

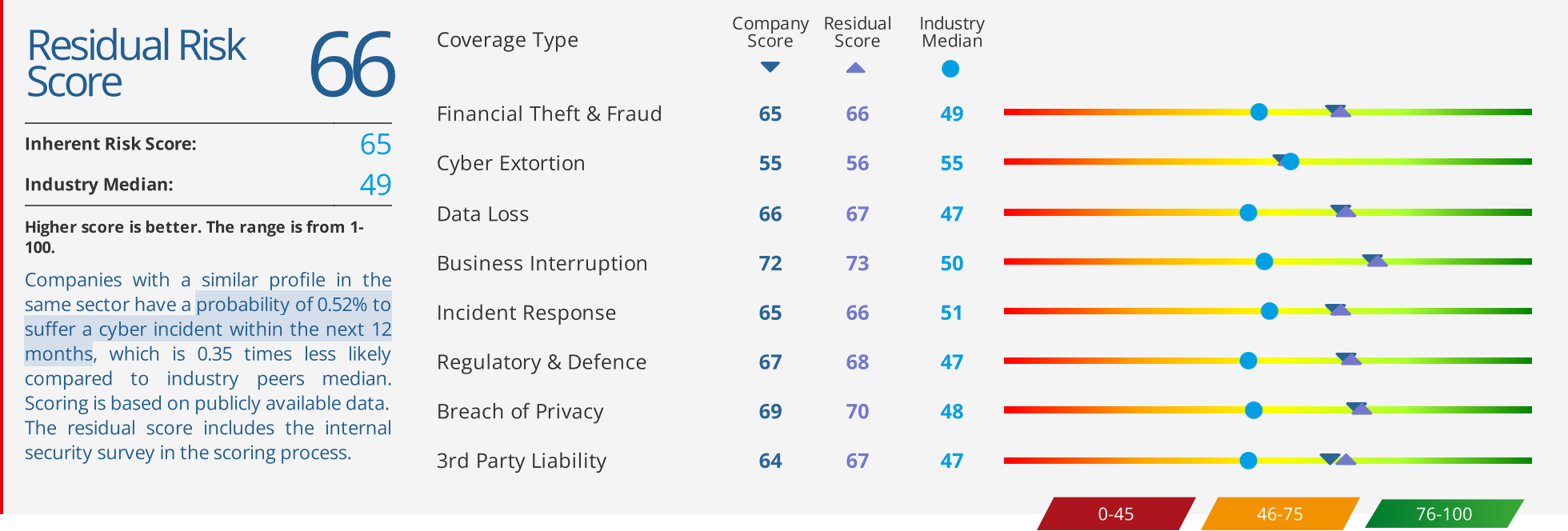
northerntool

United States

Communications

www.northerntool.com

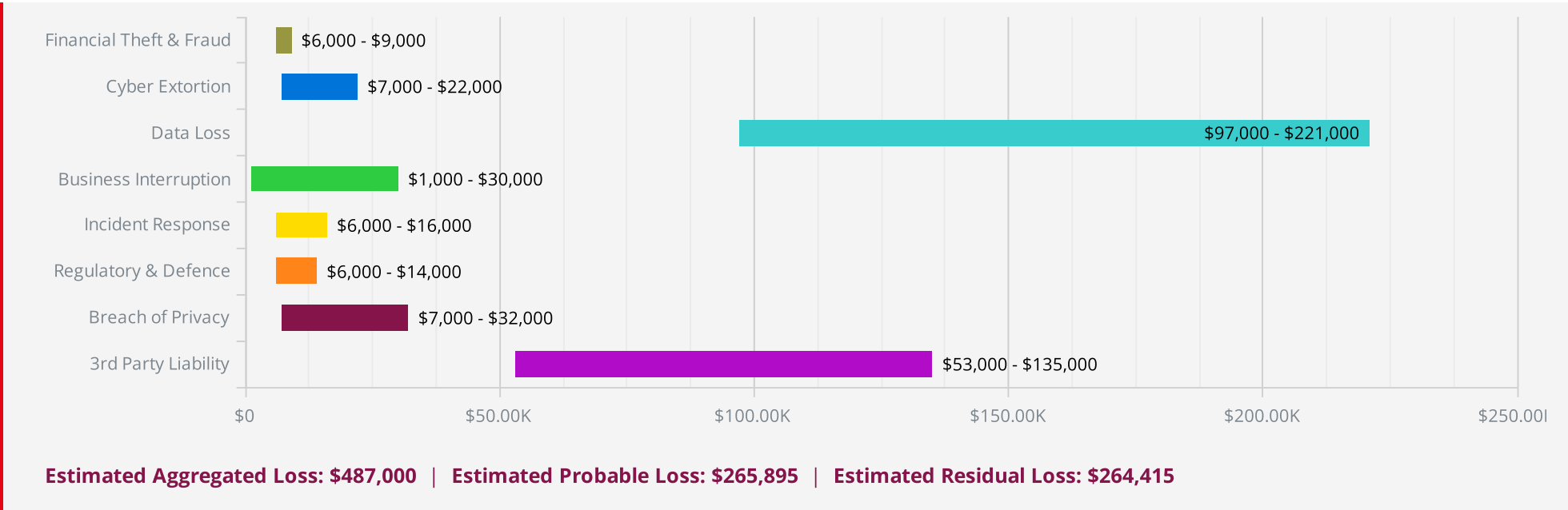
CYBER RISK BENCHMARKING



RISK INDICATORS

RISK DOMAIN	STATUS	DETAILS	RISK INDICATORS EXPLANATION
Open Ports	●	2	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	●	Implemented	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	●	679	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



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



northerntool
United States
Communications
www.northerntool.com

UNDERWRITING SCORE

Inherent Underwriting Score
(-24 to +24)

7

Inherent Risk Score: 65

RANGE RECOMMENDATION
Positive Score Insure

This underwriting score is used for overall benchmarking of cyber risk compared to relevant population in the target industry and geography and presents recommended underwriting actions.

