GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

How to Identify and "Contain" Some of the Information Security Problems Created by Unique Business Environments

John Cupps
GSEC Practical – Version 1.2e
8/10/2001

Introduction

An organization is characterized by its business environment. From an IT or information security perspective, the business environment consists of the users, the physical layout of the information systems, and the organizational requirements of the information systems. Every entity has a different business environment and network administrators must understand the organization's setting in order to contain or eliminate potential security problems.

A university setting will be used to illustrate this idea, that an organization is characterized by its business environment. Several aspects of the university's business environment are unique only to universities. One such aspect to be explored in detail is the effect of the student user group within the environment and the problems they can create for information security initiatives. In order to contain the problems within this environment an analysis of the student user is necessary.

What qualifies an individual to write on this subject? In my case experience is my primary qualification. I've spent the last five and half years in the same university environment. The first four years, as a business school undergraduate student, I did almost everything imaginable to make information security workers cringe. After graduating, I pursued a position working in the IT department of the business school and have spent the last four months researching and developing solutions to help contain the problems created by the university business environment.

Analysis of the Student Users – The Problem

University users can be broadly classified under four different types: students, staff, faculty and administrators. Compared to other business organizations, there seems to be nothing unique about this list of users; all have email accounts, Internet access and various rights throughout the network. However, after examining the details of users in the university setting, it will become clear that there are several information security problems that are unique to academic institutions.

Although users can create problems for information security initiatives in any environment, the group that causes the most problems in the university setting is the student body. There are many reasons why this user group presents problems for administrators. For example, this fall, thousands of 18-year-old students will take their "Out of the Box" secured Windows 9x/Me/XP computers, plug them into a university network, surf the internet while unsupervised and at a high speed, sign up for six different file sharing or chat services while opening every single forwarded attachment they receive via email.

© SANS Institute 2000 - 2005 Author retains full rights.

Two general factors characterize this user group: carelessness and a lack of knowledge regarding information security due to their relatively young age[1] or experience level. Most college bound students today comfortably use computers and navigate the Internet, however, many do not know about the existing and new threats targeted at their personal computers. In addition, the relaxed atmosphere of college contributes towards the careless decisions regarding their information security.

The table below provides a few examples of situations where students' lack of knowledge and carelessness lead to security problems. Alan S. Horowitz complied a top ten list of security mistakes on July 10th 2001.[2] I have found, based on my personal experience as a student and network administrator, inexperienced students routinely make five of these ten mistakes.

Alan S. Horowitz's Security Mistakes	Student Security Mistakes
Posting password and username information on the not-so-subtle Post-it note, on the monitor.	Students today are generally more resourceful and have too much time on their hands to use only Post-it notes. They use Excel spreadsheets to neatly organize their usernames and passwords. Although these spreadsheets are too big to tape to monitors, students still post this information near by. When I was a student, I used the wall right next to the keyboard to post my valuable information.
Leaving the machine on, unattended.	During midterms and finals, the computer labs are crowded. Students want to save their place at a workstation and leave the lab to get a bite to eat or take a break. Often times when they do this, they leave themselves logged on the computer. I have seen this maneuver countless times.
Opening email attachments from acquaintances or strangers.	Students look to email attachments as a source of comic relief. Apparently, this is necessary in order to take a break from, or to deal with, the stress of college life. When I was in school, I logged into my email account and first opened all of my forwards. Later I read the rest of my emails only if the computer did not crash because I opened a malicious email attachment.

[1] According to the US Census Bureau of the 8,434,000 full-time undergraduate students enrolled in college in the year 2000, 6,026,000 were between the ages of 14 – 21 and 7,505,000 were between the ages of 14 – 24.
[2] www.info-sec.com/internet/01/internet_071001b_j.shtml

© SANS Institute 2000 - 2005 Author retains full rights.

Poor password selection.	While an undergraduate, my first password was my username; my next password was the school nickname plus my football jersey number. These are typical examples of poor password selections.
Being slow to update security information.	The first computer I used in college still has its original Windows 98 out-of-the-box configuration on it (of course the Pentium 133 with 32 Megabytes of RAM is no longer in use). I did not even know operating systems had "patches," let alone what patches were, until I started working full time for the university.

