SECURITY CHECK OF AUSTRALIA'S HEALTHCARE INFORMATION

CYBERSECURITY ACROSS THE AUSTRALIAN HEALTHCARE SECTOR

Final report of a national survey,
June 2018

HISA AUSTRALIA'S DIGITAL HEALTH COMMUNITY

Acknowledgements

HISA's Cybersecurity Community of Practice (CoP) was established to inform and engage stakeholders and healthcare providers across the Australian health ecosystem regarding cybersecurity.

The CoP would like to specifically acknowledge the following members for their contribution in crafting the survey, performing the initial analysis and communicating the findings:

Tony Abbenante, David Bunker, Dr Damian Claydon-Platt, Dr Josie Di Donato, Raana Monshi, Dr Louise Schaper, Prof Trish Williams and Dr John Zelcer.

1. Background (Why we did the survey and who responded)

HISA's Cybersecurity Community of Practice (CoP) was established to inform and engage stakeholders and healthcare providers across the Australian health ecosystem regarding cybersecurity.

There are those who ask "who would be interested in hacking patient data?" It is precisely this attitude together with the rate at which healthcare refreshes its technology that exposes healthcare organisations to high risk of cyber attack. Professor Trish Williams presented at HIC 2017 a list of reasons why the healthcare industry is appealing to hackers: ransom for money; denial of service for malice and money; stealing confidential data; compromising data; identity theft and compromising devices. The scale of disruption and impact to busy healthcare settings already operating at capacity caused by a cyber attack needs no explanation.

To better understand the current state of perceptions and cybersecurity practice in Australian healthcare, the CoP conducted a survey over a period of five weeks in September/October 2017. The survey posed questions across four broad domains to assess awareness and maturity across the healthcare ecosystem. The survey investigated:

- **Leadership**: Ownership of the issue
- **Culture/Staff responsibility/awareness**: Training and awareness of cybersecurity and its related implications
- **Policies and procedures**: Understanding of business continuity processes and incident response procedures
- **General cybersecurity knowledge**: Utilisation of fundamental security processes that are currently followed within the organisation to mitigate security breaches e.g. use of USB, on- and off-boarding processes, password policies, organisational asset register, and so on.

There were 157 responses to the survey, from a cross-section of organisations.

Initial analysis of survey findings provided insights into healthcare's cybersecurity posture at a point in time.

2. Why the Results are Important

The survey has taken an initial pulse of cybersecurity that ought to be repeated annually.

It has also raised the profile of cybersecurity in the healthcare sector.

The Cybersecurity CoP is committed to responding to the information needs of the diverse digital health community. When we asked the healthcare community on which areas the CoP should focus, we received reasonably balanced feedback which endorsed our stated mission of informing, engaging, and influencing (Figure 1). Other suggestions included providing warnings about breaches in healthcare and understanding global trends.

Cybersecurity Community of Practice Focus Areas

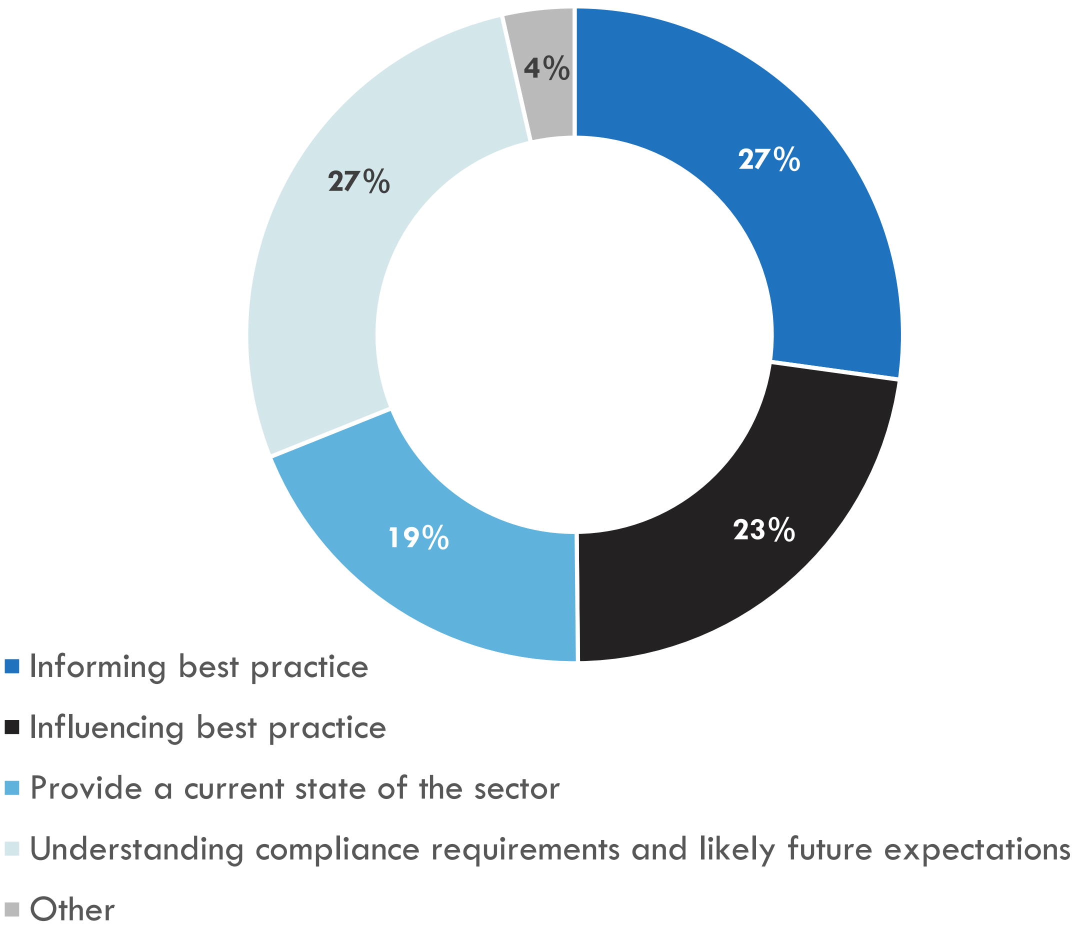


Figure 1: Suggested areas of focus for the CoP

STATE OF CYBERSECURITY MATURITY

Patients place their trust in our healthcare services to **safeguard their information** and ensure it is not accessed inappropriately.

A large portion of clinical and other staff think they **have no responsibility for cyber security.**

As healthcare **continues to digitise,** the results from the 2017 survey suggest there is room to improve.

STATE OF CYBERMATURITY

Identify

33% of organisations said they did a **cybersecurity risk assessment** at least annually

65% had a formal business or **governance plan** which included managing **cybersecurity issues**

Protect

84% **backup systems** and data on a daily basis

15% declared **never using work devices** for personal use which means a lot more do

40% **install operating system** patches and updates within 48hrs

31.8% patch only after extensive **testing by the IT team**

STATE OF CYBERSECURITY MATURITY

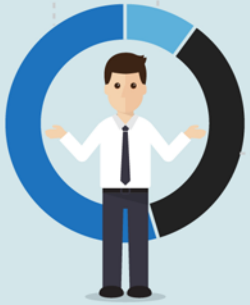
Detect

43% maintain a **central register** of end user devices and what information is accessed and by whom

35% were either unaware of any process or were certain **no tracking procedures** were in place

Respond

In the event of a cybersecurity incident



54.5% of respondents indicated that they knew what to do

9.8% were unsure

35.6% were NOT clear at all

34% of organisations will **refresh their systems** and hardware prior to or shortly after vendor support ceases

22% of organisations continued to **use end-of-life systems** without vendor support

Recover

22.7% organisations indicated that there was regular **business continuity testing**

25.8% **didn't do regular testing** at all

3. Review of data: initial findings

3.1 Respondent profile

157 people responded to the survey. The majority of participants were aged between 41-60 years (62%), almost a quarter were under 40yrs old, and only 12% were aged over 60. 40% of respondents were female. Most respondents had accumulated significant experience in the healthcare industry; with almost half having worked more than 20 years in health, and another quarter had between 11 to 20 years of experience in the field.

There was a broad spread of roles represented. One-fifth of the respondents were executive managers (20%), another fifth were IT staff (20%), although notably only 2.55% of these had formal cybersecurity qualifications. Non-healthcare specialists made up around 17% of the respondents, and only about 13% were actually clinical staff.

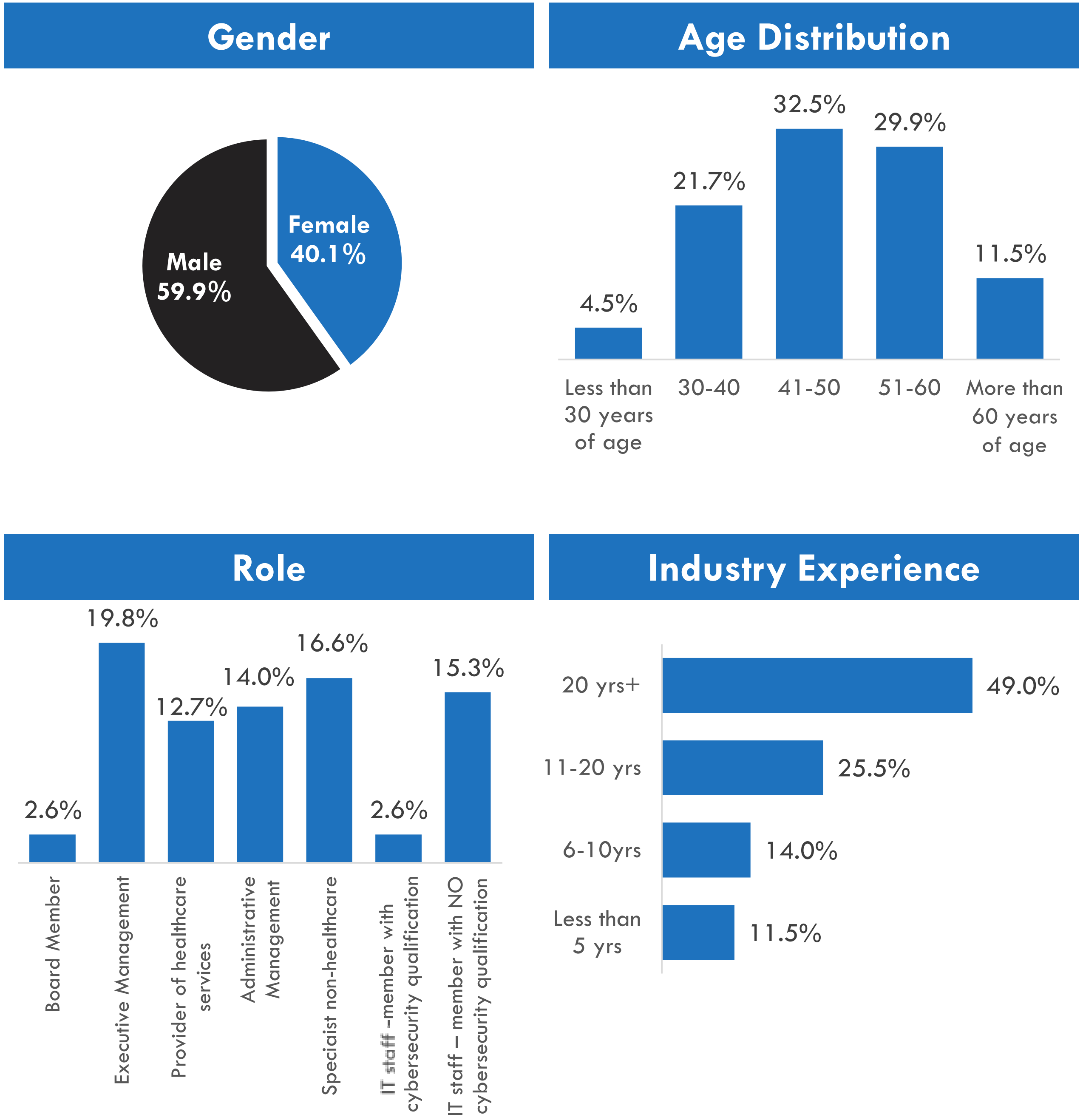


Figure 2: Respondent Profile (n=157)

