A Normative Campus Security Agenda

Educause Security Professionals Conference
10:45-11:45, Monday, May 5th, 2008, Arlington, Virginia

Joe St Sauver, Ph.D.
(joe@uoregon.edu or joe@internet2.edu)
Internet2 Security Programs Manager,
Internet2 and the University of Oregon

http://www.uoregon.edu/~joe/spc2008/

Disclaimer : The recommendations expressed in this presentation are solely those of the author and do not necessarily represent the opinion of any other entity.
About the Format of This Talk: These slides are provided in a detailed format for ease of indexing, for the convenience of the hearing impaired and those for whom English is a second language, and for those who may not be in the audience today.

I. Introduction

A Core Set of IT Security Activities

- Higher education is a well defined environment with a relatively small number of fundamental activities (teaching, research, administration, etc.), and with well defined consistent stakeholders (applicants/prospective students, faculty, students, staff, alumni, etc.)

- It is therefore hardly surprising that **each of our campuses tends to end up doing a common set of IT security tasks**.

- **Those tasks effectively define an emergent norm, or de facto standard, or "best practices" if you will, for IT security practice in higher education.**

Vendor and Miscreant Activity Also Drive IT Security Agendas in Common Directions

- Vendors (including IT security vendors) obviously work hard to market their message/products to targeted populations, and higher education IT security folks generally receive significant vendor attention. Why? Well, obviously vendors want to sell you their products for your campus, but higher education also tends to have individuals who are thought leaders in this space.

- The existence of the Internet, and automated tools which allow hacker/crackers to target large populations, also results in a certain consistency when it comes to higher education’s IT security activities -- we all tend to get attacked by, and react to, the same set of 'sploits.

A Sample Core IT Security Task: Antivirus

- An example of a sample IT security task that each of our campuses addresses is desktop/laptop antivirus software.

- It's unheard of to find any major university which has not selected some sort of antivirus software, although obviously not all campuses run exactly the same antivirus product, nor do they do so in exactly the same way.

- For example, some campuses may cover all systems (regardless of whether those systems institutionally owned or privately owned, used by faculty/staff or students, etc.), while others may have more limited coverage.

A 2nd Example: Responding to “Incidents”

- Another example of a virtually ubiquitous IT security task is responding to information technology security incidents, such as discovery of a system that’s been hacked/cracked.

- Every campus needs (and usually will have) someone (or some group of folks) designated to handle this, and when a significant system is compromised those are the “emergency responders” who handle the incident.

- Just like antivirus service, incident management happens in different ways at different sites, but as you talk with other folks, you’ll see an amazing degree of inter-site consistency on this point, just like offering antivirus.

A 3rd Example: Campus AUP

- All (or almost all) institutions also have “acceptable use policies” governing what’s allowed and what’s not allowed on the campus network and on institutional systems. Those AUPs tend to cover common topics, such as:

  -- limitations on use (e.g., commercial use is prohibited, sharing one’s password is forbidden, etc.)

  -- respect for copyrighted software and other materials is required, as is

  -- an explanation of what happens when the AUP is violated (e.g., access may be curtailed), etc.

“So What/Who Cares???”

- That’s a very important question! At a minimum, I believe **new IT security officers will (or should) care.** They may find themselves in a new job wondering:

  -- “Heck, where do I even begin?” or

  -- “How do other campuses address <this issue?> I don’t want to have to reinvent the wheel!”

- A normative set of IT security tasks would give a new IT security officer a starting foundation for developing local programs, and confidence that they’re not overlooking key issues that are on "everyone else's" radar.

Managerial Guidance

- **Managers** responsible for IT security operations may also find a normative list of higher education security issues to be helpful.

- If you're a general IT manager, there's no way you'll be able to personally oversea and be expert in all the substantive areas you and your staff handle -- you may happen to come from an administrative systems background, or a telecom background, for example, but over time you may have also been asked to keep an eye on security, despite having only limited IT security experience. Wouldn't it be helpful to have an list of relevant topics to focus on?

Audit Staff

- Still another group that may find a normative list of IT security issues and approaches to be helpful might include internal auditors and risk assessment staff.

- Comparing what's currently being emphasized/what's currently being done with what's being done elsewhere will go far to highlight areas where a departure from best common practices may be occurring.

No Site Will Fit a Template or Checklist 100%

- I **don't** want anyone to think that the material we'll describe today represents a template or checklist that should drive lockstep 100% compliance -- that's certainly not my intent, and I think you'd have to be pretty foolish to attempt to use this talk that way. Every site, despite superficial similarities, is unique, with different demands, a different culture, and different approaches shaped by the institution's experiences and history, etc.
- In particular, I'd be particularly unhappy if this list was misused as a basis for criticizing anyone -- failure to do something mentioned in this talk does **NOT** mean that your IT security person is "asleep at the wheel" or doing a bad job. In particular, I'd urge you to recognize that…

Some Missing Bits May Be Missing for a Reason!

- When there is a discrepancy between what one site is doing and what another site is doing, at least some of the time that discrepancy may be due to resource limitations, e.g., a lack of money or staff.

- Having a normative IT security agenda can help to identify those situations, and perhaps even lay the foundation for additional funding or additional staffing.

- Do NOT assume that stuff which may be missing is missing because your IT security person doesn't think it is important.

A Taxonomy Isn't Just A Random Unstructured List of Items

- The other thing that comes out of a taxonomy is order, or structure.

- Rather than just having a long laundry list of topics, developing a taxonomy forces you to organize the tasks you face. That organization helps you to identify potential synergies, and to identify common reinforcing themes.

- So speaking of organization…

How Will The Rest of This Talk Be Organized?

- Having established a rationale for why a normative taxonomy may be helpful, and having briefly touched on why some elements may not be present at all sites, we can now begin to flesh out some parts of the taxonomy. Let's begin with data/information.

- Before we do, however, a couple more items:

  -- In one hour, it isn't possible to cover everything that's routinely done in any depth. I hope you'll bear with me when we just glance over an item and then move on.

  -- I've tried to minimize technical jargon and keep this talk at a "plain english" level as much as possible.

II. Data/Information

Paraphrasing Bill Cosby,
"They **want** the data."

Why Begin With Data/Information?

- If you look at recent news stories, the biggest/worst IT security problems have all involved data/information breaches: loss of personally identifiable information (PII), unauthorized access to credit card data, exfiltration of confidential institutional or government materials, etc.
- What does this mean? Well, the miscreant emphasis has shifted from a fascination with networks or systems to the data/information* that those networks or systems process or store.

———

* Data's the "raw stuff," information is data which has been processed enhanced via interpretation, analysis, etc. When we use either term, consider it used broadly/inclusively.