Another factor making this group of users a potential problem for administrators, is the unsupervised use of private computers while attached to a high-speed Internet connection. Students take advantage of the 24-hour high-speed Internet access in their dorm rooms and, thus, are capable of creating any number of information security problems. The use of file sharing applications, instant messaging and "late night" web surfing are the major culprits that lead to security problems.

One such culprit, file-sharing programs, can cause several problems in a university setting. The first concern relates to denial of services throughout the university network. The use of programs, such as Napster[3] and Gnutella,[4] are responsible for filling up the university's bandwidth and, thus, interfere with regular network services. The use of these programs is increasing and is having a growing impact on the disruption of services. According to Wayne Heyward, in an article publish on ZDNet.com last year, as much as 40% of a university's bandwidth is used for non-academic purposes.[5] In my own experience, the use of bandwidth for non-academic purposes is even higher. In fact, at the university where I work, Internet traffic drops significantly when students are not on campus. These types of programs not only consume bandwidth, but also increase the risk of malicious code or viruses entering the network. This risk is heightened when other tools, such as Wrapster,[6] are used to disguise files.

While attending university, students desire to stay connected to family and friends on and off campus regularly. The most convenient means of communication is through computers using email or instant messaging. The use of IRCs and instant messaging, in particular, can cause several problems at a university. Two of these problems include buffer overflow attacks on certain versions of AOL's IM and the potential for zombie attacks through IRCs. AOL's IM (AIM) versions prior to 4.3.2229 are mainly susceptible to these buffer overflow attacks.[7] In

[3] www.napster.com
[4] http://gnutella.wego.com
[5] http://www.zdnet.com/anchordesk/talkback/talkback_230995.html
[6] Wrapster is a tool that allows users to exchange any type of file as an MP3. For more information please see http://www.zdnet.com/downloads/stories/info/0,10615,59953,00.html .
[7] http://www.infosecuritymag.com/articles/february01/cover.shtml

© SANS Institute 2000 - 2005 Author retains full rights.

addition to the problems associated with instant messaging, IRC clients are also used to launch major distributed denial of services (DDOS) attacks. Steve Gibson of the Gibson Research Center (GRC) explains how a 13-year-old child used 100s of IRC zombies to launch a DDOS attack on www.grc.com.[8] Most of the zombies used in the attack were home personal computers with corrupt IRC clients and a high-speed Internet connection. Thus, computers with high-speed connections and weak security implementation are targets of crackers for this type of an attack. Thousands of these potential targets are connected to university networks in student dormitories. Thus, poorly configured personal computers combined with high-speed Internet access can create a problem for security administrators.

What are we to do? Student Users – The Containment

In order to contain the problems arising from the student user group, administrators must first analyze and identify the problems. As described above, there are five main security concerns associated with the student user group. Each one of these concerns will be discussed in detail to demonstrate how an administrator can develop solutions that are necessary to contain potential problems. The word "contain" is used because all security problems will never be completely mitigated, especially in a university setting. Unlike most users of other organizations, student users compute on both university owned workstations and private workstations attached to the university network. Despite the challenges of the university environment, it becomes clear after analysis, education and precautionary steps, administrators can help contain many concerns in both settings.

Concern # 1 Student users often write down passwords and leave this information very close to their computer increasing the chances of security violations by unauthorized users. This problem presents itself as a double-edged sword. As a security administrator we hope students will select difficult passwords that prevent unauthorized access, but at the same time, we do not want the students to make their passwords so difficult that they feel they need to write them down to remember the information. To combat this situation, we require all user passwords to be unique and at least six characters long. We also set the passwords to expire after 45 days. In addition to these requirements, we attempt to contain this problem through user education. All incoming freshmen and transfer students are required to take a computer orientation class. This course runs for 60 minutes and covers various computer related issues. During the class, we explain to the students that a "good" password includes special characters and numbers in addition to letters. We also advise the students to not record password information anywhere, (especially not next to their computer), and to not share password information with anyone. These recommendations seem very simple and logical, but based on experience, without user education on security issues; student users will continue to make these mistakes.

