NIST
Cybersecurity Framework Success Story
University of Pittsburgh Information Technology

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.

"We're really happy with the NIST Cybersecurity Framework. Using NIST 800-171 assessments eases the grant proposal and submittal process – allowing us to focus on our passion for research."

- Jonathan C. Silverstein, MD, MS, FACS, FACMI, Chief Research Informatics Officer, Department of Biomedical Informatics, University of Pittsburgh School of Medicine

Benefits from Using the Framework:

- **As part of the University's implementation of the NIST Cybersecurity Framework**, an organization-wide security assessment resulted in a **prioritized data security mitigation and remediation plan** – which became **a launch point for an ongoing dialogue** on a more holistic approach to security issues in general.
- **Consistent data management standards across a decentralized environment**: Utilizing the Framework, as well as NIST 800-171, provides all schools and departments – across the University—with the tools needed to meet shared security goals.
- **Compliance with multiple standards**: Adopting NIST 800-171 as the superseding standard—a decision made during a Framework implementation pilot—eliminates the need for further data management changes ahead of the Department of Education's 2019 student financial aid audits; it also meets other standards required elsewhere in the University.

Situation

- The University of Pittsburgh – with 5,400 faculty members serving 16 schools on five campuses and close ties to the University of Pittsburgh Medical Center – ranks in the very top cluster of U.S. public research universities. The decentralized nature of cybersecurity management made it challenging for the University's central IT organization to understand and manage multiple cybersecurity risk efforts and plans.
- The University receives hundreds of millions of dollars in government funding each year – from student financial aid, to a wide variety of competitive grants for faculty research in science and engineering – resulting in varying compliance requirements from multiple federal agencies.
  As a result, varying standards and a mixture of approaches for information security are used across the University; coordination has been difficult.
- Departments, faculty, and researchers store multiple classifications of sensitive data. They include controlled unclassified information (CUI), personally-identifiable information (PII), personal health information (PHI), student education records, intellectual property, and other data that have legal, regulatory, or contractual requirements for protection.
- This combination of regulatory requirements and good business practices increases the need for a standardized way to meet security requirements in an agile, decentralized IT environment.
- The University's initial use of the Cybersecurity Framework provided the organization with better knowledge and perspective about its management of cybersecurity risks and identified multiple opportunities for better coordination of its cybersecurity approaches, investments, and priority needs.

Drivers

- The need to meet cybersecurity needs associated with managing federal grant recipients while alleviating complexity.
- The U.S. Department of Education's yearly auditing to NIST 800-171 compliance for student financial aid was projected to start in 2019.
- A sense of duty to ensure the University holds all student, research, and healthcare records within reasonable protections, policies, and procedures.
- Recognizing the value and advantage of the voluntary Cybersecurity Framework and the need to comply with NIST 800-171 in some situations, the University decided that adopting both as standard practice across the institution will ensure that its information is more secure, while also demonstrating compliance.

Process

Pitt Information Technology initiated a three-step hybrid approach, which builds an environment for those needing NIST 800-171 compliance and fits within the Cybersecurity Framework, as the basis for all risk assessment across the University.

Step 1: Two-Part Risk Assessment
All departments within the University completed an exploratory questionnaire to identify where each stores data and determine if they have sensitive data.

Step 2: Mitigation Plan
A plan was put in place to Identify existing mitigations, prioritize gaps using standard risk management methodology, develop a mitigation and remediation plan – outlining a priority listing, timeline, costs, and resources, and finally to begin work on and track the mitigation actions.

Step 3: Periodic NIST 800-171 Assessments

University of Pittsburgh Information Technology Framework Implementation Overview

- Diverse decentralized organization with approximately 35,000 students, faculty, and staff.
- Determined current cybersecurity capabilities at the Framework Subcategory level in narrative format.

Results and Impacts

- The common approach has streamlined documentation and allows all units in the University to demonstrate that they are complying with requirements.
- There is increased awareness and a broader view of security risks and compliance issues across the University, resulting in units proactively seeking security support from the Information Technology department on issues broader than federal grant management requirements.
- Many previously reluctant units are now looking to centralize security and other infrastructure items through the Information Technology department, allowing each unit's internal IT staff to focus on unique business needs.

Lessons Learned

- Departments that did not embrace the initial pilot Information Technology risk assessment process due to its complexity would welcome a process organized along the lines of the Cybersecurity Framework and NIST 800-171.
- Adopting specific guidelines like NIST 800-171 could actually make requirements for compliance easier to communicate and more widely accepted.

What's Next

- Standardize risk assessment as part of the procedure for all future data use requests.
- As more units source security responsibilities to central Information Technology, central IT will gain visibility for better monitoring, identifying, and responding to potential incidents – and units will be more likely to use servers hosted at the Network Operations Center or remote desktop management provided by Information Technology.
- The University will continue to rely on the Cybersecurity Framework as well as 800-171.

Contact Information & Resources

University of Pittsburgh Office of the CIO:
technology.pitt.edu/about-us/office-of-the-cio

University of Pittsburgh IT Security website:
technology.pitt.edu/security

Cybersecurity Framework website:
https://www.nist.gov/cyberframework

NIST contact: cyberframework@nist.gov