Cybersecurity to protect the Australians private personal data & minimize cyberattacks on organization should:-

1. Start with regulating ISPs to increase their cybersecurity footprint . Since data that flows into the Australian continent enters mainly through under water cables ABA should enforce strict regulations to the entities providing internet access to increase their cybersecurity footprint . ( before data enters into the continent it should undergo scrutiny using multiple AI cybersecurity solutions ). At the end of the day why do all public / private organizations have to invest hardware / software technology & cyber professionals to protect their infrastructure . Does it not make sense to focus on the entry point of data & put substantial resources to detect cyberattacks.
2. For organizations penalties are not the answer . At the end of the day an organization if hacked can go bankrupt if private personal data is leaked . So how does penalizing an organization that's about to default solve the issue . The answer should be focus first on the cyber awareness of the employees & the elderly . Effort should be on this aspect as humans remain to be the weakest link .
3. Yes organizations need to improve their cybersecurity landscape but this requires cyber security professionals which is in shortage.( me for example I've left the Middle East to migrate to Australia to serve the country with my skills have not yet had one interview even after submitting job applications . You need to set quotas to allow people with working visas to enter the working circus )
4. Companies private & government alike need to have a risk profile assessment to determine we're they stand . This needs to be not an iso or any standard but should be treated as the main requirement to allow the entity to sell services or sell products . ( continuous monitoring with kpis should be administered by a third party at all times. Just like a managed services but more if grand scale . Any organization whose kpis goes below a threshold should be reviewed and immediate assistance should be taken to identify the root cause . Lessons learnt should be shared with all .
5. As data moves to the cloud it is now makes it more difficult to contain the leakages and cybersecurity hardening so moving to the cloud for those organizations having people data should remain on the continent cloud . This requires more data centers to be set up and allows local Australian regulations to be enforced

In summary start with identifying the organizations Risk appetite and cybersecurity posture . And have them conduct red team & pen testing asap .