The Hanover Insurance Group®

RESET SAVE PRINT

Ransomware Supplemental Questionnaire

INCIDENT RESPONSE PLAN

1. Does the CISO have direct access to executive management? ☑ Yes ☐ No
2. Is your Incident Response Plan phased with executive communications at each phase (e.g. identify and contain, recover, etc.)? ☐ Yes ☐ No
3. When was the last time you tested your Incident Response Plan? _____
4. Please provide your anticipated customer count for the next 12 months. _____
5. List your top 3 IT supply chain providers. _____
6. Are your servers virtual or located on premise? _____
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

1. Do you use a privileged access management software? ☐ Yes ☐ No
   a. If yes, does this software include MFA? ☐ Yes ☐ No
2. 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
   c. If RDP is enabled, is it secured through ☐ MFA or ☐ simply username and password
3. 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 ☐ No
4. 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
5. Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails? ☐ Yes ☐ No
6. Do you use Office 365 in your organization? ☐ Yes ☐ No
   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	☐ Safe attachment validation
☐ Safe link validation	☐ Investigation & Response

7. Can users run MS Office Macro enabled documents on their system by default? ☐ Yes ☐ No
8. 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 ☐ No
9. 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

114-10174 (1/22)

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

PROTECTION	NETWORK		
	Laptops	On Premise Servers	Virtual Servers
Firewalls	☐ Yes ☐ No ☐ NA	☐ Yes ☐ No ☐ NA	☐ Yes ☐ No ☐ NA
IDS	☐ 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 platform and process? ☐ Yes ☐ No

12. Do you use a protective DNS service (e.g. Quad9, OpenDNS or the Public Sector PDNS)? ☐ Yes ☐ No

13. Do you use a privileged user management software to protect administrative log-in? ☐ Yes ☐ No

a. If not, do you use any other type of password vaulting software? ☐ Yes ☐ No

14. In what time frame do you install critical and high severity patches across your enterprise? _____

15. In what time frame do you install zero-day exploit patches once available across your enterprise? _____

16. Is your operational technology environment segmented from your information technology environment(s)? ☐ Yes ☐ No

a. If yes, how is the segmentation implemented? Please choose all that apply:

☐ Firewalls	☐ VLANS	Other_____
☐ Unidirectional Security Gateways	☐ DMZs	_____

17. 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	Other_____
☐ Unidirectional Security Gateways	☐ DMZs	_____

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

TRAINING

1. Do you train employees on the following: Please choose all that apply:

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	☐	☐	

114-10174 (1/22)

BACK-UP AND RECOVERY

1. Are your back-ups segregated from your network? ☐ Yes ☐ No
2. Are your back-ups encrypted? ☐ Yes ☐ No
3. Do you test the integrity of back-ups prior to restoration to be confident they are free from malware? ☐ Yes ☐ No
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? ☐ Yes ☐ No
6. 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	

7. Is the time frame you chose above commensurate with what you represent in the contracts with your customers? ☐ Yes ☐ No

COMPLETE IF YOU PROVIDE MSP, SAAS OR ASP SERVICES

1. Do you maintain an asset inventory or listing of all critical systems of your customers (e.g. servers, workstations, applications, etc.)? ☐ Yes ☐ No
2. Is each of your customer's data segregated from one another? ☐ Yes ☐ No
3. Are you responsible for the security of your customers' environments? ☐ Yes ☐ No

   If yes, check all the tools that apply and the range of services you provide for each tool.

TOOLS	RANGE OF SERVICES				
	Resell	Installation	Configuring	Monitoring	Responding
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)	☐	☐	☐	☐	☐

4. Do you provide the Security Operations Center (SOC) for your customers? ☐ Yes ☐ No
5. What products (e.g. Kaseya, Connectwise, etc.) do you use to remotely connect to your customers' systems? _____

   _____

   a. Do you require MFA to use these products? ☐ Yes ☐ No
   b. When you receive patches for these third-party products,

      ☐ do you automatically implement them

      or

      ☐ do you conduct testing through change management prior to implementation

114-10174 (1/22)

6. Do you maintain a list of customers inclusive of primary executive contacts and locations? ☐ Yes ☐ No

7. Do your users have local admin rights on their laptops and desktops? ☐ Yes ☐ No

   a. Are admin rights and/or access to personal information limited to those who need access based on their roles? ☐ Yes ☐ No

   b. Is such access withdrawn when someone leaves that role or the company? ☐ Yes ☐ No

   c. Do you use MFA to protect admin accounts? ☐ Yes ☐ No

8. Do you actively support administrative functions for customers? ☐ Yes ☐ No

   a. Are your customers' admin rights and/or access to personal information limited to those who need access based on their roles? ☐ Yes ☐ No

   b. Is such access withdrawn when someone leaves that role or the company? ☐ Yes ☐ No

   c. Do you use MFA to protect admin accounts? ☐ Yes ☐ No

9. In what time frame do you implement critical and high severity patches for customers? _____

10. In what time frame do you install zero-day exploit patches once available for your customers? _____

11. 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 stored on-line only? ☐ Yes ☐ No

   d. Are copies of their back-ups stored on-line and off-line? ☐ Yes ☐ No

12. 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	