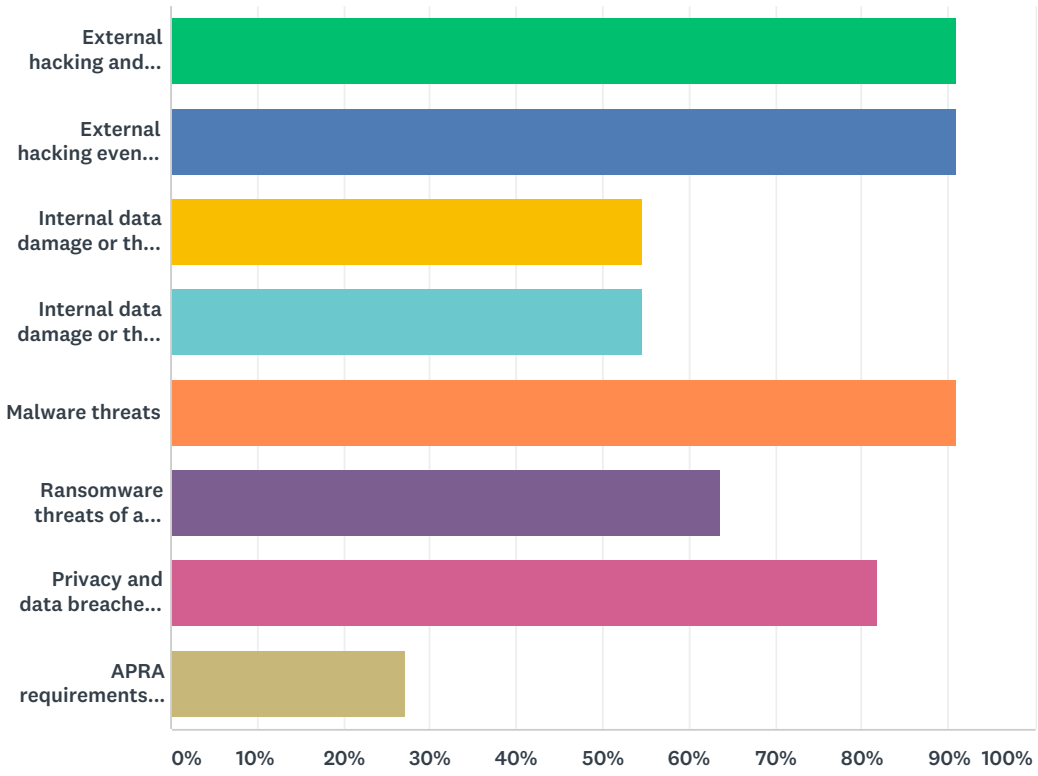
Q1 What are the areas of cyber security that you are concerned about for your organisation - you can tick as many as are applicable

Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
External hacking and theft of data or IP	90.91%	10
External hacking events that disable core technology processes	90.91%	10
Internal data damage or theft - deliberate	54.55%	6
Internal data damage or theft - accidental	54.55%	6
Malware threats	90.91%	10
Ransomware threats of all varieties	63.64%	7
Privacy and data breaches generally	81.82%	9
APRA requirements for Directors being fully understood	27.27%	3
Total Respondents: 11		

