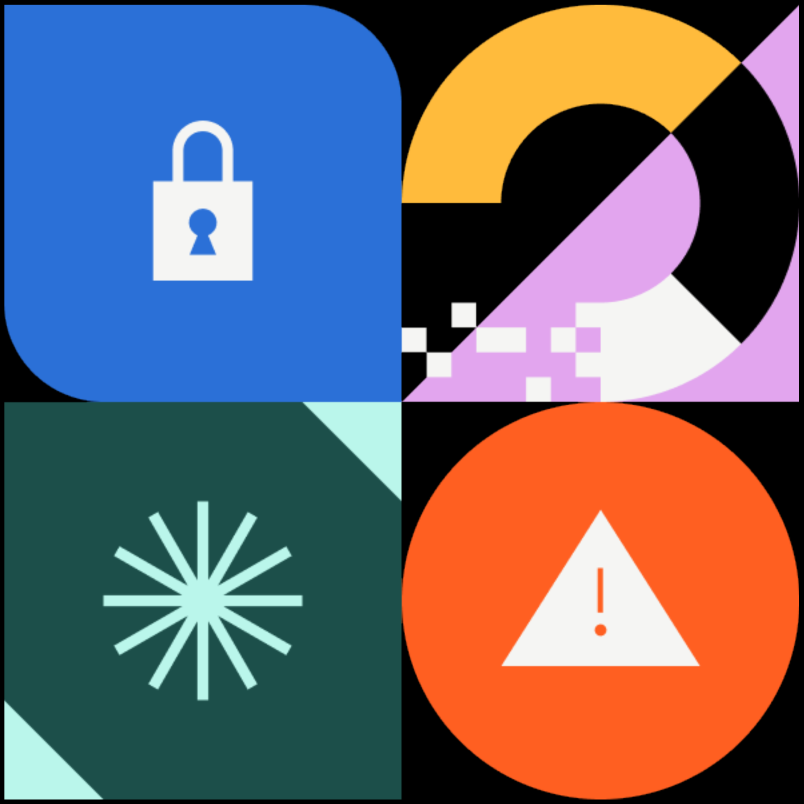
Generated on March 8, 2024

Cyber Risk Assessment

PREPARED FOR

Innovative Title Solutions



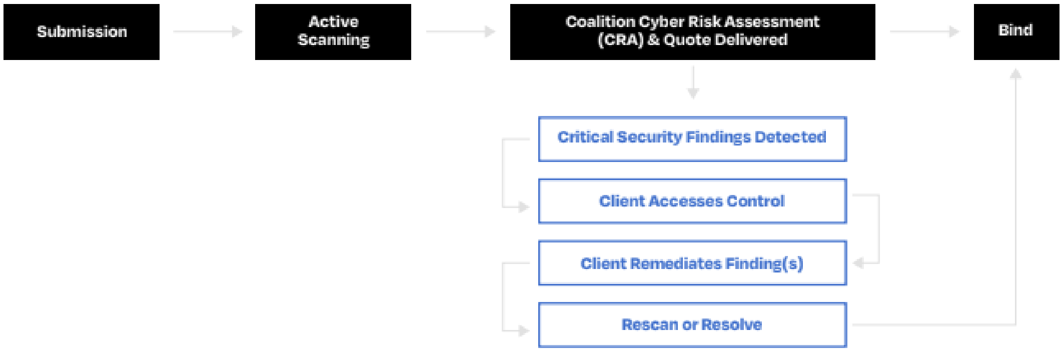
coalitioninc.com

Coalition Control™

Simplify contingency resolution with pre-bind access

Every organization that receives a quote and Cyber Risk Assessment (CRA) from Coalition also receives exclusive access to Coalition Control. This allows Coalition to guide you through remediating critical exposures identified by our Active Risk Assessment and help you resolve them before binding coverage.

How does it work?


Submission
Active Scanning
Coalition Cyber Risk Assessment (CRA) & Quote Delivered
Bind
Critical Security Findings Detected
Client Accesses Control
Client Remediates Finding(s)
Rescan or Resolve

Follow these easy steps to make cybersecurity less daunting with Coalition Control:

1. **Coalition Conducts Active Risk Assessment**
   Coalition uses proprietary attack surface monitoring technology and real-time threat intelligence to provide a customized view of the exposures that are the most severe, likely to impact insurability, and if not resolved could result in claims.

