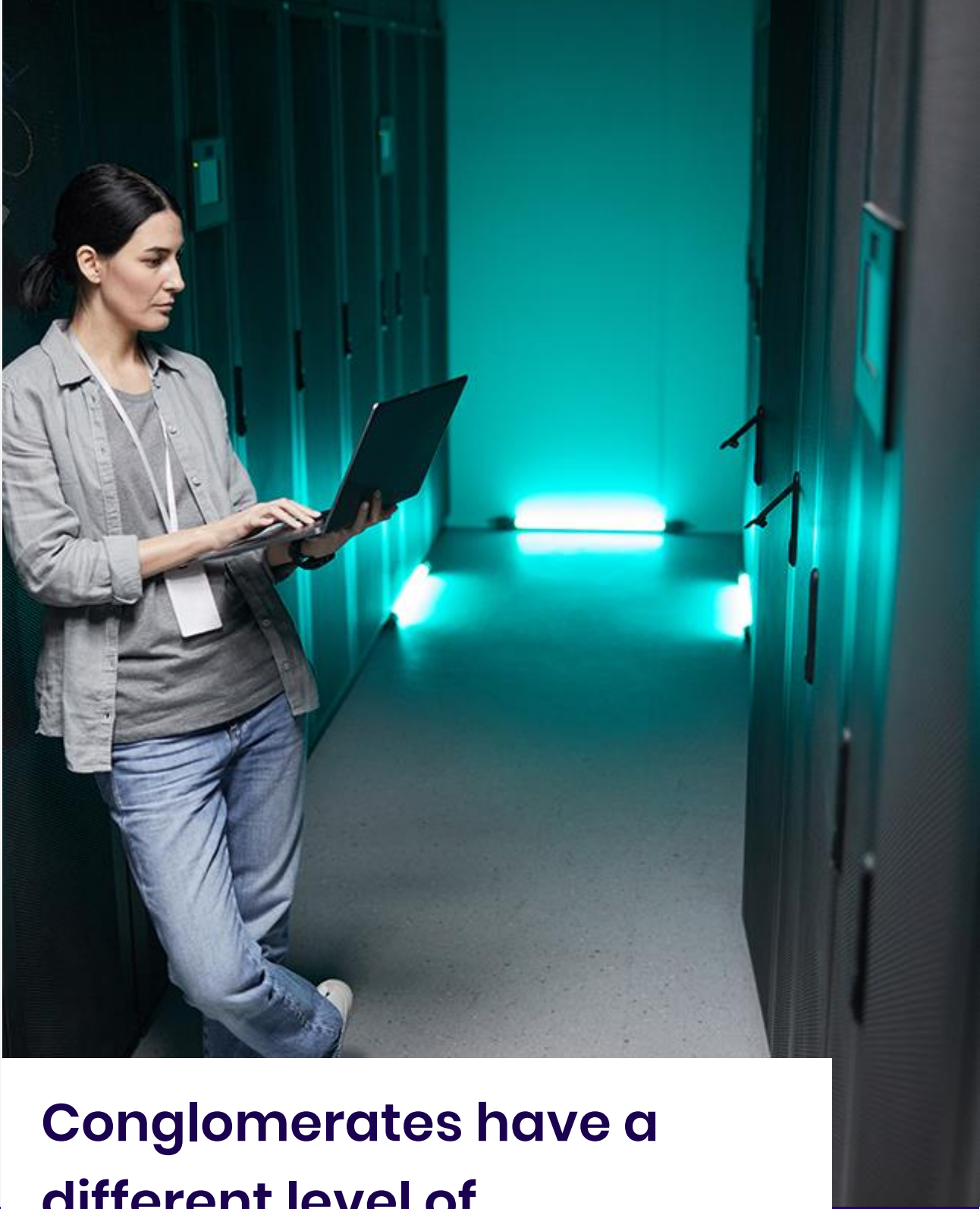
2021

CASE STUDY

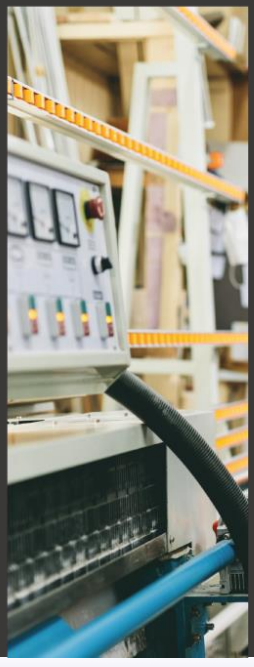


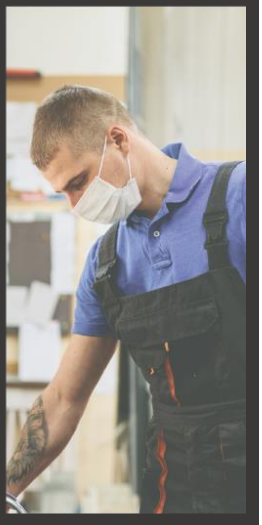
Conglomerates have a different level of Cybersecurity Challenges