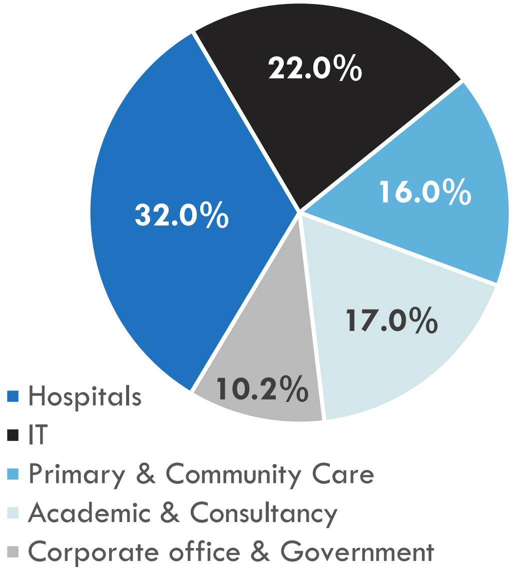
3. Review of data: initial findings

3.2 Organisational Profile

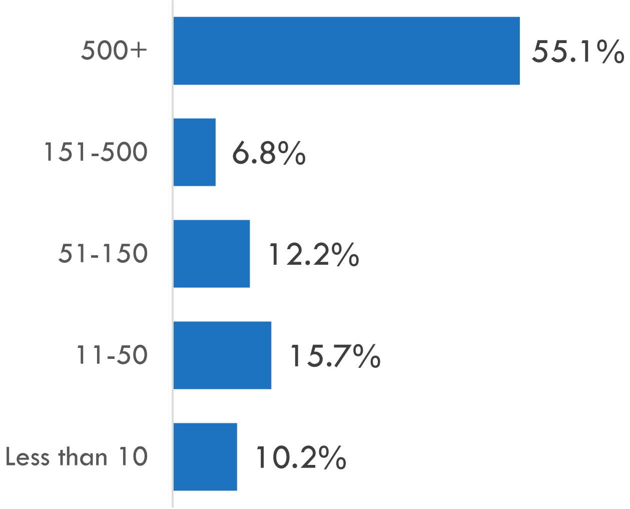
Respondents came from a broad range of settings, though the greatest representation was from Hospitals (private and public) (30%) and IT vendors (20%) followed by Primary & community care (13%). Respondents also predominantly came from larger organisations across the state or multiple sites across the community (52%). Though half of respondents worked at large organisations (500+ employees), smaller and medium sized organisations were also well represented.

The majority of organisations had a metropolitan presence (85%), although a third also were rural services (33%). And finally, while we had respondents from every state and territory in Australia, the majority came from health services in Victoria (53%), NSW (31%), and QLD (27%).

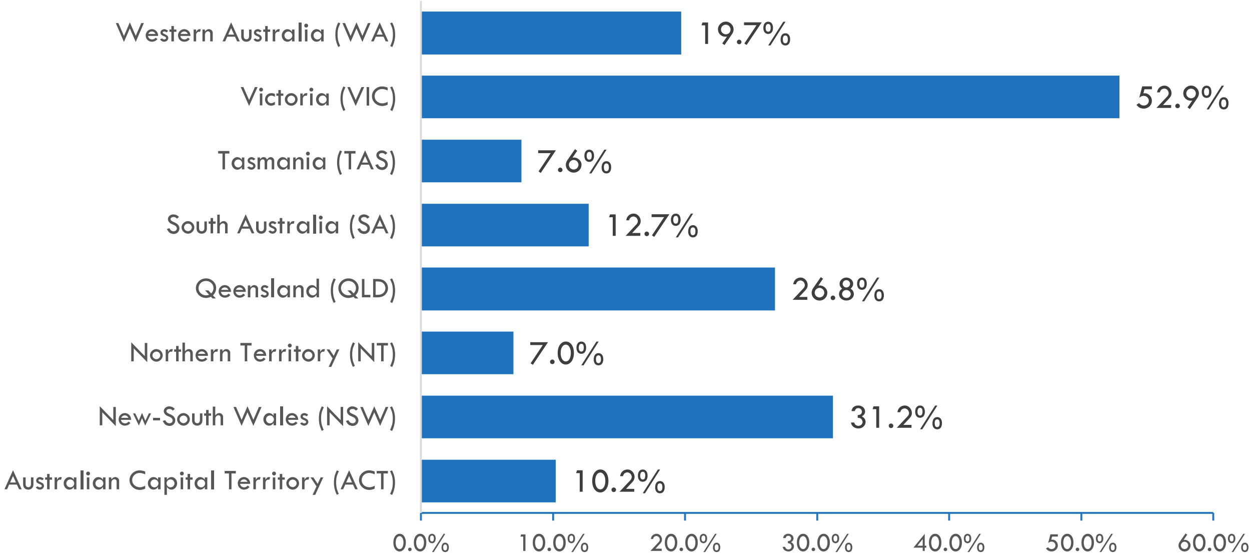
Organisations



Number of Employees



Geographical Setting



3.3 Governance and Leadership (Q11-Q14)

Respondents indicated that (figure 3)

- Almost two-thirds (65.5%) of organisations had a formal business or governance plan which included managing cybersecurity issues.
- Less than half (46.5%) of organisations actually employ a senior information security leader who has responsibility for assuring cybersecurity
- More than two thirds (68.3%) of organisations actually employ staff that have specific responsibility for managing cybersecurity
- But less than one third (31.7%) of organisations have dedicated budget for managing cybersecurity.

All of these questions were highly correlated ($p < .0001$). This would suggest that organisations which took cybersecurity seriously would be more likely to ensure that they had a dedicated budget, a senior security leader, staff for managing cybersecurity, and a formal business / governance plan in place.

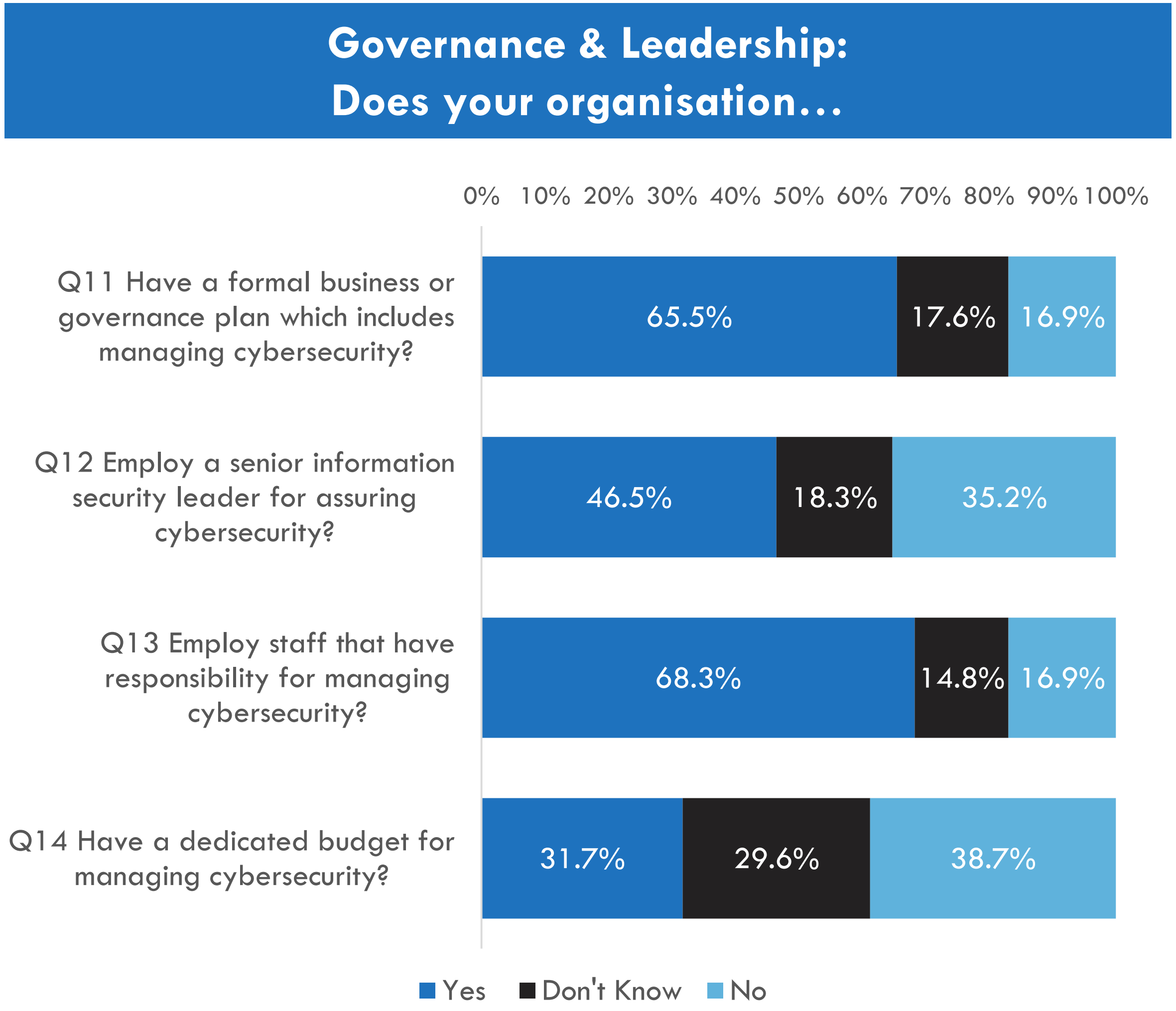


Figure 3: Governance and Leadership

3. Review of data: initial findings

When looking more closely at the budget question (Figure 4), a significant correlation with organisational profile became apparent
[χ2 (28, n = 142) = 41.614, p < .05].

Notably, only a relatively small proportion of hospital and primary care providers had a dedicated cybersecurity budget.

Healthcare tends to have a lower security posture. Of note however, in some organisations there were a large proportion of respondents who were unclear about this question (as indicated by the black bar) which increases the uncertainty of this data.

Q14 Does your organisation have dedicated budget for managing cybersecurity?

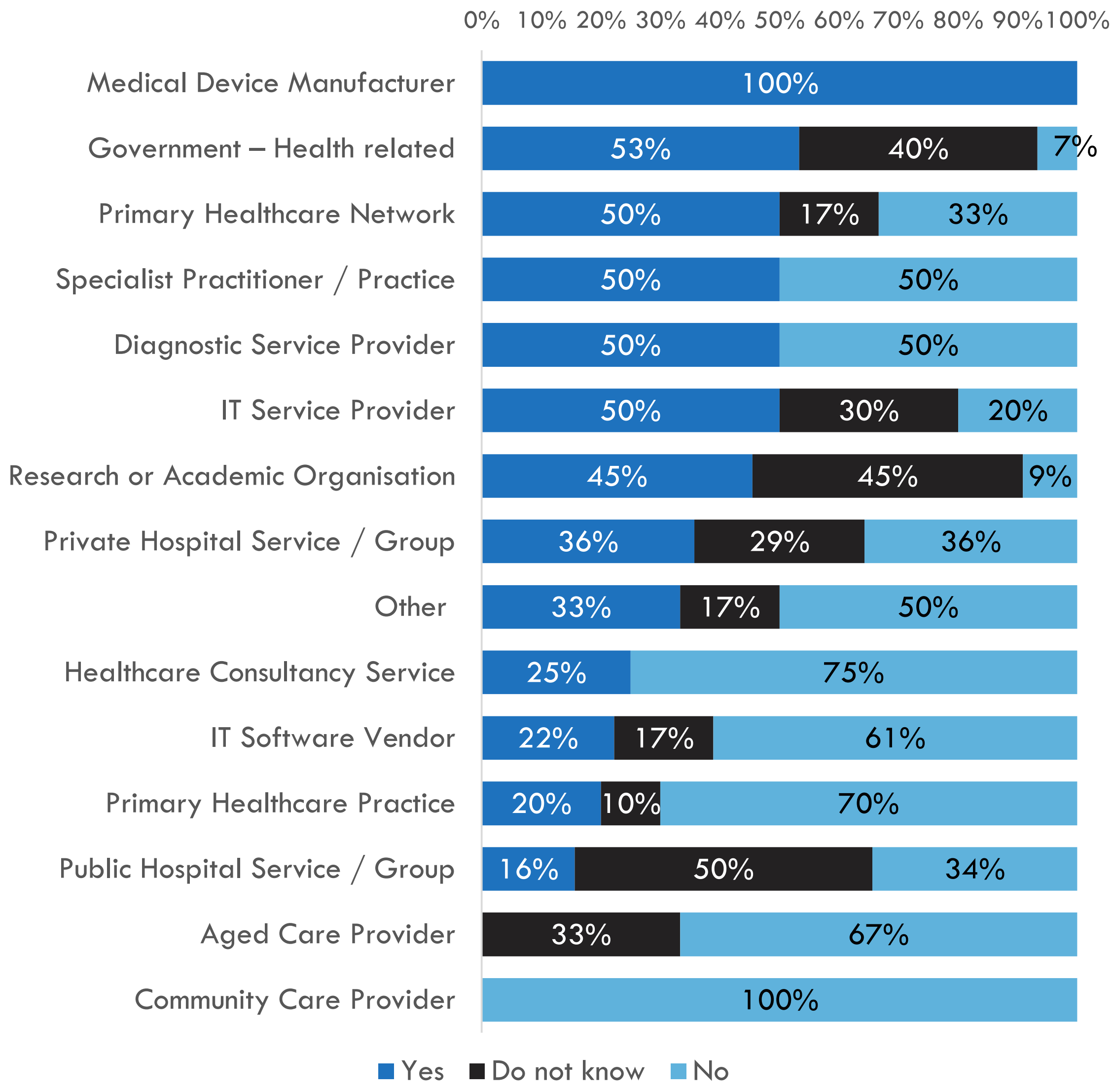


Figure 4: Dedicated cybersecurity budget, by organisation

When reviewed through a geographic lens (Figure 5), the data not unsurprisingly demonstrated the significant disparity between metropolitan and rural organisation's ability to obtain dedicated budget for cybersecurity [χ2 (8, n = 142) = 10.504, p < .05].