2. **Critical Security Findings Detected by Coalition**
   If Critical Security Finding(s) are detected that impact insurability, they will be noted on the quote document as contingencies and in the Coalition Cyber Risk Assessment (CRA) provided with the quote.

3. **Activate your Coalition Control Account by following instructions provided by your broker**
   Every current and prospective Coalition policyholder receives access to Coalition Control, not just those with security findings. New clients can request pre-bind access by contacting their broker. Existing policyholders can log into Coalition Control with a valid email address and policy number.

4. **Remediate Exposures**
   Log into Coalition Control to review the technical details of any security findings, suggested remediation best practices as well as additional support resources.

5. **Rescan and Resolve**
   After exposures have been remediated, follow the instructions to initiate a rescan and resolve contingencies directly in Control. As soon as contingencies are cleared an updated bindable quote will be reissued. Depending on the security finding, rescans could take up to 48 hours.

Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc.(“CIS”), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company (“CIC”) a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers.

Coalition's Active Insurance approach incorporates continuous Risk Assessments, Active Protection, and Active Response, providing policyholders with holistic benefits in protecting their organizations against dynamic risks.

This Coalition Risk Assessment provides a customized view of your organization's risk. Coalition collects and analyzes externally observable security data and integrates these findings with our proprietary claims and incident data to identify your organization's risk exposures. This objective assessment of your cyber risk enables your organization to take proactive measures to mitigate risk and improve your security.

Coalition's Active Protection and Response provide a holistic risk management solution that incorporates both cutting edge software and support services for your organization, including:

- Attack Surface Monitoring and Third-Party Risk Management software, Coalition Control, valued at $12,000/year and included for FREE with your policy
- In-house claims and incident response support
- Cybersecurity education resources and discounted cybersecurity solutions

Sections

Active Protection

Monitoring and alerting to identify and prevent risk before it escalates

Active Risk Assessment

Underwriting, quoting, renewals, and digital risk scores powered by real-time data

Active Response

In-house resources that accelerate response and coverage if an incident occurs

47% Percentage of incidents handled at no additional expense outside the policy

64% Coalition policyholders experience fewer claims than the cyber industry average

24/7 Support from our claims team

This assessment is provided for informational purposes only. Risk-related analyses and statements in this assessment are statements of opinion of possible risks to entities as of the date they are expressed, and not statements of current or historical fact as to the security of any entity. YOUR USE OF THIS ASSESSMENT IS AT YOUR OWN DISCRETION AND RISK. THE ASSESSMENT IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, COALITION EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. COALITION DOES NOT WARRANT THAT (i) THE ASSESSMENT WILL MEET ALL OF YOUR REQUIREMENTS; (ii) THE ASSESSMENT WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE; OR (iii) THAT ALL ERRORS IN THE ASSESSMENT WILL BE CORRECTED.

Risk Summary

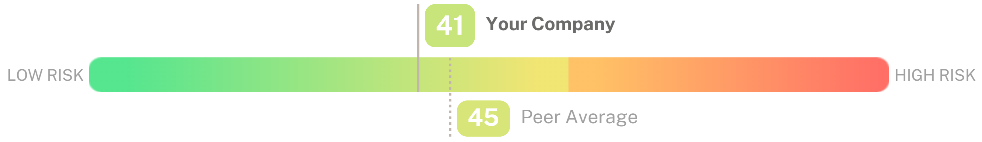
Innovative Title Solutions

CRITICAL

0

Security Findings

Your Risk Score from 1 to 100



Domains	title-solutions.com	Employees	25
Last Scanned	Mar 8, 2024	PHI/PCI/PII	100,000
Industry	Industrials	Revenue	$375,000

Incident likelihood compared to average Coalition insured

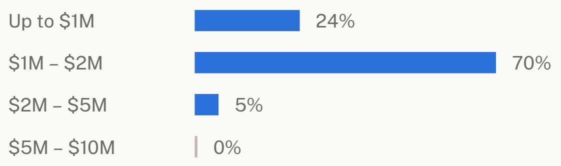
0.5× as likely

Estimated loss based on your organization's risk profile

Type of loss	Median	1 in 10 years	1 in 100 years
Composite	$86,046	$643,949	$3,316,612
Ransomware	$156,107	$951,614	$4,147,246
Funds Transfer Fraud	$75,724	$498,518	$2,313,045
Data Breach	$54,578	$424,466	$2,255,736

Using demographic data on your organization, together with Coalition's global claims data, we've modeled the probability that organizations in your peer group will experience a cyber loss over the next 12 months, as well as the expected severity of loss using a statistical model derived from 10,000 simulated years of cyber incidents. By comparison, we've also included benchmarking on the insurance limits purchased by your peer group.

