Cyber Insurance Risk Report

Snapshot date: 12/06/2023

Cyberwrite

Acme - Demo Company
United States
Technology
acme.com

CYBER RISK BENCHMARKING

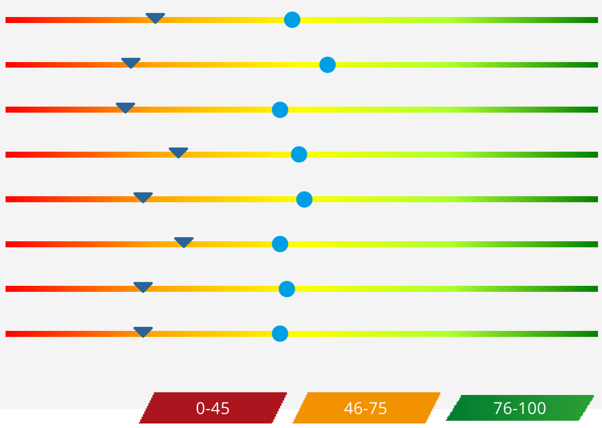
Inherent Risk Score 26

Industry Median: 49

Higher score is better. The range is from 1-100.

Companies with a similar profile in the same sector have a probability of 8.93% to suffer a cyber incident within the next 12 months, which is 5.95 times more likely compared to industry peers median. Scoring is based on publicly available data.

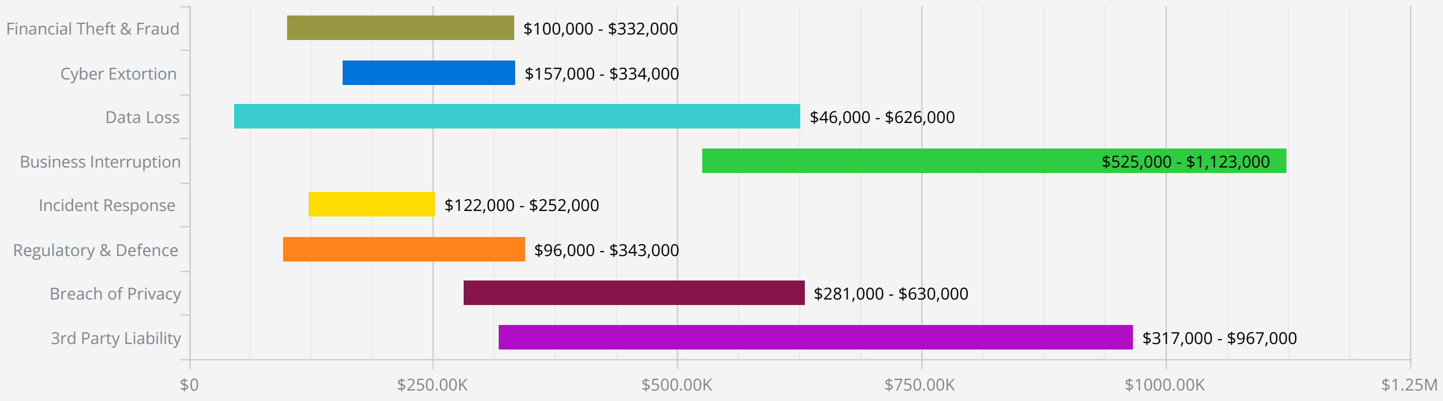
Coverage Type	Company Score ▼	Industry Median ●
Financial Theft & Fraud	27	49
Cyber Extortion	23	55
Data Loss	22	47
Business Interruption	31	50
Incident Response	25	51
Regulatory & Defence	32	47
Breach of Privacy	25	48
3rd Party Liability	25	47



RISK INDICATORS

RISK DOMAIN	STATUS	DETAILS	RISK INDICATORS EXPLANATION
Open Ports	🔴	3	The number of identified open ports across the digital assets of the organization. The best practice is to have a few open ports as possible. The majority of all the public-facing web servers will have ports 80 (HTTP) and 443 (HTTPS) open and listening for incoming connections.
DDoS Mitigation	🟢	Implemented	A distributed denial-of-service (DDoS) is a type of computer attack that uses many hosts to overwhelm a server, causing a website to experience a complete system crash. Implement dedicated Anti-DDoS solutions to reduce the risk of business interruption.
SSL Certificate	🟢	Valid	Secure Sockets Layer (SSL) is the standard technology for keeping an internet connection secure while safeguarding any sensitive data being sent between two systems, preventing cybercriminals from reading and modifying any information transferred.
Spam Mitigation	🔴	Missing	Cybercriminals often abuse and impersonate organizational domain names and their mail servers to distribute Spam and Phishing emails. Implement dedicated mitigation controls and protocols (e.g., SPF, and DMARC) to help protect customers and the brand.
Exposed Credentials	🔴	1,077	The number of exposed username and password combinations related to the organization. This information is collected from data dumps of data breaches across various cybercrime-related forums on the dark web. Implement MFA to reduce the risk of unauthorized access.
Vulnerabilities	🟢	0	The number of identified software vulnerabilities across the digital assets of the organization. Cybercriminals often exploit software vulnerabilities to gain illicit access to personal information. Enforce a timely patch management policy to reduce the risk of a breach.

