

MTU's Risk Assessment

GLBA (Gramm Leach Bliley Act) Information Sheet, Risk Assessment Process, Risk Assessment Required Data Sheet and Compliance Survey

Draft Issued: February 23, 2006

Please return by March 22, 2006

Introduction

The GLBA is a comprehensive law affecting institutions and departments that deal with financial information which includes nonpublic personal information such as addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. Due to the fact that MTU does significantly engage in student loan making and provides other financial services that use nonpublic personal information, MTU falls within the definition of "financial institution" under the Gramm-Leach-Bliley regulations. For these reasons, MTU will be reviewing policies and systems to ensure compliance with the requirements of the Safeguards Rule of the Gramm Leach Bliley Act (GLBA). MTU's current FERPA initiatives will ensure compliance with the Privacy Rules required by the GLBA, limiting the scope of this assessment to the Safeguards Rule.

Requirements

The GLBA includes requirements to protect the security, integrity, and confidentiality of this consumer information. To be GLBA compliant, organizations must develop, implement, and enforce a comprehensive information security program including administrative, technical, and physical safeguards as determined appropriate for the institution and data. In addition to developing their own safeguards, organizations are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

Due to these requirements, the ITS Security and Policy group will be performing risk assessments on all areas that must meet GLBA compliance requirements.

Actions required

The following basic actions must be taken to satisfy GLBA requirements:

- Assess risk
- Manage and control risk
- Oversee service provider arrangements
- Adjust the program to work with new technologies.

MTU's Risk Assessment

Appendix B (continued)

Risk Assessment Process

The following document describes the ITS Security and Policy Risk Assessment process. It should help you understand what elements of your systems, network, and policies that we will be analyzing, and our process for doing so.

Process Outline

Step 1: Identify assets (i.e. data, encryption software, processors, etc.) and their value.

Step 2: Identify threats to assets such as deliberate removal, accidental corruption, etc.

Step 3: Identify the likelihood of occurrence that the threat could happen (Low, Medium, High).

Step 4: Identify the consequence or impact if threat did occur (high expense, low destruction, high embarrassment, etc.).

A table similar to the following is created to break down the assets, risks, value, likelihood, and impact. Please note that this table is generalized to help you understand what the process entails. More specific asset listings will be needed, and exact values may not be necessary or available.

Asset	Value	Threat	Likelihood	Impact
Software	50,000	Unauthorized disclosure	High	High Expense, High Embarrassment
		Unauthorized modification	Low	High Expense, High Embarrassment
		DoS attack	Low	Loss of service

From this table, we make recommendations with considerations such as: if the likelihood and impact are high “do something about it”, whereas if the likelihood and impact are low “maybe do something about it”. This helps us to assess acceptable levels of risk and to perform cost/benefit analysis.

Once this process is done, we consider:

- 1) Procurement of protection tools.
- 2) Time and expenses to implement security protections
- 3) Does cost to implement tool / controls outweigh the impact?
- 4) Will other applications continue to function properly and with minimal necessary disruption if the tools and controls are put into place?
- 5) Will policy / procedures or security awareness lessen the impact and/or likelihood of the threats?

MTU's Risk Assessment

Appendix B (continued)

Risk Assessment Required Data Sheet

In order to begin the security assessment process, the following data is required:

- Data flow diagrams
 - What data is sent
 - Where is the data sent
 - What protocols are used
 - Any security methods used
 - How is data stored, and how is it accessed.

- Infrastructure diagrams
 - Servers
 - Operating system, service pack, services running
 - Network hardware
 - Security systems (firewalls, IDS systems)
 - Client connections and administrative systems

Security and Vulnerability Scan

We will need to schedule a security scan of the systems involved in the deployment. A suitable time and date when the machines will be on and a scan will not disrupt network traffic should be chosen. Administrators of the machines involved in the scan should be notified, as the scan can result in anomalous log entries and other system events. Please contact ITS to schedule a scan of your systems.

General System, Application, and Process Information

Please answer the following questions for each system or software package that they are applicable for:

- 1) What are your current security policies? Please provide copies or reference existing policies.
- 2) (Where applicable) What is your system or application's name?
- 3) Does your system collect user data? If so, what data does it gather. Do any special compliance requirements apply, such as the GLBA, FERPA, HIPAA, or other legal or policy requirements?
- 4) Does your system transfer data to outside entities? If so, what data does it transfer? Do you transfer data via email? If so, detail any security processes involved for transferring documents and attachments.
- 5) How is data queried on the system? Where are the results of any queries done on your system stored?
- 6) What are your password requirements (such as: length, complexity, display of plaintext, history, and frequency of required change?)?
- 7) Do systems have a "lock out" capability when users are away, and do you have policies regarding access to systems when users are logged in but not at their station?