Limits purchased by peer organizations



Data is from multiple sources, including Coalition's own global data. Actual numbers may vary significantly from calculator estimates based on additional factors for a given business. The data provided is for informational and educational purposes only. Use of the Coalition Coverage Calculator should not be used as a replacement for a company's own due diligence in regards to their cyber risk. Access and use of the Coalition Coverage Calculator is predicated upon the acceptance of Coalition, Inc. Terms of Use.

Security Findings

◆ CRITICAL	△ HIGH	○ MEDIUM	▽ LOW
0	0	1	5
Critical risks are contingencies that **impact premium and insurability** if not resolved.	High Risks can turn into critical risks if not resolved upon recognition.	Medium Risks do not impact premium or insurability but should be resolved.	Low Risks do not impact premium or insurability. We still recommend remediation.

Attack Surface Analyzed

Sub Domains	3
IP Addresses	13
Applications	15
Services	0

For full list, go to control.coalitioninc.com

Critical Findings

Our Active Risk platform has identified the following critical security findings for your organization. To avoid a **negative impact on insurability or a potential increase in your premium**, resolve these critical security findings using the information provided.

Your organization is Cyber Savvy!

No critical security findings have been detected.

◆ Critical △ High ○ Medium ▽ Low

SECURITY FINDINGS

Non-Critical Security Findings

Non-critical security findings have a risk severity of High, Medium, or Low. We still recommend remediating them as they could expose your organization to other types of cyber risk or become critical security findings later as threat actors change their tactics.

SECURITY FINDING	ASSETS
○ **HTTP Service without SSL/TLS found** HTTP service found without SSL/TLS. HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the site. Users expect a secure and private online experience when using a website. Using SSL/TLS... For full details, go to control.coalitioninc.com/active-findings/	1
▽ **Missing X-Frame-Options Header** The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid... For full details, go to control.coalitioninc.com/active-findings/	1
▽ **Missing Content-Security-Policy Header** Content Security Policy (CSP) is an HTTP response security header that developers and security architects can leverage to specify domains from which the site is allowed to load resources. This header provides an in-depth security protection from critical vulnerabilities such as cross-site scripting... For full details, go to control.coalitioninc.com/active-findings/	1
▽ **Missing X-Content-Type-Options Header** The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type. By not having this header the website could be at risk of a Cross-Site Scripting (XSS) attack.	1
▽ **Missing Referrer-Policy Header** Referrer Policy provides mechanisms to websites to restrict referrer information (sent in the referrer header) that browsers will be allowed to add.	1
▽ **DMARC Record Missing** DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”, is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling... For full details, go to control.coalitioninc.com/active-findings/	1

How can I test my fix and resolve a security finding?

1. Go to https://control.coalitioninc.com/active-findings/.
2. Select the security finding you want to test and click **Rescan**.
3. Your security findings will update and a new Risk Score will appear!

Not a Coalition Control user?

Sign up for free at control.coalitioninc.com

◆ Critical △ High ○ Medium ▽ Low

Complete Risk Posture

Your complete risk posture is a holistic look at your organization's cyber exposure. This includes assets, data exposures and technologies that threat actors may exploit identified by our Active Risk Platform. The detections in this section, while important to fix, do not impact your insurability or premium.

RISK	Data Breaches	**4** leaks
SECURE	Malware	**0** detected
SECURE	Spam	**0** detected
SECURE	Malicious Events	**0** detected
SECURE	Honeypot Events	**0** detected
SECURE	Blocklisted Domains	**0** detected
SECURE	Torrents	**0** detected
RISK	DMARC	**1** failures
SECURE	SPF	**0** failures

COMPLETE RISK POSTURE

Data Breaches

This section details the potential impacts of data breaches and phishing. Phishing is often the initial entry point in breaches, and exposed data, like passwords, can be used in subsequent attacks. Email server misconfigurations are also reflected here.