FINANCIAL LOSS ESTIMATOR



Estimated Aggregated Loss: $4,607,000 | **Estimated Probable Loss: $2,171,400**

FOR QUESTIONS ON THE FINDINGS OF THIS REPORT, PLEASE CONTACT: SUPPORT@CYBERWRITE.COM

Report Data

Snapshot date: 12/06/2023

Acme - Demo Company
United States
Technology
acme.com

Analysis snapshot

Information that an attacker may find out by external examination of the organization in question.

41
Unique Technologies

4
Subdomains

3
Open Ports

0
Vulnerable Technologies

0
Total vulnerabilities identified

1077
Total Exposed Credentials

Overview

External Network Footprint

Information that an attacker may collect about the organizational network by an external examination.

41

Unique Technologies

A wide collection of all the identified technologies across the digital assets of a given organization. For example, on its websites and any of their publicly exposed services (open ports). This information sheds a light on the level of investment in IT and Security technologies of a given organization in comparison to its peers. The higher the number of technologies identified, the wider the digital attack surface of a given organization is.

acme.com

Name	Description
API Developer	*Description:* This website contains a link to an API or Developer page. *First Detected:* 2023-09-20 07:00:00 *Last Detected:* 2023-12-03 08:00:00 https://kb.builtwith.com/special-reports/link-tracking/
Adobe Connect	*Description:* Adobe Connect web conferencing software offers online meeting functionality, virtual classrooms and large scale webinars. *First Detected:* 2022-04-11 07:00:00 *Last Detected:* 2023-12-03 08:00:00 https://www.adobe.com/products/adobeconnect.html
Apple Whitelist	*Description:* This website domain is on the Apple TLD whitelist which may potentially mean these domains will appear in autocomplete when looking up URLs on Apple products. *First Detected:* 2022-04-03 14:00:00 *Last Detected:* 2023-12-03 08:00:00 https://apple.com
Cloudflare Radar	*Description:* The website appears on the Cloudflare Radar Top 1m sites list *First Detected:* 2023-07-25 07:00:00 *Last Detected:* 2023-11-16 08:00:00 https://radar.cloudflare.com
Cloudflare Radar Top 500k	*Description:* The website appears in the Cloudflare Radar Top 500,000. *First Detected:* 2023-07-25 07:00:00 *Last Detected:* 2023-11-16 08:00:00 https://radar.cloudflare.com
Dublin Core	*Description:* The website contains dublin core meta data extensions. *First Detected:* 2003-01-30 08:00:00 *Last Detected:* 2023-12-03 08:00:00 https://dublincore.org
Events Page	*Description:* The website contains a link to an "Events" or "Calendar" page. *First Detected:* 2021-03-19 23:00:00 *Last Detected:* 2023-12-03 08:00:00 https://kb.builtwith.com/special-reports/link-tracking/
Google Adsense	*Description:* A contextual advertising solution for delivering Google AdWords ads that are relevant to site content pages. *First Detected:* 2003-10-10 07:00:00 *Last Detected:* 2023-12-03 08:00:00

	https://google.com/adsense
Google Adsense Asynchronous	*Description:* Fully asynchronous version of the AdSense ad code. *First Detected:* 2019-06-12 23:00:00 *Last Detected:* 2023-12-03 08:00:00 https://support.google.com/adsense/answer/3221666?hl=en
JavaDoc	*Description:* Generates HTML pages of API documentation from Java source files. *First Detected:* 2020-04-30 23:00:00 *Last Detected:* 2023-12-03 08:00:00 https://docs.oracle.com/javase/1.5.0/docs/tooldocs/solaris/javadoc.html
LetsEncrypt	*Description:* Let's Encrypt is a free open Certificate Authority. *First Detected:* 2016-06-30 23:00:00 *Last Detected:* 2023-12-03 08:00:00 https://letsencrypt.org
My Salesforce	*Description:* This business has a Salesforce login page. *First Detected:* 2021-08-04 07:00:00 *Last Detected:* 2023-12-03 08:00:00 https://salesforce.com
SPF	*Description:* The Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery. *First Detected:* 2014-04-09 23:00:00 *Last Detected:* 2023-11-29 08:00:00 http://www.open-spf.org/
Slack	*Description:* Messaging app for teams that makes working together simple and efficient. *First Detected:* 2022-12-08 08:00:00 *Last Detected:* 2023-12-03 08:00:00 https://slack.com
Sonic	*Description:* Sonic offers fiber-optic internet service with speeds up to 10 Gigabits. *First Detected:* 2023-11-04 07:00:00 *Last Detected:* 2023-12-03 08:00:00 https://sonic.com
WebEx Panel	*Description:* WebEx system. *First Detected:* 2018-02-20 23:00:00 *Last Detected:* 2023-12-03 08:00:00 https://webex.com
eNom DNS	*Description:* DNS services provided by eNom. *First Detected:* 2022-08-26 07:00:00 *Last Detected:* 2023-12-03 08:00:00 https://enom.com
jQuery	*Description:* JQuery is a fast, concise, JavaScript Library that simplifies how you traverse HTML documents, handle events, perform animations, and add Ajax interactions to your web pages. jQuery is designed to change the way that you write JavaScript. *First Detected:* 2017-11-20 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://jquery.com
thttpd	*Description:* thttpd is a simple, small, portable, fast, and secure HTTP server. *First Detected:* 2011-01-03 13:00:00 *Last Detected:* 2023-12-03 08:00:00 https://www.acme.com/software/thttpd/