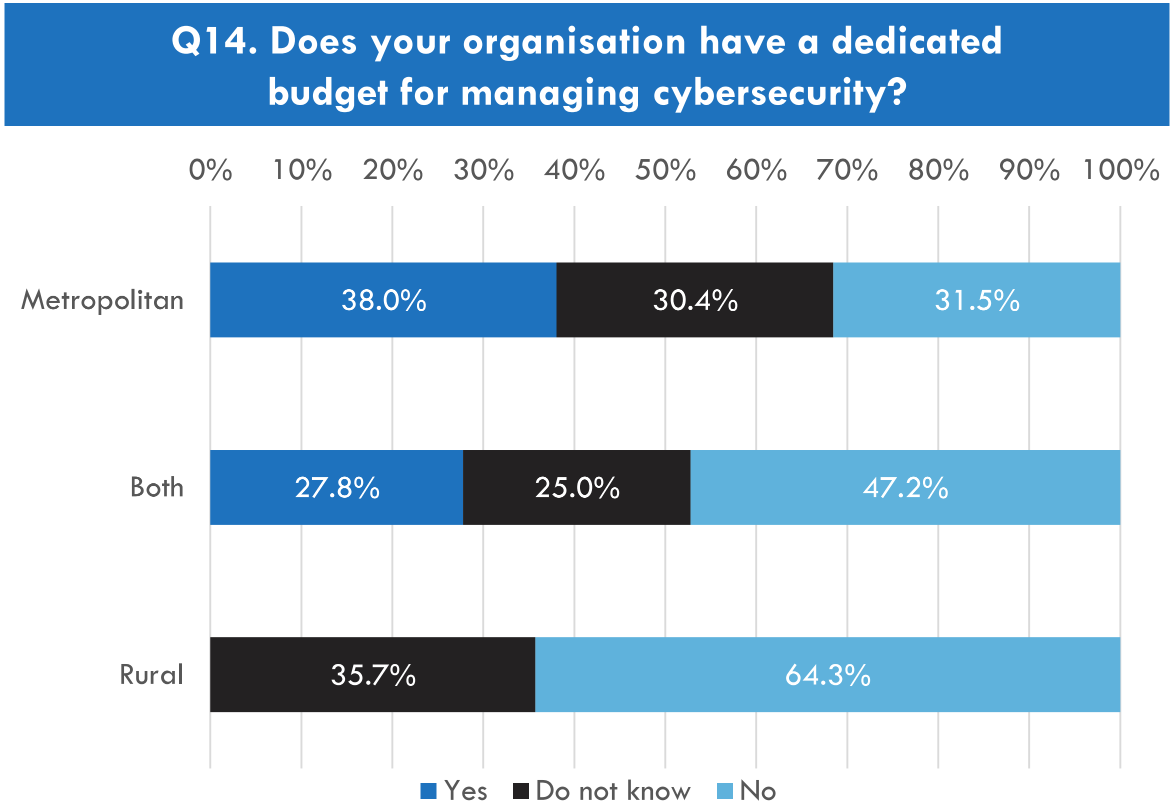

Q14. Does your organisation have a dedicated budget for managing cybersecurity?

Figure 5: Dedicated cybersecurity budget, by geographic location

Organisation size was found to significantly influence the response on all four of these questions (Table 1).

Correlation Chi-Square Rank (χ^2)		Q11	Q12	Q13	Q14
Q8 Approximately how many employees work within your organisation? (n = 142)	χ^2	20.591	29.966	23.144	32.347
	df	8	8	8	8
	p	.008	.000	.003	.000

Table 1: Chi-Square correlation ranks for Q11-Q14 correlated with organisational size

Specifically, the smallest organisations (defined by staff numbers) were least likely to have optimal governance and leadership in cybersecurity. Unexpectedly, medium sized organisations seem to be punch above their weight outperforming the larger organisations. Although, there was a larger proportion of "do not know" responses for larger organisations, reflecting the fact that there is a greater chance of employees not being in roles with specific knowledge of such information. Thus the actual proportion of larger organisations with dedicated funding, staff and formal governance may actually be higher than the proportion of "yes" responses suggests (Figure 6).

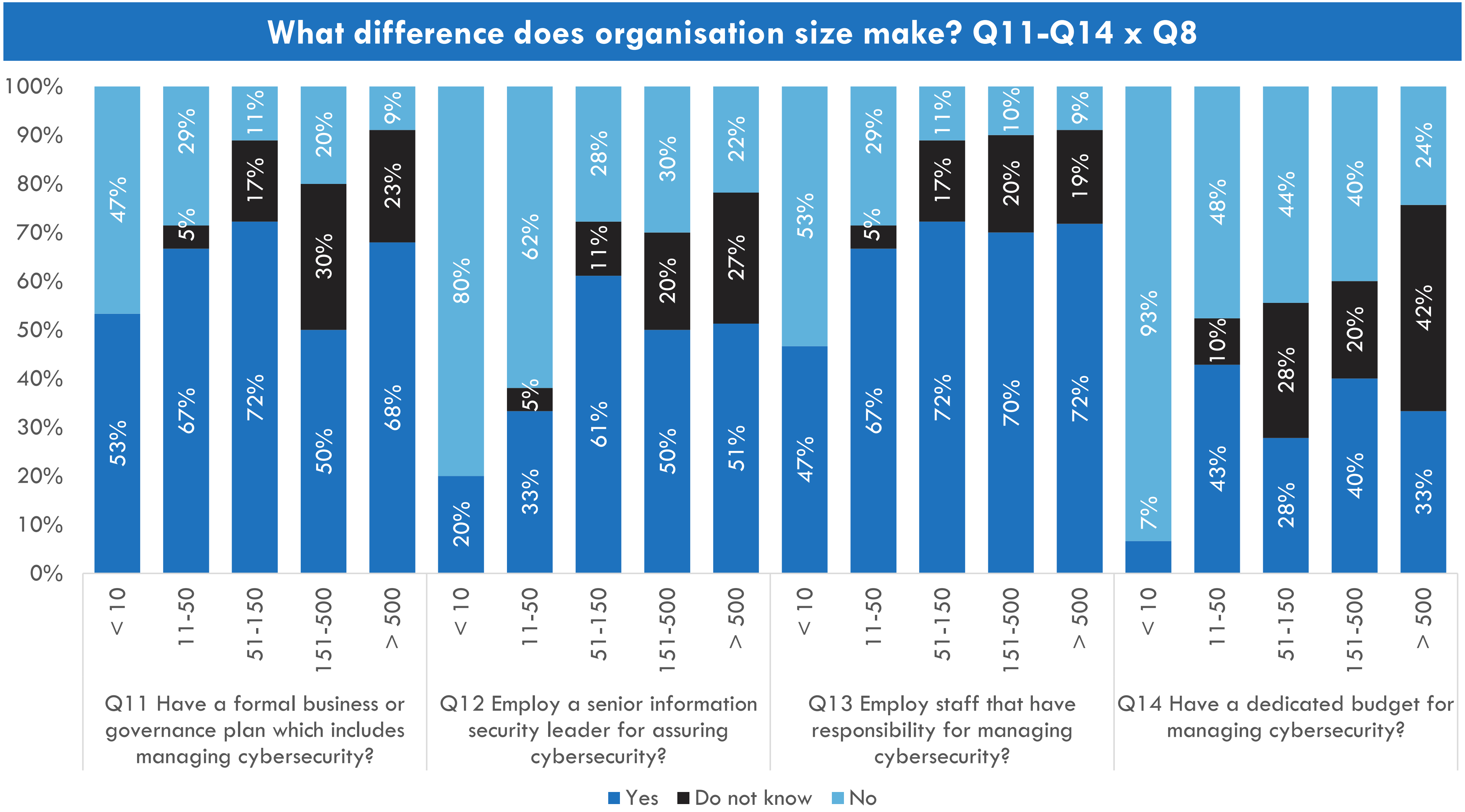


Figure 6: Governance and leadership, by organisation size

3.4 Culture, staff awareness and responsibility (Q5, Q15-Q17)

While almost 70% of respondents indicated having some responsibility for cybersecurity, almost a third (31.2%) declared “No responsibility”. There was a significant difference in the perception of responsibility depending upon the role within the organisation [χ2 (21, n = 157) = 54.864, p < .0001].

What was notable, was the large portion of clinical, specialist non-clinical, admin and other staff who think they have no responsibility for cybersecurity (Figure 7). **However, cybersecurity is actually everyone’s responsibility – it’s just a different responsibility depending upon your role.** For these non-IT staff, their responsibility would not be about procedures, policies and IT solutions, but it is paramount that they understand the potential for introduction of attack vectors through malicious websites, phishing emails, and infected USB drives, and the potential privacy risks issues of using personal email or phones to capture or transmit sensitive patient information. **There is risk here amongst our care provider organisations that needs attention. This is a significant education opportunity – it’s about data privacy, responsibility, staff obligations.**

