Protecting the Super Bock Group business

The increasing dependence of business operations on information systems has made the group increase the risk perception associated with exposure to cyber threats.

The goal was to create a single point of contact, available 24x7 to monitor and respond to security incidents.

The Super Bock Group

The main activity of the Super Bock Group (SBG) is based on the business of beers and bottled waters. It is an extremely competitive field in which competition, local or international, is strong and very active. SBG seeks to be a differentiator in these markets, both for its brands and products and for its agility and ability to meet the needs of its customers.

SBG is also present in the segments of soft drinks, wines, production and marketing of malt and tourism business, owning two reference assets in the region of Trás-os-Montes: the Leisure-Thermal Parks of Vidago and Pedras Salgadas. The company is mostly owned by Portuguese capital, 56% by VIACER Group and 44% by Carlsberg Group.

Digital transformation may potentiate the group's proximity to its customers and a differentiation vehicle in the offer to the market of big consumer goods. André Miranda, IT Architect and Project Manager at Super Bock Group at SBG, states that "*digital media for relations between companies, and between the latter and consumers of their products, may be differentiating factors and growth enhancers, both for SBG and its partners*".

One of the characteristics of the business that Information Systems have to deal with is the geographical dispersion of business. The existence of several production centers, logistics platforms or a distribution network scattered throughout the country or in foreign markets, increases the capillarity of action of information systems. In this sense, the path that has been followed is "*the centralisation of systems in order to optimise the reuse of our infrastructure and business applications*", explains André Miranda.

Super Bock Group in 2018

26 Brands

585 Million litres produced

458 Millions in sales

51 Million euros in net profits

1.310 Collaborators

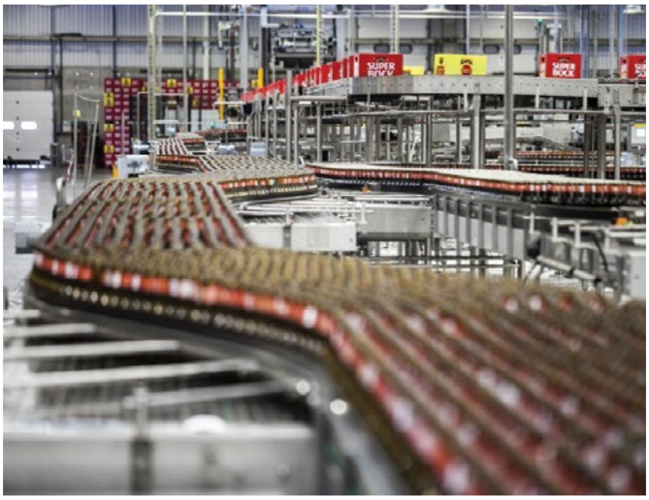
(Source: 2018 Management Report)

> *There are increasingly sophisticated incidents of attempted fraud. These complex situations, which usually involve social engineering, are also reviewed by SOC."*
>
> **André Miranda**
> IT Architect and Project Manager
> at **Super Bock Group**

The importance and relevance of this industrial group on the national scene, associated with scanning and increased reliance on information systems, led to an increased risk perception associated with exposure to cyber threats.

The results of the first audits and security reviews brought the issue of cyber security into the agenda with two obvious options. The first was to recognise the need for a Security Operations Center (SOC), a single point of contact, available 24x7 to monitor and respond to security incidents. The second is that these powers should not be indoors. The bet was to resort to an external specialised service able to monitor events in real-time. The choice was Claranet.

> *We have an increased visibility in our infrasructure safety incidents, and we´re supported by a team of specialists."*
>
> **André Miranda**
> IT Architect and Project Manager
> at **Super Bock Group**



claranet cyber security

Key services:

- Security Operations Center
- SOC as a Service
- Security Testing
- 24x7 Support
- Phishing & Social Engineering

For more information about Claranet's services, and the benefits these deliver, go to: www.claranet.pt

Super Bock Group
creates a Security Operations Center

When beginning to measure threats to cyber security, Super Bock Group concluded that there was an average of 100 incidents per year.

It needed the help of an expert to monitor and control threats in real-time and be able to react quickly to incidents identified.

Super Bock Group (SBG) has digital exposure both due to brands and to the need to provide different applications for business partners who access them over the Internet. On the other hand, both SBG and its partners are highly dependent on information systems to operate. In this scenario, the availability of systems is critical for normal business continuity. The vast digitisation of internal processes of the organisation, such as the increasing dependence of the relationship with customers on digital media, made the security of the group's information systems gain relevance. André Miranda, manager of architecture and IT projects at SBG, approaches the importance of the Security Operations Centre (SOC) implemented and acknowledges the improvements achieved with the services provided by Claranet in the field of cyber security.

