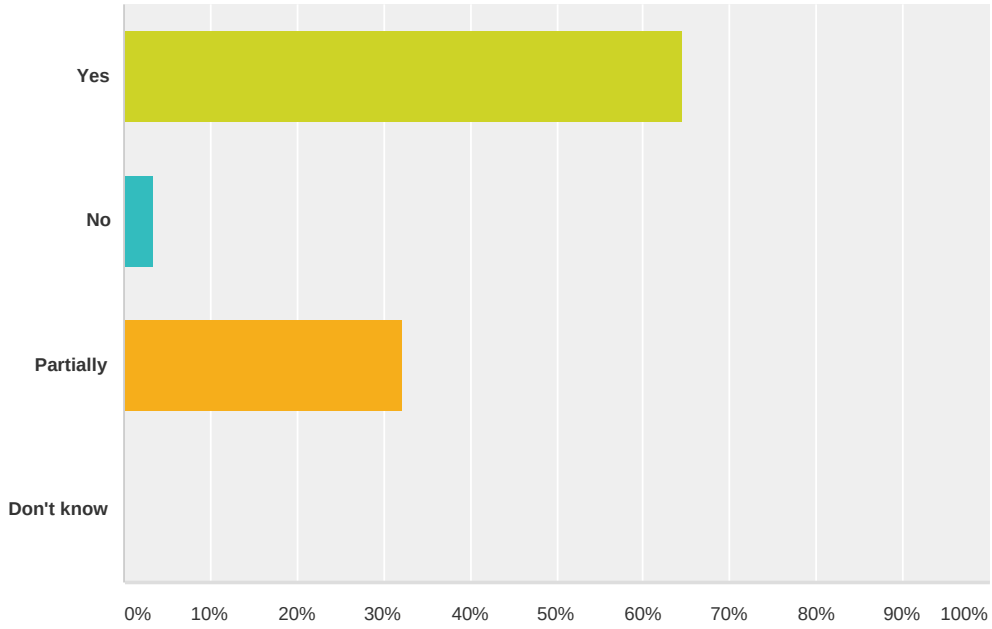
Q1 Do you see information security as a business continuity issue?

Answered: 180 Skipped: 2



Answer Choices	Responses	
Yes	**64.44%**	116
No	**3.33%**	6
Partially	**32.22%**	58
Don't know	**0.00%**	0
Total		**180**

#	Optional: Please explain your response to this question
1	A large data leak could threaten the continuity of the business through reputation damage, fines and civil action. In addition it maybe be necessary to take down affected systems until all issues have been investigated and the system re-secured.
2	As a law firm the confidentiality of our client data is critical and we could lose serious business if we had a breach.
3	Because the norms followed by organization during BAU should be replicated or probably more scrutinized when BCP is invoked.
4	The implication of a cyber attack and response is certainly a BC issue
5	It has always been a source of interruption. There were DDOS attacks on mainframes in the late 70's/early 80's. An Interruption caused by an IS attack is still an interruption.
6	Both are part of an overarching Organisational Resilience Function including Physical and Cyber Security, Incident and Crisis management
7	As Continuity Team, we include Info Security as part of our continuity planning.
8	Availability of information is a key factor in ensuring the business can continue to operate.
9	An example from health care where the two converge: ransom ware attacks that prevent access to patient (and other) operational data
10	While information security is not a direct business continuity issue, there is a strong dotted line. There must be close collaboration and coordination. Information security has as its primary focus to mitigate and prevent security breaches; business continuity manages the impacts a breach has on business operations.

11	Business Continuity needs to be involved when an incident occurs to understand the scope and impact of the incident.
12	it is other way. business continuity is now a security issue
13	BIA should focus information security
14	How can I.S. NOT be a business continuity issue? A loss of data integrity/privacy or complete IT service outage is potentially devastating to a business!
15	Our risk assessments clearly indicated that we are more prepared for data recovery and restoration (a known event) than a security event (an unknown event)
16	Resilience of the business, and therefore its ability to survive major disruption, is dependent upon many factors, one of which is information security, failure of which could cause that disruption.
17	Security must not be compromised in the event of any discontinuity.
18	Information is an important part of a business and crucial for Continuity but information Security is also very wide and can includes separate activities.
19	InfoSec defence can only go so far in mitigating the risk. Good continuity plans are necessary to respond, should those defences fail and impact your business.
20	It is no different from any other threat that requires a response
21	If the business uses an IT tool or application, then it needs to be considered, and possible alternatives identified in the plan.
22	An information security breach poses a clear threat to business-as-usual either through the denial of access to systems or data (be that directly as a consequence of the incident or because of a need to "quarantine" systems as part of the response) and / or because of reputational impacts which may in turn cause business disruption (e.g. large volumes of calls from concerned customers)
23	According to the 2017 Horizon Scan Report, the current global top ten threats to business continuity are: Cyber attack (the same as the 2016 report) Data breach (the same as the 2016 report) Unplanned IT and telecom outages (the same as the 2016 report) Security incident (up one from the 2016 report)
24	they are clearly close cousins to say the least because one gets a cold then the other follows close behind
25	In that the security breaches create a crisis, it is part of business continuity
26	Lack of information security altogether, or an information security program that fails to protect the organization is most assuredly a business continuity/resilience issue. Those organizations that fail to accept this fact are domed to lose it all if a security breach occurs and there are no measures in place to mitigate the breach.
27	A security breach would almost always impact continuity of operations at some level.
28	it might start initially as an information security issue but then move into being a business continuity issue so not as easily defined
29	Maintenance of ISM issues in a continuity event
30	It is an IT function, not managed by Bus Cont....you are either a Bus Cont Leader or an IT professional. Events are managed by Bus Cont, IT is a function that has to coordinate through an event with everyone else.
31	Yes, although not ownership for resolution or management, I rely on experts to do this but mindful of reputation and business impact information security incidents may have on an organisation.
32	It depends on how an attack or breach occurs. What's the effect on the business.
33	Information security issues in themselves do no disrupt operations, but have the potential to. InfoSec matters one of those horizon scan topics to keep an eye on.
34	Information Security has a link with the loss of information / unauthorised use etc. which can lead to disruption of the business.
35	A breach or DDoS attack can affect a workplace environment causing the relocation of mission critical processes to their alternate worksite depending on the network, ASP, etc.
36	Information security is part of the core infrastructure. To the extent that without InfoSec it would be impossible to perform most other processes, an impact in this area would trigger a continuity event.
37	Could lead to BC issue
38	The BC team would facilitate the response and support the InfoSec team that would have activated the InfoSec specific Incident Response Plan. Should the incident impact expand in scope, the BC team may activate the corporate level BC Plan along with the full EOC.
39	Information are resource needed to run a business. Availability of information (which is one of the pillar of infosec) is also a pillar for bc.

