Premera Elevates Level of Organizational Energy with HITRUST, Facilitating Communication and Collaboration

Sean Murphy, VP & CISO, Premera Blue Cross

Overview
Premera Blue Cross wanted to apply a risk-based approach to IT security that would map to its capabilities for identifying risks, protecting assets, detecting attacks, responding to breaches, and restoring systems. The organization also wanted to adopt a framework for which independent, third-party attestation was available to prove compliance with the required security standards. Premera found the answer to this challenge in the HITRUST CSF. The framework enables Premera to measure internal security control as well as the security posture of third-party business partners that handle sensitive information. IT and business units can communicate more easily enabling conversations to occur regarding the changes needed to close risk-based security gaps. Perhaps most importantly, the HITRUST CSF certification creates a mark of distinction in the eyes of customers who understand the value of a security framework that truly protects their sensitive information.

The Challenge: Go Beyond Compliance and Attest to a Valid Risk-Based Security Approach
Premera Blue Cross is the largest health plan in the Pacific Northwest. The organization serves more than two million people from individuals and families to members of Fortune 100 employer groups. As a not-for-profit, independent licensee of the Blue Cross Blue Shield Association, Premera provides healthcare services to members in Washington and Alaska—including health, life, vision, dental, stop-loss and disability programs focused on wellness, prevention, disease management and patient safety.

The entire Premera organization is committed to controlling rising medical costs while ensuring access to quality healthcare. Premera is also steadfast in protecting the personal information of members and making sure all company data remains safe from cyber attacks at all times.

Sean Murphy, the Vice President and Chief Information Security Officer for Premera, remembers the cultural shift that the organization went through with respect to IT security in 2015, shortly after he came onboard. The organization
did not have a risk-based management framework to assess the maturity level of its security programs at that point in time.

“We utilized COBIT, which is good for achieving compliance with industry regulations, but we wanted to go further,” Murphy says. “We also wanted to apply a risk-based approach that would map to our capabilities for identifying risks, protecting assets, detecting attacks, responding to breaches, and restoring systems back to normal operations when necessary.”

To achieve this vision, Murphy says Premera considered security frameworks such as NIST 800-53 and ISO 27001. But both programs lacked attestation protocols as far as utilizing independent third parties to prove that the organization met the required security standards. In addition to driving Premera’s security maturity forward, Murphy also had his eye on leveraging a framework to measure the security capabilities of the third-party business partners that handle member information.

The Solution: HITRUST CSF Integrates Major Security Frameworks

After evaluating the options, Premera determined that the HITRUST CSF is the best framework for guiding its security program and for meeting Murphy’s requirements. “HITRUST integrates the major security frameworks into one framework and provides a way to achieve independent third-party attestation,” Murphy says. “This enables us to definitively prove we meet the common body of security requirements to customers, business partners, and our Board of Directors.”

The HITRUST CSF enables organizations of any size—from small supplier businesses to large organizations—to address the challenge of complying with the multitude of federal, state and industry regulations, standards and frameworks pertaining to information security—both on-premises and in the cloud. By incorporating a risk-based approach, the HITRUST CSF provides a comprehensive and flexible framework of security controls:

- Harmonizes and cross-references globally-recognized standards, regulations and business requirements—including ISO, NIST, PCI, HIPAA and state laws.
- Scales controls according to organizational type, size and complexity.
- Provides prescriptive requirements to ensure clarity.
- Offers multiple implementation requirement levels as determined by specific risk thresholds.
- Allows for alternate control adoption when necessary.
- Evolves according to user input as well as changing industry and regulatory conditions.

By identifying the maturity level of various IT systems, the HITRUST CSF helped drive changes across the entire organization with respect to the security controls deployed and how IT manages those controls. “We can also point to the results of the attestation report to prove our security maturity when answering questions from our top-level executives,” Murphy adds. “They are very diligent about making sure we properly protect the information of our organization and our members.”

Murphy realizes that achieving a strong security posture is not a one-time effort but rather a living and breathing process that must continually evolve. During the HITRUST implementation, it was not just a matter of replacing another set of security controls; it was also an organizational, enterprise-wide endeavor. “Our control owners and our desk-level employees found that there was new information and training available on security, and they started to embrace HITRUST as a way to improve their security awareness,” Murphy points out.

