Information Security:
A Perspective for Higher Education

A White Paper By

NEC Unified Solutions, Inc.
Introduction

On a well-known hacker website, individuals charged students $2,100 to hack into university and college computers for the purpose of changing academic grades. Although many students paid for these services, the website turned out to be a scam.

In another incident, the University of Texas at Austin was subject to a brute force attack of the school database that disclosed the Social Security numbers and e-mail addresses of some 59,000 students, alumni and university employees.

These examples illustrate the potential for manipulating and exploiting technologies commonly utilized by universities and colleges today. The proliferation of e-mail use, distance learning and other services that enhance the quality of the student experience and extend education beyond the campus carry a potentially significant price when privacy is not maintained.

As federal and state regulations for information technology and privacy gain visibility from well-publicized incidents, all organizations regardless of industry are reviewing the potential liability implications resulting from lack of compliance. Due diligence has become a primary occupation for all, where client or patient information is considered a fundamental data component of the business process, operating under a regulatory umbrella. The obligation on the part of any institution is well-defined and presents specific challenges. Higher Education is no exception; this environment has a strong need for open and accessible networks, but that requirement also generates an obligation on the part of each college to protect the systems and the data they contain. NEC Unified Solutions has the experience to address these challenges by providing regulatory expertise and a comprehensive strategy for information security compliance.

This white paper discusses the regulatory obligations each institution must consider and provides a practical approach to help colleges and universities meet the challenges related to data asset protection.

Regulatory Overview

Several key privacy regulations apply to educational institutions, including a combination of both federal and state directives in some cases. The following list is just a sampler of those of concern to colleges and universities.

Family Education Rights and Privacy Act (FERPA)

FERPA is perhaps the most applicable federal regulation targeting colleges and universities in that it specifically prohibits the disclosure of personally identifiable education information regardless of state, i.e. written records or electronic data. This includes information pertaining to
student financial aid records as well as grades. Furthermore, institutions require written permission from students to disclose such information to any other party.

Computer Fraud and Abuse Act (CFAA)
The CFAA applies to individuals who gain unauthorized access to “protected computers” under the intent to obtain information that may be of specific value and the premise to commit fraud. The definition of a “protected computer includes any computer device that is utilized for communication or commerce by a financial institution or the U.S. government.

Gramm-Leach-Bliley (GLBA)
This act targets financial institutions, but also applies to colleges and universities whenever customer financial information is maintained. This information includes names, Social Security numbers as well as customer account numbers. The regulation requires such institutions to protect this data and information to ensure integrity.

USA Patriot Act
The Patriot Act was passed as a result of the terrorist events that took place on September 11, 2001. This act provides law enforcement agencies with greater access to electronic communications. A key provision that applies directly to educational institutions includes requiring colleges and institutions to grant access to student records related to any suspected terrorist investigations or activities.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The intent of the HIPAA Act of 1996 is to protect patient rights and certain health plan participants. As part of this act, patients must receive written policies related to information policies. Furthermore, this act requires any college or university that may be affiliated with health care providers to alert students of such health care provider information policies. In addition, HIPAA requires such entities to detail and internally publish information security policies, educate employees, perform security assessments as well as maintain other security-related activities that protect data assets covered under the act.

A Practical Approach
Regardless of regulatory compliance, it behooves any organization to exercise due diligence with respect to the protection of student information or any other data assets. It is also imperative for educational institutions to recognize that information can be maintained and disclosed in any manner, i.e. verbally, electronically or in a written document.
Regardless of how data is transmitted, most regulations require measures that control information at appropriate levels within the context of the intended regulation and therefore appropriate control mechanisms must be applied.

The section below provides an overview of a practical approach for the protection of data assets based in part on information security “best practices” derived from ISO 17799.

