

## Case Study:

---

### DG Health Cyber Security Strengthening Program

The purpose of the project is to put in place a program designed to help achieve Cyberconfidence, by moving to an active approach to cybersecurity awareness and response.

#### Client

DG Health - Melbourne

#### Challenge

Cybersecurity is a major threat to the security of healthcare organisations.

Inevitably, the growing use of technology in healthcare means an increased risk of cybercrime. Research suggests that cybercriminals explicitly target healthcare organizations, with the intent of stealing medical records, credit card details and Social Security numbers. Every year, over three-quarters of healthcare organizations experience some kind of data breach or security incident, potentially exposing them to reputational damage, loss of intellectual property and, most importantly, the loss of patient data.

- Understanding and defining areas of exposure, and putting in place remediation plans
- Focusing on policies and procedures that embed security into the clients' operations
- Using a security roadmap to inform long-term organizational decisions

#### The Outcome

Building on the findings from these workstreams, Powerdata and the client identified priority activities with the aim of delivering security and compliance at the lowest cost and performance impact

#### Our Work

Staying ahead of cybercriminals requires active effort; simply focusing on compliance is no longer enough.

Powerdata helped this client achieve cyberconfidence through an active program addressing the risks of data security, patient harm, reputational damage and financial loss, as well as delivering regulatory compliance.

---

#### Contact

501 Dandenong Road  
Armadale, VIC. 3143  
+61 3 9507 2052  
[info@powerdatagroup.com.au](mailto:info@powerdatagroup.com.au)

