Case study

dimension data
an NTT company

South Africa | Healthcare

Restoring the Western Cape Blood Service's digital pulse after a cyberattack

Client profile

The Western Cape Blood Service is an independent, nonprofit organization operating throughout the Western Cape. They work without prejudice to supply safe blood and blood products to all communities in the region, from Cape Town all the way up to George.

Each year they collect more than 150,000 units of safe blood from unpaid volunteers. These donations of whole blood or blood plasma affect the lives of more than 445,000 people every year.

The blood service uses the latest technology and research to protect people and excel in the science of transfusion medicine. The safety of blood donors and blood recipients is their priority.

> **"If you haven't been through something before, you think you know what to do.** But when you bring in Dimension Data, they have done it before. And that just helps you recover so much quicker."
>
> **Jacques Breslaw,** Head of IT, Western Cape Blood Service

Summary

In 2021 the Western Cape Blood Service experienced a ransomware attack that blocked access to the technology they use to safely get the right blood product to the right person at the right time. The attack put lives at risk. Despite not having a formal relationship at the time, we worked together to investigate the attack and recover from it. The systems that underpin their medical services were up and running again just 36 hours after the attack.

Vision

Managing a cyberattack

At around four in the morning of 29 July 2021, the Head of IT at the Western Cape Blood Service received a call to say that their systems were down. A cyberattack had blocked access to the environment by encrypting workstations and taking out servers.

While an attack like this is any company's nightmare, in this instance it was a threat to lifesaving care for thousands of people. The Western Cape Blood Service is the only source of blood products in the region and issues about 7,000 units a month. Their technology ensures that the right patient gets the right blood product at the right time and that the blood is safe.

The attack disrupted the systems that track blood from the volunteer donor's vein to the patient's vein. In addition to affecting personal and health records, it prevented the service's laboratories from doing automated, batch blood testing. While these tests can be done manually, the manual process causes significant delays and doesn't have the same safeguards built in as the digital system.

Paying the hackers to restore the system and rewarding their criminal intent was never an option. The focus had to be on recovering the systems that underpin their medical services and getting them up again as soon as possible.

"It was quite frightening because I was worried about operational paralysis – that we would not be able to do what we need to do as a blood service for the next hours or perhaps days. It was also a little confusing why any entity thought it was a good idea to ransomware or cyberattack a nonprofit entity that's doing good," says Dr Gregory Bellairs, CEO and Medical Director, Western Cape Blood Service.

Western Cape Blood Service
Do something remarkable

Which services?

- Incident Response

Which partners?

- CloudStrike

"It was quite frightening because I was worried about operational paralysis – that we would not be able to do what we need to do as a blood service for the next hours or perhaps days. It was also a little confusing why any entity thought it was a good idea to ransomware or cyberattack a nonprofit entity that's doing good."

Dr Gregory Bellairs, CEO and Medical Director, Western Cape Blood Service

Transformation

A shared goal of savings lives speeds up recovery

At the time of the cyberattack, Dimension Data and the Western Cape Blood Service didn't have a formal relationship with contracts in place. But we had worked together in the past and had even donated some services to the nonprofit.

When they contacted us, we put together a cyber-response team in just a few hours. Our recovery experts supported their team throughout the recovery process, starting with cutting internet access and isolating machines.

We then conducted a forensic investigation to identify the full extent of the attack. The next steps were to contain the damage and recover the environment.

Getting licenses for CrowdStrike – a next-generation antivirus solution – including implementing the solution was an important part of maintaining and managing the environment.

The cyberattack took out the service's online backups, but fortunately they had offsite backups as well, and these could be restored.

Results

36 hours to get a lifesaving system back on track

The recovery team had the the systems that underpin their medical services up and running again only 36 hours after the attack. Although the other systems took longer to recover, in total the blood service lost only six hours of data.

"If you haven't been through something before, you think you know what to do. But when you bring in Dimension Data, they have done it before. And that just helps you recover so much quicker," says Jacques Breslaw, Head of IT, Western Cape Blood Service.

Using past threats to predict future threats

Forensic investigations track exactly how the attack happened. This information can be used to prepare for, and hopefully prevent, future attacks.

Mitigating future threats

CrowdStrike's advanced cloud-native platform provides cloud workload and endpoint security, threat intelligence, and cyberattack response services.

Technology plays a crucial role in driving business outcomes, which is why 85% of the Fortune 500 companies come to us. Find out how our full range of capabilities will empower your people, strategy, operations and technology to achieve your business modernization and transformation goals.

Explore our services