

Paper records: A Square

Electronic records: B-Square

Answer: Yes

Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints?

Do you process, store, or handle credit card transactions?: Yes

Do you tag external emails to alert employees that the message originated from outside the organization?:

Do you pre-screen emails for potentially malicious attachments and links?: No

Have you implemented any of the following to protect against phishing messages?: Sender Policy Framework

Can your users access email through a web application or a non-corporate device?: Yes

Do you use Office 365 in your organization?: No

Do you use a cloud provider to store data or host applications?: Yes

Do you use MFA to secure all cloud provider services that you utilize?: No

Do you encrypt all sensitive and confidential information stored on your organization's systems and network?

Do you allow remote access to your network?: Yes

Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise?: No

Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging?

Do you use MFA to protect access to privileged user accounts?: No

Do you manage privileged accounts using privileged account management software?: Yes

Do you actively monitor all administrator access for unusual behavior patterns?: No

Do you roll out a hardened baseline configuration across servers, laptops, desktops, and managed mobile devices?

Do you record and track all software and hardware assets deployed across your organization?: No

Do non-IT users have local administration rights on their laptop/desktop?: Yes

How frequently do you install critical and high severity patches across your enterprise?: 1-3 days, 4-7 days

Do you have any end-of-life or end-of-support software?: No

Do you use a protective DNS service to block access to known malicious websites?: Yes

Do you use endpoint application isolation and containment technology on all endpoints?: No

Can users run Microsoft Office Macro enabled documents on their system by default?: Yes

Do you implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft?: Yes

Do you utilize a Security Information and Event Management (SIEM) system?: No

Do you utilize a Security Operations Center (SOC)?: Yes

Do you use a vulnerability management tool?: No

Do you use a data backup solution?: Daily, Weekly, Monthly

Estimated amount of time it will take to restore essential functions in the event of a widespread malware or ransomware attack?: 1-24 hours

Please check all that apply:: None

Do any of the following employees at your company complete social engineering training:: Yes

Does your organization send and/or receive wire transfers?: Yes

In the past 3 years, has the Applicant or any other person or organization proposed for this insurance?: Yes