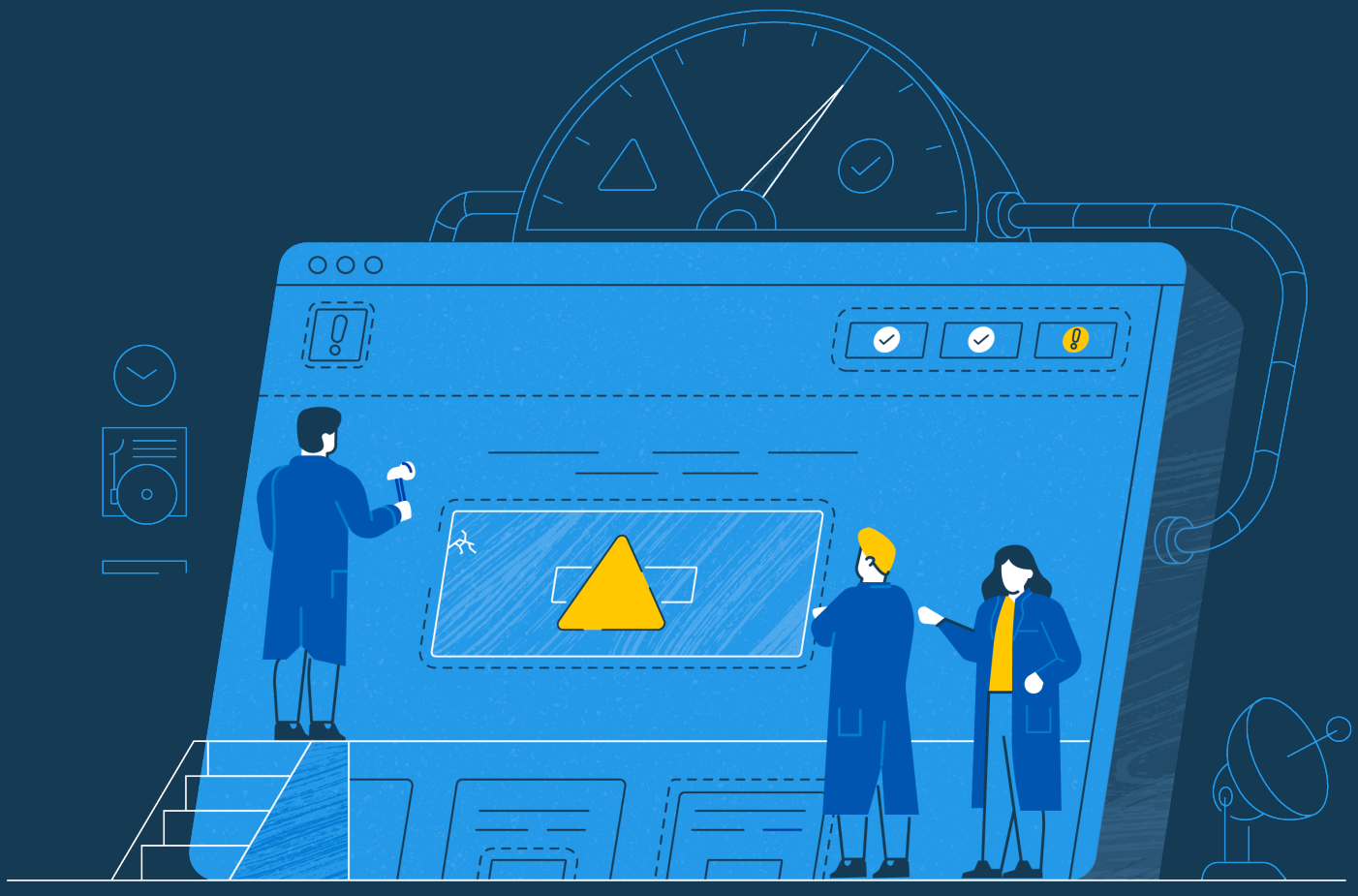
Coalition®

GENERATED ON NOVEMBER 5, 2020

Risk Assessment

PREPARED FOR

Acme org.