Concern # 2 Student users often leave workstations unattended while they are logged into the network. This creates a security problem because an authenticated workstation abandoned by the student provides easy access to the network for unauthorized users. Prevention of this problem requires the intervention of the administrator. In dormitories, students leave themselves

[8] http://grc.com/dos/grcdos.htm (Note: Very interesting reading)

© SANS Institute 2000 - 2005 Author retains full rights.

logged into their computer when they leave the room. In this setting, the physical access to the workstation can be denied with a locked door and the risk of unauthorized users decreases, (with the exception of the roommate). However, the lab environment presents a different situation. University labs are very busy during midterms and finals; many times a line forms to use one of the workstations. In addition, there are a few resources available only in the computer labs. As a result, users are reluctant to log off their computer and loose their workstation if the need to take a break or run an errand arises. This action by the user is both unfair to other users and potentially creates a security problem. There are several actions administrators can take to prevent unauthorized access to the network in this situation: run an event triggered executable resetting the workstation after the screen saver has been active for several minutes; lock the workstation and force the user re-authenticate to the network after the screen saver has been activated; or patrol the lab and log users out of abandoned workstations. However, in the university environment, the first two options present concerns of their own. Resetting the machine after screen saver activation may potentially erase or corrupt students' work. Setting the workstation to lock after the screen saver activates allows students to walk away from the workstation when the lab is crowded and return to the computer whenever they please. This is unfair to those students waiting to use the workstations. Therefore, in a university environment we find it is best to patrol the lab with student workers logging out workstations with active screen savers. (Note: In our environment, screen savers start after 15 minutes of inactivity on the workstation). In addition, during the orientation class, we attempt to educate our users regarding the possible activities of unauthorized users with access to the network while under their name. Thus through the use of education and a simple procedure we are able to contain unauthorized uses of our network via abandoned workstations.

Concern # 3 Student users open almost every email attachment they receive. There is an increasing risk involved with carelessly opening every email attachment with the large number of viruses[*] in existence today. As administrators, we attempt to alleviate the security problems created through malicious email attachments with user education, Antivirus software and a weekly workstation image restore. During the orientation class, we explain to the users what viruses are and touch on the many forms that they may appear as. However, from experience we found education was not enough to prevent the careless opening of email attachments. Thus, we use Antivirus software on both the email servers and the workstations.

Despite user education and the use of Antivirus software, we have found viruses enter the system through other means such as web-based POP email systems, for example Hotmail or Yahoo! Mail. In order to repair any damage from the virus payload or to clear the workstation of any undetected viruses, we run a workstation restore on the entire lab at least once a week, thus providing a clean workstation for the students' use at the start of each week. The weekly restore ensures that the longest a workstation could be down is seven days. However, the administrator can manually run the restore anytime, thus the minimal time a workstation is out of service due to virus damage is approximately 60 minutes. Thus, through the use of education, Antivirus

[*] For the purpose of this paper, the word virus is used to represent all forms of malware: viruses, worms, trojans, malicious applets, etc… According to the SANS Institute's TRACK 1—LevelOne SANS SECURITY ESSENTIALS workbook: "A virus is a piece of parasitic code (or program) written specifically to execute on behalf of the user without the user's permission (or knowledge)." [Harris and Cole. Pg. 7-3] Baltimore, MD. May 2001

© SANS Institute 2000 - 2005 Author retains full rights.

software and workstation restores, administrators can contain the security problems created with email attachments.

Restoring a clean image on workstations requires a workstation-imaging tool such as Norton's Ghost.[10] The following steps are taken to set up a workstation in order to use imaging software to run a restore. When setting up the original image on the workstation, a two Gigabyte partition is created to hold the restore image. Having the restore image stored locally minimizes network traffic during the restore process. Once the original image is pushed down to each workstation and finalized, a clean copy is created onto the partition created earlier. Depending on which imaging software is used, it is possible to set up when the restores will be run via the management software or to use diskettes to complete the process manually. In my experience, running the restores very early Monday morning eliminates any trash accumulated on the workstations over the weekend. This restore process significantly helps to contain a majority of user created problems on university workstations.

