The Princeton University Information Security Program

The information security program at Princeton University is a collaborative initiative comprised of several internal teams brought together for the purpose of proactively managing security exposures or vulnerabilities, and reactively handling incidents that may arise in Princeton's computing environment.

The purpose of the information security program is to develop, coordinate, drive, and maintain the cross-functional efforts necessary for Princeton University to effectively manage security exposures, critical vulnerabilities, or cybersecurity incidents that span Princeton's various technology platforms. The program also aims to maintain capabilities in several procedural areas, including security awareness, readiness, detection, communication, remediation, incident root cause analysis, education, and process improvement.

The need for solid cybersecurity practices is necessary due to the inherent threats in using networked information systems and the Internet. These threats or vulnerabilities continue to manifest themselves among enterprises of all sizes through the actions of software vendors, hackers, disgruntled insiders, and witting or unwitting employees. The program therefore includes management and procedural guidelines, policies, and training and awareness opportunities to assist staff in recognizing, identifying, and coordinating an appropriate response to attacks on Princeton University information assets.

Documentation and procedures are also an integral piece of the program, designed to reduce overall security event exposure for Princeton University, initiate a more effective and efficient incident response, decrease total time to incident resolution, outline basic regulatory responsibilities, and promote the ethical obligations surrounding the handling of sensitive data or personal information.

It is the mission of the Incident Response Team (IRT), a keystone of the program, to provide for the coordination of the response and investigation of attacks on Princeton University information assets. The IRT also provides guidance on detecting, containing, and recovering from computer security incidents. Coordinated by the Information Security Office, the IRT is responsible for managing responses to computer security events throughout the Princeton infrastructure, including third-party-hosted systems. The degree of involvement of IRT personnel in an event is dependent upon the event's severity or potential impact to University operations.

Princeton's cybersecurity program, therefore, is truly a collection of University-wide competencies, bringing together the arrays of expertise necessary to effectively manage security exposures, technology vulnerabilities, threats, suspicious activity, and computer incidents that threaten its environment.

The remainder of this document outlines the necessary components of an effective cybersecurity program. Technologists, managers, and business staff who have either a responsibility or an affinity for security are encouraged to adapt the following practices.
Introduction to Cybersecurity: Key Ingredients of an Effective Program

The majority of planning and response activities of an effective cybersecurity program revolve around a security lifecycle model. Princeton utilizes the recognized standard of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. This framework represents the key elements that should be factored into all security planning and response activities:

Security Awareness

Any major enterprise that relies on heavy use of technology must stay aware of the vulnerabilities and emerging threats associated with those technologies. Protective techniques and safeguards must be consistently reviewed and updated using outside sources, vendors, partners, and other alliances that provide information about new technology threats.

In addition, all members of the community must be made aware of threats and practices via methods relevant to them. Princeton has established and maintains a comprehensive and expansive security awareness program.

Readiness

Whether one's responsibilities are technological, operational, or professional, staff must understand clearly the security concerns that may exist within their realm of responsibility. Staff should be familiar with University policy, Office of Information Technology and Information Security Office policy, and the inherent security risks or responsibilities that exist within their job role. People, systems, policies, and processes need to remain organized to make the University computing environment suitable for effective management of threats.
Detection

As a major computing enterprise, OIT must operate an array of monitoring systems suitable for the environment. Intrusion detection, monitoring of standard configurations, and early warnings of abnormal activity must be properly maintained to ensure that adverse events can be acted upon quickly.

Communication

Effective communication among technology staff, professional staff, academic departments, strategic vendors, and sometimes the external community is critical when handling security incidents. Information must be communicated clearly and accurately to affected areas about any developing security crisis and the active management of an ongoing incident. Sound communications plans allow for the expedient gathering of resources when emergency efforts are needed. It is also imperative that internal Princeton technical and professional teams work together when wider communications to the University community is necessary.

Remediation, Mitigation, Eradication, Containment and Control

In the event of a cybersecurity incident, prompt remediation of the situation includes one or more of the following actions: stopping the attack, applying vendor software patches, implementing creative solutions to eliminate the risk, or containing and controlling a propagation-based malware threat. Whatever the situation, plans and scenarios need to be discussed to ensure that short-term effective strategies can be implemented quickly to contain a problem.

Root Cause Analysis

Identification of a problem's root cause is essential to making sure the same incident does not recur. Root cause analysis is also important for regulatory reporting requirements which may be necessary in some cases. Whatever exercises are necessary, teams must work to facilitate the analysis necessary to determine problem causes. Such exercises include forensic investigations where appropriate.

Education and Process Improvement

Teams must study the root causes of incidents and how they are handled. Process improvement and implementation of lessons learned is essential to grow cybersecurity defense capabilities. After studying incidents and the effectiveness of response to them, team must work to implement new processes as necessary to ensure better protection in the future.