coalitioninc.com

Coalition is the leading provider of cyber insurance and security, harnessing the power of technology and safety of insurance to help organizations solve cyber risk. This Coalition Risk Assessment is the first step in this continuous monitoring process. Using externally observable data, this report provides an objective, evidence-based assessment of your cyber risk and overall security preparedness. As your dedicated risk management partner, our security team is available to provide additional context and help you to implement security and loss controls. Coalition policyholders receive 24/7 continuous security monitoring, all at no additional cost.

Sections

1 Executive Summary

This assessment evaluates cybersecurity risk using data-driven, objective, and publicly available metrics together with Coalion's proprietary claims data. The findings and recommendations in this report are intended to help proactively identify, quantify, and manage cybersecurity risk. All findings can be investigated in greater detail using Coalition's BinaryEdge Security Platform.

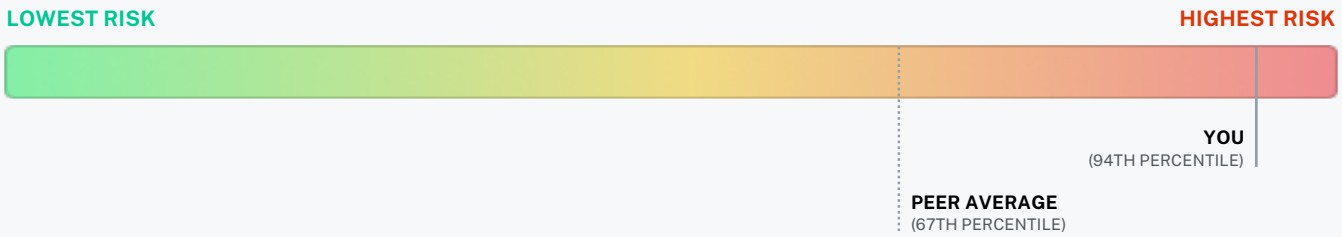
Acme org.

Domain: acme.com
Last scan: November 5, 2020
Revenue: $100,000,000

Industry: Financials
Employees: 150
Records: 0

You rank in the 94th percentile of all Coalition policyholders

Discovered vulnerabilities will not impact your coverage. However, resolving them may reduce your premium.



Vulnerabilities by Criticality

Prioritized list of vulnerabilities we found on your assets. Critical vulnerabilities represent an active threat and should be remediated as soon as possible.

CRITICAL RISK	HIGH RISK	MEDIUM RISK	LOW RISK
1	0	20	6

Detected Assets

Outside-in view of the Web properties we identified.

DOMAINS	IPS	APPLICATIONS	SERVICES	HOSTING
36	262	27	23	4

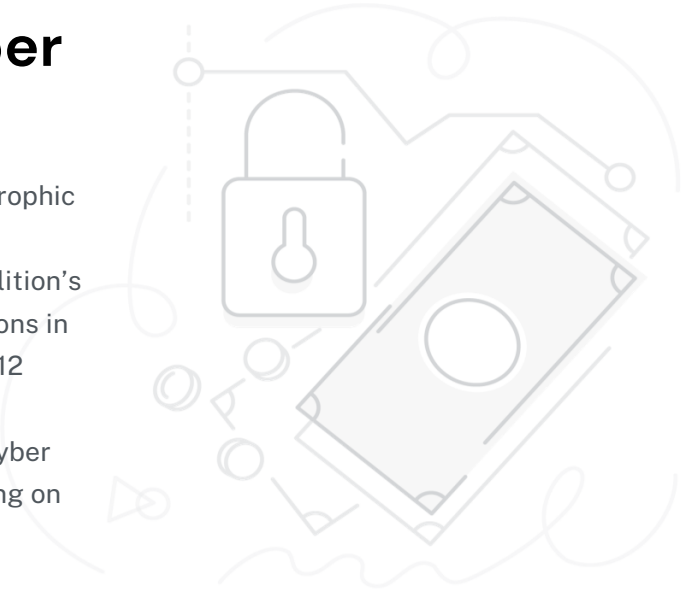
Vulnerabilities by Category

Security vulnerabilities found associated with your assets by level of security impact.

