Winterhawk

Client Profile:

Carlsberg

The Carlsberg Group is a brewing company founded in 1847 by J. C. Jacobsen who established a state-of-the-art brewery on a hill outside Copenhagen, Denmark. The brewery was named for his son Carl, and the hill (or berg) that it was built on. Since Jacobsen's death in 1887, the majority owner of the company has been the Carlsberg Foundation. The city as we know it has now expanded far beyond that hill, and Carlsberg has expanded far beyond the city to become the fourth largest international brewery group in the world. The company's flagship brand is Carlsberg but it also brews Tuborg, Kronenbourg, Somersby Cider and more than 500 local beers.

Nine markets in Western Europe, along with Group, Central Supply Chain and Shared Services functions, are now live and operating on a common SAP platform.

About Winterhawk

Winterhawk is the leading global SAP Security, GRC and Data Privacy consultancy practice. Supporting over two million users worldwide, we are proud to be innovative, independent and cost effective. Our services are complemented with domain expertise, software content, accelerators and toolkits which help us to provide our clients with fast, efficient and expert implementation and support.

Winterhawk addresses and resolves SAP ECC risks for Carlsberg's Western European Markets

Overview

With a large SAP authorisation redesign project already underway, Carlsberg identified immediate risks to their soft drinks businesses which were too great to wait for the redesign's completion. The job was to close the obvious loopholes in existing roles and, as much as possible, ensure that the roles being assigned to users were appropriate to their country responsibilities.

"The simple explanation as to why we used Winterhawk is that they are very effective, high-level SAP Security professionals."

Daniel Hansen
SAP Security Manager

Carlsberg's original SAP implementation did not take design, standards, efficiencies in role building, or even segregation of duties rules into consideration. There was no governance around role changes, nor procedure for testing, go-live or ongoing operational phases of the project cycle. Poorly designed roles deteriorated further over the duration of the implementation project.

Even under ideal circumstances, embarking on an SAP centralisation project is a daunting task. Taking multiple unique country markets with their own ways of working, putting them onto a new shared SAP platform, and having them follow a standardised process requires compromise on all sides. In addition to multiple markets, there was the Global Supply Chain, a full Shared Services function and various other central and corporate functions to consider.

The Challenge

Beyond simply producing and selling beer products around the globe, Carlsberg is a licensed producer and bottler for several third party companies. In Europe, they have contracts with multiple soft drinks companies, and in some cases these third party companies may be in direct competition with each other. While Carlsberg is able to license and sell products from one company in a given market, they would be contractually prohibited from selling a competitor's products in that same market. The company is able to sell the competitor's products in a different market but must avoid any appearance of promoting one company's product over the other.

From a legal point of view, this means ensuring that persons involved in the promotion and selling of one brand must not be allowed to see and/or transact with data related to the opposing brand.

Daniel Hansen, SAP Security Manager explains, "*Before our Pan-European project, this was not a huge problem – most of the systems were physically separate from one market to the next, and even if there were shared systems, the data itself was not always sensitive enough to be cause for concern. But when you put all of these markets onto a common SAP ERP platform you have the potential for an issue.*"

Role design during the original implementation did not maintain adequate firewalls between the different markets. Users were able to see and transact for markets other than the ones within which they normally operated. A role designed for a user in France, for example, could be opened up for processing in every other country due to lack of proper legal entity restrictions. Understanding the contractual obligations with the soft drinks partners is not simple, however in this case, even basic security measures were lacking. The lack of due diligence and governance at the user access management level meant users were routinely being granted inappropriate roles.

With four different country markets in Western Europe alone dealing in competing soft drinks sales, immediate and drastic action was required.

The Solution

Solving the problem was not as simple as restricting roles to proper legal entities or removing wrongly assigned roles. One of the great selling points of being on a shared ERP system is the ability to see and use data across different areas of the system, including different legal entities. With ten thousand users operating in a system specifically designed to take advantage of common logistics, procurement and finance processes, there are endless scenarios where an individual user legitimately needs access to a legal entity other than the one to which that user belongs. Processes were often set up to permit this, and there was an expectation that users should at least have view of other entities.

Addressing the issues required an understanding of when users required what appeared to be conflicting access, which many planning and cross-border logistics functions required to function properly. Knowing what should be allowed, and subsequently what should be forbidden, was the first hurdle to overcome.

Authorisations in the Roles: Addressing roles on a "master role" level was not an option in the end; while there were nine country markets, there was a mandate to fix roles for only four markets, and the project could not impact any of the other markets using those same roles.

A large number of the existing roles included open values for legal entity fields; wrong or inconsistent values and/or issues with the governance processes around role design. Therefore, there was no guarantee that a role created for a specific country actually limited access to that country.

Benefits to Carlsberg

Authorisations in the Roles:

- Creation of a matrix outlining which legal entity values were appropriate for each market.
- Categorisation of SAP roles in the system in accordance with that matrix.
- Governance controls around role design in place.
- Open values for legal entity fields were updated, wrong values corrected.
- Roles created for a specific country were corrected to limited access to that country.
- Review of categorised roles and corrected authorisations.

General:

- Improved focus on challenges to system security created by moving to a common ERP system.
- Better understanding of the need to secure the Basis layer of access, where client level access to data exists.
- Realisation of the need for better standards in role design and governance processes.
- Improved Change Management with the requirement to use the proper design and transport path going forward.
- Synchronisation of roles across the landscape.
- Don't assume compliance, verify it. This has led to more than one instance of re-considering an approach or decision in some areas.

The first task was to create a new matrix outlining which legal entity values were appropriate for each market. The second was to categorise every role in the system in accordance with that matrix, followed by the arduous process of going through every role for the relevant countries and correcting the authorisations.

For this job, we brought in two very competent technical resources from Winterhawk. They did all of the heavy-lifting, not only helping to complete this task efficiently, but also helping us to improve our governance processes around role building and transport administration,"
said Daniel Hansen

Role Assignments to users: Fixing roles was time consuming, but did not address the whole issue. Across the four markets, every user had to be reviewed to understand which assigned roles might be causing further issues. By leveraging the work already done on the User Master, it was easier to spot where users had role assignments that granted access to an opposing market; these were subsequently negotiated with country representatives to determine alternative roles or to justify the need for continuing access.

Daniel Hansen said: *"After many stakeholder meetings and re-planning sessions, we went live with remediated roles and role assignments for all four markets. Literally, thousands of roles were changed and 3,000 plus users in those markets were potentially impacted. Again we relied heavily on support from Winterhawk, as one of the key consultants to the role remediation process was also the key resolver of issues during the subsequent hyper care and support phase. In the end, there were only a few manageable issues, and we were able to close our hyper care support after one week.*

"We will continue to leverage Winterhawk in each of our different project tracks as well as our daily operational work. Their expertise has meant that we have been able to accomplish things we would not have been able to on our own. Going a step further, it also means they gain knowledge and experience in our business which makes it easier to plug them into new challenges as they arise. These people are an indispensable part of our security team now, and our first choice of partner when considering new projects."

united VARs Global Partner

Kinship PARTNERS