rr.acme.com

Name	Description
Amazon	*Description:* This site is hosted on Amazon AWS EC2 Infrastructure. *First Detected:* 2018-10-04 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://aws.amazon.com
Amazon Virginia Region	*Description:* Amazon Hosted EC2 Instances in Virginia *First Detected:* 2018-10-04 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://aws.amazon.com
Apache	*Description:* Apache has been the most popular web server on the Internet since April 1996. *First Detected:* 2018-07-02 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://httpd.apache.org/
PHP	*Description:* PHP is a widely used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. *First Detected:* 2018-07-02 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://www.php.net
SSL by Default	*Description:* The website redirects traffic to an HTTPS/SSL version by default. *First Detected:* 2018-08-05 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://trends.builtwith.com/ssl
jQuery UI	*Description:* jQuery UI provides abstractions for low-level interaction and animation, advanced effects and high-level, themeable widgets, built on top of the jQuery JavaScript Library, that you can use to build highly interactive web applications. *First Detected:* 2020-07-21 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://jqueryui.com/
jsTimezoneDetect	*Description:* Automatic Timezone Detection Using JavaScript. *First Detected:* 2020-07-21 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://pellepim.bitbucket.org/jstz/

root.acme.com

Name	Description
Apache	*Description:* Apache has been the most popular web server on the Internet since April 1996. *First Detected:* 2018-07-02 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://httpd.apache.org/
Apache 2_4	*Description:* Apache version 2.4.* *First Detected:* 2019-06-01 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://httpd.apache.org/docs/2.4
BlueFish	*Description:* Bluefish is a powerful editor targeted towards programmers and webdesigners, with many options to write websites, scripts and programming code. *First Detected:* 2015-03-24 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://bluefish.openoffice.nl/
CreativeWork Schema	*Description:* Generic type of work i.e. books, movies etc.. *First Detected:* 2019-11-10 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://schema.org/CreativeWork
Debian	*Description:* Debian is a free operating system (OS) for your computer. *First Detected:* 2015-03-24 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://www.debian.org
Hetzner	*Description:* German based dedicated and virtual hosting running on 100% green energy. *First Detected:* 2015-03-24 23:00:00 *Last Detected:* 2023-11-29 08:00:00 http://www.hetzner.de
Person Schema	*Description:* A human being. *First Detected:* 2019-11-10 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://schema.org/Person
Popper_js	*Description:* A library to manage your pop ups. *First Detected:* 2020-02-02 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://popper.js.org/
SSL by Default	*Description:* The website redirects traffic to an HTTPS/SSL version by default. *First Detected:* 2018-08-05 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://trends.builtwith.com/ssl
Twitter	*Description:* The website mentions twitter.com in some form. *First Detected:* 2022-08-27 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://twitter.com
Twitter Platform	*Description:* The page embeds the Twitter platform in one method or another. *First Detected:* 2015-03-24 23:00:00 *Last Detected:* 2023-11-29 08:00:00 http://twitter.com/about/resources
UNPKG	*Description:* unpkg is a fast, global content delivery network for everything on npm. *First Detected:* 2021-06-01 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://unpkg.com
html5shiv	*Description:* HTML5 IE enabling script shim. *First Detected:* 2015-03-24 23:00:00 *Last Detected:* 2023-11-29 08:00:00 https://github.com/afarkas/html5shiv

ck.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

si.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

mail.rr.acme.com

Name	Description

Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

bugs.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

rhino.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

santan.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

charta.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

login.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

heartmaker.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

music.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

fbi.acme.com

Name	Description
Domain Not Resolving	*Description:* This domain or subdomain is not resolving to an IP. *First Detected:* 2023-07-18 07:00:00 *Last Detected:* 2023-11-29 08:00:00 https://builtwith.com

mapper.acme.com

Name	Description
Edit-in-Place	*Description:* Provides the ability to edit text without reload ajax style. *First Detected:* 2011-12-18 13:00:00 *Last Detected:* 2023-12-03 08:00:00 https://24ways.org/2005/edit-in-place-with-ajax
Leaflet	*Description:* Leaflet is a modern, lightweight BSD-licensed JavaScript library for making tile-based interactive maps for both desktop and mobile web browsers. *First Detected:* 2018-08-05 23:00:00 *Last Detected:* 2023-12-03 08:00:00 http://leaflet.cloudmade.com/
Leaflet JS	*Description:* LeafletJS is an an open-source JavaScript library for mobile-friendly interactive maps. *First Detected:* 2019-04-11 23:00:00 *Last Detected:* 2023-12-03 08:00:00 https://leafletjs.com

1

Hosting Providers

The technologies and services needed for the digital assets of the organization in question to be viewed and accessible online via the internet belong to these vendors.

Sonic Telecom LLC

1

DNS Providers

The primary function of the DNS is resolving domain names to IP addresses (like a public phone book).

eNom DNS

1

ISP Providers

The IP addresses that the organization in question is using for its internet-accessible digital assets belong to these vendors.

Sonic Telecom LLC

0

Payment Service Providers (PSP)

Dedicated services for accepting electronic payments by a variety of payment methods including credit card, bank-based payments such as direct debit, bank transfer, and real-time bank transfer based on online banking.

