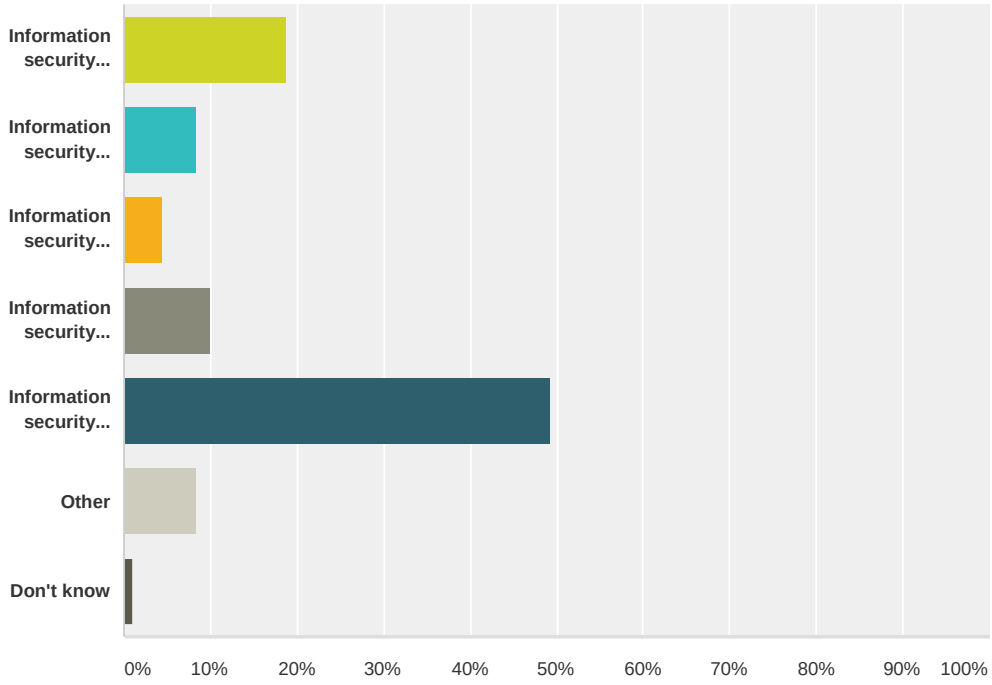
Q6 Which of the following comes closest to your opinion?

Answered: 181 Skipped: 1



Answer Choices	Responses	
Information security incident response should be led by the IT department / business unit	**18.78%**	34
Information security incident response should be led by the business continuity team	**8.29%**	15
Information security incident response should be led by the Board	**4.42%**	8
Information security incident response should be led by the risk management team	**9.94%**	18
Information security incident response should be led by a team consisting of representatives from different areas of the organization	**49.17%**	89
Other	**8.29%**	15
Don't know	**1.10%**	2
Total		**181**

#	Optional: Please explain your response to this question
1	The response should always be led by those impacted with support of the organisational specialists
2	There are lots of aspects to an IT security issue. Response will require Risk, IT, PR, HR, BC and the business to work together.
3	Every incident should be managed by an incident response teams jthst deploys technical, logistical, managerial, and specialized teams as needed.
4	A joint effotr across Incident management (Technical and Business response) in the first emergency stages then include legal and risk teams as required.
5	Response to an incident relies on Infosec team, Recovery relies on the business units affected in conjunction with Infosec and IT if technology is impacted.
6	Same comment as above.
7	Led by IT but with strong partnership / collaboration with other key areas ie business continuity, risk management, crisis management team,

