SPECIAL ANNOUCEMENT

BIZLock
BUSINESS CYBERCRIME PROTECTION

New Cyber Insurance Requirements 2022

(for all applicants seeking cyber insurance limits of $500,000 or more)

New Information Security Requirements:

1. Each applicant is required to use multifactor authentication (MFA) on cloud-based systems, including email, data, and remote network access.
2. Each applicant is required to have sufficient data backup, separated from the network.

For more information, see the below highlights starting on page 2. Please consult your I.T. / InfoSec advisor for support. Please implement the above requirements prior to your next renewal. Coverage may not be available from (any) insurer unless these items are active. If the items are not current or active, you may qualify for a lower limit of insurance at $250,000, if available.

Recommended Information Security Practices include:

1. Vulnerability / Patch Updates
2. Next Generation Endpoint Security & Monitoring
3. Ongoing Education

Background:

Cyber risks continue to evolve rapidly. Ransomware is everywhere. Cyber criminals are having excellent success finding easy pathways into organizations and their computer networks. Numerous computer vulnerabilities, together with a variety of tricks and scams are causing widespread losses to organizations and to providers of cyber insurance. Anyone and everyone are exposed and under attack.

To better combat the threats and losses, all stakeholders need to tighten their defenses. In fact, organizations are now being required to demonstrate that their Information Security Risk Profile or “cyber hygiene” is either excellent or meeting new minimum standards to be insurable. This increased scrutiny takes time to evaluate and verify. Be prepared in advance.

Please review the following two pages for more information and please share the new requirements with your I.T. / information security team. Insurance terms may not available to your organization until these items are implemented in advance of your cyber policy effective date.

SPECIAL ANNOUCEMENT

BIZLock
BUSINESS CYBERCRIME PROTECTION

Core Cyber – New Requirements

1) Multi-Factor Authentication

Multi-Factor Authentication (MFA) or 2-Factor Authentication (2FA), is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. This "second" factor could come from one of the following categories:

- **Something you know:** This could be a personal identification number (PIN), a password, answers to "secret questions" or a specific keystroke pattern
- **Something you have:** Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token
- **Something you are:** This category is a little more advanced, and might include biometric pattern of a fingerprint, an iris scan, or a voice print

Please visit the following for more information on 2FA: https://authy.com/what-is-2fa/

Why MFA is Important*

MFA can help mitigate the risk and potential for a compromise to your computer network. When a compromise occurs, an intruder can masquerade inside your network as an authorized user and have access to sensitive information, software and similar controls. They will often set up new computer rules to communicate and/or exfiltrate data and once they have learned about your network, they often inject malware at critical network locations to maximize damage and destruction.

Implement MFA as Follows:

Remote Network Access / Remote Desktop Protocol (RDP): MFA is essential for any/all remote access to networks. Lost or stolen passwords, keylogging and/or brute-force attacks are popular attack vectors for cyber criminals. MFA can help mitigate the risk and potential for a compromise to your computer network by requiring an extra level of authentication to gain access.

Restrict Access to Administrative User Accounts: Requiring MFA to access administrative accounts helps reduce the potential for an intruder to increase their level of role-based access. It is one thing to have access to a network and yet an entirely more severe incident to have an intruder capable of making changes to your computer code and systems. This broader access often allows intruders to deploy malware/ransomware broadly across the network, potentially impacting all aspects of the organizations' operations.

Remote Access to Email: MFA is essential for any/all remote access to email and it can usually be easily activated. If an intruder has access to your email, they will monitor the email and masquerade as you, communicating with your clients and employees, intercepting sensitive data and sending bogus emails with bogus instructions. The impact can be severe and is a major attack vector used in cybercrimes that redirect wires/ACH payments to fraudulent accounts.

**Implementing MFA may be required to secure and/or maintain your cyber insurance*

BIZLock
BUSINESS CYBERCRIME PROTECTION

Core Cyber – New Requirements

2) Data Backup

Data backups are the best way to recover your data from a natural disaster (e.g. fire or flood) or a man-made disaster, like a critical error or ransomware attack. Hackers and their software programs (often with artificial intelligence) are constantly searching for vulnerable organizations. Once found, they will penetrate your network, find your data assets and wreak havoc by encrypting your data. Without access to your data, you might have no choice but to pay a large ransom in an effort to retrieve your data and resume operations. Because hackers know many organizations have data backup, they will search for it and encrypt it as well. Therefore, it is essential to have proper data backup that includes a backup solution that is not connected to your network.

Certain data backup protocols and best practices include the 3-2-1 Rule and/or the 3-2-2 Rule. Essentially, you should always:

i) Maintain an isolated copy of your critical data (including Quickbooks!) Remember that all backups connected to your network are accessible to hackers. At this level, having MFA to access your data backup is one additional important layer of security and it may be a requirement to qualify for cyber insurance.
ii) Consider immutable data backups, which means the data is fixed and unchangeable.
iii) Test your backup!! For disaster recovery efforts arising from a natural disaster or man-made hack attack, your data backup solution does not work until you have tested and actually restored from it. Too often, a drive failure, software update or other issue causes your data backup to stop working. That makes it mission critical to test your system to ensure it is working properly.
iv) Select a strategy and keep it current.
    a. The 3-2-1 backup rule says: keep at least three (3) copies of your data, store two (2) copies on different storage media, and make sure one (1) of them is stored offsite.
    b. The 3-2-2 backup rule says: keep at least three (3) copies of your data, store two (2) backup copies locally but on different storage media, and store two (2) of the copies offsite, with one (1) copy being stored in the cloud.

Unfortunately, if you are unable to restore your data, computers and operations quickly following a hack attack/ransomware attack, the losses can be catastrophic. Don't assume that your efforts will work, but rather, test and practice it.

Finally, consider what data you backup. Don't backup data that you don't need to. Destroy and properly shred data that is no longer needed. The less data you have, the less data the hacker will have access to and the less privacy and operational risk you will be exposed to.

END