0

Email Security Providers

Cloud email security solutions are secure email platforms used to prevent phishing scams that trick users into divulging privileged information. The platforms, hosted by the cloud email security vendor, also ensure emails containing links to malicious sites or trigger malware downloads are blocked before reaching the end-user. Businesses use cloud email security solutions to prevent data loss and the release of privileges or credentials and increase endpoint security by blocking malware and other web-based threats.

4

Subdomains

A subdomain is a child domain under a larger parent domain name. In the larger scheme of the Domain Name System, it is considered a third-level domain, used to organize site content. For example, in the web address: "gallery.mysite.com", the suffix ".com" is the first-level domain, "mysite" is the second-level domain and "gallery" is the third-level domain.

Subdomain	IP	Country
root.acme.com	85.10.225.138	Germany
acme.com	23.93.76.124	United States

Subdomain	IP	Country
rr.acme.com	54.243.193.135	United States
mapper.acme.com	23.93.76.124	United States

0

Associated Domains

Additional domain names associated or owned by the same organization. Larger organizations tend to own multiple domains, representing the different brands and business units reporting to the same entity. Every domain may have its unique IP address or share the same IP address with the parent domain, according to the needs and preferences of the organization. The higher the number of associated domains, the wider the digital attack surface of a given organization is.

1

Parent Domain

In case the original domain in question is a child domain related to a higher level domain in terms of DNS hierarchy, the higher level (parent) domain will be presented here.

albertsons.com

8

Hostnames

A Fully Qualified Domain Name that uniquely and absolutely names a computer is composed of the host name and the domain name. The domain name, in turn, is one or more domain labels that place the computer in the DNS naming hierarchy. The host name and the domain name labels are separated by periods, and the total length of the hostname cannot exceed 255 characters.

23-93-76-124.fiber.dynamic.sonic.net	mail.acme.com
poskanzer.org	www.poskanzer.org
acme.com	gate.acme.com
www.acme.com	mapper.acme.com

3

IP Addresses

A collection of all the organizational IP addresses. The higher the number of IP addresses, the wider the digital attack surface of a given organization is.

IP Address
23.93.76.124
54.243.193.135
85.10.225.138

1

Network ASNs

AS46375

1

SSL/TLS Certificates

SSL/TLS Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the HTTPS protocol, allowing secure connections from a web server to a browser. Every SSL certificate has an expiration date. An expired SSL certificate may increase the exposure for MITM (Man In The Middle) attacks against the organization in question, as its customers and employees will find it challenging to distinguish between the expired certificate and a rogue one.

Issuer	Issue Date	Expiration Date
Let's Encrypt	2023-10-28T10:16:13.000000Z	2024-01-26T10:16:12.000000Z

External Network Risks

Potential attack vectors that an attacker may exploit to gain unauthorized access to the organizational network and data.

How risks are evaluated?

The methodology for evaluating the severity level of identified threats.

NVD provides qualitative severity rankings of "Low", "Medium", and "High" for CVSS v2.0 base score ranges in addition to the severity ratings for CVSS v3.0 as they are defined in the CVSS v3.0 specification.

The list of relevant CVEs is examined and sorted by severity level, as rated by the National Institute of Standards and Technology (NIST).

The higher the chance for exploitability and potential impact of a given vulnerability, the higher its severity level is (maximum severity: 10).

CVSS v3.0 Ratings	
Severity	**Base Score Range**
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

0

Vulnerable Technologies

The higher the number and severity of vulnerable technologies, the wider the digital attack surface of a given organization is.

3

Open Ports

Each host (domain/subdomain) can have multiple IPs due to the use of a CDN. The IPs are dynamic and change over time. The number of all the identified open ports across the digital assets of the organization. Attackers commonly use port scanning software to find which ports are "open" (unfiltered) in a given computer, and whether or not an actual service is listening on that port. They can then attempt to exploit potential vulnerabilities in any service they find. The best practice is to have a few open ports as possible. In practice, the vast majority of all the public-facing web servers will have ports 80 (HTTP) and 443 (HTTPS) open and listening for incoming connections. This is considered to be the norm.

Open port	Description
443	*Default usage:* http protocol over TLS/SSL *Potential malware:* W32.spybot.nps, Slapper
80	*Default usage:* World Wide Web HTTP *Potential malware:* 711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Code Red, Executor, God Message, God Message 4 Creator, Hooker, IISworm, MTX, NCX, Nimda, Noob, Ramen, Reverse WWW Tunnel Backdoor, RingZero, RTB 666, Seeker, WAN Remote, Web Server CT, WebDownloader, BlueFire, Duddie, Intruzzo, Latinus, Lithium, MscanWorm, NerTe, Optix Lite, Optix Pro, Power, Remote Shell, Scalper, Screen Cutter, Slapper, God Message Creator
25	*Default usage:* Simple Mail Transfer *Potential malware:* Ajan, Antigen, Barok, BSE, Email Password Sender - EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Stukach, Tapiras, Terminator, WinPC, WinSpy, Laocoon, Nimda

✓

RDP

Remote Desktop Protocol (RDP), the Microsoft Windows component that allows remote access to employees is commonly abused by Cybercriminals to gain illicit access to business networks to steal sensitive information and spread Ransomware infections.

Security Incidents

Severe security-related incidents (e.g., malware infections, exposed emails, usernames, passwords, and data breaches).