Data, De-Perimeterization, the Jericho Forum and RSA 2008

- An emphasis on data (rather than traditional IT security building blocks such as firewalls), also meshes nicely with the realities of today's networks, systems and applications.
- I provided some discussion of this migration away from traditional firewalls in an Internet2 Member Meeting talk I did in April entitled "Cyberinfrastructure Architectures, Security and Advanced Applications," see http://www.uoregon.edu/~joe/architectures/architecture.pdf but a data centric emphasis is something that has long been advocated by those who follow the Jericho Forum: http://www.opengroup.org/jericho/commandments_v1.2.pdf
- Data centric security was also a theme at RSA 2008, including one keynote entitled, "Information Centric Security: The Next Wave" by John Thompson of Symantec

Data Inventory

- A first step when it comes to controlling your institution's information is simply figuring out what you've got, typically by conducting a campus data inventory.

- And why shouldn't you? You periodically take an inventory of campus capital assets -- your data is certainly worth far more more than computer hardware or lab equipment is!

- Some sites may focus just on personally identifiable information or financial information, while others may seek to understand all the data that's being collected, why it's being collected, the information systems on which it is being stored, etc.

Data Classification

- Once you know where data lives, you can begin to improve institutional control over it. Classifying data is a key part of that process of getting data in hand.
- When I speak of classification, I’m not talking about classification in the governmental "top secret" sense. Rather, I mean: Is a given dataset publicly shareable? Is it for institution internal use only? Is disclosure of particular data prohibited by law? Would disclosure of particular data hurt university interests? Classifying datasets helps users know how data should be handled, stored and disclosed.
- In other instances it may be worth looking at larger or smaller units of analysis -- maybe (only) particular columns or rows in a dataset are sensitive, while in other cases all data on an entire system may need to be carefully controlled.

Discovery of Hidden Data Caches

- Other times, sensitive data may exist -- and be potentially publicly exposed -- without any institutional knowledge or review. In those cases, what's needed most of all is simply for someone to simply discover that data exists.
- Automated tools can crawl institutional web servers (and there may be hundreds of web servers on a typical campus, not just one or two). Other tools may exhaustively traverse the institution's network address space, looking for things such as excessively permissive file sharing. Those tools may help turn up some real "surprises" before someone else finds and exploits them.
- Later in this talk, we'll chat a bit about reviewing vulnerabilities associated with particular applications, too.

Data Minimization

- When non-public data is discovered in unexpected places, like on a public web page, most schools will work to remediate that disclosure.
- Some schools, however, may also carefully scrutinize the data **collection** process, paying attention to things such as forms where students and others are asked to supply data. Is all the data that’s requested **really** needed (or even being looked at/used)? Or is there data that we’re only asking for because, well, we‘ve always asked for it?
- **These less data you collect, the lower your exposure during a potential breach.**
- Eliminating, or at least minimizing the use of social security numbers on campus, is a nice example of a common campus data minimization project.

Data "Aging"

- Higher education institutions are particularly and uniquely predisposed to a “pack rat” mentality, never wanting to “throw anything away.”
- Data aging, including the elimination of records that are no longer required, directly challenges that instinctive preference. In today’s litigious society, and given the substantial costs associated with retaining records beyond required dates, housekeeping and deletion of no-longer-needed business records (consistent with established record retention policies and laws applicable to your school) is a very important task.
- Visit with your archivist or record manager and make sure you know what must be kept, and for how long, and what you can safely delete.

Data Protection

- Having just talked about destroying data, let me now turn right around and talk a little about data protection.
- More than ever before, your institution is generating research data, discovering new inventions, producing reports, authoring software, creating web pages, saving student records, etc. All of that’s intellectual property of data potentially covered by FERPA, and you need to protect it from loss or unauthorized modification.
- In most cases, data protection will drive storage management projects, with a nearby (but not *too* close) hot site continually mirroring data that’s on the institution's primary disk farm (perhaps backed up by something like offline magnetic media at yet a third location).
- Encryption projects are another example of data protection.

Access Control and Identity Management

- Campuses are also increasingly coming to recognize that sound identity management practices are a prerequisite to tightening access controls and improving data protection.
- We can’t decide if you have a legitimate “need to know” when attempting to access a particular record unless we know **who** you are, or at least **what** you are.
- Tightening up that area is something that requires more than just the knowledge that:

  -- a person has a username and a password for the campus email server, or

  -- they’re accessing the network from an on-campus network jack.
- Campus identity management initiatives address this need, setting the foundation for better control over access to data, and improved accountability.

Ongoing Data Stewardship

- Securely managing your institution’s data is not a project that can be assigned to a data security specialist, done once, and then forgotten. Data needs to be cared for **continually** and **primarily** by those who create and use the data.
- If a scientist is actively collecting research data, she will likely be the only one who will know what has been collected recently, or what it all means.
- Similarly, no one will have a better sense of institutional student data than your registrar. It makes sense for those individuals to have primary responsibility for keeping that data safe, and that why many institutions now have drafted and adopted formal data stewardship policies.