2 Passwords Breached

Characters

Lowercase	100%
Uppercase	100%
Numbers	100%
Special Characters	0%

Use long passwords or passphrases, which are more challenging to guess or brute force. Do not reuse passwords.

Composition

Letters Only	0%
Numbers Only	0%
Letters & Numbers	100%
With Everything	0%

Create complex passphrases or passwords that use a combo of random alphanumeric characters and symbols.

RISK 3 Emails	RISK 2 Phone Numbers	SECURE 0 Auth Tokens
SECURE 0 Credit Cards	SECURE 0 Credit Card PINs	SECURE 0 SSNs

What are your most common breaches?

3	Email addresses
2	Passwords
2	Phone numbers
2	Physical addresses
2	IP addresses
2	Geographic locations
2	Employers
2	Names
2	Dates of birth
2	Job titles

Where are your breaches occuring?

2	Verifications.io
1	Big data breach database
1	the-collections

Need more info?

Go to control.coalitioninc.com/data-leaks/ for a full list.

Not a Coalition Control user?

Sign up for free at control.coalitioninc.com

COMPLETE RISK POSTURE

Malware

Assets we discovered where malware activity was detected.

SECURE
0
Assets Detected

ASSET	SOURCE	LAST DETECTED

Scan performed and no results were found

Spam

Assets we discovered that send unsolicited communication.

SECURE
0
Assets Detected

ASSET	SOURCE	LAST DETECTED

Scan performed and no results were found

COMPLETE RISK POSTURE

Malicious Events

Assets detected by Coalition or a third-party partner, noted for their performance leading to attempted or successful unauthorized network intrusion by a threat actor. These attempts can lead to malware, ransomware, or other cyber incidents.

SECURE

0

Assets Detected

ASSET	TAGS	LAST DETECTED

Scan performed and no results were found

Honeypot Events

A honeypot is a legitimate security mechanism that is purposely vulnerable to high-risk exploits in order to identify malicious assets that attempt to infiltrate it. Our distributed network of honeypots listens for unsolicited connections and attacks. Your assets should not communicate with our honeypots. Events in this section indicate malicious activity on your network is likely. Shared assets are not an indicator of malicious events.

SECURE

0

Assets Detected

ASSET	TAGS	LAST DETECTED

Scan performed and no results were found

COMPLETE RISK POSTURE

Blocklisted Domains

Domains found in public blocklists — if one of your assets is found on these lists typically means that some type of malicious activity was performed.

SECURE

0

Assets Detected

ASSET	SOURCE	LAST DETECTED

Scan performed and no results were found

Torrents

Torrent downloads are often illegal and you risk bringing files infected with malware into your network. In this section, we list the torrents seen being downloaded by your assets.

SECURE

0

Assets Detected

ASSET	NAME	LAST DETECTED

Scan performed and no results were found

COMPLETE RISK POSTURE

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that is designed to give email domain owners the ability to protect their domain from unauthorized use (known as email spoofing). The purpose of implementing DMARC is to protect a domain from being exploited in business email compromise attacks, phishing emails, email scams, and other cyber threat activities.

RISK

1

Domains Failed

PASS (0)	FAIL (1)
	`title-solutions.com`

SPF

Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of an email. This measure specifies what email servers are allowed to send email from your domain. It helps ensure that someone cannot create an email server and send it as your domain unless you have authorized them to do so in your DNS records.

SECURE

0

Domains Failed

PASS (1)	FAIL (0)
`title-solutions.com`	

What is Cyber Insurance?

Cyber insurance enables businesses to transfer the costs associated with recovery from the tangible and intangible losses related to a cyber-related security breach or similar event. Traditional insurance policies often do not cover these risks and often only accept the transference of known physical risks such as damage to equipment, stock, or locations. By bridging the gap between physical and digital risks, cyber insurance allows companies to get back online and resume normal business operations faster, minimizing the cost to their recovery.

Third Party Liability Coverages

We cover the expenses to defend you and any damages resulting from your liability to a 3rd party.

