HITRUST

CASE STUDY: CRANEWARE AND THE HITRUST CSF AND MYCSF

Craneware Leverages HITRUST to Strengthen Security Posture and Accelerate Process to Demonstrate GDPR Compliance to Customers and Regulators

The Challenge: Streamlining the Process for Demonstrating Strong Security

Based in Scotland, with U.S. headquarters in Atlanta, Craneware (AIM: CRW.L) provides automated value cycle solutions—collaborating with U.S. healthcare providers to plan, execute, and monitor value-based economic performance.

Craneware faces two primary challenges in demonstrating its security posture. Each hospital customer has its own criteria for measuring security, which often involves asking Craneware to fill out an extensive security questionnaire. Craneware also has to comply with many regulations, ranging from HIPAA to GDPR, and the myriad of state regulations beginning to emerge in the U.S. Some customers also require compliance with SOC 2 and a report to show how Craneware stacks up against the NIST Cybersecurity Framework.

Craneware solutions simplify the complexities of medical coding by ensuring hospitals' insurance claims accurately reflect correct diagnoses and treatment codes along with all the necessary supporting details to expedite claim payments and speed up revenue cycles. "We help identify potential issues related to claims data so hospitals can generate the revenue they are entitled to and accelerate cash flow," says Craneware Special Projects Consultant Donna Nodson, who works with IT to mitigate Craneware risk and compliance needs while also overseeing data privacy audit activities. "This helps our customers operate more profitably and manage claims more efficiently, whilst having confidence that their data remains protected."

Another key mission for Craneware is to protect data just as rigorously as customers do, as mandated by HIPAA for Business Associates that provide services to healthcare Covered Entities.

Craneware

This HITRUST case study examines how Craneware utilized the HITRUST CSF® and the HITRUST MyCSF® portal to deploy a strong security posture to protect customer data in compliance with industry and regulatory standards. The portal provides the framework and tools that give Craneware an effective way to evaluate security controls, identify any gaps in their security defenses, and comply with regulations such as GDPR. By achieving HITRUST CSF Certification, Craneware gained the ability to quickly demonstrate its security posture to customers and regulators. Achieving HITRUST certification has also helped communicate the importance of security across the organization—not only for Craneware's IT assets, but also for customer data.

Headquarters: Edinburgh, United Kingdom
Number of Employees: over 350
Industry: healthcare technology

"We have to be just as concerned about the security of sensitive data as our healthcare customers and partners," says Nodson.

While Craneware offers customers the option of deploying its technology on-premises, the company also offers solutions in the cloud. Nodson focuses her efforts on making sure the company deploys a universally robust security program to protect customer data in compliance with industry and regulatory standards.

The Craneware senior executive team also recognizes the need for HITRUST CSF Certification for companies that operate applications for customers in the cloud. "We recognized that, as we built out the Trisus product line with our value cycle vision, we were moving to processing and handling much more PHI in new ways. Craneware needed to make sure best practice technologies and processes were in use and we had a framework to monitor and measure that," says CIO Derek Paterson. "We already had SOC1 and SOC2 but felt they didn't go far enough. Whilst NIST and ISO27001 would cover those frameworks, they were not sufficiently tied to healthcare and our particular challenges."

The HITRUST CSF also helps Craneware address the challenge of making sure its cloud environment complies with all regulations pertaining to information security. The MyCSF portal supports the trusted framework that affords Craneware the ability to demonstrate security health in the cloud.

The Solution: HITRUST Framework and Building Blocks Quickly Identify Security Gaps

Craneware found the answer to the challenge of efficiently demonstrating compliance by leveraging the HITRUST CSF. "The framework gives us an efficient way to evaluate our security controls and identify any gaps that we may need to address," Nodson says. "And by achieving HITRUST CSF Certification, we gained the ability to efficiently demonstrate our security to anyone who needs to know—whether it's a customer or a regulator."

In addition to the HITRUST CSF, Nodson also utilizes the HITRUST MyCSF portal to compare how Craneware security controls match up to various regulations and standards.

"With this information, I can provide guidance to our Engineering teams and IT on which gaps we need to close first," Nodson says. "This helps us work more efficiently and prioritize the areas we are most concerned about. It is especially helpful when analyzing the privacy regulations for a particular U.S. state in which we have a significant customer base."

Security Attestation Validates Cybersecurity Resilience

Incorporating a risk-based approach across all critical systems, the HITRUST CSF provides Craneware with a comprehensive and flexible framework for security controls assessment and reporting by:

- Covering global standards, regulations, and business requirements—including ISO, NIST, PCI DSS, GDPR, SOC 2, HIPAA, and state laws;
- Scaling the controls according to organizational type, size, and complexity;
- Providing prescriptive requirements to ensure clarity;
- Offering multiple implementation requirement levels as determined by risk thresholds;
- Allowing for alternate control adoption when necessary; and
- Evolving according to user input as well as changing industry and regulatory conditions.

