Cyber Security Controls Checklist

WRS Waldorf Risk Solutions
INSURANCE PROFESSIONALS SINCE 1928

Key Control Items	Status
1. Multi-factor authentication (MFA) for email, remote access, and privileged access is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).	
2. Best practices offline backup procedures where your system's data is copied and stored offline or in the cloud. This practice dramatically improves your chance of recovering from a ransomware event without having to pay the ransom. It is essential to test back-ups by restoring the data every six months to ensure nothing is wrong with the back-ups when required.	
3. Email filtering is the process of blocking unwanted or potentially malicious code or links that redirect the user to suspicious websites. It prevents emails that seek entry into the system from getting access to sensitive data. Email filtering is essential in avoiding phishing emails.	
4. Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. This arrangement allows network administrators to control the flow of traffic between subnets based on granular policies. Organizations use segmentation to improve monitoring, boost performance, localize technical issues and – most importantly – enhance security.	
5. Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.	
6. The establishment of formal procedures to defend against zero-day attacks when a patch is required. A patch is a set of changes to a computer program or supporting data designed to update, fix, or improve it. This corrective action includes fixing security vulnerabilities and other bugs, with such patches usually being called bug fixes.	
7. Business Continuity Plan (BCP) is the process of creating preventive and recovery systems to deal with potential cyber threats to an organization or to ensure process continuity in the wake of a cyberattack. BCP's secondary goal is to ensure operational continuity before and during the execution of disaster recovery.	
8. Security awareness training teaches employees to understand vulnerabilities and threats to business operations. Employees need to be aware of their responsibilities and accountabilities when using a computer on a business network.	

This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond provided by WRS. It is not a representation that coverage does ordoes not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy orbond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.