Global Information Assurance Certification Paper

Defining the Risk, Creating a security policy, and Fixing the Top 20
Security 101 for a small school with limited resources

John Bruggeman
GSEC – v 1.4b

Abstract: This paper was written for non-technical administrative personnel and technical support staff who do not have a security background and work at a small[1] College. It is meant to raise questions and expose hidden liabilities that are frequently glossed over, due to the limited resources of smaller schools, until a serious security breach occurs.

With the growth of information systems, small department level databases, and portable media storage devices, it is critical to understand what security risks exist for a schools data. Who can access the data, when they can, and where they can, need to be clearly defined and policies created to provide a guideline for all departments to follow and implement. Even if you feel that you don't have enough time, at least address the Top 20 vulnerabilities. You can significantly reduce the risk of a successful amateur attack if you address the top security vulnerabilities defined by SANS and the FBI http://www.sans.org/top20.

These three simple steps, defining the risk, creating a security policy, and fixing the top 20 vulnerabilities, form the basic security structure for a small school with limited resources.

What is at Risk?

If this is an "Information Age" – and we are an information driven economy, what are we doing to make sure our information is safe, secure, unaltered and accessible? If I am responsible for computers or information systems at a small school, what should I worry about? Am I a target if I have a low profile?

The answers to these questions are both simple and complex. Should you worry? Yes. What should you worry about? Probably much more than you think you should.

There are basic security rules and policies everyone should implement at school and at home to make sure your data is safe and secure. What you need to focus on will vary depending on your risk assessment, not your budget.

What is at risk could be the confidentiality of your student records, your payroll information, the health records of your students, the reputation of the school, perhaps, even your admissions policies and procedures. Yale found this out when Princeton hacked into their database[2]. You might even lose your job over a security or confidentiality breach or policy lapse[3].

A small school with a very low profile is still at risk. You need to seriously assess the threat to your data. Every computer connected to the Internet is at some risk to hackers

or other possible breeches of security. Below are three points that define a basic security platform, Security 101 for a small school.

- Defining Risk
- Creating a security policy for computer usage
- FBI/SANS Top 20 vulnerabilities (http://www.sans.org/top20/)

Defining Risk

The first thing you need to do is define your risk. What do I need to protect? The three core principles that you want to keep in mind as you think about your data are:

Confidentiality, Integrity, and Availability

What data do you need to protect from prying eyes, probing fingers, or careless users?
Would I know if data was changed in my database or on my website?
What if I can't get access to my data for a hour, a day, a week, a month? How will that impact my school?

When you think about risks to your data, think about the threat vector (where would an attacker strike and why) and what is vulnerable (a workstation, server, website).

Risk = Threat x Vulnerability

Keep in mind that a vulnerability can exist (and you might delay fixing it) if there isn't a threat that targets that vulnerability.

Would someone have to be on campus to attack me?
What could they attack or steal if they were on campus vs. over the Internet?
Why would anyone target me to attack or hack?
Who knows the root password, or the admin or administrator password?
Are my internal and external servers and workstations fully patched?

This might seem like too daunting a task to even begin to address. Or you might feel that you won't get time from your supervisor or manager to focus on security. Consider the legal liability to which your institution is exposed if you don't address the vulnerabilities you have and document the security and audit measures in place to mitigate the vulnerabilities. What access control methodology do you have in place and can prove works, if you are taken to court?

Some liability is clearly legislated, like the Health Insurance Portability and Accountability Act (HIPAA) http://www.sans.org/rr/policy/HIPAA_policy.php, http://www.hhs.gov/news/press/2002pres/hipaa.html, (http://www.medsoftusa.com/hippa.htm) or Family Educational Rights and Privacy Act (FERPA) http://nces.ed.gov/pubs97/p97527/CONTENTS.HTM and http://www.nyu.edu/apr/ferpa.htm.