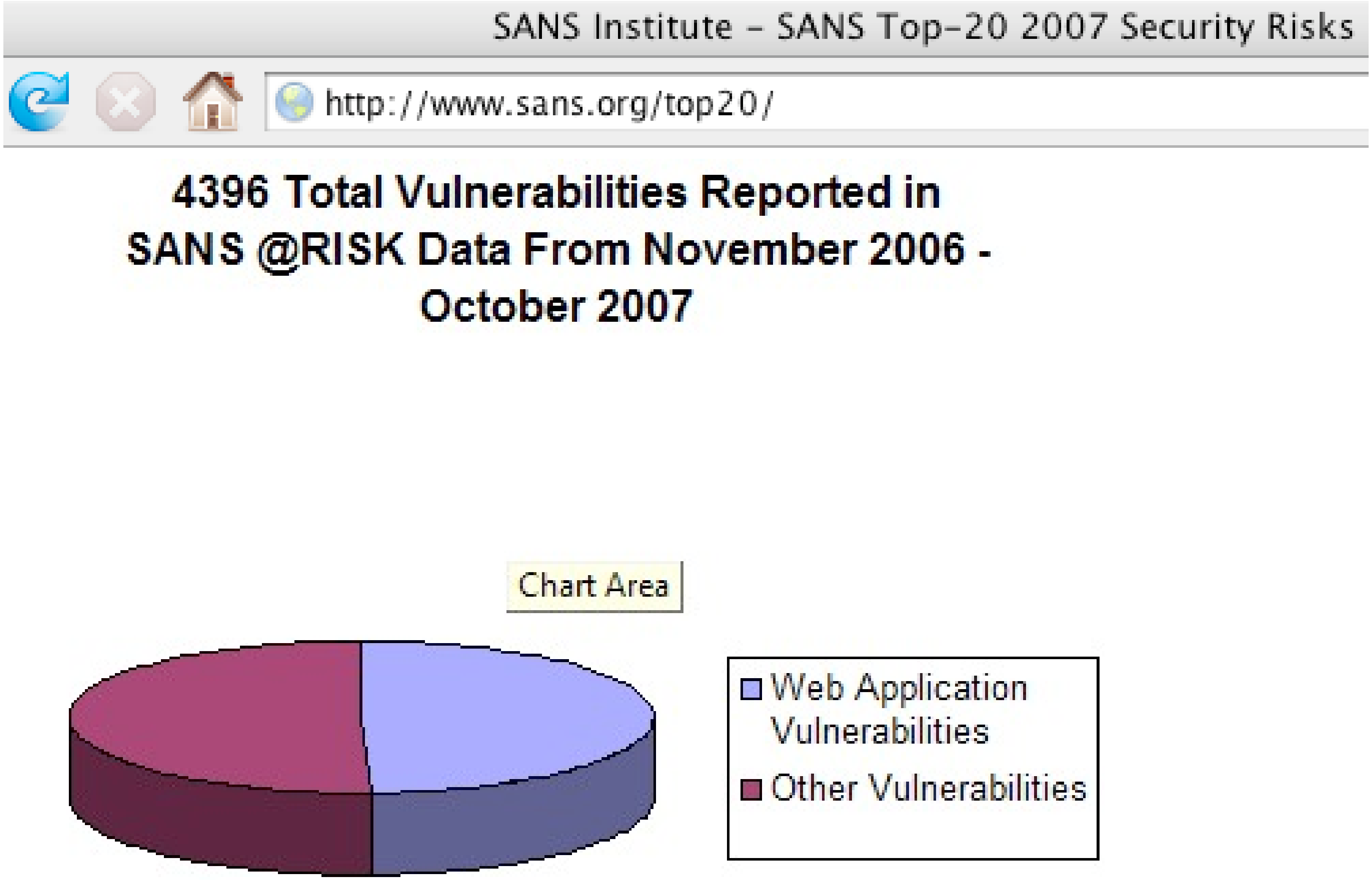
III. Applications

Why We All Need to Worry About Applications

- I promised to minimize my use of technical jargon in this talk, but let me renege for just a second. If you're a non-technical person and you haven't heard of:

  -- "Php Remote File Inclusion" vulnerabilities,
  -- "Cross Site Scripting (XSS)" attacks
  -- "SQL Injection" attacks, or
  -- "Cross Site Request Forgery" attacks

  among other attacks, that's okay -- the names are arcane and somewhat confusing.
- What you DO need to know is that those terms all represent attempts to exploit vulnerabilities in web based applications, and as a group, **web based application vulnerabilities accounted for nearly half the vulnerabilities SANs saw from Nov 2006-Oct 2007.**



SANS Institute - SANS Top-20 2007 Security Risks

http://www.sans.org/top20/

4396 Total Vulnerabilities Reported in SANS @RISK Data From November 2006 - October 2007

My Favorite Site for XSS Examples

- Because it sometimes helps to have concrete examples, you may want to check out the “XSS (Cross Site Scripting) Cheat Sheet,” that’s at http://ha.ckers.org/xss.html
  That page shows multiple examples of cross site scripting vulnerabilities, with each vulnerability tagged according to the browsers which are vulnerable. While it is certainly true that many exploits work on Internet Explorer, there are also **plenty** of exploits which work on Firefox and Opera, too, so don’t assume that “I’m safe because I’m running something other than Internet Explorer.” (That’s simply not true)
- Because this may be read by a non-technical audience, let me also note that popping up a box reading “XSS” is NOT the only thing these exploits could be used to do. (I’m told that sometimes folks miss that point, and then wonder, "So what’s the big deal about making a box that says XSS?”)

Nice Web App Vulnerability Example

- While there were many excellent talks at RSA 2008 in San Francisco, one of the best talks was Sullivan and Hoffman’s “Ajax Applications: A Blueprint for Disaster.” If you didn’t have the pleasure of being there, a nice summary is at www.regdeveloper.co.uk/2008/04/14/ajax_charlatans_old_school_attack/ (and yes, these **are** the same guys who wrote the fine book Ajax Security, published this past December)
- Scrutinizing one **five** line chunk of real code, the audience identified **seven** major vulnerabilities. In another example, the presenters did a great job of showing how Firebug, a web debugging tool, could be used to attack a sample “bid for an airline ticket” web application, including "naming your own price" (with any price always being acceptable) and reserving **all** seats on **all** flights (thus DOS’ing the service).

Identifying Applications With Security Issues

- There are a variety of approaches to identifying web applications with security issues, and I'm not here today to advocate one approach over another. Automated testing has a place, as does manual code review, and most sites will employ a combination of both.. The important thing is that institutions ARE spending time looking at web app vulnerabilities.
- Some critical resources to help get you bootstrapped (if you're not already on your way) include:
  -- NIST SP800-95 Guide to Secure Web Services
  csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf
  -- The Open Web Application Security Project (OWASP)
  http://www.owasp.org/index.php/Main_Page
  -- there are also MANY commercial tools in this space, but don't just "buy a tool" and assume that you're done…

Code Control and Change Management

- Once you get past concerns about web-related application vulnerabilities, a lot of old-but-still-important security considerations associated with applications still remain.
- For instance, consider code control and change management for production systems. How do changes to applications get reviewed and vetted before they're rolled onto production systems?
- How are changes to code tracked? Is a version control system employed so that you can tell WHAT was changed, and by WHO, WHEN? Do you have a central code repository, or is code fragmented, laying around in a dozen coder's individual accounts?
- Subversion (see http://subversion.tigris.org/) is one popular open source option for managing source code which many schools use.

Secure Coding

- Let me conclude this section by making a plea/request, and that's to say that **if** in addition to the IT security stuff you do, if you teach programming, or help to hire programmers, or supervise programmers, insist on secure coding practices. We need to do a better job of building security in, rather than trying to bolt it on after the fact.
- A relatively small number of issues account for the majority of coding problems, so if folks just know what to pay attention, this is a battle we **can** win… For *nix, see www.securecoding.cert.org or if you're coding for MS Windows, see Howard & LeBlanc's **Writing Secure Code**.
- Speaking of Microsoft, they're a fine example of a company that has made a commitment to secure coding, and the result has been a huge improvement in application security. This is once when we should ALL emulate MS!

