Cybersecurity for healthcare

HISA’s 2018 Cybersecurity in Australian Healthcare survey reached 48% of health services in regional/rural areas and 52% in metropolitan areas. We received responses from executives (23%), administrative staff (22%), IT staff (18%), clinicians (12%) and the remainder a mix of researchers, consultants, vendor specialists and board members. Respondents felt a strong sense of organisational responsibility for the security of information assets and information systems with the following measures in place: formal plans (73%), staffing (75%) and dedicated security budget (42%). Compared to 2017, there has been a notable improvement in security awareness training (59%, from 36%) documented procedures (68%, from 45%) and evaluation of systems at procurement (51%, from 36%).

95% Understand they have personal responsibility for security and integrity of patient and corporate data

69% Performed data and system backups daily

17% Experienced a data breach

28% Experienced a hacking incident

60% Were clear on procedures to follow in the event of a cyber incident

36% Were aware cybersecurity risk assessments were performed at least annually

27% Reported more than 2 hours to recover from a system outage

Where the message is yet to get through

51% Ongoing use of legacy and end-of-life systems and hardware, with (20%) and without (31%) vendor support.

33% Individually assigned user credentials although shared or generic credentials used also.

85% Reasonable use of work devices for non-work related tasks is acceptable. It is a staff privilege that requires staff to be security savvy at all times.

www.hisa.org.au