Policy on Security Incident Response

MICHIGAN
ROSS SCHOOL OF BUSINESS

Purpose

The Stephen M. Ross School of Business at the University of Michigan ("Ross") has established a security incident response plan to correspond with and complement University plans for Information Security Policy (SPG 601.27) and Information Security Incident Reporting (SPG 601.25). The plan includes components to assist the entire community being more aware of the nature of security incidents; establishes technology standards for devices to ensure compliance; and ensures that incidents, when known, are reported to the Information Technology Security Services (ITSS) campus group and locally monitored until resolution.

The Community as Partners in Security Awareness

Information resources, in any medium or form, such as printed-paper, digital files, audio/video recordings, etc, are vital Ross School assets. Much of this information must be properly secured to protect the electronic identity of people, the confidentiality of sensitive information in cases of theft or loss, and to comply with state and federal laws. Every community member, department, institute and center that creates, uses or provides information resources has a responsibility to maintain and safeguard these assets. Everyone is expected to use these shared resources with consideration for others. Everyone is expected to be informed and responsible for protecting their own information resources in any environment.

A Shared Responsibility to Identify and Protect our Information Assets

All members of the Ross community have individual and shared responsibilities to protect our information assets in accordance with federal, state and local law. Examples include:

- Unauthorized use of computer systems or data.
- Unusual behavior you observe on your computer or your network connection that might be the result of a virus or network attack.
- Sharing of UM uniqnames, MCards or other forms of electronic identity
- Loss or theft of any equipment that has the potential to store private or sensitive data. This could be a laptop, a thumb drive, a DVD or even a computer printout.
- Loss of any personally identifiable information, such as health information, social security numbers, etc.

Everyone is expected to promptly report any information security incident, security breach or loss of equipment to the Director of Computing Services immediately when first suspected, even if it is unclear whether any private or sensitive data was involved. We all must work together to minimize the negative consequences that may result from any incident and to improve the University's ability to promptly restore operations affected by any incident.

Security Communications, Procedures & Controls

The University, primarily through the office of Information Technology Security Services (ITSS), and the Ross School, primarily through the department of Computing Services, takes reasonable steps to implement information security via appropriate policies, procedures and controls.

Each summer, usually close to August 1, Computing Services will require the viewing and electronic acceptable of a video-based Proper Use of Technology Resources compliance agreement. A goal of this compliance agreement is to remind all members of the Ross community of our shared responsibility to protect our information assets. Chapters in the Proper Use agreement include: understanding the proper use of University technology resources, protecting ones electronic identity, complying with applicable copyright and software license laws, understanding and reporting security incidents, recording and viewing classroom recordings, personal responsibility, and similar.

Computing Services, working closely with ITSS, other members of the University technology community, and the leadership of the Ross School, is responsible for creating technology-related security controls, policies and procedures that appropriately and reasonably prevent, detect, contain and correctly identify risks to the confidentially, integrity and availability of information resources. Examples of appropriate technologies include: a network firewall to prevent unauthorized access of information resources to persons outside of our community; data security restrictions required to access information assets from mobile devices, and data encryption algorithms placed on laptops to safeguard against the loss of equipment.

Security Incident Response

Computing Services has identified an Information Security Liaison and Information Security Coordinator to participate on campus information technology security meetings and proceedings as required in SPG 601.27.

The Information Security Coordinator is responsible for conducting annual risk assessments of critical services. The risk assessment, along with prioritized risks and recommendations, are shared each Fall (November) with the Dean’s Office and ITSS.

The Information Security Coordinator is also responsible for maintaining our Disaster Recovery Plan (DRP), which documents our critical network and information resources.

Every security incident reported to Computing Services is acted upon with the highest priority. Each is tracked in our Computing Services Management System (CSMS). An email distribution list has been established (Ross-CSOutage) to route the detail, action steps and resolution of each security incident to all members of the appropriate technology teams. Calls are escalated to the ITCS User Advocate, Office of General Council and ITSS as appropriate.