Concern # 4 Student users often fail to update their computers with current security patches. This problem is very difficult to contain because it involves the user's private computer, which administrators rarely have physical access too. These private computers are directly connected to the university's network and without current updates they create a security problem for administrators. The solution to this problem depends on education and an organization's policy regarding this type of usage. At universities, the best way to contain this problem is through the education of the user. Before incoming students can directly access their network files or run network applications via a non-university computer, our technology center staff must configure their private computers. During this process, technicians configure the computer for proper access and verify that the OS contains current security patches. This is also a good time to eliminate unnecessary communication protocols. While the technician is verifying the computer's OS, he or she also educates the user about the importance of keeping computer security updates current. Additionally, the technician demonstrates how to access the Window's Update site.[11] If desired by the user, technicians also install Window's Critical Update Notification to alert the user when an addition update is required. Thus, through this configuration process, the user is taught what a security patch is, how to access and install these patches, and at the same time the security problems associated with computers without current updates are contained

Concern # 5 Student users consume a large amount of university bandwidth. This consumption can lead to problems such as network lag or in extreme cases loss of critical network services. This bandwidth consumption is directly related to the students' use of various file sharing and chat software. The bandwidth consuming software or tools are usually installed on the student's personal computer, making it difficult to contain. In addition, university environments encourage open ideas and information exchange. Thus, the people involved in the containment of this problem must take into consideration the university's policy on student bandwidth consumption.

[10] http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=3&PID=3431876
[11] http://windowsupdate.microsoft.com/

© SANS Institute 2000 - 2005 Author retains full rights.

There are several steps administrators can take to help reduce the amount of bandwidth that is consumed with these tools. Administrators can educate the users about these tools or limit the amount of bandwidth they consume. Lawrence Walsh of *Information Security* magazine notes, "Except for computer science majors and the self-taught techno-geeks, most college students have no idea that the services they're using for free music and instantaneous communications are peer-to-peer technologies.[12]" For the first time this fall, during mandatory freshman and transfer student computer orientation, we are going to explain exactly what these applications are, how they work and their potential pitfalls. In addition to user education, we run a weekly restore on workstations to help prevent the use of such applications on shared university computers. Thus by taking these steps, an administrator can contain the security problems created with the use of these tools. Unfortunately, the containment of this problem is limited at my university, as policy prohibits the infringement of the flow of information in the university.

However, there are several other steps administrators can take to contain the bandwidth consumption of these file-sharing applications. These solutions are discussed in detail in the cover story article of February 2001 issue of *Information Security* magazine.[13] Al Berg, the author of the cover story, recommends that administrators use the organization's firewalls to block the traffic coming from and going to the servers. As he acknowledges in the article, firewall configuration is an effective way to limit traffic created by instant messaging software, but it is not as effective at blocking file-sharing services. File sharing software's ability to run across any open port prevents filtering of this application at the firewall. Thus, Lawrence Walsh, the author of the case study, sites examples of organizations using other software solutions such as Packetshaper[14] by Packteer to contain this problem. According to the Packteer's website, an administrator can contain the effects of mass file sharing and, through the use of seven-layer classifications, Packetshaper limits incoming and outgoing traffic traveling through dynamically assigned ports.[15] MP3s, the media file type used with Napster, requires this seven-layer classification and thus network administrators can limit the bandwidth traffic allocated to such tools. Thus, depending on the organization's policy of the use of these tools, network administrators have choices to contain the problem.

Conclusions and Lessons Learned about an Organization's Business Environments

A business environment for information security workers includes the users, the physical layout of the information systems, and the organizational requirements of the information systems. These different segments of the business environments must be examined and analyzed by security administrators for potential problems when considering the information security of the organization. No two organizations are going to have the same information security problems. Through the detailed analysis of student users at a university, it has been proven that the users within the business environment of an organization can create different challenges for security administrators. Several factors contribute to the potential problems that student users create in the university business environment, and this paper presented several different ideas to help

[12] http://www.infosecuritymag.com/articles/february01/cover.shtml -- Case Study
[13] http://www.infosecuritymag.com/articles/february01/cover.shtml -- Cover Story and Case Study
[14] http://www.packeteer.com/products/packetshaper/
[15] http://www.packeteer.com/PDF_files/packetshaper/psFeatures.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

contain these problems. These factors are applicable to all users and should be considered by security administrators when determining the potential problem of a user group.