#	OTHER (PLEASE SPECIFY)	DATE
1	Regulatories compliance	3/24/2019 3:23 AM

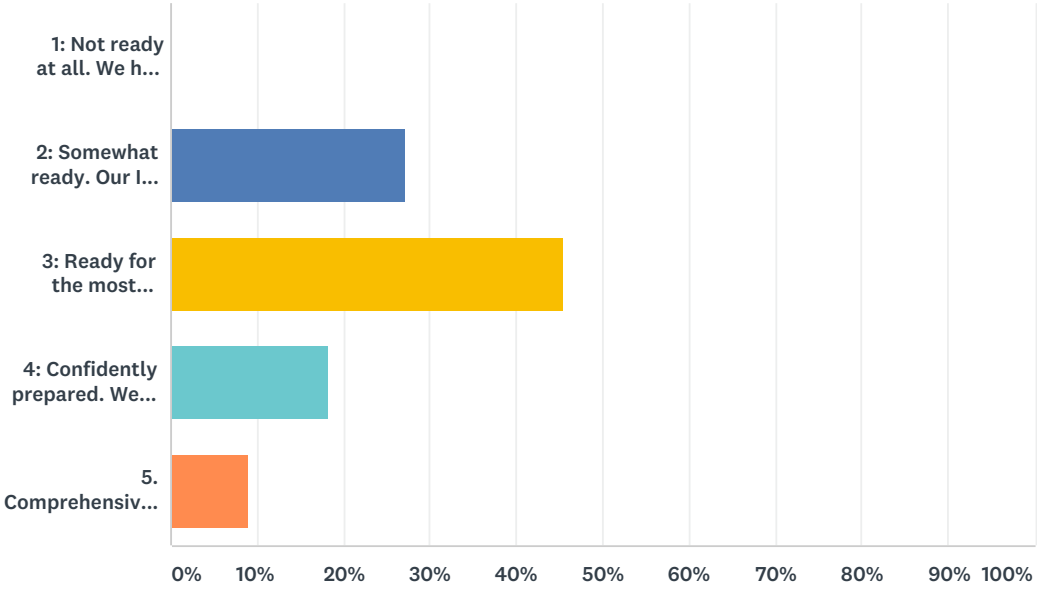
Q2 What is the one cyber issue that is keeping you awake at night?

Answered: 10 Skipped: 1

#	RESPONSES	DATE
1	3rd Party Breaches	3/26/2019 9:44 AM
2	Internal Threat.	3/24/2019 3:23 AM
3	External	3/22/2019 6:55 PM
4	Data breaches - hacking	3/20/2019 8:39 PM
5	Privacy and Breaches threats	3/20/2019 8:10 PM
6	Privacy and data breaches	3/20/2019 12:20 PM
7	That the IT Security expert's view is incorrect (i.e. that recovery would be easily done in a few days by wiping everything and restoring.	3/20/2019 12:07 PM
8	cost - benefit of prevention	3/17/2019 2:05 PM
9	my financial online accounts	3/14/2019 6:44 PM
10	Lack of appropriate skill sets	3/11/2019 12:09 PM

Q3 Please rate your organisation's maturity in regard to preparedness for a cyber incident or issue