IV. Usernames and Passwords

Passwords

- Basic as it may be, many security issues **still** relate to passwords.

- While a university IT security office will usually not be directly involved in issuing usernames and passwords, it may have (and often may **need** to have) substantial influence on a number of password-related policies.

- For example, how will new user accounts be created? How will users receive their username and password?

Distributing New Usernames & Passwords

- This is a classic "bootstrap" issue: without a username and password, users cannot login to securely download their username and password (recurse as desired). Common solutions for new students and new faculty/staff include:
  -- having the user show up in person with photo ID is secure, but that process is inconsistent with the trend toward early username issuance as part of the admissions process, and difficult for distance ed students
  -- snail mailing usernames and passwords to an address of record (but that introduces snail mail delays, and can be expensive if you're sending out 1,000's of passwords)
  -- others may wait and allow students to create a username and password of their choice online after they've been issued an alternative campus credential (such as an ID card with a personal identification number)

Resetting Forgotten Passwords

- Password resets may be the #1 helpdesk issue, and how they get handled may determine in large measure the overall strength of your password security.

- Strong passwords with weak password reset mechanisms are weak passwords.

- So how do people reset passwords? Options basically break down into two categories:

  -- traditional face-to-face requests, backed up by photo ID

  -- “self-service” options

What Do You Mean By "Self Service" Options?

- Use of alternative credentials (such as the campus ID number and PIN) to pick a new password
- User successfully providing answers to a set of pre-completed “secret questions” (but it can be very hard to arrive at a good set of 'non-researchable' questions)
- Out-of-band authentication (such as sending a new password to a pre-registered phone number belonging to the user -- you just hope that it isn't a shared "house phone" in a group living environment)
- Sending a password reset link to a pre-registered alternative email address), or
- Biometric approaches (such as voice recognition systems)

Password Minimum Strength Enforcement

- We know that if given the opportunity, at least some users will select weak (short, guessable) passwords for their accounts.
- This may be an issue that's handled at password selection time (e.g., don't even **allow** users to select a bad password in the first place), or password selection may be audited on a post hoc basis by periodically "cracking the password file" and forcing the user to pick a new password the next time they login.
- Password complexity enforcement may be particularly frustrating for users since, given sufficiently rigorous rules, users may have a hard time even finding a password which will work unless the system provides acceptable generated password suggestions.

Required Password Changes, Password Reuse, Same PW on Multiple Sites, etc.

- Beyond password strength issues, we see some sites struggling with required password change policies, users who respond to password change requirements by trying to toggle between just two repeatedly reused passwords, and users who cope with the problem of everything being passworded by using the same password on multiple sites (everything from their high security administrative system login to their “joke-of-the-day” site hosted in Eastern Europe).
- More than any other area, the problems that higher education sites are running into in this area convince me that plain passwords are rapidly becoming an end-of-life technology. (I believe two factor authentication will be the replacement)

Anti-Sniffing Efforts

- Having strong passwords does no good if the miscreants can simply eavesdrop on network traffic to intercept them. Protecting users against sniffing attacks implies that protocols supporting strong encryption (ssh, ssl/tls, etc.) are used, and protocols which rely on plain text passwords (such as telnet, ftp, etc.) are banned.

- Some sites, which can live without end-to-end encryption, may get some degree of crypto protection through the use of VPNs.

- Other sites may attack the issue by eliminating use of reusable passwords, going to hardware tokens instead, as previously mentioned.

Anti-Phishing Efforts

- Attention needs to also be paid to anti-phishing efforts. In recent days, a number of attackers have specifically targeted higher education user credentials, seeking access to accounts which can then be used for the purpose of spamming or other malicious activity.
- Users need to be cautioned against social engineering attempts, but they also need to be trained to understand **technical credential harvesting approaches**, such as man-in-the-middle (MITM) attacks, and why it is important to pay attention to things like ssh key change warnings and SSL certificate details. (But we all know that user education can be difficult and time consuming and imperfect at best).
- One thing that I’ve NOT seen take off has been use of extended validation certificates (so-called “green bar certificates”) in higher education (if you’re in higher ed and your site is using an EVL, I’d love to hear from you)

Passwords and Distributed Applications

- Distributed applications need a way to authenticate, authorize, and do access control, but a proliferation of multiple discrete accounts scales poorly and argues for something like single sign on, instead.

- On a campus basis, this often implies a campus identity management initiative based around LDAP, or perhaps a RADIUS based solution.

- Nationally/internationally, a federated approach based around Shibboleth is one leading approach, allowing user identity to be decoupled from user status (e.g., I can confirm for an online academic publisher that a user's an enrolled student, w/o telling them the student's real name or other private attributes)

Detecting Brute Force Attacks

- If a large shared system is the focus of a brute force attack, assuming it is running a security-oriented operating system, after a specified number of unsuccessful login attempts, even an attempt which happens to include a correct username/password pair will be ignored, thereby hampering brute force password guessing attacks (albeit while enabling an interesting denial of service attack).
- But now let's move from a traditional login-to-a-large system environment to a more distributed environment. Is there still an effort to detect and deter brute force password guessing attacks? If so, why do I hear about ssh probes on various security lists, but nothing about LDAP probe attacks? My hypothesis: such attacks are occurring, but no one's paying attention to them (and anti-brute-forcing techniques are not being widely employed)

V. Desktops and Laptops

A Ubiquitous Resource, A Ubiquitous Challenge

- This is probably the section you expected to see first. :-)
- Virtually all users will have a desktop or laptop personal computer, and some users will have multiple systems.
- Unlike a corporate environment, it will be routine to see a mix of institutionally owned systems and personally owned systems, some running the latest version of Windows Vista, others running Windows XP (or even older versions of Windows), plus OS X, Linux & other operating systems
- This diversity can provide some protection from “monoculturality” (and boredom!), but at least on some campuses, it seems like old gear never dies -- it just gets continually handed further down the local pecking order. That frugality can sometimes mean that unpatchable operating systems remain perpetually in circulation.

Vista or XP?

- Speaking of PC operating systems, there’s also the question, “Is higher ed using Vista or XP?”

- While Vista has a number of security features which are designed to help protect the system from things like unauthorized changes, uptake of Vista in higher education, as in the world at large, has been rather… deliberate… although Vista’s market share in higher education continues to grow as users buy systems with Vista pre-installed (but beware “downgrade rights,” allowing users to downgrade from at least some versions of Vista back to Windows XP).

Managed or Unmanaged?

