the risks associated with data retention.

Here are few suggestions:

1. Create a department-wide process for records retention, write it down, communicate it and adhere to it. The department's Information Access and Protection Plan may already contain much of what is needed in your department.
    - This action protects your department from open ended discovery of all records,
    - It has the potential to retain records that are necessary to your operations.
2. Determine if another unit at RIT (Registrar, Human Resources, etc.) are charged with and have a retention process for records you are keeping.

   - Ask the office most familiar with the legal requirements for retention to safeguard the information for you.
   - This action protects the information from discrepancies and the issues associated with records handling and custody.
3. Consider the data when converting to a new technology
   - Include in your conversion plans the need to destroy or convert records stored in the old format.
   - Include in your conversion plans any need to retain some or all of the old technology for the purpose of accessing information. Include a phase-out date for any technology retained.
4. Determine what, if any records, you are legally required to retain.
   - Make sure your college or department is retaining in a usable format, any record it is legally required to retain.
   - Transfer any record that needs to be retained by another entity and destroy your copy.
5. Consider periodic review of records retention.
   - Records might be a risk at some point. Make it part of an annual, documented process to have older records destroyed, with documentation of the destroyed materials and dates.
6. Educate everyone in your department about what a record is (email, voucher, receipt, catalogue, resume, etc.) and what your department process is for retention and destruction of the records. Make sure everyone is aware that working outside this process creates risk.
   - Include in your training any students who handle sensitive records.
   - Consider make records handling education a yearly event. The policies and laws governing records change over time as do the methods of retention the department has in place.

A lesson learned from the recent campus-wide effort to replace the use of security numbers as an identifier was that identity information exists in many forms on campus. Adding to this the information on degree requirements, portfolio formats, meeting minutes, grades, electronic research notebooks, and a host of other information essential to the operations of RIT, underscores the importance of best practices in data retention as a key to ongoing success.

Minimizing the risks associated with records retention is the responsibility of each person. Developing that culture will minimize the risk of being required to produce material and may even keep a few obsessive cleaners happy!

For more information about data retention and information access, see the RIT Institute Information Access and Protection policy: http://security.rit.edu/iap.html

Consider attending a Digital Self Defense 103 (Information Handling) class. Sign up through CPD.

Online Training Available for Microsoft Windows Vista and Office 2007

Want to learn more about Microsoft Office 2007 or Windows Vista? As of the end of February 2007, the following self-paced courses were available through CPD’s E-Learning Zone (http://www.rit.edu/cbt/ - you will need your RIT username and password to login):

- Microsoft Office Word 2007: New Features(First Look)
- Microsoft® Office Access™ 2007: New Features
- Microsoft® Office Excel® 2007: Level 2
- Microsoft® Office Excel® 2007: New Features
- Microsoft® Office PowerPoint® 2007: Level 1
- Microsoft® Office PowerPoint® 2007: Level 2
- Microsoft® Office PowerPoint® 2007: New
- Microsoft® Office Word 2007: New Features
- Microsoft Office PowerPoint 2007 New Features (First Look)
- Microsoft® Office Excel® 2007: Level 1
- Microsoft Office Access 2007: New Features (First Look)
- Microsoft Office Excel 2007 New Features (First Look)
- Microsoft® Office Access™ 2007: Level 1
- Microsoft® Office Access™ 2007: Level 2
- Microsoft® Office Word 2007: Level 1
- Microsoft® Office Word 2007: Level 2
- What's New in Microsoft® Office InfoPath® 2007
- What's New in Microsoft® Office OneNote® 2007
- What's New in Microsoft® Office Outlook® 2007
- What's New in Microsoft® Office Visio® 2007 (Revision B)
- Getting Started with Microsoft® Office Groove® 2007
- What's New in Microsoft® Office Visio® 2007 (Beta)
- Microsoft® Windows Vista™: New Features