Applying the Cybersecurity Framework at the University of Chicago – An Education Case Study

The Biological Sciences Division of the University of Chicago is pleased to share the following use case as a helpful resource to aid other organizations in applying the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Background

Since the University of Chicago was founded in 1890 by John D. Rockefeller, the institution has been a leader in science and research. The Biological Sciences Division (BSD), with 5,000 faculty and staff in 23 departments, is the largest division of the university. These departments support basic research, clinical research, education, and patient care led by award-winning faculty. These functions, including groundbreaking discoveries in fields such as cancer research and advanced genomics, are enabled by an array of information technology resources.

In 2014, the BSD appointed Plamen Martinov as the Chief Information Security Officer to institute an information security program that enables and protects the research and academic functions of the division. After evaluating various security frameworks, Plamen Martinov, working together with Robert Grossman, the BSD's Chief Research Informatics Officer (CRIO), selected the U.S. Framework for Improving Critical Infrastructure Cybersecurity (aka Cybersecurity Framework) for organizing and implementing the new information security program. The implementation efforts of the Cybersecurity Framework were supported by G2, Inc., a cybersecurity service provider. As the primary contractor support for the National Institute of Standards and Technology's (NIST) Computer Security Division, G2 played a major role in the development and deployment of the Cybersecurity Framework.

The Challenge

The 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 staff, hired to fulfill specific departments' technology needs. This model provides departments with the agility to support research projects with unique Information Technology requirements. However, autonomous Information Technology resources within departments, each with its own management and governance processes, results in the following security challenges:

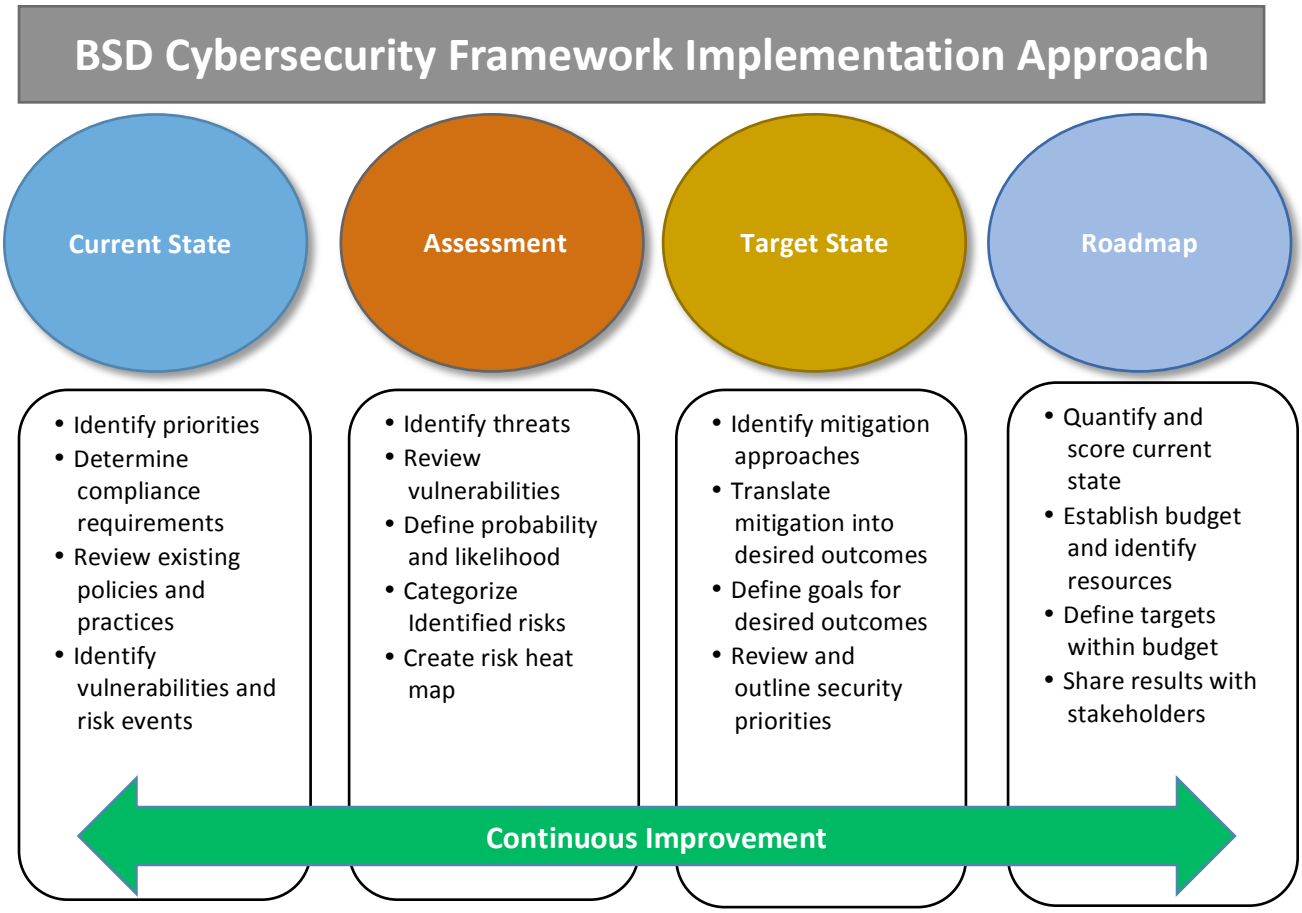
- risks due to inconsistent applications of security controls;
- risks due to gaps in security controls across departments;
- increase in spending on security; and,
- duplication of effort.

