cowbell®

CYBER RISK REPORT

PREPARED FOR

Neti Group State Bank

GENERATED ON March 09, 2025

www.cowbell.insure

ABOUT YOUR CYBER RISK REPORT

This Cyber Risk Report is an overall evaluation of your organization's risk profile, presenting individualized findings with personalized recommendations for remediation. By following the outlined recommendations, you can proactively address risk exposures, improve your risk profile, and strengthen your organization's resilience. You can further analyze all scan results from the Insights page in the Cowbell Platform.

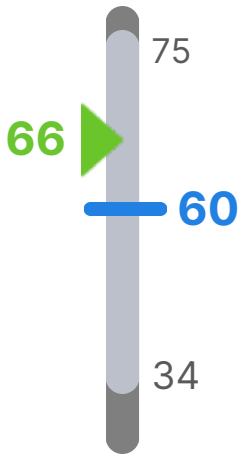
TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Executive Summary is an overview of our findings identified with top-of-the-line risk monitoring technology. We have compiled data from public databases, third-party vendors, proprietary external scanners, dark web intelligence, and compliance information to describe your cyber risk posture and identify targeted risk points in your organization's infrastructure.

COWBELL FACTOR COMPARISON

Your Company Cowbell Factor compared to other organizations in your industry.



Company Name: Neti Group State Bank

Domain: netigroupstatebank.com

No. of Employees: 3

Company Cowbell Factor: 66

Industry: 522110 - Commercial Banking

Industry Cowbell Factor: 60

Your Company Cowbell Factor is **higher than** the Industry Cowbell Factor, presenting a **lower risk** than your industry peers. A good Company Cowbell Factor is greater than or equal to the Industry Cowbell Factor.

Min/Max Industry Cowbell Factors | Industry Average | Cowbell Factor ≥ Industry Average | Cowbell Factor < Industry Average

SPOTLIGHTS

Spotlights are any software or system vulnerabilities actively being exploited in real-world attacks. You currently have **0 Spotlights** that need immediate remediation.

SPOTLIGHTS	0

INSIGHTS

Insights are identified risk exposures categorized by risk level. You currently have **2 'Medium'** Insights that require immediate attention.

VERY HIGH	HIGH	MEDIUM	LOW
0	0	2	0

DARK WEB EXPOSURE

Dark Web Exposure is exposed data related to your organization discovered by dark web scanners.

2025

EXPOSED EMAILS	EXPOSED PASSWORDS	HASHED PASSWORDS
0	0	0

Request a Dark Web Report for a detailed view of your most recent exposure.

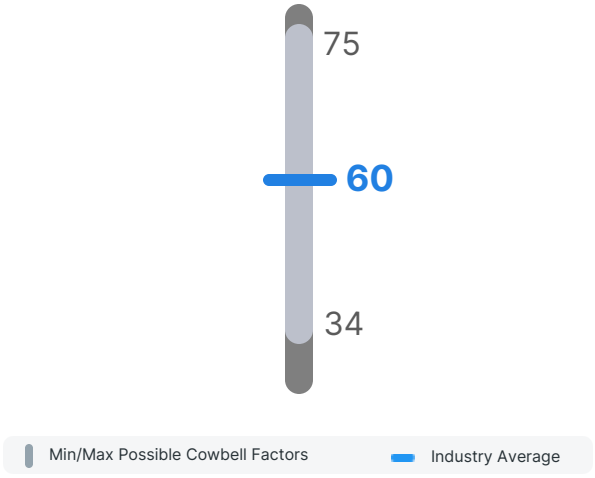
YOUR INDUSTRY OVERVIEW

NAICS: 52

Industry: Finance and Insurance

The Industry Overview provides deeper insights into your industry's risk profile, examining the common risks associated with your industry and standard security best practices to help keep your business safe.

The Industry Cowbell Factor presents the average risk rating for your industry.



Common Risks

- Cyberattack
- Data Breach
- Lost or Stolen Devices

Recent Cyber Incidents

MOVEit

On May 31, 2023, a critical SQL injection vulnerability was discovered in a document transfer solution service by MOVEit Transfer, compromising many firms utilizing the software.