RDP	IoT	Encryption	Malware
0	0	14	0

SSL / TLS	Web	Storage
9	1	1

2 How Much Would a Cyber Incident Cost?



Most cyber incidents are manageable, however it is catastrophic loss that organizations need to be prepared for. Using demographic data on your organization, together with Coalition's 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.

Incident likelihood compared to average Coalition insured

3.7x as likely

Limits purchased by peer organizations

Estimated cost based on your organization's risk profile

	Overall	Ransomware	Funds Transfer Fraud	Data Breach
MEDIAN	$316,902	$181,500	$28,374	$107,028
1 IN 10 YEAR LOSS	$1,862,022	$1,002,381	$163,032	$696,609
1 IN 100 YEAR LOSS	$7,923,104	$4,037,218	$678,177	$3,207,710

* Data is from multiple sources, including Coalition's own 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 Service.

3 Email Security

Improperly configured email servers make it easier for cybercriminals to commit fraud against your organization. Social engineering and email compromise are the leading root cause for losses reported by Coalition policyholders. This section identifies common email security measures to protect your organization.

3.1 DMARC

PASS 0

FAIL 1

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.

Pass

None

Fail

acme.com

3.2 SPF

PASS 1

FAIL 0

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.

Pass

acme.com

Fail

None

4 Vulnerabilities

This section describes the security vulnerabilities we detected on your assets, including vulnerabilities identified on your web applications and services.

4.1 Web Application Security

Securely configuring web applications can prevent cybercriminals from compromising your, and your user, systems and data.

Directory Listing

MEDIUM RISK
1
Assets

Directory listing is a web server function that displays the directory content when there is no index file in a specific directory, which can result in exposure of sensitive files that can lead to further attacks against the application or services. Directory listing can be caused by: Poor default configuration, Input Validation, Encoding, Traversal Vulnerabilities, Access Control Errors

Recommendations

- Restrict directory listing from the web server configuration.
- Make sure no sensitive information is disclosed.

References

- CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory

54.243.193.135 Source: **DNS A**

4.2 Services

Issues found with technologies and software running on your assets.

RSYNC Service exposed

CRITICAL RISK
1
Assets

An asset exposing RSYNC has been detected. As it contained no authentication any attacker can access the files on this RSYNC.

Recommendations

- Disable the service if not in use.
- Limit access only to the specific IP addresses that need to access it.

References

- RSYNC

54.243.193.135 Source: **DNS A**

Expired Certificate

MEDIUM RISK
3
Assets

The host is serving a certificate which has already expired.

Recommendations

- Purchase or generate a new SSL/TLS certificate to replace the existing one.

References

- Cloudflare: What is an SSL Certificate?

66.111.7.8 Source: **DNS A**

54.243.193.135 Source: **DNS A**

Self-Signed Certificate

MEDIUM RISK
1
Assets

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Recommendations

- Purchase or generate a proper SSL certificate for this service.

References

- Cloudflare: What is an SSL Certificate?

66.111.7.8 Source: **DNS A**

HTTP Service without SSL/TLS found

MEDIUM RISK
7
Assets

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 provides three layers of protection: Encryption, Data integrity, Authentication.

Recommendations

• Review the service usage and implement HTTPS.

References

• SSL Research: SSL and TLS Deployment Best Practices
• Mozilla Wiki: Security/Server Side TLS

66.111.7.8	Source: **DNS A**	54.243.193.135	Source: **DNS A**
173.239.66.194	Source: **DNS A**	157.131.251.23	Source: **DNS A**

Email Service without SSL/TLS found

MEDIUM RISK
6
Assets

Email service was found without SSL/TLS. This enables applications to communicate across a network in a private and secure fashion, discouraging eavesdropping, tampering, and message forgery. Using SSL/TLS provides three layers of protection: Encryption, Data integrity, Authentication.