- Another fundamental point of inflection can be found when it comes to the question of whether or not a system is “managed.”
- That is, if one is following a corporate model, what the user can do on his or her PC may be limited, with a PC system administrator handling most day-to-day chores such as reviewing and installing applications, patching the system, making sure the system is backed up, updating antivirus definitions and scanning for viruses, etc. Doing these tasks in a scaleable way usually requires that the site use Active Directory, with users routinely logging on to a fileserver.
- On the other hand, it is by no means uncommon to see unmanaged systems in higher education

Assessing The Condition of Unmanaged Machines

- One reason why there will always be at least some unmanaged systems on a typical campus is privately owned student or faculty systems. Because of the existence of those unmanaged systems, Network Access Control (NAC) has become a popular network security technique in higher ed.
- When a campus deploys a NAC solution, systems accessing the network will have their status assessed, and information about the user may also be collected (which can be very helpful if there's a problem with that system).
- NAC allows a site to ensure that critical patches have been applied, security software is running, unwanted services are not operating, etc.
- Most NAC environments provide solutions which allow non-NAC-able Macs, Linux boxes and other "corner cases" (such as gaming systems) to still safely get on the network

NAC and Machines Which Aren't "Up to Snuff"

- When a NAC system finds a machine that isn't "up to snuff," it may block network access for that system and provide a point for where help can be obtained, or it may drop the user into a limited network environment where the user can access the network resources the need to meet minimum thresholds, but not much else.

- But consider an interesting conundrum:
  -- a visiting user runs into NAC-detected deficiencies,
  -- their laptop is managed, so they don't have the technical ability to download and install the required updates
  -- without those updates, they can't get online, etc.

Installing Standard Campus Software

- Another common security service at many campuses relates to locally tailored software builds, typically pre-configured with the site's recommended browser and email client, site licensed software (such as antivirus software, antispyware software), local documentation, etc.

- Because of the size of many common programs, these campus' "software build" are most commonly distributed on CD, however on-campus users and broadband connected remote users may simply download the products they need instead.

- Obviously, for any proprietary software, authorized users need to be authenticated to insure that licensed products aren't inadvertently distributed to unauthorized parties.

Configuration Can Also Be Key

- Although a campus software CD's primary job may be installing customized software, it may also do things like confirm that the system firewall is enabled, or that the Windows Messenger Service is off.

- Assuming that a campus software CD is just for distributing software is a mistake, although a software CD can have a profound impact when it comes to influencing de facto choices on campus.

Browser Selection

- Alternative browsers, such as Firefox and Opera, are widely accepted and used in higher education, in part because it is believed that these applications may have a lower attack surface or better security than Microsoft IE.

- It is also common for higher education audiences to configure their web browsers in a more security conscious way than typical corporate or home users, perhaps disabling scripting, or disallowing routine use of cookies.

Helper Applications

- Helper applications are common in higher education settings, including standard helper applications such as QuickTime, Flash, Acrobat Reader, Java, etc.

- Procedures to identify and update out of date helper applications are less refined and consistent than is desirable (including things like rooting out old vulnerable versions of Java which remain installed even after new, updated versions have been installed)

- Patch management and application version checking tools may help to address this problem.

Software Site Licensing Programs: Two Birds with One Stone

- Some schools may sign up for software site licensing programs such as the Microsoft Campus Agreement Program, which provides access to both operating system products and applications for covered users.

- Doing so can potentially address two critical issues:

  -- when the operating system and popular applications (such as the Office suite) are site licensed, it is less likely that users will limp along with old and potentially unpatched/unpatchable copies of those applications

  -- potential unauthorized use of licensed software become far less of an issue

Legal Online Music Programs

- Another example of an area where schools may attempt to solve multiple problems in a single stroke can be seen in legal online music programs. Without such a program, some members of the university community (just like other Internet users) may be tempted to turn to peer-to-peer applications to get “free music online.”

- Unfortunately, that “free online music” may turn out to be virally infected (which makes it a security concern), or may pose an unacceptable bandwidth burden on the institution, or there may be copyright problems which result in DMCA notices to the institutions.

- To avoid those issues, some schools may purchase legal locally-delivered online music programs for their users.

Mobile Systems: Whole Disk Encryption

- If laptops or tablet PCs (such as those that may be used by your Admissions, Financial Aid staff, or Health Center staff) contain sensitive personally identifiable information, those systems should receive special treatment, including but not limited to installation of whole disk encryption.
- The institution may also wish adopt policies describing how laptops and tablet devices will be physically secured when off campus. For example, is it okay to leave one in an unattended car? In one's hotel room? Do systems need to be physically marked with the university's name and an inventory control number? Is a security cable required? What about use of a special screen to prevent "shoulder surfing" on airlines and in other public places? How will network access be handled? Will a VPN always be used to secure network links?

Physical Security of Desktop Systems

- Everyone worries about laptops and other mobile devices, but desktop systems also need a little tender loving care, too, particularly since they often sit unattended. That is…

  -- Desktop systems are often in exposed areas, such as reception areas, or labs, or shared office spaces -- are they secured against physical theft by a cradle or cable or other security device?

  -- Loosing a laptop (and the data on it) is a very bad thing, but what if a a hard drive gets stripped out of a desktop?

  -- You know, I assume, that there are small devices which can be plugged into USB or PS2 ports which can do all sorts of interesting things? You can buy USB or PS2 keystroke loggers, for example, or for those who are more whimsical, have you seen ThinkGeek's "Phantom Keystroker"? I'd urge you to pay attention to spontaneously appearing "replacement keyboards," too.

Educating Users

- As tempting as it may be to fantasize that automated tools (such as a university produced software CD) or centrally managed all PC systems can eliminate all desktop or laptop security issues, that **IS** just a fantasy, not a reality.
- We actively need the cooperation of our users when it comes to minimizing the risks we face. We need them to be skeptical/cynical online, and we need them to take the time to learn and understand the risks they face, and the traps that may be laid for them online, and we need them to engage in safe and sane computing practices.
- As a result, any university desktop/laptop security program also needs to include a user education component, whether that's in the form of web pages and FAQs, face-to-face instructional programs, online instruction that can be taken at the user's convenience, or other outreach.

Being Available to Address User Questions

- The flip side of the “push” education channel is being available to address user questions when they arise. Spending just a minute or two on a user’s question can avoid a tremendous amount of work later…

  -- “Microsoft sent me a patch in the email, but I don’t completely understand how I’m supposed to install it…”

  -- “Ever since I let me nephew play on the web using my laptop, it’s been running slowly and crashing all the time. Do I need to do anything about that?”