Premera also made changes to system access and authorization controls and conducted a review of privileges that impacted the entire organization. The process of implementing the HITRUST CSF changed the organizational culture as to the importance of implementing a control framework.

The Results: A Culture of Security Can Be Felt Throughout the Organization

The HITRUST CSF drives change at Premera by helping people communicate and understand risk so that conversations can occur at every level of the organization on what modifications are needed to close any security gaps. Murphy particularly appreciates how the framework establishes a foundation for security controls that can endure even as Premera goes through organizational and personnel changes.

“Changes are sometimes driven by personalities—a new boss or corporate owner comes in and makes sweeping alterations,” Murphy explains. “But then the next person comes along and makes new changes that may not align with what was done. With the prescriptive nature of HITRUST, the adjustments we made in the last two years
HITRUST CSF Solution Highlights

- Maps IT security risks to capabilities for identifying risks, protecting assets, detecting attacks, responding to breaches, and restoring systems.
- Provides attestation protocols utilizing independent third parties to prove an organization meets the required security standards to customers, business partners and the Board of Directors.
- Measures internal security capabilities as well as the capabilities of third-party business partners that handle sensitive information.
- Enables IT and business units to communicate and understand risk so conversations can occur at every level of the organization on what changes are needed to close security gaps.
- Establishes a foundation for security controls that can endure even as organizational and personnel changes occur.
- Creates a mark of distinction in the eyes of customers who understand the value of a security framework that truly protects their sensitive information.

Murphy also values the flexibility that the CSF framework provides by giving Premera multiple ways to apply controls and enabling the information security team to leverage a solid framework to which it can anchor security recommendations. This way, Premera can make sure each system administrator runs their systems the same way when it comes to access, patching, and configurations.

“We all come together to figure out how best to make security controls work,” Murphy says. “We can succinctly communicate to the business units what cybersecurity controls need to be in place so they can proceed more efficiently in getting new IT services deployed onto the network or to start exchanging data with a vendor.”

“We've seen some organizations where dozens of admins might be running their systems using dozens of different processes,” Murphy says. “With HITRUST, each admin has one way of providing security. Our organization welcomed this; it gave us the ability to guide the control owners on how things should be done. We also created procedures on how to run a system that align with other system admins rather than everyone doing it their own way. We build-in security from the beginning rather than bolting it on at the end in ad hoc fashion.”
Premera also came up with creative ways to promote the implementation of the HITRUST CSF program. “We are a very social organization,” Murphy reveals. “We used posters and displays roped off by stanchions to help motivate the company and communicate the value of HITRUST. We also held brown-bag seminars and even handed out baseball caps for each corrective action program—with our logo and the HITRUST logo. This approach helped create a lot of buy-in and a sense of energy in implementing the program.”

**Certification Creates Mark of Distinction in the Eyes of Members**

Murphy emphasizes how the HITRUST CSF helps with cybersecurity collaboration. “You can communicate succinctly what the requirements are in order to get a service onto the network or to work with a vendor,” Murphy says. “Non-technical people can understand the requirements and see they are not rooted in opinion; they’re the right thing to do based on the framework. The earlier security is embedded into the process, the better that process will be. It’s a transparent, honest conversation.”

Murphy adds that giving security and non-technical people an easier way to communicate is a key benefit: “There’s a natural tension between security requirements and business requirements. If you go too fast, you can risk the protection of the information. For example, when we decided to micro-segment our network, the HITRUST CSF helped communicate why this was important from a security standpoint. It was not just an IT idea—it was rooted in NIST and ISO standards and demonstrated why it was the right thing to do.”

While it’s still not easy to balance business and security requirements when implementing a new service, such as moving an application service to the cloud, it’s easier with the CSF because there’s a framework to underpin what’s needed, why it’s needed, and how to employ the required controls. The IT team at Premera can thus have a conversation with the business, and the business is supportive of what IT needs to do. This helps business initiatives move forward while making sure data remains secure.

“Our members gravitate toward the idea that we are HITRUST certified,” Murphy says. “They understand the HITRUST brand and what certification means. Knowing that our members value the HITRUST CSF mark of distinction provides great value to us in our efforts to promote our brand.”