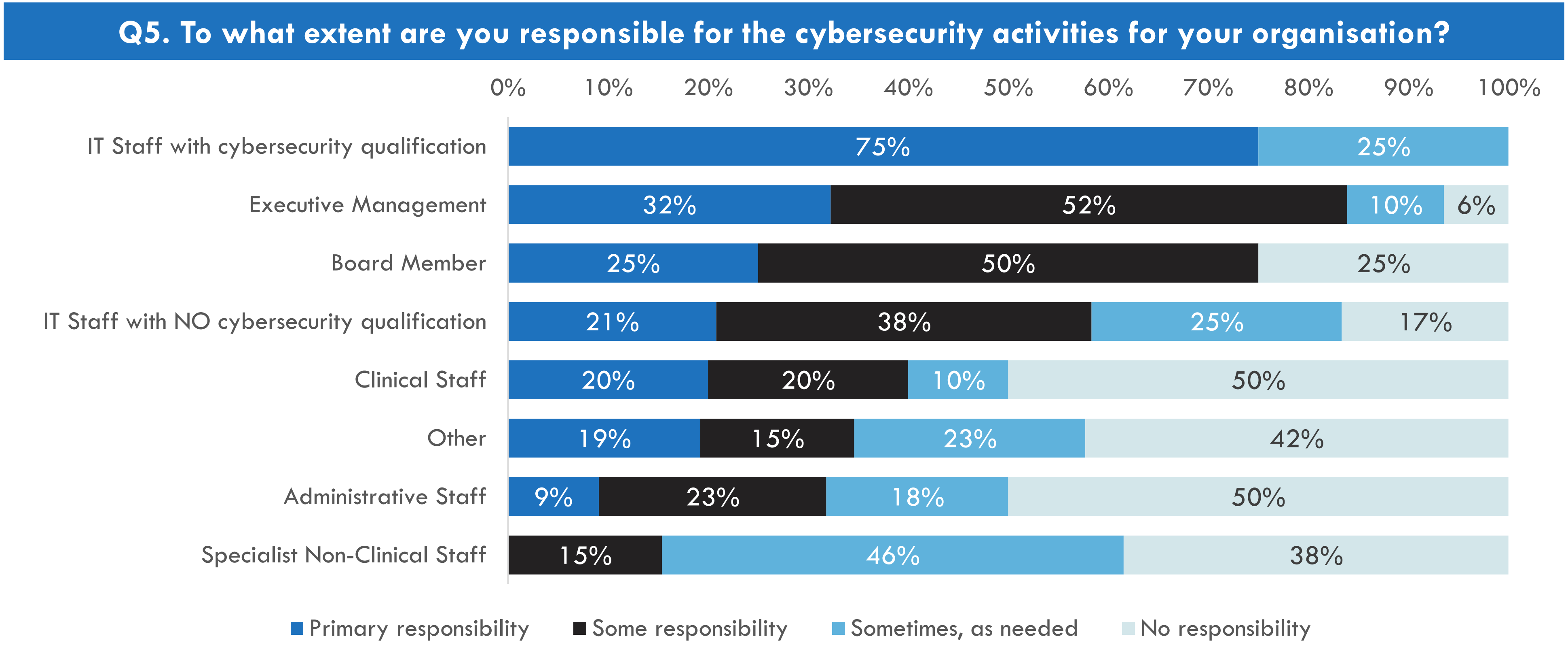


Figure 7: Personal responsibility for cybersecurity, by role

Perceptions around cybersecurity practices also varied notably by role (Figure 8). There was an expectation from board members that this was done at least some of the time, but IT staff were aware of this NOT being a routine part of the procurement process in more than 30% of cases. This shows a key disconnect between expectation and practice which poses risk for organisations.

In 2018, a cybersecurity assessment of new products should be mandatory.

Digging further into expectations (Figure 9), significant variation was noted across roles around responsibility to protect the integrity of patient and corporate data. This time, it was the IT staff who had higher expectations than all other roles. Again it was the clinical, administrative and other staff who had the least confidence that people in their organisation understood their responsibility in this area.

Q15. Is a cybersecurity assessment part of standard practice when acquiring a product or service for your organisation?

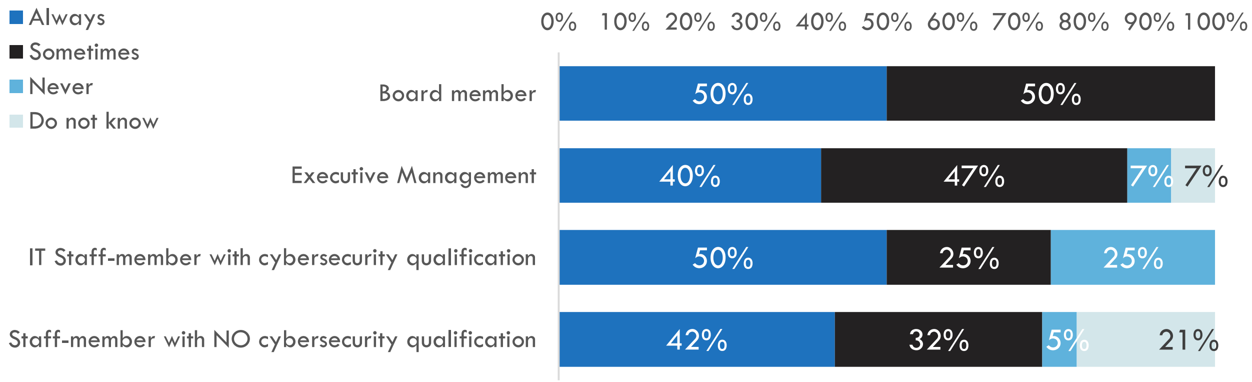


Figure 8: Cybersecurity assessment, by role

Q16. Employees, service providers and vendors working in my organisation understand their responsibility in ensuring security and integrity of patient and corporate data.

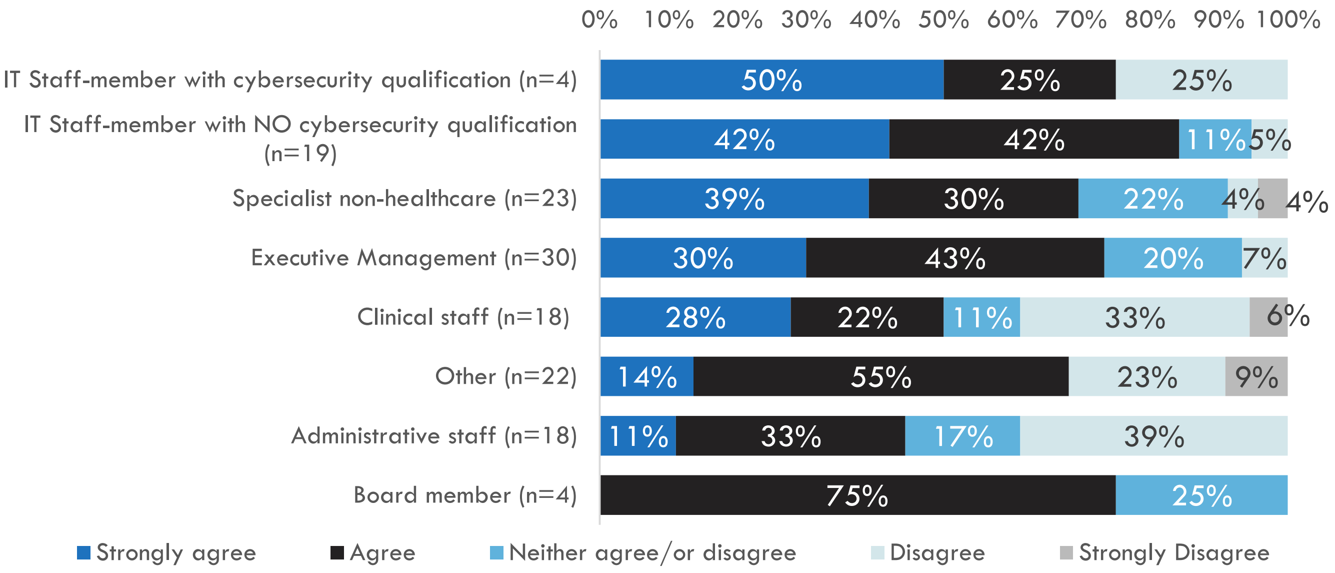


Figure 9: Understanding of cybersecurity responsibilities, by role

However, self-reported knowledge of responsibility around cybersecurity was more consistent (Figure 10), and actually greater than expectations previously reported.

Notably, only clinical staff and a few "other staff" admitted to not actually being sure of their responsibilities in this space.

This highlights an opportunity for education, particularly given that clinical staff proportionately comprise the largest portion of healthcare provider's workforce.

Q17 I understand my responsibility for ensuring security and integrity of patient and corporate data

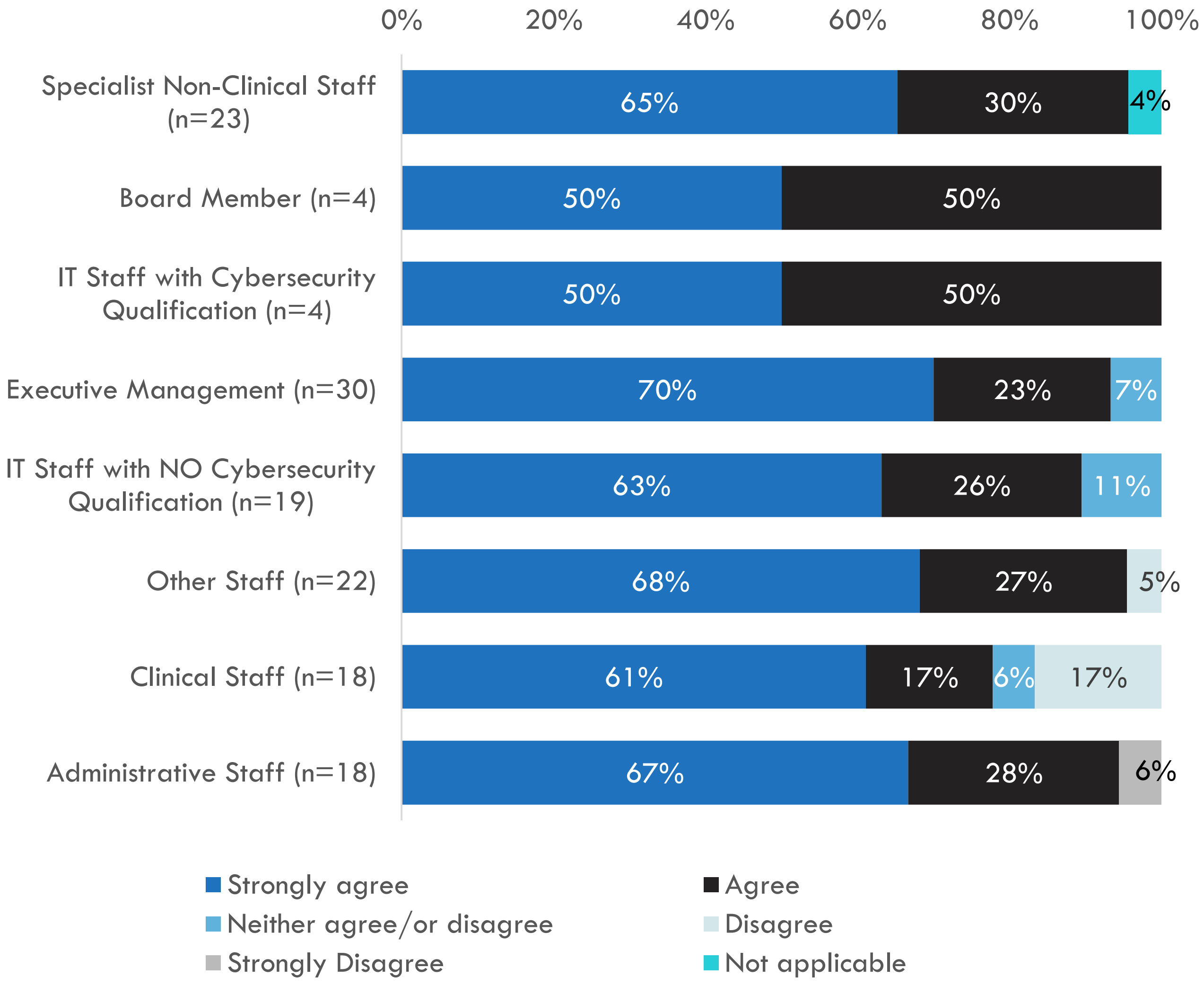


Figure 10: Understanding of personal responsibility, by role

3.5 Policies and Procedures (Q18-24)

Clinical staff likely to be largest cohort of staff – least aware or exposed to cybersecurity training

The next set of questions was intended to explore the current policies and procedures in the cybersecurity domain (Figure 11).

- Less than half of respondents (44.7%) were aware of the presence of a documented cybersecurity procedure or guide in their organisation, with a third saying one did not exist (32.6%), and almost a quarter not knowing (22.7%).
- In the event of a cybersecurity incident a little more than half (54.5%) of respondents indicated that they knew what to do, however about one third (35.6%) were NOT clear at all, and the rest were unsure (9.8%), suggesting an opportunity for education and perhaps even some drills. This is reflected in the responses to the next two items.
- Only a third (36.4%) of respondents indicated that Cybersecurity awareness and training was embedded within their organisation's policies and procedures, and almost half (46.2%) said that it was not.
- Finally, with regards to frequency of testing of business continuity testing in the event of a cybersecurity incident:
  - less than a quarter (22.7%) indicated that their organisation did regular testing;
  - less than one quarter (22.7%) only tested sometimes;
  - one quarter (25.8%) of organisations didn't do regular testing at all; and
  - the remainder (28.8%) of respondents were unsure.