739

Exposed Clear Text Credential Count

Count of the exposed clear text username and password combinations related to the organization in question. This information is collected from data dumps of data breaches as they surface in various cybercrime-related forums on the dark web.

681

Exposed Weak Password Count

Count of exposed weak passwords related to the organization in question. This number is a part of the exposed clear text credential count and it sheds light on the security posture and maturity of a given organization by observing whether their employees use strong passwords across their accounts.

338

Exposed Hashed Credential Count

Count of the exposed hashed ("encrypted") username and password combinations related to the organization in question. This information is collected from data dumps of data breaches as they surface in various cybercrime-related forums on the dark web.

Exposed Credentials by Date

Date	Exposed Credential Count
2022	152
4 November 2020	18
23 June 2020	1
2 October 2019	1
24 May 2019	2
May 2019	1
7 January 2019	270
2018 and earlier	632
Total	1077

0

Malware Infection Count

Count of the malware infections related to the organization in question. This information is collected from public IP blacklists, botnet nodes, Command and Control (C&C) servers, and proprietary threat intelligence services.

Mitigation Controls

A collection of mitigation controls that can assist the organization to reduce its risk from various security incidents.

✓

SSL/TLS Implemented?

SSL/TLS technology is making sure that any data transferred between users and sites, or between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which may include credit card numbers, other financial information, and names and addresses.

✓

Anti-DDoS Mitigation Implemented?

A distributed denial-of-service (DDoS) is a type of computer attack that uses a number of hosts to overwhelm a server, causing a website to experience a complete system crash. This type of denial-of-service attack is perpetrated by hackers to target large-scale, far-reaching and popular websites to disable them, either temporarily or permanently. This is often done by bombarding the targeted server with information requests, which disables the primary system and prevents it from operating. This leaves the site's users unable to access the targeted website.

X

DMARC Implemented?

Domain-based Message Authentication, Reporting & Conformance (DMARC) ensures that legitimate email is properly authenticating against established DKIM and SPF standards. DMARC is the first and only widely deployed technology that can make the “header from” address (what users see in their email clients) trustworthy. Not only does this help protect customers and the brand, but it also discourages cybercriminals who are less likely to go after a brand with a DMARC record.

Status: Not Valid

Details: A DMARC record does not exist for this domain or its base domain

X

SPF Implemented?

Sender Policy Framework (SPF) is an email authentication protocol that allows the owner of a domain to specify which mail servers they use to send mail from that domain. Brands that are sending emails have to publish SPF records in the Domain Name System (DNS). These records list which IP addresses are authorized to send emails on behalf of their domains. An SPF-protected domain is less attractive to phishers and is, therefore, less likely to be blacklisted by spam filters, ensuring legitimate email from that domain is delivered.

Status: Not Valid

Details: acme.com does not have a SPF TXT record

X

Security Headers

HTTP security headers help protect websites against common attacks like XSS and clickjacking. They should be configured on all web applications to improve security. Any item listed below requires an improvement.

Header	Details	Severity
x-frame-options	Header 'x-frame-options' is missing	WARN
strict-transport-security	Header 'strict-transport-security' is missing	WARN
content-security-policy	Header 'content-security-policy' is missing	WARN
x-content-type-options	Header 'x-content-type-options' is missing	WARN
referrer-policy	Header 'referrer-policy' is missing	WARN
permissions-policy	Header 'permissions-policy' is missing	WARN
server	Header 'server' contains value 'mini_httpd/1.31 ??May2019'	WARN

Digital Exposure

The level of presence, exposure, popularity, and recognition of the company’s brand and additional digital assets across the web.

Glassdoor

Glassdoor is a website where employees and former employees anonymously review companies and their management.

N/A - Reviews

N/A - Average Rating

Alexa

Alexa Internet often referred to just as Alexa, is a web traffic information, metrics, and analytics provider.

112,985 in Global Rank

378 mil/sec at Website Loading Time

N/A - Page View

1,102 Linking Websites

Facebook

Facebook is a social networking website where users can post comments, share photographs and post links to news or other interesting content on the web, chat live, and watch short-form videos.

N/A - Followers

N/A - Handle

Twitter

Twitter is an American online news and social networking service on which users post and interact with messages known as "tweets".

N/A - Followers

N/A - Handle

N/A - Following

LinkedIn

LinkedIn is a business and employment-oriented service that operates via websites and mobile apps.

"company/acme-communication-inc" Handle

Crunchbase

Crunchbase is a platform for finding business information about private and public companies. Crunchbase information includes investments and funding information, founding members and individuals in leadership positions, mergers and acquisitions, news, and industry trends.

"organization/accuware-inc-2" Handle

Google Search

"208,000"

Business Information

Business metrics, administrative metadata, country, vertical market, and business tags associated with the organization.

Business Metrics

The key business and financial metrics describing the organization in question.

1,000 Employees

N/A - Market Cap

100,000,000 Annual Revenue

Administrative Metadata

Administrative information describing the organization in question.

"54" SIC Code

1891 Year Founded

N/A - Ticker Symbol

1

Country

Countries where the organization in question has a significant business presence.

United States

1

Vertical Market

The market in which the organization in question offers goods and services specific to an industry, trade, profession, or other groups of customers with specialized needs.

Technology

16

Business Tags

Business-related tags describing the organization in question.