COVERAGE TYPE	INHERENT UNDERWRITING SCORE
Financial Theft & Fraud	1
Cyber Extortion	0
Data Loss	1
Business Interruption	1
Incident Response	1
Regulatory & Defence	1
Breach of Privacy	1
3rd Party Liability	1

PROBABILITY ANALYSIS

Companies with a similar profile in the same sector have a probability of 0.52% to suffer a cyber incident within the next 12 months, which is 0.35 times less likely compared to industry peers median.

Probable loss: \$265,895 Aggregated loss: \$487,000

DESCRIPTION

Highly Negative

Negative

Moderate

Positive

Highly Positive

-24 to -16

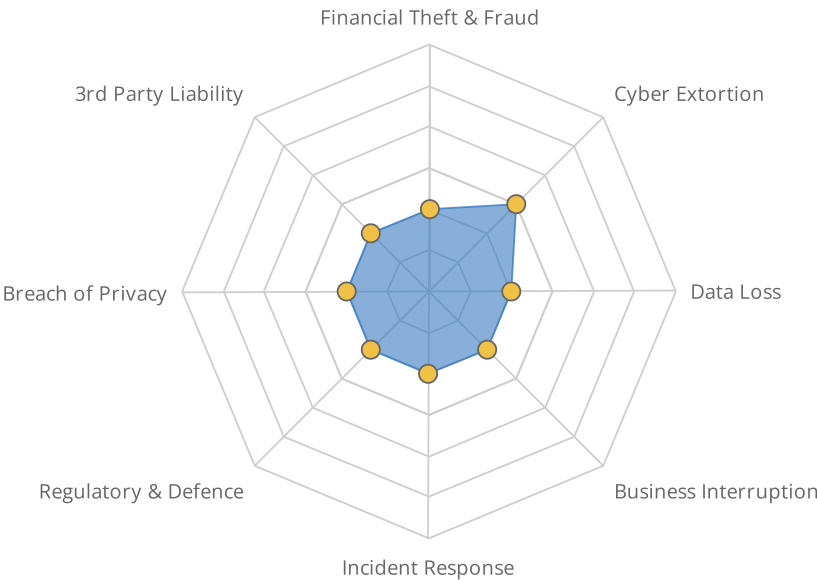
-15 to -6


-5 to 5

6 to 15

16 to 24

RANGE	RECOMMENDATION
Highly Negative Score	Consider to avoid
Negative Score	Additional review
Moderate	Filter by sector risk
Positive Score	Insure
Highly Positive Score	Insure