To address the growing cybersecurity threats in a cost-effective and programmatic manner, the BSD selected 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,” explains Plamen Martinov.

Approach

The BSD established a group of G2 Subject Matter Experts and BSD Security Analysts, referred to as “the team.” The team used a combination of risk management and Framework guiding principles to develop four distinct stages that would guide the implementation,: Current State, Assessment, Target State, and Roadmap. Each of the stages is described below.



Stage 1: Current State

The implementation team first started with interviews of key stakeholders to determine what processes were previously applied to achieve the outcomes in the Framework Core, including requirements for compliance with various laws, regulations, and service agreements. To ensure a broad understanding of

the needs, the team met with Information Technology (IT) staff, business managers and executive leadership.

The interviews with management provided an understanding of the priorities of individual departments. These priorities included: current and planned security activities across the BSD, requirements for sharing research information remotely, and the need to support faculty activities in day-to-day research and education. This information was used to drive subsequent risk and resource discussions and decisions.

The team used a customized Current Profile template developed by G2 to create an internal management tool that documents existing policies, tools in use, and examples of good BSD practices. This information established the BSD's Cybersecurity Framework Current Profile. The team performed a comprehensive review of the current profile to identify potential vulnerabilities. Events were recorded and formed the basis for a Risk Assessment, described in the next section.

Stage 2: Risk Assessment

The team considered several hundred vulnerabilities that resulted from profile development, and subsequently identified a set of unique threats that could conceivably impact operations. Following the NIST Special Publication 800-30, *Guide for Conducting Risk Assessments,* the team determined the likelihood and potential impact of each risk. The risk analysis focused not only on technology, but also on potential risks and the impact upon people and related processes. The risk events were aggregated into points of commonality, creating a comprehensive register of risk categories (e.g. financial, operational, and strategic). The combined risk categories were plotted on a Heat Map, as seen in Figure 1. The heat map provided a holistic view of exposure and identified fundamental risk drivers used in the Target State Stage, described in the subsequent section.

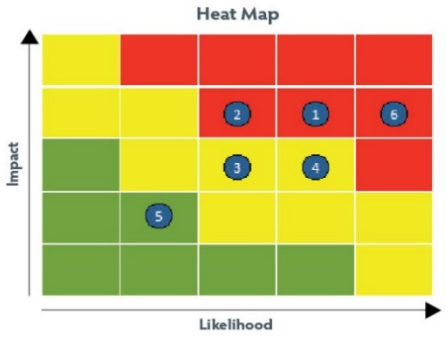


Figure 1: Assessment Heat Map

Stage 3: Target State

The team determined high-level approaches to mitigate each of the documented risks, paying particular attention to events that exhibited both high likelihood and high impact. To define how cyber outcomes would be accomplished, the BSD selected a Cybersecurity Framework Implementation Tier. In order to integrate existing processes and information sharing activities into the cybersecurity program the team translated the risk mitigation approaches into desired outcomes, using the Target State Profile categories and subcategories as a guide. The combination of these activities established the BSD's Cybersecurity Framework Target Profile. A final review was performed to ensure the outcomes were consistent with the characteristics of the selected Cybersecurity Framework Implementation Tier and would achieve the desired security objectives in a cost-effective manner.

Stage 4: Roadmap

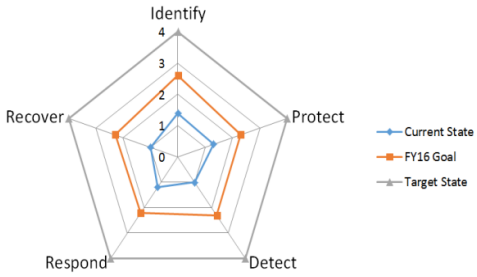


Figure 2: Roadmap Radar Chart

With the profiles defined, the BSD gained a good understanding of its existing state and what outcomes would adequately mitigate known risks. Using this information, a rating scale from 0 to 4 (derived from ISO 15504) was used to quantify the current state and to establish a baseline. Next, goals were determined based on the operational budget, resources, and competing priorities. These goals were plotted on top of the current state in the example radar chart to the right (Figure 2); this determination assisted us in establishing practical targets within a manageable budget.

