Coalition Insurance Solutions, Inc.
1160 Battery Street, Suite 350 San Francisco, CA 94111
coalitioninc.com

Ransomware Supplemental Questionnaire

In order to better understand the security and organization controls that your organization has implemented that may help or lessen the impact of a ransomware event, we would like to request the following information that can help us appropriately classify, and understand the risk that currently exists.

A. Company Name:

B. Email Security

1 Do you filter or scan incoming emails for malicious attachments and malicious links? ☐ NO ☐ YES

If so, what tools or services do you use for this?

2 Do you enable and require multi factor authentication for access to email? (more information available here) ☐ NO ☐ YES

3 Do you use Microsoft Office 365? ☐ NO ☐ YES

If yes, do you use:

Microsoft Sentinel (free or paid tier) ☐ NO ☐ YES

Advanced Threat Protection (ATP) add-on? ☐ NO ☐ YES

Other email security products? ☐ NO ☐ YES

If so, what product(s):

4 Do you use self-hosted Microsoft Exchange servers? ☐ NO ☐ YES

If yes, have you disabled on premises Exchange Web Services? ☐ NO ☐ YES

5 What other email security controls do you have in place to mitigate risk (Anti-Malware, Anti-Phishing, other)? Provide details and context.

CONTINUED ON NEXT PAGE

Ransomware Supplemental Questionnaire, contd.

C. Network Security

1 Do you use an Endpoint Detection and Response solution (e.g. Carbon Black Cloud, Cisco AMP, Crowdstrike Falcon, Cylance, Endgame Endpoint Protection, Symantec EDR, etc.) ☐ NO ☐ YES

If so, which EDR tool(s) do you use?

What is the estimated percentage of endpoints covered with EDR? %

Does it include all domain controllers? ☐ NO ☐ YES

2 Is multi-factor access enabled and required for all remote access (VPN, etc)?

3 Do you have a secure/hardened baseline configuration which is regularly reviewed and updated by an information security professional? ☐ NO ☐ YES

If "yes" to the above, is this baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices? ☐ NO ☐ YES

4 What processes or controls do you have in place to ensure that all endpoints in your network are updated with critical security patches?

What software is used to perform this function?

5 Do you have inbound and outbound firewall configurations with log retention? ☐ NO ☐ YES

If yes, for how long are these firewall logs retained?

6 Please describe any on premises servers that are exposed to the internet?

Please list the IP addresses on which any on-premises servers or other IT infrastructure are hosted:

7 *Does your network have segmentation between:*

Geographic locations? ☐ NO ☐ YES

Business units? ☐ NO ☐ YES

Databases for PII/PHI/PCI? ☐ NO ☐ YES

End of life/unsupported software and rest of network? ☐ N/A ☐ NO ☐ YES

CONTINUED ON NEXT PAGE

Ransomware Supplemental Questionnaire, contd.

D. Business Continuity

1 Do you maintain at least weekly backups of sensitive data and critical business systems? ☐ NO ☐ YES

If yes, are they disconnected and inaccessible from your primary network? ☐ NO ☐ YES

2 Do you test the successful restoration and recovery of key server configurations and data from backups? ☐ NO ☐ YES

If yes, how frequently do you perform such tests?

3 Do you have a business continuity/disaster recovery plan? ☐ NO ☐ YES

a. How frequently is it tested?

b. Based on testing, what is your proven recovery time objective for critical systems to restore operations after a cyber attack or other unplanned outage?

☐ 0-8 HOURS
☐ 8 - 24 HOURS
☐ > 24 HOURS

4 Can backups only be accessed via an authentication mechanism outside of Active Directory? ☐ NO ☐ YES

E. Network Administration

1 How do you control domain administrator access, what safeguards are in place around IT network administration?

2 Are end users prevented from having administrative access on their endpoints? ☐ NO ☐ YES

3 What controls are in place to prevent privilege escalation?

4 Do you have any endpoint management software exposed to the internet (Kaseya, etc)? ☐ NO ☐ YES

If so, what security controls do you have around that?

5 Briefly describe your IT support organization and identify any Managed Service Providers (MSP's) or Managed Security Service Providers (MSSP's) you use (If outsourced IT vendors are used, describe the vendor types, functions performed, and yearly cost approximations. If IT is staffed in-house describe the organization structure, functions performed, and FTE headcount.):

SIGNED BY:

Full Name (First/Middle/Last)

Date (MM/DD/YYYY)