Recommendations

• Review the service usage and implement SMTPS.

References

• Wikipedia: SMTPS

54.243.193.135	Source: **DNS A**	173.239.66.194	Source: **DNS A**
157.131.251.23	Source: **DNS A**		

5 IP and Domain Reputation

Your organization's IP reputation depicts the quality of your email sending environment. This section lists reputational issues found with your IPs and domains, such as sending spam or performing malicious actions. These assets' reputations impact your organization's ability to send email from your IP.

5.1 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.

NO RISK
0
Domains

Scan performed and no results were found.

5.2 Honeypot Events

Our distributed network of honeypots constantly listens for unsolicited connections and attacks. There is no reason for any of your assets to communicate with these honeypots. If an event appears in this section, there is a high probability of malware or malicious activity on your network.

NO RISK
0
Domains

Scan performed and no results were found.

6 Malware

This section lists your assets that have been connected with recent malware infections or indicators of compromise.

Assets Associated with Malware

Assets we discovered where malware activity was detected.

NO RISK
0
Assets

Scan performed and no results were found.

Assets Associated with SPAM

Assets we discovered that send unsolicited communication.

NO RISK
0
Assets

Scan performed and no results were found.

Malicious Events

Any assets that performed malicious actions detected by us or third-party partners.

NO RISK
0
Events

Scan performed and no results were found.

7 DNS (Domain Name System)

We found the following DNS records associated with your organization. DNS records let the Internet know how to reach your email server, website, and other key functions, and are used by cybercriminals to assess your organization's attack surface.

A Records

Address Record

Displaying 10 out of 36 entries

mail.xxxx.acme.com	www.hxzxzx.acme.com
www.lxxxxacme.com	www.xzzxacme.com
www.zzzz.acme.com	www.rr.acme.com
mail.zzzzzz.acme.com	www.ppp.acme.com
www.mail.zzz.acme.com	www.acme.com

MX Records

Mail Exchange Record

mail.xacme.com	

NS Records

Name Server Record

music.xacme.com

xxzzz.acme.com

SOA Records

Start of Authority Record

music.xacme.com

TXT Records

Text Record

mail.xacme.com

8 Sensitive Information Exposed

This section details information found in 3rd party vendor leaks that are associated with your organization or assets.

Leaked data in 2020

Genders, Names, Geographic Location, Email addresses, Passwords

Promo	1 leaks

1 email address found in leaks:

xxxxxx@acme.com

Leaked data in 2019

Homepage URLs, Credit status information, Genders, Physical addresses, Names, Geographic locations, Usernames, Email addresses, Phone numbers, Dates of birth, Social media profiles, Job titles, IP addresses, Passwords, Employers

Displaying 6 out of 9 data breach events

the-collections	169 leaks	**data-contacts**	18 leaks
Pastebin	2 leaks	**ApexSMS**	1 leaks
Ascension	1 leaks	**mgmresorts.com**	1 leaks

Sample of 20 out of 1,277 email addresses found in leaks:

exgggggttlwndr@acme.com, jadgggffande@acme.com

Leaked data in 2018

Genders, Physical addresses, Spoken languages, Names, Geographic locations, Usernames, Phone numbers, Job titles, Dates of birth, Social media profiles, Email addresses, IP addresses, Passwords, Employers

Displaying 6 out of 9 data breach events

datanleads.com	100 leaks	Adapt.io	30 leaks
Customers Live	17 leaks	HauteLook	8 leaks
Dubsmash	2 leaks	500px	1 leaks

