Infosys®
Navigate your next

CASE STUDY

SECURING A GLOBAL BEVERAGE MANUFACTURER

In 2017, a leading global beverage manufacturer minimized the risks associated with data breaches by adopting managed security services and moving all its data to the cloud. The manufacturer transformed its fragmented security structure into a consolidated one and outsourced it to Infosys.

Securing a fragmented landscape

Food and beverage manufacturing is an extremely competitive industry. Increased connectivity, the use of the industrial "internet of things," and sophisticated cyberattacks create more security risks. Responding to cyberattacks is not cheap, and the cost per data breach is likely to exceed $150 million by 2020.[1] Data breaches not only hurt companies financially, but also taint their reputation in the market. The blot on a company's reputation can lead to a loss of competitive advantage.

The subject of this case study is one of the world's largest multinational beverage manufacturers and marketers with more than 200 bottlers around the world. The manufacturer wanted to integrate data from all of them into a single platform, establishing common security standards across the ecosystem for bottlers of all sizes, including the franchisee bottlers. Having the bottling facilities being managed by different security providers increased costs and operational inefficiencies.

> Data breaches not only hurt companies financially, but also taint their reputation in the market

If a bottler fails to properly secure its IT systems, the manufacturer has to pay. As a result of the global nature of the company's brand, the manufacturer had to secure even the smallest of bottlers because a breach of any of them could be damaging to the global brand. To eliminate the need to hire and manage vendors, the company adopted an integrated cybersecurity solution with an integrated service provider.

The multiple vendor challenge

When a company has multiple vendors, each with its own approach to IT security and its own set of tools, there is no clear view of the company's security issues as a whole. An event on one site could lead to a significant disruption in another process. The investigation of the cause of the disruption could take a significant amount of time. Under such conditions, ensuring that all the processes work well is difficult. Unstable systems could also interrupt normal workflow. When the company in this case study started experiencing regular system failures and resolving issues in-house became challenging, it was time to seek a better solution.

The main challenges

- The manufacturer had limited or no documentation of its current state and had no defined metrics for service-level security agreements or for measuring provider performance. Another weak area in the company's IT security was in controlling user identity and access to the system. The platform for identity and access management was unstable and had no monitoring.
- The manufacturer stored all its IT operations data in multiple on-premise data centers. Running a data center is expensive. The company paid for the power supply, backup, communication systems and other devices. In addition, the data centers were maintained by in-house specialists, which also involved more spending. The company wanted to reduce its technology footprint and needed tools rationalization.
- The manufacturer wanted to consolidate its fragmented security operations. To do so, it needed to establish a standardized platform across the customer ecosystem and to monitor security across its small and large bottlers.

Transition to managed security services

In 2017, the beverage manufacturer partnered with Infosys. To facilitate the manufacturer's transition to managed security services, a team of experienced Infosys consultants created a standard operating procedure with indicators of compromise, defined and derived metrics for service-level agreements, and performance measurements. They determined five categories of risk: p1, p2, p3, p4 and p5. Each category has different priority of incident resolution. For example, a p1 risk has to be resolved within four hours, while a p5 is not time-bound future request.

Another team of Infosys experts implemented an identity and access management solution. They created standardized configurations of identity access management and established automated access provisioning. Any digital persona is an identity. Access provisioning for identity and access management is the management mechanism for identifying access to networks. It can deal with such things as passwords, identities and means of access. If the wrong people have administrative rights that allow them to access and alter confidential files, it puts the entire company at risk. Identity and access management is a key method of network control and security.

Moving to the cloud

Infosys and partner Cloud Security Alliance, together with the manufacturer, created a plan for data migration. The team worked together from the design process to the implementation stage. To reduce the costs, the team moved all data from the on-premise data centers to the public cloud. Public cloud uses a pay-per-use model and significantly reduces the costs of maintenance. Over the long term the team further consolidated all data centers, applications and security components into a single hosted environment on Azure Cloud.

To find out more about the benefits of moving to the cloud, read our "Navigate Your Digital Transformation With Cloud," report.

Outsourcing to SOC

Two of the manufacturer's goals were to have the capacity to monitor information and to manage risk. To establish a standardized platform across the customer ecosystem that ensured data segregation for compliance and regulatory needs, the manufacturer turned to security operations center services. At Infosys, an SOC is a structural unit that provides information security monitoring. It is entirely focused on the detection and investigation of attacks. The SOC deals with misauthentification events and alerts network intrusion detection systems.

The outsourced cybersecurity monitoring and management includes vulnerability scanning, virtual private network and firewall management, antiviral services, endpoint protection, network and gateway security and much more. Now the manufacturer can focus on its day-to-day work, leaving vulnerability and risk management to an outsourced IT provider.

Impact of transformation

By adopting managed security services, this beverage manufacturer secured more than 30,000 internal users, approximately 50,000 external-facing users, more than 27,000 end points, and more than 2,500 servers.

The solution also provided a single comprehensive dashboard that monitors information generated by the cybersecurity platform. The dashboard generates metrics that show the manufacturer information about the platform operations or malware detections. It allows early detection of an attack, an automated incident response and threat hunting. Now the company has visibility across its operational security landscape and can monitor security across small and large bottlers. All these activities are run from Infosys' local security operation centers in Pune and Bangalore, India.

Only 38% of global organizations claim to be prepared to handle sophisticated cyberattacks.[2] Many businesses do not prioritize cybersecurity until they experience a breach. Since cyberthreats are evolving every minute, businesses must adopt a proactive security approach and protect themselves.

The beverage manufacturer discussed in this article established a well-functioning security posture and had significant cost reduction from implementing a cloud security infrastructure. With managed security services, Infosys protects the company's information in public cloud and safeguards thousands of IoT devices with endpoint protection.

References

1. "An Insight Into the Dark Side of Cyber World," Infosys, 2019, www.infosys.com/services/cyber-security/insights/Documents/insight-dark-sight-cyber-world. pdf
2. "Cyber Security Statistics for 2019," Cyber Defense Magazine, 2019, https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

SMEs

Anil J Rajan

Delivery Manager – Cyber Security
aniljrajan@infosys.com

Ravi Kumar G

Senior Project Manager – Cyber Security
ravikg@infosys.com

Shreedharguru Vasanthrao Patil

Senior Project Manager – Cyber Security
shreedharguru_p@infosys.com

Author

Yulia De Bari

Consultant – Infosys Knowledge Institute
yulia.debari@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next