It's not just the Scale but Security as a Culture that needs to be Managed.

Infopercept

Background:





A leading consumer conglomerate of the GCC, dealing with healthcare and food products has an international presence in 7 countries. With a strong workforce of over 8000 employees working on 500 brands, the company is committed to its partners, its consumers, and is also conscious about reducing its carbon footprint on the planet.

The company's core values of integrity and efficiency, combined with its no-compromise policy on providing quality goods, make it a formidable business in the market, a force to reckon with.

The Problem

The downside of being a large sized conglomerate is that it has to deal with a number of issues pertaining to security. Security of the company's data, network and infrastructure was a big concern especially as it was constantly evolving and innovating and bringing better products into the market. It was thus imperative to maintain a high standard of security.

It was a huge concern for the Chief Security Information Officer (CISO). Lot of money was being spent on the internal team to maintain security. Although the internal team was doing its best, there was no concrete evidence or sure shot assurance that all security needs were being met. There were no regular updates being given to the CISO even though there was mention of work done. The CISO thus wanted to engage the services of an external Security Service Provider who would be able to give an overview of the current scenario and be able to provide a complete security solution.

The company was keen on hiring an *MSSP (Managed Security Services Provider)* who had sufficient experience, were certified, would be able to provide customized solutions, and who would have the technology and know-how to handle the security for all its various global operations.

Infopercept - an experienced and globally reputed MSSP

Infopercept, a global leader in providing cyber security solutions, was engaged to look into the security concerns faced by the company. Infopercept launched a detailed and an extensive operation (as it involved operations across 7 countries), to study the landscape of the security infrastructure.

It used *Offensive Security Strategies* to better understand the vulnerabilities in the network. Now offensive strategy uses ethical hacking to check the loopholes in the system. In order to do so, apart from virtual testing, teams from India were sent to Saudi Arabia and Kuwait to understand the actual ground reality. An intensive investigation using this strategy would entail checking the perimeter, network, endpoint, application, and database.

As the name suggests, scrutinizing the *perimeter* was mandatory as it is the first line of defense and acts as the gateway to enter the network. A breach here could be catastrophic as it would leave the entire network exposed. To understand the massive scale of operations Infopercept was undertaking, it is crucial to understand that it involved businesses spread across 7 countries of which every aspect and department was virtual, i.e. all operations were conducted online. For instance, their distribution channels, supply chain management, finances, sales etc. were all operating digitally.

Next in line was to protect the *network* which encompasses both software and hardware technologies. The importance of network security is quite apparent as lack of it could lead to technical, legal, and financial risks to say the least.

Endpoints or entry points are desk points, laptops, and mobile devices. From a security point of view this is crucial as it influences the admission control policy given to users and checks their security credentials.

Application security was next up in the infrastructure chain. As many applications are directly linked to the cloud, it makes them vulnerable to threats and breaches. Moreover, a number of external applications are used on the customer's mobile phones which are also a security threat.

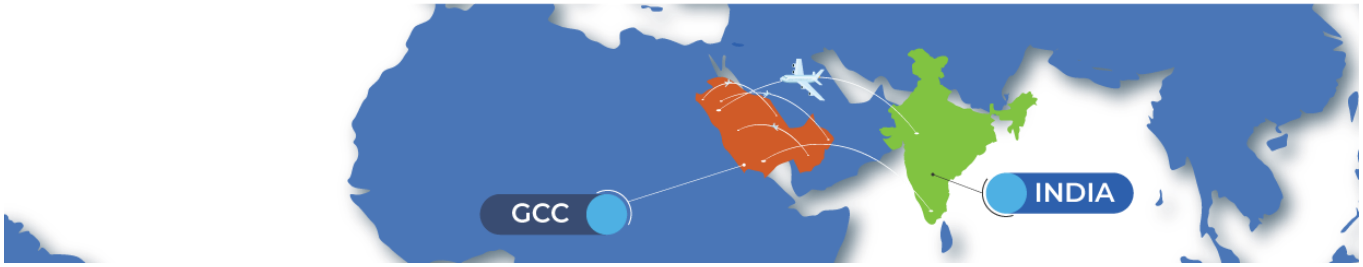
A leak in the *database* can have irrevocable consequences. Apart from financial losses from which one can manage to recover, is the almost irreversible loss of reputation, consumer confidence disintegration, and brand erosion. Thus it is of paramount importance that security safety guards are deployed to protect the enterprise.

