

A large graphic on the right side of the page consisting of a staircase of rectangular blocks. The blocks are arranged in a descending staircase pattern from top-right to bottom-left. The colors of the blocks include dark blue, light blue, and various shades of green, some with geometric patterns or circuit-like designs.

YOUR CYBER RESILIENCE ASSESSMENT

Cybersecurity is a top concern for businesses these days. Understanding where you stand and how vulnerable you are is a critical first step in securing your business. Grab a pen and walk through this assessment for an idea of how prepared you are for a cybersecurity incident:

1.

How confident are you that in the event of a cyber breach, your insurance provider will pay the claim in full?

Answer:

1 is "What insurance provider?"

10 is "I am 100% confident my insurance provider will pay in full."

2.

In the event of a disaster or even a disgruntled employee, do you have 100% confidence that you will be able to restore all data within your organization?

Answer:

1 is "No, I do not know how data will be restored or what that looks like."

10 is "Yes, our data will be 100% restored."

3.

In the event of a server failure or internet outage, do you have a 'playbook' to ensure you can keep your employees productive?

Answer:

1 is "No, we do not have a playbook in place."

10 is "Yes, our playbook is clearly defined with roles and responsibilities in the event of a server failure."

4.

Does your current IT support team understand how your business aligns with technology and are they having regular strategic discussions to roadmap your IT budget?



1 is "No, our IT support team does not have regular alignment meetings."

10 is "Yes, our IT support team has regular meetings in regards to cybersecurity alignment and plans that into our IT budget."

5.

Does your current IT support team separate IT strategy from Cyber Security strategy?



1 is "No, we do not currently have a Cyber Security Strategy."

10 is "Yes, we have a Cyber Security team that deals with specific cybersecurity concerns."

6.

Do you know what your organizations current exposure is to a cyber attack?



1 is "No, we do not understand our cybersecurity exposure."

10 is "Yes, we continually monitor our cybersecurity gaps and actively plan to fill them."

7.

Does the company have a plan to protect and manage its cloud data, especially O365?



1 is "No, we do not currently have systems in place to protect and manage our cloud resources."

10 is "Yes, our IT Support team has a plan to protect and manage cloud data that is regularly revisited and evaluated."

8.

Does your IT support team review your cyber health position and prioritize your security initiatives?



1 is "No, we are unsure of our cyber health position."

10 is "Yes, we continually monitor and assess our cyber health positioning and prioritize our cybersecurity initiatives."

9.

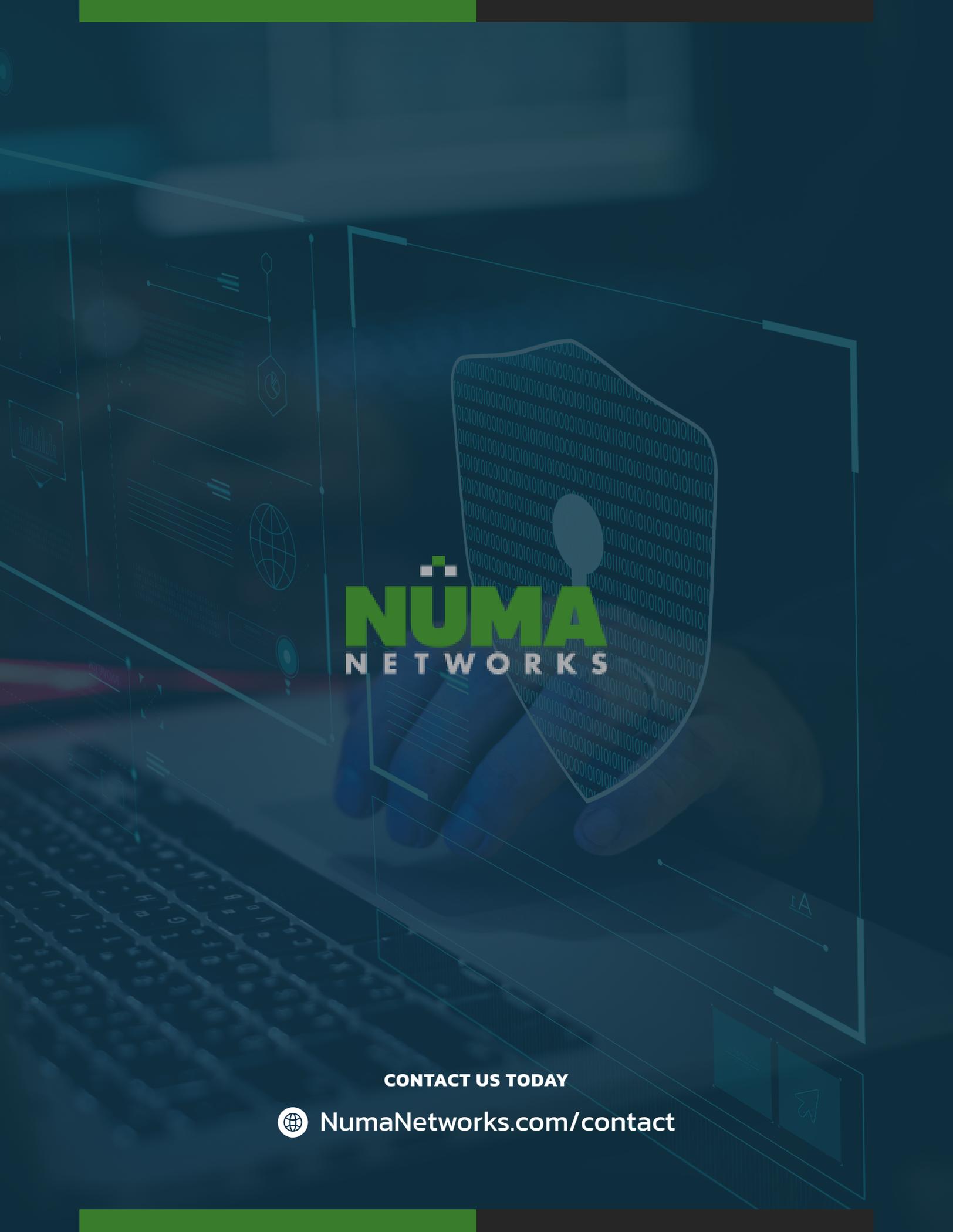
How confident are you in your cybersecurity posture?



1 is "Not confident, we need help ASAP to identify and manage our risks"

10 is "100% confidence, risks are always present but we are more than prepared!"

No matter your confidence level, if you have concerns about your cybersecurity posture and how to effectively manage risks, NUMA Networks is here to help. Call us today or visit our website for a free cybersecurity consultation.



NUMA
NETWORKS

CONTACT US TODAY



NumaNetworks.com/contact