northerntool

United States

Communications

www.northerntool.com

Residual Risk Score

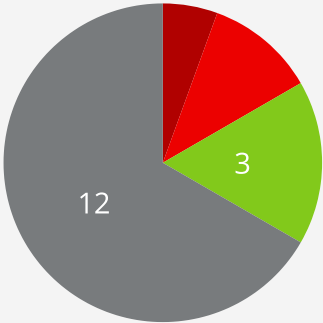
66

Inherent Risk Score:65

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



Critical

High

Medium

Low

Informational

PROBABILITY ANALYSIS

Companies with a similar profile in the same sector have a probability of 0.52% to suffer a cyber incident within the next 12 months, which is 0.35 times less likely compared to industry peers median.

RECOMMENDATIONS FOR FINDINGS


Severity	Category	Findings	Best Practice Recommendation
● CRITICAL	Threat intelligence	Identified 515 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 164 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 473 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.
● LOW	Digital attack surface	Identified 40 technologies	Review and remove unnecessary technologies to reduce your digital attack surface.
● LOW	Digital attack surface	Identified 18 subdomains	Review and remove unnecessary subdomains to reduce your digital attack surface.
● LOW	Digital attack surface	Identified 41 IP addresses	Review and remove unnecessary IP addresses to reduce your digital attack surface.
● 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	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

Severity	Category	Findings	Best Practice Recommendation
			with the person making the request.
● 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.
● 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	Social networks exposure	Identified significant presence on social networks	Subscribe to online reputation management services to protect your brand reputation and reduce your risk of electronic media liability.

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
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 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
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.								



northerntool

United States

Communications

www.northerntool.com

Security Questionnaire

Account Monitoring And Control

NIST CSF	Question	Answer	File Submitted
PR.AC-7	What percentage of your user accounts use multi-factor authentication (MFA)?	11%	No
PR.AC-1	What percentage of your accounts are included in the organization's inventory?	22%	No

Application Software Security

NIST CSF	Question	Answer	File Submitted
PR.IP-2	Have you implemented secure coding practices appropriate to the programming language and development environment being used by your software developers?	Yes	No
DE.CM-8	Have you implemented static and dynamic analysis tools to discover vulnerabilities in your internally developed software?	No	No
PR.PT-4	Have you deployed web application firewalls (WAFs) that inspect all traffic flowing to your web applications for common web application attacks?	N/A	No

Boundary Defense

NIST CSF	Question	Answer	File Submitted
DE.CM-1	What percentage of your network devices record network packets passing through the network?	12%	Yes
DE.CM-1	What percentage of your network devices have network-based Intrusion Detection Systems (NIDS) sensors to look for unusual attack mechanisms and detect a compromise of these systems?		No
DE.CM-1	What percentage of your network devices use network-based Intrusion Prevention Systems (NIPS) sensors to look for unusual attack mechanisms and prevent a compromise of these systems?		No

Continuous Vulnerability Management

NIST CSF	Question	Answer	File Submitted
ID.RA-1 DE.CM-8	What percentage of your computing devices have been scanned by a configuration monitoring system to identify all potential vulnerabilities on the organization's systems?		No
PR.IP-12	What percentage of your computing devices are regularly updated by automated software update tools to ensure that the operating systems are running the most recent security updates provided by the software vendor?		No

Controlled Access Based On The Need To Know

NIST CSF	Question	Answer	File Submitted
PR.DS-1	What percentage of your sensitive information is encrypted at rest and requires an out-of-band authentication to access the information?		No

Controlled Use Of Administrative Privileges

NIST CSF	Question	Answer	File Submitted
PR.AC-1	What percentage of your computing devices use automated tools to inventory all administrative accounts to ensure that only authorized individuals have elevated privileges?		No
PR.AC-4	What percentage of your system administrators use a dedicated machine for all administrative tasks or tasks requiring elevated access?		No
PR.PT-3	What percentage of your systems limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities?		No

Cyber Insurance

NIST CSF	Question	Answer	File Submitted
RC.RP-1	Do you have a cyber insurance policy in place?		No