40	Business continuity covers across organizations. Whether that is Info Sec, IT or other business functions.
41	Depending of the impact, a information security incident may affect to operational or reputational continuity
42	High financial impact
43	When we had a cyber attack in the previous organisation through DDOS internet banking plus other web services were unavailable, which was a business continuity issue.
44	I believe that from the moment the information leaks can expose the company at critical risks the IS is part of BCM.
45	Information Security is a close partner to the BC role, it can assist in the rating of risks and recover responsibilities.
46	A loss of data is a potential threat to the business and so becomes a continuity issue
47	We work closely with IT Security; but our BC Plan is exclusive of the DR plan. We are ready to setup if out HQ is inoperable and assume the data center will be up. That said we have had 3 incidents in the past 24 months where IT security nearly shut operations.
48	If a security threat could impact the critical functions of operations within a company to cause outages or data to be compromised then it is my feeling it is a Business Continuity issue.
49	With the ever increasing cyber security threat, if information security is not taken seriously or mitigation measures not implemented (or kept up to date), then the organisation could suffer from loss/theft of its own and client data, ultimately leading to reputational damage and a loss of client confidence. It could also lead to punitive financial impacts from the Information Commissioner's Office (ICO).
50	Cyber and information security are increasingly becoming the biggest threats to an enterprise. A recent threat matrix determined that a cyber event is the most likely cause of a business interruption for the company I work for. It's a matter of when not if with cyber and information security incidents.
51	If there is an IS incident occurs then BC gets put into place for the management of the incident. The two do go together as activities
52	Info Security has the potential to cause distruption in the same way as other types of incident like extreme weather or a utilities failure. BCM therefore has a responsibility to ensure that plans are able to respond to such an event like any other disruptive event.
53	Security breaches can cause Continuity issues
54	An Info Sec breach or issue could soon become a BC one
55	Business continuity planning addresses areas of key risk; information security breaches are a high risk.
56	Since information security is about availability of information I see connections to BCM since BCM is about availabitiy of operations
57	Yes, especially if it has direct impact to the business, branding, operations and staff.
58	InfoSec has to address the effect of the loss or breach upon owners or users of the Info. InfoSec has to alert IT for defencse and repair of the breach. Business Continuity has to address parallel and consequential emerging risks and damage to reputation.
59	Business Continuity 'Management' is (or should be) a holistic discipline covering the ability of an entity to 'continue' with minimal disruption whatever the cause & therefore should cover all potential adverse events - albeit with the expert assistance of individual discipline experts e.g. IT, Operationa Security etc.
60	It is part of business operations and the risk has to be addressed.
61	Due to IS issues service delivery has got disrupted.
62	The specialization required by the Information Security personnel will also be a reality. From business continuity prospective I believe the impact be of interest to BC folks
63	Severe impact to the Organisation (regardless of the subject of say, info security) which result in disruptions of its services is a BC issue.
64	If information is compromised, the business has to undertake several steps to "recover" which may interrupt operations, impact efficiency of operations, require new processes, and impact the customer experience causing long term changes to the entity. Given these points Information security is certainly an issue the BC professional must be cognizant of .
65	Good information security is about ensuring the confidentiality, integrity and availability of information.
66	You have to maintain adherence to the same information security classification levels throughout any recovery procedures.
67	Any impact on the ability of my organisation to access or have confidence in the integrity of its information affects the ability of the organisation to provide its services.

68	Information must be maintained securely to ensure business operations continue unabated. Most business operations are driven by some level of software, including WAN and LAN operations and manufacturing processes. Without adequate information security, Intellectual Property is at risk, data integrity becomes suspect and product integrity can be compromised.
69	Cyber risk is one of the largest BC risks facing organizations. Understanding the program, who has critical data and personal info, and the protections of the organization with custody of that info is necessary to ensure all parties are geared up should a breach occur.
70	anything that can impact the business is a buc issue
71	Partially, with a role to play in the response to the business disruption that may potentially arise from an information security incident.
72	I can understand and respect someone disagreeing with me, however, I say yes because the availability of data, when you need it, is a part of the security CIA triad. When you have to follow government regulations like HIPAA's "Security" Rule, this is required.
73	It can be
74	Information security is a threat to our organizations and, therefore, a business continuity issue. This is an area in which BC and DR must collaborate and cooperate as it includes technology, operations and PEOPLE. It is a business management as well.
75	From a levering of the response process and handling the business impact, reputation of the wider crisis management process. But the core ISM activity is related and best handled by specialists.
76	Because it ultimately could impact the reputation of the company and all roads leads to BC....
77	Everything can be considered a business continuity issue. Organizations assign roles and responsibilities differently, often depending on the organization's size.