
Security Services – Implementation Plan

November 19, 2003

Executive Summary

Information technology has allowed the University of Michigan (U-M) to make tremendous strides in its core mission of research, instruction and community support. Unfortunately, with the tremendous power of technology comes a wide range of security threats, which could put the resources of the University and the privacy of its students, staff and faculty at risk.

In order to combat these threats, the University should establish an Information Technology Security Office, which will work cooperatively with units across the University to improve the overall management of IT Security at the University. This will include establishing the IT Security Office as a single-point of contact for tracking and reporting IT security incidents.

Additionally, the U-M should create an IT Security Executive Committee, made up of a cross-section of University leadership. The IT Security Executive Committee should establish University security-related policy, and oversee the direction and priority setting of the U-M IT Security Office.

A companion funding request will be developed and submitted by Laura Patterson and James Hilton.

Background

In August 2003, the IT Commons Security Working Group (SWG) proposed the creation of a Computer Security Incident Response Team (CSIRT) modeled on the CERT Coordination Center's report "Creating and Managing a Computer Security Incident Response Team (CSIRT)" (see <http://www.cert.org/csirts/>).

According to the Security Working Group report, a traditional definition of a CSIRT is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Recently, some organizations have expanded the role of a CSIRT to include proactive services such as performing security assessments and providing quality services including education, training, and assisting in policy development. The Security Working Group recommended the U-M follow this trend, and that it creates a CSIRT with these expanded responsibilities.

Shortly before the Security Working Group issued its proposal and with no knowledge of the group's pending recommendations, Provost Paul Courant and CFO Tim Slottow charged James Hilton and Laura Patterson to develop a proposal for improving the University's approach to information technology security strategy and management. Their request was driven by a number of IT security incidents that had recently occurred on campus. They expressed concern that the university was not providing leadership and support to the community for preventing or responding to IT security issues, and that risk of a serious incident was high. Courant and Slottow charged Hilton and Patterson to submit a proposal for addressing security issues from a University-wide perspective.

In September 2003, Laura Patterson and James Hilton agreed with the conclusion of the Security Working Group that a central security organization needed to be created at the U-M, and determined in order to establish this new group, that an implementation plan needed to be developed.

This report is intended to be the preliminary implementation plan for the new IT Security Office. The goal of this report is to provide enough detail to identify the steps that should be taken to put the new IT Security Office in place. In order to help assure the success of the IT Security Office, this report includes information about challenges that the new organization may face and

recommendations on strategies that the group should use to be successful. The hope is that this report will not only provide adequate information to initiate the IT Security Office, but also can be a resource to help assure its smooth implementation.

The name “IT Security Office” was chosen instead of “CSIRT,” because the responsibilities of the group will be wider than those of a traditional CSIRT. Despite the different name, this new group is intended to have the scope of responsibility that was defined by the Security Working Group in their CSIRT recommendation.

Creation of the IT Security Office

Phased Implementation

The IT Security Office should be implemented in a phased approach. The first year of the organization should be focused on a limited set of priorities, and then additional responsibilities and initiatives should be added over the course of time. A phased approach will allow the IT Security Office to evolve into an organization that fits the needs of the U-M appropriately, by giving ample time to gather information and build support across all affected constituencies and communities.

The First Year

The primary responsibility of the IT Security Office will be the handling of computer security incidents; therefore the primary goal for the first year of the implementation should be to establish incident handling processes and procedures. The rest of the goals for the first year should focus on putting other new services in place, but should avoid initiatives that require significant ongoing operational work for the new office.

The IT Security Office should accomplish the following goals during the first year:

- Hire a Security Officer to lead the IT Security Office.
- Identify resource needs for the IT Security Office, and address those needs through a combination of a staff-sharing program with campus units, and full-time permanent staff.
- Develop incident response handling process and procedures. An important part of this goal is to establish a single-point of contact for security incident handling and reporting.
- Develop and implement a preliminary end-user awareness program and communication plans.
- Identify key security risks of the University, and work with the campus community to mitigate these risks through one or two technical and/or policy initiatives.
- Work with the IT Security Executive Committee and various campus communities to identify and address any organizational issues that may result due to the creation of the IT Security Office.
- Work with IT Security Executive Committee to develop strategic vision for security policy, set priorities for upcoming years, and to develop implementation strategies.

IT Security Office Leadership

The IT Security Office will be lead by a permanent full-time U-M IT Security Officer.

In order to get the IT Security Office implementation underway as quickly as possible, the IT Security Officer should be named immediately. If it is impossible to name the IT Security Officer immediately, then an interim-IT Security Officer should be named so implementation of the new security office can begin.

IT Security Office Home Organization

The IT Security Office will report directly to the Associate Vice President for Administrative Information Services (MAIS), or to a designated Director within the Administrative Information Services organization.

MAIS' own internal security group should remain a separate entity, and should not be directly part of the IT Security Office. The separation of the MAIS security group from the IT Security Office is deliberate and necessary to help assure that MAIS' own security efforts aren't slowed down or halted due to campus-wide activities, and also to help assure that the IT Security Office is not unduly influenced by the local requirements of MAIS.

