ADVANCED CYBER RISK REPORT

FAQs

What is the NAS Cyber Risk Report?

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

What’s the purpose or goal of the NAS Cyber Risk Report?

The Advanced Cyber Risk Report is designed to help brokers sell NAS Cyber insurance policies by educating potential policyholders that cyber risks are real and everyone (regardless of their defenses) is susceptible to a cyber attack that may result in business interruption and significant losses.

Does the NAS Cyber Risk Report influence policy premiums or underwriting?

No. The results found in the Advanced Cyber Risk Report do not influence, positively or negatively, the policy premiums or the underwriting of the policy in any way.

How was the Advanced Cyber Risk Report created?

The Cyber Risk Report is compiled from a cyber assessment tool that performs a non-intrusive vulnerability scan of an organization’s public Internet-facing systems and applications for known vulnerabilities.

The tool also performs a comprehensive search of over 100 databases of known malware, blacklists and known cybersecurity vulnerabilities.

Is the Advanced Cyber Risk Report a complete security risk assessment?

No, the Advanced Cyber Risk Report is not a complete security risk assessment and does not reflect an organization’s overall risk to a cyber attack. For example, the Advanced Cyber Risk Report does not examine any non-public or internal cybersecurity measures the organization has implemented to enhance their cybersecurity defenses. The scan only measures the public “tip of the iceberg.”

The Advanced Cyber Risk Report is designed to educate potential policyholders on how their environment looks from the outside. Hackers may decide to take further action against a policyholder based on what the hackers can see from the outside.

Does this scan hack into a policyholder’s network?

NO! The scan only looks at publicly-accessible devices and does not attempt to access a policyholder’s network. The scan does not actively inject any information into the policyholder’s system and the scan does not impact or affect any functionality or performance of the policyholder’s systems and applications.
**Is this a penetration test?**

No. This is not a penetration test. Importantly, the scan does not try to exploit any discovered known vulnerabilities.

**Will this scan crash my client’s systems?**

The scan is designed specifically to be non-intrusive and provides almost zero risk of an adverse event to the policyholder’s system. While miniscule, however, there is always a risk of an adverse event.

**What does the Overall Score mean?**

The Overall Score is a numerical illustration of an 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 highest risk to cyberattack) and 100 being the highest or best score (those with a lower risk to a cyberattack).

**How is the Overall Score calculated?**

The Overall Score is calculated from combining and weighting the individual risk scores.

**If my client gets a good (high) score, does that mean they don’t need insurance?**

No. Regardless of the score, everyone is susceptible to a cyber attack and therefore at risk to some degree. Even organizations with excellent cybersecurity programs experience data breaches.

**What are the Individual Risk Scores?**

Each individual risk score is calculated on a different assessment of varying facets of the organization's cyber posture. The five different assessments are Domain Security, Network Exposure, Web Application Risk, Web Traffic Encryption and Mail Server Security.

**How are the Individual Scores calculated?**

The Domain and Mail Server Security are determined based on whether the potential policyholder’s domain appears in one of over 100 databases of known malware, blacklists and known cybersecurity vulnerabilities. The Network Exposure, Web Application Risk, and Web Traffic Encryption scores are based on the number and severity of the vulnerabilities that are found.

For more information, please contact Erich Falke at ePlace: efalke@eplaceinc.com 760.270.4811