University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

3-17-2006

Computer Network Security and ARL Libraries

DeeAnn Allison
University of Nebraska-Lincoln, dallison1@unl.edu

Scott Childers
University of Nebraska - Lincoln, scott.childers.sels@gmail.com

Follow this and additional works at: https://digitalcommons.unl.edu/libraryscience

 Part of the Library and Information Science Commons

Computer Network Security and ARL Libraries

DeeAnn Allison and Scott Childers

DeeAnn Allison is the Systems Librarian for the University of Nebraska – Lincoln Libraries (dallison1@unl.edu)

Scott Childers is the Assistant Systems Librarian for the University of Nebraska – Lincoln Libraries (schilders1@unl.edu)

ABSTRACT:

This article will review current recommendations for computer security practices for staff computing, summarize current practices in US Association of Research Libraries and propose further areas to explore.

Computer and network security has become more and more a part of academic libraries list of concerns. Libraries collect information about their patrons that must be protected and kept confidential. They also utilize many different types of networked applications for the creation, storage, retrieval, and dissemination of information. There have also been an increase in the number and the variety of attacks and reasons why an individual would attempt to break into a computer network. Access to the machines to turn them into drones for other attacks is also a malicious goal of some attacks, ignoring what data is available on the machine. Academic libraries must have a security strategy for prevention and that strategy must include cooperation with other entities, solid risk assessment, efficient technological solutions, strong policy, and education of their staff and faculty. The authors' focus in this article is on implementing these for you staff computing, not in public computing areas such as computer labs or research stations; however, much of what is presented is applicable to the public arena.

Security Strategy for Prevention

The 2002 Federal Information Security Management Act (FISMA) established requirements for federal agencies policies and practices on information security. EDUCAUSE has also developed a series of documents outlining security practices for higher education on their website at http://www.educause.edu. The strategies for creating a secure data environment include common threads of cooperation, risk assessment, preparedness, and protection. The first step is developing cooperation between entities responsible for technology and technology policies. Assessing the potential for security risks, developing policies that address the risks and procuring and implementing

technology that reduces risks are the next steps. This is followed by educating faculty, staff and students about the policies and procedures that have been put into effect and how they contribute to a secure environment.

Cooperation

Managing network security in the library requires cooperation among computing areas to put into place policies, technology and technology practices that will reduce threats caused either intentionally or unintentionally by people using computing resources. This cooperation extends to federal, state and academic units. This is important since networks, like other utilities, cross jurisdictions making it possible to launch attacks from both inside and outside the organization. Within the university, the library must coordinate technology practices with other information technology units. "The only way to effectively protect against a cyber attack is by establishing strong risk management policies and procedures that bridge gaps between units within the enterprise." ("RMs have …" 2002) Working together, staff from the libraries and other campus units can identify and assess risks, develop policies, and design and implement hardware and software based security systems that eliminate many of the threats. These solutions incorporate best practices for managing data and hardware. Human networking is also an important part of the process. Informal and formal connections between staff working in other areas can assist in the troubleshooting of problems, consolidate training for information technology staff, and reduce reaction times when security incidents occur. It can also help increase the physical security of the in-house systems by controlling access to systems to trusted individuals.

Risk Assessment

In a time of tight budgets no administrator wants to waste dollars on prevention of risks

that are unlikely to occur. The identification of risks should ideally be done before

policies are formulated. "During the risk-assessment phase you should: identify your

important assets (firewalls, e-mail and Web servers, as well as your data); identify the

threats they are exposed to; perform a vulnerability assessment to understand current risk

levels; identify the costs of rectifying vulnerabilities vs. the cost to repair an attack should

one success-fully destroy/steal data, or otherwise render your network inoperable; and

take into consideration negligence lawsuits, due to the inadvertent exposure, theft or loss

of client data."(Ellis 2003) Another factor is the damage to an institution's reputation

when resources are compromised. It is an important factor that shouldn't be ignored,

although it can be difficult to calculate the cost of damage to an institution's reputation.

To determine the probability of an attack it is helpful to look at recent statistics on actual

attacks.   A 2004 survey conducted by CIO Magazine and PricewaterhouseCoopers

included 8,100 IT security professionals. It provides general information on the current

state of security across consulting and professional services (13%), government (10%),

computer-related manufacturing and software (9%), financial services/banking (9%),

education (7%), and healthcare (5%). "In terms the effects of attack, 50 % reported

network slowed/unavailable (flat compared to 49% in 2003) and 44 % reported that e-

mail and other applications were unavailable (down from 53% in last year's study.)

