

Information Security Three Year Plan
September 20, 2005

I. Introduction

This three year plan is designed to describe and define projects that we feel represent the most effective use of Vanderbilt resources, reflects the vision of the Information Security Architecture, and meets the goals set forth for the office of the Chief Information Security Officer (CISO). The projects described touch on a variety of aspects of information security: SLA's between IT organizations and the CISO, operational assessments, education, policy development, and risk management.

This plan is based on information gathered from a variety of sources including members of the various IT organizations, committees, and leaders throughout University Central and the Medical Center. This plan will be refreshed on an annual basis at minimum to ensure that it reflects the best information available to the office of the CISO.

II. Scope

The three year plan set forth here and in the accompanying Gantt chart represents projects and decision points for information security at Vanderbilt. It does not, and is not intended to illustrate all aspects of the day-to-day activities of the office of the CISO or any other group or individual within Vanderbilt.

III. Service Level Agreements (SLA's)

The SLA's are the crux of the relationship between the various IT organizations and the office of the CISO. These documents will define the responsibilities for information security between the various parties. The terms of the SLA's will be established through collaboration between the office of the CISO, ITS, NCS, and MIS.

Initially, a general SLA will be established. It will define the overall roles of each organization. This document will include communication, reporting and notification requirements; chain of command; overall duties and responsibilities; and remediation and conflict resolution. The negotiations for the initial SLA are currently set to begin in mid July.

In addition to the general SLA, SLA's will be generated as a result of each of the operational assessments that will be explained later in this document. These subject-specific SLA's will contain additional requirements related to the operational aspects they describe.

IV. EPI

EPI is an organization wide project under the leadership of MIS. The Office of the CISO is working with MIS to develop appropriate information security policies for the implementation of EPI.

V. Operational Assessments

Operational assessments are a key component of the information security at Vanderbilt. They provide the mechanism for the various IT organizations throughout the institution to leverage all information security resources under the leadership of the office of the CISO to improve information security operations and service delivery.

The outcome of these operational assessments will be improved, structured, and consistent procedures and control recommendations which will become part of subject-specific SLA's. These undertakings require strong collaboration between the office of the CISO, the IT organizations, Vanderbilt senior leadership, and the end-user community. The end-dates of Operational assessments that have budgetary implications are scheduled to coincide with the beginning of the budgetary process whenever possible. Two operational assessments will be undertaken during the timeline of this three year plan: Incident Response and Trusted Zones.

Incident Response

Our response is our strongest weapon against information security incidents. It is therefore paramount that we develop a clear, consistent, coordinated methodology across the institution. This incident response plan must encompass not only the actions of the office of the CISO and IT organizations in response to potential security breaches, but also the actions of General Counsel, News and Public Affairs, and Vanderbilt decision makers. The necessary documentation and communications requirements must also be explicitly spelled out.

Our approach is to document our current incident response to leverage what we currently do well, and to understand what needs improvement. After this takes place, the office of the CISO will work with all parties to develop and refine the process. The organizations that are responsible for executing the incident response plan will then be trained on these new policies and procedures. Because this operational assessment is focused on process, we foresee no budgetary impact.

Trusted Zones

Vanderbilt, like its peer institutions, requires open and flexible information resources to provide an environment in which faculty, staff, and students can

thrive. There is often a need for non-standard access to the Internet, especially in the research arena. Wireless access and remote access extends the perimeter beyond the physical limitations of campus. Though many key information resources are centrally managed, many are not. Yet, we as an institution must provide appropriate protections for sensitive information. The juxtaposition of properly protecting sensitive information against the necessity for open, flexible connectivity requires an innovative approach to information security: trusted zones.

With trusted zones, protection of data is not implemented by establishing a solid perimeter between the institution's information resources and the Internet. Rather, access between the Internet and the network has very limited controls imposed at the gateway. Within the Vanderbilt information infrastructure, zones, such as Human Resources, are created where architecture and controls enforce information security policy. Within the trusted zones hardened enclaves will be created. These enclaves will have strong security controls and proper network and application architecture to ensure appropriate access within risk tolerances. By concentrating strong security controls and architecture requirements to only those systems and applications that store and maintain sensitive data, the flexibility that is mandated by parts of the community will be impacting as little as possible. Because of its distributed nature, the trusted zone security model does not require central management of all information resources.

The goal of the initial operational assessment will be to define the concept of trusted zones as they apply to Vanderbilt. This will include defining requirements and identifying resources. The next operational assessment will look at the basic system defense requirements for all systems within the trusted zones including anti-spyware, anti-virus, patching requirements, and policy enforcement software. These minimum standards can then be offered as recommendations to those not in a trusted zone. An examination of the network requirements will also be undertaken. This will examine segmentation, control, and monitoring requirements for network architecture within a trusted zone. Application engineering will also be investigated to see what development models and interface requirements should be incorporated into the applications that host our most sensitive data. And finally, an investigation will be undertaken to determine what changes will be required to properly authorize users within a trusted zone.

VI. Education

The office of the CISO is charged with helping all members of the Vanderbilt community obtain the life skill of information security. Education is essential to that goal. The educational initiatives for the office of the CISO will be defined in the education roadmap. This will leverage many of the efforts that have already occurred at the Medical Center.

Each year, the office of the CISO will focus on expanding and improving its outreach to the various groups within the user community. This concentration does not indicate a lack of educational opportunities for the other users. It only indicates that efforts will be focused on improving the outreach to the particular group indicated. Though our initial concentration will be on the student community, opportunities to interact with staff and faculty will be undertaken. Some of these efforts have already occurred including events around the HIPAA security rule and Medical Center Security Managers.

As can be gleaned from the Gantt chart, a variety of efforts and venues will be employed to reach out into the user community. In the case of the students, the office of the CISO is participating in activities surrounding incoming first-year and returning students. Initiatives will also involve utilizing advertisements in the student newspaper and the Night at the Rand events.

Additionally, we are investigating the establishment of a CISO website. This will either consolidate or point to existing information security sites. It will also provide users opportunities to interact directly with the CISO via questions and responses posted on the site.

VII. Policy Development

In regards to policy, the office of the CISO is currently undertaking a review of the procedures for enacting security policies at the Medical Center. Part of this review is studying the possibility that separate policies should be enacted for end-users and IT organizations. The philosophy behind this effort is to ensure that end-users receive the information that they need concerning their responsibilities without being overwhelmed by highly technical information. IT organizations would be responsible for understanding the more technical policies that relate directly to their positions. The results of this examination will determine the manner in which policies are constructed and approved in the future.

The office of the CISO is currently investigating the process for approving information security policies at University Central utilizing the lessons learned at the Medical Center.

The content of the policies to be developed will be influenced by the examination of the policy approval process at the Medical Center as well as the results of the operational assessments, risk assessments, regulatory requirements, etc.

VIII. Risk Management

Developing a comprehensive, repeatable risk management process is an integral part of the overall success of Information Security. Understanding the risk tolerances, establishing risk baselines, calculating overall risk to this institution is essential. This exercise allows us to set appropriate goals and utilize our resources, both financial and human, efficiently.

The results of annual risk assessments will be used to help develop or amend the SLA's necessary to establish operational requirements. They will also provide the data necessary to make capital and human resource decisions. The risk assessments will also drive strategic decisions within the office of the CISO. Additionally, they will identify the future operational assessments, as well as inform policy development and educational curriculum.

IX. Conclusion

This plan will reviewed annually and will be republished in the fall in of each year.