- **Retail**
- **Food**
- **Fishery**
- **Local Cuisine**
- **Personal Care**
- **Broadcasting**
- **Beverages**
- **Pharmacy**
- **Baked Goods**
- **Food Products**
- **Animals & Pets**
- **Grocery**
- **E-commerce**
- **Dairy Products**
- **Home & Garden**
- **B2C**

Recommendations

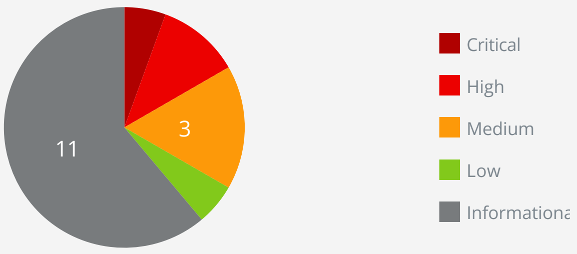
Snapshot date: 12/06/2023

Acme - Demo Company
United States
Technology
acme.com

Inherent Risk Score 26

Industry Median: 49

This page provides cyber risk improvement recommendations based on the Cyberwrite findings used in the report. Fixing these issues would potentially increase future scores and will increase security levels in the organization.


Severity Distribution

PROBABILITY ANALYSIS

Companies with a similar profile in the same sector have a probability of 8.93% to suffer a cyber incident within the next 12 months, which is 5.95 times more likely compared to industry peers median.

RECOMMENDATIONS FOR FINDINGS

Severity	Category	Title	Recommendation
● CRITICAL	Threat intelligence	Identified 739 exposed clear text credentials	Enforce Multi-Factor Authentication (MFA) solution across your network to reduce your risk of account compromises and data breaches by cybercriminals (this recommendation is a best practice and does not mean the company does not have MFA). Employ a centrally managed password manager to generate and manage passwords, and require MFA to access the password manager. Enforce a strict password policy: require a minimum length of 14 characters for password-only accounts and 8 characters for MFA-enabled accounts. Require each password to contain at least one special (non-alphabetic) character.Expire passwords at least once a year. Remember at least the last 5 passwords and prevent reuse.
● HIGH	Threat intelligence	Identified 338 exposed hashed credentials	Enforce Multi-Factor Authentication (MFA) solution across your network to reduce your risk of account compromises and data breaches by cybercriminals (this recommendation is a best practice and does not mean the company does not have MFA).
● HIGH	Threat intelligence	Identified 681 exposed weak passwords	Enforce strong password policy using a centrally managed password manager solution to reduce your risk of compromised accounts as a result of bruteforce (dictionary) attacks by cybercriminals.
● MEDIUM	Open ports	Identified 3 open ports	Review and close unnecessary open ports to reduce your attack surface, implement inbound network traffic filtering using a network Firewall to protect your open ports, and enable WAF protection for your website.
● MEDIUM	Mitigation controls	Spam mitigation control (SPF protocol) was not identified	Implement Sender Policy Framework (SPF) to protect your brand and customers from Phishing emails pretending to come from your domain names, leading to account compromises and data breaches.
● MEDIUM	Mitigation controls	Spam mitigation control (DMARC	Implement Domain-based Message Authentication, Reporting & Conformance (DMARC) to protect your brand and customers from Phishing emails pretending to come from your domain names, leading to account compromises and data breaches.

		protocol) was not identified	
● LOW	Digital attack surface	Identified 41 technologies	Review and remove unnecessary technologies to reduce your digital attack surface.
● INFORMATIONAL	Best practices	Business email compromise (BEC)	Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in an account number or payment procedures with the person making the request.
● INFORMATIONAL	Best practices	Cybersecurity awareness	Train employees in security principles. Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate Internet use guidelines, that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.
● INFORMATIONAL	Best practices	Cybersecurity hygiene	Protect information, computers, and networks from cyber attacks. Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.
● INFORMATIONAL	Best practices	Segregation of duties	Limit employee access to data and information, and limit authority to install software. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.
● INFORMATIONAL	Best practices	Payment cards	Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and do not use the same computer to process payments and surf the Internet.
● INFORMATIONAL	Best practices	WIFI networks	Secure your WIFI networks. If you have a WIFI network for your workplace, make sure it is secure, encrypted, and hidden. To hide your WIFI network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.
● INFORMATIONAL	Best practices	Access controls	Control physical access to your computers and create user accounts for each employee. Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.
● INFORMATIONAL	Best practices	Data backups	Make backup copies of important business data and information. Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.
● INFORMATIONAL	Best practices	Mobile devices	Create a mobile device action plan. Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.
● INFORMATIONAL	Best practices	Network Firewall	Provide firewall security for your Internet connection. A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.
● INFORMATIONAL	Best practices	Passwords and authentication	Require employees to use unique passwords and change passwords every three months. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

Regulatory Frameworks Impacted by Findings

The below table depicts some of the regulatory frameworks impacted by the findings.