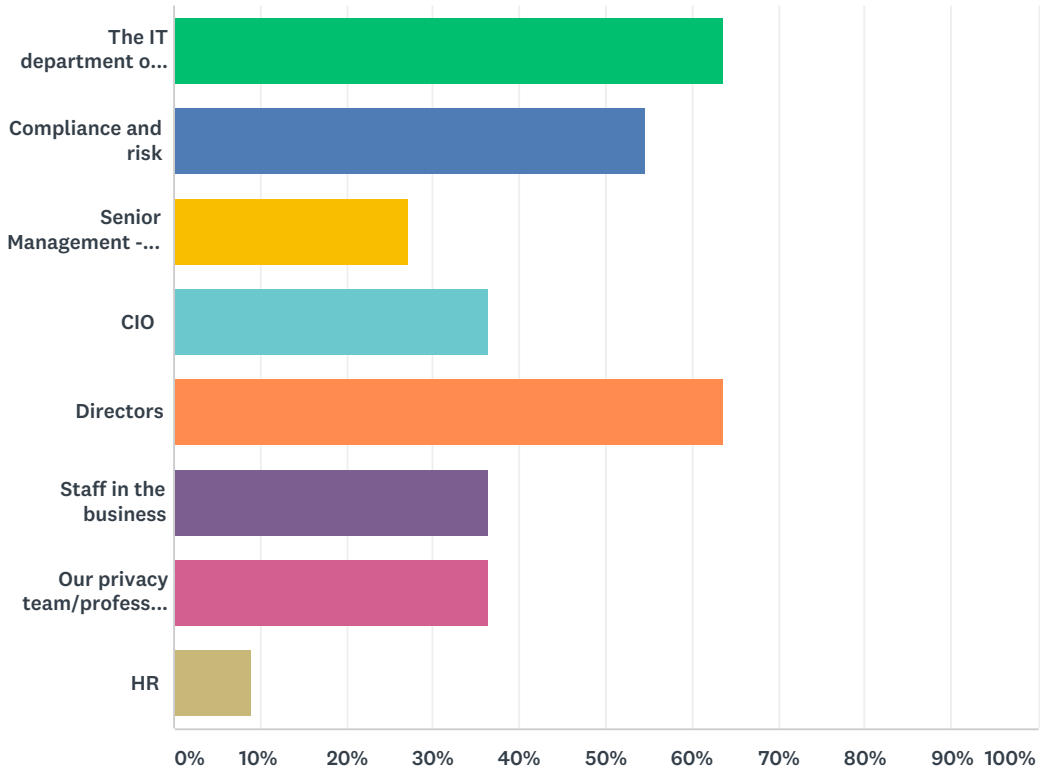
Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
1: Not ready at all. We have some virus protection and a firewall established by our IT department/supplier	0.00%	0
2: Somewhat ready. Our IT department/supplier has briefed us on some key risks and we have a plan and some aspects of that plan in place. There are some policies in regard to specific risks and privacy.	27.27%	3
3: Ready for the most obvious risks. We have an active IT program for external threats and some staff awareness in regard to policies around privacy, device use and security, suspicious emails and things like that. We have an action plan for a privacy breach. However, we don't know what we don't know, and we are aware that there are probably emerging risks we aren't aware of, or prepared for.	45.45%	5
4: Confidently prepared. We have reviewed and understand our key cyber risks and have trained staff and put in place technology solutions to mitigate these risks, as well as robust policies and procedures and action plans in case of a live incident.	18.18%	2
5. Comprehensively prepared. We have conducted a wide ranging review of exposure and cyber risks and continually review and update, given the rate of change in this space. We have technology systems established to mitigate risks, monitor potential incidents and near misses and have had these tested by an independent external party. Similarly, our policies and procedures are well established and business actively engage with these and the training and communications we provide. We have also run through comprehensive scenario and live crisis testing in our key risk areas. Our directors are fully informed of these activities, monitoring results and crisis testing results and planned improvements.	9.09%	1
TOTAL		11

Q4 Who is actively taking responsibility for cyber risk in your organisation - including anticipating and assessing risks, establishing systems, educating staff, etc: - tick as many as are applicable!

Answered: 11 Skipped: 0



ANSWER CHOICES	RESPONSES	
The IT department or external supplier	63.64%	7
Compliance and risk	54.55%	6
Senior Management - non IT	27.27%	3
CIO	36.36%	4
Directors	63.64%	7
Staff in the business	36.36%	4
Our privacy team/professional	36.36%	4
HR	9.09%	1
Total Respondents: 11		

#	OTHER (PLEASE SPECIFY)	DATE
1	All of the above.	3/17/2019 2:05 PM

Q5 And any comments or information you think might be relevant below!

Answered: 4 Skipped: 7

#	RESPONSES	DATE
1	BoD and CEO must have care.	3/24/2019 3:23 AM
2	I am concerned about employees exposure to threats	3/20/2019 8:10 PM
3	I am particularly interested in Cyber insurance - when I last reviewed it it was not worth having because there were few instances of it responding and the deductibles made it pointless. Has that moved on? Are there examples of large entities getting significant relied from Cyber insurance that can be shared?	3/20/2019 12:07 PM
4	CPS 234 has really put cyber security in the cross hairs. It's up to risk and compliance professionals to step up to the plate and be able to assist their relevant organisations.	3/11/2019 12:09 PM