

## Ransomware Supplemental Questionnaire

## **INCIDENT RESPONSE PLAN** Does the CISO have direct access to executive management? ☐ Yes □ No Is your Incident Response Plan phased with executive communications at each phase ☐ Yes (e.g. identify and contain, recover, etc.)? □ No 3. When was the last time you tested your Incident Response Plan? \_\_\_ Please provide your anticipated customer count for the next 12 months. 4. List your top 3 IT supply chain providers. \_ 5. Are your servers virtual or located on premise? \_\_\_\_ 6. 7. Do you maintain network logs and generate execution reports to monitor unacceptable or restricted transactions, correcting or reversing entries, and unsuccessful attempts to access restricted information on the network? ☐ Yes □No SECURITY AND EMAIL MANAGEMENT Do you use a privileged access management software? ☐ Yes □ No a. If yes, does this software include MFA? ☐ Yes □ No Do you have remote desktop protocol (RDP) connections? ☐ Yes □ No Please check the appropriate boxes below: a. If RDP is enabled, is it used: ☐ internally □ externally □ both b. If RDP is enabled, is it on a: □ standard port (3389) □ non-standard port If RDP is enabled, is it secured through $\square$ MFA ☐ simply username and password Can your users access e-mail through a web app on a non-corporate device? ☐ Yes □ No a. If yes, do you enforce MFA? □Yes $\square$ No Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user? ☐ Yes □No Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails? ☐ Yes □No Do you use Office 365 in your organization? ☐ Yes ПΝο a. Do you use Microsoft Advanced Email Protection / Defender? ☐ Yes □ No If yes, which categories are in use? Please check the appropriate boxes below: ☐ Inbound email protection $\square$ Safe attachment validation $\square$ Safe link validation ☐ Investigation & Response Can users run MS Office Macro enabled documents on their system by default? ☐ Yes $\square$ No Do you use an endpoint protection product (EPP) across your enterprise? ☐ Yes ☐ No a. Is it tied to a continuous monitoring platform and process? □Yes $\square$ No Do you use an endpoint detection and response (EDR) product across your enterprise? ☐ Yes □No a. Is it tied to a continuous monitoring platform and process? ☐ Yes □No 10. If you have any end of life or end of support software, is it segregated from the rest of the network? ☐ Yes □ No

11. Do you use the following protections on your network with respect to inbound traffic?

	PROTECTION	NETWORK							
	PROTECTION	Laptops	On Premise Servers Virtua			ual Servers	al Servers		
	Firewalls	☐ Yes ☐ No ☐ NA	☐ Yes ☐ I	No □NA	☐ Yes	□No □N	IA		
	IDS	☐ Yes ☐ No ☐ NA	☐ Yes ☐ No ☐ NA ☐ Yes ☐ No ☐ NA ☐ Yes ☐			□No □NA			
	IPS	☐ Yes ☐ No ☐ NA ☐ Yes ☐ No ☐ NA ☐ Yes			□No □NA				
	a. Are these protections	tied to a continuous monitoring platf	orm and process?			□Yes	□No		
12.	Do you use a protective DNS	o you use a protective DNS service (e.g. Quad9, OpenDNS or the Public Sector PDNS)?							
13.	Do you use a privileged user management software to protect administrative log-in?						□No		
	a. If not, do you use any	other type of password vaulting soft	ware?			☐ Yes	□No		
14.	. In what time frame do you install critical and high severity patches across your enterprise?								
15.	5. In what time frame do you install zero-day exploit patches once available across your enterprise?								
16.	6. Is your operational technology environment segmented from your information technology environment(s)?								
a. If yes, how is the segmentation implemented? Please choose all that apply:									
	☐ Firewalls	□VLANS	□VLANS		Other				
	☐ Unidirectional Security (	Gateways ☐ DMZs							
17.	7. Is your operational technology environment segmented from the internet?					☐ Yes	□No		
	a. If yes, how is the segmentation implemented? Please choose all that apply:								
	☐ Firewalls	□VLANS	□VLANS						
	☐ Unidirectional Security (	Unidirectional Security Gateways							
18.	. Do you permit employees to access your operational technology environment remotely?					☐ Yes	□No		
	a. If yes, do you enforce	MFA?				☐Yes	□No		
	b. If yes, do you require employees to have separate accounts (e.g. employees do not share accounts)?					☐Yes	□No		
19.	Do you permit third parties to access your operational technology environment remotely?					☐ Yes	□No		
	a. If yes, do you enforce	MFA?				☐Yes	□No		
<u>TRAINING</u>									
1.	Do you train employees on the	e following: Please choose all that ap	ply:						

Topic	Yes	No	Frequency (e.g. monthly, quarterly, annually)
Social engineering scams			
Strong password creation			
Appropriate use of technology			
Your internal security			
Your Incident Response Plan			

