HOW TO READ THE NAS CYBER RISK REPORT

The NAS Cyber Risk Report (NAS Report) provides brokers and potential policyholders ("organization") with a high-level understanding of the potential policyholder’s risk profile against some of today’s common cyberattacks.

The NAS Report is compiled from an assessment tool that includes:

- non-intrusive vulnerability scanning\(^1\) of an organization’s Internet-facing systems and applications; and
- a comprehensive search of over 100 databases of known malware, blacklists and known cybersecurity vulnerabilities.

Importantly, the NAS Report is not a complete security or risk assessment of an organization’s cyber risk because, among other things, the NAS Report does not account for any non-public and internal cybersecurity measures the organization has implemented to enhance their cybersecurity defenses.

The NAS Report is broken into four parts:

- Overall Score;
- Overall Score: Description;
- Individual Risk Scores; and
- Severity Breakdown.

The Overall Score

The Overall Score illustrates the organization’s overall preparedness against some of today’s cyber threats. Scores range from 0-100 with 0 being the lowest or worst score (those at the

---

\(^1\) The scans performed are passive and the scan tool does NOT directly interact with the potential policyholder’s systems or applications. There is almost no risk that these scans will negatively impact the potential policyholder’s systems and applications.
highest risk to cyberattack) and 100 being the highest or best score (those with a lower risk to a cyberattack). The Overall Score is calculated from the individual risk scores as described below.

**Overall Score: Description**

The Overall Score Description verbally translates the numerical Overall Score and identifies the range in which the Overall Score falls. While no organization is immune from a cyberattack, a score in the green zone indicates that the organization likely has taken affirmative steps to protect its Internet-facing systems and applications from cyberattacks. On the other hand, organizations in the red and black zones likely have taken only a few basic steps and are highly vulnerable to a cyberattack.

**The Individual Risk Scores**

The individual risk scores are each calculated based on a different assessment. Each of the individual risk scores contribute to the Overall Score and each provides insight into a different facet of the organization's readiness to defend against a cyberattack. The higher the score, the more resilient the organization is to a cyberattack in that area.

The following is a summary of the individual risk scores.

<table>
<thead>
<tr>
<th>Individual Risk Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Security</strong></td>
<td>This score reflects whether the organization’s servers appear on blacklists and malware lists as being flagged for containing a virus or as source of spam email. Flagged servers are typically a sign of weak perimeter defenses or poor intrusion detection, both of which indicate a much higher risk of a data breach.</td>
</tr>
<tr>
<td><strong>Network Exposure</strong></td>
<td>This score reflects the vulnerability and security of an organization’s network. The scanning tool uses the organization’s IP addresses to search the associated computer networks for unsecured ports, the presence of known security problems and discover potential bugs. The score indicates the degree to which the organization’s servers may host services that are vulnerable to cyberattacks.</td>
</tr>
</tbody>
</table>
| **Web Application Risk** | This score reflects how vulnerable the organization’s web applications are to a cyberattack.

A web application is one way an organization talks to outsiders on the Internet. The scanning tool identifies and analyzes public-facing web applications for susceptible areas involving unsupported, exploitable, or misconfigured software.

Cybercriminals use similar scanning techniques to find easy targets for cybercrime and those targets with known security weaknesses are easier to attack.

The score indicates the degree to which known vulnerabilities were discovered on the organization’s web applications. |
|---|---|
| **Web Traffic Encryption** | This score reflects whether the communications between the public and the organization’s web applications are secure through encryption.

These communications between the organization’s web application and the public often include sensitive personal, supplier, health, or financial information. Encryption scrambles those communications so that only authorized parties can read them.

The lower the score, the less secure the communications are and the more likely that sensitive data may be intercepted by hackers while in transit over the Internet. |
| **Mail Server Security** | This score shows indicates the resilience of the organization’s email server.

If an email server is not configured properly, malicious actors use it to send spam and other harmful content which will land an organization on a blacklist. The lower the score, the less resilient the organization’s email servers are and the more likely they have been subject to a cyberattack. |
Severity Breakdown

The Risk Report identifies various vulnerabilities and classifies them as High, Medium, or Low. This classification system alerts organizations to the severity of the identified vulnerabilities. Generally, organizations with an increased count of High and Medium vulnerabilities will result in a lower Overall Score. Typically, high vulnerabilities should be addressed as soon as possible to reduce the chance of a cyberattack.