Veeam

In August 2023, Veeam identified a high-severity vulnerability impacting their Veeam Backup & Replication (VBR) software, allowing attackers to obtain sensitive data and credentials. The VBR software is used by more than 450,000 customers worldwide.

INDUSTRY DESCRIPTION

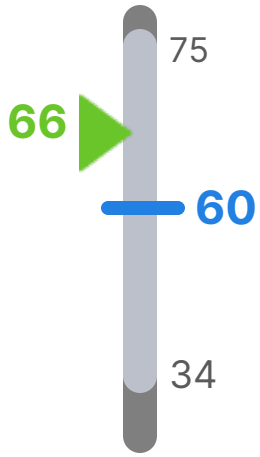
The Finance and Insurance industries can be susceptible to cyber incidents due to the sensitive nature of their business. Since financial data and claims history are often stored on shared network drives, a cybercriminal may target your organization to infiltrate your clients' private information. A lost or stolen device can be exceptionally dangerous, as it can compromise your client's data and even result in a lawsuit. In the event of a cyber incident, business can be halted completely, and backup data could be nearly impossible to restore. Cyber insurance can help you recover from a cyber incident and cover liability and damages caused to third parties.

SECURITY BEST PRACTICES

- Enforce the use of strong, unique passwords
- Deploy multi-factor authentication
- Avoid poorly secured public wifi
- Install security software on all devices
- Train employees to only access sensitive data from company devices through an encrypted VPN connection

COWBELL FACTORS

Cowbell Factors are our proprietary risk ratings that evaluate your organization's risk compared to industry peers. They are compiled from more than 1,000 data points and risk signals to present an accurate evaluation of your organization's risk. A higher Cowbell Factor represents a lower level of risk. You can improve your Cowbell Factors by addressing insights and following the recommended steps for remediation.



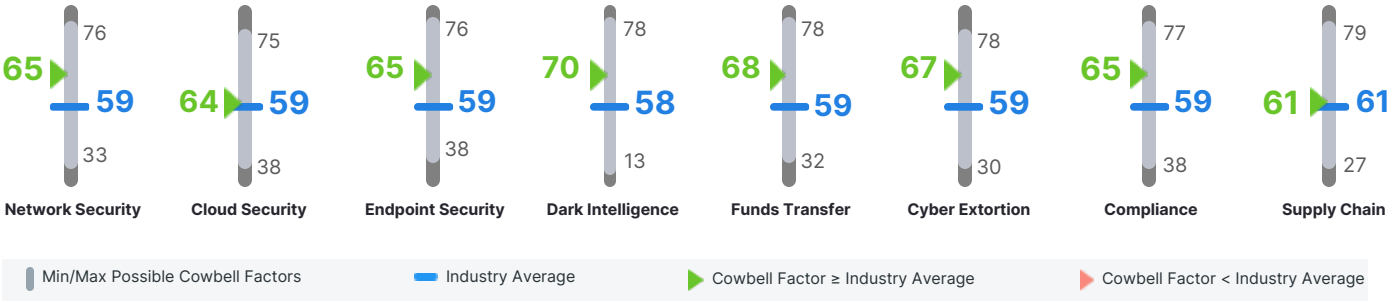
Company Cowbell Factor

The Company Cowbell Factor is the weighted average of all the Cowbell Factors and is a good metric to benchmark a company against its peers.

Industry Cowbell Factor

The Industry Cowbell Factor measures an industry's overall cyber risk factor. It is calculated for each industry based on Cowbell's risk pool, incorporating information from proprietary scanners and external data sources.

CONTINUOUS RISK ASSESSMENT



Network Security
An organization's overall network infrastructure security strength.

Cloud Security
An organization's cloud security strength based on your footprint and security best practices.

Endpoint Security
An organization's preparedness for cyberattacks.

Dark Intelligence
An organization's exposure to the dark net measured by data type, volume, and value.

Funds Transfer
An organization's susceptibility to fraudulent funds transfers.