8	A breach will in most cases impact the entire enterprise. Response will include addressing the technical, operational, employee, and stakeholder impacts of the breach.
9	See above.
10	The IT security incident response should be led by IT but be overseen by the Business Continuity team
11	The response should be led by the IT Security with other groups providing representation and guidance
12	The Board, responsible for Information Security, must, therefore, be aware of all incidents and have the lead in responses, even though these may be *carried out* by a lower level team / department.
13	This depends on the seriousness of the incident and the adequacy of the plans developed. If plans are robust enough, these can be dealt with under conventional incident response processes, however; where the plans are not robust; do not exist; or the execution of a plan is not working and there is significant business impact, then the incident would be led by the Board.
14	As would any incident, whatever the source.
15	It may be better to have a cross-functional team deal with a situation that arises, so that all various aspects are considered in the response, recovery and communications.
16	Ideally, the same core crisis management team comprising cross-business representatives should respond to all major disruptive events - supported by relevant subject matter experts as necessary - including for information security incidents
17	IT Information Security handles all system related incidents.
18	in todays climate, time is both money and survival.
19	The response should be led by IT respons team, but of course this will trigger crisis management team, which is business continuity team.
20	See my previous response
21	IT, Risk and BCP
22	Information Assurance/Governance should take the lead with representatives from the groups mentioned above.
23	depending on how wide spread, systems effected, risk and reputation are all at risk
24	As above
25	Led by the board as will have to be under GDPR and the requirement to notify in 72 hrs.
26	Business Continuity needs are for their to be sufficient data available to re-start business processes, this is where RPO is important; to support that need for BC the data needs to be secure and uncompromised. Protecting information is not a BC responsibility, but BC needs to be aware/alert/active.
27	It should be led within the Assurance/Compliance department
28	The InfoSec manager is best placed to handle and coordinate the response to an InfoSec incident. Only if the scope of the incident requires a corporate level response would the entire EOC organization be activated and then only selectively
29	The BCM infrastructure allows timely incident response for the cross functional team, with communication channels and thresholds of severity and tolerance built in.
30	There should be a dedicated Information Security team that will lead the response to the incident. Best practive lead by Information assurance lead taking upon defacto standard ISO27001.
31	ISM is also a BCM issue and should work closely. It is good that BCM and ISM report to the same area ideally in Risk or Finance, but better not IT due to independence.
32	Incident response is led by the Information Security Office, they will pull in area specific compliance resource,communications, IT, legal and executives and become the conduit for the communication up and out.
33	We did a scenario exercise earlier this year where our website had been hacked and also some data had been stolen. This involved several teams to manage the incident. Legal, marketing, Executive, info sec, IT platforms, apps and networks and of course Risk and BCP
34	All incident responses should be cross functional to ensure communications and prevent accidental operational impact due to misunderstanding of how everything interacts in our complicated world.
35	The type and severity of a security incident would determine the level of management involvement, consequently a clearly defined escalation procedure should be developed to ensure that senior management are always informed, but involved in the management of the incident when considered appropriate or necessary.
36	Information Security incidents should be led by a dedicated team of certified and experience professionals. An IS team or department should be created led by a Chief Information Security Officer with the authority to oversee, lead, and manage security efforts. The IS Team and CISO collaborates and works with other business areas.

37	It should be led by whoever leads it day to day. In the same way as any other incident there should be a process by which it gets esclated to BCM/Crisis Management.
38	The above depends on the type of incident. A major one would require a multifunction approach. If business' are certified to ISO2701 or 22301 they will have Incidnet Management teams in place which I would expect to be multifunctional
39	The business owns their own risks, hence they should respond to information security incident
40	The BC team should lead the overall incident coordination and response working closely with the IT /BU team.
41	See 4) above
42	you need to understand to over all business impact.
43	See above
44	When it comes to Security Incident Response various represnetatives - RM, IT, BC, HR, etc. needs to work together
45	Tactical responses to security incidents, should initially dealt with by the companies,call centre, help desk, or other single point of contact for all company incidents, then handed over to a Security Incident Response Team (SIRT) for resolution.
46	same question
47	Depends upon the actual event as to which organizational elements are most involved. For example, a data breach response may be led more by Public Relations and Legal, with IT providing subject matter expertise.
48	In our organization: - if an incident dealing with electronic info with no suspicion of actual breach of security, IT handles - if an incident with suspected or actual penetration of electronic systems, incident response team leads - if an incident localized to a few individuals as a result of internal human error or physical security, Privacy Office handles unless determined to be a significant breach at which point incident response team handles
49	while it and risk may take the initial lead, eventually overall response is a multi-departmental issue.
50	For a large incident (i.e. crisis), escalation to crisis management leadership would be expected.
51	An incident can occur anywhere (department) in the organization. The department affected will be able to identify that this is actually a security incident, and should direct remediation efforts. Someone outside of the department may take action that can make matters worse. Also, I believe this is necessary for communication during an incident.
52	Incident response should be led by appropriate management which might be led by different people according to the nature of the incident. IS incidents need to draw upon representation from all areas of the business.
53	All of the above. Initially, IT should lead the response in close coordination with the BC team.
54	Should use the BC response process for Business / Mgt issues but will need its own response teams
55	Depending where the threat is manifested will determine which departments may need to be involved