Making the IT Security Office Successful

As a central group in a decentralized university, the IT Security Office will face many obstacles. Ultimately the IT Security Office will be most effective if it can be created within the following guidelines:

- Leadership from the IT Security Office should focus on outreach to University units to assure that initiatives pursued by the central group are in line with University goals. Fundamental organizational distinctions between “academic” and “administrative” computing exist at all levels of the University and across all units. Leadership will need to establish excellent communication in order to assure that the concerns and ideas of each constituency and community are addressed properly.
- The IT Security Office will need to have processes, groups and forums in place to assure that the all parts of the campus community can provide appropriate input and influence over security directions. Existing processes, groups or forums should be leveraged, and new ones created as appropriate.
- The IT Security Office may assist in the development of policies, but they are not a policy-making organization. They will not dictate security policy for campus. Policymaking should occur at an executive level removed from the IT Security Office. The IT Security Office should be a resource to help units successfully implement security policy, not as policy enforcement group.
- The IT Security Office should leverage existing University services as much as possible, and avoid creating a large operational unit. For example, instead of hiring trainers and technical writers into the IT Security office, staff from existing user services groups within MAIS and ITCS should be leveraged.

IT Security Governance

Establishing an IT Security Executive Committee

Within thirty days of the approval of this implementation plan, Laura Patterson and James Hilton, on behalf of the Provost and CFO, should establish an IT Security Executive Committee. The charge of the committee should include the following goals:

1. To establish security policies for the University
2. To assure that all University constituencies, including students, researchers, instructors and administrators have the proper input into decision-making relating to security issues.
3. To set direction and priorities for the University Information Technology Security Office.

Making the IT Security Executive Committee Effective

A successful security effort at the U-M will require a strong and effective IT Security Executive Committee. The characteristics of the committee should include:

- The membership should include a cross section of University leadership including representation from: the Provost's office; the CFO's office; Dean's offices; non-academic offices (e.g. General Counsel, Student Affairs); and the Michigan Student Assembly (MSA).
- The committee must be a resource that Executive Officers rely upon to establish and interpret security policy. If the committee is regularly ignored or uninvolved in policy setting, its value will be diminished, and the success of the University's security effort will be threatened.
- The committee must have an effective process for overseeing the work of the IT Security Office. In particular, the committee must gather input from campus and assure that efforts of the IT Security Office align with the priorities of the University. The U-M IT Security Officer should have the autonomy to manage the day-to-day work of the IT Security Office, but ultimately the group should be accountable to the IT Security Executive Committee.
- The committee must have processes for gathering input from various campus constituencies and communities including students, researchers, instructors and administrators. This may require that special resource groups be identified to collect information on important security matters.

Staff-sharing Program

An important part of the IT Commons Security Working proposal was the recommendation for the creation of a staff-sharing program. The Security Working Group envisioned an organization staffed by volunteers from various campus units. These volunteers would have a significant assignment (50% or more) to the central security group, but would eventually return to their home offices after six to nine months.

This type of program is exciting to many members of the University IT community. Not only is it an innovative approach to staffing the central group, it provides a vehicle to build expertise across campus, strengthen communication among units, and provide additional input in setting direction for campus IT security efforts.

The staff-sharing program should be part of the implementation of the IT Security Office. A successful implementation will require funding for "back filling" for staff in their home units.

Because a staff-sharing program could be relatively expensive to implement, and in some ways it is an experiment for the University, the program should be evaluated after two years. If it's successful it should be extended, otherwise it should be modified or ended.

Overall Campus IT Security

It would be a mistake to think of the IT Security Office as the University's complete answer to IT security. There is already a great deal of security expertise distributed around campus, and these experts are already following best-practice approaches to securing systems and privacy. By working together as a team, IT Security Office and campus units will best be able to assure that security and privacy of university resources are protected.

Appendix 2: Guiding Beliefs and Ambitions

Guiding Beliefs

“Guiding beliefs” are the truths or realities, within which we believe we must operate to be successful. The recommendations in this proposal are based upon the following guiding beliefs:

- Security is a process, not a result.
- University leadership such as deans and executive officers need to play an active role in setting policy and strategic direction for University security. It may also be important for campus IT leadership to play both an advisory role in these activities, and an important implementation role in the units. Campus IT leadership will not, however, play a governance or administrative role.
- Although the security office will be administratively housed in MAIS it is charged with focusing on university-wide IT security issues. Its existence does not eliminate the need for existing unit-focused security efforts and should not be viewed as a replacement of those efforts.
- Security should be addressed in a distributed fashion across all U-M units, where units take ownership not only of security and well-being of their environment, but also for the security and well-being of the overall University environment.
- A central security organization is necessary to coordinate campus efforts and to provide some services more efficiently than could occur in a fully distributed model. Strong and early involvement of campus units in the planning and implementation of the security office will be important for its success.

Ambitions

“Ambitions” are the broader goals that we hope to achieve for our organization. The recommendations in this proposal are specifically designed to further the following U-M ambitions:

- To establish, in the spirit of the Security Working Group CSIRT proposal, a security organization to coordinate and support campus security efforts and provide appropriate security services.
- To develop a pool of IT professionals across campus, who are highly trained in various aspects of IT security and are able to use this knowledge in a practical fashion to secure local and campus IT environments.
- To have educated end-users of campus IT resources that are aware of risks and able to follow best practices to secure University and personal resources and privacy.