Cyber Extortion
An organization's exposure to extortion-related attacks.

Compliance
An organization's level of compliance with security standards.

Supply Chain
Your organisation's susceptibility to software supply chain incidents.

SPOTLIGHTS

Spotlights are any software or system vulnerabilities that are actively being exploited in real-world attacks. These vulnerabilities have a heightened level of urgency and importance, and we have identified that your organization is potentially exposed to the following Spotlights.

0 **Spotlights were identified for your organization.**

INSIGHTS

Insights present risk information that has been compiled for your organization. This report includes your Insights that require immediate action. You can view a complete list of your identified Insights in the Cowbell Platform.

Severity
Medium

Date Captured
March 09, 2025

Most Impacted Cowbell Factor
Network Security

INSIGHT

An MX record was found and is not secured by Domain Name System Security Extensions (DNSSEC). DNSSEC is a feature of the Domain Name System (DNS) that authenticates responses to domain name lookups.

Data Source: cowbell®

Recommended Action

Strengthen the security of your domain by implementing Domain Name System Security Extensions (DNSSEC) to authenticate and secure MX records, fortifying your defense against potential DNS-related vulnerabilities.

Severity
Medium

Date Captured
March 09, 2025

Most Impacted Cowbell Factor
Network Security

INSIGHT

SPF record found is not secured by Domain Name System Security Extensions (DNSSEC) DNSSEC is a feature of the Domain Name System (DNS) that authenticates responses to domain name lookups.

Data Source: cowbell®

Recommended Action

Strengthen SPF record security by implementing Domain Name System Security Extensions (DNSSEC) to authenticate and secure responses to domain name lookups, preventing potential DNS-related vulnerabilities.

DOMAIN NAME SYSTEM (DNS)

DNS is a system that translates domain names into IP addresses, allowing browsers to load internet resources. Each device connected to the internet has a unique Internet Protocol (IP) address that web browsers use to interact. Bad actors can use your DNS records to identify your attack surfaces, making it important for you to identify records associated with your organization. We have compiled your organization's identified DNS records.

A Records

An A Record matches a domain to an IPv4 address.

Domain [2]	IPv4 Address
netigroupstatebank.com	13.248.243.5
netigroupstatebank.com	76.223.105.230

MX Records

A Mail Exchange (MX) Record directs emails to a mail server, indicating how emails should be routed.

Domain [1]	Mail Servers
netigroupstatebank.com	netigroupstatebank-com.mail.protection.outlook.com

NS Records

A Nameserver (NS) Record contains the name of the authoritative name server within a domain name.

Domain [4]	Mail Servers
netigroupstatebank.com	ns16.domaincontrol.com
netigroupstatebank.com	173.201.75.8
netigroupstatebank.com	ns16.domaincontrol.com
netigroupstatebank.com	2603:5:22b0::8

TXT Records

A TXT record contains text information for sources outside of your domain.

Domain [2]	Records
netigroupstatebank.com	netigroupstatebank.com v=spf1 include:secureserver.net -all
netigroupstatebank.com	NETORGFT18409445.onmicrosoft.com

* Contact Risk Engineering to get a complete copy of your DNS records.

DARK WEB EXPOSURE

The Dark Web Exposure evaluation provides high-level details on exposed data related to your organization on the dark web. You can request a comprehensive dark web intelligence report by emailing our risk engineering team directly.

2025

EXPOSED EMAILS	EXPOSED PASSWORDS	HASHED PASSWORDS
0	0	0

No Dark Web Exposures were identified for your organization in 2025.

FREQUENTLY ASKED QUESTIONS

How do I improve my Cowbell Factors?

The best way to improve your Cowbell Factor rating is to utilize the services bundled in your policy. You can improve your rating and strengthen your risk posture by addressing actionable insights, activating connectors, and scheduling a risk engineering assessment call.

How are Cowbell Factors calculated?

Cowbell Factors are compiled from more than 1,000 data points and risk signals. The collected information is normalized and standardized with a weighted mapping to Cowbell Factors.

I cannot close some open ports because we do not host our environment. How should I address these insights?