Some are privacy issues that would be settled in a civil court, like a lawsuit filed over the release of personal information intercepted via email or voicemail. You have to know, and consult your own legal counsel regarding what you can and can't do, what is legal. You are able to monitor some conversations at the work place, Carter, Ledyard, and Milburn indicate here http://www.clm.com/pubs/pub-914447_2.html. Some issues are clearly criminal in nature, like this grade manipulation for money case http://www.vnunet.com/News/1132421.

For many small institutions the answers to the above questions can be glossed over until after an incident has taken place (i.e. a loss of data, data manipulation, loss of confidentiality). Some small schools have not addressed the issue of data privacy and data integrity because they think they don't have the time, or think security is too complex, or believe they are too small to be of interest to hackers. I know this first hand, I was one of those small schools. Two distributed denial of service (DDOS[4]) attacks and three hacking attacks have convinced me otherwise.

The simple fact is that any computer that is connected to the Internet (even briefly via modem) is at risk[5]. A computer that sends and receives email can be compromised with a worm or virus which can then send confidential information to other people either randomly http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html or to one particular email account http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html.

Risk factors can be broken down into the basic reporters questions: who, what, when, where, why, and how[6].

- Who are you interested in keeping out, or in?
  - Do you only want the registrar to have access to student records?
- What are you keeping secure?
  - Are you protecting grade information? Passwords for accounts? Payroll information?
- When are you worried about keeping people out?
  - Forever (e.g. grade information)? Just for a few months or days (e.g. enrollment data for a particular year. Alumni contact information?)
- Where is the data located?
  - On a network server? On a website? On a floppy disk on someone's desk?
- Why do you need to keep it secure?
  - Federal regulations (FERPA, HIPAA), user trust (e.g. passwords, emails, payroll data), business operations (enrollment policies and procedures, target markets, etc.).
- How do you secure the data?
  - Does it have to be encrypted or just hard to access?

WHO

A factor in the assessment stage is asking the question, "Who should have access to this data?" Defining who has access to data at your school is not a task that is

restricted to the Information Technology (IT) department. Most schools have defined some risks, like who can have a master key, who can get into the main office, etc. They have locks on the doors, photo ID's to identify faculty, staff, and students. They have taken care of physical security. But what about data security?

With the growth of data[7], information systems[8], and fast easy access to data[9], the need to identify data security risks has risen faster than many IT departments expected. Sensitive data can be diffuse and portable. Some IT departments may not even know where all sensitive data is stored. Department level databases can contain as much sensitive information as the student records database, but fit on a floppy, a ZIP disk or a memory stick. That makes risk assessment a multi-faceted challenge that requires engagement at the VP level and by all departments[10].

Who can and can't have access to the data helps identify where it should reside. If only the registrar should have access to certain information, then it makes sense to restrict access at the department level, or perhaps to a single person. Data shouldn't be stored in more than one place – both in terms of data integrity and in terms of keeping the data secure. You don't want a copy of the data floating around without access controls and auditing. If the registrar needs to do some work at home, do you want to allow them to take a copy of the database home? Probably not, because you can't control or know who has access to the data when it leaves your network.

Knowing who should have access to the data also helps identify who might want to have access to this information. A student hacker might want to have access to his/her grades in order to change them just to prove it can be done http://www.techtv.com/news/internet/story/0,24195,3412170,00.html or as we have seen before, a competing school might want to have access to the admissions data to see how students are recruited[11].

Now that you know who should have access and who should not, you have an idea where some of your threats originate. If you need to secure your data from students who want to change grades you know that you need to screen student staff members closely to ensure they don't modify grades when the supervisor isn't around. If you need to protect admissions data from a competing school, you know you need to restrict who can access the admissions database and maybe not allow web access to sensitive data.

WHAT

Once you have defined the who, you know part of the what. Some data tends to be more clearly in need of security than other kinds of data. Students records, payroll information, donations, health records, all tend to be data that we know needs to be secure.

Passwords are also obvious candidates for secrecy. You need to keep the password for the administrator account of a NT server, the admin account in a Novell server, or the root account of a Unix or Linux server limited to the fewest number of people and

yet still make it available if needed in an emergency. So maybe you do write down those kinds of passwords but they are literally locked in a safe that requires two people present to access the passwords.

