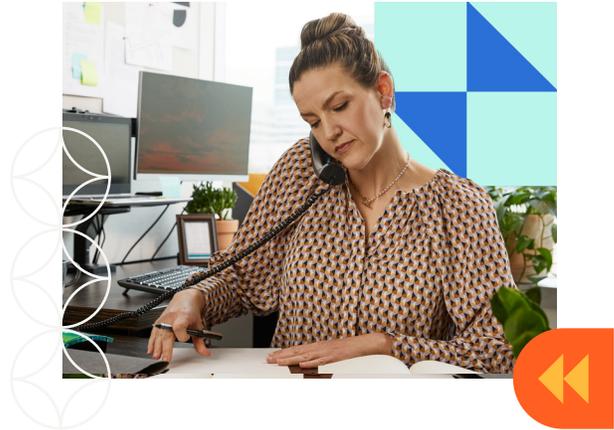


THE CYBER SAVVY BROKER'S GUIDE

# Cyber Risk Assessments



## The Opportunity for Brokers

Your clients rely on technology to run their businesses, exposing them to cyber risks. Threat actors look for easily exploitable targets with specific vulnerabilities, such as:

- Open Remote Desktop Protocol (RDP)
- Weak or Reused Passwords
- Unpatched Systems
- Weak Email Security
- Lack of Employee Awareness

As a trusted risk advisor, you can help spot cyber risks using security scans, such as the Cyber Risk Assessment. Below is a guide on how to educate your clients on the sources of cyber risk.

## A Personalized Snapshot of Your Client's Risk

Using a consultative approach helps grow your cyber book



### Shed light on unprotected exposures

The Cyber Risk Assessment (CRA) creates a personalized profile for your clients' cyber exposures, beginning with a risk summary and risk score. It not only includes a prioritized list of critical vulnerabilities but also actionable recommendations to make organizations more secure and insurable. Coalition's CRA helps you build value as a trusted risk advisor to improve security posture, help retain renewals, and prospect for new opportunities.



### Analyze risk in real-time

Unlike traditional insurers, Coalition has built proprietary technologies that combine attack surface monitoring with public and dark web scanning in real-time — including insights from our internal claims data. We identify the most critical cyber exposures and personalize a list of them for your clients, making you the hero who uncovers their most significant risks.



### Create an action plan

The first step towards improving each client's risk posture is to identify the cyber threats to their business. Security scans can be a powerful tool to identify and explain technical exposures when presenting cyber insurance options to your client.

## Coalition's Cyber Risk Assessment: What we scan for



### Data Breaches

Details the potential impacts of data breaches and phishing, the most common initial entry point in breaches leading to ransomware and funds transfer fraud.



### Malicious Events

These may indicate attempted or successful intrusion by a threat actor and can lead to malware, ransomware, or other incidents.



### Honeytrap events

Honeytraps listen for internet-wide problems, allowing Coalition to observe threat actor behavior and detect upcoming potential vulnerabilities.



### Email Security Loopholes

Email services lacking controls increase the likelihood of a hacker successfully executing a phishing attack or impersonating your organization.



### Blocklisted Domains

Found in public blocklists, if one of your client's assets is found on these lists typically means that some type of malicious activity was performed.



### Torrents Domains

Assets in your network have been observed offering peer-to-peer torrents, often associated with downloading and hosting malicious files, and software piracy.



### Lookalikes

Domains have been registered that look like your company's domain. This activity is very commonly associated with a threat actor using these domains to conduct phishing campaigns against your organization.



### Risky Infrastructure & Applications

A view of an organization's complete cyber risk exposure including assets exposed to the public internet, vulnerabilities on your network, and risky technologies.



**CONTROL**

Risk doesn't sit still. **Coalition Control** protects your clients from emerging cyber threats throughout the policy term with our continuous monitoring and alerting.

## Get Ahead of Digital Risks with **Active Insurance**

Coalition combines comprehensive insurance and proactive cybersecurity tools designed to help businesses manage and mitigate cyber risks. Coalition policyholders experienced 50% fewer claims with Active Insurance compared to organizations with passive cyber coverage.\*

Get Active for your clients. [Get started](#) quoting with Coalition today.

[www.bigmarkets.com](http://www.bigmarkets.com)

\*From the Coalition 2022 Claims Report: Mid-year Update