Building the Regulatory “Compliance Roadmap”

In order for any educational institution to comply with regulations or perhaps internal directives, appropriate steps must be taken in order to recognize those areas where opportunities exist to better protect data assets and in turn provide greater degree of privacy. A “compliance roadmap” should be developed to highlight specific regulations that an institution needs to address as part of its compliance and information security program. This process should include regulations and mandates that are both federal as well as state specific. As an example, the states of Arizona, California and New York, prohibit schools and colleges from displaying student Social Security numbers on student rosters or identification cards as well as any other documents that may collectively list individuals attending such institutions.

The Compliance Roadmap should include a matrix of specific regulatory requirements and the correlation between such regulations and an organization’s specific information security processes and computing assets. In other words, the matrix should identify gaps in current processes that may pose compliance challenges. This approach can be utilized as an excellent starting point for the identification of activities tied to the compliance process. Furthermore, such a matrix can be used to identify challenges as simple as a lack of intelligence, i.e. the identification of the fact that the institution does not have enough information to determine what to protect and how to address such challenges.

Furthermore, such “roadmap” documentation can serve as a basis for designing an effective security program as well as the security architecture including policies, procedures, intrusion detection, virus control, auditing and assessments as well as metrics associated with the measurements of associated risk and risk remediation.

Defining Information Security Risk and Vulnerabilities

In order for organizations to address potential gaps, a comprehensive information security assessment should be conducted to identify vulnerabilities and define specific risks associated with such
vulnerabilities within the context of regulatory directives. The assessment should focus on the organization as a whole and not just its technology components. It must be understood that security is a process. Therefore, assessing only the technology may, in fact, provide merely a partial picture of the security posture. The following phases should be considered rudimentary assessment activity requirements.

**Security Assessment Approach**

**Phase I - Information Security Program and Security Strategy Assessment**

This phase includes the discovery and verification of processes associated with the management and maintenance of the information security initiative. This assessment phase should cover all non-technical technology risk management processes, such as:

- Compliance monitoring
- Physical data protections
- Policies and procedures
- System configuration templates
- Liability coverage
- Intrusion detection/prevention
- Anti-virus management
- Incident handling and response
- Remote access
- E-mail risk management (Anti-virus and SPAM management)
- Security Awareness
- Vulnerability alert handling and dissemination

**Phase II - External Network Vulnerability Assessment**

This assessment component is focused on the discovery of vulnerabilities related to networks and devices that maintain a presence outside of the institutions administrative, protected or private network, including the following:

- Connectivity or segregation of the administrative and student networks
- External routers
- Firewalls
- Web servers
- DMZ architectures
• Modems (war-dialing)
• Campus-campus VPN connectivity and protections
• Wireless networks

Phase III - Internal Network Vulnerability Assessment

This phase includes the discovery of vulnerabilities associated with an institution’s internal network computing devices such as:

• Routers
• Switches
• Servers
• Desktops
• Gateways
• VoIP (Voice over IP)
• Any other IP based device located on the school network

Information Security Policies

Policies are a key component and the center point of any information security program. Such documents should define clearly and concisely the required activities that protect data and ensure privacy. These documents also serve as a definition of due diligence on the part of the institution. For example, “data classification” policies ensure that all data protection measures are applied across the organization in a uniform manner regardless of state, i.e. handwritten or electronic. In conjunction with an effective security awareness program, where all employees are trained in information security rudimentary concepts and the use of information security policies, this process will ensure that all employees will become full participants in the information security effort aiding in the regulation of privacy and disclosure. At a minimum, most policies address the following areas:

• Privacy
• Access to Electronic Information
• Categories of Responsibility
• Ownership of Information, Data and Software
• Data Integrity
• Classification of Data and Information
• Personal Use of Computers
• Downloading Software
• Passwords
• Storage of Passwords
• Computer Viruses
• Destruction of Information and Data
• Modems
• Use of Personal Computer Equipment
• Positioning Computer Display Screens
• Locking Sensitive Information
• Disclosing Information About Computer Security
• Tools to Compromise Computer Security
• Intellectual Property Rights
• Login Banner
• Password System Set-Up
• Log-In/Log-Off Process
• System Privileges and User Account Set-Up
• Revoking System Access and Notification
• Data Back-Up
• Data Encryption
• Computer System Logs
• Data Center and Physical Security
• E-Mail Security
• Internet Acceptable Usage
• Establishing Internet-Based Network Connections
• Mobile Computers