What about the Financial Aid records? There is very confidential information in the Financial Aid department – social security numbers of the students and parents as well as tax information for the student and family tends to be stored in that department.

What about the Development department records? Knowing who gave how much or how little could be both valuable and embarrassing. What donor would like to have that information released or publicized? Correspondence of the President, or the HR department can be very sensitive as well.

Each department needs to review what data they have and what they do to prevent un-authorized access. They also need to have some way to prove that they control access. They might need to prove that they restrict access in a court of law if confidential information is released.

What are you doing to allow only authorized users access to that data? When you know what you are trying to secure you can then begin to assess how valuable the data is and what risks you will accept if the data is compromised (either discovered or manipulated or lost). Once you know that you can begin to put an accurate budget together for protecting your data.

WHEN

The when question can be easily overlooked, but it should not be forgotten. Do you have to restrict access forever or can you relax or remove the security level after a period of time? For some information you will need to keep it secure essentially forever, like student grades. For other data it might only need to be secure for a certain period of time. Student records will most likely need to be protected for the natural life of the student or you might create a disposal date for inactive records like the Univeristy of Illinois at Urbana-Champaign http://www.uiuc.edu/cgi-bin/print_hit_bold.pl/admin_manual/code/rule_67.html.

Enrollment information might be very valuable for a particular year, or a semester, but after a year it might become public knowledge in a final year-end report. Alumni contact information, like an alumni directory, might be private information that only other alumni have access or it might be published in a directory that is generally available. FERPA and HIPAA guidelines can be helpful here for some of the data, for other types of data (Alumni, enrollment) you will be able to develop those guidelines on your own.

WHERE

Where is the data? Is it on the main file server with the NT/Novell/Macintosh file access controls in place or is it stored on a shared drive of someone's PC with limited or no

access control? Is the data small enough that it could fit on a floppy or a Zip drive or a memory stick?

Could someone make a copy of the data on their PC, take it on the road, lose the laptop and allow anyone access to that data? Do you need to allow the data to be portable? Do you need to provide access to the data to people who travel? Do you allow access to data over the Internet via the Web or FTP? Is there only one copy of the data? Do you back up the data and are your backups secure? Do you need to encrypt the data? Do you need to encrypt the backups? Do you need to be prove who can access the data and when they accessed it?

The where question is both simple and complex. You need to know where you are storing the data and what access you need to provide. You also must have some type of file access control in place (Novell/NT/Macintosh file security) with auditing turned on so you can prove who accessed what files. This is where it can get complex because you need to be able to check the access log both now and in the future. Storing and searching these log files can be cumbersome. Creating a standard weekly procedure of saving NT event logs to a ZIP drive and locking it in a safe place can provide a minimum level of auditing, but check with your legal and auditors to see what is required.

WHY

This might seem obvious, but why do you need to keep the data secure? The Federal government requires that some data be kept private (HIPAA/FERPA)? What are the penalties if privacy is lost? Some data is internally sensitive (passwords, HR information, memo's) that if compromised will impact the trust and morale of an institution in ways that are not easy to quantify but can have a very large impact on a school. It might be a matter of a school's external or public face that needs to be protected. If a hacker stole internal data and published it on a public website – what would be the impact to the school's reputation, enrollment, fund raising, etc.?

This last question can actually help in releasing or reassigning the appropriate funds for security projects. If the risk is very high that sensitive data would be lost or released and the cost is high if that happens, then the funding needed to address that risk is more likely to be budgeted.

HOW

How you secure the data will depend greatly on where it is, what value it has, and how secure you want to make it. If the data is on a server that has no access to the Internet, is limited to only a small set of users, and you monitor access on a regular basis, you might have a low cost or no cost to meet your risk assessment. Making the data hard to get at (i.e. no Internet access or network access at all) lowers the cost of securing it. If all HR data is on one computer that is not connected to your network, and is in a secure office then you don't need to worry about network based intrusions or

remote hackers. You only have to make sure only the right people can access **that** computer in **that** office.