Data Protection

NIST CSF	Question	Answer	File Submitted
ID.AM-5	Do you maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider?		No
PR.DS-5	Have you deployed a Data Leakage Prevention (DLP) solution that monitors for sensitive information and blocks such transfers while alerting the information security personnel?		No
PR.DS-5	Do you allow access to only authorized cloud storage or email providers?		No
PR.DS-1	What percentage of your mobile devices utilize full disk encryption?		No

Data Recovery Capabilities

NIST CSF	Question	Answer	File Submitted
PR.IP-4	What percentage of your computing devices back up system data automatically regularly?		No
PR.PT-5	Have you implemented any high availability solutions (e.g., CDN, load balancer, DR)?		No

Email And Web Browser Protections

NIST CSF	Question	Answer	File Submitted
DE.CM-7	What percentage of your computing devices utilize network-based URL filters?		No
DE.CM-1 DE.CM-7	What percentage of your DNS servers use DNS filtering to help block access to known malicious domains?		No
DE.CM-4	Have you implemented a sandboxing solution to analyze and block inbound email attachments with malicious behavior?		No

Implement A Security Awareness And Training Program

NIST CSF	Question	Answer	File Submitted
PR.AT-1 ID.AM-6	Have you implemented a security awareness program for all employees to complete regularly to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization?		No

Incident Response And Management

NIST CSF	Question	Answer	File Submitted
PR.IP-9	Have you prepared written incident response plans that define the roles of personnel, and provide instructions for operating incidents?		No

Inventory And Control Of Hardware Assets

NIST CSF	Question	Answer	File Submitted
DE.CM-7	What percentage of your networks have been scanned by an active asset discovery tool?		No
ID.AM-1 PR.DS-3	What percentage of your computing devices are included in the organization's asset inventory?		No

Inventory And Control Of Software Assets

NIST CSF	Question	Answer	File Submitted
ID.AM-2	What percentage of your software are included in the organization's software inventory?		No
PR.DS-6 DE.CM-7	What percentage of your computing devices use application whitelisting technology to block unauthorized applications from executing on the system?		No
DE.CM-7	What percentage of high-risk business applications are segregated from other business systems?		No

Limitation And Control Of Network Ports, Protocols, And Services

NIST CSF	Question	Answer	File Submitted
DE.CM-8	What percentage of your computing devices are regularly scanned by a port scanner to alert if unauthorized ports are detected on a system?		No
PR.IP-1	What percentage of your computing devices use host-based firewalls or port filtering tools on endpoints, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed?		No
PR.IP-1	What percentage of your critical servers use application layer firewalls to verify and validate the traffic going to the server?		No

Maintenance, Monitoring, And Analysis Of Audit Logs

NIST CSF	Question	Answer	File Submitted
DE.AE-3	What percentage of your computing devices use at least three synchronized time sources from which all servers and network devices retrieve time information regularly so that timestamps in logs are consistent?		No

NIST CSF	Question	Answer	File Submitted
PR.PT-1 DE.AE-3	What percentage of your computing devices collect and send logs to a central log management system for analysis and review?		No

Malware Defenses

NIST CSF	Question	Answer	File Submitted
DE.CM-4	What percentage of your computing devices use centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers?		No
PR.IP-1	What percentage of your computing devices use anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR)?		No

Penetration Tests And Red Team Exercises

NIST CSF	Question	Answer	File Submitted
DE.DP-5	Have you implemented a plan for penetration testing against your networks, computing devices, and applications?		No

Secure Configuration For Hardware And Software On Mobile Devices, Laptops, Workstations, And Servers

NIST CSF	Question	Answer	File Submitted
PR.IP-1	What percentage of your computing devices use secure images or templates based on the organization's approved configuration standards?		No

Secure Configuration For Network Devices, Such As Firewalls, Routers, And Switches

NIST CSF	Question	Answer	File Submitted
PR.IP-1	What percentage of your network devices use a standard, documented security configuration standard for the device?		No

Wireless Access Control

NIST CSF	Question	Answer	File Submitted
DE.CM-1	What percentage of your facilities have a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network?		No

Financial Questionnaire

Question	Answer
Medical Data Records	100
Personal Data Records	200
Credit Card Data Records	300
Full Time Employees	111
IT Employees	11
Cyber/Information Security	1
Percentage from online business	11
Firewall	Yes
Antivirus	No
Using Backup	No
Other	No
Annual total revenue	\$ 100,000

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.

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.