Continuous Improvement

To drive continuous improvement and track progress with security initiatives for departments, the team developed the Framework Assessment Collaboration Tool (FACT). The tool provides information for periodic self-assessment by departments, supporting questionnaires regarding current and planned activities for department staff, external partners, information security processes, security tools, training systems, etc.

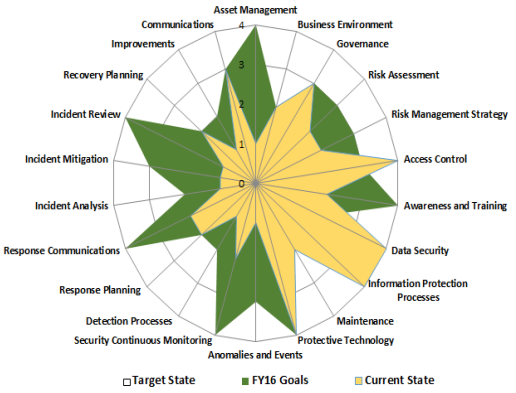


Figure 3: FACT Radar Chart

"Cybersecurity is a journey, not a destination. Making this journey successfully requires the use of consistent processes and tools," explains Plamen Martinov.

The tool provides a consolidated view of how individual departments are meeting the cybersecurity targets set for the specific fiscal year. Most importantly, the information gained is used to improve and mature the cybersecurity program in alignment with the BSD's business objectives. Ultimately, this determination ensures optimal value from the cybersecurity program by aligning expenditures with those activities that have the most impact on reducing risks to important research and education programs.

Benefits

The Cybersecurity Framework enabled the BSD to identify security requirements as a set of target outcomes to be achieved, while enabling departments to maintain internal processes and procedures regarding how to achieve those outcomes. As a result of the implementation of the Cybersecurity Framework, each department has gained an understanding of BSD's cybersecurity goals and how these may be attained in a cost-effective manner over the span of the next few years. Using the Cybersecurity Framework helped foster information sharing and good practices among departments.

Another important benefit of the Cybersecurity Framework is the ease in which it can support BSD departments with quite different cybersecurity requirements. For example, some departments are focused on basic research involving model (non-human) organisms, some departments support research using controlled access human genomic data, some work with Protected Health Information, and some require systems that must operate with FISMA Low or Moderate procedures and controls. Since the framework outcomes will be achieved through individual department activities, rather than through prescriptive and rigid steps, each department is able to tailor their approach based on their specific departmental needs.

"The Cybersecurity Framework enables us to operate biomedical data commons using FISMA Moderate procedures and controls," explains Robert Grossman, "and supports an effort within our unit to use automation to improve our information security measures."

Conclusion

The team worked to create a roadmap (illustrated in Figure 4) that addresses known risks, ensures ongoing accountability, and achieves the objectives of BSD's leadership. While we cannot guarantee that the Division is immune from attacks, this approach provides a way to organize, communicate and act upon common policies and practices.

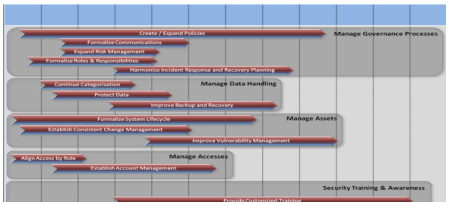


Figure 4: Multiple Year Program Roadmap

University of Chicago – Biological Sciences Division

The University of Chicago – Biological Sciences Division (BSD) encompasses a wide range of fields of inquiry spanning the basic biological sciences and clinical disciplines. BSD's basic, translational, and clinical research enterprise is characterized by a fundamental commitment to original inquiry. We provide a full spectrum of education—collegiate, graduate, medical, and postgraduate—characterized by a passionate commitment to rigorous scholarship and interdisciplinary effort.

G2, Inc.

G2 is a small business focused on addressing our nation's most challenging cybersecurity problems. Throughout G2's 15-year history, G2 has assisted the Department of Defense, Department of Commerce, and many commercial companies achieve business objectives securely. Some of G2's most notable accomplishments include assisting in the development of the Secure Content Automation Protocol (SCAP) and, most recently, assisting NIST with developing the *Framework for Improving Critical Infrastructure Cybersecurity* – the Cybersecurity Framework.