The following two factors were primarily used in the analysis of student users when determining some of the potential problems they could create at a university. These ideas are also a good place to start when characterizing all types of users found in any organization:

Age/Computer experience – Age and experience do not correlate. College interns in an organization might be more computer savvy then a middle-aged executive who has been in the system for 30 years. However, although the same college intern may be computer literate, he or she may also open every email attachment that they receive because they are unaware of the potential security threat this action creates. Whereas, the executive, who may be less savvy with computers, may be more aware that viruses can be spread via email attachments. The common solution for containment of this issue in both situations, regardless of age or experience, is education. No matter whom the user is, when they enter the organization, do your users understand what is expected of them in order to help contain information security problems within the organization?

Attitude towards computing – For example in the university setting, the careless attitude of the student users correlated to their lack of knowledge in regards to potential security problems. Do your users have a laid back approach to computing? Will they open any email attachment? Do they care about the information systems? Are they aware of the potential vulnerabilities their actions can create? Do they care?

The following questions can be asked to help analyze any type of user in any organization:

Prior employment – What type of computer skills have they acquired in previous employment? Did their prior employer have security policies? Were they enforced? What type of Internet access did they have?

Job function within the organization – Are they a high-level employee or principal of the company? Will they be busy during office hours? Or will they spend time free time on the Internet at the end of the day, emailing friends and trading music? Is there workstation in an office or in a cubicle? What will happen to their job or the company if there is an information security problem? Will they care?

Access of the employee – What type of information does this employee have access too? Could they accidentally put proprietary information in a Gnutella network? Can they dial into the company network from home? How difficult or easy is an executive's password?

© SANS Institute 2000 - 2005 Author retains full rights.

References

Berg, Al. "P2P, OR NOT P2P?" Information Security. February 2001.
URL: http://www.infosecuritymag.com/articles/february01/cover.shtml (Cover Story).

Gibson, Steve. "The Strange Tale of the Denial of Service Attacks Against GRC.COM."
4 July 2001. URL: http://grc.com/dos/grcdos.htm

Harris, Daniel and Cole, Eric. TRACK 1—LevelOne SANS SECURITY ESSENTIALS.
Pg. 7-3. SANS 2001. Balitmore, MD. May 2001

Heyward, Wayne. "Why Universities are banning Napster." 24 February 2000.
URL: http://www.zdnet.com/anchordesk/talkback/talkback_230995.html

Horowitz, Alan S. "Top Ten Security Mistakes" ComputerWorld. 9 July 2001.
URL: http://www.info-sec.com/internet/01/internet_071001b_j.shtml (10 July 2001).

United States Census Bureau. Table A-7.
College Enrollment of Students 14 to 34 Years Old, by Type of College, Attendance Status, Age and Sex: October 1970 to 2000.
Internet Release Date: June 1, 2001.
http://www.census.gov/population/socdemo/school/tabA-7.pdf

Walsh, Lawrence M. "Blocking Napster Isn't Elementary." Information Security. February 2001.
URL: http://www.infosecuritymag.com/articles/february01/cover.shtml (Case Study).

Software and Application References

Gnutella – http://gnutella.wego.com/
Product Info – http://www.gnutellanews.com/information/what_is_gnutella.shtml

Microsoft Windows Update – http://www.microsoft.com/
Product Info – http://windowsupdate.microsoft.com/

Napster – www.napster.com
Product Info – http://www.napster.com/company/

Norton's Ghost Corporate Edition 7.0 – http://www.symantec.com/
Product Info – http://www.zdnet.com/downloads/stories/info/0,10615,59953,00.html

Packteer's PacketShaper – http://www.packeteer.com/index.cfm
Product Info – http://www.packeteer.com/products/packetshaper/

Wrapster – http://www.unwrapper.com/
Product Info – http://www.zdnet.com/downloads/stories/info/0,10615,59953,00.html

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: September 25th, 2017

Upcoming Training

Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event