Phase 1

The Infopercept team began intense scrutiny of the aforementioned parameters and found a number of vulnerabilities. The internal security team of the company was unable to detect any of the hacks done by Infopercept. A micro combing of the entire network was done, no areas were left untouched. It revealed flaws in every aspect of the landscape. It was alarming to say the least. A detailed report was handed over to the CISO mentioning in detail the security loopholes.

The CISO then sent out feelers to vendors looking for the right solution. A number of vendors applied, providing new solutions of their own. The CISO came back to Infopercept with the new solutions and with an intent of procuring the new solutions, not comprehending that they already had over 20 of the best solutions in hand which could solve the current issues.

Now the Infopercept team was aware that budget was not a constraint for the company but it would be prudent to use the existing solutions rather than incur more expenditures. The Infopercept team apprised the CISO of the same and as strategic partners it was their duty to provide the best security solutions to the company. The CISO had already seen the team in action over the offensive strategies used in identifying the breaches.



Outcome:

It was now time for the Infopercept team to showcase its technology optimization skills put forth by the *Technology Optimization Center* (TOC) team. The TOC team would use the existing tools and technologies to patch the loopholes found. As the operations spanned 7 countries, the security network infrastructure was massive. The TOC team had its work cut out for it.

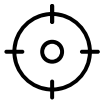
Proper planning, taking corrective measures of initial deployment, preparation for acceptance in organizational change, impact and capacity analysis were a few of the practices that had to be incorporated into the system. This estimated time allotted was up to 6 months involving a three-member team.

Once the process was initiated, it was smooth sailing then on. The company saw a complete turnaround and met expectations on their return on investment which included the current and past investments. The CISO was extremely pleased with the result. The company realized that security is an ongoing journey and not a destination and that it is a continuously evolving process.

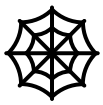
Phase 2

The company was apprised of the need for a Security Operations Center (SOC). An SOC team would monitor, detect, analyze, and respond to cybersecurity incidents. Management approved the SOC and sent out requirements for the same. A number of solutions were received. Infopercept then proposed the use of *Invinsense*.

Invinsense, an integral tool designed by Infopercept, combines a number of cyber security solutions to cater to different types of hacks and attacks. Apart from tackling the *techniques* used by the adversaries to attack the system, the Invinsense platform looks to understand the *tactics* used by attackers and combats them effectively. Some of the tools that were used are



ODS (Operational Data Storage) -
a kind of interim digital warehouse that stores data.



OODA (Observe-Orient-Decide-Act)-
a military strategy adapted for security purposes and is used to assess risk and respond to incidents.

RBAS (Risk Based Authentication Solutions) -
a multi-level authentication process that provides access to a system and whose authentication process becomes more stringent as the risk level increases.

G-SOS (Green Secure Optimize Strengthen) –
a platform designed to integrate various practices into the businesses and manage the IT landscape in its entirety.

Benefits

Being a large conglomerate, the designing of IT security involved integrating various processes and departments across 7 countries. The involvement of devices, applications, people and data increases exponentially. Each division had its own set of problems and challenges that had to be catered to. Infopercept stepped up to the challenge and was successfully able to deliver not only what the company wanted initially (an offensive strategy) but went above and beyond, and delivered a complete and total long lasting cyber security package which involved technology optimization and security operations centers as well.

With its highly competent and certified workforce, Infopercept was able to effortlessly tackle the various issues the company faced. Especially during the pandemic times with its own set of challenges, Infopercept was able to incorporate real patching with virtual patching and is now ready for more additional and advanced solutions. The idea was to enforce and strengthen the existing solutions and build from there. This resulted in enormous cost saving for the company thus laying the foundation for a long and trusting relationship with Infopercept.

About INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint

Publisher
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E : sos@infopercept.com

Global Offices

UNITED STATES OF AMERICA
+1 516 713 5040

UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 909

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

Infopercept