Cybersecurity Assessment Questionnaire

This comprehensive tool covers the key questions needed to accurately assess an organization’s cybersecurity posture

IDENTIFY		
	Q	**A**
1	Do you have visibility of all connected users, devices, data and services across your network? **ID.AM**	
2	Is your approach to cybersecurity correctly aligned with the needs and objectives of your organization, taking into account regulatory and legal requirements? **ID.DE and ID.GV**	
3	Are you regularly performing risk assessments to measure your threat exposure (including those from your supply chain, users, business partners and customers)? **ID.RA. ID.RM ID.SE**	
4	Are you correctly insured against any damage or loss from cybersecurity incidents, including employee negligence or insider threats? **ID.RM**	
5	Is your organization compliant with the industry's and/or region's cybersecurity operational requirements, as appropriate? (e.g. HIPAA, PCI, GDPR) **ID.GV**	

PROTECT

	Q	A
6	Do you centrally manage and monitor all user accounts and login events on your network? **PR.AC**	
7	Can you monitor and manage all file permissions on your network to ensure that data sets are only accessed by active and authorized users? **PR.AC**	
8	Do you prohibit account sharing across all services and users as part of your information security policy? **PR.AC**	
9	Do you control and monitor what applications your users are allowed to install and use? **PR.AC**	
10	Do you enforce best security practices, such as unique complex passwords, multi-factor authentication, and where advisable, single sign- on to users? **PR.AC**	
11	Do you have an up-to-date inventory of all third-party applications running on your system, including their patch level? **PR.AC**	
12	Do you allow IoT devices such as digital assistants, smart white goods etc. to connect to your network? **PR AC**	
13	Do you prevent users from connecting non- authorized devices to your network (physically or wirelessly)? **PR.AC**	
14	Have you renamed or disabled default accounts and passwords for all devices, services and software, including IoT devices (e.g. smart white goods, wearables, digital assistants, etc.)? **PR.AC**	
15	Do you allow "Bring Your Own Device" (BYOD) at your organization and if so, do you have an up-to- date policy to manage and control their access to your services and data? **PR.AC**	

16	Do you allow users to access your network remotely (e.g. from home or while travelling), and are you confident the connection is properly authenticated, encrypted, and tracked? **PR.AC**	
17	Can you remotely access, configure, audit, track and securely wipe any devices you allow on your network, even when they are outside of your network? **PR.AC**	
18	If you provide guest access to your networks, do you provide segregation from your critical systems and sensitive data? **PR. AC**	
19	If you are storing any data in the cloud (e.g. AWS, Google, Office 365, etc.), have you used all available tools and best practices to harden its security? **PR.AC, PR.DS**	
20	Do you track all systems, services, users, and contact lists to ensure anything unwanted or expired is deactivated or disabled? **PR.AC, PR.DS**	
21	Are all users given regular cybersecurity awareness information and training, covering how to avoid the latest threats (e.g. malvertising, cryptomining, phishing, social engineering, and ransomware techniques)? **PR.AT**	
22	Do you perform regular staff testing to identify poor security practices (e.g. simulated phishing attacks)? **PR.AT**	
23	Do you encrypt all sensitive traffic? **PR.DS**	
24	Do you encrypt all sensitive data? **PR.DS**	
25	Do you have a reliable and regularly-tested backup and restore strategy for all important data and systems, with appropriate duplication and diversity of storage? **PR.DS**	
26	Do you monitor all data leaving your devices and networks to prevent unwanted leaks (e.g. being copied to USB sticks)? **PR.DS**	

27	Are all devices and storage media properly encrypted and secured against unwanted access or theft? **PR.DS**	
28	Have you properly documented and regulated which users require access to which systems, data and other services (following the principle of least privilege)? **PR.IP**	
29	Have you accurately documented your security procedures and policies and involved all the appropriate parties, including external business partners and the supply chain? **PR.IP**	
30	Do you track that all Operating System, device firmware, software and security patches are upto-date and automatically updated where appropriate? **PR.MA**	
31	Do you have fully operational, correctly configured, patched and updated firewalls on your endpoint devices and at your network perimeter? **PR.PT**	
32	Do you have up-to-date, good quality malware protection installed, active and updated on all devices that access your network? **PR.PT**	
33	Is your email traffic being scanned to remove any malware, spam, phishing attacks, and other unwanted content? **PR.PT**	
34	Is your web traffic being scanned to detect and block malicious, fraudulent, distracting or unwanted traffic? **PR.PT**	
35	Are you regularly scanning all the data on your network, including backups and archives, to ensure it is not harboring malware and has not been tampered with? **PR.PT PR.DS**	

36	Do you have systems in place to ensure that all external services you provide (including websites, web applications and databases, remote login systems, etc.) are resilient to traffic spikes and distributed denial-of-service (DDoS) attacks? **PR.PT**	
37	Do you monitor for insider threats, such as analyzing user activity to spot any anomalous behavior (e.g. logging in from an unusual location, accessing unauthorized files, etc.)? **PR.PT**	
38	Do you ensure regular penetration tests, including vulnerability scans, are performed across all your systems, networks, and services (including third- party and cloudbased services)? **PR.PT**	
39	Do you employ a defence-in-depth approach to cybersecurity, e.g. multiple layers of security controls throughout your network and services? **PR.PT**	
40	Are you aware of any systems or devices in your environment that cannot be patched or updated? **PR.PT**	

DETECT			
Q			**A**
	41	Have you an automated alert system to inform key IT personnel of unwanted behavior or activity on the network? **DE.AE**	
42	Do you regularly review the output from your security systems - anti-malware, firewall, IDS, traffic filters, etc. - to spot unwanted behaviors or activity on the network? **DE.CM**		
43	Are your security monitoring systems correctly configured to produce accurate, informative and easily accessible logs? **DE.DP**		
44	Do you secure your logs (using encryption, archiving, reliable backups, tamper prevention) as well as monitoring their access? **DE.DP**		

RESPOND		
	Q	**A**
45	Do you regularly test your incident response plan to ensure that it's not only up-to-date and effective at mitigating dangers, but that it is also easily understood and actioned by all parties? **RS.AN RS.IM RS.MI**	
46	Does your incident response plan include coordinating with your business partners, users, customers and where necessary law enforcement? **RS.CO**	
47	Have you created and maintained a comprehensive incident response plan to help guide your action during an unwanted cybersecurity event? **RS.RP**	

RECOVER		
	Q	**A**
48	Should a cybersecurity event take place, can you ensure that any restoration processes are properly coordinated with affected partners, users, customers and law enforcement? **RC.CO**	
49	Does your incident response policy include a postmortem plan so that you can learn from a cybersecurity event and incorporate any lessons learned? **RC IM**	
50	Do you regularly test that you are able to quickly repair or restore any data, devices or services that may have been compromised by a cybersecurity event? **RC.RP**	

FUNCTION AND CATEGORY UNIQUE IDENTIFIERS

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications