NIST
Cybersecurity Framework Success Story
Saudi Aramco

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:

- Improves cybersecurity-related communication among Saudi Aramco corporate management, CISO's office, Information Technology (IT) organizations, and Operational Technology (OT) organizations.
- Enables the company to measure the cybersecurity maturity of IT and OT organizations regularly and set the desired maturity target at a corporate level.
- Provides a cybersecurity roadmap for each part of the organization and a way to monitor the progress of their short- and long-term initiatives.
- Eases adherence to national and international regulations, such as Saudi Arabia's National Cybersecurity Authority (NCA) requirements.
- Enables Saudi Aramco to conduct benchmarking with best-in-class organizations, and to learn from each other by leveraging its Operational Excellence Program.

Situation

- Saudi Aramco traces its beginnings to the Concession Agreement of 1933 between the Standard Oil Company of California and the Kingdom of Saudi Arabia, and it is a leading producer of energy and chemicals.
- A multinational company with over 70,000 employees, Saudi Aramco is represented in the three major global energy markets of Asia, Europe, and North America.
- The Operational Excellence Program is the corporate Framework to achieve and sustain excellence, by raising performance standards through continuous improvement of processes, systems, and policies.
- Multiple standards and best practices are used by IT, OT, and cybersecurity teams, with no unifying concept to prioritize initiatives and capabilities.

"To enable Saudi Aramco to weather sophisticated cyberthreats, the NIST Cybersecurity Framework for Critical Infrastructure is being adopted. Saudi Aramco has adopted this Framework to ensure the organization's overall approach to cybersecurity supports high standards of governance."
– Khalid S. AlHarbi, CISO.

Drivers

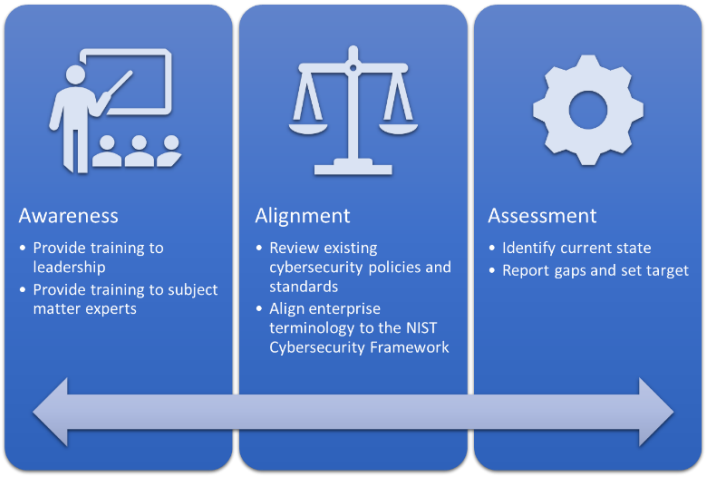
- The cybersecurity program corporate-wide utilizes multiple cybersecurity frameworks, which has introduced communication challenges among different departments.
- The desire to develop a comprehensive cybersecurity program that is aligned with local regulations, best practices, and existing practices to enable the benchmarking of cybersecurity capabilities with leading oil companies globally – and then apply it to IT and OT environments.
- The company has desired to assess the state of the overall corporate cybersecurity program and establish meaningful cybersecurity metrics and utilize the simple logic and language supplied by the NIST Cybersecurity Framework (Framework).
- Saudi Aramco has desired to prioritize the implementation of cybersecurity initiatives and capabilities based on the Framework.

Process

- A team was formed from the CISO's office to explore the best way to adopt and implement a single framework Corporate-wide that would meet its multiple cybersecurity needs.
- Once a decision was made to use the Framework, Saudi Aramco selected a consultant to expedite adaptation across the company.
- An Adaptation and Implementation Strategy was presented to corporate management for its buy-in.

Process (Continued)

- Workshops were conducted for leadership and subject matter experts, to provide an overview about the Framework.
- The Framework implementation plan was discussed with key players and stakeholders from IT and OT organizations to ensure awareness.
- The cybersecurity team analyzed and reviewed existing cybersecurity projects, policies, resources, and related processes and procedures to determine the current maturity level based on the Capability Maturity Model Integration (CMMI) and the Cybersecurity Capability Maturity Model (C2M2) for both IT and OT. This helped to identify, measure, and achieve a capability maturity level based on the organization's security risk tolerances.
- The team leveraged the CMMI's five-level maturity scale that redefines each level for cybersecurity capabilities to provide tailored recommendations and a road map for stakeholders to enhance their maturity level. The maturity level is monitored by corporate management to ensure the target level is achieved; resources and funding are allocated accordingly.
- Stakeholders' progress with implementation was continuously monitored; regular meetings were conducted with stakeholders to discuss challenges and capture good practices.
- Corporate management and stakeholders were updated regularly with reports to highlight progress and challenges.
- The CISO's office built in-house capability to perform cybersecurity maturity assessment.
- Benchmarking with the world's leading oil companies is conducted regularly to share best practices and enhance cybersecurity and IT process and capabilities.



Results & Impact

- All levels from corporate management to subject matter experts started using the same language to communicate cybersecurity.
- IT and OT proponents understand the importance of cybersecurity and address the identified gaps from the assessment phase.
- Alignment with the Framework has prepared the organization to comply with national and international regulations, and to incorporate multiple best practices and frameworks.
- The Framework was translated into Arabic to enable universities, organizations, and governments in Arab countries to stay up-to-date and informed about the cybersecurity field, and to leverage the Framework to raise their cybersecurity capabilities.

What's Next

- Conduct an annual assessment to ensure full Framework alignment and identified gaps.
- Fully automate the maturity assessment process to provide management with frequent update about corporate cybersecurity posture.
- Conduct benchmarking with best-in-class organization(s) to capture their cybersecurity best practices.
- Assist the local community to enhance their overall cybersecurity posture.
- Develop cybersecurity Key Performance Indicators that are aligned with Framework functions.

Contact Information & Resources

Saudi Aramco Website:
https://www.saudiaramco.com/
Saudi Aramco contact: Cybersecurity@aramco.com
Cybersecurity Framework Website:
https://www.nist.gov/cyberframework
NIST contact: cyberframework@nist.gov