Twenty-five percent reported unauthorized outgoing spam sent from company servers

(we did not ask this question last year) and 20 % listed OS programs or files were altered

(again, question was not asked last year.) Only 37 % reported that records or files were

compromised, damaged or lost (combining customer records, employee records,

confidential records, internal records) down significantly from last year (58%)." (Ware

2004)

For most libraries, the area of greatest vulnerability is database content that might include

personal information on library patrons. The next vulnerable area is damage to operating

system software or other virus-like attacks on library computers. The labor costs of

dealing with compromised systems can be enormous when it is necessary for technical

staff to visit individual computers and remove dangerous code, or rebuild servers.

Libraries will also be impacted by vulnerabilities in less obvious ways such as the amount

of time staff spend dealing with spam e-mail or cleaning infected computers.

Calculating the potential cost of damage to library systems can be difficult. There are

different formulas for expressing this risk. One commonly used formula is the total

amount of loss to the institution times the probability that the event will happen. For

example, a rare book housed in a secure location will have a low probability of loss but a

high value. The formula would be the loss of a rare book valued at $10,000 times a

probability that a loss will actually happen of 1%, gives the damage estimate of $10,000

x .01 = $100. Overall, this might be evaluated as a small risk. However in the event that

it was actually lost, the real cost would be $10,000 plus the damage to the library's

reputation.

Another way to look at this problem is to consider system down time. In the modern

academic library, down systems are more than an inconvenience, down systems cause a

loss in productivity as staff are forced to find "off-line" work they can do while they wait

for the systems to come up. In addition, most patrons walk away when they discover the

computer(s) are down. Using the previous formula we developed the estimated costs in

Table 1.

TABLE 1
ARL Library Data
2002-03

Amount of Downtime	Median Combined Salaries & wages	75% Prod with 50% chance	50% prod with 50 percent chance	25% prod with 50% chance
1 day	$2,785.59	$348.20	$696.40	$1,044.60
4 hours	$696.40	$87.05	$174.10	$261.15
1 hour	$348.20	$43.52	$87.05	$130.57

According to the 2002-2003 Association of Research Libraries (ARL) statistics, the

median expenditure for library staff in a university library is $724,253. (Kyrillidou and

Young 2002, p. 41) Table 1 illustrates how the calculation changes as dependency on

automated systems increases. The 50% probability factor was taken from the CIO

Magazine and PricewaterhouseCoopers survey. (Ware 2004) The first column shows the

combined salaries of staff for one day, four hours and 1 hour time periods. The second

column indicates the cost if the staff are able to continue to work with 75% of their

productivity. The fourth column shows an estimated cost if the staff could only be 50%

effective. The final column shows the calculation if the staff can only be 24% effective.

As predicable, the cost increases dramatically with the dependence on technology and the

length of down time. This is just one measure of potential risk. A complete picture of

losses would include any additional factors that were identified during risk identification.

Policies can be put into place that will articulate the institution's regulations and

expectations for computing behavior once risk assessment has identified the greatest

areas of vulnerability and targeted the areas of greatest loss. These policies will provide

the foundation for selecting security technology, developing procedures for handling data

and hardware, and for educating staff on acceptable computing behavior.

Policies

Information technology polices are the cornerstone of a security program. They must

provide clear information to those using computing facilities and data about what is and

what is not acceptable behavior. These policies will both inform people on acceptable

computing practices and provide the basis for enforcement in cases of non-compliance.

The CIO Magazine and PricewaterhouseCooper 2004 survey indicates that organizations

are increasingly developing policies to address security.   "Eight percent of those

surveyed said their organization had no formal security policy, down slightly from 10

percent reported last year." (Ware 2004)

Effective policies must be in a format that can be easily communicated with very

unambiguous wording on acceptable and responsible behavior. They should be written in

plain English that requires minimal interpretation, more like "10 commandments" instead

of a large manual that would only gather dust. (Nicolle 2004)

Technology

Technology is often the first choice to solve the security problem after an organization is

attacked.   The 2004 CIO Magazine and PricewaterhouseCoopers survey indicates that

expenditures for information security are consuming a larger portion of expenditures for

technology.   "Infosecurity budgets remained relatively flat compared to last year;

however, infosecurity budgets as a percentage of the overall IT budget rose slightly (3%

on average) from 10.93 percent in 2003 to 11.27 percent in 2004." (Ware 2004) On

university campuses security includes on-site departmental computers and personal

computers that students and faculty bring to campus. Technology based solutions try to

address both of these areas by protecting the network and individual resources on the

network through a combination of hardware and software solutions.

 Security does not stop at the physical boundaries of the campus. Most universities

support telecommunicating activities for their staff and students. This is particularly

important for universities engaged in distance education.   This requires security to

authenticate and control off-campus access to private information. Another growing

concern is managing lap-top computers that may carry sensitive information when

employees store confidential information on their personal computers for work purposes.