If the data is on a computer connected to your local network, but not allowed access to the Internet (i.e. protected by a firewall) for any reason (i.e. no web browsing on the server/workstation), then you don't need to worry about Internet attacks but you do need to assess your network vulnerabilities. Can someone steal the network passwords and log in from anywhere on your network? Perhaps you can restrict access to the data by an internal IP address scheme to create a secure domain[12], or require ID tokens for two factor authentication (username and password and the token based ID[13]). If you don't allow web access to the data then you don't need to worry about a Virtual Private Network[14] (VPN) to secure the data channel. You can also encrypt the data on the server so that is someone steals the computer or the backup tapes, the data is not easily recovered.

If the data is diffuse and you can't identify who has access, the difficulty is raised significantly. If you have to allow remote access to some or all of your data, and you need to allow users to take copies of the data along with them on laptops or a PDA[15], you will need to encrypt the data in some form to ensure that if the data is lost it's not easily recoverable by an un-authorized user.

The cost of the how will be determined by the value of the data.

CREATE A SECURITY POLICY

Creating a security policy is a starting point for a schools total security strategy. It will flow from the risk assessment stage and will be an organic document that changes as new security needs and risks are discovered and evaluated. The policy will help enforce and educate your users to the various risks that they are exposed to and the fundamental rules that they need to follow when conducting business.

Each school needs to defend their data and networks, using a layered approach, what is known as Defense in Depth (http://www.sans.org/rr/securitybasics/univ_level.php) to protect their assets. The security policy defines who is responsible and what level you are protecting: the edge of your network, the server, the workstation, or the data itself.

A security policy is not one document but a series of small, easy to read and update, documents[16] that outline the methods that you have in place to reach a particular goal. A policy will exist at the macro level (i.e. for the entire school or school system) to give a general direction and at the micro level to address a particular need. For example:

In order to protect our computers against email virus attacks, the network administrator will check for updates to Microsoft Internet Explorer on a daily basis and apply new updates once a week.

This is a micro level policy to address the issue of security issues in Microsoft's Internet Explorer. A macro level policy might look more like this:

The security department is responsible for establishing, maintaining, and coordinating the guidelines and policies for each department so that they are consistent, effective and regularly tested.

A policy will address the question of who is responsible, what are they responsible for, and why they are responsible. There are many examples of security templates on the SANS website http://www.sans.org/resources/policies/#template.

FBI/SANS Top 20 List (http://www.sans.org/top20/) and Macintosh vulnerabilities

Last but not least, a small school can eliminate a good degree of risk with basic perimeter defense by regularly (weekly) monitoring of the Top 20 list from SANS and the FBI. This list provides both the risk and the remediation of the top security vulnerabilities for Windows and Unix operating systems. Macintosh vulnerabilities can be found on Apple's website (http://www.info.apple.com).

Fixes and tools for these vulnerabilities can be found on the SANS website as well: http://www.sans.org/top20/tools.pdf

Listed below are the top 10 Windows, Unix, and Macintosh Vulnerabilities

Windows:	Unix / Linux:
1) Internet Information Server (IIS)	1) Remote Procedure Calls
2) Microsoft Data Access Components	2) Apache Web Server
3) Microsoft SQL Server	3) Secure Shell
4) NETBIOS – Unprotected Shares	4) SNMP (Simple Network Management Protocol)
5) Anonymous Logons	5) FTP (File Transfer Protocol)
6) LAN Manager Authentication	6) Remote Services RLOGIN, etc.
7) General Windows Authentication	7) Line Printer Daemon (LPD)
8) Internet Explorer	8) Sendmail
9) Remote Registry Access	9) BIND/DNS
10) Windows Scripting Host	10) General Unix Authentication