  -- “I’m putting up a web site for my department, and I found a great script that I want to install so that people send email to us via a web form…”

Coping With Compromised PCs

- If, in spite of all best efforts, a user’s PC is infected with malware or otherwise compromised, each campus needs a solution for dealing with those compromised PCs.
- Some sites may attempt to disinfect compromised systems using an antivirus product, but others, based on less than favorable experiences doing that, may elect to recommend that the system be “nuked and paved,” formatting it and reinstalling it from scratch (or at least from a known clean backup).
- This can be a difficult/time consuming process if each system is different, but if you’re fortunate enough to be at a site that has standardized on a common student laptop, you may be able to reformat the system and drop a copy of the standard system image on the compromised host in short order, much as lab machines routinely get reimaged.

Coping With "EOL" PCs

- Eventually, even in higher education, PCs go end of life (EOL) and are surplus’ed or otherwise disposed of.

- In my opinion, higher education has developed a good sense of the risks associated with sending EOL systems off site with media intact, and as a result, use of data sanitization software is now fairly routine (although not perfect).

- Systems which have hardware failures are at more risk of being disposed of with inadequate media sanitization.

VI. Servers

Server Operating Systems

- It is hard to make any hard and fast comment about what operating system is most popular for servers in higher education, except to note that Linux and Windows continue to both have strong followings.

- One approach that you can take to seeing what operating systems are important in higher education is to review what platforms are supported for important academic applications such as:

  -- **Mathematica** (Windows, Mac OS X, Linux, Solaris, HP-UX and AIX),
  -- **Matlab** (Linux, Mac OS X, Solaris, Windows),
  -- **SAS** (AIX, HP-UX, Linux, Windows, OpenVMS for Itanium, Solaris, z/OS)

Security and System Administrators

- When it comes to servers, regardless of the operating system chose, the security orientation and the technical skills of the server's administrators can be key.
- In higher education, we are fortunate to have some truly excellent system administrators, but at least in some cases "system administrators" have been dragooned into service without having adequate training and experience. That's not fair for anyone.
- A more consistent program of system administrator training, one-on-one mentoring, or at least delivery of sysadmin "bibles" such as Evi Nemeth, et. al.'s **UNIX System Administration Handbook** or Thomas Limoncelli and Christina Hogan's **The Practice of System and Network Administration** would be tremendously helpful when it comes to boosting technical sys admin proficiency.

Privileged System Access

- An example of one technical issue that arises in server administration is how privileged system access takes place, an important issue that may get little thought.
- Some sys admins may simply ssh in to their machine, logging in as root. But think of the issues that raises: passwords (the most important password of all in this case!) must be shared, and shared passwords mean that you may not be able to tell who actually logged in and installed new software or created new accounts or reconfigured settings -- ugh.
- That's one reason why use of su (or better yet, sudo) is so common as an alternative in higher education…
- Sudo also is good in that it lets you grant a particular person access to just a subset of administrative "powers," rather than a root login's "all or nothing" approach.

Logging

- Local vs. centralized logging: most servers do syslogging to local files by default. In higher education, however, where there may be dozens or hundreds of servers in play, centralized logging is an important alternative.
- Centralized logging insures that logs cannot be surreptitiously edited on a compromised system in an effort to conceal details of a breach.
- Centralized logging also facilities log event correlation and syslog summarization/reduction (processes which make the syslog “firehose” usable, and insuring that exceptions which require attention/intervention will be noticed)
- Centralized logging is also more likely to result in trustworthy time stamps (how often have you seen servers that fail to run NTP for time synchronization?)

Detecting Unauthorized Changes

- Another cornerstone of good system security in higher education is the use of tools to detect unauthorized changes to critical system files and settings.

- A classic tool for detecting unauthorized changes of that sort would be “Open Source Tripwire,” see http://www.tripwire.com/products/enterprise/ost/

Maintaining Software Currency (Patching)

- You are probably already familiar with Microsoft Update, or OS X's Software Update functionality, but I’ve found that some non-Linux people may not know that automated software update tools are available for Linux hosts, too.

  Examples would include:

  -- apt-get (originally a Debian program, but now also used by OpenSolaris, and by the Mac Fink project)

  -- up2date (RedHat)

  -- yum (most closely associated with Fedora Core)

Hardening Servers

- Especially in a de-perimeterized environment, hardening servers by disabling unneeded services and protocols and other similar steps is key.
- There are many good guides to hardening servers, but http://www.nsa.gov/snac/downloads_all.cfm remains an excellent source of free hardening guidance, and the Bastille Unix project an excellent automated hardening tool (see http://bastille-linux.sourceforge.net/)
- Windows Server 2003 admins often will turn to “Windows Server 2003 Security Guide” http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx and the Microsoft Baseline Security Analyzer is an excellent automated tool; see www.microsoft.com/technet/security/tools/mbsahome.mspx

Anti-Spam

- Higher education generally employs one of two main anti-spam strategies…

- Smaller colleges will often use a commercial anti-spam appliance, or route mail traffic to a hosted anti-spam solution by redirecting their MX records appropriately.

- Larger colleges will often handle anti-spam efforts in house, with a common “recipe” being a block list such as the Spamhaus Zen list used at connection time, followed by SpamAssassin or another content based spam filter.

Server Side Anti-Malware

- Complementing (but not replacing) desktop antivirus software, it is also routine to see colleges and universities use a server side antivirus product, typically a product that's different from the product used on the desktop. One popular open source server-side product is ClamAV (see http://www.clamav.net/)

- Servers may also filter or defang potentially dangerous attachments or message constructs using a filter such as Procmail Email Sanitizer (PES), see http://www.impsec.org/email-tools/procmail-security.html

Hardening Production DNS Servers

- Just as campus mail servers were once vulnerable to being exploited as open relays, open recursive campus DNS servers can also be exploited and need to be secured.

- For a discussion of some issues associated with campus name servers, see “Port 53 Wars: Security of the Domain Name System and Thinking About DNSSEC,” http://www.uoregon.edu/~joe/port53wars/port53wars.pdf

Departmental Servers

- The distributed nature of computing at many campuses means that important systems may be located out in departments rather than in a tightly controlled data center.

- I've previously attempted to outline some of the considerations that may pertain to that sort of a distributed environment; see:

  "Running a Server? How Does It Score on the Server Administration Self-Assessment Scorecard?"
  www.uoregon.edu/~joe/sasas/north-dakota-server.pdf

What About Outsourced Servers?

- An emerging trend in higher education is a willingness to consider outsourcing key services.

- For example, a growing number of institutions are now entrusting their students' email to Google or Microsoft.

- Does making a change of that sort improve the security of that traffic? Worsen the security of that traffic? Exchange one set of security concerns for another?

