The Organisation Information & Employees		Write your responses in the blank space provided below
1	Name of Organisation	
2	How long have you been working for this organisation?	
3	What position do you occupied?	
4	How long did it take to notice breach detection gap (the period in between the beginning of the breach and the discovery of the breach)?	
5	Why did it take this amount of time to detect the breach(es)?	

Cyber Security & Policies		Mark x in the respective question boxes below				
		less 3 months	within 3 to 6 months	within 6 to 1 year	within a year to 2 years	2 years & More
5	Are there policies or documentations for cyber security created, updated, or reviewed to be up-to-date within which period?					
	Before breach time, were there any policies or documentation for cyber security last created, updated, or reviewed to be certain they were up-to-date within which period?					
	When the last time cybersecurity training or awareness traising session was was carried out?					
	Prior to the time of the breach, when was the last time you carried out any cybersecurity training or awareness raising sessions?					

7	Please answer the following questions about breach detection time (the length of time between when a breach occurs and when it is detected)					
	Mark X in the respective question boxes below					
	Likert Scale	Disagree	Mostly disagree	Neither agree nor disagree	Mostly agree	Agree
	Technology impacts breach detection time in general.					
	Corporate and government policies impact breach detection time in general.					
	Human error impacts breach detection time in general.					
	Technology impacts breach detection time at my organization.					
	Corporate and government policies impact breach detection time at my organization.					
	Human error impacts breach detection time at my organization.					

8	State of technology at your organization prior to the breach or breaches.					
	Mark x in the respective question boxes below					
	Likert Scale	Disagree	Mostly disagree	Neither agree nor disagree	Mostly agree	Agree
	My organization has adequate cyber security technology					
	Cyber security technology is applied efficiently at my organization					
	Cyber security technology is applied effectively at my organization.					
	My organization has good cyber security configurations.					
	My organization's digital operations are secure.					
	My organization has good cyber hygiene practices.					
	My organization makes use of (an) intrusion detection system(s).					
	My organization's IDS works					
	My organization frequently updates its software.					
	My organization makes an effort to secure remote services like VPNs.					
	My organization's remote services include adequate unauthorized access controls.					
	My organization's online services are properly configured.					
	My organization makes use of authentication tools.					
	My organization routinely backs up information.					
	My organization encrypts sensitive or private data.					
	My organization stays up-to-date on the latest vulnerability and patch updates.					
	My organization uses antivirus software					
	My organization has established centralized log management.					
	My organization has adopted a zero-trust security model.					
	My organization controls who has access to our data and services.					