This information is then transported back and forth from home in and out of the campus

security measures. Five years ago, this would have been about 5% of the users, but now

it could be close to half. (Conry-Murray 2002) Although off-campus computers are

outside the direct control of the university, campus data is certainly under the protection

of the university and should be covered by security policies. This problem is beyond the

control of most technology based solutions but it can be addressed with policies and staff

education.

Education

Most security holes in a networked environment are not technological ones, but human

ones. A majority of those holes are created unintentionally by users not understanding

fully the policies that are in place, or not knowing the consequences of their actions. "Although there are many methods and tools for breaking into systems, a vast majority of attacks are aimed at what are likely the weakest and most easily exploitable aspect of your security—human users and well-known software bugs." (Banerjee 2003) This is one reason why the federal government put emphasis on training in FISMA. "FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks." (USGAO 2005 p. 18)

Too much reliance on technology based solutions can lead to staff complaisance about security; the attitude that security is someone else's job. "Higher education offers many examples of security incidents leading to confiscation of hardware by federal authorities, loss or corruption of critical research data, and worse…most could have been prevented with better education." (Payne 2003) An educated staff and library clientele adds an additional layer of protection by creating a "human firewall" against social engineering ploys used in computer attacks and unsafe activities that would compromise security. "Employees can play a big part in keeping sensitive information inside the organization and out of the wrong-hands. But without the proper education and training, a well-meaning worker can negate the success of your security products." (Coe 2003)

There are two goals for a staff security education program: first to generate a culture of security vigilance- where it is second nature to be aware of concerns for privacy and

protection of information resources, and secondly to cultivate cyber ethics. Cyber ethics

often gets lost in the fast moving world of technological developments. An individual

who would never consider shop-lifting a CD from a store might nevertheless think

nothing of downloading copyrighted music or movies off the Internet. Education about

the importance of intellectual property rights and acceptable computing behavior is

becoming just as important as showing people how to use a database.

A network and data security education program should include topics such as:

- good password practices

- safe email habits on how to avoid viruses, scams and hoaxes

- applicable policies on computer use from the university, local, state, and federal

    levels including HIPAA, Gramm-Leach-Bliley, and the Patriot Act information

- related physical security aspects such as needing ID proof, with no exceptions, for

    access to restricted areas or preventing unauthorized viewing of screens containing

    protected data

- what to do in the case of an actual computer emergency such as a wide spread virus

    infestation

- requiring proof of identity before providing or confirming patron information to a

    patron

A successful education program will concentrate on explaining the reasons for having

certain policies and why certain behaviors are considered "bad" as much as informing

users on what the policies are, and defining unacceptable behaviors. A successful

program not only improves security at our institutions, it may actually reduce information

technology costs as other IT training has proven. "The positive impact of formal user training has been shown by a study of NHS staff in Manchester who have achieved the qualification, It found that the number of people calling regularly on IT support dropped from 71% to less than 5%. In addition, these staff were saving an average of 38 minutes a day because they were no longer struggling with IT." (Kavanagh 2004)

Survey of ARL Libraries

In light of current recommendations for information security programs the authors sent a survey in March of 2005 to 100 academic ARL libraries in the United States to solicit information on security practices in their institutions. Thirty-four institutions responded for a 34 % response rate. This survey revealed some interesting trends among the ARL academic libraries.

Only 6% of the ARL libraries responding to the survey reported that they had no security policies. This is lower than the 8% reported in the CIO Magazine and PricewaterhouseCooper survey.   Eighteen percent reported that decisions or policies were made by a central authority at their system-wide or state level. Fifty-three percent reported that policies were formulated at the campus-wide level, with 6% reporting responsibility at the library level. Thirty-two percent reported a shared responsibility between multiple units.   Since most libraries do not control all the vulnerable points of security, it is imperative that staff in the library coordinate and work closely with IT staff from the campus.

Libraries are struggling with ways to control threats to systems while supporting

beneficial flexibility in computing. A combination of software and hardware technology

is being employed to protect sensitive data and the network infrastructure. Table 2

summarizes the technologies employed by the libraries responding to the survey.

TABLE 2

ARL Academic Libraries Security Technology	% of All Respondents
Automated anti-virus updates	100%
Automated operating system patches	88%
Using profiles and permissions to restrict activities	88%
"Turning off" functions/features	82%
Password expiration	79%
Requiring complex passwords	79%
Filtering extensions in E-mail	71%
Networked based security	68%
White lists of allowed executables	38%

These results show that ARL libraries are doing what they can, as far as using

technological solutions. The majority of respondents were doing every technological

aspect that the authors asked in the survey, except using "white lists" of allowed

executables. White lists are lists of programs that are explicitly allowed to run on a

computer. Programs not on the white list will not be allowed to run. For example, you

could put a web browser, word processor, and the automated library system client in the

white list, but leave out everything else to lock down a computer. White lists are often

easier to define than black lists, or lists of prohibited executables, but it does cut down on

the flexibility to make changes in software packages on that computer.