THIRD PARTY SECURITY AND PRIVACY	
Network and Information Security Liability	We cover the expenses to defend you and any damages resulting from your liability to a 3rd party for a security failure, data breach or privacy liability.
Regulatory Defence and Penalties	We cover the expenses to defend you and any regulatory fines or penalties from a regulatory proceeding for a security failure or data breach.
PCI Fines and Assessments	We cover the expenses to defend you and PCI fines and assessments arising from a data breach that compromises payment card data.
Funds Transfer Liability	We cover the expenses to defend you and damages arising from the distribution of fraudulent payment instructions to your vendors, business partners or clients as a result of a security failure.

WHAT IS CYBER INSURANCE?

TECHNOLOGY AND MEDIA PROFESSIONAL

Technology Errors and Omissions

We cover the expenses to defend you and damages arising from your liability to a 3rd party when the failure of your technology service or product is the cause of loss.

Multimedia Content Liability

We cover the expenses to defend you and damages arising from your liability to a 3rd party for media content related claims (such as copyright infringement, violation of privacy rights, defamation).

First Party Coverages

We cover the direct expenses and losses that your organization incurs as a result of a cyber incident.

EVENT RESPONSE

Breach Response Services

We provide services in the first 72 hours to help you with the initial response to a cyber event including access to a 24/7 hotline, advice from legal counsel and preliminary forensic information gathering.

Breach Response Costs

We pay the costs to respond to a breach including computer forensic fees, legally required customer notification, legal expenses, credit monitoring and identity theft restoration.

Crisis Management and Public Relations

We pay the costs to mitigate other first party loss or third party liability such as public relations consultancy, media purchasing and voluntary customer notification.

Ransomware and Cyber Extortion

We cover the costs to respond to an extortion incident, including money, securities, and even virtual currencies paid.

Direct and Contingent Business Interruption, and Extra Expenses from Security Failure and Systems Failure

We cover business interruption loss including extra expenses resulting from interruption to your computer systems or to hosted computer systems, arising from a failure in security or a systems failure.

Proof of Loss Preparation Expenses

We cover the cost of a forensic accountant to help you prepare your claim for business interruption and reputational harm losses.

Digital Asset Restoration

We pay for the costs to replace, restore, or recreate your digital assets that are damaged or lost following a security failure or systems failure.

Computer Replacement and Bricking

We pay for the costs to replace or restore computer hardware or tangible equipment impacted by a loss of firmware integrity resulting from a security failure.

WHAT IS CYBER INSURANCE?

EVENT RESPONSE

Reputational Harm Loss

We cover you for your lost net profit arising from an adverse publication related to a security failure, a data breach, cyber extortion or privacy liability.

Court Attendance

We cover your reasonable expenses in attending a trial or other proceeding in the defence of a 3rd party liability claim.

Criminal Reward

We cover an amount offered by us for information that leads to the conviction of persons committing illegal acts against you that resulted in a claim under the policy.

CYBER CRIME

Funds Transfer Fraud and Social Engineering

We pay for funds transfer losses incurred as a result of the receipt of fraudulent payment instructions including through social engineering. We will also pay for loss incurred from the bank account of a senior executive if caused by a security failure at the named insured.

Service Fraud including Cryptojacking

We pay for the additional amounts you're billed by a cloud or telephony provider when you incur fraudulent charges.

Impersonation Repair Costs

We pay for the cost of removing websites, reimbursing your customers, legal and PR costs incurred as a result of fraudulent electronic communications or websites that impersonate you.

Invoice Manipulation

We cover the net costs that you are unable to collect for the provision of goods or services under a fraudulent invoice or payment instruction that has resulted from a security failure.

COVERAGES AVAILABLE BY ENDORSEMENT

Bodily Injury and Property Damage – 1st Party

We cover specified 1st party losses including business interruption loss for bodily injury or property damage arising from a security failure.

Bodily Injury and Property Damage – 3rd Party

We cover the expenses to defend you and damages arising from your liability to a 3rd party when a security failure results in physical damage or injury.

Pollution

We cover claim expenses and damages arising from pollution caused by a security failure.

Reputation Repair

We pay the Crisis Management & Public Relations costs required to mitigate harm to your reputation.

WHAT IS CYBER INSURANCE?

Coalition's Features

These are some of the tools available to help you improve your cybersecurity.

Security & Incident Response Team
(SIRT)

Coalition is a cyber insurance provider with a dedicated team of cybersecurity experts available to you at all times.