What is the log in process, and does it have any security methods such as limiting logins after failure, auditing for logins, use of a login banner, requirement for unique user IDs, and does it disclose any information on a failed attempt to log

MTU's Risk Assessment

Appendix B (continued)

- 8) in (such as stating "invalid password" instead of "login failed").
- 9) What logging methods and options are available? Can you audit based on failure, success, or other methods?
- 10) How are privileges granted on the system? Who may grant them?
- 11) What usage rules are users presented with, and are they required to accept them?
- 12) How are users removed from the system, and when?
- 13) Who has data steward responsibility on the system?
- 14) How does the system handle denial of service attacks or system failures? Is there a single critical component that could become a single point of failure?
- 15) How is data backed up? (backup plan, offsite storage, accessibility) How is data stored, and how is it protected? Is duplicate data stored in hard copy or other form? How is archived email handled?
- 16) How is the integrity of information stored on the system protected?
- 17) Do you have a patch management or update system in place? How are patches handled, and how are they monitored?
- 18) Do you have any external service provider contracts? What security measures are included in them?

MTU's Risk Assessment

Appendix B (continued)

GLBA Compliance Survey

The following survey will help to establish your organization's current compliance with GLBA standards and requirements. This is not a complete survey or a full risk assessment, but it will provide valuable information to assist us in further determining your organization's status and needs.

Please answer the following questions in as much detail as possible:

Administrative Safeguards

- 1) Do you check references prior to hiring employees who will have access to customer information?
- 2) Do you ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information?
- 3) Do you train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
 - a. locking rooms and file cabinets where paper records are kept;
 - b. using password-activated screensavers;
 - c. using strong passwords (at least eight characters long);
 - d. changing passwords periodically, and not posting passwords near employees' computers;
 - e. encrypting sensitive or confidential customer information when it is transmitted electronically over networks or stored online;
 - f. referring calls or other requests for customer information to designated individuals who have had safeguards training; and
 - g. recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.
- 4) Do you instruct and regularly remind all employees of your organization's policy - and the legal requirement - to keep customer information secure and confidential. This includes providing employees with a detailed description of the kind of customer information you handle (name, address, account number, and any other relevant information) and posting reminders about their responsibility for security in areas where such information is stored - in file rooms, for example?
- 5) Do you limit access to customer information to employees who have a business reason for seeing it? For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent they need it to do their job.
- 6) Do you impose disciplinary measures for any breaches?
- 7) Do you use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information? For example, supplement each of your customer lists with at least one entry (such as an account number or address) that you control, and monitor use of this entry to detect all unauthorized contacts or charges.

MTU's Risk Assessment

Appendix B (continued)

- 8) Do you maintain systems and procedures to ensure that access to nonpublic consumer information is granted only to legitimate and valid users? For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with the financial institution electronically.
- 9) Do you notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access?

Technical Safeguards

- 1) Do you provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit customer information? Specifically:
 - a. if you collect credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit;
 - b. if you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive or confidential data, like account numbers, via electronic mail; and
 - c. if you must transmit sensitive or confidential data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.
- 2) Do you take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure? For example, back up all customer data regularly.
- 3) Do you maintain up-to-date and appropriate programs and controls by:
 - a. following a written contingency plan to address any breaches of your physical, administrative or technical safeguards;
 - b. checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
 - c. using anti-virus software that updates automatically;
 - d. maintaining up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations; and
 - e. providing central management of security tools for your employees and passing along updates about any security risks or breaches.

MTU's Risk Assessment

Appendix B (continued)

Physical and Other Safeguards

- 1) Do you store records in a secure area and make sure only authorized employees have access to the area? For example:
 - a. store paper records in a room, cabinet, or other container that is locked when unattended;
 - b. ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;
 - c. store electronic customer information on a secure server that is accessible only with a password - or has other security protections - and is kept in a physically-secure area;
 - d. don't store sensitive or confidential customer data on a machine with an Internet connection; and
 - e. maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.
- 2) Do you dispose of customer information in a secure manner? For example:
 - a. hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;
 - b. shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up;
 - c. erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information;
 - d. promptly dispose of outdated customer information.
- 3) Do you maintain a close inventory of your computers?