Procedures

In order for educational institutions to demonstrate due diligence and provide auditors with the appropriate documentation related to security and privacy control, it is imperative that detailed processes exist with respect to change management. The value of any security or privacy process-related activity is its “audit ability.” In other words, the ability to demonstrate a procedural approach to managing activities. These procedures must include documents such as incident handling, system configuration and system development as well as, for example, processes that control the purchasing process. This procedure must define the required criteria for evaluating vendors and suppliers with respect to pre-
existing security controls in hardware, software and consulting services. These types of procedures play a key factor in ensuring that internal policies are not violated due to the introduction of less-secure systems and services, so that security and privacy are maintained at acceptable levels of risk.

Liability Insurance Coverage

An area that educational institutions continue to overlook with respect to information security is the area of insurance coverage. Every institution purchases a policy that covers the organization for a number of potentially costly events; however, few consider the fact that the “errors and omissions” policy sections are an opportunity to extend coverage into the information security arena. This type of coverage is often associated with “hacker” related events and circumstances that directly affect a school’s ability to control privacy. In addition, this type of insurance coverage should be well scrutinized and developed in concert with the overall information security program, so that capital allocation related to the security initiative will be balanced by coverage. This type of coverage, however, can only be obtained once the due diligence related to data and information protection has been exercised.

Information Security Program Management

With respect to capital constraints, many institutions have allocated the responsibility of information security to all Information Technology staff, in effect making this “everyone’s” responsibility. This approach is simply not effective in the real world, due to the lack of ownership. A key factor to ensure that an effective information security program exists within the institution is to designate a specific individual or individuals with the responsibility for the development, coordination and on-going development of the security program. This individual should be tasked with both process and technology as well as vendor management and the reporting of security-related activities. Furthermore, this individual should work in concert with the compliance office to ensure that the intent of specific state and federal regulations has been met by the institution as whole.

Conclusion

Implementing robust information security standards for higher education requires not only a knowledge of the pertinent regulatory requirements but a practical approach to ensuring full compliance. NEC Unified Solutions can help your organization develop a Compliance Roadmap to identify regulatory requirements and evaluate how your organization measures up in each area. Such a roadmap can serve as a basis for designing an effective security program as well as the security
architecture. This program will include policies, procedures, intrusion
detection, virus control, auditing and assessments as well as metrics
associated with the measurements of associated risk and risk
remediation.

If you are interested in partnering with NEC Unified Solutions for your
information security strategy, contact us at 1-800-240-0632.

About NEC Unified Solutions

NEC Unified Solutions Inc., a leader in integrated communications solutions for the
enterprise, delivers the industry’s most innovative suite of products, applications and
services that help customers achieve their business goals. With more than a century of
communications and networking expertise, NEC Unified Solutions, Inc., a subsidiary of
NEC America and affiliate of NEC Corporation (NASDAQ: NIPNY), offers the broadest
range of communications services and solution choices, flexible product platforms and
applications, and an open migration path to protect investments. NEC Unified Solutions,
Inc. serves the Fortune 1000 and customers across the globe in vertical markets such as
hospitality, education, government and healthcare. For more information, visit
www.necunifiedsolutions.com or call 1-800-240-0632.

All trademarks are property of their respective owners.

Additional Resources


2. Ralph K. M. Haurwitz, “Hackers steal vital data about UT students, staff,” Austin American-Statesman, March 6, 2003, available via
www.austin360.com/aas/metro/030603/0306authack.html