BAG	CK-UP AND RECOVERY						
1.	Are your back-ups segregated from your network?						
2.	Are your back-ups encrypted?						□No
3.	Do you test the integrity of back-ups prior to restoration to be confident they are free from malware?						
4.	Are copies of your back-ups stored on	-line only?				☐ Yes	□No
5.	Are copies of your back-ups stored on-line and off-line?						□No
6.	If your network were to go down, how						
	Please choose from the hours below:						
	☐ Within 12 hours ☐ Within 13 — 48 hours	□ 49 hour	s or more				
7.	Is the time frame you chose above con	mmensurate wi	th what you represe	nt in the contracts w	th your customers?	☐ Yes	□No
CO	MPLETE IF YOU PROVIDE MSP, SAAS	OR ASP SERV	'ICES				
1.	Do you maintain an asset inventory or	listing of all cri	tical systems of you	r customers			
	(e.g. servers, workstations, application	s, etc.)?				☐ Yes	□No
2.	Is each of your customer's data segreg					☐ Yes	□No
3.	Are you responsible for the security of	•				☐ Yes	□No
	If yes, check all the tools that apply ar	nd the range of	services you provid	e for each tool.			
	TOOLS RANGE OF SERVICES						
	10013	Resell	Installation	Configuring	Monitoring	Respond	ling
	Firewalls						
	Antivirus						
	EDR without quarantine						
	EDR with quarantine						
	MFA						
	Third party email filters						
	IDS/IPS (intrusion detection systems / intrusion prevention systems)						
	SIEM (security information and event management)						
<ul><li>4.</li><li>5.</li></ul>	Do you provide the Security Operation What products (e.g. Kaseya, Connects  a. Do you require MFA to use the b. When you receive patches for	vise, etc.) do yo	ou use to remotely c		mers' systems?	☐ Yes	□ No

Do you maintain a list of customers inclus	☐ Yes	□ No					
Do your users have local admin rights on their laptops and desktops?			□No				
a. Are admin rights and/or access to based on their roles?	p personal information limited to those who need access	☐ Yes	□No				
b. Is such access withdrawn when so	omeone leaves that role or the company?	□Yes	□No				
c. Do you use MFA to protect admi	n accounts?	□Yes	□No				
Do you actively support administrative fu	☐ Yes	□No					
	□ Yes	□No					
b. Is such access withdrawn when so	□Yes	□No					
c. Do you use MFA to protect admi	n accounts?	□Yes	□No				
In what time frame do you implement critical and high severity patches for customers?							
In what time frame do you install zero-day exploit patches once available for your customers?							
If you are responsible for providing back-up services to your customers, please answer the following questions:							
a. Are their back-ups encrypted?	☐ Yes	□No					
b. Do you test the integrity of back-	ups prior to restoration to be confident they are free from malware?	□Yes	□No				
c. Are copies of their back-ups store	ed on-line only?	☐ Yes	□No				
d. Are copies of their back-ups store	e copies of their back-ups stored on-line and off-line?						
If your network were to go down, how long would it take you to be fully operational?							
Please choose from the hours below:							
☐ Within 12 hours	☐ 49 hours or more						
☐ Within 13 — 48 hours							
	a. Are admin rights and/or access to based on their roles?  b. Is such access withdrawn when so c. Do you use MFA to protect admin Do you actively support administrative fural. Are your customers' admin rights need access based on their roles?  b. Is such access withdrawn when so c. Do you use MFA to protect admin In what time frame do you implement critin what time frame do you install zero-dated If you are responsible for providing backara. Are their back-ups encrypted?  b. Do you test the integrity of backara. Are copies of their back-ups stored. Are copies of their back-ups stored. Are copies of their back-ups stored. Please choose from the hours below:	based on their roles?  b. Is such access withdrawn when someone leaves that role or the company?  c. Do you use MFA to protect admin accounts?  Do you actively support administrative functions for customers?  a. Are your customers' admin rights and/or access to personal information limited to those who need access based on their roles?  b. Is such access withdrawn when someone leaves that role or the company?  c. Do you use MFA to protect admin accounts?  In what time frame do you implement critical and high severity patches for customers?  If you are responsible for providing back-up services to your customers, please answer the following questions:  a. Are their back-ups encrypted?  b. Do you test the integrity of back-ups prior to restoration to be confident they are free from malware?  c. Are copies of their back-ups stored on-line only?  d. Are copies of their back-ups stored on-line and off-line?  If your network were to go down, how long would it take you to be fully operational?  Please choose from the hours below:  Utithin 12 hours	a. Are admin rights and/or access to personal information limited to those who need access based on their roles?    Yes				