VII. Campus Network Security

Bandwidth Management

- Years ago, it was routine for sites to deploy bandwidth shaping appliances (such as those made by Packeteer) to control bandwidth usage associated with peer-to-peer applications. At one point in time, I made what I *think* was a pretty strong case for their consideration, see “The Case For Traffic Shaping at Internet2 Schools,” January 2002, http://www.uoregon.edu/~joe/i2-traffic-shaping.pdf
- Half a dozen years later, a combination of increasing use of encryption by P2P programs, plus dynamic port hopping by those applications, higher network speeds, aggressive legal enforcement and other factors have changed/reduced the utility of bandwidth management appliances and have caused me and many others to change perspective. See http://www.uoregon.edu/~joe/missing-half/missing-half.pdf at PDF page 83.

Perimeter and Interior Firewalls

- I treated the issue of perimeter and interior firewalls in some depth in the talk I mentioned earlier, “Cyberinfrastructure Architectures, Security and Advanced Applications,” so I won’t discuss them here (except to provide this placeholder so you won’t think I’ve forgotten they exist as a network security building block).

VPNs

- VPNS (both traditional IPSEC VPNs and SSL VPNs) are increasingly common in higher education, albeit for reasons which may seem uncommon to non-higher education users.
- For example, it is routine for resources to be controlled by IP address range -- if you’re coming from the right IP address range, you can access the resource, while if you’re coming in from a home broadband connection, you’d be denied access. VPNs fix that issue by giving the user an “on campus” IP address, a function that's over and above any encryption/firewall bypass functionality.
- VPNs also can be an important part of campus wireless security, since many campuses prefer to leave encryption to the application rather than deploying WPA or WPA2 directly.

Proxy Servers?

- Except at some (comparatively rare) higher education institutions where proxy servers are used as a control point for things like anti-malware filters or content filters, I don’t believe that proxy servers are a highly emphasized part of higher education network security (unlike many corporate environments where ALL web traffic is routinely forced through a proxy server).

- Some sites may have proxy servers optionally available to safely accommodate browsers attempting to do WPAD (proxy server auto discovery), see en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol for information about WPAD

Passive Monitoring (Snort, Bro, Etc.)

- A classic component of many higher education IT security programs is passive network monitoring using an intrusion detection system such as Snort (http://www.snort.org/) or Bro (http://www.bro-ids.org/).

- Use of such tools makes it possible to identify inbound and outbound attack traffic, and to readily identify compromised systems. The value of passive monitoring may be challenged as encryption of traffic becomes more common.

- Intrusion detection systems may be complemented by Netflow flow monitoring, which summarizes traffic flowing through campus routers on a flow-by-flow basis.

Active Scanning (Nessus, NMAP, etc.)

- Active scanning takes a page from the hacker/cracker book, with local security staff running scans for vulnerabilities against locally connected systems using tools such as Nessus (http://www.nessus.org/nessus/) or NMAP (see http://nmap.org/).

- Like passive monitoring, the value of active scanning is diminishing as we move forward: active scanning has been decreasing in effectiveness over time, as users deploy host based software firewalls, or hardware based “personal firewalls.”

SNMP and RRDTool, etc.

- One simple indication of abnormal activity may be unusually high traffic levels.

- Campus traffic levels are often monitored using SNMP, with counters getting graphed using RRDTool or another time series-oriented data reduction and display tool.

Hardening Layer 2

- Carefully managed campuses will routinely harden layer two devices (e.g., securely configure* their ethernet switches) to insure that ARP poisoning and similar MITM-oriented attacks aren't possible.

- For more information on L2 issues, see pps. 80-83 of www.uoregon.edu/~joe/architectures/architecture.pdf

_____

* Yes, I know, not all ethernet switches have much in the way of per-port security. And yes, I fully agree that some other approaches to dealing with L2 issues, such as static MAC address assignment, really don't scale very well. Nonetheless, you need to be paying attention to this, seriously. Really.

Wireless Networks

- Most universities “get it” when it comes to not using WEP; some may do WPA or WPA2, while others may leave encryption to the application or rely on VPNs.

- Some universities are now doing 802.11x

- Others may prefer to start all users in a sandbox, have the user authenticate using a secure web page, giving the authenticated user access to another network with full Internet access.

- Another aspect of wireless security: most universities do not allow private wireless access points; some may actively monitor campus airspace for rogue ones.

BCP38

- BCP38 refers to network anti-spoofing filters.

- That is, if you’re the University of Oregon and your addresses are all drawn from the 128.223.0.0/16 block, there’s no reason why you should be emitting spoofed traffic that’s pretending to be “from” some other address space.

- Because of the problems associated with "tracking back" spoofed traffic once it hits the Internet, routine deployment of BCP38 filters at the campus border is extremely important, and should be a routine part of every campus' network security. See slides 4-16 of “A Brief Practical Security Punch List,” http://www.uoregon.edu/~joe/punchlist/punchlist.pdf

VIII. Policies

AUPs

- Earlier in this talk I mentioned that campus acceptable use policies ("AUPs") are a nice example of a virtually universal campus IT security practice. I wonder, though, how long it's been since many of those AUPs were last updated?

- Higher education often likes to treat AUPs like national constitutions, keeping them very high level, and thus avoiding the need for frequent updates, but I wonder if that doesn't represent a hold over from simpler and less legalistic times? You might be shocked if you were to compare a typical higher education AUP with terms of service for a commercial broadband service provider!

- AUPs may also not be keeping up with changes in the importance of the online world…

Sample Issue: Employee Accounts

- Assume Jane Doe works for your school, and uses her university account for:
  -- work correspondence (perhaps she counsels some of her students by email),
  -- for professional purposes (such as publishing web pages), and
  -- for personal purposes (such as in conjunction with an airline frequent flyer program)
- What happens when Jane is no longer with your school?
  -- "As soon as she's no longer an employee, terminate her account!"
  -- "Let Jane's supervisor have access to her account so that she can make sure that work correspondence is handled"
  -- "Set up an autoresponder telling people what's changed"
  -- "Jane was a nice person, let her keep her account"

But…

- What if Jane had mixed roles, and is a student as well as having been an employee? Should she be forced to get a new email? Should she be allowed to keep her old one?
- What if Jane had broadly-relied-upon network resources on her account (such as highly respected/influential web pages)? Is it in the institution's best interest to make those pages break/suddenly disappear? Or is it desirable/fair to Jane to force those pages continue to be available (albeit frozen in time like bugs in amber)?
- What if Jane's username got promptly recycled and reassigned, and a new student got Jane's old username, and a "real eyeful" w.r.t. student requests for advice that were in all likelihood meant for Jane, not the new student? Or what if the student user her new account to obtain access to all of Jane's accumulate frequent flyer miles by doing a password reset via email?