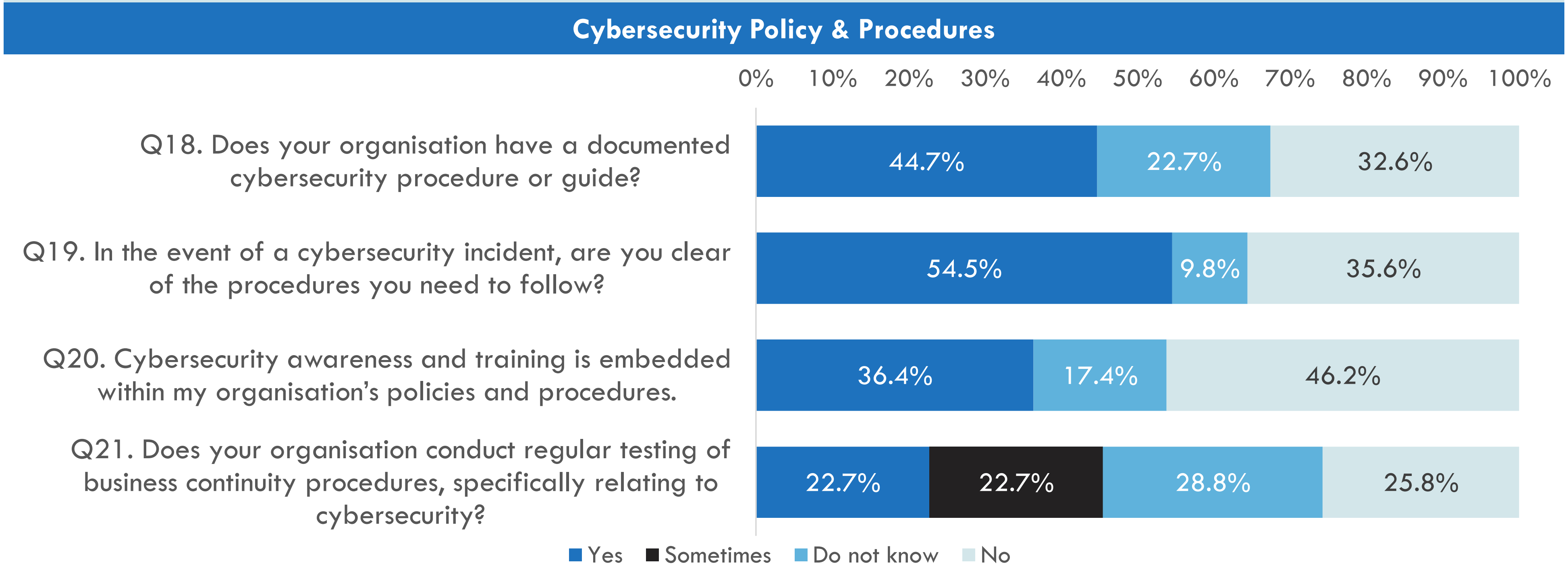


Figure 11: Cybersecurity policy and procedures

Not unsurprisingly, knowledge of cybersecurity training was significantly varied between different roles in the organisations (Figure 12), with clinical staff the least aware of the policies and procedures [χ2 (14, n = 132) = 27.277, p < .05].

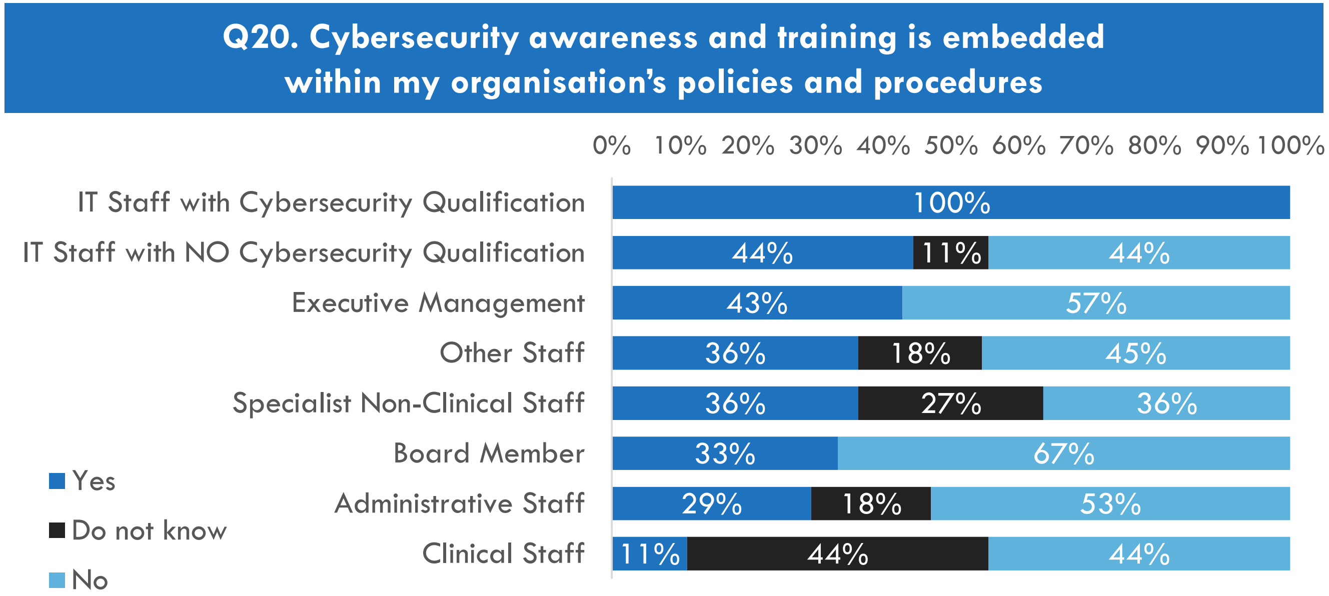


Figure 12: Cybersecurity awareness and training, by role

The frequency of organisational cybersecurity risk assessment and penetration testing was quite variable, but on the whole, done poorly (Figure 13). There is certainly room to improve on this front. Of note though, almost half of respondents were unsure of the frequency of risk assessments. Regardless, only one third of organisations (32.9%) were known to do at least annual testing.

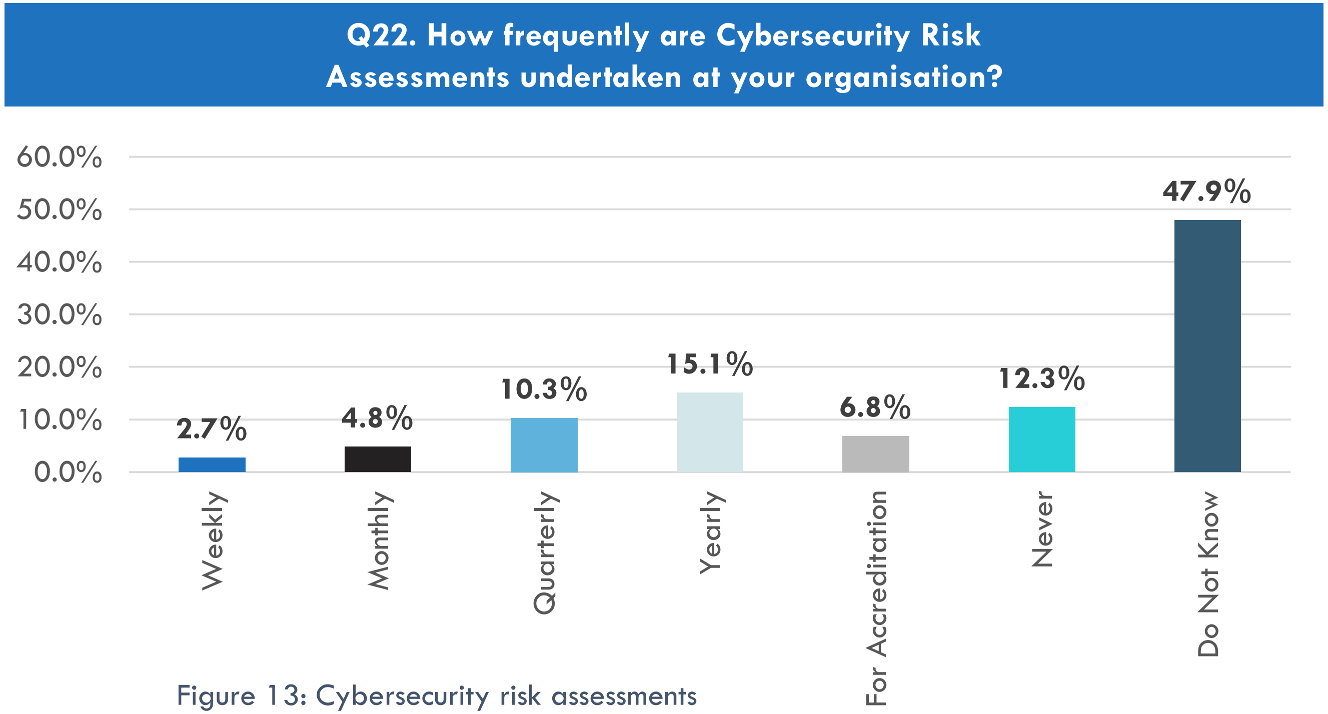


Figure 13: Cybersecurity risk assessments

Given the large number of unknown responses by non-IT staff it made more sense to analyse the response to this by IT staff only (Figure 14). The data reflects responses from a total of 22 IT staff, with and without cybersecurity qualification. Out of the 22 IT staff that responded, 7of these still did not know about the frequency of cybersecurity penetration testing. Of note: 2 out of the 7 were cybersecurity qualified.

Q23 How frequently is cybersecurity penetration testing conducted at your organisation?
(Responses from IT Staff only n=22)

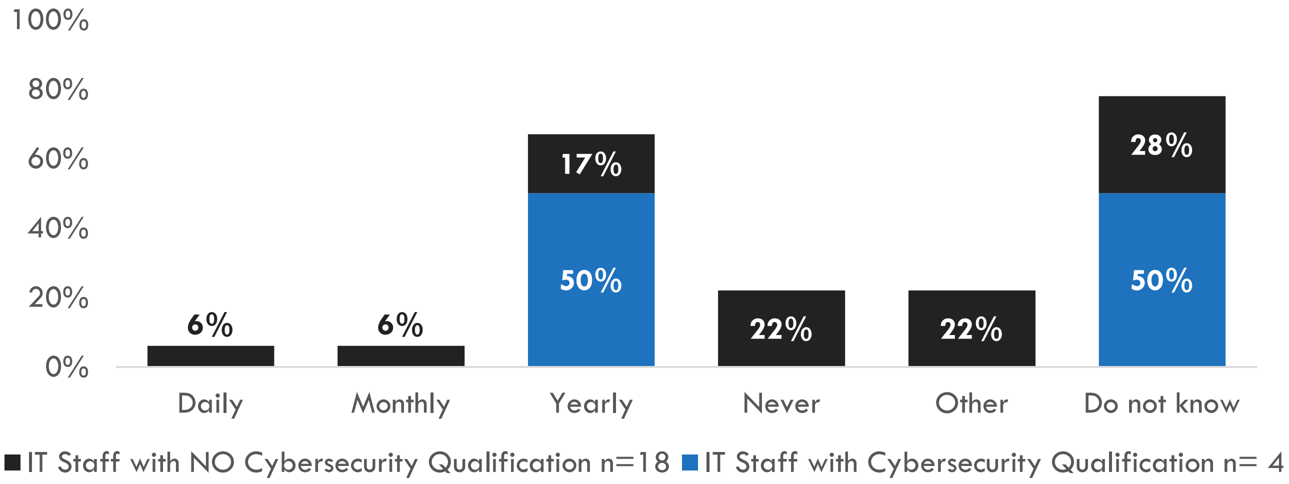


Figure 14: Cybersecurity penetration testing, only IT staff responses

In relation to how organisations manage and maintain an inventory of end user devices and what information is being accessed and by whom (Figure 15), 43% kept a central register; another 22% decentralised this responsibility to departments or individuals. Of concern was that 35% were either unaware of any process or were certain that no tracking procedure was in place. Patients place their trust in our healthcare services to safeguard their information and ensure it is not accessed inappropriately. As healthcare continues to digitise, this is an area they may need to improve.

Q24. Does your organisation track and classify all digital devices that access information (computers, tablets, communication devices, etc.)?