How did the issue of cyber security enter the agenda of Super Bock Group?

The main factors for the group's stakeholders growing awareness of the risk of cyber security in recent years has been the performance of audit processes, which showed improvement opportunities in this field.

On average, how many attacks are sustained per year?

We have low maturity in accounting for cyber security incidents, but currently we record about 100 per year. Each of these incidents is processed by experts.

What solutions or management tools have thus far ensured operations at the Super Bock Group and what were its limitations?

Although we used auditing tools, we had an internal and very occasional approach to cyber security. We felt a lack of capacity both of knowledge and availability of the internal SBG teams regarding cyber security. We carried out some external audits, both technical and procedural, and we concluded that we needed to address this area with greater focus and dedication.

What caused the need for Super Bock Group to use a Security Operations Centre service?

The advantage of resorting to a SOC service is the active monitoring of our infrastructure and applications while maintaining the orientation of information systems to develop applications and areas where we believe we can bring more value to the business of SBG.

What does the solution implemented by Claranet consist of?

It is not specifically a solution, but a multi-year roadmap of activities related to cyber security that fits the establishment of a SOC. In addition to that we have other activities aimed at carrying out regular tests, both technical and behavioural, as well as awareness-raising and training of end users. In our view, the approach to cyber security should try to be holistic.

Does the frequency of attacks increase every year? Are threats increasingly complex and difficult to detect?

We have been aware that there are increasingly sophisticated incidents of attempted fraud. These complex situations, which usually involve social engineering, are also reviewed by SOC. However, it is a path that we are starting to tread.

Has the solution implemented by Claranet allowed detecting threats to Super Bock Group that could not be detected or would be very difficult to detect without it?

Yes. We have evidence of situations of exposure to risk that we would not have detected before we had the Managed Security Services service. In our experience, these situations did not materialise in costs or business losses for SBG.

Did you recently have an episode of phishing? What constraints did it entail and how was it neutralised?

Phishing episodes have occurred, but users are already quite aware of the issue and usually we realize that the behaviour is correct. The most worrying situations today are spear-phishing, sometimes associated with social engineering and combined with domain squatting. These more sophisticated attacks, involving multiple techniques and attack vectors for long periods of time, are complex and require organisations to also prepare timely and in multiple layers, from active monitoring offered by a SOC through the robustness of its processes and for training and awareness-raising among users. It is also important to face cyber security as something that goes beyond the organisation and includes its business partners, since the risk may come from them.

How do you reach this solution and Claranet as a supplier/integrator?

When we began the market research process for Managed Security Services solutions, we already knew Claranet's offer in this sector. It seemed appropriate, given the diagnosis that we made, to adopt an outsourced SOC service.

How long did the implementation process take?

The beginning of the service was made in about three weeks. The subsequent tuning process lasted about three months, but there is always a continued adjustment to be performed. Right now, we are reaching the point of stability with the service at "cruising speed".

How was the experience with Claranet in the onboarding process?

Early in the process we realised that Claranet had experience in customer onboarding, the structured process used to prepare the service for Super Bock Group. Although the service has many contact points with what they already performed for other companies, there was a phase of mutual introduction, important for the service to be adjusted to the reality of our company and business. I think that was a part of reciprocal learning in this process.

What procedures and precautions did you take in implementing this project?

Super Bock Group handles the management of its information systems with multiple external partners. The main point of concern in the introduction of the Managed Security Services component was the integration of new processes with existing support processes and the relationship between the different entities for day-to-day cyber security services to run as smoothly as possible.

Is the project already finished? What advantages did it bring to the company's business processes?

The project is finished, but we are aware that throughout the service delivery we will continue to need to make adjustments. The SOC service should act as cross lift of the level of security of business processes.

In an information security perspective, what has changed with the introduction of SOC services?

We have much better visibility of security incidents in our infrastructure and are supported by an expert team. We also have improved ability for cyber security reports, at both operational and management level.

What business areas achieved the greatest benefits with this project?

A cyber security project should be seen across the organisation. All business areas are clients highly dependent on information systems, thus they must face cyber security risks as inherent to the reality of an increasingly digital business.

What improvements are planned to be introduced in the near future?

Our cyber security plan was enriched with the addition of the Managed Security Services, but we have other initiatives planned for the future, focused on awareness of employees and the protection of our infrastructure. We do not see cyber security as a race with a goal to achieve, but as a continuous workout that makes Super Bock Group be ever more able.

For more information about Claranet's services, and the benefits these deliver, go to: www.claranet.pt