Macintosh:	
1) Web servers with Dynamic content	2) Mac OS X Internet Explorer version 5.1.4
3) Microsoft Word	4) AppleShare IP 6: Pass Protocol
5) Macintosh Manager	6) OS X 10.2.2
7) Stuffit Expander Security Update	8) Mac OS X client
9) Open SSH	10) Apache Web Server

Many of the **Windows** security vulnerabilities can be addressed by regular visits to the Microsoft update page – http://windowsupdate.com. This site automatically checks your system for missing patches based on the software you have installed on your system (laptop, workstation or server). Another version of the site that is very useful for network administrators with slow Internet connections is the service pack download section of the Microsoft support site: http://support.microsoft.com/default.aspx?scid=fh;EN-US;sp

This site allows you to download the service packs without using Internet Explorer and it's Active X discovery program. Instead you can download the service pack for an OS once, store it on your local network and then install it over your local network. This can greatly decrease the time it takes to install the many service packs that Microsoft issues because you don't have to wait for the same file to download over and over again.

Unix security threats will vary by vendor. The major Unix vendors (HP, Sun, IBM) have proprietary flavors of Unix that they develop and support. This is both a blessing and a curse in that they control when an OS fix/patch is released or revealed, but on the plus side, they have most likely done more testing before releasing the fix/patch. Each vendor distributes an update CD with patches, this is not always free, but is worth evaluating as you determine your overall security needs.

The **Linux** operating system (a Unix like OS) has several distributions (RedHat http://www.redhat.com, SUSE http://www.suse.com, Debian http://www.debian.com) to name just three. Each has their own list of patches and tools for updating their OS.

RedHat has an utility called UP2DATE that can be configured to automatically check for patches. Debian has an application update tool, APT, you can issue the apt-update command which will get the latest version of the Debian kernel.

Updates for the Macintosh OS are available at the main Apple support website, http://www.info.apple.com. Apple computers tend to be less vulnerable to hackers due to their proprietary operating system but that has changed recently with the latest version of their operating system, OS X. This version is based on the Unix operating system[17] and is therefore now at risk to Unix like attacks.

Conclusion

Computer security is frequently not addressed until something bad happens. People assume that their computers, software, and networks are secure, and that the data is secure, unmodified, and always available until a hacker breaks in or a virus infects the main server or someone changes grades or steals enrollment information. Proper planning and risk assessment will not eliminate security threats, but it will identify what is at risk, the value of the data, and what risks an institution is willing to accept. Creating the needed security policies will be an ongoing process that identifies who can access what, when and where. The policies make concrete what is often known but not documented or communicated. Correctly implemented, these policies make everyone responsible for data security. Removing the top 20 vulnerabilities from Unix, Windows, and Macintosh workstations and servers is a very easy first step toward securing your information resources.

References:

1) SANS Top 20 vulnerabilities: http://www.sans.org/top20
2) *HIPAA Security Policy Development: A Collaborative Approach,* Miles M. Sato, April 30, 2001 http://www.sans.org/rr/policy/HIPAA_policy.php
3) US Department of Health and Human Services, October 15th 2002 Fact sheet, *Administrative simplification under HIPAA*. http://www.hhs.gov/news/press/2002pres/hipaa.html
4) Sample HIPAA compliance statement from a medical transcription company. http://www.medsoftusa.com/hippa.htm
5) National Center for Education Statistics, *Protecting the Privacy of Student Records*, *Guidelines for Education Agencies.* http://nces.ed.gov/pubs97/p97527/CONTENTS.HTM
6) New York University, *Guidelines for Compliance with the Family Educational Rights and Privacy Act.* http://www.nyu.edu/apr/ferpa.htm
7) Carter Ledyard and Milburn, *Monitoring Employee E-mail, Voice Mail and Computer files without violating Employees' privacy rights.* http://www.clm.com/pubs/pub-914447_2.html
8) VNUNET.COM, UK Technology News, reviews, downloads. *High School hackers make the grade.* http://www.vnunet.com/News/1132421
9) Symantec Corporation Anti-Virus Security Response website. *Report on W32.Sircam Worm* http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html
10) IBID, *Report on W32.Badtrans worm* http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html
11) TechTV.COM, *High School hacker leaves mark*, December 23rd, 2003 http://www.techtv.com/news/internet/story/0,24195,3412170,00.html
12) University of Illinois at Urbana-Champaign, *Code of Policies and Regulations Applying to all students. Disposal of Inactive Records.* http://www.uiuc.edu/cgi-bin/print_hit_bold.pl/admin_manual/code/rule_67.html
13) SANS Reading Room, *Implementing Defense in Depth at the University Level,* G Michael Runnels, May 14, 2002 http://www.sans.org/rr/securitybasics/univ_level.php
14) SANS Security Policy Project, http://www.sans.org/resources/policies/#template
15) Apple Computer information database, (Note: Need to search on security. http://www.info.apple.com
16) SANS security website, *Tools and Services that Find the Top 20 Vulnerabilities on your system and Networks,* http://www.sans.org/top20/tools.pdf
17) Windows automatic update website, http://windowsupdate.com
18) Windows Support website, Service Pack download site, http://support.microsoft.com/default.aspx?scid=fh;EN-US;sp

