Coalition®

coalitioninc.com

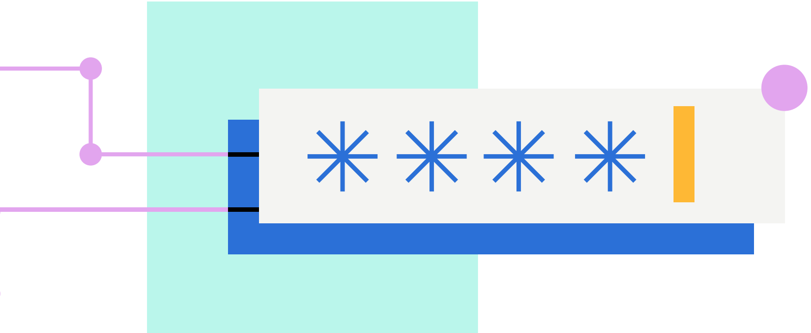
THE CYBER SAVVY BROKER'S GUIDE

Security Controls

Cybersecurity is complex and evolving quickly as security teams race to stay ahead of the latest threats. Many small businesses lack the resources to tackle cybersecurity on their own.

Your role as a broker is to advise clients about holistic risk management, giving you a unique opportunity to guide your clients on cyber controls. We've identified these critical security controls that can help to protect your clients and enable them to procure insurance coverage.

This guide will empower you with the tools and knowledge to deepen your expertise on cyber risk, advise your clients, and grow your business.



How to use this guide

Securing a cyber insurance policy may require in-depth information about your client's network and operations. Your client may even have to take action to address specific risks before they can bind coverage, plus involve their security or IT teams.

As a broker, you may use this guide to learn the essential controls we recommend for all organizations. It's also a great resource to help your clients understand why certain controls may be required in order to bind coverage and advise your clients on protecting their critical business data.

This guide covers the five essential security controls, but every business is unique. Coalition's **Small Business Cybersecurity Guide** provides more advanced controls, implementation information, and vendor recommendations to keep your clients safe.

Contingencies are actions to remediate high-risk security issues your client must resolve before Coalition can release a bindable quote. We may require that your client implement one or more security controls to help reduce their cyber risk and protect them from common incidents such as phishing or ransomware.

Insurance products underwritten by Coalition Insurance Solutions, Inc. (CA License # 0L76155). This is marketing material only, and does not form part of the policy.

5 Essential Security Controls

01. Implement Multi-factor Authentication (MFA)

Why it's important

MFA, also known as 2FA (two-factor authentication), increases account security by requiring multiple forms of verification. MFA is one of the most effective ways to protect business-critical systems such as email and accounts containing personally identifiable information (PII).

What to do

Use MFA on all online accounts. In the event of a breach, MFA adds an additional level of protection to prevent threat actors from accessing sensitive information. Most major email providers support MFA. In best practice, MFA should be enforced for all members of your organization.

Proof point

According to **Coalition's 2022 claims data**, phishing accounted for 57.9% of reported claims. Phishing often leads to business email compromise (BEC) and can lead to ransomware.

02. Enable Secure Remote Access

Why it's important

Many organizations now support remote and hybrid work models. Without the proper security controls, remote connections can be a gateway for cyber criminals to access your devices and sensitive data.

What to do

When possible, utilize an authentication proxy or identity and access management (IAM) solution for all remote access. Use MFA, and implement a policy for strong passwords. Have an IT admin or security operations center regularly audit access to the VPN and respond to risky logins.

Proof point

Popular for facilitating employee remote access, Remote Desktop Protocol, or RDP, remains in Coalition's top five contingencies and is a common root cause for claims among policyholders.

03. Use a Password Manager

Why it's important

Threat actors use weak and reused passwords to gain unauthorized access to an organization's network. Passwords should be unique for each online account and never reused.

What to do

Password managers are encrypted vaults that help keep track of multiple passwords and randomly generate new ones. Password managers are most effective when paired with MFA.

Proof point

The devastating 2021 ransomware attack against Colonial Pipeline impacting multiple supply chains was reportedly due to a stolen, weak password, and MFA was not in place.

Insurance products underwritten by Coalition Insurance Solutions, Inc. (CA License # 0L76155). This is marketing material only, and does not form part of the policy.

04. Update Your Software

Why it's important

Companies routinely release software updates. These updates, also known as patches, may contain new features or fixes for bugs and vulnerabilities. Old software can leave your network vulnerable, and Coalition may issue contingencies based on out-of-date software.

What to do

Implement a program to keep all company assets updated to the most recent available version. Regularly update all connected devices, web browsers and plugins, third-party applications, mobile devices, and apps.

Proof point

The 2017 Equifax data breach resulted in the compromise of 150 million consumers' data. Reportedly, the breach was due to Equifax security officials failing to install a software upgrade.

05. Implement an Endpoint Detection & Response (EDR) Solution

Why it's important

EDR collects and analyzes information from devices on your client's network to respond to suspicious activity. Traditional antivirus software cannot detect all forms of malware. EDR provides more in-depth scanning, containment, and alerting. Be sure to monitor and respond to EDR alerts.

What to do

EDR solutions can identify and quarantine threats, such as malware before a human can respond. An IT team should install, deploy, and review notifications the EDR solution pushes. Keep EDR up-to-date and schedule a set time (weekly or monthly) to review EDR detections.

Proof point

Coalition Incident Response worked with a policyholder that had a malware infection. We took the impacted devices offline and deployed EDR, which scanned the network and stopped a potential ransomware event.

Deepen your knowledge with Cyber Savvy broker resources

Cyber insurance is one of the fastest-growing insurance products and a huge opportunity for brokers to expand their offering and protection for clients. Coalition's Cyber Savvy program equips you with the tools and knowledge you need to deepen your expertise on cyber risk, advise your clients, and grow your business.

You can access more Cyber Savvy Broker resources to continue your learning journey at Coalitioninc.com/campaigns/cyber-savvy

Insurance products underwritten by Coalition Insurance Solutions, Inc. (CA License # 0L76155). This is marketing material only, and does not form part of the policy.