Education is another area where libraries are making progress. Six institutions (14%) reported that they had some type of required education on security. Table 3 shows the areas covered during instruction and the percentage of libraries reporting training in that concept.

TABLE3

ARL Academic Libraries with Education Programs	% of Libraries with Education Programs
Information on academic (university) policies/regulations that affect personnel.	100%
Information on library policies that effect personnel.	100%
Privacy and confidentiality of personal information.	100%
Password security including tips or requirements for strong passwords.	100%
Information of computer viruses.	83%
Information on email scams and hoaxes.	83%
Patriot Act procedures.	67%
Information on federal/state laws and regulations that affect personnel.	50%
Security hazards or restrictions on installing "free" software from the Internet.	50%
Information on Spyware and/ or Adware.	50%
Institutions requiring sign-off documents	33%

Of the institutions who reported they had education efforts, we found that the focus was mostly on policy. All education programs had curriculum that included university and library policies. All institutions also reported covering privacy, confidentiality, and proper password protocol. A majority also gave information on network security topics

such as computer viruses, email scams and hoaxes and Patriot Act procedures. Only one

half discussed federal and state laws and regulations which may leave staff without a

complete picture of their legal obligations. Also only being covered by half was

distributing information about possibly hazards of installing software that had not been

investigated and could be spyware or other malicious programs

Only a third required their staff to sign-off that they had participated in security training.

Having a signed document gives administrators better footing if employee discipline

problems arise, preventing a scenario where a staff member could claim they did not

know their responsibility to protect their password or that the records they worked with

were confidential.

One important finding from the survey is that training in security seems to have similar

benefits as general technology training. Respondents to the library survey that have no

mandatory training covering security estimate that they spend an average of 20 hours per

week on security issues. These issues included updating software, virus cleaning,

managing passwords and training. Libraries with mandatory education programs

reported an average of 10 hours per week. That is a fifty percent reduction in technical

support for libraries with security education programs.   This survey covered a small

sample of libraries but it is certainly worth further research to verify that staff education

programs helps to counteract the increasing cost for security. One specific example is at

the authors' home institution where a security education program was implemented. In

the year after the program was instituted, virus and other malware infestations were down

39% from the year before the program was instituted.

Conclusions

Libraries are becoming more involved in the security area, not only as users of networked resources, but also as repositories of protected or confidential data. A comprehensive security defense relies on cooperation between technology units and requires risk assessment, sound policies, technology and education. Our survey reveals that libraries are cooperating with other units and are beginning to respond to the educational challenges posed by security questions. Our survey also suggests that a strategy that emphasizes using education as an important element can improve security and reduce the labor costs associated with security. Libraries have always embraced their call to share information, but they must also be cognizant of their responsibilities to protect information and the systems that information resides on.

References

Kyle Banerjee, (2003) "How Much Security Does Your Library Need?" *Computers in Libraries*, volume 23, number 5 (May) p. 14.

Kathleen Coe, (2003) "Closing the Security Gap," *HR Technology*, volume 48, number 8 (1 August) p. 95.

Andrew Conry-Murray, 2002 "Securing End Users from Attack," *Network Magazine* (October) p. 28

C. Ellis, 2003. "7 Steps' for network security", *Communications News* volume 40, number 2 (February) pp. 36-7.

John Kavanagh, (2004) "NHS end-user computer training scheme slashes IT support costs", *Computer Weekly* (13 January) p. 32.

Martha Kyrillidou & Mark Young, 2003. *ARL Statistics 2002-2003* Washington D.C.: ARL.

Lindsay Nicolle, 2004. "Take Control of Your Staff" *Computer Weekly* (9 November) accessed
http://www.computerweekly.com/articles/article.asp?liArticleID=134847&liFlav , March 17, 2006

Shirley Payne, 2003. "Developing Security Education and Awareness Programs," *Educause Quarterly*, number 4 p. 49.

 "RMs have what it takes in war against terrorism", 2002. *National Underwriter (Property & Casualty/Risk & Benefits Management Edition)* volume 106, number 15 (15 April) p 10.

United States Government Accountability Office, (2005) *Information Security; Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO Report 05-552 Washington D.C.: GAO

Lorraine Cosgrove Ware, 2004. "The State of Information Security, 2004," at http://www2.cio.com/research/surveyreport.cfm?id=75, accessed March 17, 2006.