[1] Small means schools with less than 1500 students.
[2] CNN news story, Princeton accused of Ivy League hacking, July 25th 2002 http://www.cnn.com/2002/US/07/25/yale.princeton/
[3] USA Today news story, *Princeton dean loses job over hacking flap*, August 8th, 2002,

http://www.usatoday.com/news/nation/2002-08-13-princeton-yale-hacking_x.htm

[4] To better understand a DDOS please see DeokJo Jeon's paper on *Understanding DDOS Attack, Tools and Free Anti-tools with Recommendation* http://www.sans.org/rr/threats/understanding_ddos.php

[5] A faculty member at my institution had a laptop running Windows 2000 that was infected with the Code Red worm. The faculty member only connected via modem and for short periods – less than 10 minutes.

[6] James Bayne paper, *An Overview of Threat and Risk Assessmen* covers this topic in more detail: http://rr.sans.org/audit/overview.php

[7] Student records, student emails, faculty emails, faculty course information, might need to be preserved for extended periods of time based on the legal guidelines at your institution.

[8] A small access database on a department level could be more at risk than the main database on a server because it's more portable and has less file security and auditing than on a managed server.

[9] Many schools allow students to view grades and course information via the web. How do FERPA regulations impact your schools web portal? You might have to add your web portal to your privacy policy like UT. http://www.utexas.edu/policies/privacy/

[10] Good security involves more than just one department and is more than a one time project, it's an ongoing process. Mark King covers the security lifecycle in his SANS paper: http://www.sans.org/rr/securitybasics/lifecycle.php

[11] Princeton accessed Yale admissions information and the associate dean of Admissions at Princeton lost his job: http://www.usatoday.com/news/nation/2002-08-13-princeton-yale-hacking_x.htm

[12] For more on Secure Domains please see Mikael Trosell paper, *Protecting Sensitive Data in Secure Domains* http://www.sans.org/rr/encryption/protect_data.php

[13] SecurID by RAS Security Inc (http://www.rsasecurity.com/products/securid/) is a token based ID system that has a unique number generated every minute so that you have very strong two factor identification. See Steven Krychiw's paper, *SecurID: A Secure Two-Factor Authentication* in the SANS reading room for more information: http://www.sans.org/rr/authentic/securid.php

[14] VPN's and encryption are covered in much more detail Kenneth Forward's paper, *Appropriate Use of Network Encryption Technologies* : http://www.sans.org/rr/encryption/appropriate.php

[15] Susan Guerrero covers basic PDA security in her paper: *PDAs – A security Primer* http://www.sans.org/rr/pdas/sec_primer.php

[16] For more on building a security policy see Martyn Elmy-Liddiard paper, *Building and Implementing an Information Security Policy* http://www.sans.org/rr/policy/building.php

[17] The Apple website details more about how OS X uses Unix as the base of the new operating system. http://www.apple.com/server/