The Princeton University Information Security Program

Overview

The information security program at Princeton University (the "Program") is a collaborative initiative comprised of several internal teams brought together for the purpose of insuring the security, integrity and confidentiality of University information and protecting such information against unauthorized access or use. The Program operates within the framework of Princeton University's policies and procedures, including Rights, Rules, Responsibilities, the Information Security Policy and the Acceptable Use Policy. Princeton University's Chief Information Security Officer, who heads the Information Security Office (ISO), is responsible for coordinating and overseeing the Program.

The purpose of the 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 University's various technology platforms. The Program aims to maintain capabilities in several procedural areas, including security awareness, readiness, detection, communication, remediation, incident root cause analysis, education, and process improvement. It also addresses the proactive management of security exposures or vulnerabilities, and reactive handling of cybersecurity incidents that may arise in Princeton's computing environment. The 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.

.

Risk Identification and Assessment

The need for solid information security 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 service providers, hackers, staff and other users of University information systems. The Program therefore includes risk assessments, 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. Periodic risk assessments are performed by the ISO to identify risks to University information, devices and systems.

Employee Training and Management

The ISO offers training to employees and organizes awareness raising events to help minimize risk and safeguard Princeton University information. The ISO also offers position papers, tips and other resources on its website (https://informationsecurity/princeton.edu) to inform and equip staff and other users of University information systems on best security practices.

Information Systems

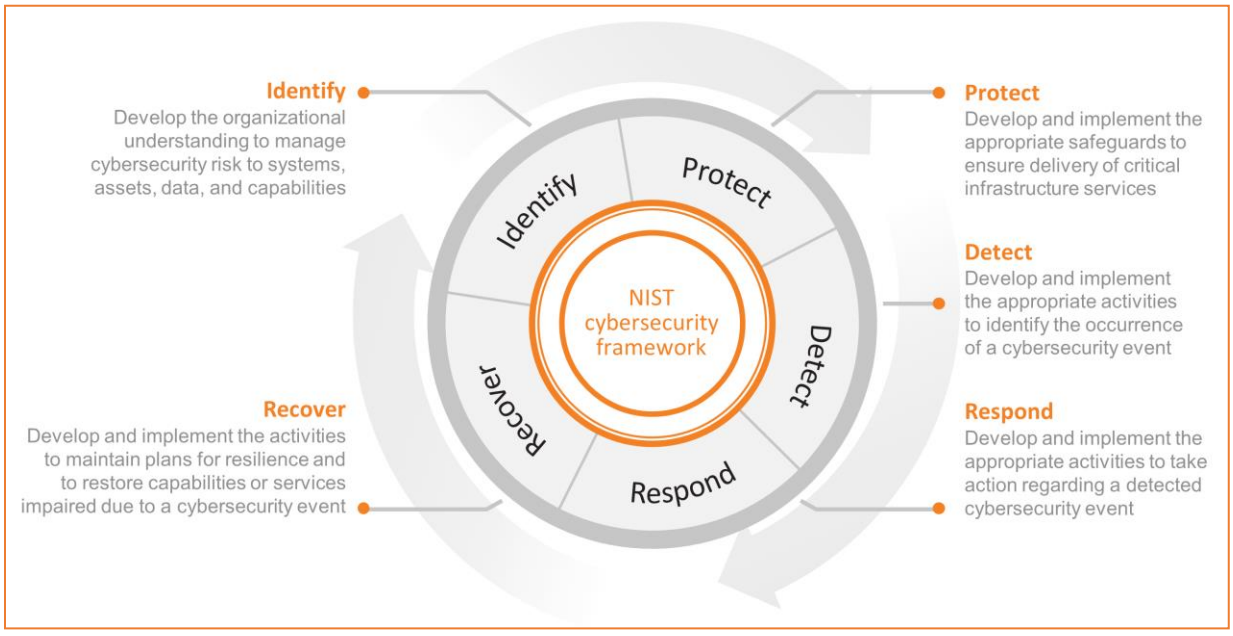
Under the Information Security Policy, Princeton University information is categorized into one of four classification levels. The classification level determines the security protections that must be used for the information. Princeton University has physical and technical safeguards to protect its information systems based on the classification level of the information stored in these systems.

Incident Response

It is the mission of the Data Breach Investigation and 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 ISO, the IRT is responsible for managing responses to computer security events throughout the Princeton University 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.

Information Safeguards

The majority of planning and response activities of an effective cybersecurity program revolve around a security lifecycle model. Princeton University 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. Therefore, Princeton University 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 policies, including policies relating to information security, 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.

Documentation and Procedures

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.

Detection

As a major computing enterprise, Princeton University operates an array of monitoring systems suitable for the environment. Intrusion detection, monitoring of standard configurations, and early warnings of abnormal activity are 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. Princeton University's 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 work to facilitate the analysis necessary to determine problem causes. Such exercises include forensic investigations where appropriate.

Education and Process Improvement

Teams 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, teams work to implement new processes as necessary to ensure better protection in the future.

Oversight of Service Providers

The Program ensures service providers implement and maintain appropriate safeguards with respect to Princeton University information. The ISO identifies service providers who are required to go through Architecture and Security Review (ASR). Among other things, ASR reviews vendors to ensure their products and services are compatible with the University's information technology and security principles. The ASR also works with the Office of the General Counsel and other offices, as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of confidential data.

Continuing Evaluation and Adjustment

The Program is subject to periodic review and adjustment. The Chief Information Security Officer, in consultation with appropriate offices, is responsible for evaluating and adjusting the Program, as well as any material changes to Princeton University's operations or other circumstances that may have a material impact on the Program.