Security Awareness Training

Send simulated phishing tests targeting your own employees. Phishing awareness training simulates real-world phishing attacks, then trains your employees how to defend against them.

Attack Surface Monitoring
(ASM)

Continuous monitoring, attack surface discovery, scanning, reporting, and alerting for organizations of any size.

DDoS Prevention

Distributed denial of service (DoS) attacks attempt to make your Internet-based services inaccessible when you need them. Protect your websites and applications, and prevent disruptions from malicious traffic through our partnership with Cloudflare.

Endpoint Detection and Response
(EDR)

Coalition offers a comprehensive threat detection solution, with a Coalition-negotiated discount, that includes protection from dangerous attacks such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions.

FAQs

Who is Coalition?

Coalition is the world's first Active Insurance company. The team at Coalition brings together in-depth technology, cybersecurity, and insurance expertise to help organizations assess, prevent, and respond to an emerging set of digital risks. We support brokers and policyholders before, during and after an incident occurs, taking a holistic approach to mitigating digital risk. Coalition's Active Risk Platform analyzes complex sets of public data, threat intelligence, and proprietary claims information to create personalized risk assessments and threat monitoring that goes far beyond traditional insurance. Coalition now serves over 160,000 customers with Active Cyber, Active Executive Risks, and P&C policies.

How do I determine my security ranking?

Our security ranking provides a relative measure of an organization's risk and security posture compared to other organizations we have evaluated. In order to determine the ranking of an insured, we correlate identified risk conditions with Coalition's proprietary loss and claims data. Unlike traditional security ratings, Coalition uses actual loss and claims data to identify the most significant risks that could potentially threaten that organization. The result is not only a more accurate assessment of risk, but actionable prescriptions to help an organization invest its resources against the most impactful remediation actions.

Where does the underlying data from Coalition's risk assessment come from?

Coalition's Active Risk Assessment and monitoring technology helps small and medium-size organizations protect themselves in a digital world. We learn from every scan, incident, and claim — building an advantage others can't match. We passively collect external data on an organization's Internet facing IT infrastructure. We do not perform active collection of information, including penetration testing against an organization's networks, without the explicit permission of that organization.

What is Active Insurance?

At Coalition, we believe that all businesses should be able to embrace technology and thrive in the digital economy. That's why we've created a new way to **solve digital risk before they strike: Active Insurance**. Active Insurance combines the power of technology and insurance to provide coverage that is built for the digital economy. Active Insurance stands in stark contrast to traditional insurance, which wasn't built for the speed and amorphous nature of digital risks, leaving many organizations unprepared.

How can I learn more?

To learn more about Coalition visit coalitioninc.com, or our knowledge base at help.coalitioninc.com. As a dedicated risk management partner to our policyholders, Coalition's team of security and insurance experts are committed to helping you implement security and loss controls, all at no additional cost.

Glossary

asset
Web properties that your organization owns, such as an IP Address, Domain, or Subdomain.

data breach
A cyber incident where your customer or employee data is accessed, and possibly exfiltrated, by a third party.

domain
Web address associated with the organization. Example: coalitioninc.com

hosting
Some type of hosting provider or hosting technology being used in one or more of your assets.

IP address
An IP address associated with your company. Example: 1.1.1.1.

Remote Desktop Protocol (RDP)
RDP is a feature that enables employees to remotely log into their corporate computer from home. While it may be convenient for employees, RDP can also function as an open door for hackers to break into your corporate network.

Secure Sockets Layer (SSL)
SSL is a cryptographic protocol designed to provide secure communications over a computer network.

services
Technologies used to deliver services from your assets.

technologies
Technologies found being used in one or more of your assets.

torrents
Torrenting is a peer-to-peer file-sharing mechanism whereby assets that are hosted on your computers may be downloaded by other people who are outside of your organization.

This assessment was prepared by

Coalition, Inc.
55 2nd Street
Floor 25
San Francisco, CA 94105

For more information, visit coalitioninc.com

Coalition's products are offered with the financial security of Swiss Re Corporate Solutions (A.M. Best A+ rating), Arch Insurance Group (A.M. Best A+ rating), Lloyd's of London (A.M. Best A rating), and Argo Pro US (A.M. Best A- rating).