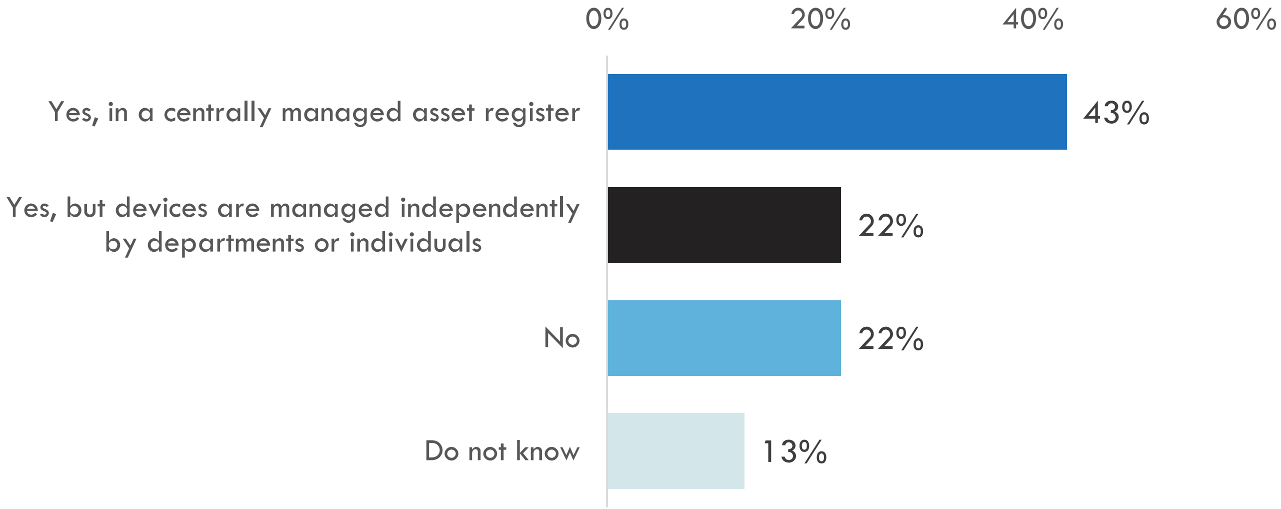


Figure 15: Digital device tracking

General Cybersecurity Practices (Q25-35)

When looking at who can install software across the organisation (Figure 16), almost two-thirds (58.9%) of staff reported that only IT administrators can install software. More than a fifth (22.6%) of users were able to install from an approved list, but of concern almost an eighth of respondents (12.1%) reported an ability to install whatever software they required, which poses a significant security risk. Analysis by organisation showed notable variation. Interestingly, the IT Vendors or Device Manufacturers, and Research and Academic organisations were far more flexible than healthcare providers.

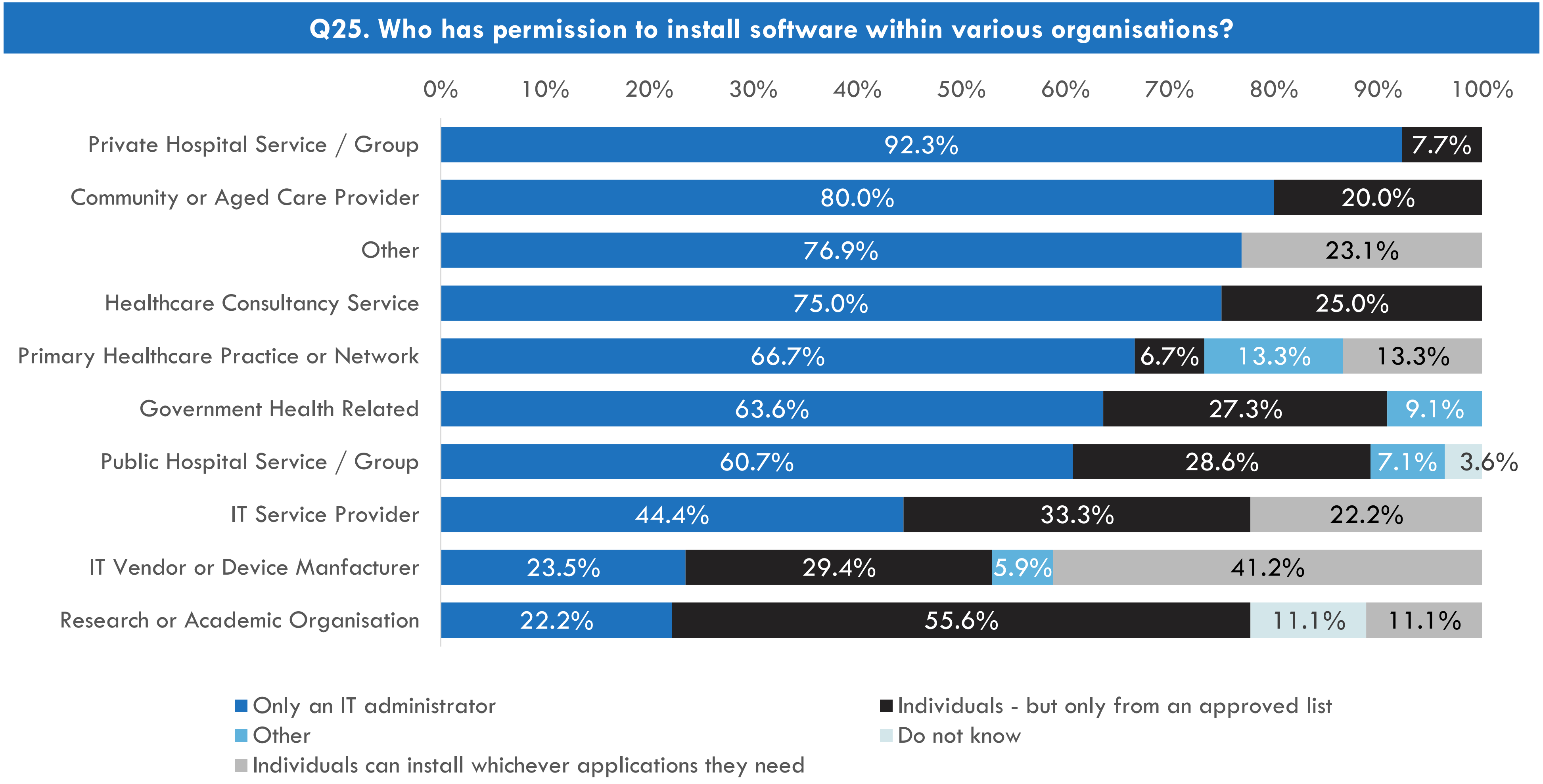


Figure 16: User permissions, by organisation

Risk of data breaches increases with operating systems that are not updated regularly. When looking at how soon operating system patches and updates were available to end users once deployed (Figure 17), 40.2% of organisations would have them within 48hours, another 31.8% only after extensive testing by the IT team, 15.5% after a few weeks and 6.2% not at all because of legacy and end of life systems. While 6.2% may seem small relative to the other organisations, if the organisations within the 6.2% was a major tertiary referral hospital, the implications for patient care may be significant in the event of system failure. Should we tolerate health care services operating end of life systems at all?

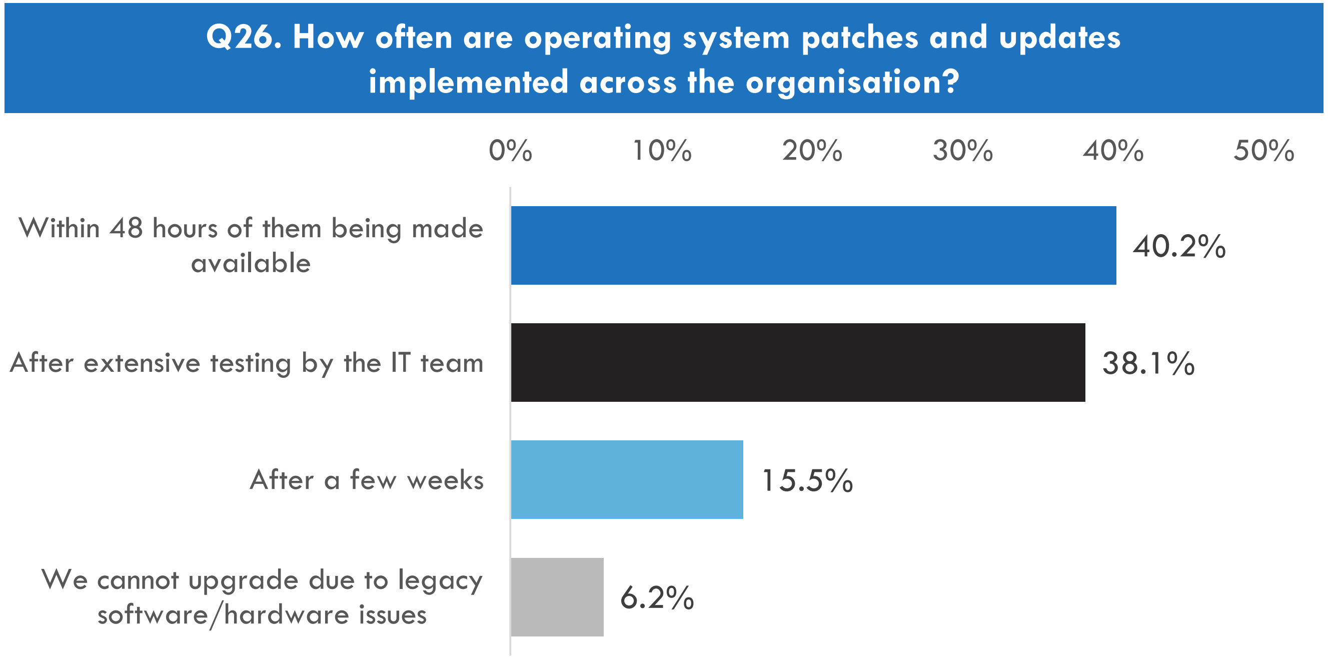


Figure 17: Patch frequency

In the majority of cases (77.9%), responsibility for performing operating systems patches and upgrades primarily sat with the organisation's IT team or IT service provider (Figure 18). In 12.2% of organisations, software or hardware vendors or 9.9% of end users would perform these.

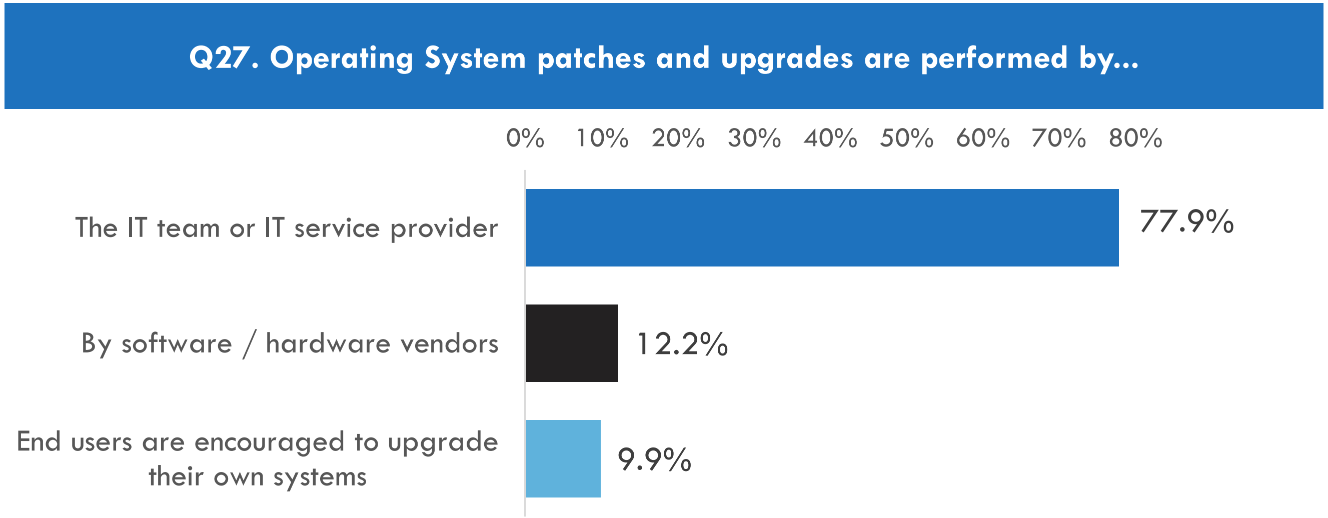


Figure 18: Responsibility for patches and upgrades

When asked how administrator privileges for systems and software were shared (Figure 19), in 77% of organisations only system administrators, management or super users would have this access. In 19% of cases system controls were very loose with individuals able to tinker in the backend of their own systems and devices if they desired. Only a very small proportion had no idea (3%).