What gives HITRUST CSF Certification true credibility is that evaluation is conducted by Authorized HITRUST External Assessors, and then HITRUST validates the results. With two independent organizations confirming security measures, customers can be confident Craneware has achieved a consistent and high level of maturity in cybersecurity resilience.

"HITRUST MyCSF portal offers many resources to help connect controls with evidence; there is also a range of reporting options," Nodson says. "I found it very helpful to attend the HITRUST conference and learn additional techniques and instruction on how to use the portal and maximize our HITRUST investment. Talking with other organizations about their HITRUST journey was invaluable."

The HITRUST CSF makes it easy and cost-effective for Craneware to manage information risk and comply with privacy and security regulations. Craneware can also leverage the HITRUST MyCSF portal to make sure its evolving assessment needs align with risk management efforts as the landscape changes in relation to cyber threats, information risk, and global regulations.

The Results: The Strongest Security Posture Anywhere

Craneware's investment in HITRUST CSF Certification results in great credibility and it demonstrates that their security posture is comprehensive, meeting and exceeding strict legislative and industry requirements. HITRUST CSF Certification proves to third-party vendors and other stakeholders that you have taken the necessary steps in mitigating risk and safeguarding data at the highest levels.

"One of our customers told us how happy they were that we were HITRUST certified," Nodson reveals. "She said we made her job a lot easier."

HITRUST CSF Highlights

- Protects PHI, PII, and digital assets from cyber-criminals
- Proves attestation to regulations pertaining to sensitive information and digital assets
- Generates one report that demonstrates to all customers that their data is secure
- Reduces the cost and time spent by IT on compliance audits requested by customers
- Provides a framework to measure the security and compliance postures of partners
- Raises the level of awareness of security and compliance importance across the company

HITRUST MyCSF Highlights

- Best-in-class software as a service information risk management platform for assessing and reporting information risk and compliance
- Makes it easy and cost-effective for an organization to manage information risk and meet international, federal, and state regulations concerning privacy and security
- Reduces overall assessment management costs
- Provides continuous visibility of risk posture
- Features are built to streamline and simplify your organization's risk assessment needs

Nodson also points out the added benefit of how HITRUST CSF Certification allows Craneware to sync with the mission of the Provider Third-Party Risk Management Council. This council, founded by hospital security officers, requires third-party vendors to obtain HITRUST CSF Certification in order to conduct business with any of the members.

"The efforts of the council show how much the healthcare industry values HITRUST certification," Nodson says. "I shared this with our sales team, who can use our certification as a competitive differentiator when trying to close new business. Certification can accelerate the sales cycle and on-boarding process—something our customers appreciate as much as we do."

Assess Once, Report Many™

In addition to facilitating customer relationships, Craneware is planning to leverage the HITRUST CSF Certification to demonstrate compliance with Europe's GDPR and California's CCPA that went into effect in 2020. Many U.S. states are gravitating towards independent privacy laws, which means healthcare organizations may eventually have to prove compliance with up to 50 different regulations.

"Complying with multiple state laws would require extensive work from our Engineering and IT teams," Nodson points out. "But with a framework like HITRUST's—which aligns with all existing regulations and evolves as new regulations come into play—we can streamline our efforts. It's a method for complying with many security inquiries and regulations. Otherwise, trying to figure out which data sets apply to each inquiry and regulation framework is a nightmare."

The ROI of Certification

"The return on our investment in certifying with the HITRUST CSF comes from the time and effort it saves us from answering individual security questionnaires from our customers," Nodson says. "We can also respond to security enquiries faster, which is critical for our sales cycle—not to mention the trust it instills with potential customers."

Craneware can also leverage its HITRUST CSF Certification to demonstrate the company's commitment to protecting data privacy and complying with regulations. "We want our customers to see us as a partner who makes data security easy," Nodson emphasizes.

Craneware is now looking to its vendors for HITRUST CSF Certification. "We will consider certified vendors first over those who are not certified," Nodson says. "We assume our customers will do the same with us—it's the smart way to go for the entire healthcare industry."

A Changing Security Culture

Achieving HITRUST CSF Certification has helped Nodson do more than just communicate the importance of security across the organization. "We don't do things just because HITRUST requires it, but because it's important for protecting our business and necessary as a publicly-traded company," Nodson adds. "We have a responsibility to uphold these values for our shareholders and our customers. At the core, HITRUST CSF Certification is primarily all about doing the right thing with our customer data and managing risk properly for our business—and then demonstrating that we are doing these things well to all of our customers and the regulators."