

On the Board of Directors?

Beware of These
Six Common
Cybersecurity Myths



MYTH 1:

Cybersecurity Is Only Necessary for Some Businesses

Cybersecurity is critical for all organizations, regardless of their industry. The ongoing wave of ransomware attacks has shown that attackers are opportunistic and will target any organization that has valuable data or systems that they can exploit.



MYTH 2:

Security Software Is All You Need to Stay Safe

The effort of staying safe from cyber risk may start with getting the right tool to see it all, but it does not end there.



MYTH 3:

Software Vulnerabilities Aren't an Issue for the Board

Organizations should look to partner with security-first companies that can provide a holistic approach to security. The Boards need to understand that no amount of patching is going to negate the security risk.



MYTH 4:

You Don't Need to Worry About Supply Chain Attacks

Any other service provider can unknowingly facilitate a way into your organization's network. Ensuring you have maximal protection against digital supply chain attacks is a strategic decision that needs to be taken at the board level.



MYTH 5:

You Can't Do Anything About Cybersecurity Threats

While it is true that some threats are out of your control, there are many things you can do to protect your organization from cyber attacks. Implementing strong cyber security measures can help reduce risk.



MYTH 6:

It's Impossible to Train Employees to be Cyber Secure

While employees are a key part of any organization's cyber security strategy, they cannot be expected to be experts in cybersecurity. Organizations need to provide employees with appropriate training and resources.



Learn More
at s1.ai

