COMMON CYBERSECURITY MISCONCEPTIONS FOR SMALL AND MEDIUM-SIZED ORGANIZATIONS

CyberSecure™ MY BUSINESS

Employees empowered with the resources and knowledge to protect your organization from cyber threats is one of the best lines of defense you can have. Part of that training should involve breaking down often-quoted cybersecurity misconceptions.

BROUGHT TO YOU BY: NATIONAL CYBERSECURITY ALLIANCE

Misconception #1:
My data (or the data I have access to) isn't valuable.

All data is valuable.

Take Action: Do an assessment of the data you create, collect, store, access, transmit and then classify all the data by level of sensitivity so you can take steps to protect it appropriately.

Misconception #2:
Cybersecurity is a technology issue.

Cybersecurity is best approached with a mix of employee training; clear, accepted policies and procedures and implementation of current technologies.

Take Action: Educate every employee on their responsibility for protecting sensitive information.

Misconception #3:
Cybersecurity requires a huge financial investment.

Many efforts to protect your data require little or no financial investment.

Take Action: Create and institute cybersecurity policies and procedures, restrict administrative and access privileges, enable multi-factor authentication and train employees to spot malicious emails.

Misconception #4:
Outsourcing to a vendor washes your hands of liability during a cyber incident.

You have a legal and ethical responsibility to protect sensitive data.

Take Action: Put data sharing agreements in place with vendors and have a trusted lawyer review.

Misconception #5:
Cyber breaches are covered by general liability insurance.

Many standard insurance policies do not cover cyber incidents or data breaches.

Take Action: Speak with your insurance representative to understand your coverage and what type of policy would best fit your organization's needs.

Misconception #6:
Cyberattacks always come from external actors.

Succinctly put, cyberattacks do not always come from external actors.

Take Action: Identify potential cybersecurity incidents that can come from within the organization and develop strategies to minimize those threats.

Misconception #7:
Younger people are better at cybersecurity than others.

Age is not directly correlated to better cybersecurity practices.

Take Action: Before giving someone responsibility to manage your social media, website and network, etc., train them on your expectations of use and cybersecurity best practices.

Misconception #8:
Compliance with industry standards is sufficient for a security strategy.

Simply complying with industry standards does not equate to a robust cybersecurity strategy for an organization.

Take Action: Use a robust framework, such as the NIST Cybersecurity Framework, to manage cybersecurity risk.

Misconception #9:
Digital and physical security are separate things altogether.

Do not discount the importance of physical security.

Take Action: Develop strategies and policies to prevent unauthorized physical access to sensitive information and assets (e.g., control who can access certain areas of the office.)

Misconception #10:
New software and devices are secure when I buy them.

Just because something is new, does not mean it is secure.

Take Action: Ensure devices are operating with the most current software, change the manufacturer's default password to a unique, secure passphrase and configure privacy settings prior to use.

To view more detailed descriptions and associated resources for each misconception, visit **staysafeonline.org/cybersecure-business**