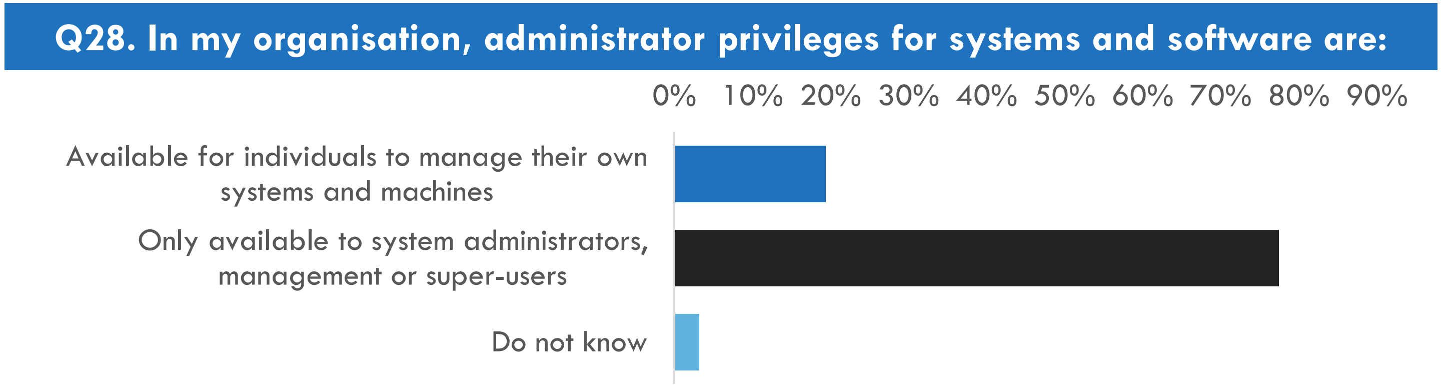


Figure 19: Administrator privileges

The results below raise some questions about the practice of generic logins (Figure 20). Does this increase a hospital's risk to security breach? Would there be a case to setting standards for use of generic passwords?

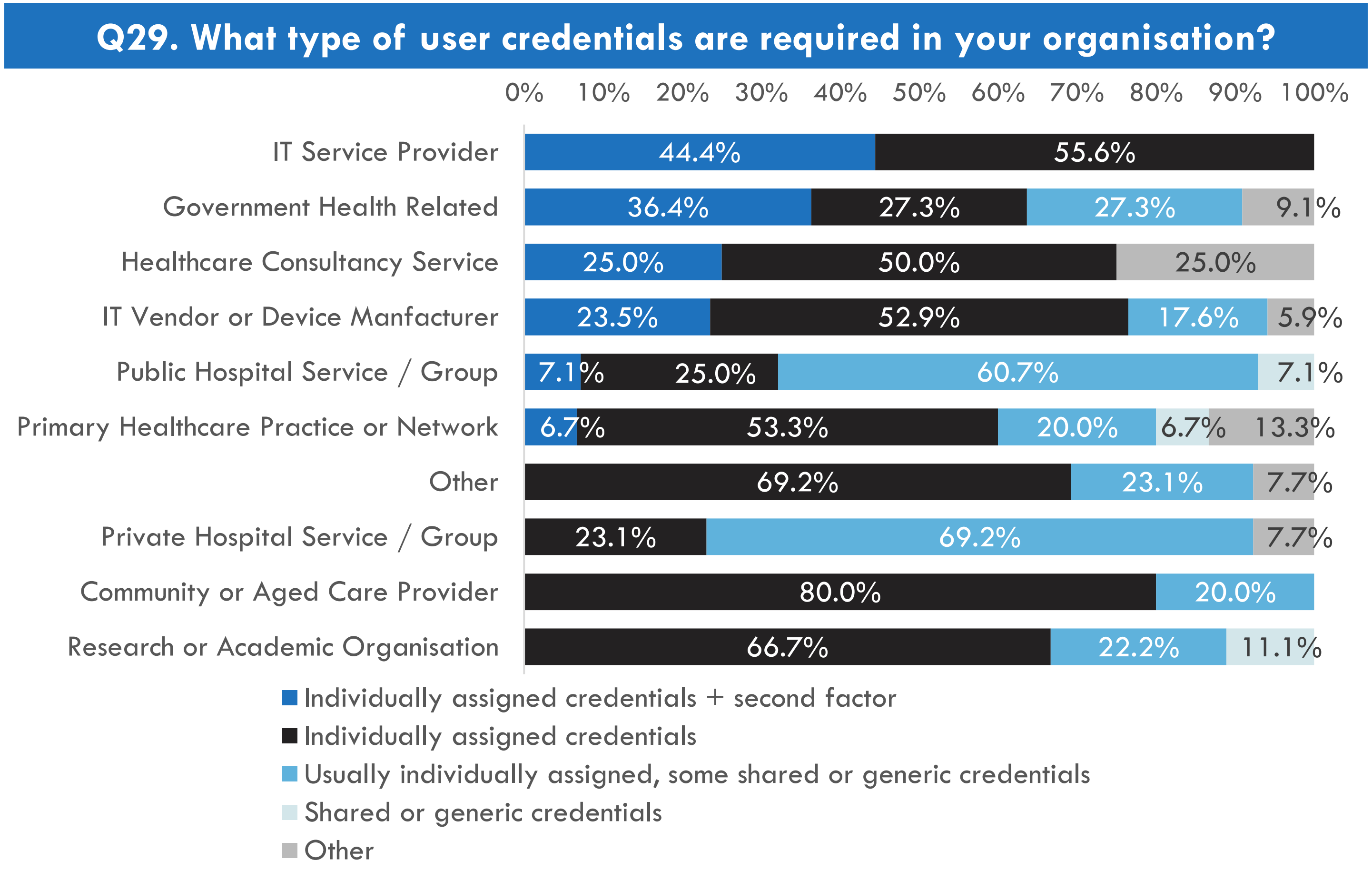


Figure 20: User credentials

Q29 Other Responses	Freq.	%	Valid %	Cum. %
	150	95.5	95.5	95.5
A mix of code generator app & biometric second factor, and great use of SSO so there is no compromise in user experience	1	.6	.6	96.2
Full spectrum. Mostly individual credentials, some with 2nd factor. But some shared passwords required as some systems requiring multiple people to perform tasks only support a single admin account.	1	.6	.6	96.8
In theatre we have auto-login machines (generic credentials); at the patient's bedside (point of care) we have biometric logins; on the ward at nursing stations, ED/ICU work areas and other non-clinical areas we have standard AD managed usernames and passwords.	1	.6	.6	97.5
Mixture, depending upon use case. On-prem LAN access is credential only, but external access is physical token. All credentials are fully managed. We also have all have a fully corporately managed O365 cloud credential.	1	.6	.6	98.1
There is a mixture of individual and shared logins. Moving to individual at the moment.	1	.6	.6	98.7
This is not a good question to ask, as it then makes this data highly attractive for attack.	1	.6	.6	99.4
username and password internally, with small amount of generic. Biometric used in some areas. All remote access requires 2 factor.	1	.6	.6	100.0
Total	157	100.0	100.0	

The following results (Figure 21) show that only 34% of organisations will refresh their systems and hardware prior or shortly after vendor support ceases. For the rest, an “if it ain’t broke then don’t fix it “mindset may exist with 22% of organisations continuing to use legacy and end-of-life systems without vendor support. Another 12% also continuing to operate legacy and end-of-life systems and hardware but with an agreement for ongoing vendor support. The remainder have no idea (26%) or selected “other” (6%) suggesting some variation on the other options although they probably have no idea either.

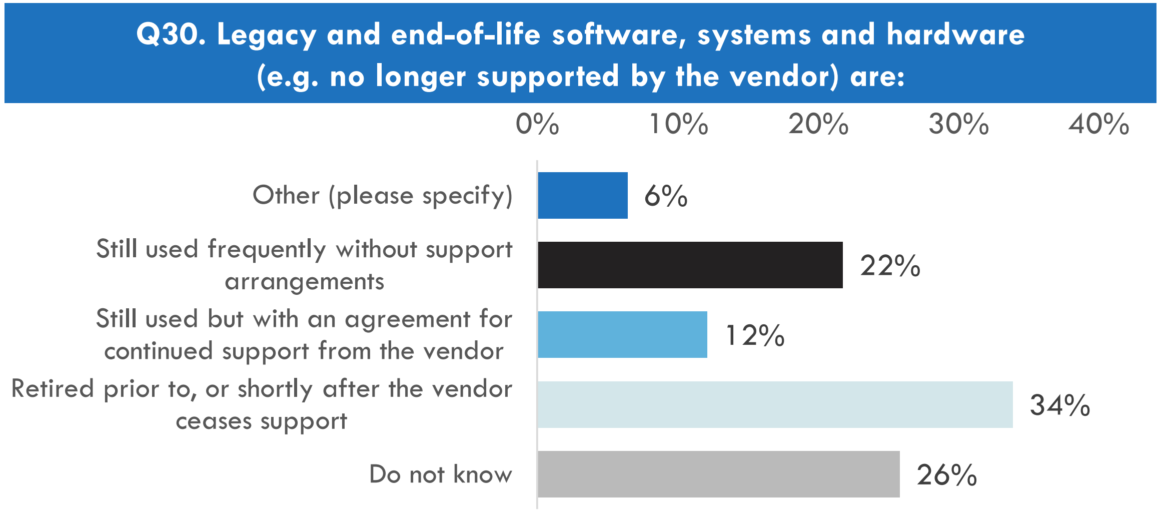


Figure 21: Legacy and end-of-life software, systems and hardware

Q30. Other (please specify)	Freq	%	Valid %	Cum. %
	149	94.9	94.9	94.9
Hardware support is by an external provider on a 24x7x2hr basis. MS software used up to the end of extended support.	1	.6	.6	95.5
Legacy systems that prevents patches being applied to operating systems. i.e application only run on 2003 servers.	1	.6	.6	96.2
n/a	1	.6	.6	96.8
No known instances have occurred to date	1	.6	.6	97.5
Not exactly sure, but it varies I think.	1	.6	.6	98.1
The nature of many open source modules that contribute to our technology mix is there is no vendor, and in some cases no ongoing development or user support forums. Naturally these are only peripheral bits of functionality and not central to the running of our business. Given time and available alternatives, these would typically be replaced as and when problems arise....but "if it's not broken, don't fix it" still usually applies.	1	.6	.6	98.7
usually extended support however for some support is no longer available but upgrades cannot occur due to specialised medical equipment requirements.	1	.6	.6	99.4
We have a software, system and hardware refresh program, however there are some systems and software that we struggle to upgrade. These have been isolated from the internet, though some are vulnerable to physical vectors.	1	.6	.6	100.0
Total	157	100.0	100.0	

When asked how individuals were issued devices at their organisations (Figure 22), the majority (33%) were supplied a device approved by management. Some organisation did offer choice from a pre-approved selection of devices (25%) or offered some choice to bring their own device provided it was on the pre-approved list (14%). In 23% of cases, individuals were able to bring any device without restriction or approval needed.