Finding Type	AICPA - Trust Service Criteria (SOC 2 SM Report)	Shared Assessments - SIG v6.0	95/46/EC - European Union Data Protection Directive	ISO/IEC 27001:2013	ISO/IEC 27017:2015	NIST SP800-53 R3	PCI DSS v3.0	PCI DSS v3.2
Open Ports				Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1	12.4.1 12.6.1 CLD.9.5.2 15.1.1 15.1.3		2.1 2.2 2.5 5.1	2.1;2.2;2.5;5.1
Email Security (DMARC, SPF)				Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1	12.4.1 12.6.1 CLD.9.5.2 15.1.1 15.1.3		2.1 2.2 2.5 5.1	2.1;2.2;2.5;5.1
Exposed Credentials	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	B.1.8, B.1.21, B.1.28, E.6.2, H.1.1, K.1.4.5,	Article 17	A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5 A.9.1.2 A.9.4.1	9.2.1 9.2.2 9.1.2 9.4.1	AC-1 IA-1	3.5.1, 7.0 8.0 12.5.4	3.5.2;7.1;8.1;12.3.8;12.3.9;12.5.4
Weak passwords	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system	B.1.8, B.1.21, B.1.28, E.6.2, H.1.1, K.1.4.5,	Article 17	A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5 A.9.1.2 A.9.4.1	9.2.1 9.2.2 9.1.2 9.4.1	AC-1 IA-1	3.5.1, 7.0 8.0 12.5.4	3.5.2;7.1;8.1;12.3.8;12.3.9;12.5.4

	configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).							

For additional security recommendations and guidelines please visit https://www.nist.gov/cybersecurity. The Cyberwrite recommendations are subject to the disclaimer at the end of this report.

Coverages Description

3rd Party Liability

3rd Party Liability provides coverage for the cost of investigation, defence cost, and civil damages arising from defamation, libel, slander, copyright/trademark infringement, and negligence in the publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.

Breach of Privacy

Breach of Privacy provides coverage for specified expenses arising from a personal data compromise involving personally identifiable information of affected individuals. Affected individuals may be customers, clients members, directors, or employees of the Insured entity.

Business Interruption

Business Interruption provides coverage for the cost of loss of income that occurred due to network degradation or interruption as a result of a cyber-attack on the Insured, or an IT service provider, or a business process outsourcer that provides services to the Insured. The cost includes expenses incurred to mitigate and investigate such a loss.

Cyber Extortion

Cyber Extortion provides coverage for the cost of an investigator retained in connection with the extortion threat, and coverage for any amount paid by the Insured in response to the threat.

Example:
While trying to balance the books, a business owner received a strange pop-up on his laptop. A ransomware virus locked the system until an extortion demand was paid. After a consultation with the insurance carrier, the Insured decided to pay the demand for unlocking the system. The insurance carrier reimbursed the Insured for the amount of demand.

Data Loss

Data Loss provides coverage for specified expenses arising from the reconstitution of data and/or software that has been deleted or corrupted due to a cyber event.

Financial Theft & Fraud

Financial Theft & Fraud provides coverage for direct financial loss resulting from criminal deception using email, facsimile or telephone communications to induce an Insured, or a financial institution with which an Insured has an account, to send money or divert a payment.

Incident Response

Incident Response provides coverage for direct costs incurred to investigate and close the incident and to minimize post-incident losses. Applies to all the other categories/events.

Regulatory & Defence

Regulatory & Defence Cost provides coverage for the legal, technical, or forensic services necessary to assist the Insured in responding to governmental inquiries related to a cyber-attack, and inquiries alleging a breach of PCI standards. It provides coverage for fines, penalties, defence costs, investigations, or other regulatory actions where in violation of privacy law and PCI standards, and other costs of compliance with regulators and industry associations. Insurance recoveries provided where it is permissible to do so.

Cyber Risk Report Explanation

About this Report

Every business is exposed to cybersecurity risks, such as ransomware, theft of customer data, misdirected payment fraud, and various other risks. These attacks can cause severe financial losses as a result of financial theft, regulatory fines, business interruption, reputational damage, and more. No company is entirely immune to threats. Even those with a limited digital presence and advanced cyber risk mitigations may suffer an incident or a breach.

As a business owner or an executive, quantifying and benchmarking your organization's exposure and making sense of cyber risks in a data-driven manner can be time-consuming, costly, and, in many cases, confusing. Cyberwrite, a leading pioneer of the patented AI-driven cyber risk orchestration and quantification technology Vivaldi™ and 4SEEN™, was established in 2017 to enable businesses worldwide to understand their organization's inherent cyber risks quickly and clearly so they can reduce their exposure and mitigate potential losses when attacks occur. Cyberwrite's platform simplifies cyber risk analysis, providing a simple-to-understand report that can enable you to be better prepared to get the cyber insurance policy you need to have and improve your company's cyber readiness level.

How it works

Cyberwrite's cyber risk report summarizes key information a business needs to be aware of in order to make an informed business decision related to cyber risk exposure and mitigation, cyber insurance policies, and cybersecurity measures.

Each Cyberwrite report is generated in a non-invasive manner. It is based on publicly available data from online sources, drawing on the unique digital exposure and attack-surface of the company being reviewed, and is combined with the company's sector and geography-related risk. The data is then compared to a large dataset collected on similar companies (by size and industry) that suffered cyber damages in the past. Using advanced analytics and actuarial science the platform calculates a normal risk distribution and a risk score for each company to provide an indication of the inherent risk level. A high score does not mean a company won't be breached and a low score does not mean a company will be breached. A company can have an effective protection program in place and still be at medium or high risk. The internal mitigation actions deployed by the company are not visible to Cyberwrite and are not considered in the inherent risk score calculation.