Sample of 20 out of 174 email addresses found in leaks:

exgggggttlwndr@acme.com, jadgggffande@acme.com

Leaked data in 2017

Email addresses, Usernames, Passwords

BreachCompilation	107 leaks	LiveJournal	5 leaks
MyHeritage	1 leaks		

Sample of 20 out of 111 email addresses found in leaks:

exgggggttlwndr@acme.com, jadgggffande@acme.com

Leaked data in 2016

Personal descriptions, Education levels, Religions, Travel habits, Physical addresses, Physical attributes, Drinking habits, Work habits, Usernames, Sexual fetishes, Phone numbers, IP addresses, Parenting plans, Relationship statuses, Passwords, Drug habits, Genders, Fitness levels, Names, Income levels, Astrological signs, Website activity, Geographic locations, Political views, Email addresses, Dates of birth, Job titles, Ethnicities

Antipublic	83 leaks	**Exploit.in**	45 leaks
Mate1	17 leaks	**Modern Business Solutions**	2 leaks
BuzzMachines.com	1 leaks		

Sample of 20 out of 96 email addresses found in leaks:

exgggggttlwndr@acme.com, jadgggffande@acme.com

Leaked data in 2015 and older

Home ownership statuses, Physical addresses, Password hints, Usernames, Phone numbers, Sexual fetishes, IP addresses, Security questions and answers, Passwords, Purchasing habits, Credit status information, Family structure, Sexual orientations, Genders, Names, Income levels, Payment histories, Website activity, Geographic locations, Dates of birth, Email addresses, Ethnicities

Displaying 6 out of 20 data breach events

Ashley Madison	18 leaks	**Webhost**	3 leaks
Experian	1 leaks	**MajorGeeks**	1 leaks
R2Games	1 leaks	**xat**	1 leaks

Sample of 20 out of 130 email addresses found in leaks:

exgggggttlwndr@acme.com, jadgggffande@acme.com

9 User Behavior

This section details risky behavior we've observed from individuals within your organization. We use open source intelligence to measure the cyber hygiene of user accounts. If compromised, these accounts could compromise your organization as well.

9.1 Password Quality

Using strong, unique passwords for all services can help prevent common criminal techniques such as 'brute forcing' or 'credential stuffing.' This section shows an analysis of the complexity and length of passwords found in data leaks for your organization.

Analysis by Characters

We recommend using longer passwords or passphrases, which are more challenging to guess or brute force.

LOWERCASE	UPPERCASE	NUMBERS	SPECIAL CHARACTERS
86.1%	8.8%	66.8%	2.5%

Analysis by Composition

We recommend creating complex passwords that use a combination of alphanumeric characters and symbols.

ONLY LETTERS	ONLY NUMBERS	LETTERS & NUMBERS	WITH EVERYTHING
32.4%	10.9%	54.2%	0.8%

9.2 Torrents

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

Scan performed and no results were found.

What is Cyber Insurance?

Cyber insurance (a.k.a. Cyber Liability, Internet Liability, Electronic Media Liability, and Network Security & Information Security Liability insurance, among other countless monikers) helps companies weather the storm from many technology-based risks they face. This includes the risks associated with a company's information technology infrastructure and data that may be impacted by a systems failure, ransomware attack, funds transfer loss, or data breach.

Our coverage

We protect your entire business from today (and tomorrow's) cyber threats, with up to $15 million of cyber and technology errors and omissions insurance coverage.

3rd Party Liability Coverages

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

Network & Information Security Liability

Regulatory Defense & Penalties

Multimedia Content Liability

PCI Fines & Assessments

We cover the expenses to defend you and any damages resulting from your liability to a 3rd party, or for regulatory fines & penalties, multimedia wrongful acts (such as infringement, defamation, piracy, etc.), and PCI fines & assessments resulting from a failure in your security, data breach, or privacy violation.

Bodily Injury & Property Damage - 3rd party

We pay for the costs of defense and damages from your liability to a 3rd party when a failure in your security results in physical damage or injury.