Q31. Individuals who require a laptop, tablet or mobile phone in my organisation are

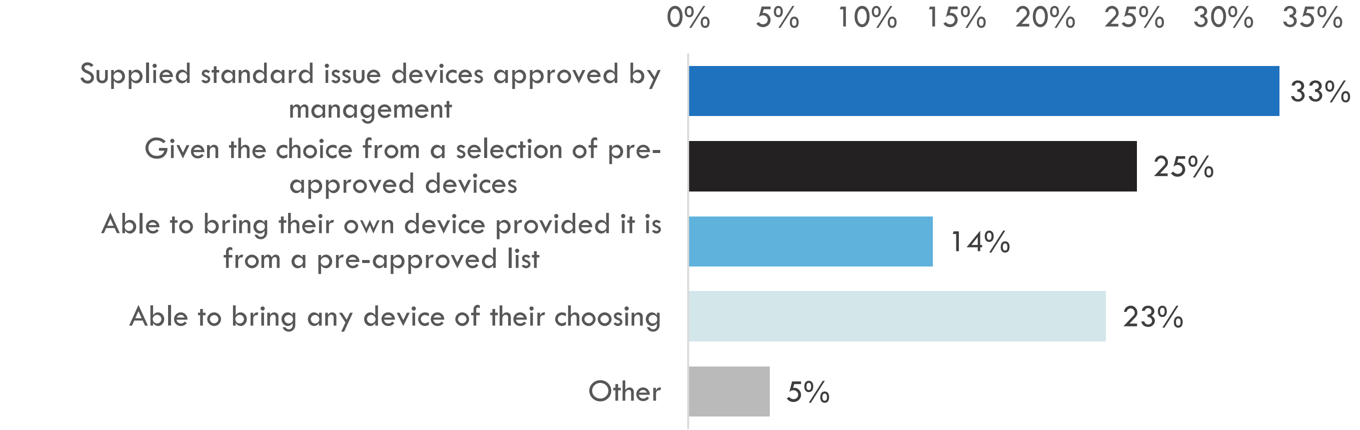


Figure 22: Mobile devices

In an increasing digitised world, individuals will use work devices for personal matters such as online banking, watching YouTube clips or checking Facebook (Figure 23). The extent to which this occurs once or twice per week is 41%, with up to 43% using more frequently such as almost daily (24%) and daily (19%). Only 15% declared never using work devices for personal use.

Q32. How often do you use your work computer, laptop, tablet or mobile phone for non-work related tasks such as online banking, watching YouTube, checking your personal email and/or social media such as Facebook?

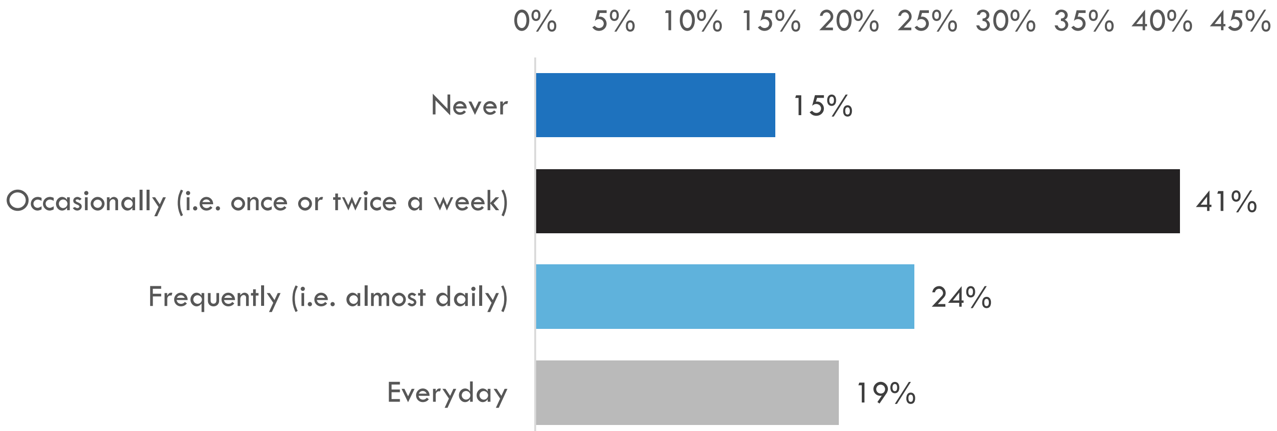


Figure 23: Work devices for non-work uses

In response to the question of what happens to devices that are no longer required, lost, stolen or when someone leaves (Figure 24), in many cases (38%) the device's memory would be erased and reset for the next end user. In other cases, organisations had remote capability to remove files and apps from the device (29%), disable and put an activation lock on the device (16%) or locate the device (13%).

Q33. When devices are no longer required, lost, stolen or when an individual leaves the organisation:

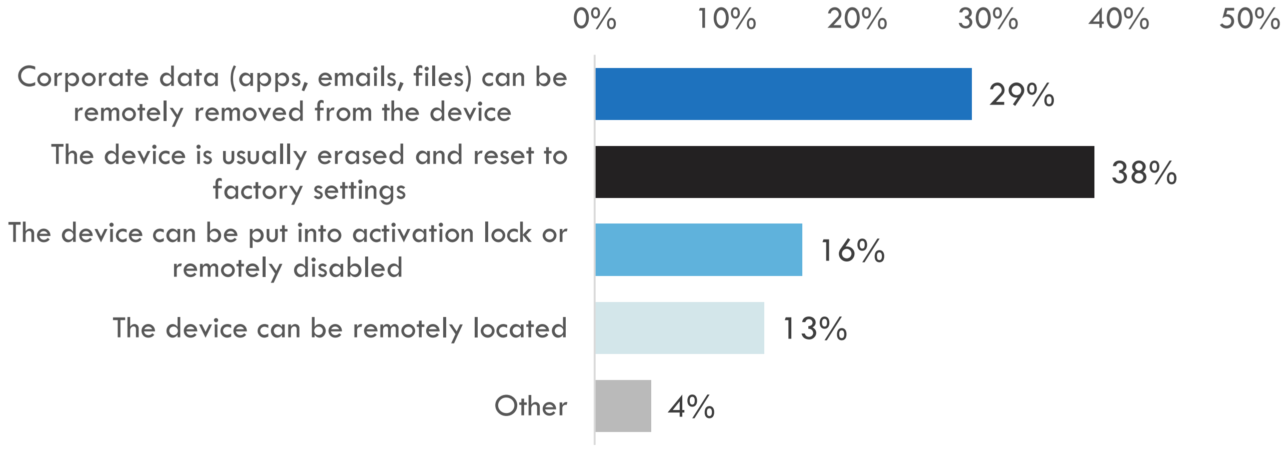


Figure 24: Management of data on devices no longer in possession of the organisation

When asked about the greatest concern for biomedical device security (Figure 25), the top four responses were: data breach (28.7%), patient safety (28.0%), spread of malware (24.2%) and device theft or loss (14.6%). Intellectual property (8.3%) or liability (7.0%) were much lower areas of concern.

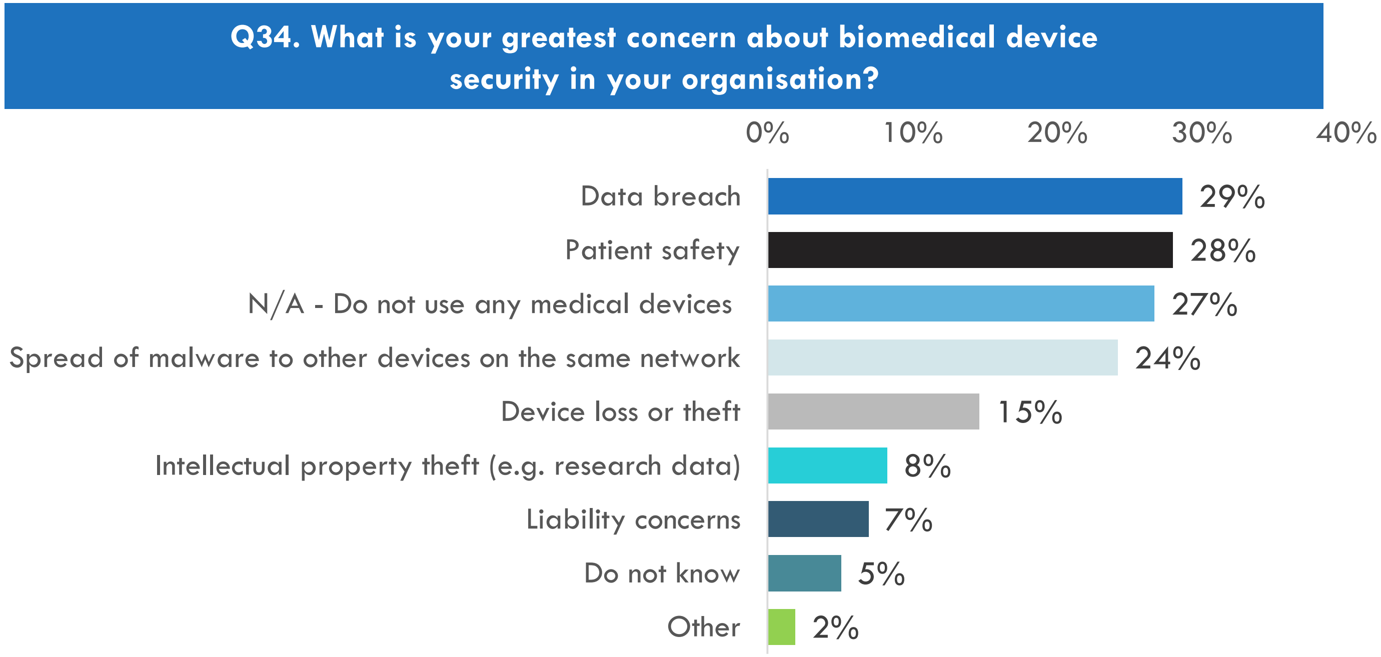


Figure 25: Biomedical device security concerns

The practice of backing up systems and data (Figure 26) on a daily basis was high at 84%.

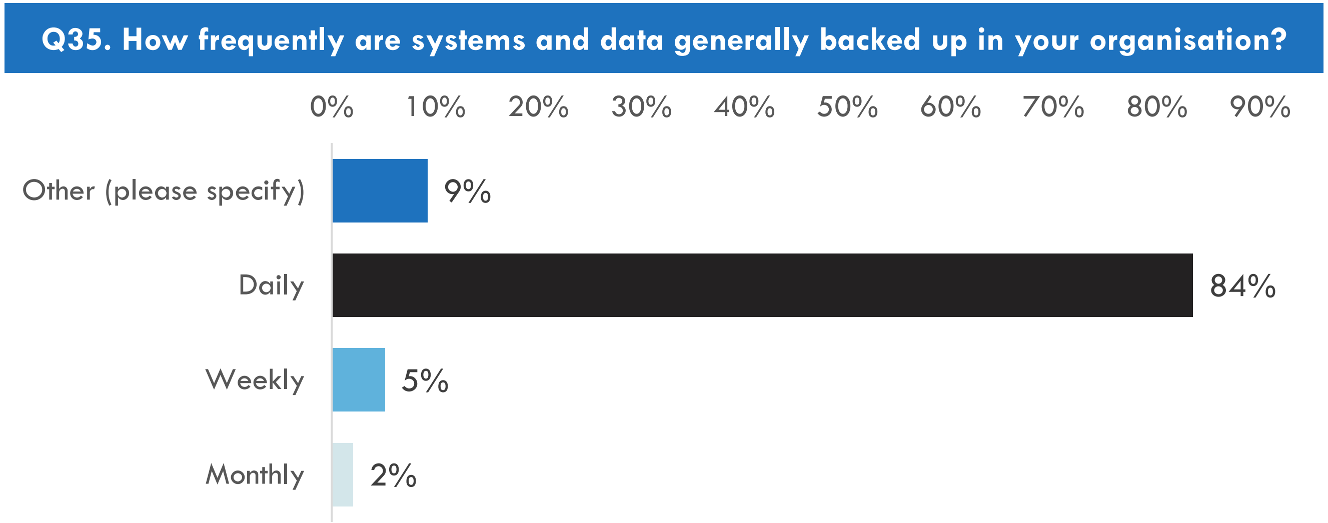


Figure 26: Back up frequency

The HISA Cybersecurity Community of Practice will be:

Conducting annual cybersecurity surveys to provide benchmark data and to monitor progress in strengthening cybersecurity practice across Australia's health sector

We will continue to work with healthcare organisations that provide their data for these surveys to provide insights into cybersecurity practice in their organisations and across the sector.

There are opportunity for individuals and organisations to support our work and we encourage those interested to get in touch.

www.hisa.org.au
hisa@hisa.org.au
+61 39326 3311

ABOUT HISA

The Health Informatics Society of Australia (HISA) is Australia's peak professional body for the digital health, e-health and health informatics community.

HISA members represent a broad and diverse stakeholder community including clinicians, researchers, healthcare managers and executives, data analysts, designers, project managers, business analysts, technologists, innovators and health informaticians.

With clinical alliances, corporate collaboration, education sector support and strong government relationships, members have unlimited opportunities for career advancement and professional development.

As a leading member of the global health informatics network, HISA is also the forum for sharing international best practice, digital healthcare trends and health system innovation.

www.hisa.org.au hisa@hisa.org.au

HISA AUSTRALIA'S DIGITAL HEALTH COMMUNITY