University of Kansas Medical Center

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.

Benefits from Using the Framework:

The Baldrige Cybersecurity Excellence Builder (BCEB) effectively complements KUMC's use of the NIST Cybersecurity Framework (CSF). The BCEB has allowed us to focus on and address the process and delivery side of our Information Security Program and related offerings. In contrast, the CSF allows us to focus on the more technical elements and ensuring that we have the necessary controls deployed within our organization. The BCEB has enabled us to bridge this gap and implement what is necessary in the CSF. The immediate outcomes of our work with the BCEB were:

- An honest assessment of where we are and where we want to be, as well as a baseline to measure against in the future.
- A new, business-oriented language to use in communicating with and working with partners and customers.
- A boost in clarity, empowerment, and morale for the Information Security team.
- A paradigm shift – a major change in how we think about and approach our work – that continues to evolve.
- A path forward!

Situation

The University of Kansas Medical Center (KUMC), an Academic Health Center in Kansas City, Kansas (with ~ 3,600 employees and ~3,500 students) has a complex operating environment that places many demands on IT and Information Security.

KUMC's Office of Information Security (OIS) is a relatively new department that formerly existed as a subunit of the IT Department. With the establishment of the OIS, we started with a CSF-based self-assessment, and this resulted in the identification of strategic gaps. This became our baseline and a common reference point to discuss our current state and demonstrate our continued progress for program development and control implementation. At present, the OIS program is in the early developmental stage in terms of overall maturity.

In support of KUMC's mission and vision, the Information Security Team strives to:

- Optimize access to and use of information to enhance the experiences of students, educators, researchers, physicians, staff, and patients, while doing so safely and securely.
- Develop and implement innovative security practices that are nation-leading in terms of advancing the tripartite mission of a leading academic health center.
- Balance information security with usability, privacy, and resource constraints.
- Succeed together through strong partnerships, customer focus, and collaboration.

"The Information Security team at the University of Kansas Medical Center is using the Baldrige Cybersecurity Excellence Builder as a framework for self-assessment and program development. The BCEB is a powerful tool, especially when used in conjunction with the NIST Cybersecurity Framework. I don't think that it's overly dramatic to say that we're going to transform our Information Security Program through this process."

Steffani Webb, Vice Chancellor for Administration

Drivers

On the heels of the newly formed OIS and combined with the gaps identified from the CSF analysis, we launched a self-assessment and improvement initiative using the BCEB in order to:

- Help with program development for our new OIS.
- Address a wide variety of specific and serious challenges identified in recent audits that highlighted the need for us to align polices, processes, and resources to support Information Security.
- Enable the technically focused Information Security team to better understand "the business" that we are serving and supporting and have a common language to use in continuing the conversation with business units.
- Foster a strong customer focus within the Information Security team.
- Contribute to the Information Security community.

Process

- In May 2017, the Executive Vice Chancellor, Vice Chancellor for Administration, and Associate Vice Chancellor for Organizational Improvement held a kickoff meeting with the Information Security Team to set the stage and emphasize the importance of Information Security to our organization. The team was assured at the outset that this wasn't a test or a "gotcha" exercise and that this would be enjoyable and worthwhile.
- The Information Security team and Vice Chancellor for Administration met for two hours weekly over six months to respond to the questions in the BCEB. We started first by answering the questions in the Organizational Context Section and then working through the self-assessment questions in Categories 1-7. The Associate Vice Chancellor for Organizational Improvement facilitated these weekly sessions, leading the team through the questions and capturing the answers.
- We also developed a conceptual crosswalk to the NIST Cybersecurity Framework (CSF), using those standards as a complementary resource for cybersecurity.

KUMC

CYBERSECURITY FRAMEWORK SUCCESS STORY

Process (cont.)

- A self-assessment document was prepared by the Associate Vice Chancellor for Organizational Improvement at the end of this process. This is a living document that we will periodically revisit, add to, and adjust as we progress through cycles of learning and improvement and as we see results.

Results and Impacts

Using the BCEB yielded benefits right away. For example,

- Previously, being an Information Security staff member meant frequently "saying no" to other employees in order to protect information. Their focus has now changed from primarily operating as a team that 'tells' others what to do, to one that 'asks' for their help in achieving their mission. This approach has helped the team to achieve deeper levels of trust, cooperation, understanding, and overall effectiveness.
- This process has helped the Information Security Team establish a better approach to intake, response, and follow-up. This has helped them improve stakeholder relationships and get the right solutions to their customers.

While short-term ROI has been primarily qualitative, long-term value will be more quantitative.

KUMC Framework Implementation Overview

- This process helped the team to better understand their own roles and to engage their customers (i.e., other employees within the medical center and key partners) in protecting the organization and helping to achieve the mission of the OIS.
- The gaps identified during this process have resulted in action plans, funding opportunities, and deep alignment to the business.

Lessons Learned

- This process created an awareness of how the Information Security Team fits within the context of the broader organization. The team used to believe that the burden of preventing cyber disasters as falling solely on them. Now they understand that it is a shared responsibility, including senior leadership. As a result, when they see a need to make recommendations to senior leadership to support risk management throughout the organization, they feel empowered to do so. This team now understands that they are not the "'no people"' or the "'yes people."'
- Language can be a powerful force for progress or the single element that can derail the best of projects. Information Security professionals are being required to use the language of the business more and technical language less. The way in which the BCEB is written is helpful. Since it is written in the language of the business, it allowed the Information Security team to link business language to technical requirements.
- Although the team was uneasy and skeptical at the outset, they quickly came to appreciate and enjoy the sessions. This was worth the time and effort, and we look forward to our continued journey as we evolve and refine our Information Security program.

What's Next?

Following its initial work with the BCEB, the team will:

- Review and update the assessment document, periodically and as needed.
- Continue working to address and close gaps through strategic improvements and customer education.
- Refine the results section -- in particular, deciding upon which metrics are the most important to track (and to use for comparative and benchmarking purposes).
- Make another pass through the BCEB criteria questions, this time inviting key customers and stakeholders to participate to validate the initial thoughts and to improve the understanding of customer and stakeholder needs.
- Incorporate use of the NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework (NIST Special Publication 800-181) to assist in addressing the gaps identified in responding to BCEB Category 5 questions.
- Use artifacts from our BCEB work to develop a strategic plan for the Information Security Program.
- Share with the Information Security community our use of the BCEB and how it has helped us.

Contact Information & Resources

University of Kansas Medical Center (KUMC):

https://www.kumc.edu/

KUMC contact: swebb@kumc.edu

Cybersecurity Framework:

https://www.nist.gov/cyberframework

NIST contact: cyberframework@nist.gov

KU MEDICAL CENTER

NIST National Institute of Standards and Technology U.S. Department of Commerce