Technology Errors & Omissions

We pay for the costs of defense and damages from your liability to a 3rd party when the failure of your technology service or product is the cause of loss.

1st Party Liability Coverages

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

Bodily Injury & Property Damage - 1st party **Pollution**	In the event of a security failure (i.e., physical cyber attack), we'll even cover losses resulting from bodily injury or damage/impairment to your tangible property, as well as damages resulting from any liability you may have to a 3rd party, including regulatory fines & penalties and pollution liability.
Computer Replacement	We cover the costs to replace your computer systems that are permanently impacted by malware.
Fund Transfer Fraud	We pay for funds transfer losses you incur from a failure in your security or social engineering.
Service Fraud	We pay for the additional amounts you're billed by a cloud or telephony provider when you incur fraudulent charges.
Digital Asset Restoration	We pay for the costs to replace, restore, or recreate your digital assets that are damaged or lost following a failure of your security.
Business Interuption & Extra Expenses	We cover financial losses resulting from a failure in your security, data breach, and even systems failure, as well as the extra expenses you incur to bring your company back online.
Cyber Extortion	We cover the costs to respond to an extortion incident, including money, securities, and even virtual currencies paid.
Breach Response **Crisis Management & Public Relations** **Reputation Repair**	We pay for the costs to respond to a breach including 3rd party incident response and public relations experts, customer notification costs and credit monitoring, media purchases, and legal fees; and advise in connection with the incident, among others.

Global Coverage

Our coverage is global, providing you with protection from cyber threats near and far.

- **Worldwide Coverage**
- **Cyber Terrorism**
- **Internet of Things**
- **Social Media**

In the event of a security failure (i.e., physical cyber attack), we'll even cover losses resulting from bodily injury or damage/impairment to your tangible property, as well as damages resulting from any liability you may have to a 3rd party, including regulatory fines & penalties and pollution liability.

Our features

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

On-demand Support and Training

Security & Incident Response Team (SIRT)
Coalition is the only 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. Curricula's phishing awareness training simulates real-world phishing attacks, then trains your employees how to defend against them.

Proactive Monitoring and Alerts

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

Security Solutions

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.

Ransomware Protection
Coalition's free anti-ransomware software is constantly scanning for malicious software, and prevents malware from infecting your computers.

FAQs

Frequently Asked Questions about Coalition Risk Assessment.

Who is Coalition?

Coalition is the leading provider of cyber insurance and security, combining comprehensive insurance and proactive cybersecurity tools to help businesses manage and mitigate cyber risk. Backed by leading global insurers Swiss Re Corporate Solutions, Lloyd's of London, and Argo Group, Coalition provides companies with up to $15M of cyber and technology insurance coverage in all 50 states and the District of Columbia. Coalition also provides CAD $20M of coverage across all 10 provinces and 3 territories in Canada. Coalition's cyber risk management platform provides automated security alerts, threat intelligence, expert guidance, and tools to help businesses remain resilient in the face of cyber attacks. Headquartered in San Francisco, Coalition has a presence in New York, Los Angeles, Chicago, Dallas, Washington DC, Miami, Atlanta, Denver, Austin, Vancouver, Toronto, Zurich, Seattle and Portugal.

How to 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, that make arbitrary assumptions on the relative impact of an identified risk condition to generate a security score, Coalition uses actual loss and claims data to identify the most significant risks to an 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 passively collects external data on an organization's Internet facing IT infrastructure, compromised system events, file sharing events, and configurations from many different sources. Coalition does not perform active collection of information, including penetration testing against an organization's networks, without the explicit permission of that organization.

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

This section defines some of the terminology used throughout this report.

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.

RDP
Remote Desktop Protocol (also known as a Remote Desktop or 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.

Services
Technologies used to deliver services from your assets.

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

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.

Coalition®

Cyber Risk, Solved.®

This assessment was prepared by

Coalition, Inc.
1160 Battery St. Suite 350
San Francisco, CA 94111

For more information, visit coalitioninc.com