What you'll learn

The first page of the cyber risk report is comprised of three parts:

Part I - Risk Benchmarking

Cyberwrite's cyber risk benchmarking first enables companies to understand how their risk compares to their peers. Each company is scored with an overall cyber risk score, ranging from 1 to 100. This is a comparative score that evaluates the company's risk in comparison to the average risk score of similar companies in the relevant industry. The higher the score, the lower the risk compared to other companies. Companies with a risk score closer to 1 are more likely to suffer impacts from a cyber incident while companies closer to 100 are less likely to suffer such impacts.

Companies can also view their risk score by risk type and exposure—for instance, data compromise, cyber extortion, misdirected payment fraud, and so on—that may result in a financial loss for the company. Each company also receives a score of 1 to 100 for each risk type that is compared to the industry average for that risk type. The company's score is marked by a triangle on the benchmarking graph, while the average score of its industry peers is marked by a circle.

Each company's risk score is calculated using a combination of industry, geographic, and customer-specific data collected using open-source intelligence, such as attack surface, digital exposure, technological profile, historical incidents, externally visible mitigation actions, geographical attack trends, patterns, and more. Cyberwrite uses each company's domain name as a unique ID to gather data online. The Cyberwrite platform collects all the data and then maps the findings to the various risk types using advanced analytics and AI, machine learning tools, and cyber risk and severity frameworks, such as those provided by NIST (National Institute for Standards & Technology).

The report also forecasts the probability of experiencing a cyber incident within the next 12 months, as well as the probability of such an incident compared to industry peers.

Part II – Example Risk Indicators

Based on the data collected by the Cyberwrite platform, the second part of the report provides insights into which risk domains require attention, including critical vulnerabilities correlated to claims and breaches, exposed credentials that may enable swift access into the insured's organization, open ports, missing mitigation technologies and more. The full data list is provided in the report.

Each indicator is associated with a green or red status signaling whether action should be taken. Additional data to help businesses understand the nature of the risk, regulatory impact, and recommendations for improvement are available in the full report provided following the one-page report. A full list of all findings is available on the report's data page.

Part III - Financial Loss Estimator

The platform also enables a company to understand its estimated potential financial loss range due to cyber damages. The Cyberwrite platform utilizes historical financial damages data and statistical models collected from government publications, research publications, and other data sources. Through its proprietary and patented algorithm, Cyberwrite enables companies to obtain a data-driven estimation of the range of the financial damages posed to their organization for each risk type. This is an estimation only and it is important to note that the actual damages may be higher or lower than the figure presented in the report. This report does not serve as a substitute for a full onsite assessment to determine the profiled company's cyber risk and potential loss. It is recommended to acquire more coverage than the estimated aggregated loss as actual future damages may be higher. Some reports may not contain financial loss estimations.

About Cyberwrite

Founded in 2017 by cyber security and insurance industry veterans, Cyberwrite products are used globally by leading insurers, reinsurers, agents, brokers, and businesses to analyze the cyber risk levels and potential economic impact a cyberattack may have on a business, benchmark risk levels, and discover potential security issues in real-time. The company's first-of-kind patented cyber insurance AI model, 4SEEN®, draws on years of proprietary historical data and extensive cyber insurance dedicated research and datasets to predict and benchmark cyber insurance risk. Cyberwrite is a Gartner Cool Vendor, Frost & Sullivan Excellence Award Winner, and a graduate of the FinTech Innovation Lab New York in partnership with Accenture. The solution is available worldwide in eight languages and accessible through both SaaS and API interfaces.

FOR QUESTIONS ON THE FINDINGS OF THIS REPORT, PLEASE CONTACT: SUPPORT@CYBERWRITE.COM

Disclaimer

CYBERWRITE PROVIDES ITS SERVICES FOR INFORMATIONAL PURPOSES ONLY ON AN “AS IS” BASIS. CYBERWRITE MAKES NO WARRANTY OR REPRESENTATION REGARDING THE SERVICES, ANY INFORMATION, MATERIALS, GOODS OR SERVICES OBTAINED THROUGH THE SERVICES, OR THAT THE SERVICES WILL MEET ANY CUSTOMER REQUIREMENTS, OR BE UNINTERRUPTED, TIMELY, SECURE OR ERROR FREE. CYBERWRITE EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. USE OF THE SERVICES ARE AT CUSTOMER’S SOLE RISK. CUSTOMER WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO CUSTOMER RESULTING FROM THE USE OR RELIANCE UPON SUCH SERVICES. CYBERWRITE PROVIDES ITS PRODUCTS AND SERVICES ONLY FOR INFORMATIONAL PURPOSES AND DOES NOT WARRANT THAT THESE PRODUCTS AND SERVICES WILL IDENTIFY OR DETECT ALL RELEVANT INFORMATION, OR THAT CYBERWRITE’S ALGORITHMS, REPORTS, OR OTHER MATERIALS OR ADVICE WILL BE ERROR-FREE OR COMPLETE. CYBERWRITE DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO ITS SERVICES, MATERIALS, AND PRODUCTS. CYBERWRITE SHALL NOT BE RESPONSIBLE OR LIABLE FOR THE ACCURACY OR USEFULNESS OF ANY INFORMATION THE COMPANY PROVIDES, OR FOR ANY USE OF SUCH INFORMATION BY USERS, CUSTOMERS OR OTHERS.