Consult your hosting provider to ensure that the open ports are necessary. If they are required, ensure that they are configured correctly.

Why should I address a Spotlight?

Spotlights are actively exploited software or system vulnerabilities, presenting a considerable risk to your organization. If you are using impacted software, patch and follow our recommended remediation steps to prevent a cyber incident.

Who should review my Cyber Risk Report?

Security professionals, including your CTO, CISO, MSPs, and IT personnel, should review your Cyber Risk Report. Your report also includes valuable insights that should be shared with C-Suite Members, ensuring that your organization makes informed decisions for preparedness. By understanding your risk posture, your organization will be more prepared to allocate resources, create a budget, determine proper defense strategies, and select the appropriate insurance coverage.

YOUR NEXT STEP

Our risk engineers are a team of cybersecurity experts prepared to asist you in interpreting your insights and improving your risk posture.

Book a call with our Risk Engineering team today!

COWBELL 365

Cowbell 365 is an around-the-clock service that offers policyholders comprehensive support for risk improvement and incident response. By providing 24-hour availability every day of the week, 365 days of the year, Cowbell 365 brings unprecedented levels of expertise and responsiveness from our in-house team of dedicated cyber claims specialists and cyber risk engineers.

While we are always available to assist you in the event of a cyber incident, our unique, closed-loop approach to risk management strives to proactively reduce your risk exposure and build your resilience. Cowbell Insights are continuously generated with recommendations to remediate cybersecurity weaknesses and identify unique opportunities to improve risk ratings. Our risk engineering professionals are available to help you strengthen your cybersecurity posture with one-on-one guidance to improve your risk profile and maximize the value of your cyber insurance policy.

OUR RISK ENGINEERING RESOURCES

Cybersecurity Awareness Training

Receive cybersecurity awareness training for all your employees.

Risk Engineering Assessment Calls

Get personalized recommendations from risk engineering professionals to improve your risk profile and identify cybersecurity gaps.

Incident response plan guide

Create your Incident Response Plan from our downloadable template that outlines the process to respond to and recover from a potential cyber incident.

And More!

TAKE ADVANTAGE OF YOUR RISK RESOURCES

We bundle risk management resources with every policy, helping strengthen your cyber environment.

Book a call with our risk engineering team to learn more!

KEY TERMS

Asset:

Any valuable component within an organization's IT infrastructure, such as hardware, software, data, or web properties that holds importance to the organization's operations.

Common Vulnerabilities and Exposures (CVE):

A standardized identifier assigned to a specific software or hardware vulnerability, making it easier to track and share information about vulnerabilities across different systems and platforms.

Dark Web:

A hidden part of the internet not indexed by search engines. It is often associated with illegal activities and provides an anonymous environment for cybercriminals to conduct illicit transactions.

IP address:

A unique numerical identifier assigned to each device connected to a computer network. It enables devices to communicate and identify each other on the internet or within a private network.

IPv4:

IPv4 (Internet Protocol version 4) is the most widely used version of the IP protocol. It uses a 32-bit addressing scheme and supports approximately 4.3 billion unique IP addresses.

IPv6:

IPv6 (Internet Protocol version 6) is the latest version of the IP protocol. It uses a 128-bit addressing scheme and provides a much larger address space to accommodate the growing number of devices connected to the internet.

Ransomware:

Malicious software that encrypts a victim's files or locks their entire system, demanding a ransom payment in exchange for restoring access. It poses a significant threat to organizations' data and can cause operational disruptions.

Vulnerability:

A weakness or flaw in a system's design, implementation, or configuration that bad actors can exploit to compromise the system's security and gain unauthorized access or control.

Zero-day exploit:

A previously unknown software vulnerability actively exploited by bad actors before a patch or fix is available. It poses a significant risk as there is no defense or mitigation strategy in place.

cowbell®

Adaptive Cyber Insurance for Today's and Tomorrow's Threats

Contact Us

Support@cowbellcyber.ai

Claims@cowbellcyber.ai

(833) 633-8666

www.cowbell.insure

VER_RR_US_JAN 10, 2024_REV1