THE FIVE KNOWS

dazychain

CORRS CHAMBERS WESTGARTH lawyers

IDC

1 *Know the value of your data*

- To your organisation and to those that want to steal it
- Can you identify the critical data - "the crown jewels" - that need to be protected?
- Are you able to classify your data by its value to the organisation?

2 *Know who has access to your data*

- Do systems exist to determine who has access to data?
- Do people have access to more data than they need?
- Do you know all of the clients, trusted partners, suppliers and contractors who can access your data?
- Do you know what those parties share with 3rd parties?

3 *Know where your data is located*

- Is data saved on local machines, mobile phones, storage devices, document management systems, servers, backup servers or a combination of all?
- Are filing and naming conventions enforced for data identification?
- Where data is being housed by 3rd party providers and/or in the cloud, do you know any contractual or jurisdictional issues that may apply?

4 *Know who is protecting your data*

- Do the people who have the role of protecting your data have the requisite experience?
- Is your organisation a reactive one who pulls a team together when an incident occurs or a threat hunting one who has a dedicated team who are constantly looking for threats?
- Does the organisation support the view that protecting data is more than just an IT problem - it is a business risk involving management and all staff?

5 *Know how well your data is being protected*

- How well are the custodians doing their job? Do you know if alerts are being monitored or is the team overwhelmed?
- How well are 3rd party vendors doing their job? Have they ever been tested on their capabilities?
- Are the security systems that are in place (eg endpoint, SIEM, IDS, DLP) proving the necessary security information that the organisation requires?