I Guarantee Your AUP Needs Updating

- That was just one "minor" example.

- I guarantee that because of changes over time, your AUP DOES need updating, and when you update it, it shouldn't be updated just by your IT security staff, or just by your university counsel, or even just by your IT leadership, but by a committee that includes all of the above plus faculty, students, and staff members, with ample opportunity for community feedback.

- And when it is time to do this, I suspect that you will also find that your IT governnance and policy development areas also need attention (because it is rare to find a school that has IT governance and policy development completely squared away)

Another Policy Area: DMCA

- Many colleges and universities have registered under the Digital Millennium Copyright Act in order to take advantage of the “safe harbor” provisions it extends to service providers. See http://www.copyright.gov/onlinesp/

  Having done so, the institution then receives DMCA notices from intellectual property holders who believe that infringement has occurred.

- DMCA-related issues are a staple of news coverage, and recently, there have been reports of a surge in DMCA notice volume; see, for example:

  blog.wired.com/27bstroke6/2008/04/riaa-sends-spik.html

Another Policy Area: Real Time Emergency Notification

- The importance of having real time emergency notification options became clear for higher education during the following the terrible tragedy at Virginia Tech, and many schools are in the process of rolling out reverse-911 systems, or campus reader boards, or campus sirens. [For a discussion of real time emergency notification, including a briefing on the Clery Act and a discussion of some real time emergency notification technical solutions, see “Real Time Notification During a Disaster or Other Emergency,” www.uoregon.edu/~joe/notification/]
- But what of policy issues relating to registration? Should it be compulsory for students to register for emergency notifications? Who should have the ability to send notices? This is a very powerful tool we're just learning to "drive."

The Obscure “Deemed Export Rule”

- Higher education is somewhat unique in that it often has both specialized resources (such as high performance computing systems) which are subject to US export controls, and international students who may be from countries that are not allowed access to those resources.

- IT security staff and institutional legal staff thus need to be familiar with things such as the “Deemed Export Rule” and how it may apply to potential access to campus specialized resources by certain foreign nationals. [The Bureau of Industry and Security of the US Department of Commerce has a helpful Q&A covering the “Deemed Export Rule” at www.bis.doc.gov/deemedexports/deemedexportsfaqs.html and additional info at www.bis.doc.gov/deemedexports/deemedexportssupplementqa.html by the way…]

The Banks Will Dictate Fundamental Aspects of Your Security: PCI-DSS

- The Payment Card Industry Data Security Standard (PCI-DSS, https://www.pcisecuritystandards.org/tech/index.htm) defines what sites must do if they want to process credit card transactions, including college and university sites.
- Because handling credit cards is a common and important higher education requirement, and because failure to meet PCI-DSS standards may result in authorization to process credit cards getting withdrawn, most universities (at least virtually all the universities which rely on processing credit cards) end up following the policies and procedures and requirements of the PCI-DSS.
- Welcome to a highly regulated environment. :-) Oh, and of course that highly regulated environment includes some other abbreviations, too…

HIPAA, GLBA, and SOX

- A good perspective on HIPAA and higher education can be found in the Educause article “HIPAA and Higher Education,” www.educause.edu/ir/library/pdf/erm0159.pdf

- For resources relating to the Gramm Leach Bliley Act, see http://connect.educause.edu/term_view/GLB%2BAct

- For the Sarbannes Oxley Act and higher education, check out http://www.nacubo.org/Documents/news/2003-03.pdf

- The complexity of these sort of compliance regimes is yet another driver that results in many schools following a common approach when it comes to these security-related areas…

IX. The Future

Let me just flag **one** "futures" issue for your consideration, one item that will have profound security implications…

IPv6

- We’re less than **1,000 days** from projected exhaustion of IPv4 address space. This *may* have security implications…
- First, IPv6 may *already* be in use on your campus if only in the form of things like Teredo tunneling; you may prefer to do native IPv6 service via Internet2 or another network
- Second, many security appliances, as well as things like Netflow version 5, just don’t know about IPv6 traffic. Other devices may do IPv6 even if/when you aren’t expecting it!
- Third, security methods that used to work in the comparatively small world of IPv4 addresses (like exhaustive IP-by-IP scans, or IP-by-IP antispam blocklists) may no longer be practical in the expanded world of IPv6
- Finally, if your school is a legacy IPv4 address holder, you should be looking at/thinking about ARIN’s Legacy RSA, see http://www.arin.net/registration/legacy/index.html

X. Conclusion

“I Think You’re Completely Wrong!…”

- Now that we’ve gone through this whole thing, some of you may be waving your hands and saying, “Hey, I think you’re SO wrong… I don’t know ANYONE at ANY college or university who’s doing <X>! I don’t think that’s really a ‘norm’ or common practice at all! And what about <Y>??? You didn’t talk about <Y> at all, and that’s a critical issue!”

- **That sort of feedback would be great!** I’d love that sort of critical review! If I’m wrong (and I’ll be the first one to freely admit that I often **am** wrong), I'd encourage you to adjust this document to reflect **YOUR** experience and perspective. This document is just **my** attempt at capturing some security norms in higher education, but I’d never claim that it is definitive or all-inclusive or error free.
  I’d be happy if it just served as a starting point for you and the IT staff and users at your campus!

"Hey, I Think You're Trying to Use This Process To Actually Actively Direct The Higher Ed IT Security Conversation!"

- Guilty as charged, yer honor. I am crassly attempting to "secretly" appeal to higher education's oft-rumored-to-be-strong herd instinct.

- There may be some schools which actually aren't thinking about some of these IT security issues. Then again, maybe they **should** be, and if you were to really hold my feet to the fire, I might even concede that some of the preceding "norms" may be prescriptive or projective rather than being dispassionately/objectively descriptive.

"And Where Are The Numbers?"

- One way to force objectivity is by demanding numerical support for any claim of "normalcy." That's actually a very fair critique -- without metrics, I suppose I could claim that anything I want is a "norm" or a "standard" but I really *should* have statistics to back up those claims.

- Consider this talk a first effort to arrive at a preliminary set of items of items which can then be empirically validated or rejected based on the data…

- ***And in the mean time, you do know that everyone else in higher education is worried about being ready for IPv6, layer 2 ethernet switch security, BCP38 network anti-spoofing filters, and securing campus open recursive DNS servers, right? :-)***

Thanks For the Chance to Talk Today!

- Are there any questions?