University of Chicago Biological Sciences Division

Cybersecurity Framework Success Story

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.

"There are many security frameworks, but we found that the Cybersecurity Framework was well-aligned with our main objective, which was to establish a common language for communicating cybersecurity risks across the Division,"

- Plamen Martinov, BSD CISO

Benefits from Using the Framework:

- **Aligned security risk expectations** across all 23 departments through a risk register aligned to the Cybersecurity Framework Subcategories.
- Identified security requirements as a **common set of target outcomes**, while enabling departments to define the approach for achieving the outcome.
- **Prioritized security goals** across the division within a resourced roadmap outlining gap-closing activities.

Situation

- The Biological Sciences Division (BSD) of the University of Chicago (UoC) implemented the NIST Cybersecurity Framework to help define a consistent, risk-informed, cybersecurity program across all of its 23 departments.
- BSD has been a leader in science and research since UoC was founded in 1890. With over 5,000 faculty and staff, it is one of the largest divisions within the university. BSD supports basic research, clinical research, education, and patient care.
- BSD supports an array of information technology resources that enable faculty, staff and students to advance their research and education. This support is supplied through a decentralized model using local Information Technology (IT) staff, hired to fulfill specific departments' technology needs.
- BSD's model provides departments with the agility to support research projects with unique IT requirements. However, autonomous IT resources within departments, each with its own management and governance processes, results in security challenges:
  - risks due to inconsistent applications of security controls and gaps in security controls across departments;
  - increased spending on security; and,
  - duplication of effort.

Drivers

- BSD is required to implement and comply with many cybersecurity requirements and regulations including HIPAA, FedRAMP, and many unique security requirements mandated through federal grants received by the university.
- The challenge of implementing the multiple security requirements is magnified due to the decentralized nature of the division. While that enables each department to operate independently to meet research and clinical practice goals, the decentralization also causes challenges when defining and aligning cybersecurity objectives.
- The Cybersecurity Framework was selected by BSD because it affords the opportunity to implement one cybersecurity program by defining a current state profile that can be reported to all regulators and compliance teams to demonstrate how the division is currently achieving the security requirements.
- The roadmap developed by the team of cybersecurity consultants assisting BSD in implementing the Cybersecurity Framework provides a mechanism for informing regulators when and how the division will achieve its target state goals.

Process

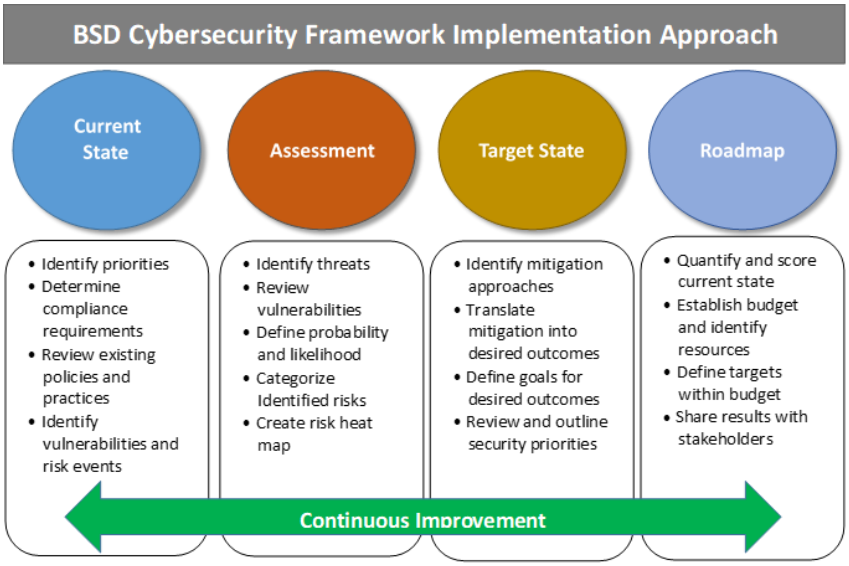
- BSD and its consultants established a team of cybersecurity engineers, Framework subject matter experts, and BSD security analysts to implement the Framework.
- The team used a combination of risk management and Framework guiding principles to develop four distinct states that would guide the implementation of the Framework. The four phases, which leveraged all seven implementation steps defined by the Framework, were Current State, Assessment, Target State, and Roadmap.

UoC Biological Sciences Division

CYBERSECURITY FRAMEWORK SUCCESS STORY

Process (cont.)

- During Stage 1, the team reviewed existing policies and practices to define the current state of BSD's cybersecurity program.
- In Stage 2, the team conducted an in-depth risk assessment across all departments within BSD.
- The team used the risk thresholds defined in stage 2 to define the target state for BSD's cybersecurity program in Stage 3. The target state aligned the required policies, procedures, and practices to the Framework subcategories to define a robust cybersecurity program.
- The Framework Implementation team concluded the project in Step 4 by developing a prioritized roadmap that outlined the activities required for the departments within BSD to achieve the target state.



UoC BSD Framework Implementation Overview

- Established a four-phase process for implementing the Cybersecurity Framework
- Enabled harmonization of cybersecurity goals and expectations across 23 departments
- Target State Profile provides clear guidance and communications for managers, faculty, and staff
- Aligned target state objectives to the Framework Core and the security risks they mitigate
- Establishing a Target State Profile enabled BSD to align automation capabilities with those areas providing greatest value

Results and Impacts

Following successful implementation of the voluntary Cybersecurity Framework, the implementation team used ISO 15504 to assign values to the gaps within BSD's cybersecurity program. The team assigned a value from 0 – 4, Not Started to Fully Achieved, to measure the gap between the current and target states. Next the team developed a self-assessment tool to help departments measure their progress as they completed projects within the roadmap. A radar chart was used to track progress across each department and the division as a whole. The radar chart was effectively used to brief the status of cybersecurity improvement activities to the leadership team within the division.

After implementing the Framework, BSD educated all users on the security program within BSD and continually monitored improvements in the program. Several key initiatives were implemented to implement enterprise wide cybersecurity capabilities to assist the departments in meeting their target state goals.

What's Next

BSD remains committed to the common language established within the Framework for describing aspects within their cybersecurity program. BSD is aligning existing cybersecurity policies to the Framework and implementing process for continual review to ensure the Target State Profile remains correct.

Contact Information & Resources

UoC Biological Science Division website:
http://security.bsd.uchicago.edu/

BSD Contact: Plamen Martinov (pmartinov@bsd.uchicago.edu)

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

NIST contact: cyberframework@nist.gov