STRENGTHEN YOUR BUSINESS CONTINUITY EFFORTS WITH CCS

Did you know that many leading enterprises spent over $144 million in 2020 to respond to the largest ransomware attacks?

Ransomware is a malware that locks down a user's files and data, with the threat of erasing it or publishing it, unless a ransom is paid to the attacker.

How it affects your business?

In addition to monetary expenses and reputational damage, a ransomware attack affects the operational reliability of your business. After a company gets cyber-attacked, customers may panic and decide to discontinue their services. Such unfortunate incidents tarnish the reputation of the attacked company, stresses out in-house security teams and impacts its bottom line.

Business risks

- Loss of private data
- Weakened client trust
- Service disruption and disablement
- Personal information/identity theft
- Interruption in the entire enterprise network infrastructure

Why Consult CCS for Business Continuity and Disaster Recovery (BC/DR)

CCS security specialists can support you in integrating relevant controls, orchestrating workload deployment, replicating data to the cloud and building effective threat management.

We help your organization resume normal operations if an attack hinders the physical access to the company DC

Protect your business, digital assets, data and users as CCS experts and proven frameworks cater to your security and compliance needs

We spot, devise, and automate threat responses confidently with centralized cloud security services

Get your organization a cloud security services provider that continually replicates critical business applications, infrastructure, systems, and data to the cloud and understands technology through-and-through both in terms of hardware and software

Our cloud security experts develop your cloud security strategy after assessing your resources and business needs and plan your RPOs and RTOs well in advance to avoid the loss of mission- or business-critical applications

CCS Helps a Leading Healthcare Organization Overcome a series of Ransomware Attacks in 2020

CCS security team carried out the Disaster Recovery process of a leading healthcare organization in South India that was attacked by ransomware in December 2020. Despite facing newer challenges throughout the recovery phase, we had all systems up and running within ten business days.

About client

Our client is one of the most advanced tertiary care hospitals in South India, providing world class patient care by blending the concepts of 'Evidence Based Guidelines' and modern technology.

Cyber-attack & recovery

Ransomware attack happens at clients on-premises data center on Dec 3rd, 2020 01

CCS quickly isolates the infection, enables DR through Azure site recovery console on the same day 02

On day 2, CCS works with Microsoft team to resolve fallback of particular VM on-premises 03

On day 3, 2nd targeted ransomware attack takes place 04

CCS identifies 2nd ransomware infection on the same day 05

Restores data from cloud to the NAS server on-premises 06

Moves about 7 TB of Azure VM data (PACS VM) to Azure storage account 07

All PACS app data are successfully moves to the Azure storage account 08

Creates the Azure Import/export jobs & requests the Microsoft team to send data on hard disk by day 8 09

CCS receives the hard disk from the Microsoft data center by day 20 and completes the DR process successfully 10

Our client's on-premises data center was attacked by ransomware, which called for efficient threat resolution. Isolating the affected servers took precedence over DR enablement. CCS security team was met with several challenges ranging from issues in failback operation to the second bout of a ransomware attack and PACS showing symptoms of the virus. In collaboration with Microsoft, CCS restores data from Azure to get the PACS up and running and rely on shippable devices for offline data transfer to the on-premises NAS server. Given latency issues, CCS sent a hard disk to the Microsoft data center and subsequently copied the received data to the client's on-premises server. CCS cloud & security team carried out the Disaster Recovery efficiently and had all systems up and running in 10 business days despite fresh obstacles cropping up throughout the recovery phase.

About CCS

CCS Technologies is an IT solutions & services company, having served over 300 customers in over 15 countries.

Along with our expertise and experience, our consultative and flexible approach to working with clients ensures they can recognize better business efficiencies and faster growth.

To learn how we can help you on your digital transformation journey and bolster your information security, visit:

www.ccs-technologies.com

collaborate@ccs-technologies.com

+91 956 767 1727